Gallagher Command Centre

Guide de l'utilisateur de Configuration Client

Volume 2

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

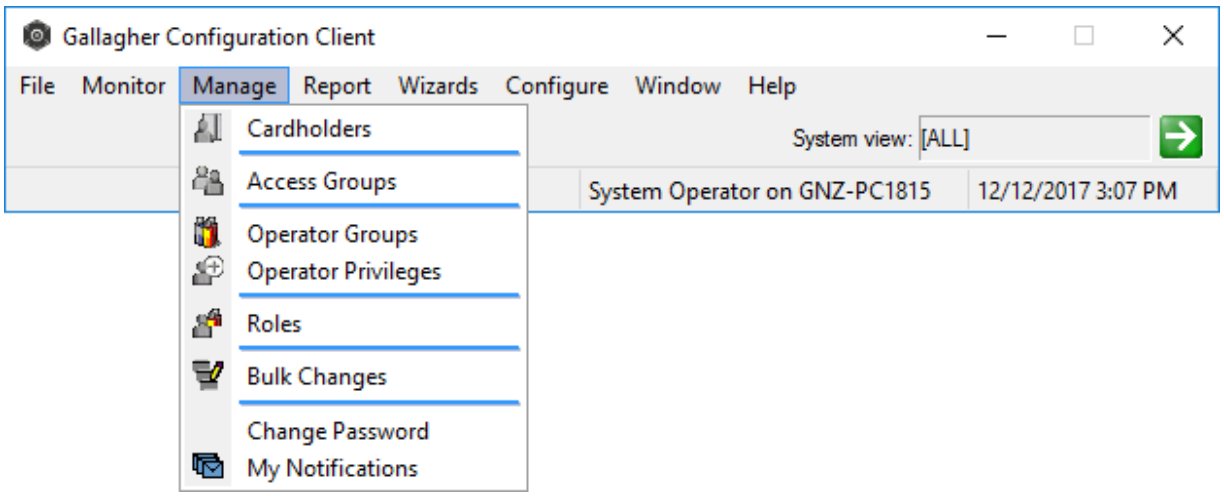
Index I-1

Partie 3 : Gestion de site

Il incombe à l'administrateur système du centre de commande de surveiller et de maintenir le matériel et les logiciels du centre de commande.

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

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



Les seules exceptions sont :

- Chapitre 33 - Champs de données personnelles, accessibles via la configuration de la barre de menus.
- Chapitre 39 - Rapports, accessible via l'option **Rapport** de la barre de menu, et
- Chapitre 40 - Archives, sauvegardes et restaurations. 'Backup' et 'Archiver' sont tous deux accessibles via l'option **Fichier de** la barre de menus, et la fonction 'Restore' s'affiche sous forme d'icône sur votre bureau (serveur uniquement, pas actuellement sur les stations de travail).

Remarque :
En fonction de vos privilèges d'opérateur ou de votre vue système actuelle, certains éléments de menu ne sont pas visibles.

Chapitre 32 : Titulaires

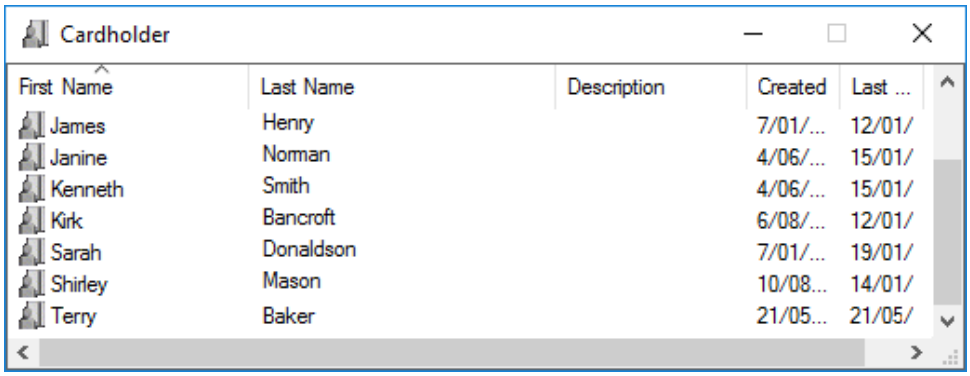
Introduction

La fenêtre Liste principale des titulaires de carte vous permet de gérer tous les titulaires de carte qui ont accès à votre site.
Vous pouvez afficher, modifier, ajouter et supprimer des titulaires de carte.

Votre licence de site déterminera le nombre de détenteurs de carte que vous pouvez avoir.

La fenêtre de la liste principale des titulaires de carte

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



Remarque :
Les opérateurs peuvent être configurés de manière à pouvoir afficher les détenteurs de cartes de n'importe quelle division du système. Bien que tous les titulaires de carte s'affichent dans la fenêtre Liste principale des titulaires de carte, les propriétés pour tous ne seront pas visibles, comme suit :

- Pour les titulaires de votre propre division, tout sera visible et modifiable.
- Pour les titulaires de carte d'une autre division, seul l'onglet **Groupes d'accès** sera visible. (Les groupes d'accès auxquels cet opérateur est affecté ne s'affichent pas s'ils sont "hors division".)

Pour plus de détails, voir ***Gestion des titulaires de carte dans les divisions*** (page 9-5).

Ajout d'un nouveau titulaire de carte

Introduction

Les détails concernant chaque personne ayant besoin d'accéder aux sites du Centre de commande doivent être définis dans le Centre de commandement.

Cette procédure se divise en deux parties :

- Création de titulaires de cartes,
  (c'est-à-dire fournir les informations minimales requises pour créer un nouveau titulaire de carte)
- Configuration d'un titulaire de carte,
  (c.-à-d., lier les différents composants à celui-ci - les types de cartes, les groupes d'accès, les groupes d'opérateurs et les champs de données personnelles sont les composants d'un titulaire de carte).

Vous pouvez créer un nouveau titulaire de carte, puis le configurer ultérieurement, une fois que vous avez configuré les composants nécessaires.
Remarque : Votre licence de site déterminera le nombre de titulaires de carte que vous pouvez avoir, donc une fois que vous avez ajouté tout ce que vous êtes autorisé, l'option de créer plus sera désactivé.

Procédure

Créer le titulaire de carte

1. Cliquez sur **Gérer** dans la barre de menu, puis sur Titulaires de carte.
   La fenêtre Liste principale des titulaires de carte s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...Titulaire de carte**.
   Par défaut, l'onglet Général s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
4. Cliquez sur le bouton **Appliquer** et le titulaire de carte est créé. Le reste de cette procédure vous permet de configurer entièrement le titulaire de carte.

Configurer le titulaire de carte

5. Assurez-vous que les informations suivantes ont déjà été configurées :

   Divisions
   Consultez la section ***Configuration de la division du système*** (page 9-3).

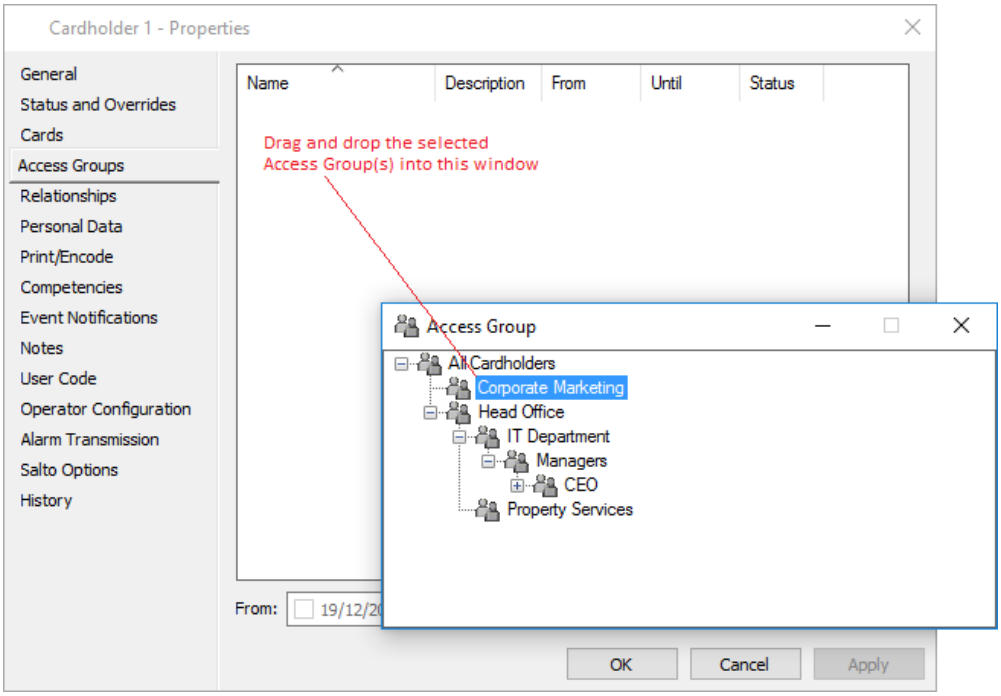
   Types de cartes
   Reportez-vous à ***Configuration des types de cartes*** (page 7-2).

   Groupes d'accès
   Reportez-vous à ***Configuration des groupes d'accès*** (page 34-4).

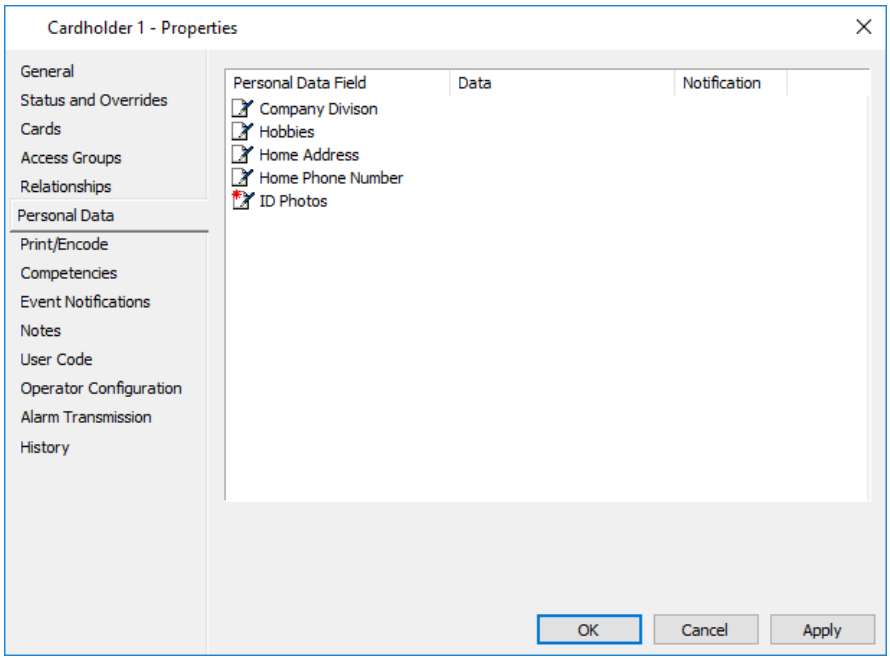
   Groupes d'opérateurs
   Reportez-vous à ***Configuration des groupes d'opérateurs*** (page 36-5).

Champs de données personnelles
Reportez-vous à la section ***Création d'un nouveau champ de données personnelles*** (page 33-2).

6. Cliquez sur l'onglet **Cartes**. (Voir ***Ajout d'une carte à un titulaire de carte*** à la page 32-9 pour la procédure)
7. Cliquez sur l'onglet **Groupes d'accès**.
8. Cliquez sur **Gérer** dans la barre de menus, puis sur **Groupes d'accès**.
   La fenêtre **Liste** principale **du groupe Access** s'ouvre.
   Sélectionnez le ou les groupes d'accès auxquels le détenteur de la carte appartiendra. Faites-les glisser et déposez-les dans l'onglet Groupes d'accès.
   Remarques :
   - Il est recommandé de ne pas affecter de titulaire de carte à plus de dix groupes d'accès, car un trop grand nombre de groupes d'accès par titulaire de carte entraînera une réponse d'accès lente. Voir ***Configurer des groupes d'accès*** (page 34-4) pour plus de détails.
   - Un détenteur de carte peut bénéficier d'un accès temporaire à un groupe d'accès. Voir Accès temporaire pour plus de détails.



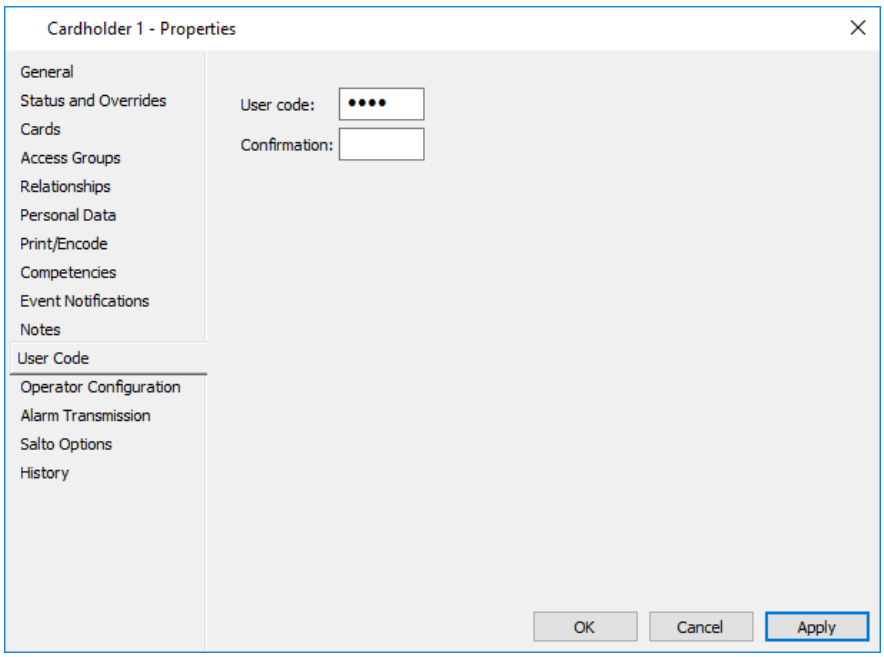
9. Fermez la fenêtre Liste principale des groupes d'accès.
10. Cliquez sur l'onglet **Données personnelles (Personal Data)**.



Voir ***Modification des données PDF des titulaires de carte*** (page 32-20) pour la procédure.

11. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou des remarques sur ce détenteur de carte.
    Remarque : En fonction de vos privilèges d'opérateur, l'onglet **Notes** peut s'afficher ou non.
    Pour plus de détails concernant l'**onglet Notes,** voir ***Notes*** (page 6-81).
12. Si des terminaux HBUS sont installés sur votre site et que ce titulaire de carte est requis pour accéder à ces terminaux, cliquez sur l'**onglet Code utilisateur**.
    Si non, passez à l'étape 15.

    Remarque : Les codes utilisateur peuvent également être utilisés comme NIP pour n'importe quel lecteur doté d'un clavier. Ceci est défini via une case à cocher dans l'onglet **Connexions** des propriétés du lecteur.



13. Entrez un code d'utilisateur à 4 ou 8 chiffres qui sera utilisé pour identifier ce détenteur de carte à un terminal HBUS.
    Remarque : Vous pouvez savoir quels titulaires de carte ont des codes utilisateur en exécutant un rapport de synthèse des titulaires de carte et en sélectionnant le champ Code utilisateur. Bien que le rapport indique qui a un code d'utilisateur, les codes réels ne seront pas divulgués.
14. Ce titulaire de carte est-il un opérateur ?
    Si **non**, passez à l'étape 15.
    Si **oui**, cliquez sur l'**onglet Configuration de l'**opérateur et consultez Configuration des opérateurs (page 36-14) de procédure.
    Remarque : L'onglet **Configuration de l'opérateur** ne s'affiche que si vous disposez des privilèges "Modifier les titulaires de carte" et "Modifier les opérateurs".
15. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Un nouveau titulaire de carte est ajouté.

Conseils

Modification et suppression des titulaires
Reportez-vous à la section ***Modification des éléments*** (page 3-26) et ***Suppression des éléments*** (page 3-27) pour connaître les procédures sur la façon de modifier et de supprimer les titulaires de carte.
Remarque : Bien qu'elles soient supprimées, les actions d'un titulaire de carte peuvent toujours apparaître dans un rapport d'activité. Consultez le ***rapport d'activité*** (page 39-15).

Copier et coller
Une alternative à la méthode glisser-déplacer consiste à utiliser la méthode copier-coller.

Copie des détails du détenteur de la carte
Pour accélérer le processus d'ajout de nouveaux titulaires de carte, les détails du nouveau titulaire de carte peuvent être copiés à partir d'un titulaire de carte existant. Voir ***Copie des détails des titulaires de carte*** (page 32-7).

Détails de la configuration de l'opérateur
Lorsqu'un administrateur système configure un détenteur de carte en tant qu'opérateur dans le Centre de commandes, il fournit à l'opérateur un nom d'ouverture de session et un mot de passe. Lorsque l'opérateur se connecte au Centre de commandes pour la première fois, il doit modifier son mot de passe. Voir ***Modification des mots de passe des opérateurs*** (page 2-16).

Fonctionnalité avancée de glisser-déplacer
Les titulaires de carte peuvent être déplacés et déposés directement de leur propre fenêtre de liste principale dans une autre fenêtre de liste principale. Voir ***Utilisation de la fonction avancée de glisser-déposer*** (page 2-24) pour plus de détails.

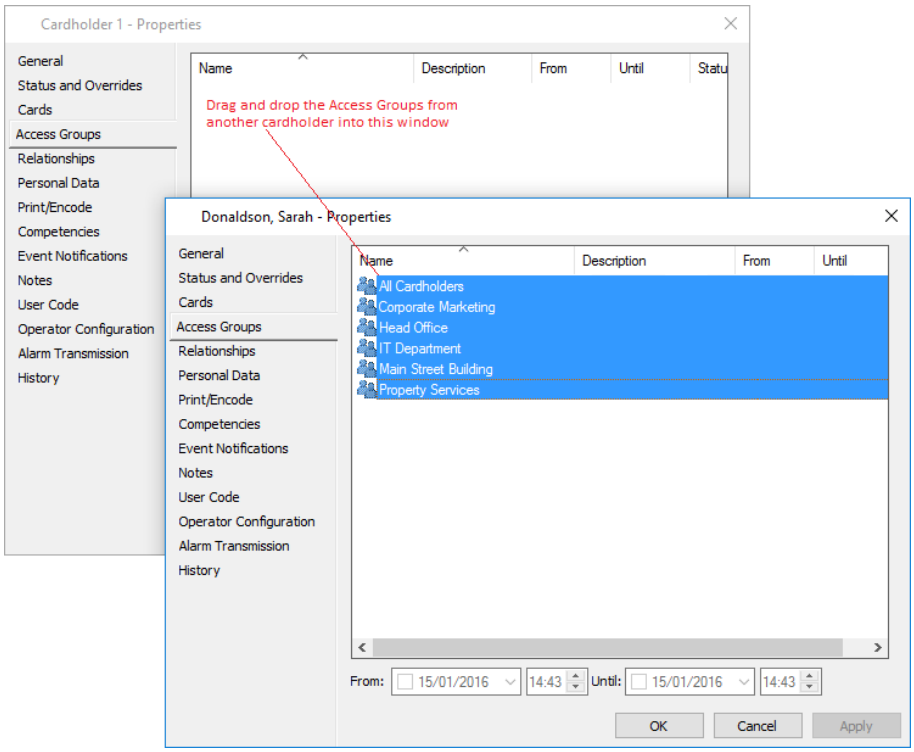
Copie des détails du titulaire de carte

Introduction

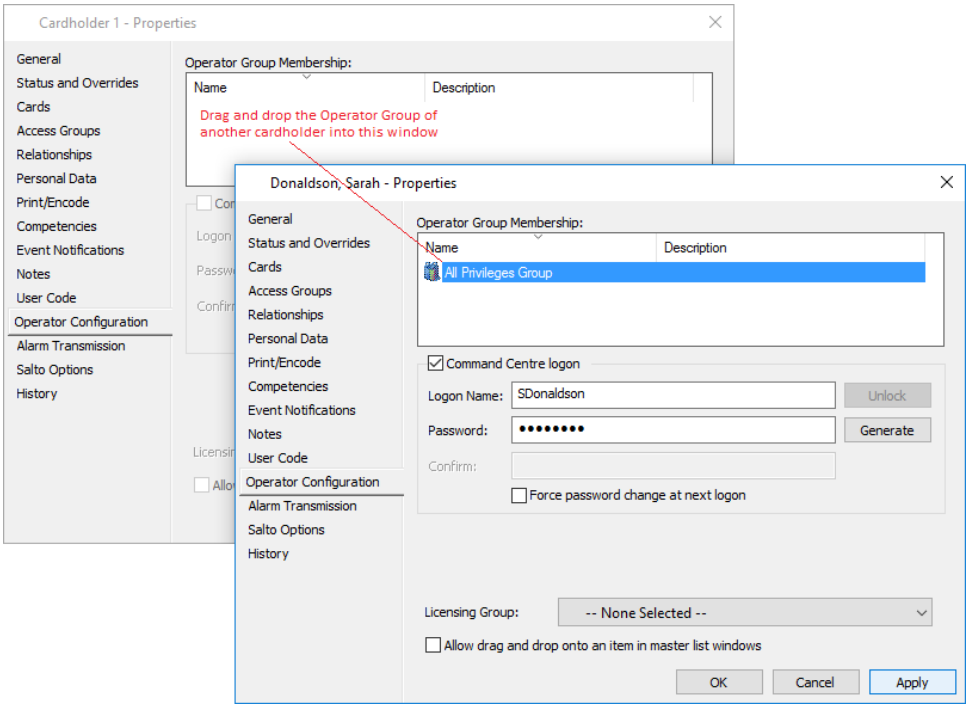
Les détails des nouveaux titulaires de carte peuvent être copiés à partir d'un titulaire de carte existant. De même, si un titulaire de carte reçoit plus d'une carte, les données doivent être dupliquées.
La copie des détails des détenteurs de cartes accélère le processus d'ajout de nouveaux détenteurs de cartes.

Procédure

1. Cliquez sur **Gérer** dans la barre de menu, puis sur Titulaires de carte.
   La fenêtre Liste principale des titulaires de carte s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...Titulaire de carte**.
   Par défaut, l'onglet Général s'affiche.
3. Entrez le nom du nouveau titulaire de la carte, une description et une division appropriées.
4. Cliquez sur l'onglet **Cartes**.
   Voir ***Ajout d'une carte à un titulaire de carte*** (page 32-9) pour la procédure.
5. Cliquez sur l'onglet **Groupes d'accès**.
6. Dans la fenêtre Liste principale des titulaires de carte, ouvrez la fenêtre Propriétés de l'existant Titulaire de carte dont vous souhaitez copier les détails.
7. Cliquez sur l'onglet **Groupes d'accès** du titulaire de la carte "existant" et sélectionnez les groupes d'accès.
   Faites-les glisser et déposez-les dans l'onglet **Groupes d'accès** du nouveau détenteur de la carte.



8. Si le titulaire de la carte est un opérateur, cliquez sur l'onglet **Configuration de l'opérateur**. Sinon, passez à l'étape 10.
9. Dans la fenêtre Propriétés du titulaire de carte "existant", cliquez sur l'**onglet Configuration de l'opérateur** et sélectionnez le groupe d'opérateurs. Faites-le glisser et déposez-le dans l'onglet **Configuration de l'opérateur** du nouveau titulaire de carte.



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

Résultat

Un nouveau titulaire de carte, avec des détails copiés d'un titulaire de carte existant, est ajouté.

Ajout d'une carte à un titulaire de carte

Introduction

Une carte est un jeton d'accès. Le titulaire de la carte présente la carte à un lecteur pour avoir accès à une zone ou un ascenseur.

Un titulaire de carte peut se voir délivrer plusieurs cartes ; par exemple, ils nécessitent l'accès à différents sites.

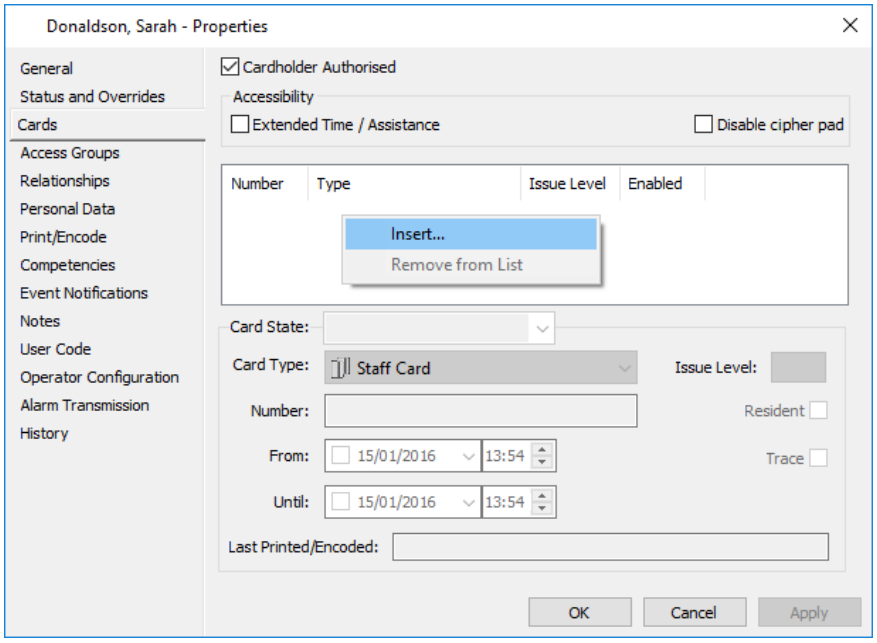
Remarque : La limite par défaut est de 500 cartes par titulaire.

Procédure

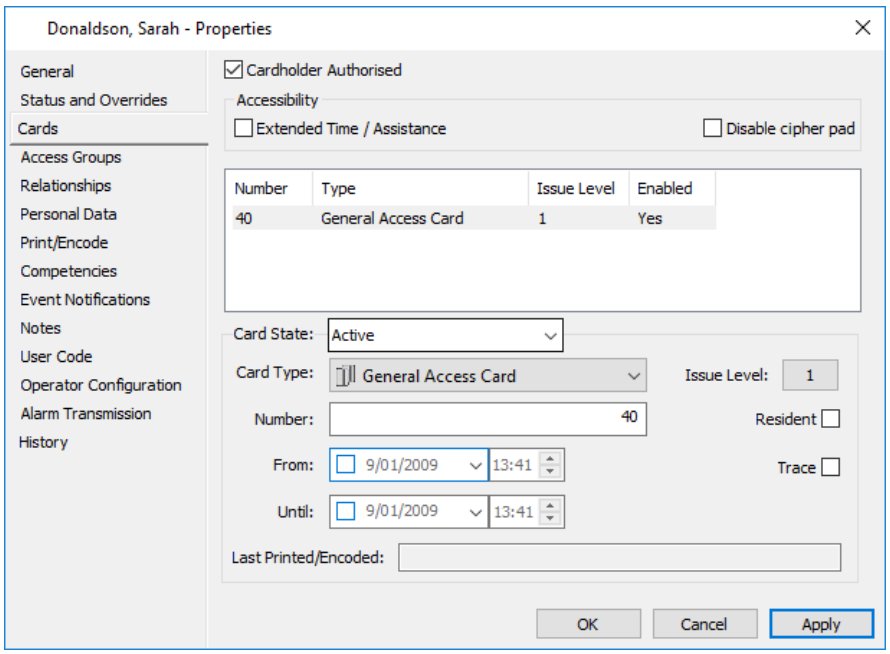
1. Cliquez sur **Gérer** dans la barre de menu, puis sur Titulaires de carte.
   La fenêtre Liste principale des titulaires de carte s'ouvre (en mode grille).
2. Localisez et mettez en surbrillance le détenteur de carte à modifier.
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Cartes**.
   La case **Titulaire autorisé** est cochée par défaut. Cela autorise le titulaire de la carte à utiliser ses cartes. Ce n'est pas spécifique à une carte - il autorise l'utilisation de toutes les cartes répertoriées.
5. Activez les fonctions d'accessibilité comme requis :

Option	Description
Temp étendu / Assistance	L'activation de case à cocher permet à une porte de rester déverrouillée plus longtemps que la normale. Si ce titulaire de carte nécessite cette fonctionnalité, reportez-vous à la section ***Configuration du temps d'accès étendu pour une porte*** (page 22-13) pour obtenir des instructions sur la façon de configurer cette fonctionnalité.
Désactivé pave chiffrement	Pour plus de sécurité, les terminaux T20 et/ou T21 lecteur clavier peuvent être configurés comme chiffriers pour Carte + PIN (sur la page de propriétés Avancé), afin que chaque fois qu'un utilisateur badge sa carte le pavé numérique aléatoire s'affiche sur écran terminal/lecteur. Cette fonctionnalité n'est pas adaptée à la pour les détenteurs de carte avec la vue déficientes. Par conséquent, si la case cette carte-est malvoyant est lorsqu'ils présenteront leur carte, ils reviendront à un clavier normal.

6. **Faites un clic droit** n'importe où dans la grille supérieure (c'est-à-dire sur un en-tête de colonne, sur la barre de défilement, dans la zone vide ou sur une carte s'il y en a une), et sélectionnez **Insérer**.



Une "nouvelle carte" est ajoutée à la grille supérieure et mise en surbrillance. Cette nouvelle carte est activée et, si les paramètres par défaut de la carte ont déjà été configurés (voir Configuration des types de carte), les champs "De", "Jusqu'à" et/ou "Niveau d'émission" seront renseignés avec ces paramètres par défaut. La carte sera également attribuée au prochain numéro disponible.



7. Est-ce que la "nouvelle carte" est le type de carte requis ?

Si...	**alors...**
oui	passez à l'étape 7.
non	cliquez **maintenant sur la** zone de menu déroulant **Type de carte (Card Type)** et sélectionnez le type de carte correct. Par exemple, carte de proximité, carte mag-stripe, etc. **Remarque :** Les paramètres par défaut sont modifiés en celui de la carte sélectionnée.

8. Définissez les détails de la carte restante.
   Remarque : Si les champs "De", "Jusqu'à" et/ou "Niveau d'émission" sont renseignés avec les paramètres par défaut, ils peuvent être remplacés si nécessaire. Le numéro de la carte peut également être écrasé avant d'enregistrer les modifications.

   État de la carte
   Chaque carte nécessite un état actuel. L'état sélectionné initialement est configuré à partir de l'ensemble d'états de carte du type de carte et la liste déroulante est remplie avec tous les états de carte qui sont disponibles.

   Nombre
   Chaque carte nécessite un numéro codé pour l'identifier de manière unique. Une fois que vous cliquez sur **Appliquer**, le numéro de la carte devient grisé et ne peut pas être modifié. La plage de numéros de carte pouvant être affectée à un type de carte est définie dans les propriétés Type de carte. Le format du numéro de carte du type de carte sélectionné détermine quels caractères peuvent être utilisés, comme suit :

Si le type de carte est...	alors...
Format **décimal**,	une plage de cartes décimales est prise en charge. Le système "alloue automatiquement" un numéro de carte, mais il peut être écrasé si nécessaire en tapant un autre numéro sur celui alloué avant d'enregistrer les modifications sur cet écran.
Format **du texte**,	si une chaîne de syntaxe d'expression régulière a été configurée dans les propriétés Type de carte, vous serez obligé d'entrer un numéro de carte correspondant à cette définition. **Remarques :** • un maximum de 251 caractères alphanumériques sont pris en charge. Cependant, avec certaines langues, cela peut être moins, car certains caractères utilisent plus d'un octet. • Si vous entrez un numéro de carte non valide, un message d'erreur s'affiche pour indiquer qu'il n'est pas valide et montrer le modèle de chaîne de syntaxe.

   De
   Définissez la date et l'heure d'activation de la carte - le système du Centre de commande accepte les détails de la carte.
   Remarque : Si vous n'entrez pas de date dans le champ "De", lorsqu'un titulaire de carte reçoit une carte de ce type et que la carte est activée, l'activation sera immédiate.

   Jusqu'à
   Définissez la date et l'heure d'expiration de la carte - le système du Centre de commande n'acceptera pas la carte après cette date.
   Remarque : Si vous n'entrez pas de date dans ce champ, la carte n'expire pas.

Niveau de la question (1 à 15)
Si une carte est remplacée, vous n'avez pas besoin de passer par le processus de création d'une nouvelle carte ; vous pouvez simplement incrémenter le numéro de émission. Une carte peut devoir être remplacée si le titulaire de la carte a perdu sa carte, par exemple.

Résident
Cochez cette case si vous souhaitez que les détails de ce titulaire de carte soient stockés (résident) au Contrôleur.

Le contrôleur stocke une base de données de paramètres de sécurité et de détenteur de carte "résident" pour lui permettre d'effectuer des fonctions de contrôle d'accès et de sécurité. La base de données des détenteurs de cartes stocke les données d'accès des détenteurs de cartes qui utilisent régulièrement les appareils reliés à ce contrôleur. Il permet au contrôleur de prendre des décisions de contrôle d'accès instantanément.

Pour les titulaires de carte qui ne sont pas inclus dans la base de données des titulaires de carte résidents, lorsqu'ils présentent leur carte, le contrôleur demande des informations d'accès au Centre de commande. Leurs informations sont alors stockées dans la base de données résidente, mais peuvent être ignorées si la base de données des titulaires de cartes contrôleur devient pleine et qu'un autre utilisateur inconnu présente sa carte. Si les communications échouent et que les informations sur le titulaire de la carte ne figurent pas dans le contrôleur, ce titulaire ne pourra pas avoir accès.

Suivi
Un message et/ou une alarme est généré chaque fois que la carte est présentée à un lecteur, y compris les lecteurs associés aux terminaux d'armement à distance.

Dernière impression/encodage
Champ en lecture seule affichant les informations "Dernière impression/Encodé" (c'est-à-dire la date de la dernière impression et/ou encodage et le niveau d'émission utilisé), pour la carte actuellement sélectionnée.

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.

   Remarques :
   - Lorsque vous enregistrez les modifications à ce stade, selon la date d'expiration définie pour la carte, un événement "carte activée" ou "carte expirée" peut être enregistré dans la fenêtre **Événement**.
   - Une fois que vous avez enregistré vos modifications, les champs Type de carte et Numéro deviennent grisés et ne peuvent pas être modifiés.

Résultat

Les détails de la nouvelle carte sont mis à jour pour refléter les changements que vous avez apportés.

Indication

Il ne peut pas y avoir deux cartes dans le système avec le même numéro de carte *et* le même type de carte.

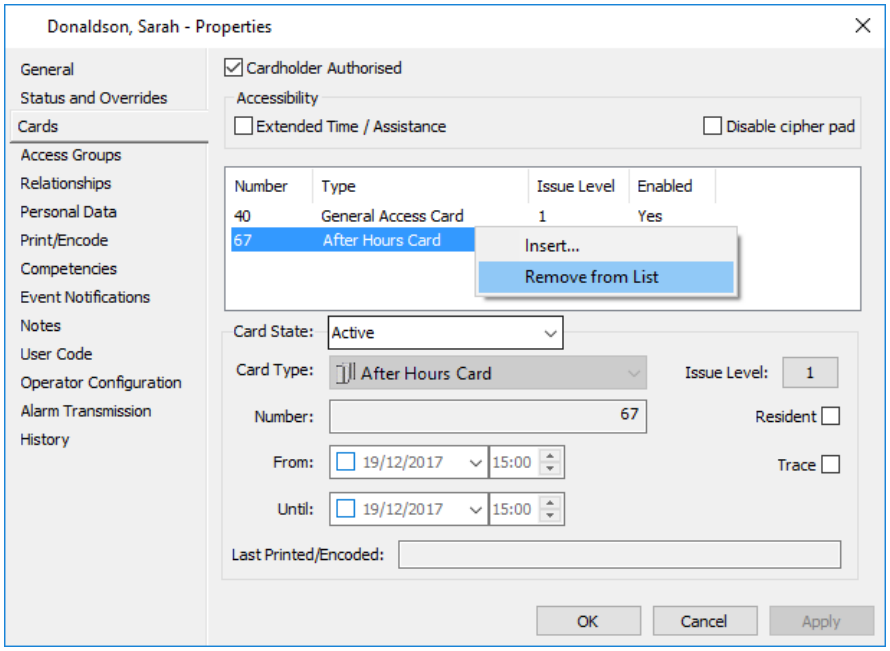
Retrait d'une carte d'un titulaire de carte

Introduction

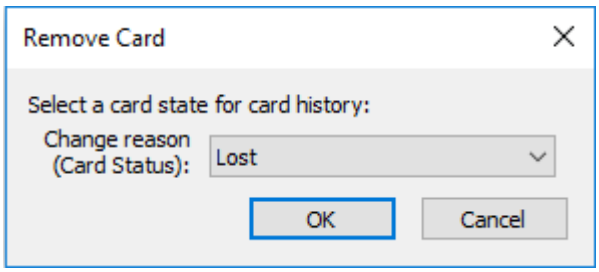
Lorsqu'une carte n'est plus nécessaire, elle peut être retirée de la liste des détenteurs de cartes.

Procédure

1. Cliquez sur **Gérer** dans la barre de menu, puis sur Titulaires de carte.
   La fenêtre (en mode grille) s'ouvre dans la liste principale des **titulaires de carte**.
2. Localisez le porte-carte à modifier et mettez-le en surbrillance.
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Cartes**.
5. Cliquez sur la carte que vous souhaitez supprimer.
6. **Cliquez avec le bouton droit** de la souris et sélectionnez **Supprimer de la liste**.



Une fenêtre contextuelle Supprimer la carte s'affiche.



7. Sélectionnez l'état de la carte approprié pour l'historique de la carte (par exemple Perdu, Endommagé, etc.) dans la liste déroulante **Motif de modification (Statut de la carte)** des états disponibles.

8. Cliquez sur le bouton **OK**.
   La fenêtre contextuelle Supprimer la carte se ferme et la carte disparaît de la liste des cartes de la grille supérieure.
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

Les détails de la carte sont supprimés.

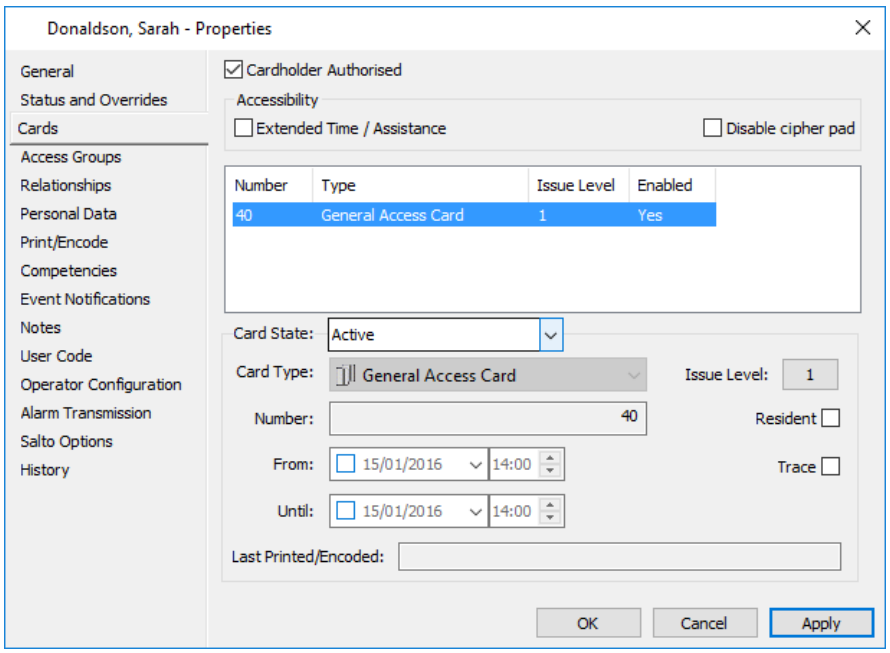
Modification des détails de la carte

Introduction

Vous devrez peut-être modifier les détails de la carte pour un titulaire de carte particulier. Par exemple, une carte de remplacement est remise à un titulaire de carte et vous devez modifier le numéro de délivrance de la carte.

Procédure

1. Cliquez sur **Gérer** dans la barre de menu, puis sur Titulaires de carte.
   La fenêtre Liste principale des titulaires de carte s'ouvre (en mode grille).
2. Localisez le porte-carte à modifier et mettez-le en surbrillance.
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Cartes**.



5. Sélectionnez la carte qui nécessite une modification.
6. Modifiez les informations de la carte selon les besoins.
   Pour plus de détails sur les champs, consultez la section ***Ajout d'une carte à un titulaire de carte*** (page 32-9).
7. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
   Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
   Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Les détails de la carte sont mis à jour pour refléter les modifications que vous avez apportées.

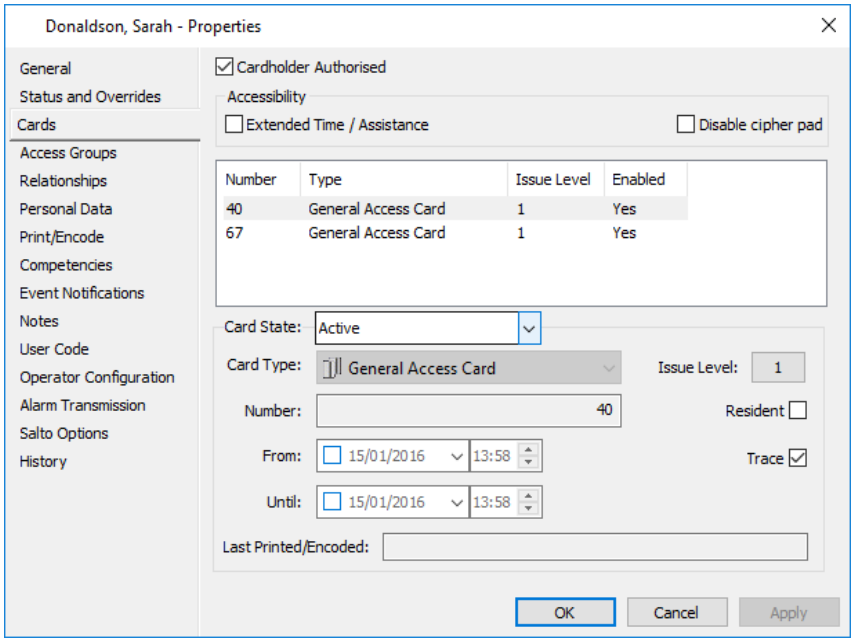
Activation du suivi de la carte

Introduction

Lors de l'ajout d'un nouveau titulaire de carte ou de la modification de données de titulaire de carte dans le Centre de commandes, vous pouvez spécifier qu'une "trace de carte" doit être placée sur le titulaire de carte. Cela déclenchera une alarme chaque fois que le détenteur de la carte présente sa carte d'accès ou son jeton.
Remarque : Le paramètre d'événement par défaut des alarmes de suivi de carte peut être modifié via l'onglet **Event Defaults (Valeurs par défaut des événements)** des propriétés du serveur du Centre de commandes (voir ***Event Defaults (Valeurs par défaut des événements)*** à la page 6-12.

Procédure

1. Cliquez sur **Gérer** dans la barre de menu, puis sur Titulaires de carte.
   La fenêtre Liste principale des titulaires de carte s'ouvre (en mode grille).
2. Repérez le support de la carte que vous souhaitez tracer et mettez-le en surbrillance.
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Cartes**.



5. Mettez la carte appropriée en surbrillance en cliquant dessus.
6. Cochez la case **Trace**.
7. Répétez les étapes 5 à 6 pour appliquer la trace de la carte à d'autres cartes d'accès appartenant à ce détenteur de la carte si nécessaire.
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

Card Trace a été appliqué à la carte du titulaire de la carte.

Réactivation des cartes périmées ou désactivées

Introduction

Lorsqu'une carte a expiré, un message approprié s'affiche en rouge sur le **Cartes** onglet de la carte, selon ce qui a causé l'expiration, comme suit :

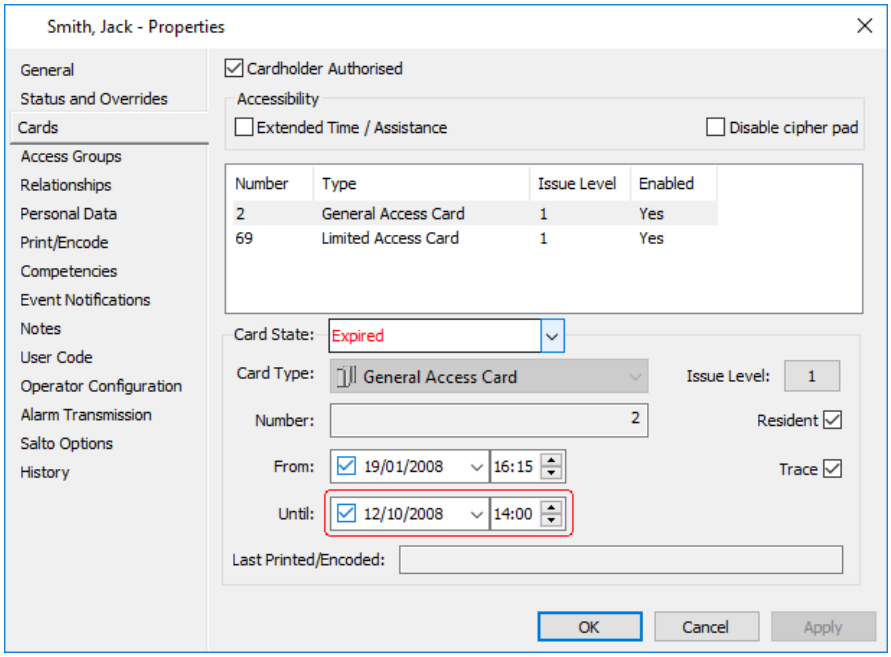
- **Expiration programmée de la carte**
  La durée de vie d'une carte a été spécifiée en définissant une date et une heure "de" et une date "jusqu'à" et une date.
- **Expiration de la carte inactive**
  Une carte est désactivée après une période d'inactivité spécifiée.

La procédure suivante décrit la réactivation des cartes périmées.

Procédure

Expiration programmée de la carte

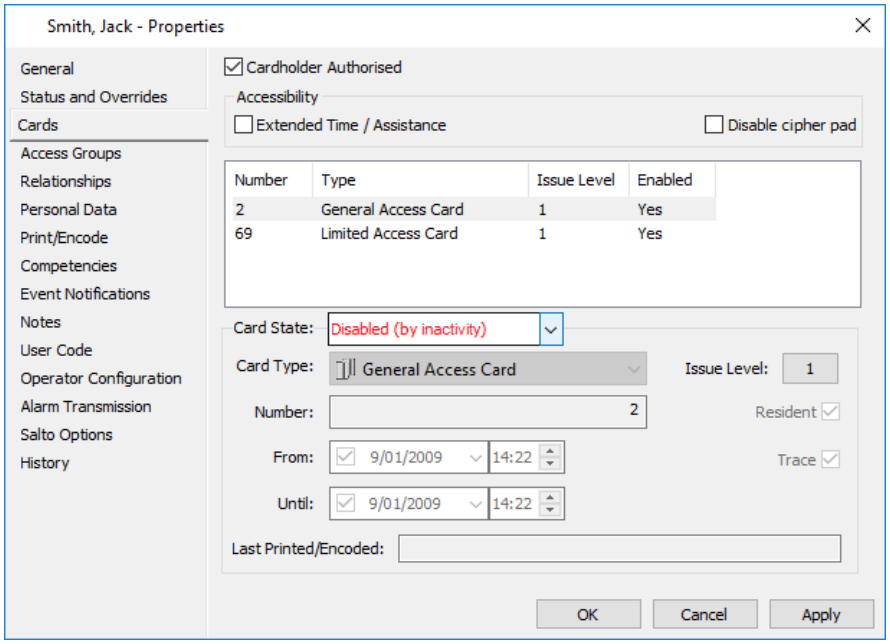
1. Ouvrez l'onglet **Cartes** du titulaire de carte.
2. Mettez en surbrillance la carte qui a expiré (c'est-à-dire que la date de la colonne "Jusqu'à" est passée).
   Le message Expiré **(en** texte rouge) remplit le **champ État de la carte**.



3. Prolongez les dates "De" et/ou "Jusqu'à" et/ou les heures selon les besoins.
4. Cliquez sur **Appliquer**.
   Le message dans le champ **État de la carte** passe de **Expiré** (en texte rouge) à **Actif** (en texte noir). La carte est réactivée.
   Remarque : Si vous étendez la date et/ou l'heure "De" à quelque chose dans le futur, le message **Expiré** changera en **Pas encore activé** (en texte bleu) une fois **que vous cliquerez sur Appliquer**.

Expiration de la carte inactive

1. Ouvrez l'onglet **Cartes** du titulaire de carte.
2. Mettez en surbrillance la carte qui n'est pas activée (c'est-à-dire la carte dont le numéro figure dans la colonne "Activé").
   Le message **Désactivé (par inactivité)** (en texte rouge) remplit l'état de la carte s'affiche.



3. Sélectionnez l'état actif dans la liste déroulante État de la carte.
4. Cliquez sur **Appliquer**.
   Le message dans le champ **État de la carte** change de **Désactivé (par inactivité)** (en texte rouge) **Actif** (en texte noir). La carte est réactivée.

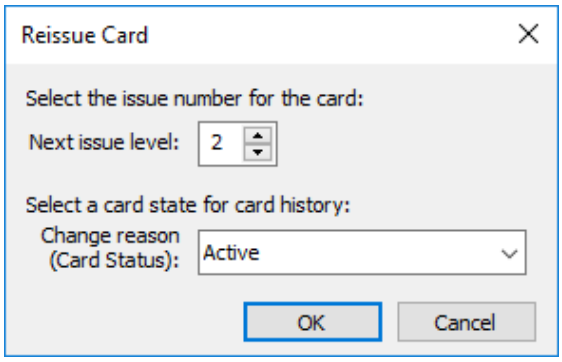
Réémission d'une carte pour un titulaire de carte

Introduction

Si une carte est remplacée, vous n'avez pas besoin de passer par le processus de création d'une nouvelle carte ; vous pouvez simplement incrémenter le numéro d'émission à partir des propriétés Titulaire de carte.
Une carte peut devoir être remplacée si le titulaire de la carte a perdu sa carte, par exemple.

Procédure

1. Cliquez sur **Gérer** dans la barre de menu, puis sur Titulaires de carte.
   La fenêtre (en mode grille) s'ouvre dans la liste principale des **titulaires de carte**.
2. Localisez le porte-carte à modifier et mettez-le en surbrillance.
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Cartes**.
5. Cliquez sur la carte que vous souhaitez réémettre.
6. Cliquez sur le bouton **Niveau d'émission (Issue Level)**.
   La fenêtre contextuelle Carte de réédition s'affiche.



7. Le niveau d'émission de la carte doit être incrémenté d'un.
   Vérifiez que le nombre par défaut dans le **champ** Prochain **niveau d'émission** est correct.
8. Sélectionnez la raison appropriée pour laquelle vous réémettez la carte (par exemple, Perdu, Endommagé, etc.) dans la liste déroulante **Changer** le **motif (Statut de la carte)** des états de la carte disponible.
9. Cliquez sur le bouton **OK**.
   La fenêtre contextuelle Carte de réémission se ferme et le numéro du bouton **Niveau d'émission** a été incrémenté d'un.
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

La carte a été réémise.

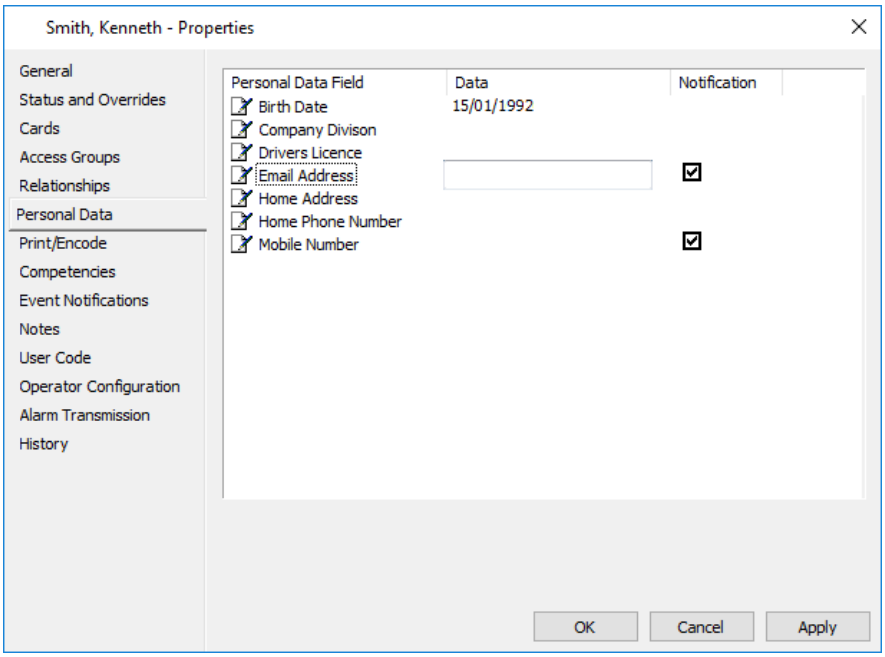
Modification des données d'un titulaire de carte PDF

Introduction

Cette procédure vous permet d'entrer les données personnelles d'un titulaire de carte dans les champs de données personnelles (PDF).

Procédure

1. Cliquez sur **Gérer** dans la barre de menu, puis sur Titulaires de carte.
   La fenêtre Liste principale des titulaires de carte s'ouvre (en mode grille).
2. Localisez le porte-carte à modifier et mettez-le en surbrillance.
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Données personnelles (Personal Data)**.
   Remarque : Si un groupe d'accès contenant des fichiers PDF a été affecté à ce titulaire de carte, les fichiers PDF associés au groupe d'accès s'affichent ici. Sinon, la grille sera vide.
5. **Faites un clic droit** sur la section des données du PDF que vous souhaitez saisir les données des détenteurs de carte contre.
   Le champ Saisie de données est activé pour ce fichier PDF.



Remarque : Les champs de données personnelles dont l'accessibilité est "Révélable" ou "Révélable et modifiable" affichent - - Cliquer pour révéler - - dans le champ de saisie des données. Cette accessibilité est définie dans l'onglet Type des propriétés du champ de données personnelles. du champ de données personnelles.



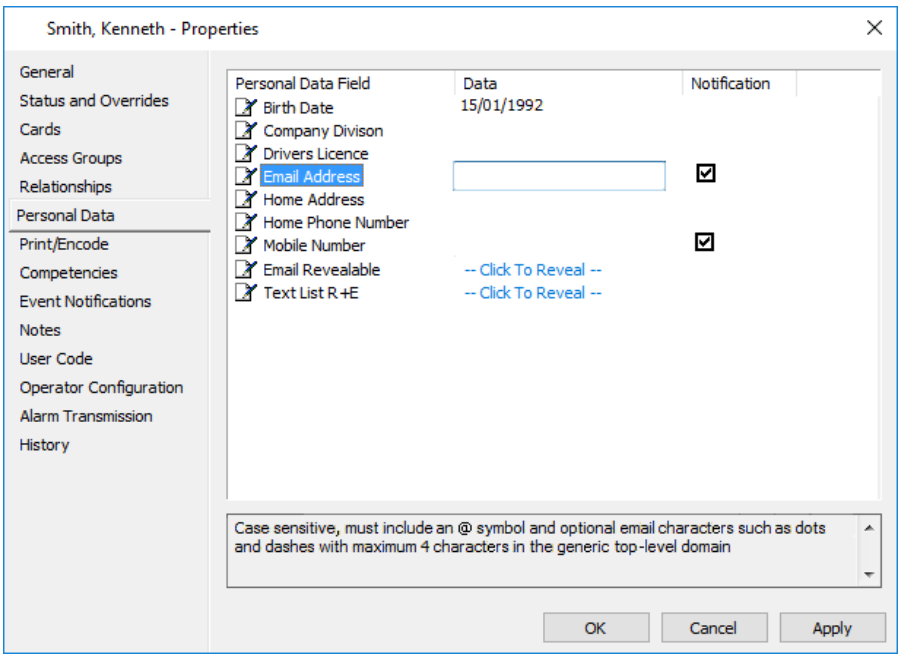
Avec les privilèges appropriés, les opérateurs peuvent soit visualiser, soit créer et modifier la valeur d'un champ de données personnelles en cliquant sur - - Cliquer pour révéler - -, puis en cliquant sur le bouton Reveal qui s'affiche.

La case à cocher Notifications par défaut sera révélée lorsque le bouton Révéler sera actionné (c.-à-d.qu'il s'agit d'un espace vide jusqu'à ce que cela se produise).



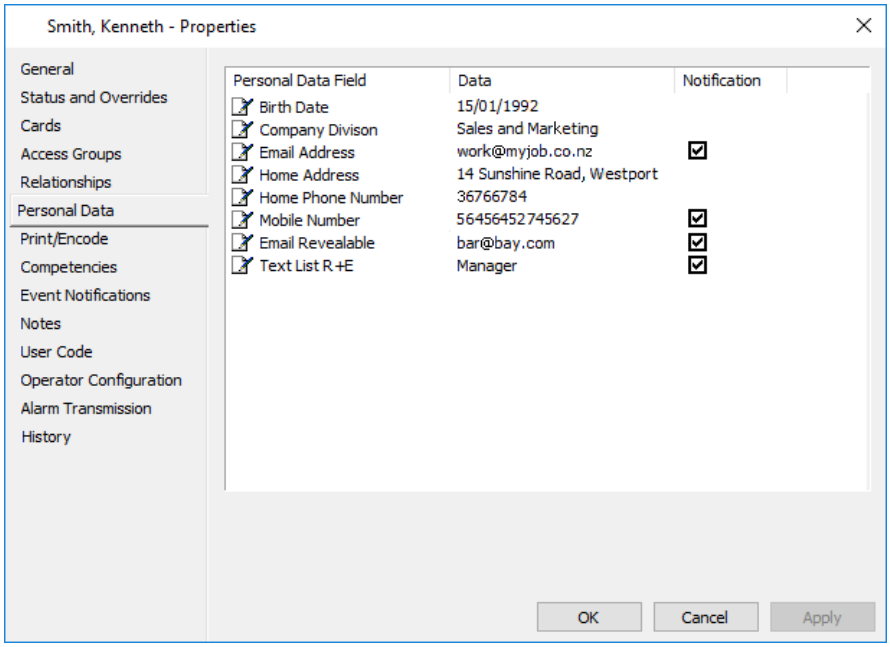
Pour plus de détails concernant l'accessibilité "Révélable" et "Révélable et modifiable" et les privilèges d'opérateur requis, voir ***Création d'un nouveau champ de données personnelles*** (à la page 33-2).

6. Entrez les données personnelles appropriées.
   Remarques :
   - Les images (logos d'entreprise, photos des détenteurs de cartes, etc.) peuvent être capturées et utilisées pour les PDF "Image". Reportez-vous à Capturer une image pour la procédure.
   - En cliquant sur un PDF "Date", un contrôle Date apparaît. Aucune valeur de date n'est attribuée si la case à cocher n'est pas cochée.
     Une date doit être fournie pour les fichiers PDF requis.
   - En cliquant sur un PDF "Texte - Liste", une liste déroulante prédéfinie apparaît. S'il s'agit d'un PDF **restreint** "Texte - Liste", un détenteur de carte ne peut avoir que des valeurs remplies à partir de la liste prédéfinie, ou une valeur vide. Cependant, si elle est **illimitée**, l'entrée de texte libre est autorisée.
   - La colonne **Notification** contient une case à cocher uniquement pour les PDF de type "Mobile" et "Email". Lorsque ces cases à cocher sont cochées, cela indique que la valeur PDF est utilisée dans la fonction Notifications pour l'envoi et la réception de notifications, (i.e. "Mobile" pour les SMS et "Email" pour les notifications par e-mail).
   - En cliquant sur un "Texte" type PDF, ou n'importe quel type de contact PDF, (i.e. "Adresse", "Téléphone", "Courriel" ou "Mobile"), une zone de texte apparaît en bas pour décrire la syntaxe de l'expression régulière si la **fonction** Utiliser l'**expression** régulière a été activée et définie sur l'onglet Type du PDF.



Remarque : Lors de l'application des modifications, un message d'erreur s'affiche pour indiquer que les données PDF entrées ne correspondent pas à la syntaxe de l'expression régulière.

7. Répétez les étapes 5 à 6 pour chaque document PDF.



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

Le titulaire a maintenant des données personnelles enregistrées au format PDF.

Configuration d'un code utilisateur pour l'accès Terminal

Introduction

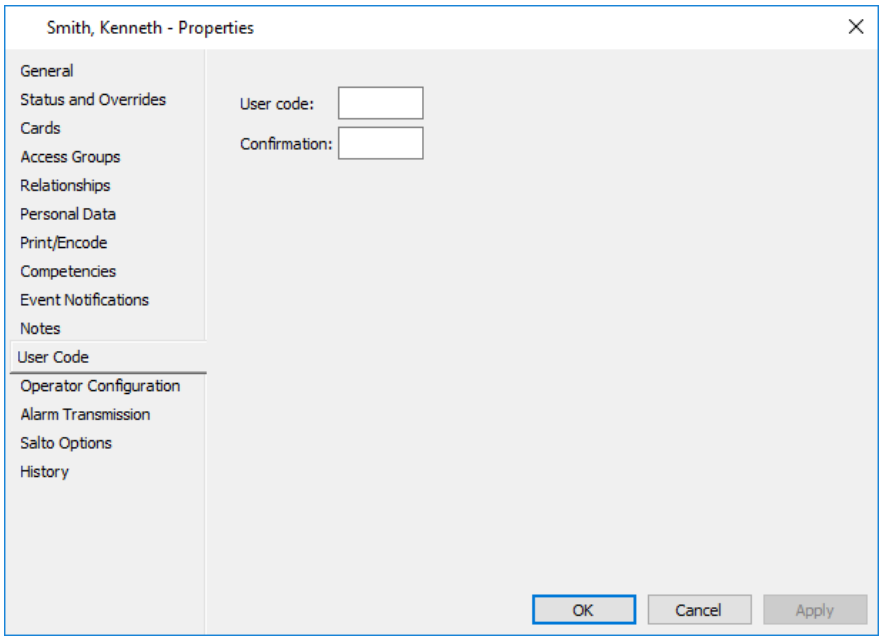
Cette procédure décrit comment spécifier un code utilisateur pour un titulaire de carte, afin d'identifier le titulaire de carte dans un terminal HBUS ou un terminal HBUS Alarms Only.

Les opérateurs ont besoin du privilège de l'opérateur "Modifier les titulaires de carte" et doivent être dans la même division ou une division parente du titulaire de carte. Sans ce privilège d'opérateur, les champs de cet onglet ne seront pas activés.

Remarque : Les codes d'utilisateur peuvent également être utilisés comme NIP pour tout lecteur doté d'un clavier. Cette option est activée via une case à cocher sur l'onglet Avancé des propriétés du lecteur.

Procédure

1. Cliquez sur **Gérer** dans la barre de menu, puis sur Titulaires de carte.
   La fenêtre Liste principale des titulaires de carte s'ouvre (en mode grille).
2. Mettez en surbrillance le titulaire de carte **auquel vous** souhaitez donner un code d'utilisateur.
3. **Double-cliquez sur** le bouton de la souris.
4. Cliquez sur l'onglet **Code utilisateur (User Code)**.



Remarque : Ce code sera masqué de tous les opérateurs, indépendamment des privilèges.

5. Entrez un code d'utilisateur de 4 à 8 chiffres dans le champ Code d'utilisateur.
   Remarques :
   - Lorsque vous entrez le code utilisateur, des astérisques s'affichent à la place de chaque chiffre.

- Le Centre de commandes applique une plage de codes utilisateur comprise entre 1 et 99999999. Par conséquent, le code doit contenir au moins un chiffre différent de zéro (par exemple, 0000 ou 000000000 sont non valides et une erreur sera générée).

6. Confirmez le code utilisateur en le saisissant à nouveau dans le **champ Confirmation**.
7. Cliquez sur **Appliquer**.

Résultat

Un code utilisateur a été spécifié pour identifier un titulaire de carte dans un terminal HBUS ou un terminal HBUS Alarms Only.

Configuration des codes utilisateur pour l'accès aux lecteurs de cartes à l'aide de claviers

Introduction

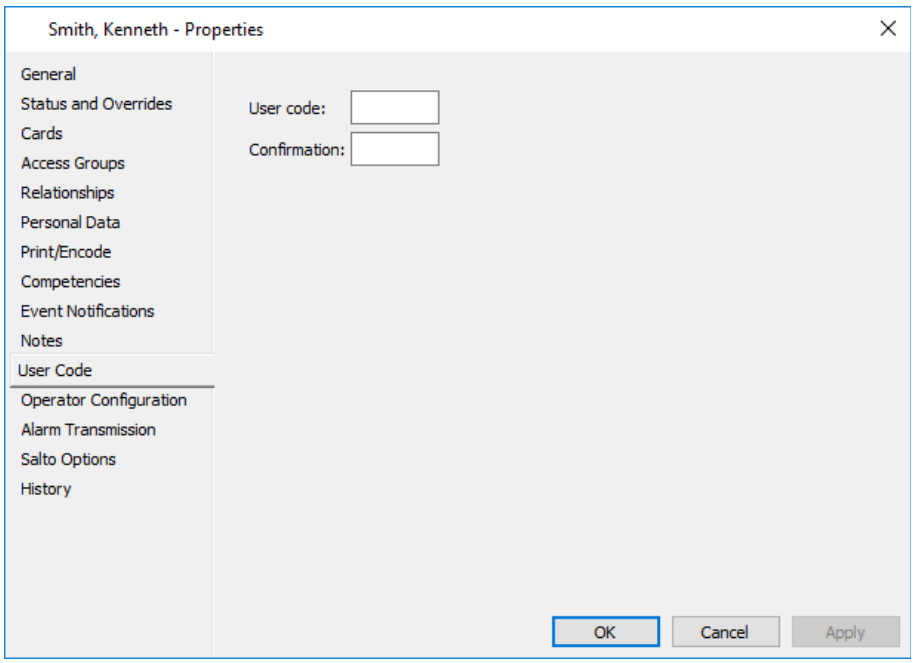
Les codes utilisateur peuvent être configurés, à la place des codes PIN, pour accéder aux lecteurs de cartes avec des pavés clavier (c'est-à-dire les lecteurs Gallagher et les lecteurs tiers qui sont pris en charge par Command Center).

Restrictions

- Le mode "Code ou Carte - NIP" ne fonctionne pas pour le mode Code utilisateur uniquement. Le mode de la zone d'accès doit être "Code ou Carte - Pas de NIP" pour que cette fonction fonctionne correctement.
- Cette fonctionnalité ne prend pas en charge.
- Le code Access Zones Code Only n'autorise pas l'accès lorsque le lecteur est configuré avec l'activation du code confidentiel. L'accès ne peut être accordé que par entrée de code d'utilisateur ou par une carte valide.
- La longueur maximale du code utilisateur accepté est de 6 chiffres.
- Les remplacements de double carte ne sont pas pris en charge.

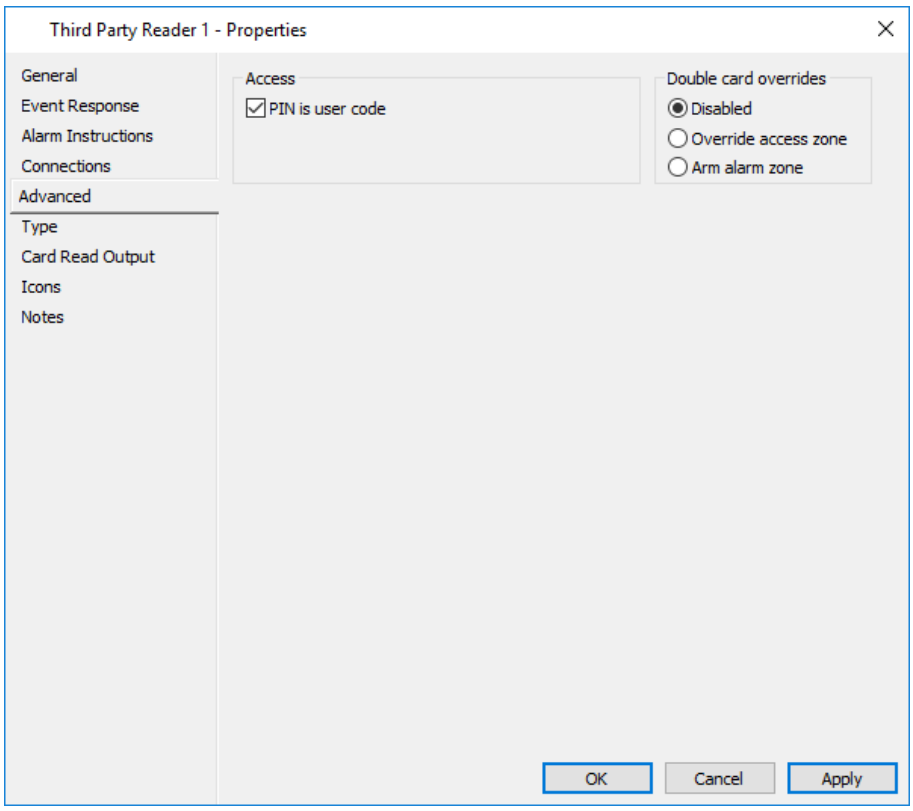
Procédure

1. Cliquez sur **Gérer** dans la barre de menu, puis sur Titulaires de carte.
   La fenêtre Liste principale des titulaires de carte s'ouvre (en mode grille).
2. Mettez en surbrillance un titulaire de carte qui nécessite l'accès via le lecteur.
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Code utilisateur (User Code)**.



Remarque : Ce code sera masqué de tous les opérateurs, indépendamment des privilèges.

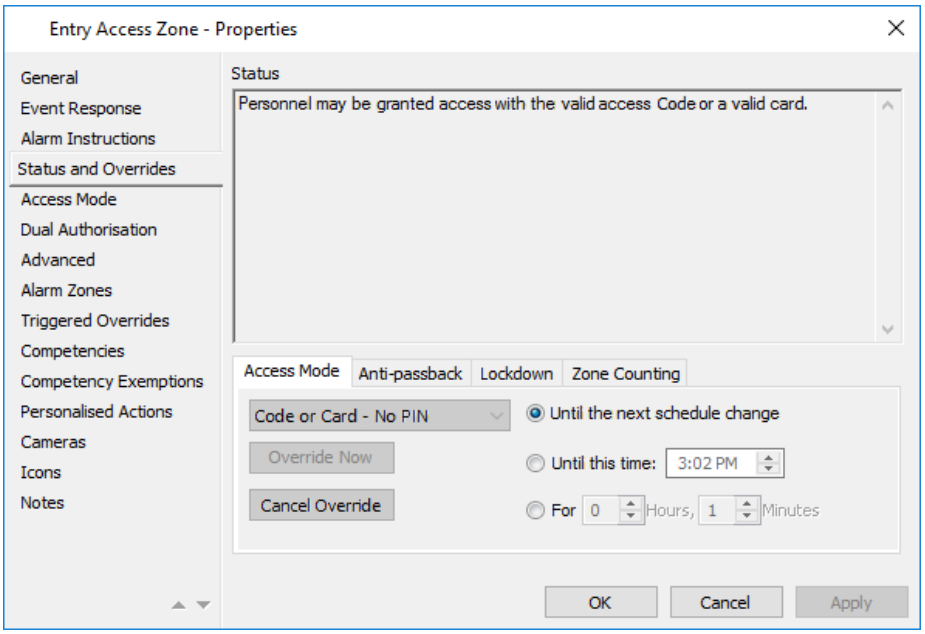
5. Entrez un code utilisateur à 4 ou 6 chiffres dans le champ Code utilisateur.
   Remarques :
   - Lorsque vous entrez le code utilisateur, des astérisques s'affichent à la place de chaque chiffre.
   - Le code doit contenir au moins un chiffre différent de zéro (par exemple, 0000 n'est pas valide et une erreur sera générée).
6. Confirmez le code utilisateur en le saisissant à nouveau dans le **champ Confirmation**.
7. Cliquez sur le bouton **OK**.
8. Répétez les étapes 2 à 7 pour chaque titulaire de carte qui doit avoir accès au lecteur.
   Remarque : Vous pouvez savoir quels titulaires de carte ont des codes utilisateur en exécutant un rapport de synthèse des titulaires de carte et en sélectionnant le champ Code utilisateur. Bien que le rapport indique qui a un code d'utilisateur, les codes réels ne seront pas divulgués.
9. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du matériel s'ouvre.
10. **Cliquez avec le bouton droit** de la souris sur **Propriétés**.
11. Cliquez sur l'onglet **Avancé (Advanced)**.



12. Cochez la **case à cocher Code utilisateur du PIN**.
    Lorsque le **code PIN est** vérifié, le code utilisateur est requis à la place du code PIN pour toute transaction effectuée au lecteur qui nécessiterait normalement un code PIN. Cela inclut l'accès et les remplacements de porte.

    Remarque : Les remplacements de carte double ne fonctionnent pas dans ce mode, par conséquent, laissez les remplacements de carte double **désactivé**.

13. Cliquez sur le bouton **OK**.
14. Définissez le mode d'accès de la zone d'accès du lecteur sur "Code ou Carte - Pas de NIP". Cela peut être fait à partir de :
    - **Calendrier**. Voir ***Créer un nouvel horaire*** (page 12-2) pour plus de détails. La planification est ensuite appliquée à la zone d'accès via le mode d'accès des propriétés de la zone d'accès.
    - **Zone d'accès**, comme suit :



a) Sous l'onglet **Statut et Remplacements**, sélectionnez l'onglet **Mode d'accès**.
b) Sélectionnez le mode "Code ou Carte - Pas de NIP " dans la liste déroulante.
c) Cliquez sur le bouton **Remplacer maintenant**, puis sur le **bouton OK**.

Résultat

Des codes d'utilisateur ont été spécifiés pour identifier les détenteurs de cartes à un lecteur pour l'accès au NIP seulement.

Lorsque les détenteurs de carte entrent correctement leur code d'utilisateur dans le lecteur, l'événement Door Access Granted suivant sera généré dans le Centre de commandes :

"[Titulaire] a obtenu l'entrée dans [Zone d'accès] par [Porte]"

Audit des changements de titulaire de carte

Introduction

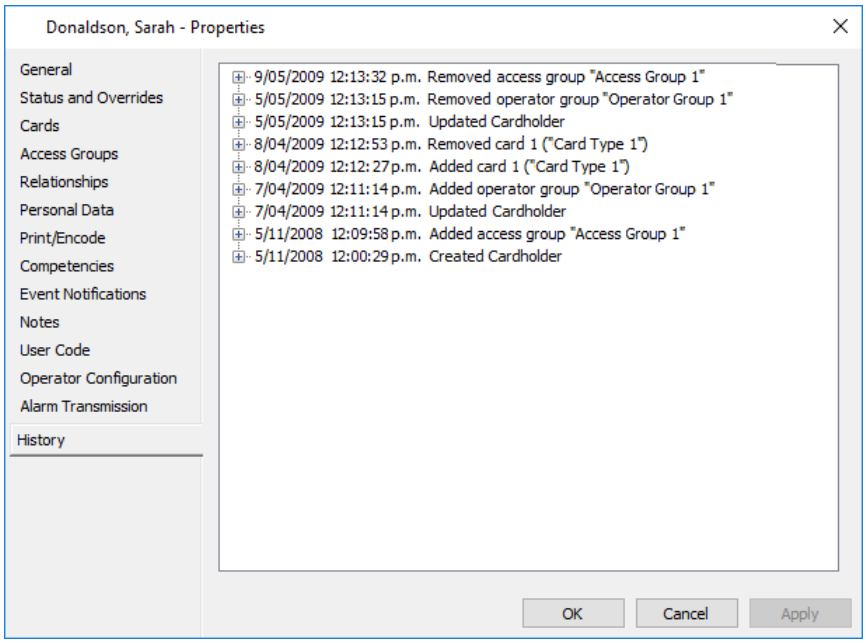
Cette procédure vous permet d'afficher une piste d'audit des modifications apportées à un titulaire de carte. Les privilèges suivants sont requis :

- "Afficher les titulaires de cartes",
- "Afficher les notes du titulaire de carte" (pour voir les modifications apportées aux notes), et
- "Afficher les opérateurs" (pour voir les modifications apportées à la configuration des opérateurs).

Remarque : Cette fonctionnalité a été introduite dans la version vEL6.01 du Centre de commande. Par conséquent, si votre site a été mis à niveau à partir d'une version antérieure à vEL6.01 de Command Center, les détenteurs de carte créés dans des versions antérieures afficheront leur statut du moment où ils ont été mis à niveau (par exemple, les cartes qu'ils avaient, les groupes d'accès auxquels ils ont été ajoutés). Certains détails de l'historique d'audit avant la mise à niveau seront perdus (par exemple, le moment où une carte a été ajoutée, une carte a été ajoutée au titulaire de la carte et supprimée ultérieurement).

Procédure

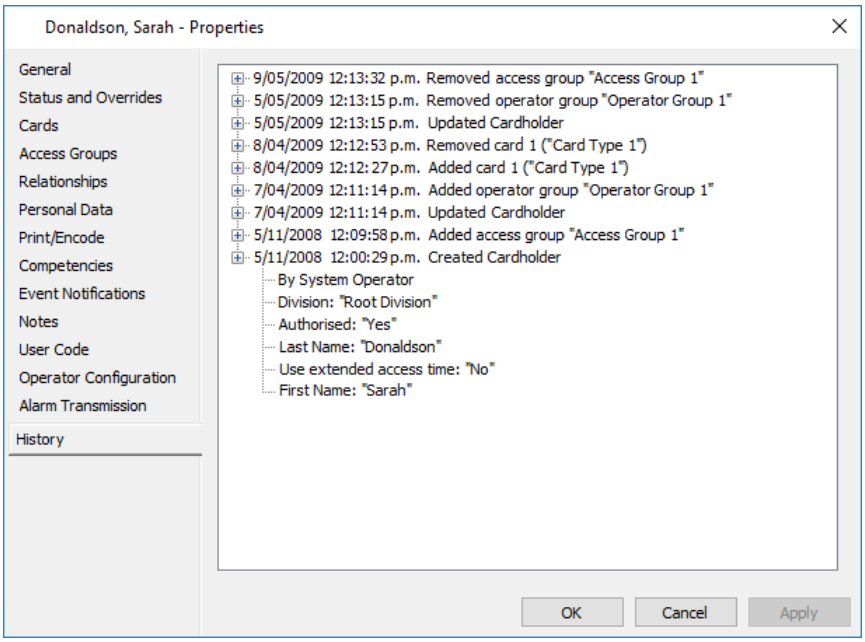
1. Cliquez sur **Gérer** dans la barre de menu, puis sur Titulaires de carte.
   La fenêtre Liste principale des titulaires de carte s'ouvre (en mode grille).
2. Localisez et mettez en surbrillance le titulaire de carte dont vous souhaitez voir les modifications.
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Historique (History)**.



Les entrées de cette page s'affichent en arborescence et chaque entrée représente une modification apportée au détenteur de la carte. Ils sont triés par

temps, en ordre décroissant, avec le dernier changement en haut. Les titres des entrées indiquent quand la modification a été apportée et ce qu'elle a été. Des informations supplémentaires sont parfois incluses dans les titres pour apporter un changement facilement identifié (par exemple, lorsqu'une carte a été créée, le numéro et le type de carte sont inclus dans le titre, comme indiqué dans la capture d'écran ci-dessus).

5. Cliquez sur ⊞ l'une des entrées ci-dessous pour développer la liste des éléments qui se trouvent en dessous.



Le premier élément sous l'entrée indique l'opérateur qui a effectué la modification, et le poste de travail où la modification a été effectuée. Tous les autres éléments qui suivent affichent les détails.

Remarques

- Bien que les informations de cette page soient en lecture seule, le texte peut être copié et collé dans n'importe quelle autre application conformément aux fonctionnalités courantes de Microsoft Windows. Pour ce faire, **cliquez avec le bouton droit** n'importe où dans la grille et sélectionnez **Copier**. Une copie de tout le texte de l'onglet **Historique** (y compris les lignes normalement visibles seulement après avoir développé une entrée) sera placée dans le Presse-papiers, précédée par le titre : *Historique du détenteur de la carte "<nom>"*.
- La modification de groupes d'accès existants peut produire une entrée "Ajouté" puis "Retiré", (par exemple, changer une date d'adhésion d'un titulaire de carte).
- Les activités suivantes n'apparaissent pas dans l'historique des titulaires de carte:
  - Modifications de la sélection du doigt Morpho
  - Carte expirant (sous l'onglet **Cartes**)
  - Modifications de l'ID du contact
  - Changements de salto
  - Access Groups expirant
  - Ré-activation d'une compétence

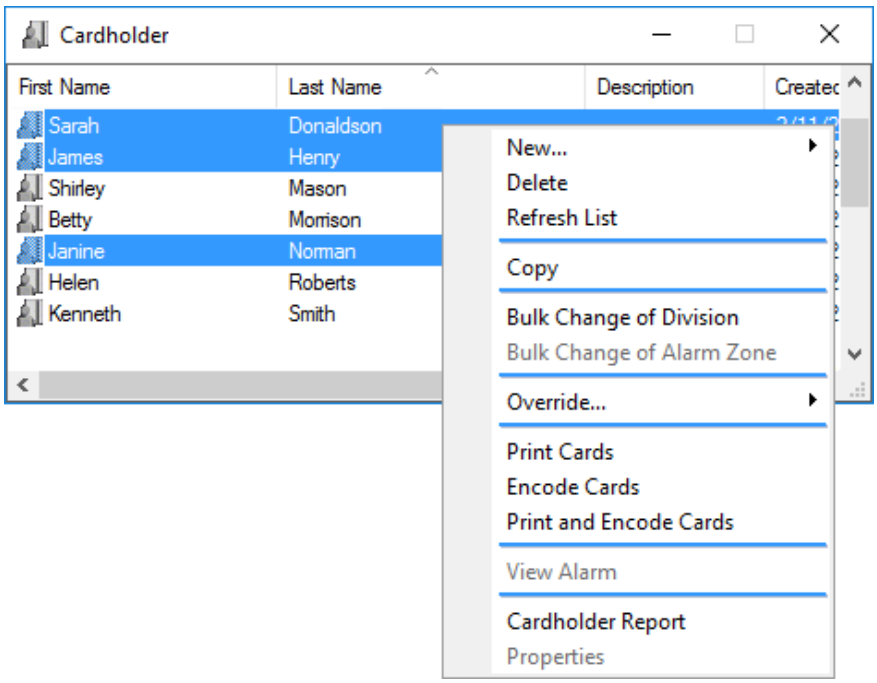
Exécution d'un état de titulaire de carte

Introduction

Cette procédure vous permet d'exécuter un état des titulaires de carte à partir de la fenêtre Liste principale des titulaires de carte.

Procédure

1. Cliquez sur **Gérer** dans la barre de menu, puis sur Titulaires de carte.
   La fenêtre Liste principale des titulaires de carte s'ouvre (en mode grille).
2. Sélectionnez le(s) titulaire(s) de la carte sur lequel vous souhaitez exécuter un rapport, **puis cliquez avec** le bouton **droit** de la souris.



3. Cliquez sur **Rapport de titulaire** de carte dans le menu contextuel.
   L'Assistant Rapport du titulaire de carte passe automatiquement à la page **État de la progression de la génération de rapports** et un rapport détaillé du titulaire de carte commence à s'exécuter. Le rapport ne contiendra que le ou les détenteurs de cartes sélectionnés.
   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 dans le rapport.

Lecture des cartes MIFARE à l'aide d'un encodeur USB MIFARE

Introduction

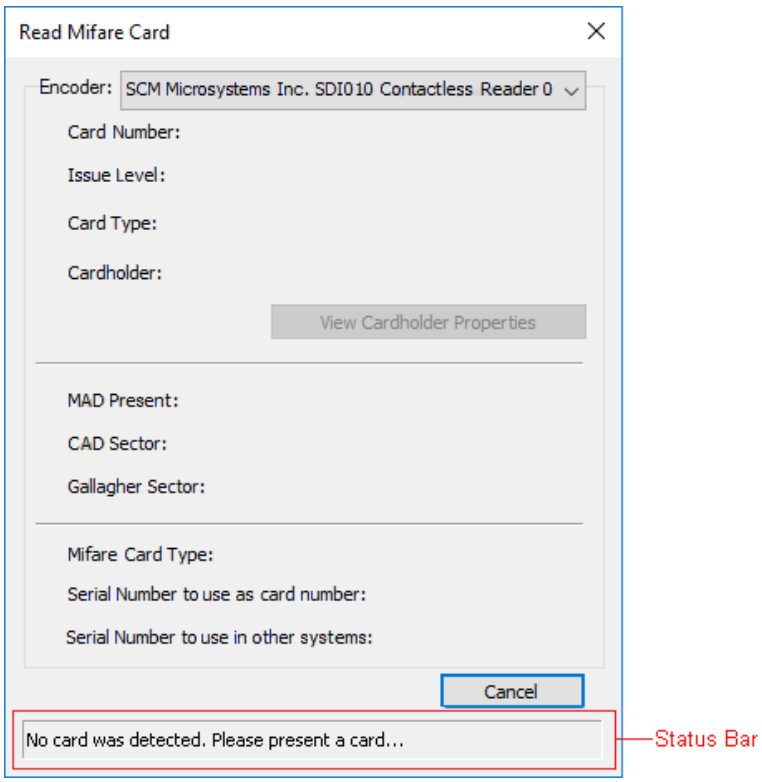
Lorsque vous perdez une carte sans nom, cette fonction vous permet d'identifier le détenteur de la carte qui a perdu sa carte. Les données des titulaires de carte s'affichent lorsque l'utilisateur demande au système d'activer une carte active, que ce soit un *lecteur et un encodeur MIFARE sans contact SDI010* ou *SDI011G, ACR1252.*
Remarques :

- Cette fonctionnalité **n**'est **pas** sous licence et ne fonctionne qu'avec les codeurs suivants :
  - *PICC 0 lecteur ACSACR1252CLS*
  - *SCMMicrosystems Inc. SDI010 Lecteur sans contact 0*
  - *SCMMicrosystems Inc. SDI011G Lecteur sans contact 0*
- Les opérateurs ont besoin du privilège de l'opérateur "Afficher le détenteur de la carte" pour utiliser cette fonctionnalité.

Cette procédure décrit la lecture d'une carte MIFARE à l'aide d'un encodeur USB ACS ou SCMMIFARE dans le Centre de commandes Gallagher.

Procédure

1. Cliquez sur **Moniteur** dans la barre de menus, puis sur **Lire la carte MIFARE**.
   La boîte de dialogue **Lire la** carte **MIFARE** s'affiche.

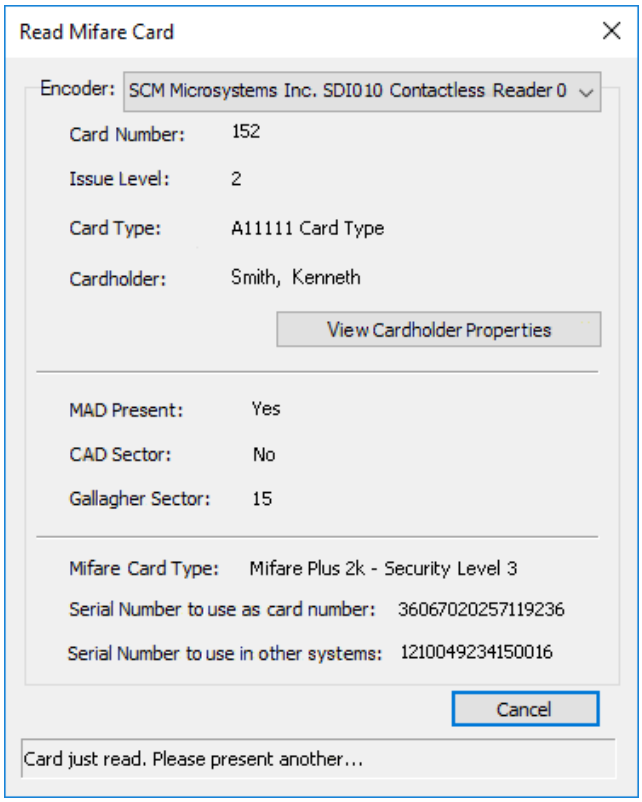


   Par défaut, le premier encodeur USB disponible est utilisé pour la lecture et remplit le champ **Encoder.** Si d'autres codeurs USB sont connectés à la station de travail, ils apparaissent également dans la liste déroulante.

2. Sélectionnez l'**encodeur requis** dans la liste déroulante.

Si...	alors...
aucun encodeur USB n'est détecté	le message *"Aucun encodeur USB n'a été détecté"* apparaît dans la barre d'état.
la station de travail est activée pour l'ouverture de session SmartCard	• la fonction "Lire la carte MIFARE" sera désactivée sur la station de travail, • le champ **Encoder** sera vide, et • le message *"Désactivé sur les postes de travail activés pour la connexion par carte à puce"* s'affiche dans la barre d'état.

3. Placez la carte sur l'encodeur.
Les détails de la carte s'affichent dans la boîte de dialogue Lire la carte MIFARE si la carte contient des données Gallagher et le détenteur de la carte correspondante peut être trouvé dans le système.



Remarques :

- Si le type de carte et le titulaire de la carte se trouvent dans le centre de commande Gallagher mais que le niveau de problème est différent (par exemple, une nouvelle carte a été délivrée au titulaire de la carte avec le même numéro de carte mais un niveau de problème différent), alors le message *"*Le niveau de problème diffère"* s'affichera à gauche du bouton Annuler.
- Si aucune donnée Gallagher n'est trouvée sur la carte, les détails de la carte seront grisés et le message *"Aucune donnée Gallagher n'a été trouvée"* apparaîtra dans la barre d'état.

- Si des données Gallagher sont trouvées sur la carte, mais que celle-ci n'appartient pas au système, alors :
  - le **champ Type de carte** s'affiche sous la forme "Type de carte inconnu",
  - le champ "Détenteur de carte inconnu", et
  - le bouton Afficher les **propriétés** des **détenteurs** de carte sera désactivé.
- Les **types de cartes MIFARE** qui peuvent s'afficher sont les suivants :
  MIFARE Classic 1k
  MIFARE Classic 4k
  MIFARE Plus S - Niveau de sécurité 0
  MIFARE Plus X - Niveau de sécurité 0
  MIFARE Plus S 2k - Niveau de sécurité 3
  MIFARE Plus X 2k - Niveau de sécurité 3
  MIFARE Plus S 4k - Niveau de sécurité 3
  MIFARE Plus X 2k - Niveau de sécurité 3
  MIFARE DESFire 2k
  MIFARE DESFire 4k
  MIFARE DESFire 8k
- Le champ **Numéro de série à utiliser comme numéro de carte** affiche le numéro de série de la carte (CSN) unique au format décimal et dans l'ordre inverse des octets de la carte. Le champ Numéro de série à utiliser dans d'autres systèmes affiche le numéro de série unique de la carte (UID).

  Remarque : Si la carte est assignée à un titulaire de carte, est d'un type où le réencodage est empêché, et qu'elle a un CSN différent de celui enregistré dans le passé pour cet identificateur, une alarme "Carte en double potentiel" sera générée. Si cela se produit, nous vous recommandons de prendre la mesure la plus sûre pour votre site, c'est de délivrer au titulaire de la carte qui se voit actuellement attribuer une carte avec cet identificateur, une nouvelle carte.
- Si la carte est inconnue, le champ **Type de carte MIFARE** peut afficher "ISO1444-3 inconnu". De même, le message "La carte sélectionnée est une *carte ISO14443-3 non prise en charge"* peut s'afficher dans la barre d'état si la carte est détectée comme un des types connus non pris en charge.

4. Cliquez sur le bouton **Afficher les propriétés du titulaire de carte (View Titulaire de carte Properties)**.
   Les propriétés du titulaire de carte auquel la carte appartient s'ouvrent.
5. Présentez la prochaine carte si il y a plus à lire.

Remarques

- L'encodeur émet un signal sonore la première fois qu'une carte est placée dessus et que l'**utilitaire** Read **MIFARE Card** dans le Centre de commandes est utilisé, et se calme ensuite.
- L'encodeur émet un signal sonore lorsqu'une carte est placée dessus, avant l'ouverture du Centre de commandes et l'**utilisation de la carte MIFARE en lecture**.

Désactivation de l'opérateur système

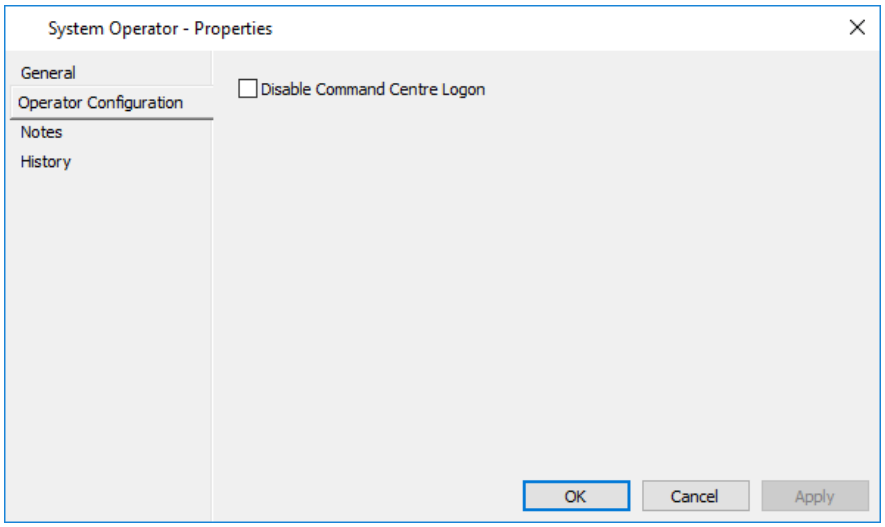
Introduction

Le compte Opérateur système est initialement utilisé pour configurer le Centre de commandes. Une fois que des opérateurs distincts ont été créés, l'opérateur de réseau n'est pas entièrement nécessaire et doit être désactivé par un autre opérateur à des fins de sécurité.

Les opérateurs ont besoin du privilège "Afficher/Modifier les opérateurs" pour effectuer cette procédure.

Procédure

1. Cliquez sur **Moniteur** dans la barre de menus, puis sur **Rechercher...**.
   L'**outil de** recherche s'ouvre.
2. Cliquez dans le champ **Regarder dans** et sélectionnez l'option "Opérateur de système".
3. Cliquez sur le bouton **Démarrer la recherche**.
   L'opérateur système s'affiche dans la fenêtre de recherche.
4. **Cliquez avec** le bouton **droit** sur l'opérateur système et sélectionnez **Propriétés**.
   Par défaut, l'onglet **Général** s'affiche.
5. Cliquez sur l'onglet **Operator Configuration (Configuration de l'opérateur)**.



6. Cochez la **case Désactiver la connexion du centre de commande**.
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

Le compte de l'opérateur système est désactivé.
Remarque : Si un opérateur tente d'ouvrir une session en utilisant le nom et le mot de passe de l'opérateur du système, le message "Nom ou mot de passe d'ouverture de session non valide" s'affiche sur l'écran d'ouverture de session.

Chapitre 33 : Champs de données personnelles

Les données personnelles sont des informations qui sont stockées pour un titulaire de carte individuel. Ces informations peuvent inclure des éléments tels que la plaque d'immatriculation de la voiture, la date de naissance, la signature, les photographies, la division de l'entreprise, etc.
Les champs de données personnelles (PDF) sont créés en tant qu'entités distinctes et sont joints aux groupes d'accès. Les titulaires de carte héritent des champs de données personnelles du(des) groupe(s) d'accès(s) auquel ils appartiennent.
Lors de la consultation d'un enregistrement de titulaire de carte, il contiendra tous les champs de données personnelles spécifiés dans le ou les groupes d'accès auxquels le titulaire de carte appartient.
Il existe neuf types différents de champs de données personnelles, comme suit :

- Texte (un opérateur peut saisir tout texte à main libre)
- Texte - Liste (si l'option "Restreindre à la liste" est activée, l'opérateur peut choisir une entrée dans une liste d'entrées prédéfinies ou la laisser vide. Si l'option "Restreindre à la liste" n'est pas activée, l'entrée de texte libre est autorisée)
- Numérique
- Date
- Image (un opérateur peut capturer une image, par exemple des signatures, des photographies de détenteurs de cartes, etc.)
- Adresse
- Téléphone
- Mobile
- Adresse électronique

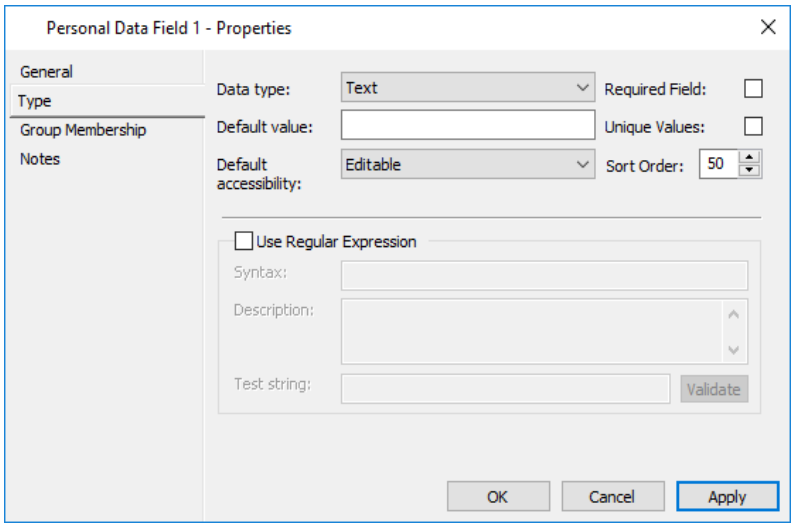
Création d'un champ de données personnelles

Introduction

Cette procédure explique comment créer un champ de données personnelles.

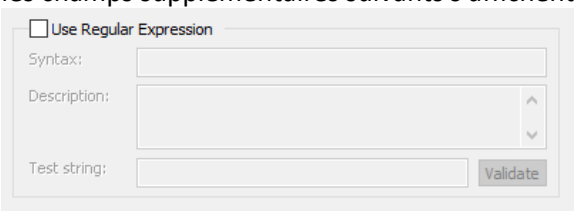
Procédure

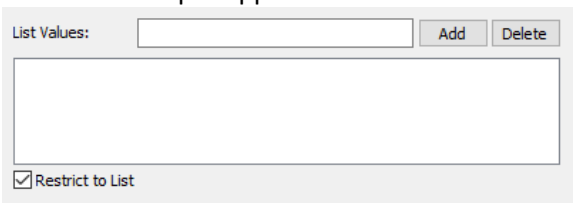
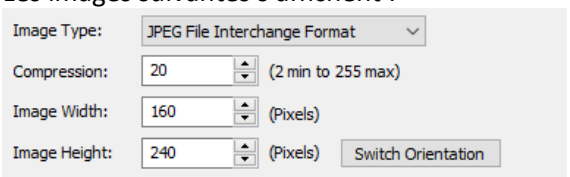
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Champs de données personnelles**. La fenêtre **Champ de données personnelles -** Liste principale s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...Champ de données personnelles**. Par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

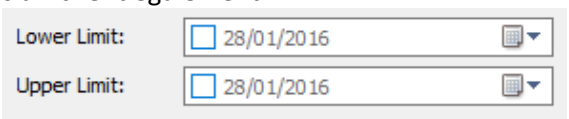


Cet onglet détermine le type de données à entrer dans le fichier PDF. Par défaut, le champ Type de données est renseigné par le champ "Texte".

5. Cliquez dans le champ **Type de données** et sélectionnez le type approprié dans la liste déroulante.
   Remarque : A l'exception du type numérique, chaque type comporte des informations supplémentaires qui doivent être entrées, dont certaines sont communes à tous les types, tandis que d'autres informations sont spécifiques à des types individuels, comme suit :

Si vous sélectionnez...	alors...
Texte, ou tout type de document PDF, (p. Adresse, téléphone, e-mail ou mobile)	les champs supplémentaires suivants s'affichent :  La fonctionnalité **Utiliser l'expression régulière** est

Si vous sélectionnez...	alors...
	destinée à la validation des données PDF de type texte et de contact pour permettre l'application des valeurs de texte. Il vous permet d'écrire une expression régulière qui forcera les valeurs saisies dans le PDF à respecter les règles de l'expression. Si des valeurs sont entrées qui cassent l'expression, un message d'erreur s'affiche pour détailler les conditions requises pour l'expression. Voir ***Réglages d'expression régulière*** (page 33-6) pour plus de détails sur la saisie d'informations dans cette section. **Remarque :** Si 'Email' ou "Mobile" soit est le **type de données**, une case à cocher supplémentaire **Notifications par défaut** est utilisée par l'application Gestion des visiteurs. Si vous souhaitez que les hôtes puissent envoyer des invitations aux visiteurs, cette case à cocher doit être cochée. Lorsqu'elle est cochée, elle détermine également si la case **Notifications** est cochée ou non lorsqu'un groupe d'accès avec ce PDF est ajouté à un détenteur de carte, ou lorsque le détenteur de carte est ajouté au groupe d'accès.
Texte - Liste	Liste des champs supplémentaires :  Ces champs vous permettent de définir un ensemble d'entrées parmi lesquelles vous pouvez sélectionner, lors de la saisie de données sur un titulaire de carte. Pour ce faire, entrez une valeur dans le champ 'Lister les valeurs', puis cliquez sur le bouton Ajouter. Lorsque l'option Restreindre à la liste est activée, la **valeur par défaut** doit être l'une des valeurs de la liste ou vide. Si l'option "Restreindre à la liste" n'est pas activée, des entrées de texte libres peuvent être saisies contre un détenteur de carte.
Image	Les images suivantes s'affichent :  Ces champs vous permettent de spécifier des détails sur l'image enregistrée dans la base de données. Le **type d'image** peut être JPEG, Bitmap ou PNG. Cochez la case Image du profil si vous voulez cette image CDP (contenant la photo du titulaire de la carte) à afficher sur l'écran Détails du client mobile. **Remarque:** Un seul fichier image CDP sera utilisé pour

Si vous sélectionnez...	alors...
	chaque titulaire de carte. Si un titulaire de carte a plus d'une Image CDP capturés et ils ont tous la case cocher Image du profil activée, l'image avec l'ordre de tri le plus bas sera affiché. Reportez-vous à ***Capture d'une image*** (page 33-10) pour la procédure de capture d'images pour un champ de données personnelles d'image.
Date	Le champ **valeur par défaut** change en un contrôle Date :  Laissez la case à cocher désactivée si vous ne voulez pas d'option par défaut. Les champs supplémentaires suivants s'affichent également:  Une plage de dates inférieure et/ou supérieure peut être spécifiée pour contrôler les dates entrées dans le PDF. **Remarque :** Les dates s'afficheront à l'écran et dans les rapports dans le format de date spécifié dans les paramètres du poste de travail.

6. Cochez les cases suivantes :

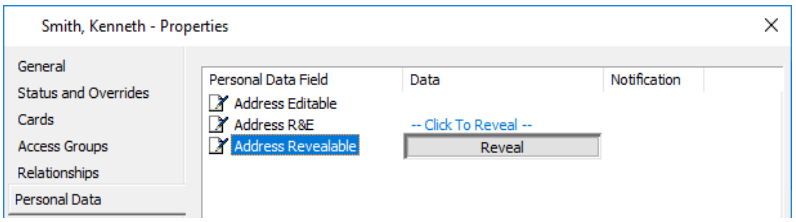
Si...	est cochée, alors...
Champ obligatoire :	Les données du champ Données personnelles seront obligatoires lors de la modification d'un titulaire de carte.
Valeurs uniques :	un opérateur ne pourra pas saisir la même valeur pour plusieurs détenteurs de cartes (même si le système permettra de saisir plusieurs fois une valeur "aucune donnée"). Le champ **Valeur par défaut** est désactivé.

Remarque : "Valeurs uniques" est désactivé pour **Texte -** Type **de liste**, Type d'**image** et Type de date.

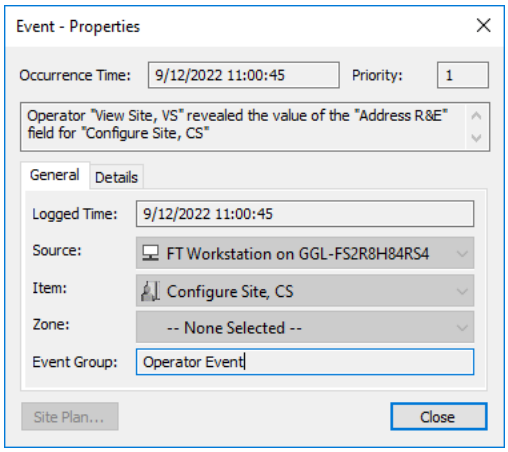
7. Cliquez dans le champ **l'accessibilité par défaut** et sélectionnez le privilège approprié (type d'accès) dans la liste déroulante. Ce champ détermine les droits de l'opérateur de base pour ce champ de données personnelles.

Si...	alors...
Modifier (par défaut)	les opérateurs disposant du privilège "Voir les détenteurs" dans une division peuvent consulter la valeur du champ de données personnelles, mais pas la créer ni la modifier. Les opérateurs disposant du privilège "Modifier les données personnelles du détenteur" dans une division peuvent créer ou modifier les valeurs des champs de données personnelles d'un détenteur dans cette division.
Caché	les opérateurs qui ne disposent pas du privilège « Utilisateur avancé » ne verront pas les informations enregistrées pour ce champ de données personnelles pour les détenteurs de cartes des divisions de ce groupe, et ne verront même pas qu'il existe.

Si...	alors...
Révélable	Les opérateurs disposant du privilège "Voir les détenteurs" dans une division peuvent visualiser la valeur du champ de données personnelles (à partir de l'onglet Données personnelles des propriétés des détenteurs), en cliquant sur le bouton Révéler. Les opérateurs disposant du privilège "Modifier les données personnelles des détenteurs" peuvent visualiser la valeur du champ de données personnelles en cliquant sur le bouton Révéler, mais ne peuvent ni la créer ni la modifier.
Visualisation uniquement	Les opérateurs disposant du privilège "Voir les détenteurs" dans une division peuvent consulter la valeur du champ Données personnelles. Les opérateurs disposant du privilège "Modifier les données personnelles des détenteurs" peuvent consulter la valeur du champ Données personnelles, mais pas la créer ni la modifier.
Révélable et modifiable	les opérateurs disposant du privilège "Voir les détenteurs" dans une division peuvent visualiser la valeur du champ de données personnelles (à partir de l'onglet Données personnelles des propriétés des détenteurs), en cliquant sur le bouton Révéler, mais pas la créer ou la modifier. Les opérateurs disposant du privilège "Modifier les données personnelles du détenteur" dans une division, en cliquant sur le bouton Révéler, peuvent créer ou modifier la valeur du champ des données personnelles d'un détenteur dans cette division. **Remarques :** • Les PDF révélables et modifiables ne sont pas disponibles dans les applications REST ou Mobile Client. • Les champs de données personnelles dont l'accessibilité est "Révélable" ou "Révélable et modifiable" affichent un bouton Révéler dans l'onglet Données personnelles des propriétés du détenteur. • Les fichiers PDF révélables ou révélables/modifiables qui sont inclus n'enregistrent pas le nouvel événement d'accès lorsqu'un rapport est exécuté, qu'une recherche via REST est effectuée ou qu'un événement d'opérateur s'est produit.



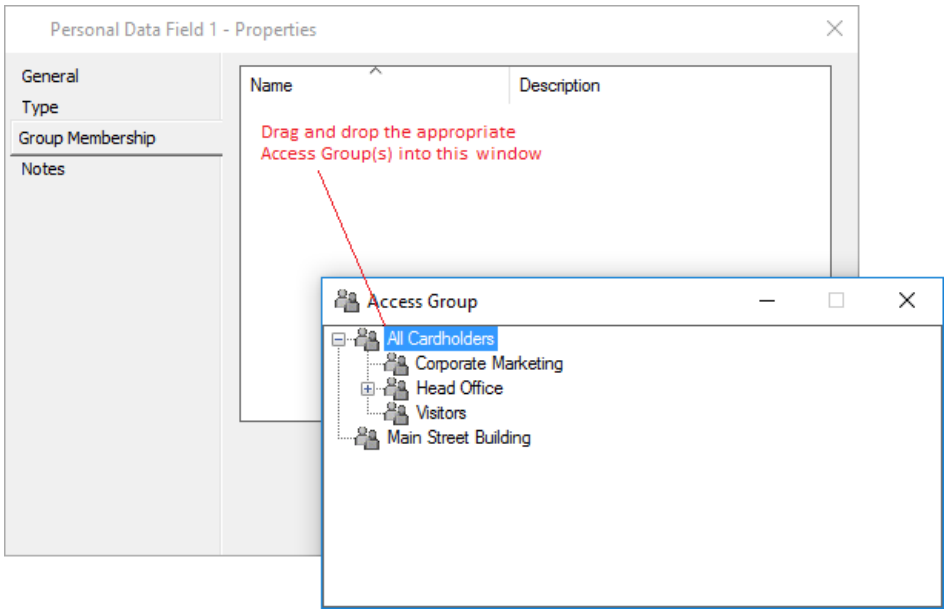
Chaque fois qu'un bouton Révéler est actionné, il y a un événement opérateur sous la forme de l'opérateur "View Site, VS" qui révèle la valeur du champ "Address R&E" pour "Configure Site, CS", à partir de la "Source" du poste de travail sur lequel l'opérateur était connecté.



Remarques :

- La case à cocher Notifications par défaut sera révélée lorsque l'on appuiera sur le bouton Révéler (c'est-à-dire qu'il s'agit d'un espace vide jusqu'à ce que cela se produise).
- L'opérateur du système n'a pas l'option de révélation visible, puisqu'il peut tout voir de toute façon.
- Le titre d'un champ qui n'est pas modifiable est affiché en gris.

8. Modifiez le champ **Trier Ordre** si nécessaire. Ceci contrôle l'ordre dans lequel les enregistrements PDF sont affichés dans la page de propriétés du détenteur de la carte.
   Remarque : Plus le nombre est bas, plus la liste affichée est haute (par exemple, 1 affichera le PDF en haut de l'écran, 100 le placera en bas, et si tous sont définis au même nombre, ils l'afficheront par ordre alphabétique).
9. Cliquez sur l'onglet Appartenance au groupe (Group Membership).
10. Cliquez sur **Gérer** dans la barre de menus, puis sur **Groupes d'accès**.
    La fenêtre **Liste** principale **du groupe Access** s'ouvre.
    Sélectionnez les groupes d'accès appropriés pour ce champ de données personnelles. Faites-les glisser et déposez-les dans l'**onglet Appartenance au groupe**.



11. Cliquez sur l'onglet **Remarques** si vous souhaitez ajouter une ou des remarques sur ce champ de données personnelles.
    Pour plus de détails concernant l'**onglet Notes**, voir ***Notes*** (page 6-81).
12. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Un nouveau champ de données personnelles est créé.
Remarque : Une fois qu'un champ de données personnelles a été créé et que des données ont été enregistrées, la possibilité de modifier son type de données ne sera plus disponible. Pour l'enregistrement des données personnelles des titulaires de carte au moyen de PDF, consultez Modification des ***données PDF des titulaires de carte*** (page 32-20) pour la procédure.

Conseils

Modification et suppression de champs de données personnelles
Reportez-vous à la section ***Modification des éléments*** (page 3-26) et ***Suppression des éléments*** (page 3-27) pour connaître les procédures sur la façon de modifier et de supprimer les champs de données personnelles.
Remarque : La suppression d'un champ de données personnelles n'est autorisée que s'il n'est pas actuellement affecté à une utilisation quelconque dans le système, sauf s'il est enregistré dans un rapport.

Copier et coller
Une alternative à la méthode glisser-déplacer consiste à utiliser la méthode copier-coller.

Détails de l'appartenance au groupe
Le(s) groupe(s) d'accès que vous avez ajouté(s) à ce champ de données personnelles (à l'étape 11) affichera à présent ce fichier PDF dans l'onglet **Données personnelles** de leur écran Propriétés.

Paramètres d'expression régulière

Introduction

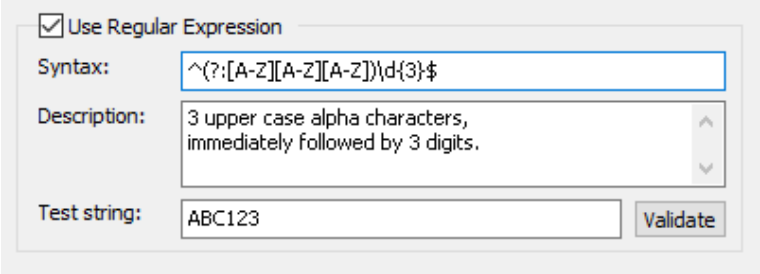
Des expressions régulières peuvent être utilisées pour définir les données valides et peuvent être entrées dans un champ de données personnelles. Par exemple, une expression régulière peut être utilisée pour s'assurer que les ID employé contiennent toujours deux lettres suivies de six chiffres maximum.

Procédure

La case à cocher Utiliser l'expression régulière (onglet Type des propriétés Champ de données personnelles) active tous les champs de cette section.
Configurer comme approprié :
Remarque : Reportez-vous à ***Expressions régulières courantes*** (page 33-8) pour obtenir la liste des expressions régulières d'exemple.

du champ	**Description**
Syntaxe	Ce champ permet une syntaxe d'expression régulière, jusqu'à 2048 caractères, qui est utilisée pour valider les données PDF du détenteur de la carte. Il permet des retours chariot multiples lignes.
Description	Ce champ peut contenir jusqu'à 2 048 caractères pour décrire la syntaxe d'expression régulière. Il permet plusieurs lignes et des retours chariot. **Remarque :** Il s'agit du message qui sera affiché à un opérateur si la valeur entrée ne peut pas être enregistrée car elle ne répond pas à la validation de l'expression régulière.
Chaîne de test	Ce champ permet d'utiliser un exemple de chaîne, d'un maximum de 2048 caractères, qui aide les techniciens à écrire/tester la syntaxe d'expression régulière. **Remarque :** Ce champ n'est pas enregistré dans la base de données du Centre de commandes.
Valider bouton	Ce bouton valide la chaîne de test par rapport à la syntaxe de l'expression régulière lorsque vous cliquez dessus. Les messages renvoyés peuvent être l'un des suivants : • "Le champ Syntaxe ne peut pas être vide.", • "Le champ TestString ne peut pas être vide.", • "Validation réussie.", ou • "Échec de la validation, car la valeur ne correspond pas à l'expression régulière."

Remarque : Les PDF de type "Mobile" et "Email" comportent une case à cocher supplémentaire Notifications par défaut dans cet onglet. Si cette option est cochée, elle fournit une valeur par défaut pour les contacts des titulaires de carte.



Lorsque la case à cocher Utiliser l'expression régulière est activée:

- Le champ Syntaxe ne doit pas être vide.
- Si le champ **Valeur par défaut** n'est pas vide, sa valeur doit respecter la syntaxe de l'expression régulière.
- Pour un fichier PDF existant, si le champ **Syntaxe** est modifié et que ce fichier PDF est utilisé par un ou plusieurs groupes d'accès, le système validera toutes les données PDF liées au détenteur de la carte par rapport à la nouvelle syntaxe d'expression régulière. Si la validation échoue, une boîte de message d'erreur apparaît :
  "Le titulaire de la carte possède une valeur de données PDF non valide ou plus."
- L'expression régulière ne peut pas être enregistrée tant que toutes les données existantes ne sont pas validées par rapport à cette expression.

Expressions régulières courantes

Le tableau suivant fournit un certain nombre d'exemples d'expressions régulières qui ont été testés et peuvent être utilisés pour valider les données de type texte PDF.

Catégorie	Expression régulière		Description
Adresse électronique	^[A-Za-z0-9._%+-]+@(?:[A-Za-z0-9-]+\.)+[A-Za-z]{2,4}$		Insensible à la casse, doit inclure un symbole @ et des caractères facultatifs de l'e-mail tels que des points et des tirets avec un maximum de 4 caractères dans le domaine de niveau supérieur générique.
Téléphone (exemple)	^0[1-9]\s\d{3,4}\s\d{4}$		Nécessite un préfixe STD 01.09 suivi d'un espace obligatoire puis de sept ou huit chiffres avec un espace obligatoire séparant les quatre derniers chiffres, (p.ex. 07 34827520 ou 07 386 4902)
Numéro de téléphone, format international (exemple)	^[+]\d{7,18}$		Force un caractère '+' au début de la chaîne, suivi de 7 à 18 entiers (pas d'espaces).
Numéro de licence/ID (exemple)	^(?:CNS|BNE|TNS)\d{4,6}(?:-(:?[1-9]|1[0-5]))?$		Trois lettres majuscules CNS, BNE ou TNS, immédiatement suivies de 4-6 entiers, éventuellement suivies d'un tiret et d'un entier de 1-15 (p.ex. CNS15425-13 ou BNE928362).
ID numérique (exemple)	^\d{4,8}$		Uniquement des entiers, mais doit comprendre un minimum de 4 chiffres et un maximum de 8.
Enregistrement de voiture (exemple)	^[A-Z]{3}\d{3}$		Trois lettres majuscules immédiatement suivies de trois entiers (ex. KMO512).
Valeur numérique unique limitée (exemple)	^[0-4]$		Valeur numérique, 1, 2, 3 ou 4
Caractères alpha seulement	^[A-Za-z]+$		Tous les caractères majuscules ou minuscules uniquement, sans espaces.
En majuscule	^[A-Z]+$	(chaîne continue)	Tous les caractères en majuscules.
	^(?:[A-Z]\s?)+$	(espaces uniques autorisés, par exemple ASD BD GHJ)	

Catégorie	Expression régulière		Description
Minuscule	^[a-z]+$	(chaîne continue)	Tous les caractères en minuscules.
	^(?:[A-Z]\s?)+$	(espaces uniques autorisés, par exemple rgag dhgdh afg)	
Véritable cas	^(?:[A-Z]\w*\s?)+$		La Première Lettre De Chaque Mot Doit Être En Majuscule.
Booléen	^0|1$		Un simple on/off en utilisant uniquement les valeurs 0 ou 1.

Capture d'une image

Introduction

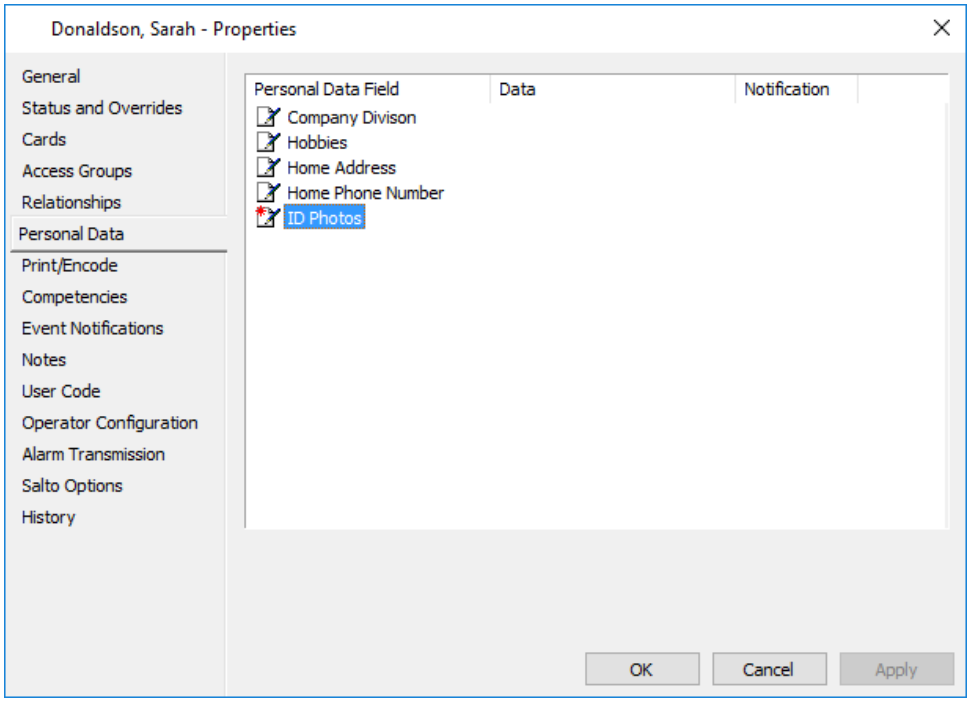
Cette procédure permet à l'opérateur de capturer une image (logos d'entreprise, photos de titulaires de cartes, etc.) pour un champ de données personnelles "Image" (PDF) d'un titulaire de carte.

Remarques :

- Les images des titulaires de carte peuvent être utilisées pour les cartes d'identité avec photo. Voir PhotoID pour plus de détails.
- Les sites qui souhaitent capturer des images pour des fichiers PDF sur un système d'exploitation Microsoft Windows Server 2008 doivent installer la fonctionnalité Expérience utilisateur, comme suit :
  1. Dans le menu Démarrer, cliquez sur Panneau de configuration > Outils d'administration > Gestionnaire de serveur.
  2. Dans le volet **Détails**, localisez la zone Résumé des fonctionnalités, puis cliquez sur **Ajouter des fonctionnalités**.
  3. Dans l'Assistant Ajout de fonctionnalités, cochez la case **Expérience utilisateur**, puis cliquez sur **Suivant** et ensuite sur Installer.
  4. Une fois la fonctionnalité Expérience utilisateur installée, cliquez sur Fermer pour quitter l'Assistant Ajout de fonctionnalités, puis cliquez sur **Oui pour** redémarrer l'ordinateur r.

Procédure

1. Cliquez sur **Gérer** dans la barre de menu, puis sur Titulaires de carte.
   La fenêtre Liste principale des titulaires de carte s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** sur le détenteur de la carte et sélectionnez **Propriétés**.
3. Cliquez sur l'onglet Données personnelles (Personal Data).

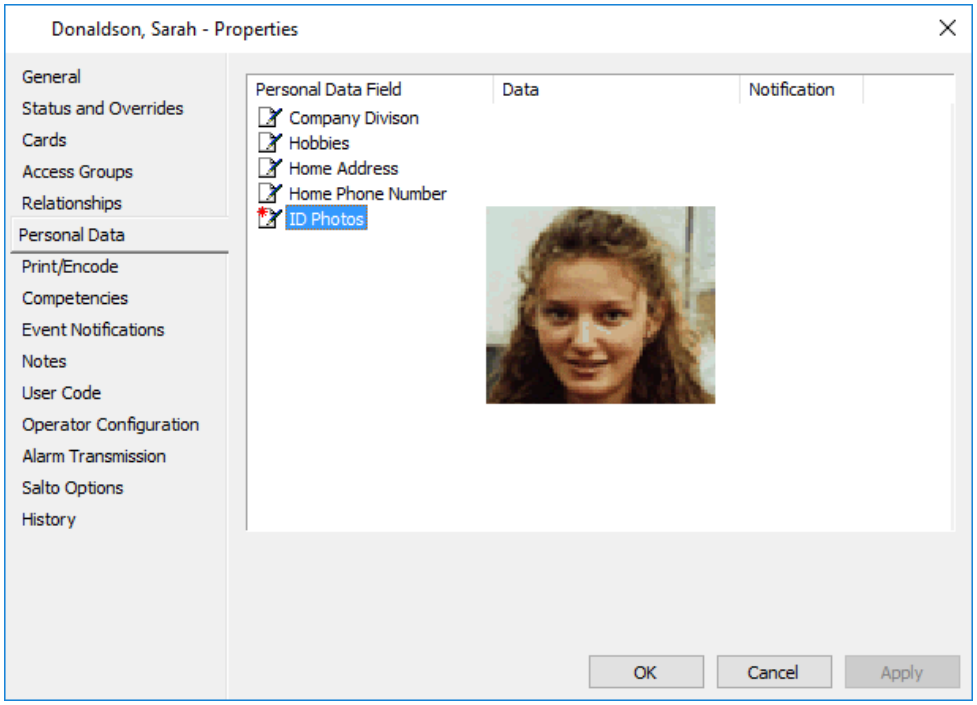


4. **Faites un clic droit** sur la section des données du PDF "Image", puis cliquez sur **Capturer l'image**.
   La fenêtre **Capturer l'image** s'affiche. Il sera vide si c'est la première fois que vous avez capturé ou chargé une image sur ce poste de travail, sinon il sera par défaut à la dernière méthode de capture que vous avez utilisée.
5. Si vous disposez d'une fenêtre Capture vide ou si vous souhaitez modifier la méthode de capture, cliquez dans la zone de sélection déroulante et sélectionnez la caméra souhaitée dans la liste des périphériques reliés à l'ordinateur.
6. Cliquez sur le bouton **Capturer... (Capture...)**.
7. Vous pouvez charger une image existante ou capturer une nouvelle image.

Si tu...	**alors...**
charger une image précédemment enregistrée	• Sélectionnez Charger à partir du fichier... dans la liste déroulante. La fenêtre Sélectionner l'image à charger s'affiche. • Accédez à l'emplacement de l'image dont vous avez besoin et cliquez sur le bouton **Ouvrir**. L'image s'affiche dans la **fenêtre Capturer l'**image. **Remarque :**  Pour ajuster le contraste et/ou la luminosité d'une image enregistrée, cliquez avec le bouton droit de la souris et déplacez l'indicateur si nécessaire.

Si tu...	alors...
capturer une nouvelle image	selon la façon dont la caméra que vous utilisez a été installée sur le PC, il peut vous donner la vidéo "en direct", auquel cas si vous recadrez vous devez recadrer une image en mouvement. Alternativement, la caméra peut afficher sa propre fenêtre, auquel cas vous "acquérez" l'image, ce qui la ramène ensuite à la fenêtre **Capture Image** comme une image statique que vous pouvez ensuite recadrer. **Remarque :** Si vous devez ajuster l'apparence de l'image, cliquez avec le bouton droit de la souris sur l'image affichée, puis cliquez sur **Configurer la source**. Une fenêtre s'affiche et vous permet de régler l'image (netteté, luminosité, couleur, etc.)

8. Repositionnez le cadre de recadrage.
9. Cliquez sur le bouton **OK**.
   La fenêtre **Capturer l'image** se ferme.
   L'image capturée s'affiche désormais dans l'onglet Données personnelles et dans l'onglet **Appliquer** est activé.



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

L'image est enregistrée dans le support de carte.

Chapitre 34 : Groupes d'accès

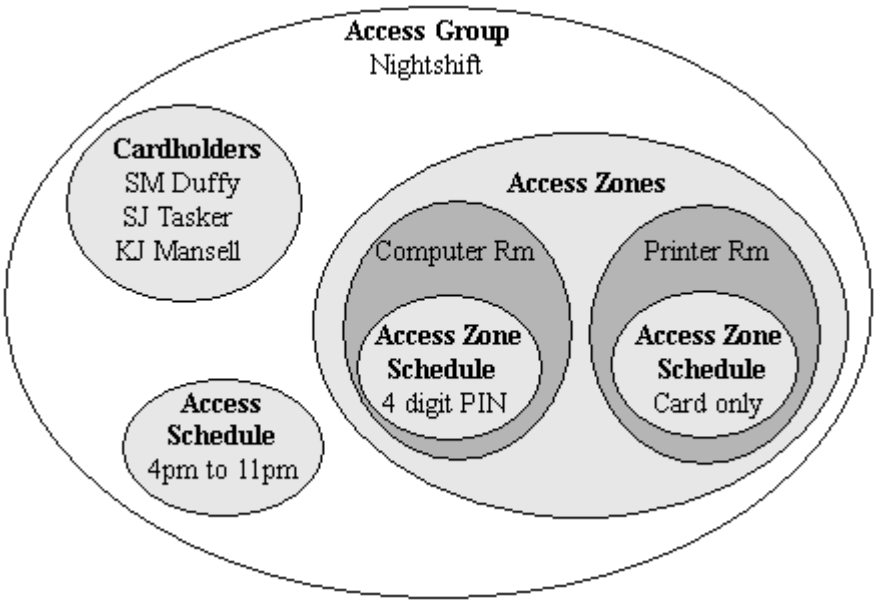
Présentation des groupes d'accès

Un groupe Access est un groupe de détenteurs de cartes.

Un groupe d'accès définit également l'accès (et d'autres propriétés) que ces détenteurs de carte possèdent.

Vous pouvez définir le "nom" et les "privilèges" d'un groupe d'accès et affecter les propriétés suivantes à un groupe d'accès :

- Membres (propriétaires)
- Zones d'accès (où les membres ont accès)
  Remarque : Il y a une limite de 255 zones d'alarme/zones d'accès par groupe d'accès et par contrôleur. Si cette limite est dépassée, une alarme sera générée (dans la fenêtre de visionneuse d'alarme) et les 255 premières zones seulement seront envoyées au contrôleur.
- Accès Calendrier (lorsque les membres ont accès))



Accès aux groupes et à la liaison

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

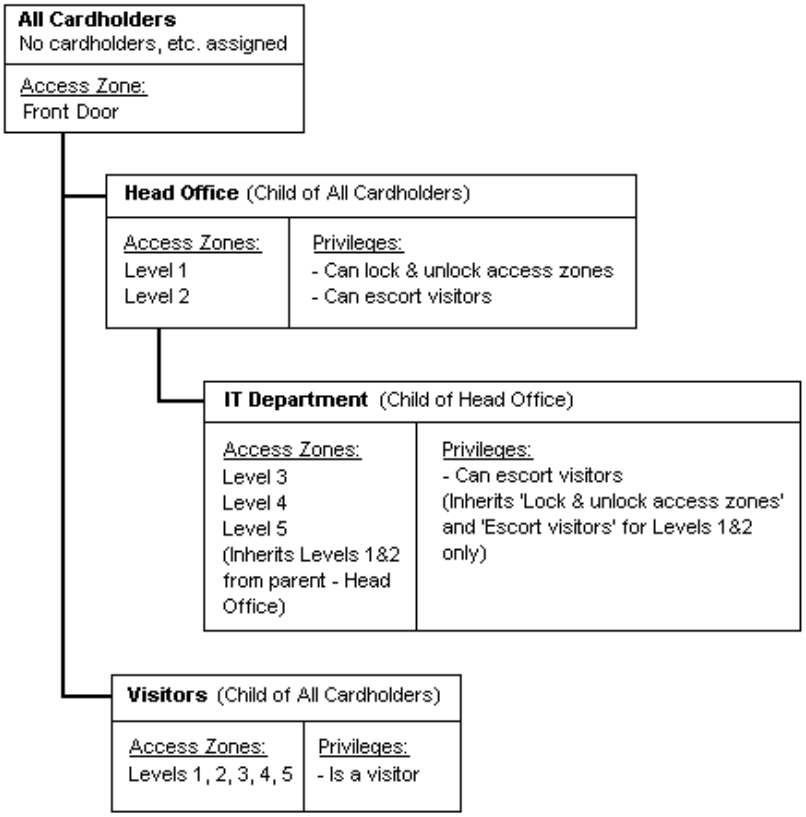
La procédure de configuration de Lineage est la même pour les groupes d'accès et les divisions. Cependant, dans une certaine mesure, la lignée fonctionne de manière opposée pour ces deux domaines. Cette rubrique explique comment la lignage fonctionne pour les groupes d'accès. Voir Divisions et lignage pour une explication de la façon dont cela fonctionne pour les divisions.

Héritage des privilèges de groupe d'accès

Si vous appartenez à un groupe d'accès, vous disposez automatiquement des privilèges de ses parents dans la hiérarchie.

Un titulaire de carte peut avoir besoin d'appartenir à plus d'un groupe d'accès pour obtenir l'ensemble de ses exigences en matière d'accès (c.-à-d. zones d'accès et horaires). Il y a aussi des privilèges attribués aux groupes d'accès (p. ex. pour escorter les visiteurs). Ces privilèges concernent les zones d'accès et les planifications définies pour ce groupe d'accès.

Les groupes d'accès pour enfants héritent à la fois des privilèges d'accès (c'est-à-dire les zones et les horaires d'accès) et de groupe d'accès (p. ex. pour escorter les visiteurs) de leurs parents. La façon dont cela fonctionne est illustrée dans l'exemple suivant.



Dans cet exemple, les titulaires de carte du groupe d'accès "Siège social" peuvent verrouiller et déverrouiller des zones d'accès, ainsi qu'escorter un visiteur à travers les niveaux 1 et 2. Ils peuvent également accéder à la porte d'entrée car ils héritent des droits d'accès de leur parent immédiat (p. ex. 'Tous les titulaires').
Un visiteur souhaitant passer par les niveaux 3, 4 et 5 devra toutefois être escorté par un titulaire de carte du groupe d'accès "IT Department".

Dans le cadre de la configuration d'un groupe d'accès, vous pouvez configurer la fonctionnalité Lineage (via l'onglet **Lineage**). Voir ***Configurer des groupes d'accès*** (page 34-4) pour la procédure.

Configuration des groupes Access

Introduction

Cette procédure se divise en deux parties :

- Création d'un groupe d'accès,
  (c.-à-d. fournir les informations minimales requises pour créer un nouveau groupe d'accès)
- Configuration d'un groupe d'accès,
  (c'est-à-dire relier les divers éléments à celui-ci - Les divisions, les titulaires de carte, les annexes, les zones d'accès et les champs de données personnelles sont les éléments d'un groupe d'accès).

Vous pouvez créer un nouveau groupe d'accès, puis le configurer ultérieurement, une fois que vous avez configuré les composants nécessaires.

Procédure

Créer le groupe d'accès

1. Cliquez sur **Gérer** dans la barre de menus, puis sur **Groupes d'accès**.
   La fenêtre Liste **des groupes Access** s'ouvre (en arborescence).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...Groupe d'accès**.
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs.
   Pour plus de détails, ***voir l'onglet général*** (page 3-18).
4. Cliquez sur le **bouton** Appliquer**,** et le groupe d'accès est créé.
   Le reste de cette procédure vous permet de configurer entièrement le groupe d'accès.

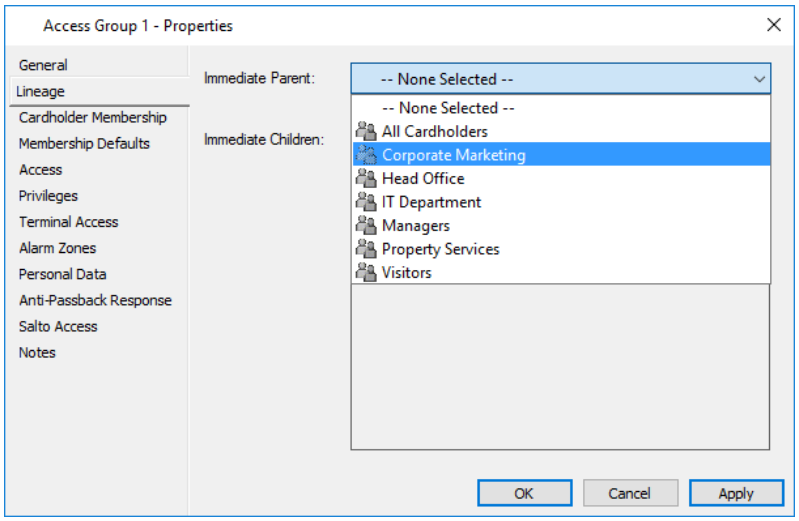
Configurer le groupe d'accès

5. Assurez-vous que les informations suivantes ont déjà été mises en place :
   Divisions
   Consultez la section ***Configuration de la division du système*** (page 9-3).
   Titulaires
   Reportez-vous à la page 32-2 du document ***Ajouter un nouveau titulaire de carte***.
   Horaires
   Accès Horaires = relatifs aux titulaires
   Zone d'accès Horaires = se rapportant à la façon dont les portes de la zone se comportent Voir les ***Horaires*** (page 12-1).
   Zones d'accès
   Inclut une planification de zone d'accès liée
   Reportez-vous à ***Ajout d'une nouvelle zone d'accès*** (page 10-3).

Champs de données personnelles
Reportez-vous à la section Création ***d'un nouveau champ de données personnelles*** (page 33-2).

Notifications
Reportez-vous à Création ***d'un filtre de notification*** (page 35-4).

6. Cliquez sur l'onglet **Lignée**.

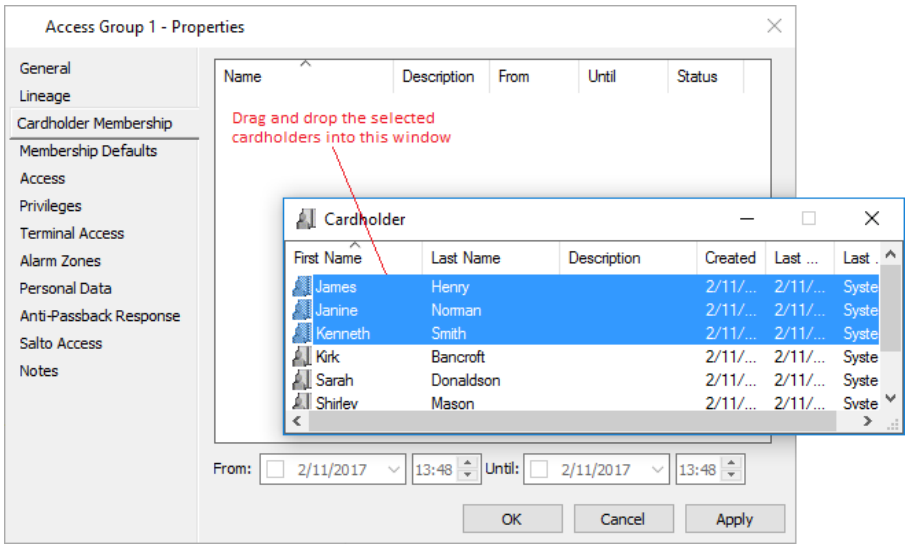


7. Si ce groupe d'accès fait partie d'une hiérarchie, sélectionnez le groupe d'accès "Parent immédiat" dans la liste déroulante.
Tous les privilèges attribués au parent seront hérités par ce groupe d'accès.

8. Cliquez sur l'onglet **Appartenance aux titulaires de carte**.

9. Cliquez sur **Gérer** dans la barre de menus, puis sur **Titulaires de carte**.
La fenêtre Liste principale des titulaires de carte s'ouvre.

10. Sélectionnez les titulaires de carte à appartenir au nouveau groupe d'accès.
Faites-les glisser et déposez-les dans l'**onglet Appartenance au titulaire de carte**.

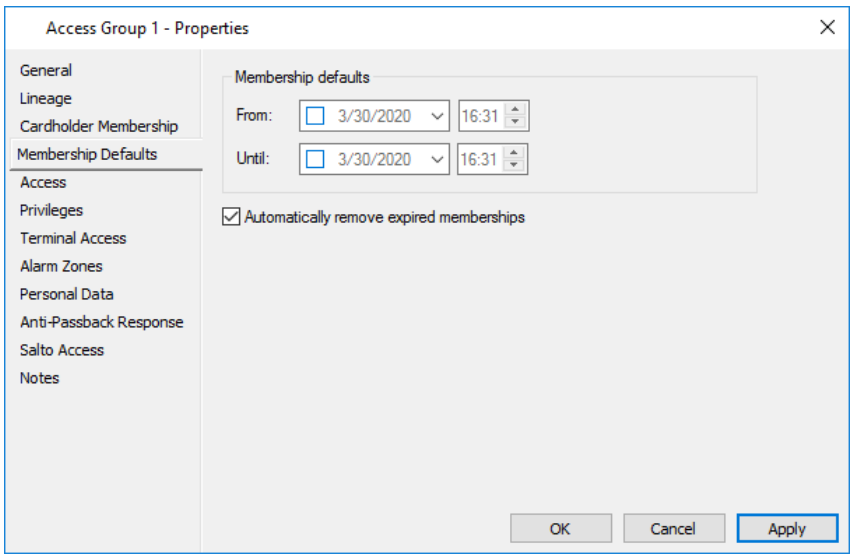


11. Fermez la fenêtre Liste principale des **détenteurs de** carte.

12. Les titulaires de cartes qui n'ont pas de dates "De" et "Jusqu'au" à côté de leurs noms sont membres permanents du groupe Accès.

Si vous voulez que les titulaires de carte soient des membres temporaires (c'est-à-dire qu'ils aient accès pour une période limitée), consultez la section Octroi d'un accès temporaire par ***groupe d'accès (***page 34-18) pour la procédure.

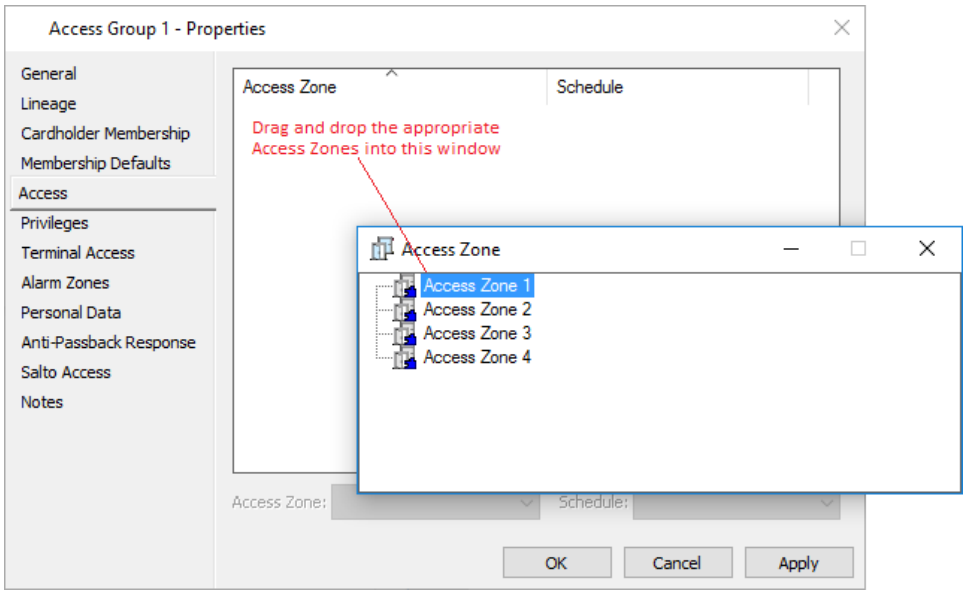
13. Cliquez sur l'onglet **Valeurs par défaut de l'appartenance (Membership Defaults)**.



Cet écran permet de configurer une période d'adhésion pour le groupe d'accès. Par défaut, les dates de début et de fin sont définies sur aucune, par conséquent l'adhésion est permanente. Voir ***Octroi de l'accès temporaire par groupe d'accès*** (page 34-18) pour plus de détails.

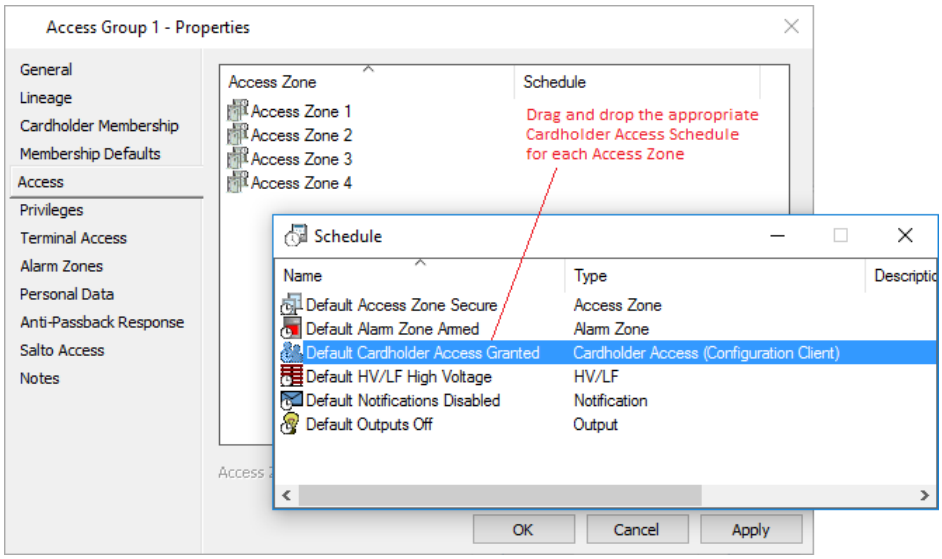
14. Cliquez sur l'onglet **Access**.

15. Cliquez sur **Configurer** dans la barre de menus, puis sur **Zones d'accès**.
La fenêtre Liste principale des zones **Access** s'ouvre.
Sélectionnez les zones appropriées pour ce groupe d'accès.
Faites-les glisser et déposez-les dans l'onglet **Accès**.

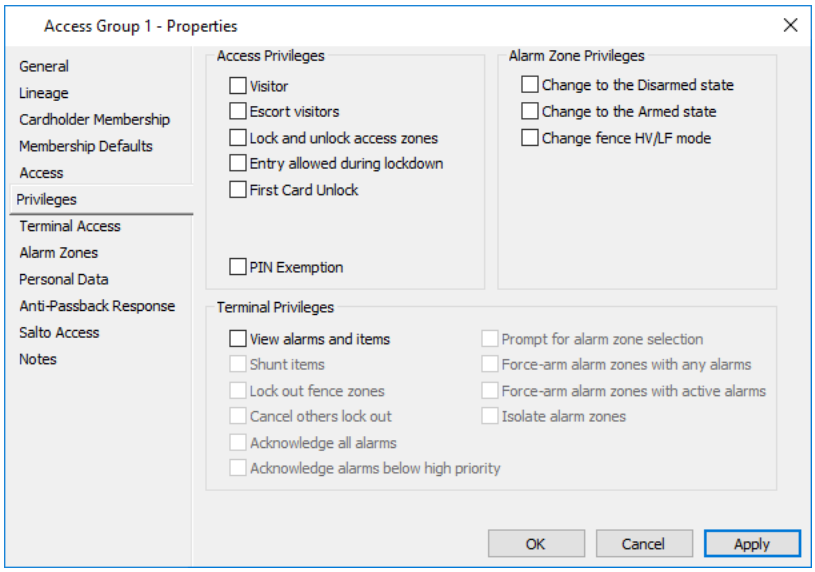


Remarque : Il y a une limite de 255 zones d'alarme/zones d'accès par groupe d'accès et par contrôleur. Si cette limite est dépassée, une alarme sera générée (dans la fenêtre de visionneuse d'alarme) et les 255 premières zones seulement seront envoyées au contrôleur.

16. Fermez la fenêtre Liste principale des **zones d'accès**.
17. Cliquez sur **Configurer** dans la barre de menus, puis sur **Horaires**.
    La fenêtre **Horaires** la liste principale s'ouvre.
18. Sélectionnez les calendriers d'accès appropriés pour ce groupe d'accès.
    Faites-les glisser et déposez-les dans l'onglet **Accès**.



19. Fermez la fenêtre Liste principale **des programmes**.
20. Cliquez sur l'onglet **Privilèges**.



Les privilèges des titulaires de carte sont configurés dans les groupes d'accès. Lorsque vous ajoutez des titulaires de carte à un groupe d'accès, ils héritent automatiquement des privilèges configurés pour ce groupe d'accès. (Pour une explication plus détaillée, voir page 34-2 ***Héritage des privilèges du groupe d'accès***.)

21. Sélectionnez les **privilèges d'accès** appropriés requis pour le groupe d'accès.

Accès privilégié	Permet aux membres...
Visiteur	être escorté à travers les zones d'accès sélectionnées par certains - un avec les privilèges 'Escort' pour les mêmes zones d'accès.
Escorter les visiteurs	escorter les visiteurs dans les zones d'accès (selon les horaires) assignées au groupe d'accès.
Verrouiller et déverrouiller les zones d'accès	modifier l'état d'une zone d'accès à laquelle le groupe d'accès donne accès, à partir d'un lecteur de carte. Ceci est connu sous le nom de "remplacement local". Pour plus de détails, consultez la section ***Configuration des remplacements locaux à l'adresse Lecteurs de cartes*** (page 45-14).
Entrée autorisée pendant le verrouillage	entrez les zones d'accès contenues dans le groupe d'accès lorsque ces zones d'accès sont en mode verrouillé, à condition qu'elles répondent aux critères d'accès requis lors du verrouillage. Lorsqu'un site est placé en mode de verrouillage, certaines personnes (p. ex. les services d'urgence) doivent toujours y entrer. Pour plus de détails, reportez-vous à la section ***Exécution d'une substitution de verrouillage*** (page 10-11).
Premier déverrouillage de la carte	déverrouillez une zone d'accès de l'état SECURE à l'état FREE, une fois l'accès accordé.
PIN Exemption	être exempté de la saisie du code PIN lors de l'entrée dans une zone d'accès configurée pour exiger des identifiants d'accès « Carte + NIP ». La fonction d'exemption de code PIN est prise en charge sur les parkings, mais pas sur les ascenseurs et les casiers. **Remarques :** • **Modes d'accès :** tous les modes d'accès existants avec des codes PIN sont pris en charge. Lorsque le mode Accès est réglé sur le mode « Double authentification - NIP », seules les cartes exemptées de NIP sont exemptées de saisir le NIP et les cartes sans dispense de NIP sont invitées à saisir le NIP. • **Privilèges de zone d'accès :** les utilisateurs appartenant à un groupe d'accès avec exemption de code PIN seront toujours invités à saisir un code PIN lorsqu'ils tenteront de changer de mode d'accès via le lecteur. • **Privilège de zone d'alarme :** les utilisateurs appartenant à un groupe d'accès avec exemption de code PIN seront toujours invités à saisir un code PIN lorsqu'ils tentent d'armer ou de désarmer une zone d'alarme lorsqu'ils sont privilégiés. • **Terminaux :** Si un groupe d'accès avec une exemption de code PIN attribuée a l'une des options de remplacement de double carte « Zone d'accès prioritaire » et « Zone d'alarme d'armement » définie sur le lecteur, les utilisateurs sont exemptés de la saisie du code PIN. « Le code PIN est un code utilisateur » n'est pris en charge que lorsqu'un utilisateur disposant d'une exemption de code PIN a un code utilisateur attribué.

Remarque : Lorsqu'un site est homologué pour porte Aperio, il y aura deux privilèges d'accès supplémentaires comme suit :

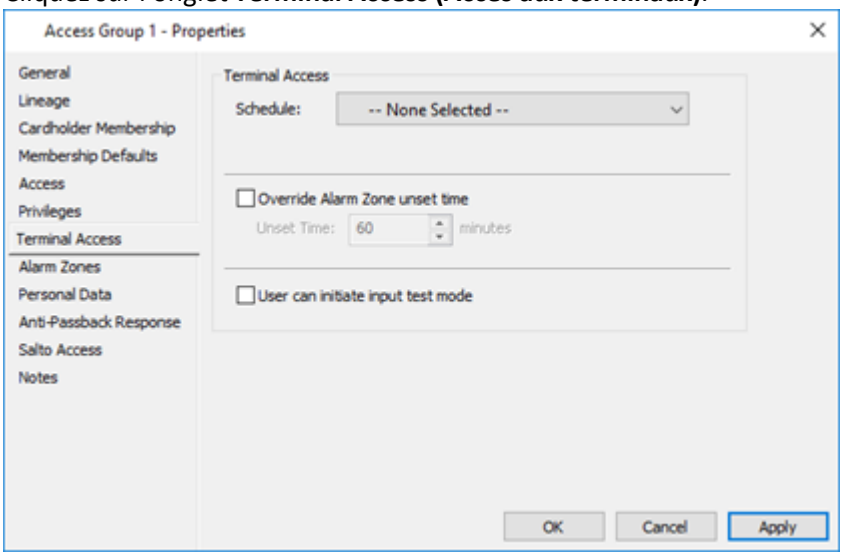
Accès privilégié	Permet aux membres....
Aperio Privacy Override	déverrouillez les portes même en mode Confidentialité. Par défaut = non coché. **Remarques :** • Le mode Confidentialité est activé par un bouton sur certains verrous Aperio. Cette fonctionnalité doit être activée dans le protocole PAP (Aperio Programming Application Protocol) pour prendre effet. • Une porte Aperio fermée, verrouillée et en mode Confidentialité affiche une icône de cadenas rouge et jaune dans la fenêtre **Matériel** de Configuration Client.
Accès hors connexion Aperio	Les détenteurs de carte dans un groupe d'accès avec ce privilège activé auront leurs détails de carte conservés à la porte / serrure Aperio, permettant ainsi au verrou de s'ouvrir pour ces détenteurs de cartes sans connectivité sans fil.

22. Sélectionnez les **privilèges de zone d'alarme** requis pour ce groupe d'accès.

Privilège de zone d'alarme	Permet aux membres...
Passage à l'état Désarmé	désarmer les zones d'alarme associées à toute zone d'accès associée au groupe d'accès.
Changement d'État	Zones d'alarme associées à toute zone d'accès associée au groupe d'accès.
Modifier le mode HV/LF de la clôture	modifier le mode HV/LF d'une zone d'alarme associée à toute zone d'accès associée avec Access Group.

Remarque : La section **Privilèges Terminal** de cet onglet concerne uniquement les terminaux HBUS ou les terminaux HBUS Alarms Only. Par conséquent, ces privilèges ne doivent être sélectionnés que si votre site utilise un de ces terminaux et que ce groupe d'accès les utilise.
Reportez-vous à la section ***Configuration des privilèges de groupe d'accès pour l'accès aux terminaux*** (à la page 34-13) pour plus de détails.

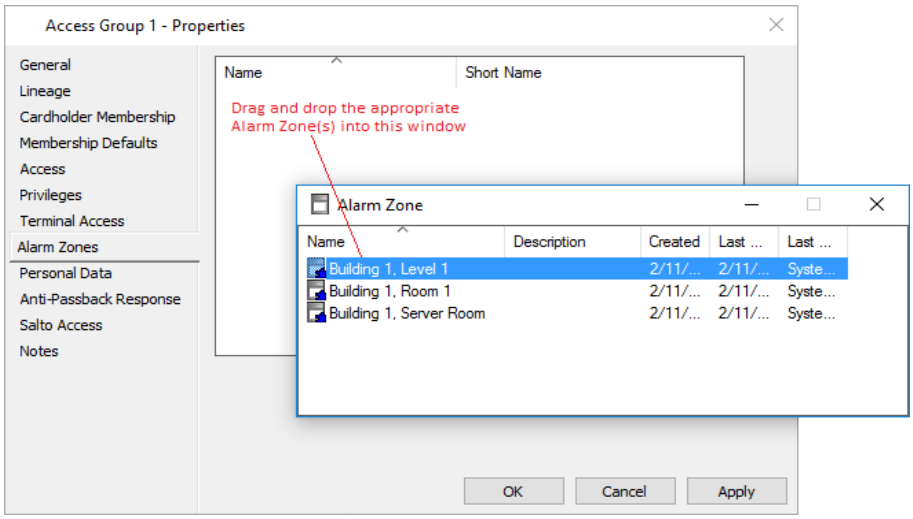
23. Cliquez sur l'onglet **Terminal Access (Accès aux terminaux)**.



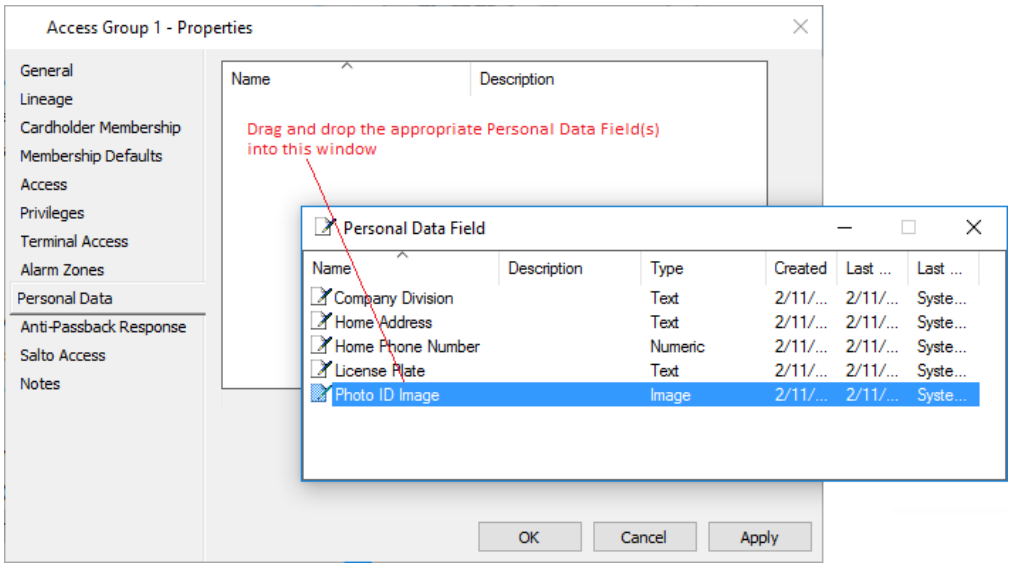
Le calendrier d'accès des titulaires de carte sélectionné ici détermine quand les membres de ce groupe d'accès peuvent se connecter à un terminal HBUS ou à un terminal HBUS Alarmes.

L'onglet **Accès au** terminal peut être utilisé pour configurer des tests périodiques, pour permettre aux membres de ce groupe d'accès de désarmer le système via un terminal. Si cette fonctionnalité est nécessaire, reportez-vous à la section ***Configuration des groupes d'accès pour les modes de test*** (page 47-9) pour plus de détails.

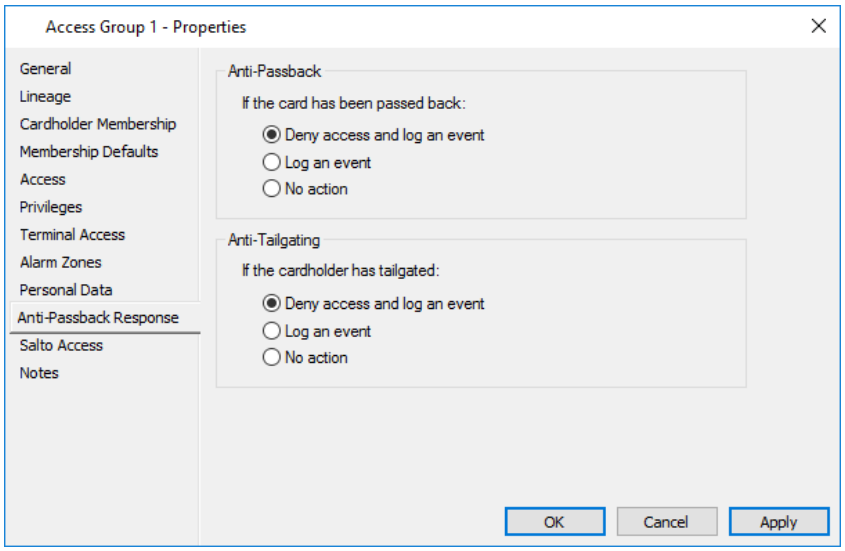
24. Cliquez sur l'onglet **Zones d'alarme**.
25. Cliquez sur **Configurer** dans la barre de menus, puis sur **Zones d'alarme**. La fenêtre de liste principale de zones d'alarme s'affiche.
Sélectionnez les zones d'alarme appropriées pour ce groupe d'accès.
Faites-les glisser et déposez-les dans la fenêtre de l'onglet Zones d'alarme.



26. Fermez la fenêtre de liste principale de la zone d'alarme.
27. Cliquez sur l'onglet **Données personnelles (Personal Data).**
28. Cliquez sur **Configurer** dans la barre de menus, puis sur **Champs de données personnelles**. La fenêtre **Données personnelles - Champ** principal de liste s'ouvre. Sélectionnez les champs de données personnelles appropriés pour ce groupe d'accès. Faites-les glisser et déposez-les dans l'onglet Données personnelles.



29. Fermez la **fenêtre de la liste principale des données personnelles**.
30. Cliquez sur l'onglet **Réponse anti-retour arrière**.



Cet onglet vous permet de configurer les réponses dont vous avez besoin pour les violations anti-retour de passe et les violations anti-balisage.

Terme	Définition
Violation anti-retour	Condition dans laquelle le système a détecté qu'un retour de carte a été effectué (c'est-à-dire qu'un détenteur de carte a tenté d'entrer dans une zone d'accès ou un groupe de zones d'accès, lorsqu'ils sont déjà enregistrés comme dans celle-ci).
Violation de la législation anti-balisage	Condition dans laquelle le système a détecté qu'un détenteur de carte s'est faufilé (c'est-à-dire qu'un détenteur de carte a tenté d'entrer dans une zone d'accès alors qu'ils sont actuellement enregistrés comme étant en dehors de la zone d'accès ou du groupe de zones d'accès à partir duquel ils entrent). **Remarque :** Alors que la réponse anti-tailgating est configurée ici sur le groupe d'accès, l'option "Vérifier la tailgating à la sortie de la zone" est configurée sur la zone d'accès.

31. Cliquez sur les boutons radio appropriés pour les réponses dont vous avez besoin.
32. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes sur ce groupe d'accès.
    Pour plus de détails concernant l'onglet **Notes**, voir ***Notes*** (page 6-81).
33. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Les titulaires de carte appartenant au groupe d'accès peuvent accéder aux zones spécifiées aux heures spécifiées.
Remarque : Ce nouveau groupe d'accès est défini par défaut dans la zone "Enfants immédiats" de l'onglet Lignée du groupe d'accès que vous avez sélectionné comme "Parent immédiat".

Conseils

Outil de recherche
Le déplacement d'éléments individuels (par exemple des zones d'accès) peut être fastidieux. Grâce à l'outil Rechercher, vous pouvez accélérer la procédure :
- Ouvrez la fenêtre Rechercher.
- Définissez les critères de recherche appropriés.
- Dans la fenêtre de liste Rechercher, sélectionnez une plage continue ou les éléments séparés requis.
- Faites glisser les éléments dans la fenêtre Access Group appropriée.

Modification et suppression de groupes d'accès
Reportez-vous à la section Modification des éléments et suppression d'éléments pour obtenir des procédures sur la modification et la suppression de groupes d'accès.

Copier et coller
Une alternative à la méthode glisser-déplacer consiste à utiliser la méthode copier-coller.

Données personnelles, détails
Le ou les champs de données personnelles que vous avez ajoutés à ce groupe d'accès (à l'étape 27) affichent désormais ce groupe d'accès dans l'onglet **Appartenance au groupe** de l'écran Propriétés.

Configuration des privilèges de groupe d'accès pour l'accès aux terminaux

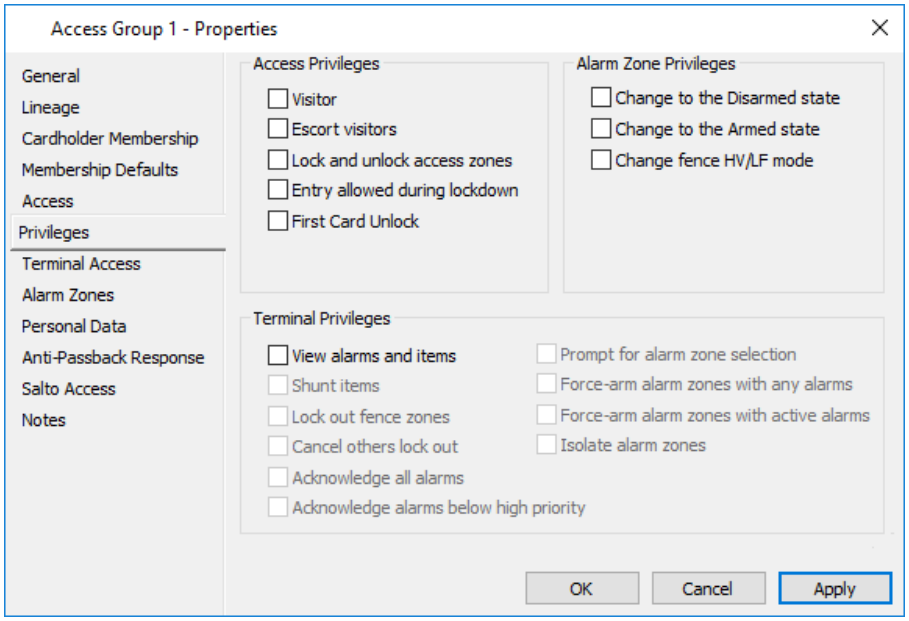
Introduction

Cette procédure décrit comment affecter des zones d'alarme à un groupe d'accès et spécifier les privilèges associés pour l'utilisation du terminal HBUS et du terminal HBUS alarme seulement.

Les opérateurs ont besoin du privilège d'opérateur "Modifier le groupe d'accès" et doivent se trouver dans la même division ou la division parente du groupe d'accès et des zones d'alarme.

Procédure

1. Cliquez sur **Gérer** dans la barre de menus, puis sur Groupes d'accès.
   La fenêtre Liste **des groupes Access** s'ouvre (en arborescence).
2. Mettez en surbrillance le groupe d'accès auquel vous souhaitez affecter des zones d'alarme et **double-cliquez sur** le bouton de la souris.
3. Cliquez sur l'onglet **Privilèges** du groupe d'accès.



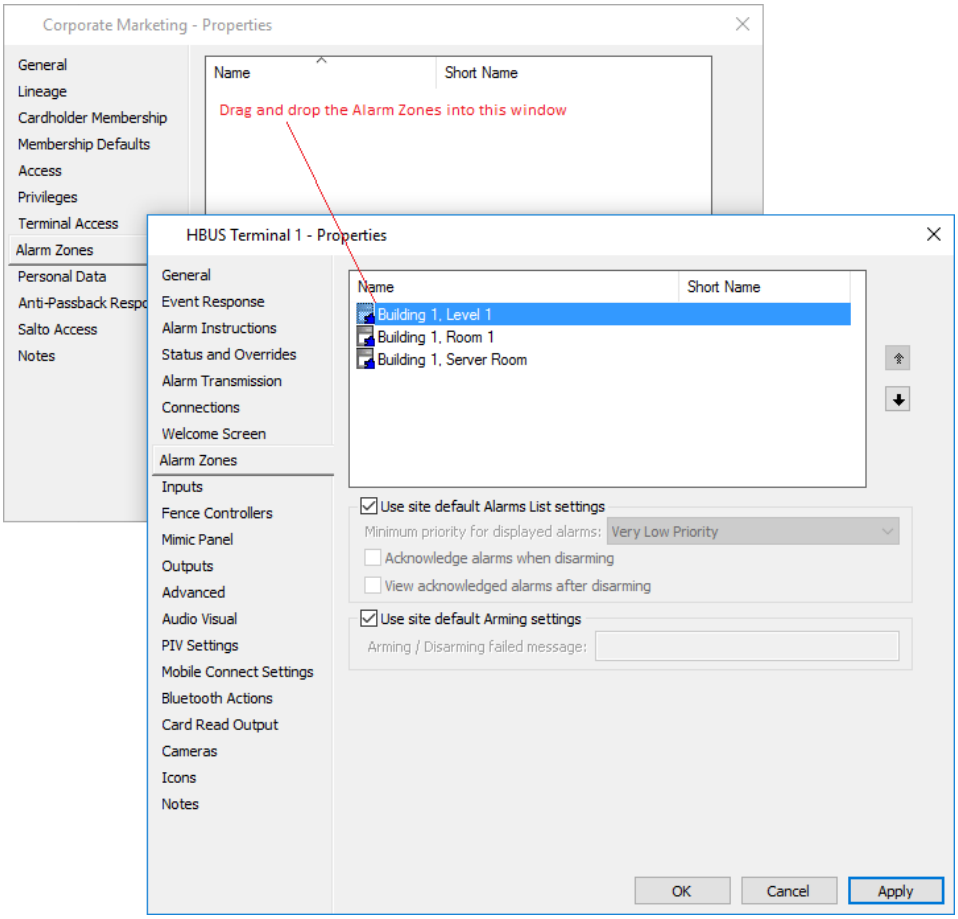
4. Les privilèges d'accès et les privilèges de zone d'alarme ont probablement déjà été configurés lors de la création de ce groupe d'accès. Changez si nécessaire.
5. Dans la section **Privilèges Terminal** de cet onglet, sélectionnez les privilèges appropriés selon les besoins pour le groupe d'accès.

Privilège	Terminaux HBUS
Afficher les alarmes et les éléments	Ce privilège permet à un utilisateur d'afficher toutes les alarmes et tous les éléments disponibles sur un terminal HBUS Alarms Only ou HBUS.

Privilège	Terminaux HBUS
Éléments de fermeture	Ce privilège permet à un utilisateur de fermer et de déverrouiller des éléments à l'aide d'un terminal HBUS ou d'un terminal d'alertes HBUS uniquement.
Reconnaître toutes les alarmes	Ce privilège permet à un utilisateur d'accuser réception de toutes les alarmes disponibles à l'aide d'un terminal HBUS ou d'un terminal d'alarmes HBUS uniquement.
Reconnaître les alarmes en dessous de la priorité élevée	Ce privilège permet à un utilisateur d'accuser réception de toutes les alarmes disponibles en dessous de la priorité élevée à l'aide d'un terminal HBUS ou d'un terminal d'alarmes HBUS uniquement.
Verrouiller les zones de clôture	Ce privilège permet à un utilisateur de verrouiller les zones de clôture sélectionnées à l'aide d'un terminal HBUS Alarmes ou Alarmes HBUS uniquement. La clôture ne peut pas être activée en mode verrouillage. Le verrouillage est persistant lors du redémarrage d'un contrôleur de clôture ou d'un contrôleur (il n'est pas persistant lors du redémarrage d'un contrôleur DIP2). Seul l'utilisateur qui a placé la clôture en mode de verrouillage peut supprimer le mode de verrouillage (sauf si le privilège "Annuler d'autres verrouillages" a été attribué à un autre utilisateur). Le mode de verrouillage ne peut être supprimé qu'à l'aide du terminal HBUS ou du terminal d'alarme HBUS uniquement qui a été utilisé pour mettre la clôture en verrouillage.
Annuler les autres verrouillages	Ce privilège permet à un utilisateur d'annuler le verrouillage des zones de clôture sélectionnées initié par un autre utilisateur. Ceci n'est possible qu'à partir du terminal HBUS ou du terminal HBUS Alarms Only qui a été utilisé pour mettre la clôture en lock-out.
Demander la sélection de la zone d'alarme	Ce privilège permet à un utilisateur d'afficher une liste des zones d'alarme pour lesquelles l'affectation de groupe d'accès de l'utilisateur fournit un privilège, à partir de l'écran Menu d'un terminal ou d'alarmes HBUS uniquement Terminal.
Zones d'alarme force-bras avec alarme	Si une zone d'alarme n'a normalement pas d'armement parce qu'il y a des alarmes potentielles, non reconnues ou actives, en ayant ce privilège et le privilège opérateur "Remplacer" ou "Remplacer par priorité moyenne", un utilisateur aura la possibilité de forcer l'armement de la zone d'alarme, lorsqu'il s'arme à partir d'un terminal HBUS ou d'un terminal HBUS Alarmes seulement. **Remarques :**

Privilège	Terminaux HBUS
	• Si cette option est sélectionnée, la **zone d'alarme Force-arm avec l'**option Alarmes actives (ci-dessous) devient désactivée. • Sans ce privilège, les options force-bras ne sont pas disponibles.
Zones d'alarme force-bras avec alarmes actives	Si une zone d'alarme n'a normalement pas été activée en raison de l'existence d'alarmes actives, en disposant de ce privilège et du privilège d'opérateur "Remplacer" ou "Remplacer par priorité moyenne", un utilisateur aura la possibilité de forcer l'activation de la zone d'alarme, lors de l'armement à partir d'un terminal HBUS ou d'un terminal d'alarmes HBUS uniquement (à condition que cela n'entraîne aucune nouvelle alarme). **Remarques :** • Si cette option est sélectionnée, la **zone d'alarme Force-arm avec une** option d'**alarme** (ci-dessus) devient désactivée. • Sans ce privilège, les options force-arm ne sont pas disponibles sur le terminal HBUS ou le terminal HBUS Alarms Only.
Isoler les zones d'alarme	Si une zone d'alarme n'est normalement pas définie parce qu'il y a des entrées ouvertes ou qu'une zone de clôture est en état d'alarme, en disposant de ce privilège, un utilisateur aura la possibilité d'isoler automatiquement les zones d'alarme d'entrée, lors de l'armement à partir d'un terminal HBUS ou d'un terminal d'alarmes HBUS uniquement. **Remarque :** Sans ce privilège, les options d'auto-isolation ne sont pas disponibles.

6. Cliquez sur l'onglet **Zones d'alarme**.
   Cet onglet fournit une grille de zones d'alarme qui peuvent être contrôlées à l'aide des terminaux HBUS et des terminaux d'alarmes HBUS uniquement.
7. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**. La fenêtre Liste principale du matériel s'ouvre.
8. Mettez en surbrillance le terminal HBUS approprié ou le terminal HBUS Alarms Only, et **double-cliquez sur le bouton de la souris**.
9. Cliquez sur l'onglet **Zones d'alarme** du terminal HBUS ou du terminal HBUS Alarms Only Terminal.
10. Mettez en surbrillance les zones d'alarme à gérer par ce groupe d'accès, puis faites-les glisser etles déposer dans son onglet Zones d'alarme.



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 groupe d'accès a été mis à jour avec les nouvelles zones d'alarme et les privilèges pour l'utilisation du terminal HBUS ou du terminal HBUS Alarms Only.

Accès temporaire

Présentation de l'accès temporaire

Un titulaire de carte peut être un membre temporaire d'un groupe d'accès (c'est-à-dire qu'il n'est membre que pour une période spécifiée entre la date de début et la date de fin et l'heure de l'adhésion temporaire). Pendant ce temps, un détenteur de carte ayant un accès temporaire a les mêmes droits que tout autre membre de ce groupe d'accès.
L'accès temporaire peut être configuré par un groupe d'accès ou par un titulaire de carte.

Champs de données personnelles

Tous les champs de données personnelles (PDF) appartenant à un groupe d'accès particulier peuvent être associés au titulaire de la carte dès que les informations d'accès temporaire sont entrées (pas nécessairement actives), jusqu'à ce que l'enregistrement d'accès temporaire soit supprimé. Par conséquent, si les enregistrements d'accès temporaire ne sont jamais supprimés, le membre temporaire conservera ce fichier PDF. Si toutefois les enregistrements d'accès temporaire sont supprimés, le PDF sera également supprimé pour le titulaire de la carte.

Par exemple:
Un étudiant peut être inscrit à un cours qui ne commence pas avant juin et qui nécessite un accès spécial et une information particulière qui sera saisie dans un PDF. Au début de l'année, cet étudiant s'inscrit au cours et un accès temporaire est mis en place pour commencer au début du mois de juin et se terminer en novembre. Le titulaire de la carte verrait le PDF ajouté à ses informations sur le titulaire de la carte et les données requises pourront être entrées au début de l'année même si cela ne sera pas nécessaire avant plus tard.
Si le système est configuré pour supprimer tous les accès temporaires après leur expiration, le fichier PDF disparaîtra des informations des détenteurs de cartes à la fin de novembre lorsque l'accès aura expiré. Si le système n'est PAS configuré pour supprimer les enregistrements d'accès temporaire, le détenteur de la carte conservera le fichier PDF jusqu'à ce que les enregistrements soient manuellement effacés.

Plusieurs adhésions temporaires

Un titulaire de carte peut avoir plusieurs adhésions temporaires au même groupe d'accès.
Par exemple:
Une université a deux cours qui partagent une ressource.
Le cours 1 dure du 14/02 au 21/04.
Le cours 2s'étend du 18/03 au 25/07.
Les étudiants des deux cours doivent avoir accès à un laboratoire informatique, et il y a plusieurs étudiants qui suivent les deux cours. Ces étudiants doivent donc avoir accès à l'ordinateur du 14/02 au 25/07.

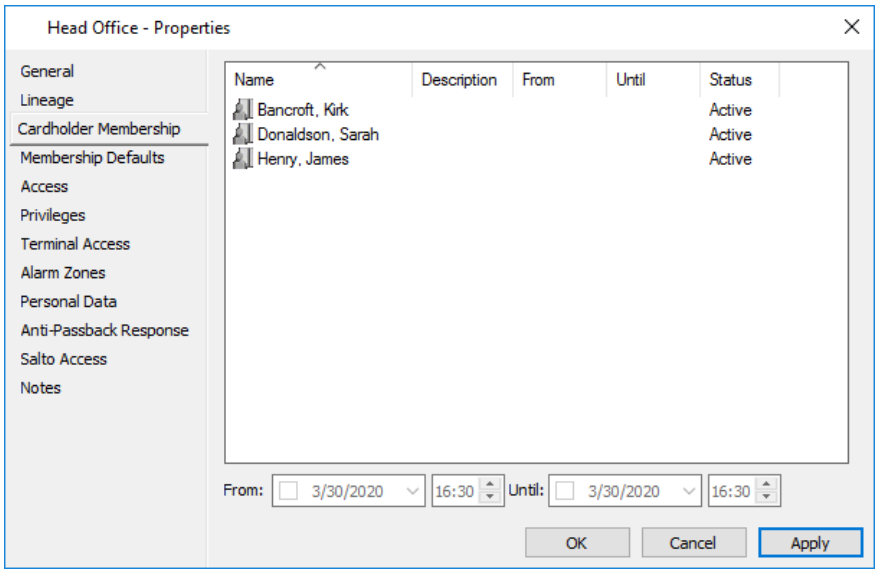
Octroi de l'accès temporaire par groupe d'accès

Introduction

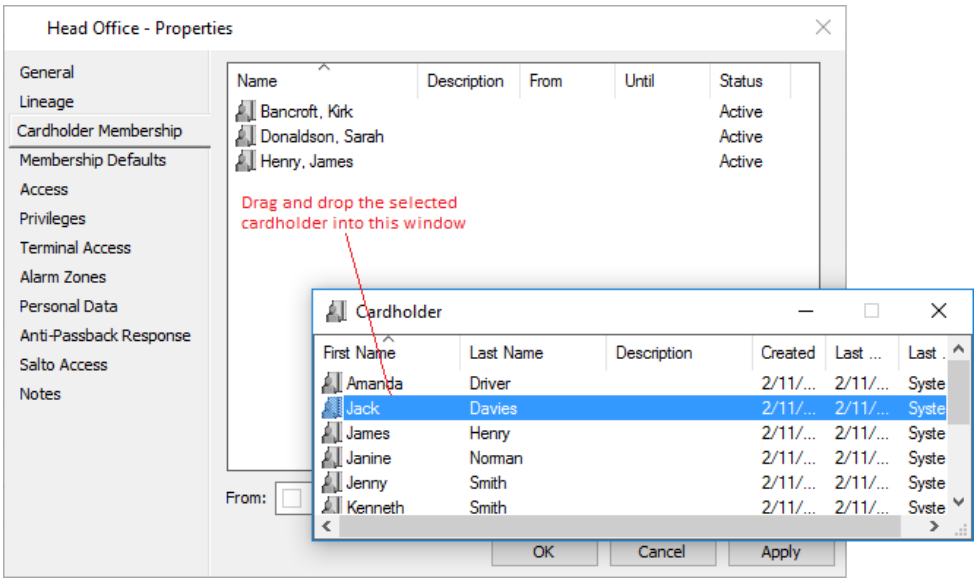
Cette procédure explique en détail comment accorder un accès temporaire aux membres d'un groupe d'accès.

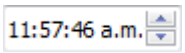
Procédure

1. Cliquez sur **Gérer** dans la barre de menus, puis sur Groupes d'accès.
   La fenêtre Liste **des groupes Access** s'ouvre (en arborescence).
2. Mettez en surbrillance le groupe Access auquel vous souhaitez ajouter des membres temporaires.
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Appartenance au titulaire de la carte**.

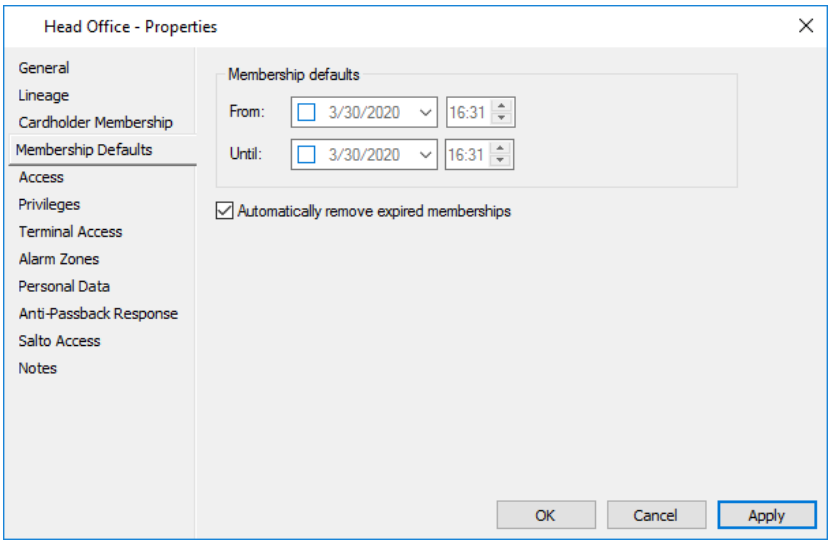


5. Cliquez sur **Gérer** dans la barre de menus, puis sur **Titulaires de carte**.
   La fenêtre Liste principale des titulaires de carte s'ouvre.
6. Sélectionnez le ou les titulaires de carte que vous souhaitez ajouter en tant que membres temporaires au groupe d'accès.
   Faites-les glisser et déposez-les dans l'**onglet Appartenance au titulaire de carte**.



7. Fermez la fenêtre Liste principale des **détenteurs de** carte.
8. Mettez en surbrillance le titulaire de la carte (onglet **Appartenance au titulaire de la carte**) qui nécessite un accès temporaire.
   Les champs Date "Du" et Date "Jusqu'au" sont activés.
   Remarque :
   L'ordre des colonnes peut être repositionné si vous le souhaitez (par exemple, vous pouvez trouver que les colonnes Date sont d'abord utiles pour que vous puissiez trier par date et voir quels détenteurs de cartes ont les mêmes périodes d'accès temporaires). Voir ***Repositionnement des en-têtes de colonne*** (page3-6) pour la procédure.
9. Cliquez sur la zone de liste déroulante "De" et sélectionnez la date à partir de laquelle le détenteur de la carte doit avoir accès.
   La case à cocher Heure de début est activée et la date de début s'affiche désormais dans la grille principale à côté du nom du détenteur de la carte.
10. Modifiez l'heure dans la case 

"De" à partir de laquelle le titulaire doit accéder à cette date.
11. Répétez les étapes 9 et 10 pour les champs "Jusqu'à" (c'est-à-dire la date et l'heure du dernier jour auquel le détenteur de la carte doit avoir accès).
    La date 'Jusqu'au' s'affiche dans la grille principale à côté du nom du détenteur de la carte.
12. Cliquez sur l'onglet **Valeurs par défaut de l'appartenance (Membership Defaults)**.



Par défaut, les dates de début et de fin sont définies sur aucune, ce qui signifie que par défaut, l'adhésion est permanente.

13. Voulez-vous que les membres temporaires soient supprimés de l'onglet **Appartenance** au titulaire de carte lorsque leur période d'accès temporaire expire ?

Si...	alors...
oui	laissez la case à cocher **Supprimer automatiquement les appartenances expirées** activée. **Remarque :** En cochant la case, toutes les adhésions expirées sont automatiquement supprimées de la liste de l'onglet **Adhésion** du **titulaire de carte** lorsqu'elles expirent.
non	désactivez la case à cocher **Supprimer automatiquement les adhésions expirées** s'affiche. **Remarque :** En décochant la case, les détenteurs de carte ayant un accès temporaire resteront dans la liste de l'onglet **Appartenance des titulaires de carte** une fois leur période d'accès expirée.

Remarque : Les titulaires de carte ne peuvent appartenir qu'à 255 groupes d'accès uniques, actifs ou en attente.

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

Résultat

Un groupe Access compte des membres temporaires.
Remarques :

- Le ou les détenteurs de carte auxquels vous avez accordé un accès temporaire s'affichent désormais dans l'onglet **Groupes d'accès**.
- Si deux opérateurs ajoutent simultanément la même appartenance temporaire (l'un via les propriétés de groupe d'accès et l'autre via les propriétés de titulaire de carte), **deux** nouvelles apparaîtront dans les propriétés de **groupe d'accès et de titulaire de carte.** Deux événements seront également générés, ce qui indique que des opérateurs distincts ont créé les nouveaux membres.

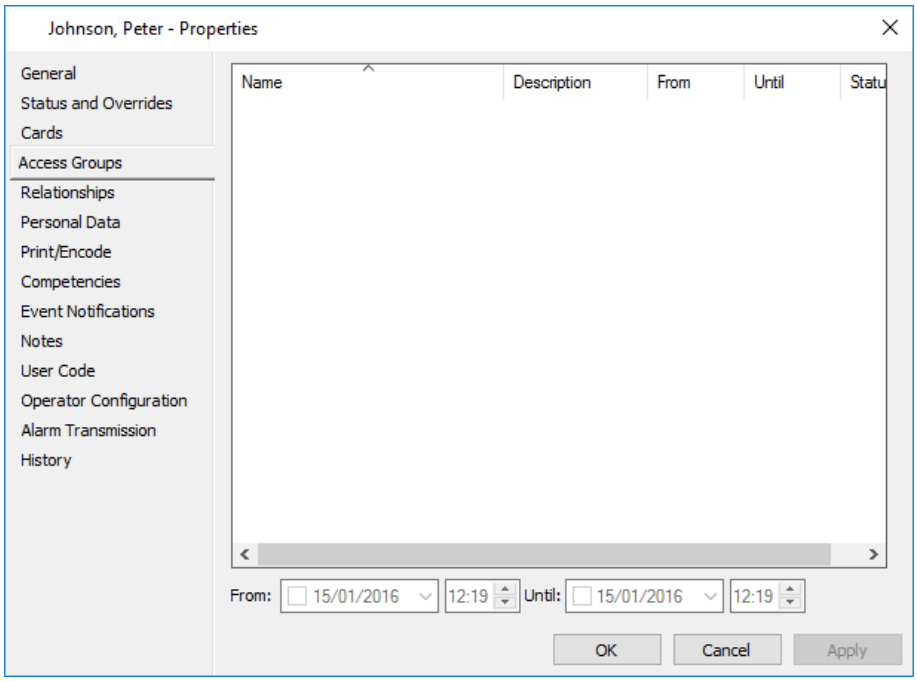
Octroi d'un accès temporaire par le titulaire de carte

Introduction

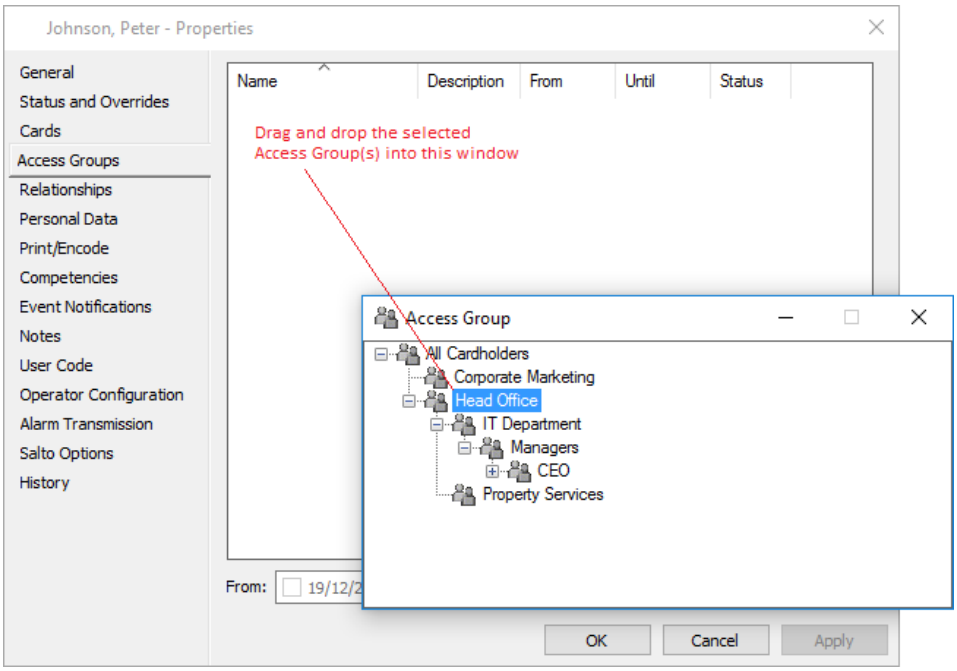
Cette procédure explique en détail comment accorder un accès temporaire aux groupes d'accès pour les titulaires de carte individuels.

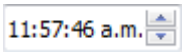
Procédure

1. Cliquez sur Gérer dans la barre de menu, puis sur Titulaires de carte.
   La fenêtre Liste principale des titulaires de carte s'ouvre (en mode grille).
2. Mettez en surbrillance le détenteur de la carte auquel vous souhaitez accorder un accès temporaire.
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Groupe d'Accès**.



5. Cliquez sur **Gérer** dans la barre de menus, puis sur **Groupes d'accès**.
   La fenêtre Liste principale **du groupe Access** s'ouvre.
6. Sélectionnez le ou les groupes d'accès auxquels vous souhaitez accorder un accès temporaire à ce détenteur de carte.
   Faites-les glisser et déposez-les dans l'onglet Groupes d'accès.



7. Fermez la fenêtre Liste principale **du groupe d'accès**.
8. Mettez en surbrillance le groupe d'accès (dans l'onglet **Groupes d'accès**) pour lequel ce titulaire de carte nécessite un accès temporaire pour.
   Les champs Date de début et Date de fin sont activés.
9. Cliquez sur la zone de liste déroulante "De" et sélectionnez la date à partir de laquelle le détenteur de la carte doit avoir accès.
   La case à cocher Heure de début est activée et la date de début s'affiche désormais dans la grille principale à côté du nom du groupe d'accès.
10. Modifiez l'heure dans la case 

"De" à partir de laquelle le titulaire doit accéder à cette date.
11. Répétez les étapes 9 et 10 pour les champs "Jusqu'à" (c'est-à-dire la date et l'heure du dernier jour auquel le détenteur de la carte doit avoir accès).
    La date 'Jusqu'au' s'affiche dans la grille principale à côté du nom du groupe d'accès.
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 titulaire de carte a maintenant un accès temporaire à un groupe d'accès.
Remarques :

- Ce titulaire de carte s'affichera maintenant dans l'onglet **Appartenance au titulaire de carte** des propriétés du groupe d'accès.

- Dans l'onglet **Adhésion des titulaires de carte**, les titulaires de carte affichent des couleurs différentes pour indiquer si leur adhésion est en état "en attente" ou "expiré".
- Si deux opérateurs ajoutent simultanément la même appartenance temporaire (l'un via les propriétés de groupe d'accès et l'autre via les propriétés de titulaire de carte), **deux** nouvelles apparaîtront dans les propriétés de **groupe d'accès et de titulaire de carte**.
  Deux événements seront également générés, ce qui indique que des opérateurs séparés ont créé les nouvelles appartenances.

Suppression des adhésions temporaires

Introduction

Les enregistrements d'adhésion temporaires expirés peuvent être supprimés des groupes d'accès. Bien que le Centre de commandes puisse être configuré pour supprimer automatiquement les appartenances temporaires à l'expiration de la période (via une case à cocher de l'**onglet Valeurs par défaut des appartenances au** groupe d'accès)**,** elles peuvent également être supprimées manuellement.
Cette procédure décrit comment supprimer manuellement les enregistrements d'adhésion temporaires expirés, ce qui peut être fait soit par un groupe d'accès, soit par un titulaire de carte individuel.

Procédure

Via Groupe d'accès

1. Cliquez sur **Gérer** dans la barre de menus, puis sur **Groupes d'accès**.
   La fenêtre Liste **des groupes Access** s'ouvre (en arborescence).
2. Mettez en surbrillance le groupe d'accès requis.
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Appartenance aux titulaires de carte**.
5. Mettez en évidence le ou les titulaires de la carte dont l'adhésion a expiré.
   Remarque : Plusieurs titulaires peuvent être sélectionnés à la fois en maintenant la touche <**Maj**> ou <**Ctrl**> sur votre clavier en cliquant sur le bouton de la souris.
6. **Cliquez avec le bouton droit** de la souris et sélectionnez **Supprimer de la liste**. Le ou les détenteurs de cartes sont supprimés de la liste et une fois que vous avez cliqué sur **Appliquer**, les enregistrements du groupe d'accès disparaissent également de l'onglet **Groupes d'accès** sur les propriétés des détenteurs de cartes.

Via le titulaire de la carte

1. Cliquez sur **Gérer** dans la barre de menu, puis sur Titulaires de carte.
   La fenêtre (en mode grille) s'ouvre dans la liste principale des **titulaires de carte.**
2. Mettez en surbrillance le titulaire de carte requis.
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Groupes d'accès**.
5. Mettez en surbrillance le **groupe d'accès**.
6. **Cliquez avec le bouton droit** de la souris et sélectionnez **Supprimer de la liste**.
   Le groupe d'accès est supprimé de la liste et une fois que vous avez cliqué sur Appliquer, les enregistrements du titulaire de la carte disparaissent également de l'onglet **Appartenance au titulaire de** la carte sur les propriétés du groupe d'accès.

Résultat

Les enregistrements d'accès temporaires expirés ont été supprimés du système.

Chapitre 35 : Notifications

Cette fonctionnalité permet aux administrateurs de configurer le Centre de commandes pour qu'il envoie automatiquement des notifications :

- les événements importants, tels que les alarmes, aux titulaires de carte par SMS sur leur téléphone mobile ou à une adresse e-mail désignée. Les destinataires de messages bénéficiant d'un privilège approprié auront la possibilité de répondre à des messages pour accuser réception d'alarmes. Voir ***Accusés de réception par SMS ou par courriel*** (page 35-28) pour la procédure.
- les avertissements d'expiration de la carte et des compétences aux personnes, aux administrateurs ou aux superviseurs.

Remarques :

- Les utilisateurs de Mobile Connect ne peuvent pas recevoir de notifications d'alarme, mais peuvent recevoir des notifications de diffusion.
  Seuls les opérateurs peuvent recevoir des notifications d'alarme, donc uniquement vers l'application Mobile Command Centre, et non vers Mobile Connect.
- Le contenu des messages ne sera écrit qu'en utilisant la langue du serveur local.
- Le Command Centre ne remplace pas les protocoles pris en charge par défaut par Mailkit, TLS1.2 et TLS1.3.

Notifications mobiles

L'activation des notifications mobiles permet à un site du Centre de commandes d'envoyer des notifications d'alarme aux utilisateurs du client mobile. La sélection d'une notification vous permet d'afficher les détails de l'alarme dans le client mobile.
Seules les notifications d'alarme du site du Centre de commandes le plus récent auxquelles l'utilisateur du Client mobile s'est connecté sero nt envoyées. Seules les alarmes sont envoyées en tant que notifications, pas en tant qu'événements.

Remarque : Si vous recevez des notifications du site A, puis que vous vous connectez au site B (où les notifications mobiles ne sont pas activées), vous continuerez à recevoir des notifications du site précédent (site A).

Notifications personnalisées

Les utilisateurs peuvent créer des notifications par e-mail personnalisées pour les gardes, les titulaires de carte, les administrateurs, les superviseurs et les membres du groupe d'accès. Les utilisateurs peuvent personnaliser le libellé de la ligne d'objet de l'e-mail, spécifier la police et la couleur du corps de l'e-mail, modifier le contenu dans le corps de l'e-mail et ajouter des images à l'e-mail, entre autres choses.

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

Notifications améliorées

Les notifications améliorées permettent d'envoyer automatiquement des e-mails à un titulaire de carte au sein d'un groupe Access lorsqu'un événement qui se rapporte directement à ce détenteur de carte. Ceci est configuré en affectant un filtre de notification à ce groupe d'accès dans la configuration du filtre de notifications uniquement. Les paramètres de « notification d'événement » pour le titulaire de carte ne s'appliquent pas aux notifications personnalisées. Les notifications personnalisées peuvent être configurées via Configuration Client ou Command Center Client, et sont liées uniquement aux événements (pas aux expirations).

Par exemple :

Le groupe d'accès A contient les détenteurs de cartes X, Y et Z. Lorsque les détenteurs de cartes Z possèdent leur carte, un courriel est envoyé au détenteur de cartes Z pour l'informer qu'un événement qui les concerne s'est produit. Les titulaires de carte X et Y ne sont pas informés de l'événement d'accès du titulaire Z, même s'ils font partie du même groupe d'accès, parce que l'événement ne concerne pas spécifiquement les titulaires X et Y.

Pour utiliser la fonctionnalité de notifications améliorées, vous devez disposer d'un contrôleur Gallagher configuré avec, au minimum, un lecteur de carte, une zone d'accès et une porte. Reportez-vous à ***Processus global - Configuration des notifications*** (page 35-3) pour plus d'informations sur la façon de configurer les notifications améliorées.

Exemples d'utilisation de cette fonction :

- Les agents de sécurité peuvent diriger tout ou partie des événements/alarmes vers leur PDA (e-mail) ou leur téléphone mobile à la sortie de la salle de contrôle.
- Les entrepreneurs en maintenance peuvent recevoir des alarmes de maintenance (par exemple un avertissement de faible batterie) par SMS ou par e-mail.
- Après les heures de bureau et les week-ends ou jours fériés, les gestionnaires de bâtiments peuvent être informés par téléphone mobile de toutes les alarmes hautement prioritaires se produisant sur leur installation.
- Le personnel concerné (gestionnaires, superviseurs, administrateurs, etc.) peut recevoir les avis d'événements d'autres titulaires de carte (p. ex., Compétence des titulaires de carte expirée) et prendre les mesures appropriées.
- Les exploitants peuvent aviser un groupe de personnel des dangers sur le site, des expirations à venir ou des avis généraux comme les essais d'alarme d'incendie.

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

- ***Processus global*** - ***Configuration des notifications*** (page 35-3)
- ***Création d'un filtre de notification*** (page 35-5)
- ***Définition des PDF "de carte électronique" et "mobile"*** (page 35-9)
- ***Activation des notifications d'événement/d'alarme pour un titulaire de carte*** (page 35-10)
- ***Définition des valeurs de seuil de notification d'expiration*** (page 35-14)
- ***Configuration des rôles*** (page 35-17)
- ***Affectation de titulaires de carte à des rôles par modification en bloc*** (page 35-20)
- ***Copie de tous les titulaires de carte*** (page 35-23)
- ***Exemples de notification*** (page 35-25)
- ***Accusé de réception d'alarmes par SMS ou par e-mail*** (page 35-28)

Processus global- configuration des notifications

Introduction

Cette section décrit le processus global (à exécuter par l'administrateur système) de configuration de Command Center for Messaging.
Cinq types de notifications peuvent être configurés dans le Centre de commandes :

- Avis d'événement/d'alarme aux détenteurs de cartes spécifiés ;
- Notifications d'événements/d'alarmes aux titulaires de cartes connexes au sein d'un groupe d'accès (Notifications améliorées) ;
- Notifications d'expiration des cartes et des compétences ;
- Les Notifications De Diffusion ; et
- Notifications mobiles pour les utilisateurs des clients mobiles.

Au besoin, ce processus fait référence à des procédures distinctes, étape par étape, qui sont détaillées ailleurs (c.-à-d., soit en tant que procédures distinctes dans cette section, soit dans d'autres sections de cette aide).
Remarque : Pour vous aider à comprendre le fonctionnement de la fonctionnalité Notifications et les différents composants à configurer en fonction de ce que votre site souhaite réaliser, consultez ***Exemples de notification*** (page 35-25).

Processus

Suivez les étapes ci-dessous pour connaître le type de notification que vous souhaitez configurer :

Configuration des notifications d'événements/d'alarmes et des notifications améliorées

1. Définissez les propriétés des serveurs SMS, e-mail et de notification. Référez-vous à Notifications, E-mail sortant, E-mail entrant et Mobile/SMS Notifications pour les procédures.
2. Configurer les filtres de notification.
   Les filtres de notification définissent les types d'événements/d'alarmes et les sources d'événements (portes, entrées, etc.) sur lesquels une personne sera informée. Reportez-vous à Création ***d'un filtre de notification*** (page 35-5) pour la procédure.
3. Créez des fichiers PDF de type "Email" et "Mobile", affectez-les à un groupe d'accès et entrez des adresses e-mail et des numéros de téléphone mobile pour tous les titulaires/opérateurs de carte qui doivent recevoir des notifications par e-mail et par SMS de certains événements et/ou alarmes.
   Reportez-vous à la section ***Définition des PDF "Courriel" et "Mobile" des titulaires de carte*** (page 35-9) pour la procédure.
4. Activez les titulaires de carte qui peuvent recevoir des messages, ainsi que le moment et la manière dont ils doivent être envoyés. Reportez-vous à la ***section Activation des notifications d'événement/d'alarme pour un titulaire de carte*** (à la page35-10) pour la procédure.
   Remarque : Passez à l'étape 5 si vous voulez configurer les notifications améliorées. Sinon, arrêtez-vous ici.

5. Affecter des groupes d'accès aux filtres de notification (ceci permet aux titulaires de carte d'être envoyés des notifications d'événements qui sont liés à eux). Reportez-vous à Création ***d'un filtre de notification*** (page 35-5) pour la procédure.
6. Si vous souhaitez qu'une autre personne (par exemple, un superviseur ou un administrateur) reçoive les mêmes notifications qu'un titulaire de carte, créez un rôle et affectez à la fois l'employé (titulaire de carte) et la personne supplémentaire au rôle.
   Reportez-vous à la ***section Configuration des rôles*** (page 35-17) pour la procédure.

Configuration des notifications d'expiration des cartes

1. Définissez les propriétés des serveurs SMS, e-mail et de notification.
   Référez-vous à Notifications, E-mail sortant, E-mail entrant et Mobile/SMS Notifications pour les procédures.
2. Définissez l'heure à laquelle la procédure quotidienne de notification d'expiration de la carte et de la compétence doit être exécutée.
   Reportez-vous aux notifications.
3. Créez des fichiers PDF de type "Email" et "Mobile", affectez-les à un groupe d'accès, et entrez des adresses e-mail et des numéros de téléphone mobile pour tous les titulaires/opérateurs de carte qui doivent recevoir un avis par e-mail et par SMS d'expiration de la carte et de la compétence en attente.
   Reportez-vous à la section ***Définition des PDF "Courriel" et "Mobile" des titulaires de carte*** (page 35-9) pour la procédure.
4. Déterminez les valeurs du seuil d'expiration des cartes et des compétences.
   Reportez-vous à ***Définition des valeurs de seuil de notification d'expiration*** (page 35-14) pour la procédure.
5. Créez des rôles pour définir les relations entre les détenteurs de cartes (aux fins des notifications d'acheminement) et affectez les détenteurs de cartes aux rôles.
   Reportez-vous à la ***section Configuration des rôles (***page 35-17) pour la procédure.

Configuration des notifications de diffusion

Reportez-vous à la rubrique *"Configuration des notifications de diffusion"* de l'aide en ligne du Centre de commandes.

Configuration des notifications mobiles

1. Activer les notifications mobiles.
   Reportez-vous à la section ***Notifications mobiles/SMS*** (page 6-54) pour la procédure.
2. Connectez le Centre de commandes au Cloud.
   Reportez-vous à ***Connexion au Cloud (***page 31-3) pour la procédure.
3. Configurer les filtres de notification. Les filtres de notification définissent les alarmes qui seront envoyées en tant que notifications mobiles.
   Reportez-vous à Création ***d'un filtre de notification (***page 35-5) pour la procédure.
4. Activez les utilisateurs du client mobile qui peuvent recevoir des notifications mobiles et le moment où elles doivent être envoyées. Reportez-vous à la ***section Activation des notifications d'événement/d'alarme pour un titulaire de carte*** (à la page 35-10) pour la procédure.

Création d'un filtre de notification

Introduction

Un filtre de notification est un ensemble de critères déterminant les événements et les alarmes qui doivent être notifiés aux titulaires de carte. Il existe deux façons d'affecter un filtre Notification à un titulaire de carte :

- Affectation du filtre de notification au titulaire de la carte dans l'onglet **Notifications d'événements du** titulaire de la carte. Voir ***Activation des notifications d'événement/d'alarme pour un détenteur de carte*** (page 35-10).
- Affectation d'un groupe d'accès que le titulaire de carte utilise dans le filtre de notification de l'onglet **Notifications personnalisées** du filtre de notification (expliqué plus loin dans cette rubrique).

Cette procédure explique comment créer un filtre de notification. Les filtres de notification sont normalement configurés par rapport aux enregistrements des titulaires de carte et envoient des notifications d'événement à ces titulaires de carte (par exemple, les gardes). Les notifications personnalisées sont configurées en affectant des groupes d'accès au filtre de notification et en envoyant les événements liés au titulaire de carte uniquement au titulaire de carte associé si ce dernier est membre de l'un des groupes d'accès attribués (ou d'un groupe d'accès enfant).

Pour envoyer un e-mail SMS à...	**affecter...**
Gardiens (ou titulaires de cartes non liées),	un filtre de notification pour chaque **onglet Notifications d'événements** de garde/titulaire de carte particulier.
les titulaires de cartes liées à un événement,	à un filtre de notification Filtrer le(s) groupe(s) d'accès contenant les titulaires de carte pour recevoir des notifications d'événement sur eux-mêmes.
Relations des titulaires de carte liées à des événements (rôles),	à une notification Filtrer les rôles pour recevoir des notifications sur les titulaires de carte pour lesquels ils jouent ce rôle. Ils reçoivent uniquement des notifications concernant les titulaires de carte qui font partie des groupes d'accès attribués au filtre de notification.

Lorsqu'un groupe d'accès est affecté à un filtre de notification, les titulaires de carte appartenant au groupe d'accès ou à l'un de ses groupes d'accès enfants reçoivent les notifications spécifiées par le filtre de notification.
Si des rôles sont attribués aux titulaires de carte dans ces groupes d'accès dans l'onglet **Relations et que ces rôles sont affectés aux côtés des groupes d'accès dans** l'**onglet Notifications personnalisées** du filtre de notification**, les notifications d'événement** sont envoyées à ces rôles.
Remarques :

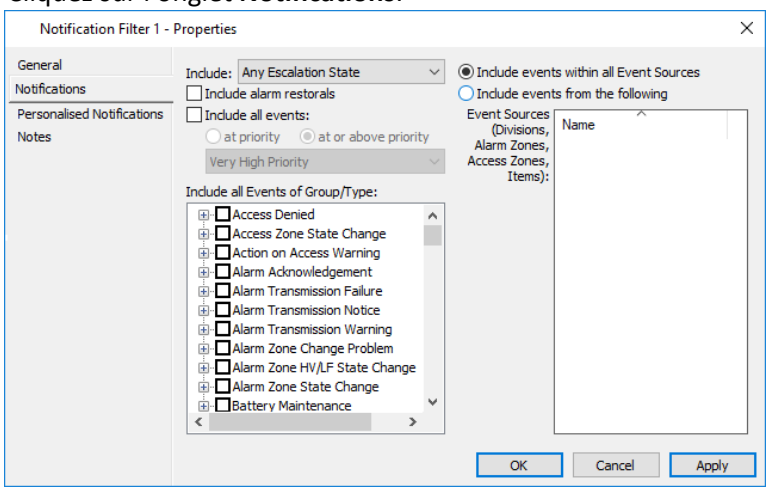
- Si vous configurez un filtre de notification pour les notifications mobiles, seules les alarmes peuvent être envoyées, pas les événements. Les notifications mobiles ne fonctionneront pas lorsque le filtre de notification est affecté à un groupe d'accès. Le filtre de notification doit être attribué à chaque titulaire de carte.
- Les notifications sont concevables.

Privilèges d'opérateur

À...	vous avez besoin de...
modifier le privilège	"Configurer le site" d'un filtre de notification division.
Modifier l'onglet Notifications personnalisées dans un filtre de notification	Privilège "Modifier les notifications personnalisées" dans la division appropriée.
voir/afficher un filtre	notification "Afficher le site" privilège dans la division appropriée.

Procédure

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

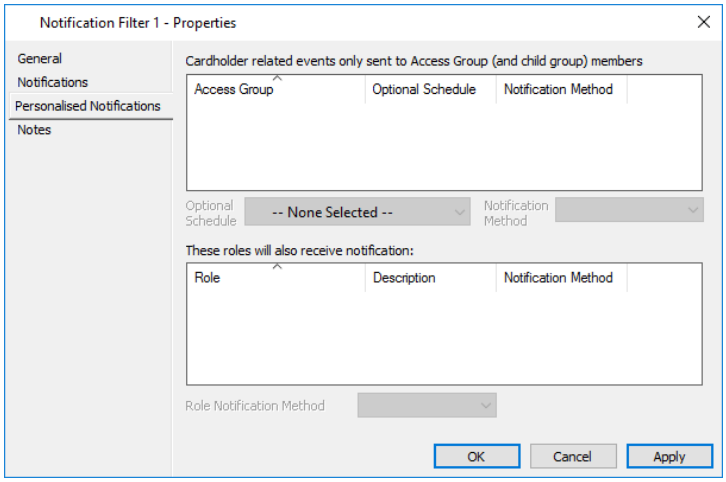


5. Pour définir les filtres de notification, configurez comme il convient :

du champ	Description
Inclure	Sélectionnez l'état d'escalade requis dans la liste déroulante. Les options sont les suivantes : **Tout état d'escalade :** les événements/alarmes qui sont dans n'importe quel état d'escalade seront notifiés. **Événements escaladés uniquement :** Seuls les événements/alarmes qui sont escaladés seront notifiés. **Événements non escaladés uniquement :** Seuls les événements/alarmes non escaladés seront notifiés.
Inclure les restaurations d'alarme	Cocher cette option enverra des notifications séparées pour chaque restauration et réactivation d'une alarme avec état.
Inclure tous les événements à (ou au-dessus) priorité :	Vérification de cette option : • active la liste déroulante des priorités, ce qui vous permet de sélectionner une autre des priorités existantes et • le texte ci-dessous passe de "Inclure tous les événements du groupe/type" à "**et aussi les événements** du groupe/type".

du champ	Description
	Remarque : Si vous ne cochez pas cette option, vous devez sélectionner au moins un groupe ou un type. Valeur par défaut = Deuxième niveau de priorité le plus élevé. La sélection de l'option à la priorité ne signale que les événements de la priorité, tandis que l'option à la priorité ou au-dessus notifie les événements de cette priorité et au-dessus.
Inclure tous les événements du groupe/type	Si un groupe d'événements est sélectionné, tous les types d'événements appartenant au groupe d'événements seront notifiés. Il est possible de sélectionner différents types d'événements au sein d'un groupe d'événements particulier. Par défaut = Aucun sélectionné
Inclure les événements dans toutes les sources d'événements	Si cette option est activée, vous ne pouvez pas restreindre les sources d'événements (c'est-à-dire que vous ne pouvez pas sélectionner des éléments source d'événements spécifiques). Les notifications ne sont pas restreintes par la source d'événements lorsque cette option est sélectionnée. Par défaut = activé
Inclure les événements des sources d'événements suivantes	Si vous cochez cette case d'option, au moins un élément doit être déplacé et déplacé dans la grille Sources d'événements. Il n'y a aucune restriction au nombre de sources d'événements (c.-à-d. divisions, titulaires de carte, zones d'alarme, zones d'accès et articles) qui peuvent être incluses dans cette grille. Les notifications seront limitées à ces sources d'événements uniquement lorsque cette option est sélectionnée. Par défaut = Désactivé (Aucun inclus)

6. Cliquez sur l'onglet **Notifications personnalisées (Personalized Notifications)**.



7. Dans la grille supérieure, faites glisser et déposez les groupes d'accès dont les titulaires de carte (et les titulaires de carte des groupes d'accès enfants) doivent recevoir des notifications personnelles conformément à la configuration de l'onglet **Notifications**. Les titulaires de carte de ces groupes d'accès ne recevront que des notifications concernant des événements qui se rapportent à eux-mêmes.
Remarque : Si un titulaire de carte fait partie de plusieurs groupes d'accès de cette grille, il ne recevra qu'une seule notification par événement associé, à moins que les différents groupes d'accès n'aient des méthodes de notification différentes, auquel cas il recevra les notifications séparées.

8. Éventuellement, affectez une planification à un groupe Access en sélectionnant Access Regroupez puis choisissez un calendrier dans la **liste déroulante Calendrier facultatif**.
9. Sélectionnez la méthode de notification (**Email** ou **SMS**) pour un groupe d'accès en sélectionnant le groupe d'accès, puis en choisissant une méthode de notification dans la **liste déroulante** Méthode **de notification**.
10. Activez ou désactivez les notifications de ce filtre de notification pour chaque groupe d'accès en cochant (pour activer) ou en désélectionnant (pour désactiver) la case à cocher à gauche du nom de chaque groupe d'accès.
11. Dans la grille du bas, faites glisser et déposez les Rôles qui doivent également recevoir des notifications conformément à la configuration de l'onglet **Notifications**. Ces rôles seront notifiés pour chaque notification qui est :
    - envoyés à un titulaire de carte avec qui ils entretiennent une relation, et
    - envoyé à la suite de ce filtre de notification.
12. Sélectionnez la méthode de notification (Email - Separate, Email - CC, or SMS) pour un rôle en sélectionnant le rôle, puis en choisissant une méthode de notification dans la **liste déroulante Méthode de notification de rôle**.

    E-mail - Separate enverra une notification par e-mail distincte au rôle pour toutes les notifications envoyées aux titulaires de carte (fonctionnalité antérieure à Command Center v8.40).
    Courriel - CC copiera le rôle dans tous les courriels envoyés aux titulaires de carte.
    SMS enverra un SMS distinct au rôle pour toutes les notifications envoyées aux titulaires de carte.

    Remarque : Pour que les rôles reçoivent des notifications via une certaine méthode, le titulaire de carte qui reçoit la notification d'origine doit se trouver dans un groupe d'accès configuré avec cette même méthode de notification.

    Par exemple, pour qu'un rôle reçoive une notification par SMS, le titulaire de carte lié à la notification doit se trouver dans un groupe d'accès configuré avec la méthode de notification SMS.
13. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes à propos de ce filtre de notification. Pour de plus amples détails, voir les ***Notes*** (page 6-81).
14. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Conseils

Suppression des filtres de notification
Reportez-vous à ***Suppression d'éléments*** (page 3-27) pour la procédure de suppression d'un filtre de notification (Notification Filter).
Remarque : Les filtres de notification ne peuvent pas être supprimés s'ils sont joints à un ou plusieurs enregistrements de titulaires de cartes.

Événements escaladés
Normalement, un événement qui correspond aux filtres de notification assignés déclenche un e-mail, et lorsque l'événement se déclenche, il déclenche un autre e-mail. Cependant, lorsque le service de messagerie est soumis à une pression importante, l'événement peut être escaladé avant l'envoi du premier e-mail, ce qui entraîne uniquement l'envoi du second e-mail. Les détails du second e-mail sont presque identiques au premier, sauf que l'événement sera "escaladé".

Définition des fichiers PDF "Email" et "Mobile" des titulaires de carte

Introduction

Les coordonnées sont conservées dans le type de contact Données personnelles, (i.e. "Adresse", "Téléphone", "Courriel" et "Mobile").Les PDF de type "Courriel" et "Mobile" comportent également une case à cocher de notification modifiable au niveau du détenteur de la carte. Ils sont définis pour les détenteurs de cartes individuels et attribués aux détenteurs de cartes via des groupes d'accès, comme c'est courant avec d'autres PDF.
Remarque : Les notifications sont disponibles sous licence.

Procédure

1. Configurez un champ de données personnelles de type "Email" et "Mobile" à utiliser avec les notifications.
   Reportez-vous à la section Création d'un nouveau champ de données personnelles.
2. Le cas échéant, sous l'onglet **Type** du champ Données personnelles, activez la case à cocher **Notifications par défaut (Default Notifications)**.
   Cette propriété fournit une valeur par défaut lorsqu'un fichier PDF est affecté pour la première fois à un titulaire de carte.
3. Affectez les champs de données personnelles à un groupe d'accès approprié, comme suit :
   a) Cliquez sur **Gérer** dans la barre de menus, puis sur **Groupes d'accès**.
      La fenêtre **Liste** principale **du groupe Access** s'ouvre.
   b) Mettez en surbrillance le groupe d'accès auquel vous souhaitez affecter des champs de données personnelles, et double-cliquez sur le bouton de la souris.
   c) Cliquez sur l'onglet **Données personnelles (Personal Data)**.
   d) Dans la fenêtre Liste principale des **champs de données personnelles**, sélectionnez les champs de données personnelles créés à l'étape 1.
      Faites-les glisser et déposez-les dans l'onglet **Données** personnelles.
4. Sous l'onglet **Données personnelles** du titulaire de la carte, renseignez les champs "Email" et "Mobile" et assurez-vous que la case **Notifications** est cochée. Reportez-vous à la rubrique Modification des données PDF d'un titulaire de carte pour la procédure.
   Remarques :
   - Tant que les adresses e-mail et les numéros de téléphone mobile saisis sont valides, la case à cocher Notifications garantit que les titulaires de carte recevront des notifications par e-mail et/ou par SMS.
   - Les numéros de téléphone mobile peuvent comporter des espaces ou des tirets. Ceux-ci seront supprimés pour les notifications utilisant ce numéro.
   - Il est possible de configurer plus d'un email et/ou plus d'un PDF mobile, et de faire en sorte qu'un titulaire de carte reçoive des notifications à plus d'un compte de courriel et/ou un numéro de téléphone mobile.

Activation des notifications d'événements/d'alarmes pour un détenteur de carte

Introduction

L'onglet **Notifications d'événements de** la page des propriétés du titulaire de carte permet à un opérateur privilégié d'activer et de désactiver instantanément ou ultérieurement ou pour une période de temps particulière des notifications pour un titulaire de carte particulier. Cette page affiche également les filtres de messagerie actifs pour le titulaire de carte, ainsi qu'un calendrier optionnel pour chaque filtre, ainsi qu'une méthode de notification (e-mail, SMS ou notifications mobiles).

Privilèges d'opérateur

Le privilège d'opérateur "Modifier la notification du détenteur de carte" est requis pour :

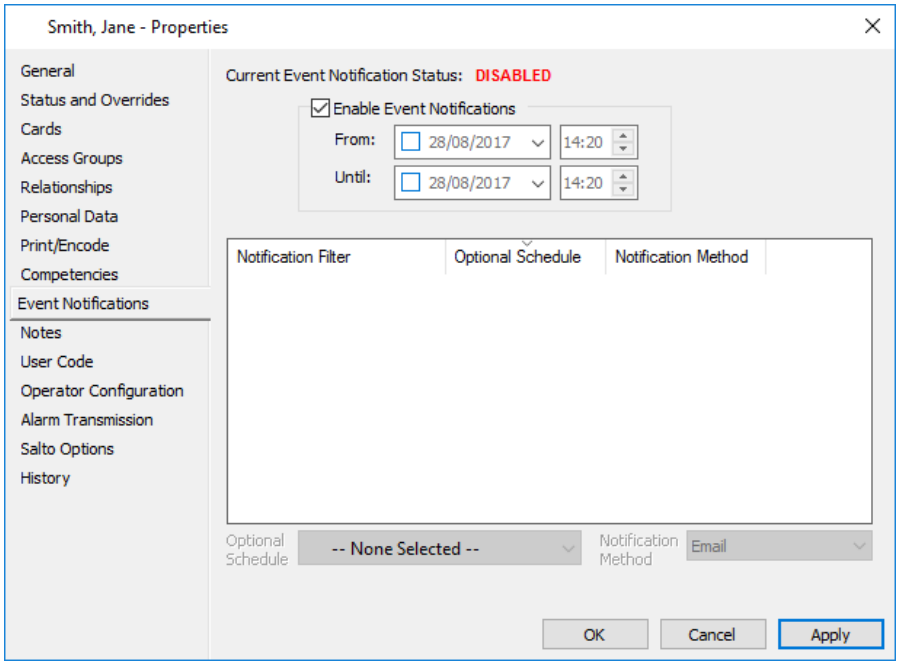
- activer/désactiver les notifications dans l'onglet **Notifications d'événements** de l'enregistrement du titulaire de carte.
- modifier la méthode de notification préférée au niveau du filtre.

En plus du privilège "Modifier la notification du titulaire de carte", vous pouvez avoir besoin d'un autre privilège en fonction de la fonction que vous voulez exécuter, comme suit :

À...	**vous avez également besoin de…**
ajouter ou supprimer un filtre de notification de l'utilisateur	Privilège "Afficher le site" dans la division du filtre de notification.
ajouter ou supprimer une planification de l'onglet des notifications du titulaire de carte	Privilège "Afficher le calendrier" dans la division du calendrier.
voir et/ou mettre à jour tout autre onglet Titulaire de carte autre que l'onglet **Notifications d'événements**	le privilège du titulaire de carte approprié (i.e. "Modifier le titulaire de la carte", "Supprimer le titulaire de la carte", "Afficher le titulaire de la carte" ou "Modifier les notes du titulaire de la carte").

Procédure

1. Cliquez sur **Gérer** dans la barre de menu, puis sur Titulaires de carte.
   La fenêtre Liste principale des titulaires de carte s'ouvre (en mode grille).
2. Localisez et mettez en surbrillance le détenteur de carte à modifier.
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Notifications d'événements (Event Notifications)**.
   Remarque : L'**état actuel des notifications d'événements** n'affecte que les notifications d'événements (c'est-à-dire qu'il n'affecte pas les notifications d'expiration). Par défaut, tous les détenteurs de carte seront désactivés **de l'état de** notification d'**événement** en cours.



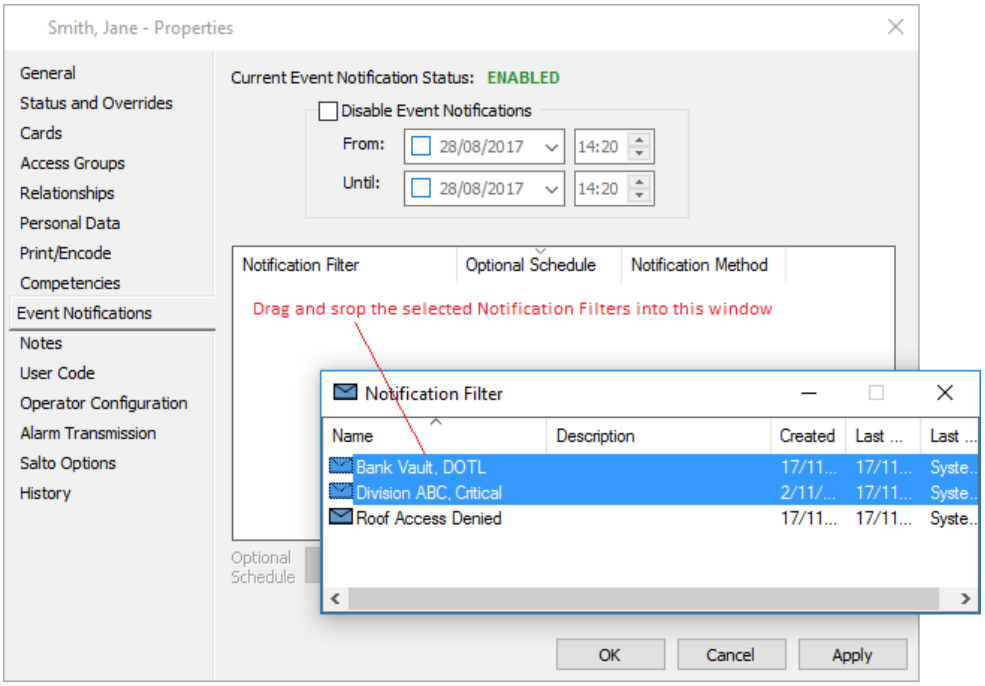
5. Cochez la **case Activer les notifications d'événements**.
   Remarque : L'état ne changera pas tant que le bouton **Appliquer n'**aura pas été cliqué et que le nom de la case à cocher ne sera plus **Activer les notifications d'événements** mais **Désactiver les notifications d'événements**.



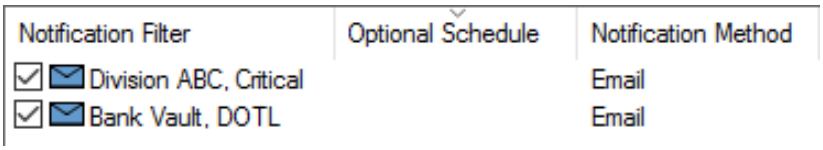
   Si vous souhaitez que les notifications soient activées pendant une période donnée, définissez l'option De et **Jusqu'aux** dates et heures.
   Remarques :

Si vous...	**lorsque l'on clique sur le bouton Appliquer État de la notification d'événement...**
saisissez une date future dans le champ **De**,	restera DÉSACTIVÉ. Il ne changera pas en ENABLED jusqu'à la date et l'heure indiquées dans le **champ De**.
N'entrez pas de date dans le champ De champ,	sera ACTIVÉ immédiatement.
N'entrez pas de date dans la zone Jusqu'à champ,	sera ACTIVÉ indéfiniment.

6. Cliquez sur **Configurer** dans la barre de menus, puis sur **Filtres de notification**.
   La fenêtre Liste principale du filtre de notification s'ouvre.
7. Sélectionnez les filtres de notification à affecter à ce titulaire de carte.
   Faites-les glisser et déposez-les dans l'**onglet Notifications d'événements**.



Remarque : Par défaut, lorsque vous faites glisser un filtre de notification dans cette fenêtre, il n'y a pas de planification qui lui est associée et la méthode de notification sera "Email".



8. Fermez la fenêtre Liste principale **du filtre de** notification.

   Les filtres de notification peuvent éventuellement être associés à une planification. Un calendrier définit les heures auxquelles les événements sélectionnés par ce filtre sont notifiés au titulaire de la carte.
   Remarque : Si aucune planification n'est affectée à un filtre de messagerie, ce filtre sera supposé être activé à tout moment.

9. Voulez-vous associer une planification aux filtres de notification ?
   Si **oui**, passez à l'étape 10.
   Si **non**, passez à l'étape 13.

10. Cliquez sur le filtre de notification requis pour le mettre en surbrillance.
    Les **champs Facultatif Planification** et **Méthode** de notification sont activés.

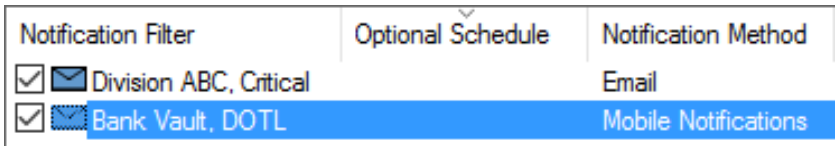
11. Sélectionnez une **planification facultative** dans la liste déroulante. Vous pouvez également faire glisser et déplacer la planification de la fenêtre Liste principale de la planification.
    Remarque : La liste déroulante contient uniquement les calendriers de type "Notification".

12. Répétez les étapes 11 à 12 pour tous les autres filtres auxquels vous souhaitez associer une planification.
    Remarque : Une page de propriétés Filtres et/ou une page de propriétés Calendrier peuvent être ouvertes à partir de cette fenêtre :

    - double-clic sur le filtre ou la planification dans la grille, ou

- en cliquant avec le bouton droit sur le filtre. Un menu contextuel s'affiche, avec l'option de sélection **Filtrer** ou Planifier les propriétés.
  Remarque : Si le filtre n'a pas de calendrier associé à ce filtre, L'option **Propriétés de planification** sera désactivée.

13. Si vous souhaitez modifier la méthode de notification de "Email", sélectionnez une autre option dans la **liste déroulante** Méthode **de notification**.
    Voir ***Mobile/Notifications SMS*** (à la page 6-55) pour plus de détails.



    Remarque : Si vous configurez les notifications mobiles, sélectionnez **Notifications mobiles** dans la **liste déroulante Méthode de notification**.

14. Par défaut, les cases ☑ à cocher situées à côté de chaque filtre de notification indiquent qu'elles sont sélectionnées pour activer le filtre.
    Pour désactiver un filtre, désactivez la case à cocher située en regard du filtre approprié. Les événements sélectionnés par ce filtre ne seront plus notifiés au titulaire de la carte.

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

Indication

Mes notifications
L'opérateur connecté peut accéder rapidement à l'onglet Notifications d'événements de ses propres propriétés de titulaire de carte (via **Gérer** > **Mes notifications**), principalement dans le but d'activer/désactiver rapidement les notifications d'événements.

Définition des valeurs de seuil de notification d'expiration

Introduction

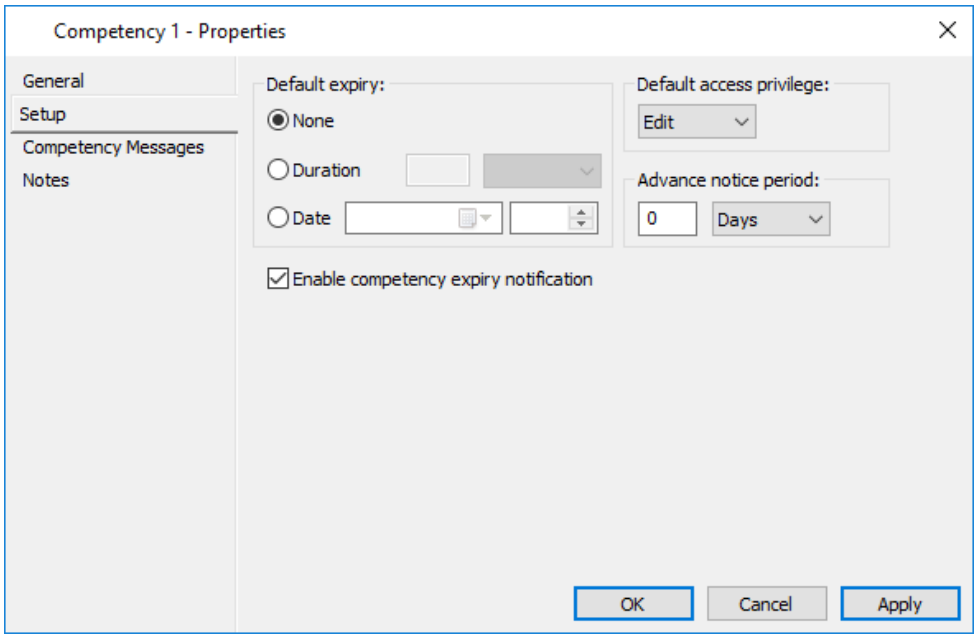
Les superviseurs/gestionnaires doivent être avisés par SMS et/ou par courriel lorsque :

- une carte d'un membre du personnel est sur le point d'expirer,
- une compétence pour l'un de leurs employés est presque expirée.

Remarque : Les titulaires de carte peuvent également devoir être informés de cette situation par SMS et/ou par e-mail.
Pour ce faire, les valeurs de seuil d'expiration doivent être définies pour ces éléments d'accès, de sorte que le système génère des événements lorsque l'accès approche de l'expiration.
Remarque : Les notifications d'expiration ne seront pas envoyées pour les "anciennes" cartes et compétences qui ont déjà expiré.

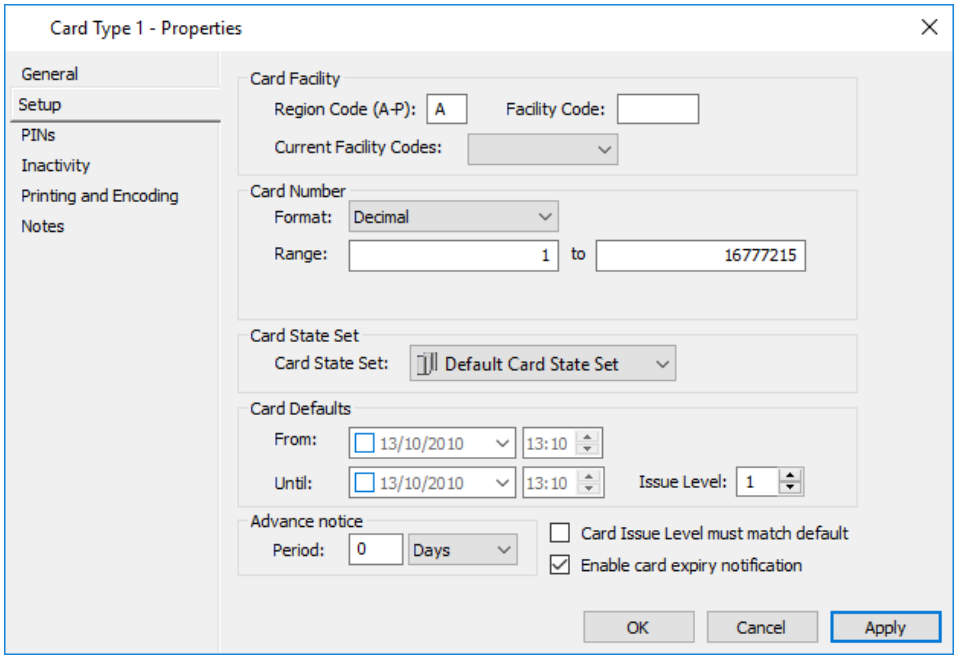
Procédure

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** sur la compétence requise et sélectionnez **Propriétés**.
3. Cliquez sur l'onglet **Configuration**.



4. Définissez la **période de préavis** à la valeur requise pour représenter le nombre de jours, de semaines, de mois ou d'années précédant l'expiration de la compétence pour lancer la notification d'avertissement.
   Remarques :
   - La période maximale équivalente est de 999 jours.
   - Cette période d'avis contrôle également la période utilisée pour afficher l'avertissement d'expiration des compétences chez un lecteur.

5. Assurez-vous que la case à cocher **Activer la notification d'expiration des compétences** est activée.
   Remarque : L'exécution des notifications d'expiration quotidiennes n'envoie pas de notification pour une compétence qui a expiré à une date antérieure à la date actuelle, moins la période de préavis. Si la période de préavis est définie sur zéro, les compétences qui ont expiré au cours des 24 dernières heures seront toujours notifiées au moment où les notifications d'expiration quotidiennes sont exécutées.
6. Cliquez sur le bouton **OK**.
7. Répétez les étapes 2 à 6 pour chaque compétence nécessitant un avis d'expiration de l'avis.
8. Fermez la fenêtre Liste principale des compétences.
9. Cliquez sur **Configurer** dans la barre de menus, puis sur **Types de cartes**.
   La fenêtre **Type** de carte principale s'ouvre (en mode grille).
10. **Cliquez avec le bouton droit** sur le type de carte requis et sélectionnez **Propriétés**.
11. Cliquez sur l'onglet **Configuration**.



12. Définissez la **période de préavis** à la valeur requise pour représenter le nombre de jours, de semaines, de mois ou d'années précédant l'expiration de la carte pour lancer la notification d'avertissement.
    Remarque : La période équivalente maximale est de 999 jours.
13. Assurez-vous que la **case à cocher Activer la notification d'expiration de la carte est activée**.
    Remarque : L'exécution des notifications d'expiration quotidiennes n'envoie pas de notification pour une carte dont la date d'expiration est antérieure à la date actuelle, moins la période de préavis. Si la période de préavis est égale à zéro, les cartes qui ont expiré au cours des 24 dernières heures seront toujours notifiées au moment où les notifications d'expiration quotidiennes sont exécutées.
14. Cliquez sur le bouton **OK**.

15. Répétez les étapes 10 à 14 pour chaque type de carte nécessitant un avertissement d'expiration.

Résultat

Les valeurs que vous avez définies par défaut sont les valeurs de seuil pour chacun des deux types d'expiration conservés sur les propriétés Titulaire de carte, comme suit :

- Expiration de la carte: la **date** et l'heure jusqu'au sur l'**onglet Cartes**
- Expiration des compétences : La date et l'heure d'**expiration** des compétences s'affiche.

Configuration des rôles

Introduction

Les titulaires de carte, les superviseurs, les gestionnaires ou les administrateurs/exploitants doivent être avisés de l'expiration de la carte et de l'expiration des compétences. Des rôles sont donc requis pour définir les relations entre les titulaires - pour acheminer une notification à la personne appropriée.
Cette procédure se divise en deux parties :

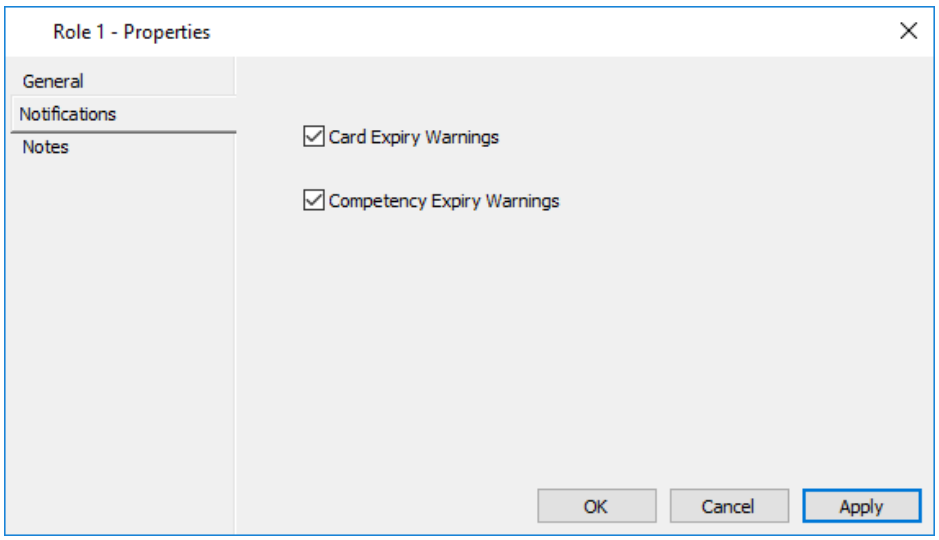
- Création de rôles, et
- Affectation des titulaires de carte aux rôles

Procédure

Création d'un rôle

Remarque : Les opérateurs ont besoin du privilège « Modifier le site » ou « Modifier les définitions de rôle » pour créer, modifier ou supprimer un rôle.

1. Cliquez sur **Gérer** dans la barre de menu puis sur **Rôles**.
   La fenêtre Liste principale des rôles s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...Rôle**.
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
   Remarque : Les exemples de **nom** sont Superviseur, Gestionnaire des RH, Administrateur.
4. Cliquez sur l'onglet **Notifications**.



   Les options de cet onglet permettent aux titulaires de carte dans ce rôle d'être informés des dates d'expiration de la carte et/ou de la compétence en attente pour leur personnel, par courriel.
5. Les deux cases sont activées par défaut.
   Laissez activée la ou les cases à cocher requises pour ce rôle, désactivez les cases à cocher qui ne sont pas requises pour ce rôle.

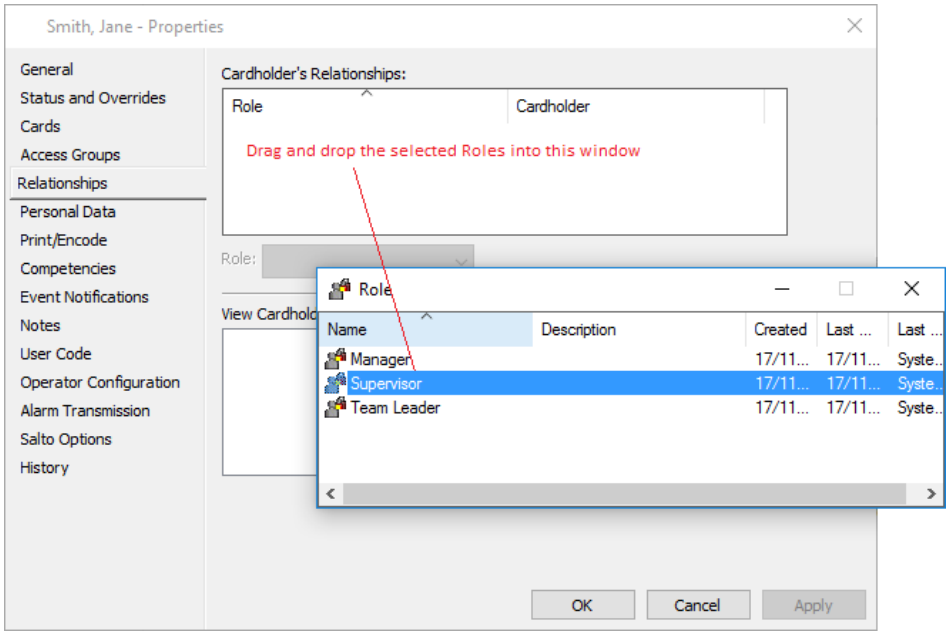
Remarque : La case à cocher **Événements liés au titulaire de carte** est nouvelle dans la fonction Notifications améliorées. Lorsqu'elle est cochée, les notifications d'événement envoyées au titulaire de carte sont également envoyées, par exemple, au superviseur du titulaire de carte (c'est-à-dire que le ou les filtres appartenant au titulaire de carte n'ont pas besoin d'appartenir au superviseur ou à qui est le destinataire supplémentaire).

6. Cliquez sur l'onglet Remarques si vous souhaitez ajouter une remarque sur ce rôle. Pour plus de détails concernant l'onglet **Notes**, voir ***Notes*** (page 6-81).
7. Cliquez sur le bouton **OK** pour quitter et enregistrer ce rôle.

Affectation des titulaires de carte aux rôles

Les titulaires de carte peuvent être affectés manuellement à des rôles ou en utilisant la fonction de modification en bloc. Cette procédure décrit la méthode manuelle. Si vous avez besoin de la méthode de modification en bloc, reportez-vous à la section ***Affectation de titulaires de carte à des rôles via la modification en bloc*** (suivante) pour la procédure.

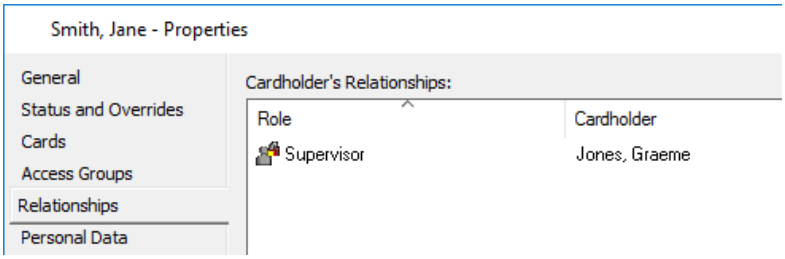
8. Cliquez sur **Gérer** dans la barre de menu, puis sur Titulaires de carte.
   La fenêtre Liste principale des titulaires de carte s'ouvre (en mode grille).
9. Localisez et mettez en surbrillance le titulaire de la carte à laquelle le rôle doit être attribué.
10. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
11. Cliquez sur l'onglet **Relations (Relationships)**.
12. Dans la fenêtre Liste principale des **rôles**, sélectionnez le ou les rôles que vous souhaitez affecter à ce détenteur de carte. Faites glisser et déposez-les dans la **grille Relations** du **titulaire de carte Relations,** onglet.



Remarque : Plusieurs rôles peuvent être attribués à un titulaire de carte (par exemple, chaque titulaire de carte peut avoir un superviseur, un administrateur de carte, un gestionnaire).

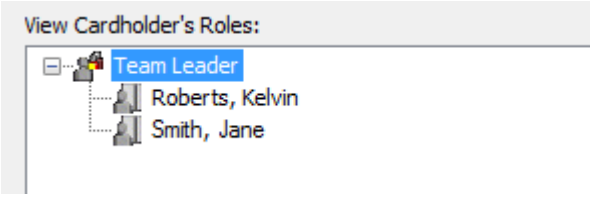
13. Cliquez sur le rôle pour le mettre en surbrillance.
    Le champ **Rôle** devient activé.

14. Faites glisser le titulaire de carte qui remplit ce rôle de la fenêtre Liste principale des **titulaires de carte** vers le rôle de la grille **Relations des titulaires de carte**.
Par exemple:
Graeme Jones est le superviseur de Jane Smith, donc Graeme Jones est traîné et déposé dans le rôle de superviseur.

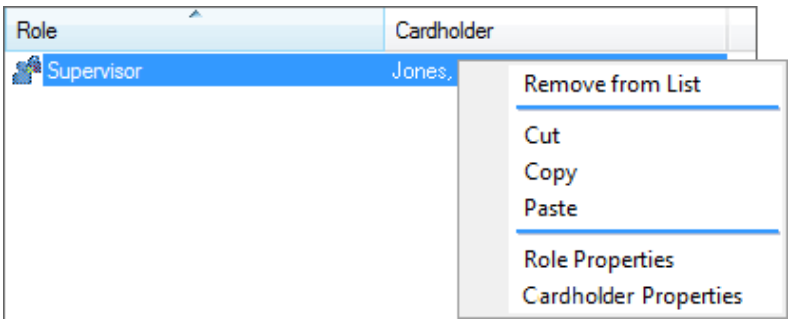


Remarques :

- La grille **Afficher les rôles des titulaires de cartes** sur cet écran affiche une vue "en lecture seule" des rôles remplis par les titulaires de cartes et pour lesquels le rôle est rempli. Cliquez sur ⊞ le bouton en regard d'un rôle pour développer la liste des titulaires de carte ci-dessous.
Par exemple:
Ce titulaire est un chef d'équipe pour Jane Smith et Kelvin Roberts.



- Les pages de propriétés d'un rôle et/ou les pages de propriétés du titulaire de carte peuvent être ouvertes à partir de :
  - double-clic sur le rôle ou le détenteur de la carte, ou
  - clic droit sur le rôle. Un menu contextuel s'affiche avec l'option permettant de sélectionner soit les **propriétés du** rôle**, soit les propriétés du détenteur de carte**.



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

Remarque : Assurez-vous que tout titulaire de carte remplissant un rôle pour d'autres titulaires de carte a un champ de données personnelles (PDF) par courriel entré dans l'onglet **Données personnelles** de ses propriétés. L'activation de notifications doit également être activée pour l'e-mail PDF.

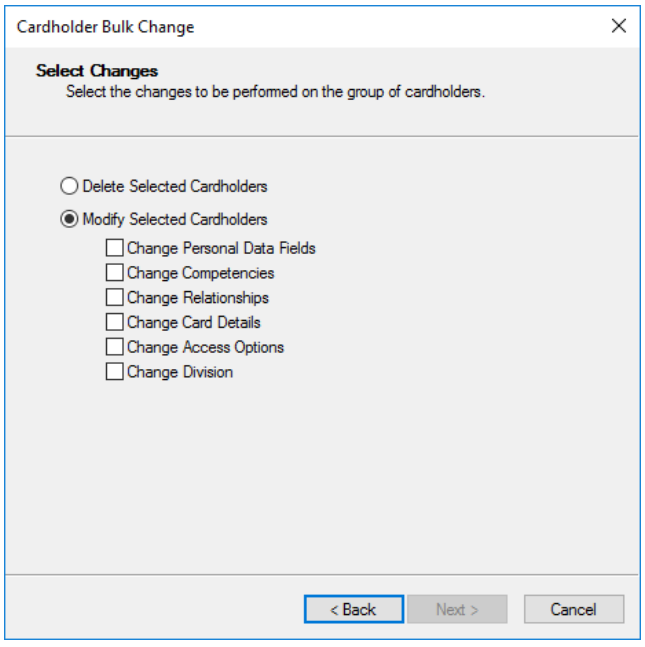
Affectation de titulaires de carte à des rôles via un changement en bloc

Introduction

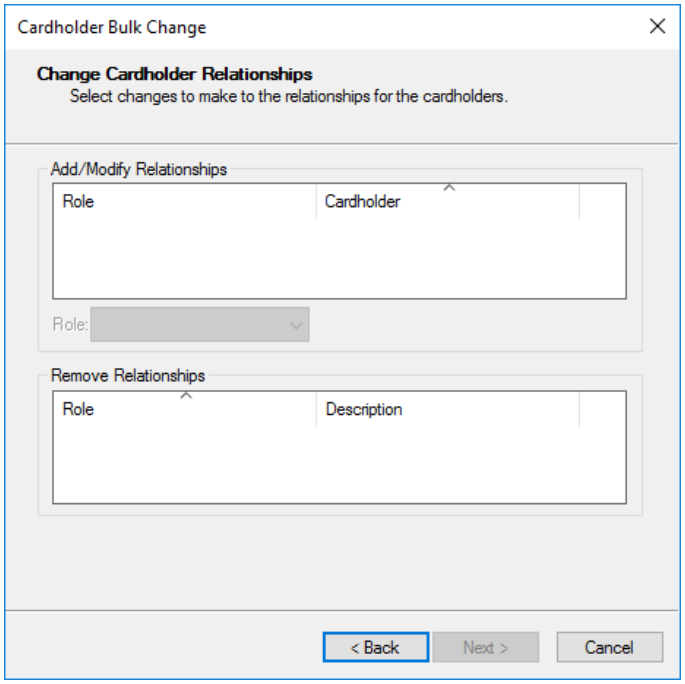
Cette procédure décrit comment initier une modification en bloc des relations de rôle de plusieurs détenteurs de cartes dans le Centre de commande. Pour effectuer cette procédure, les opérateurs ont besoin des privilèges d'opérateur "Modification en bloc" et "Modification des titulaires de carte". En outre, l'exploitant a besoin de privilèges divisionnaires et autres suffisants pour effectuer chaque changement énuméré dans un changement global.

Procédure

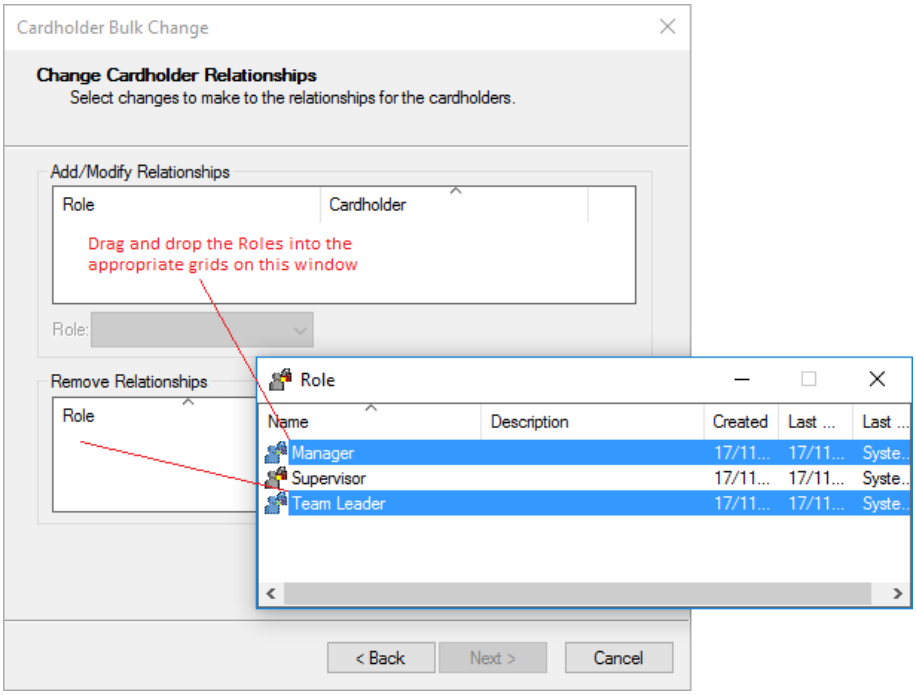
1. Exécutez les étapes 1 à 4 de la procédure Initiating a new Titulaire de carte Bulk Change (Lancement d'une nouvelle procédure de changement en bloc de titulaire de carte), puis passez à l'étape 2 de cette procédure.
   Remarques :
   - Ces étapes couvrent la sélection de tous les titulaires de carte ou groupes d'accès qui nécessitent une modification, et leur placement sur l'écran "Sélectionner les titulaires de carte ou les groupes d'accès" de l'Assistant Modifications en bloc de titulaire de carte.
   - La fonction **Copier tous les** détenteurs de cartes, qui permet un changement simple pour tous les détenteurs de cartes, peut être utilisée ici. Vous pouvez copier tous les titulaires de carte qui se présentent actuellement à une personne dans un rôle, à partir de son onglet **Relations**. Ceci est utile lorsqu'une personne dans un rôle quitte et que vous souhaitez copier les personnes qui lui rapportent actuellement vers une nouvelle personne, via un changement en bloc. Voir ***Copie de tous les détenteurs de carte*** pour la procédure ***dans*** un rôle (suivant).
2. Cliquez sur le bouton **Suivant**.
   L'écran "Sélectionner les modifications" de l'Assistant Modifications en bloc des titulaires de carte s'affiche.



3. Cliquez sur le bouton d'option **Modifier les titulaires de carte sélectionnés**, puis activez la case à cocher **Modifier les relations**.
4. Cliquez sur le bouton **Suivant**.
   L'écran "Modifier les relations entre les titulaires de carte" de l'Assistant Modifications en bloc des titulaires de carte s'affiche.



   Cet écran vous permet de sélectionner les modifications à apporter aux relations pour les détenteurs de cartes.
5. Cliquez sur **Gérer** dans la barre de menus, puis sur **Rôles**.
   La fenêtre **Liste** principale des rôles s'ouvre.
6. Sélectionnez les Rôles à ajouter et/ou supprimer des titulaires de carte, et faites-les glisser dans les grilles appropriées sur cet écran de l'Assistant, puis fermez la fenêtre Liste des **rôles principaux**.



Remarques :

- Dans la section "Ajouter/modifier des relations" de cet écran, les rôles peuvent être ajoutés à la grille à l'aide du glisser-déposer, puis les détenteurs de carte peuvent être ajoutés à l'aide du glisser-déposer ou de la liste déroulante Titulaire de carte.
  Les rôles et les valeurs des détenteurs de cartes peuvent être modifiés à l'aide de la liste déroulante applicable, avant de traiter la modification en bloc.
- Si l'action Modification en bloc consiste à "ajouter" un enregistrement de relation à un titulaire de carte pour un rôle déjà rempli, le résultat sera effectivement un changement pour le titulaire de carte détenu contre le rôle.
- Tous les Rôles ajoutés à un titulaire de carte doivent être accompagnés d'un titulaire de carte rempli remplissant ce rôle (c'est-à-dire qu'un Rôle ne peut pas être ajouté qui est "vierge").
- La suppression des relations est effectuée à l'aide du glisser-déposer du rôle dans la grille et du traitement de la modification en bloc, pour supprimer l'enregistrement de la relation rôle et titulaire de la carte de chaque titulaire de carte sélectionné pour le processus.

7. Cliquez sur le bouton **Suivant**.
8. Retournez à la procédure ***Initiating a new Titulaire de carte Bulk Change*** (Lancement d'une nouvelle modification en bloc de titulaire de carte) et effectuez les étapes 28 - 31 pour terminer la modification en bloc.

Copie de tous les titulaires de carte dans un rôle

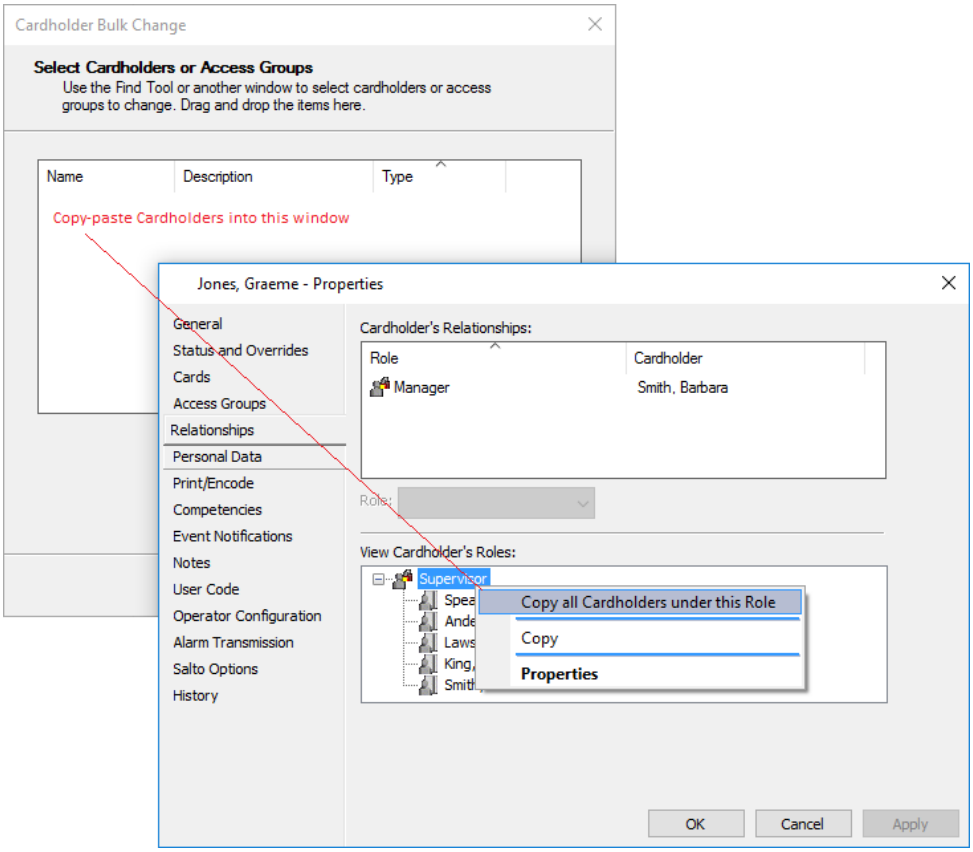
Introduction

La fonction **Copier tous les détenteurs de cartes** vous permet de sélectionner facilement tous les détenteurs de cartes qui ont un titulaire de carte particulier remplissant un rôle, et de pouvoir glisser-déposer ou copier-coller dans l'Assistant Modifications en bloc des titulaires de cartes, pour permettre une modification simple pour tous les détenteurs de cartes.

Par exemple:
Graeme Jones is currently the Supervisor of 46 staff. However, Graeme is leaving and Barbara Smith is taking over his role of Supervisor. Rather than individually dragging and dropping all 46 cardholders into the Cardholder Bulk Changes Wizard so their Supervisor can be changed, the **Copy all cardholders** feature can be used.

Procédure

1. Cliquez sur **Gérer** dans la barre de menus, puis sur **Modifications en bloc**.
   La fenêtre **Bulk Changes** List (Liste principale des modifications en **masse**) s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris **et sélectionnez...Titulaire de carte Bulk Change**.
   L'écran "Sélectionner les titulaires de carte ou les groupes d'accès" de l'Assistant de modification en bloc des titulaires de carte s'affiche.
3. Cliquez sur **Gérer** dans la barre de menu, puis sur Titulaires de carte.
   La fenêtre (en mode grille) s'ouvre dans la liste principale des **titulaires de carte**.
4. Repérez le détenteur de la carte dans le rôle et mettez-le en surbrillance.
5. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
6. Cliquez sur l'onglet **Relations (Relationships)**.
7. Mettez en surbrillance le rôle applicable (par exemple, Superviseur) dans la grille **Voir les rôles du titulaire de carte**.



8. **Cliquez avec le bouton droit** de la souris et sélectionnez **Copier tous les titulaires de carte sous ce rôle**.
9. Déplacez le curseur sur la grille de l'écran "Sélectionner les titulaires de carte ou les groupes d'accès" de l'Assistant Modifications en masse des titulaires de carte.
10. **Cliquez avec le bouton droit** de la souris et sélectionnez **Coller**.
    Tous les titulaires de carte figurant dans la liste sous le rôle apparaissent dans l'écran "Sélectionner les titulaires de carte ou les groupes d'accès" de l'Assistant Modifications en bloc des titulaires de carte.
11. Accédez à la procédure Lancement d'une nouvelle modification en bloc de support de carte et effectuez les étapes 5 - 31 pour terminer la modification en bloc.

Résultat

Un changement en bloc de titulaire de carte a été initié.

Exemples de notification

Introduction

Cette rubrique propose trois scénarios différents et la configuration requise pour configurer les notifications.

Exemple 1

Pour que le Gestionnaire de sécurité reçoive toutes les alarmes critiques 24 heures par jour, ainsi que toutes les alarmes Porte ouverte trop longue pendant les heures de travail uniquement (par SMS et par courrier électronique), configurez les éléments suivants :

1. Configurez les détails du serveur de messagerie dans l'onglet **E-mail sortant** des propriétés du serveur pour activer les e-mails sortants.
2. Configurez les détails SMS dans l'onglet **Notifications SMS** des propriétés du serveur pour activer les SMS sortants.
3. Créez un **filtre de notification** (nommé quelque chose comme "Alarmes critiques"), et sous l'onglet **Notifications** :
   - définir la priorité critique "Inclure tous les événements à priorité critique ou au-dessus :"
   - assurez-vous que le bouton radio "Inclure les événements dans toutes les sources d'événements" est sélectionné.
4. Créez un autre **filtre de notification** (nommé quelque chose comme "Porte ouverte trop longue") et sous l'onglet **Notifications** :
   - ne définissez pas de niveau de priorité minimal
   - sélectionnez le groupe/type d'événement "Porte ouverte trop longue".
5. Créez un **calendrier des notifications** (nommé quelque chose comme "Notifications heures de travail") et définissez les heures des notifications activées entre 8 h 30 et 17 h.
6. Ouvrez les propriétés du détenteur de la carte du Gestionnaire de sécurité et, sous l'onglet **Event Notifications (Notifications d'événements)** :
   - faites glisser et déposez les deux filtres de notification créés aux étapes 3 et 4.
   - faites glisser et déposez le calendrier "Notifications des heures de travail" (créé à l'étape5) contre le filtre de notification "Porte ouverte trop longue". **Remarque :** Étant donné que le filtre de notification "Alarmes critiques" est requis 24x7, il n'est pas nécessaire d'avoir un calendrier associé à celui-ci (c'est-à-dire qu'aucun calendrier ne signifie qu'il est identique à "toujours activé").
   - assurez-vous que la méthode de notification est définie sur "SMS" à côté des deux filtres. Répétez les deux puces précédentes et assurez-vous que la méthode de notification est définie sur "E-mail" à côté des deux filtres.
   - attribuez **la valeur ENABLED à Current Event Notification**.

   Sous l'onglet **Données personnelles**, assurez-vous qu'un fichier PDF "Email" et un fichier PDF "Mobile" sont correctement configurés et que les cases à cocher **Notifications** sont activées parallèlement à celles-ci.

Exemple 2

Pour que le gestionnaire des ressources humaines reçoive des notifications d'avertissement d'expiration par e-mail pour tous les titulaires de carte dont l'expiration de la carte ou de la compétence est due, configurez les éléments suivants :

1. Configurez les détails du serveur de messagerie dans l'onglet **E-mail sortant** des propriétés du serveur pour activer les e-mails sortants.
2. Pour les types de cartes et les compétences appropriés, dans les **onglets** de **configuration** :
   - fixer le **délai de préavis**, et
   - assurez-vous que les cases à cocher "Activer la notification d'expiration de la carte/compétence" sont activées.
3. Créez le rôle "Gestionnaire des ressources humaines" et, sous l'onglet **Notifications**, activez les avertissements d'expiration de la carte et des compétences pour ce rôle.
4. Ajoutez le rôle "Gestionnaire des ressources humaines" à chaque titulaire de carte (dans l'onglet **Relation de** chaque titulaire de carte) et remplissez le nom du gestionnaire des ressources humaines.
   Remarque : Cela peut être réalisé facilement pour un grand nombre de titulaires de carte utilisant le ***Titulaire de carte Bulk Change*** (page 38-3).
5. Ouvrez les propriétés des détenteurs de cartes du HR Manager et les données personnelles vérifiez :
   - il existe une configuration correcte de l'e-e-mail, et
   - la case à cocher **Notifications** est activée.

Exemple 3

Pour que John Smith reçoive un SMS pour les notifications d'avertissement d'expiration de sa carte, configurez les éléments suivants :

1. Configurez les détails du serveur de messagerie dans l'onglet **E-mail sortant** des propriétés du serveur pour activer les e-mails sortants.
2. Configurez les détails SMS dans l'onglet **Notifications SMS** des propriétés du serveur pour activer les SMS sortants.
3. Pour les types de cartes correspondants :
   - fixer le **délai de préavis**, et
   - assurez-vous que la case "Activer la notification d'expiration de la carte" est cochée pour chaque type de carte.
4. Ouvrez les propriétés du détenteur de la carte de John Smith et, sous l'onglet **Données personnelles**, assurez-vous que :
   - il est correctement configuré en PDF mobile, et
   - la case à cocher **Notifications** est activée.

Exemple 4

Pour qu'un titulaire de carte au sein d'un groupe d'accès reçoive ses propres alarmes Accès refusé par e-mail, configurez les éléments suivants.

Remarque : Les dossiers des titulaires de carte doivent chacun avoir un PDF électronique configuré correctement et La case à cocher **Notifications** doit être cochée. Vous pouvez le faire en accédant à la page **Gestion** > **Titulaires** de carte et onglet Données personnelles.

1. Configurez les détails du serveur de messagerie dans l'onglet **Notifications par e-mail** de la page Propriétés du serveur pour activer les e-mails sortants.
2. Créez un filtre de notification appelé, par exemple, "Alarmes d'accès refusé".
3. Dans l'onglet **Notifications** :
   - Sélectionnez le groupe d'événements "Accès refusé".
   - Assurez-vous que le bouton d'option **Inclure les événements dans toutes les sources d'événements** est sélectionné.
4. Sous l'onglet **Notifications personnalisées**, faites glisser le groupe d'accès dans la grille.
   Remarque : La sélection d'une planification pour ce groupe d'accès est facultative ; aucune planification signifie toujours activé.
5. Assurez-vous que la **méthode de notification** du groupe d'accès est définie sur "E-mail".

Exemple 5

Pour qu'un superviseur reçoive des alarmes Accès refusé par e-mail, configurez les éléments suivants.

Remarque : Pour chaque personne qui souhaite recevoir des notifications (qu'il s'agisse d'un superviseur qui reçoit des notifications concernant son personnel ou d'un titulaire de carte qui reçoit ses propres notifications), ses enregistrements de titulaire de carte doivent avoir chacun un courriel PDF correctement configuré et la case **Notifications** doit être cochée. Pour ce faire, accédez à **Gérer > Titulaires de carte et** consultez l'**onglet Données personnelles**.

1. Complétez l'exemple 4 ci-dessus.
2. Créer un rôle de "superviseur".
3. Ouvrez les Propriétés du titulaire de carte auquel vous souhaitez ajouter cette relation.
4. Ajoutez le rôle "Superviseur" à l'onglet **Relation**, puis faites glisser le titulaire de carte qui est le superviseur de ce titulaire de carte sur le rôle dans la grille.
5. Faites glisser et déposez le rôle de superviseur dans la grille inférieure de l'onglet **Notifications personnalisées du filtre de** notification.
6. Définissez la **méthode de notification** pour ce rôle sur "Email - Separate" ou "Email - CC" selon les besoins.

Acquittement des alarmes par SMS ou e-mail

Introduction

Cette procédure permet à un opérateur qui reçoit un SMS d'alarme ou un message électronique, de l'accuser à distance via SMS et/ou une réponse par e-mail. Les opérateurs ont besoin du privilège "Modifier l'alarme" pour accuser réception d'une alarme.

Remarque : Les utilisateurs du client mobile peuvent utiliser le client mobile pour accuser réception des notifications mobiles.

Procédure

Utilisez la procédure appropriée ci-dessous pour le type de message que vous souhaitez accuser réception :

Accusé de réception des messages électroniques

1. Sélectionnez **Répondre** ou **Répondre avec l'historique**.
   Remarque : L'une ou l'autre des options de réponse est acceptable, car l'ID d'alarme est toujours dans la ligne d'objet.
2. Tapez les lettres **ACK** dans le corps de l'e-mail.
   Remarque : Ceci n'est pas sensible à la casse, tant que les lettres sont tapées dans l'ordre sans espaces.
3. Sélectionnez **Envoyer**.

Exemple de réponse : **ACK**

Reconnaissance des messages SMS

1. Sélectionnez **Répondre**.
2. Saisissez le numéro de l'ID d'alarme.
   Remarque : Seuls les chiffres doivent être entrés. Il n'y a pas besoin des caractères "ALM".
3. Entrez un espace et tapez les lettres **ACK**.
   Remarque : Ceci n'est pas sensible à la casse, tant que les lettres sont tapées dans l'ordre sans espaces.
4. Sélectionnez **Envoyer**.

Exemple de réponse : **36 ACK** (où 36est l'ID de l'alarme).

Remarques :

- Définissez le groupe d'événements "Expéditeur non reconnu" sur "Enregistrer un événement" dans l'onglet **Paramètres par défaut des événements** des Propriétés du serveur, lors du test ou du dépannage des accusés de réception d'alarme par courrier électronique ou SMS. Cette opération enregistre un événement si un **ACK** entrant **ne peut** être traité pour une raison quelconque.
- Si votre fournisseur de services SMS en vrac de sites joint le message sortant à l'accusé de réception entrant, alors l'ID d'alarme n'est pas nécessaire, (par exemple, se comporte comme email). **ACK** uniquement).

Résultat

Command Center effectue les opérations suivantes :

- Reçoit la réponse et la met en corrélation avec l'événement/message sortant. **Remarque :** Si la corrélation ne peut pas être déterminée, un événement est déclenché.
- Traite le message entrant et reconnaît l'alarme.
- Consigne les détails d'un accusé de réception/message entrant.

Chapitre 36 : Groupes d'opérateurs

Introduction

Un groupe d'opérateurs est un groupe de détenteurs de cartes qui sont autorisés à utiliser le logiciel du Centre de commande. Chaque groupe d'opérateurs définit les privilèges dont ses membres disposent en tant qu'opérateurs du centre de commande (par exemple, accès en affichage seul, capacité de modification, capacité de configuration de site, etc.). Les privilèges ne s'appliquent qu'au sein des divisions affectées à ce groupe d'opérateurs. Les groupes d'opérateurs représentent généralement les rôles qu'un opérateur peut avoir (p. ex. "Surveillance des alarmes pour les bâtiments1 et2").

Remarque : Une vue système d'opérateurs peut être modifiée pour inclure tous les groupes d'opérateurs auxquels ils appartiennent, certains d'entre eux ou seulement un. La vue système est limitée aux éléments du site, aux détenteurs de cartes, aux champs de données personnelles (PDF) et aux privilèges d'opérateur qui leur sont attribués à partir des groupes d'opérateurs sélectionnés. Voir ***Restricting System*** (page 2-9).

Configuration des groupes d'opérateurs

Un opérateur doit disposer du privilège "Modifier les opérateurs" dans au moins une division pour créer et configurer des opérateurs et des groupes d'opérateurs.

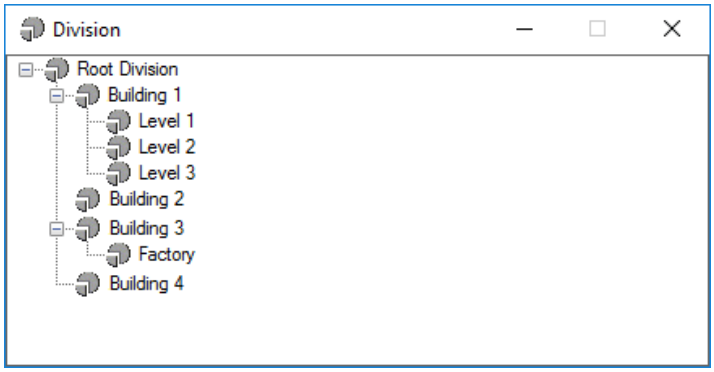
Le privilège "Modifier les opérateurs" au sein d'une division permet à un opérateur de créer des groupes d'opérateurs dans cette division et d'affecter des privilèges d'opérateurs (ou tous les privilèges) à ce groupe.

Un opérateur configurant un groupe d'opérateurs pourra uniquement :

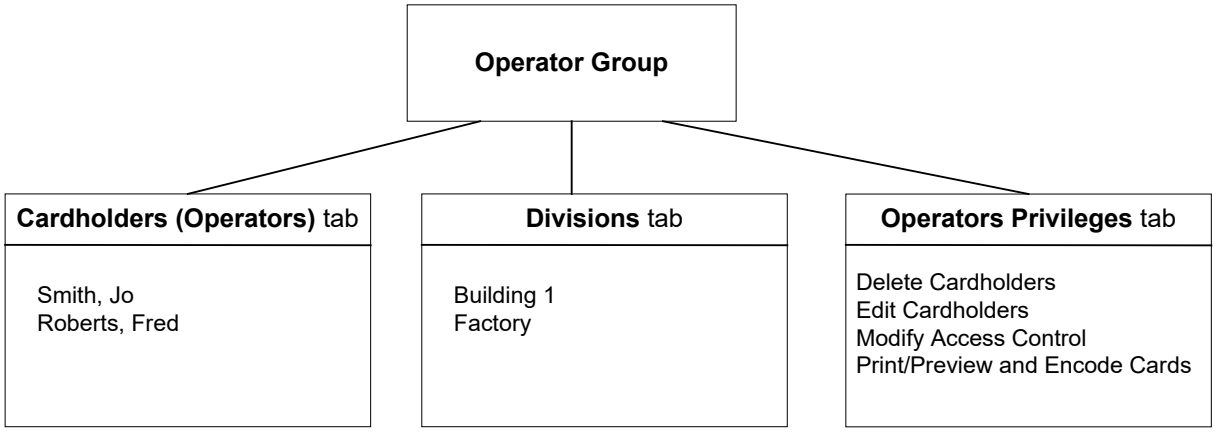
- affecter les titulaires de carte au groupe Opérateur s'ils disposent du privilège "Afficher les titulaires de carte" ou "Modifier les titulaires de carte" dans la division du titulaire de carte.
- affecter ou supprimer des divisions configurées dans le groupe d'opérateurs si elles disposent du privilège "Modifier les opérateurs" dans cette division.
- attribuez ou supprimez les privilèges de champ de données personnelles configurés dans le groupe d'opérateurs s'ils disposent du privilège "Afficher les définitions de données personnelles" ou "Modifier les définitions de données personnelles" dans la division de champ de données personnelles.

Exemple: Fonctionnement des groupes d'opérateurs

La hiérarchie divisionnaire d'un site est la suivante :

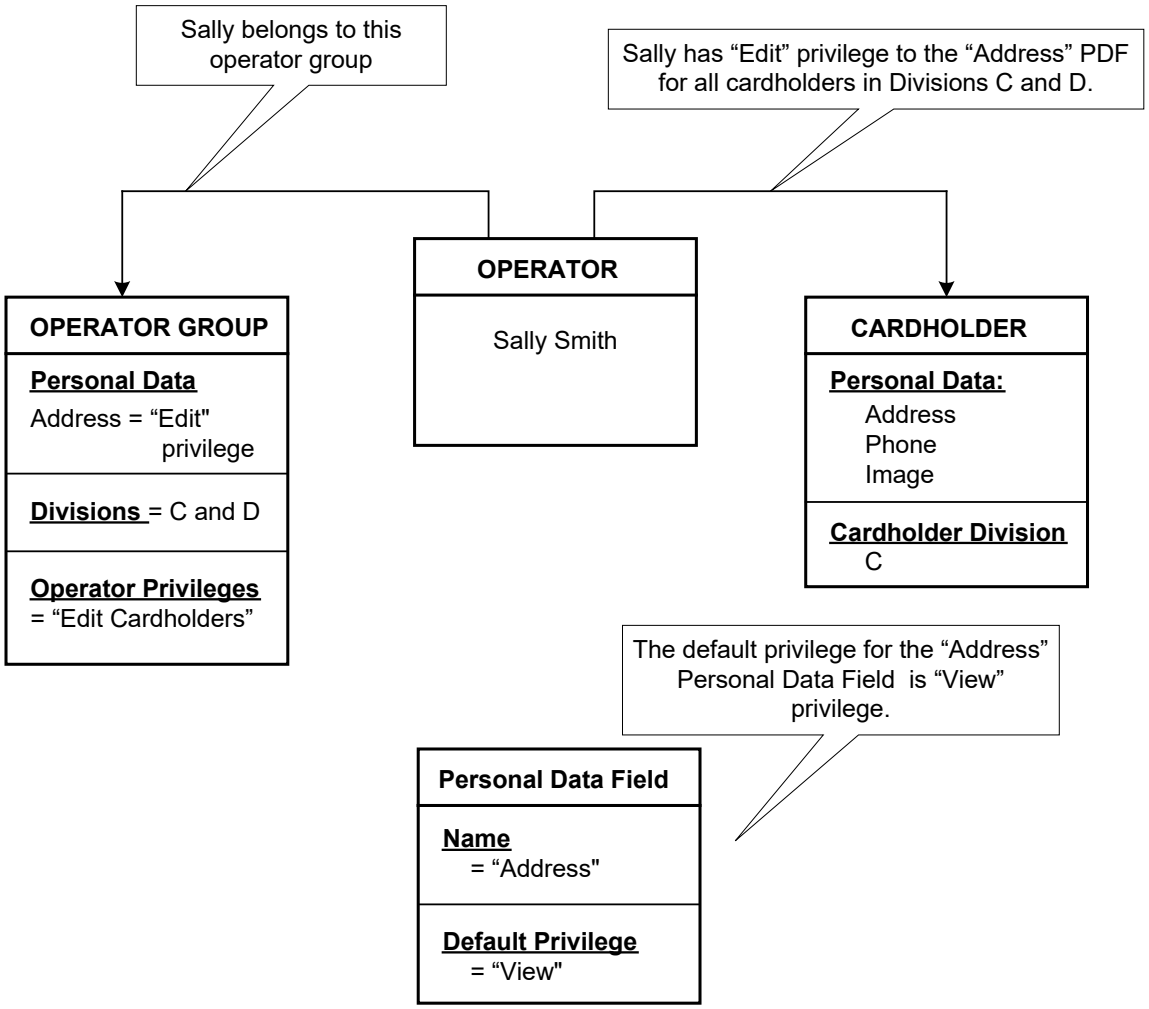


Un groupe d'opérateurs dispose des privilèges suivants pour les titulaires de cartes (opérateurs), les divisions et les privilèges d'opérateur configurés :



Cela signifie que Jo Smith et Fred Roberts peuvent "Supprimer les détenteurs de cartes", "Modifier les détenteurs de cartes", "Modifier le contrôle d'accès" et "Imprimer/Aperçu et encoder les cartes" dans les divisions "Bâtiment 1" ou "Usine". Étant donné que la division <<Bâtiment 1>> compte trois divisions pour enfants (c'est-à-dire les divisions de niveau 1, de niveau 2 et de niveau 3), elles ont également les mêmes privilèges pour ces divisions.

Affectation de privilèges de champ de données personnelles



Dans l'exemple ci-dessus, Sally Smith appartient à un groupe d'opérateurs qui lui donne le privilège "Modifier" pour le champ de données personnelles "Adresse" pour tous les détenteurs de cartes dans les divisions C et D. Ce privilège de groupe d'opérateurs remplace le privilège "Afficher" par défaut. Les autres opérateurs qui n'ont pas de privilège pour le champ de données personnelles "Adresse" qui leur est attribué par l'un de leurs groupes d'opérateurs ne pourront que consulter le contenu du champ de données personnelles "Adresse".

Un opérateur hérite des privilèges de champ de données personnelles attribués aux groupes d'opérateurs auxquels ils appartiennent. Les privilèges PDF ne s'appliquent qu'aux détenteurs de cartes appartenant à l'une des divisions du groupe d'opérateurs (tel que configuré dans l'onglet **Divisions**).

Si un opérateur appartient à plusieurs groupes d'opérateurs et que chacun d'eux attribue un privilège pour le même fichier PDF au sein de la même division, alors le privilège PDF le moins restrictif est celui dont ils héritent. Par exemple, si un groupe d'opérateurs accorde le privilège "Afficher" à un champ de données personnelles pour les détenteurs de cartes de la division C, mais qu'un autre groupe d'opérateurs accorde le même privilège "Modifier" à ce champ de données personnelles pour les détenteurs de cartes de la division C, c'est le privilège "Modifier" qu'ils reçoivent réellement.

Si les opérateurs n'appartiennent à aucun groupe qui affecte des privilèges de champ de données personnelles pour un champ de données personnelles particulier, c'est le privilège par défaut (tel que spécifié dans les propriétés de champ de données personnelles) qu'ils héritent.

Les privilèges de zone de données personnelles d'un opérateur sont attribués par division, il est donc possible de permettre à un opérateur de modifier une zone de données personnelles particulière pour les titulaires de carte dans une division, mais de voir uniquement la même zone de données personnelles pour les titulaires de carte dans d'autres divisions.

Les privilèges Champ de données personnelles sont également soumis à ce qui suit :

- L'opérateur doit avoir au moins le privilège "Afficher les détenteurs de cartes" dans la division des détenteurs de cartes avant de pouvoir afficher les champs de données personnelles de ce détenteur.
- L'opérateur doit avoir le privilège "Modifier les détenteurs de cartes" dans la division des détenteurs de cartes avant de pouvoir modifier les champs de données personnelles de ce détenteur.
- Le titulaire de la carte doit avoir reçu le champ de données personnelles par l'intermédiaire d'un des groupes d'accès auxquels il appartient.

Configuration des groupes d'opérateurs

Introduction

Cette procédure est divisée en deux parties, comme suit :

- Création d'un groupe d'opérateurs,
  (c'est-à-dire fournir les informations minimales requises pour créer un nouveau groupe d'opérateurs)
- Configuration d'un groupe d'opérateurs,
  (c'est-à-dire relier les différents composants à celui-ci - Les divisions, les privilèges, les titulaires de carte et les champs de données personnelles sont les composants d'un groupe d'opérateurs).

Vous pouvez créer un nouveau groupe d'opérateurs, puis le configurer ultérieurement, une fois que vous avez configuré les composants nécessaires.

Procédure

Créer le groupe d'opérateurs

1. Cliquez sur **Gérer** dans la barre de menus, puis sur **Opérateur Groupes**.
   La fenêtre **Liste** principale du **groupe d'opérateurs** s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...Groupe d'opérateurs**.
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).

   Remarque : La division du groupe d'opérateurs contrôle les opérateurs qui peuvent afficher ou modifier le groupe d'opérateurs. Elle n'a aucune incidence sur les divisions auxquelles les privilèges s'appliquent dans le cadre de ce groupe.
4. Cliquez sur le bouton **Appliquer (Apply)** et le groupe d'opérateurs (Operator Group) est créé.
   Le reste de cette procédure vous permet de configurer entièrement le groupe d'opérateurs.

Configurer le groupe d'opérateurs

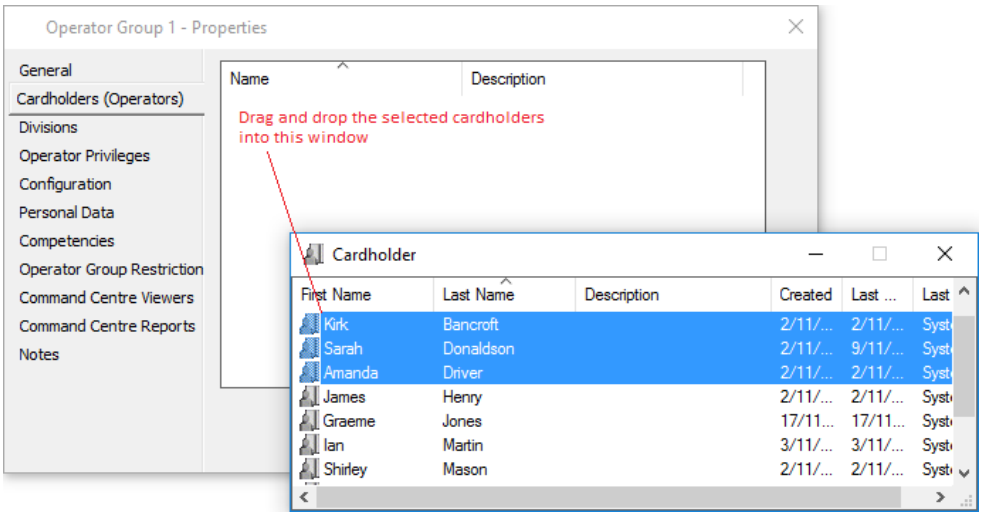
5. Assurez-vous que les composants suivants ont déjà été configurés :

   Divisions
   Consultez la section **Configuration de la division du système** (page 9-3).

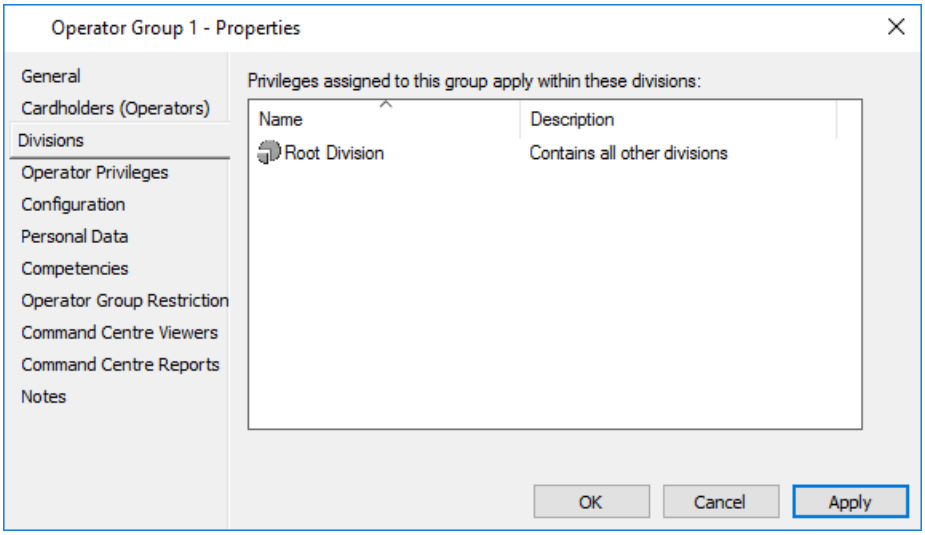
   Titulaires
   Reportez-vous à la page 32-2 du document **Ajouter un nouveau détenteur de carte**.

   Champs de données personnelles
   Reportez-vous à la section Création **d'un nouveau champ de données personnelles** (page 33-2).
6. Cliquez sur l'onglet **Titulaire de cartes (Operators) (Titulaires de carte)**.

7. Cliquez sur **Gérer** dans la barre de menus, puis sur **Titulaires de carte**.
   La fenêtre Liste principale des titulaires de carte s'ouvre.
8. Sélectionnez le(s) détenteur(s) de la carte à appartenir au nouveau groupe d'opérateurs. Faites glisser les opérateurs de carte.



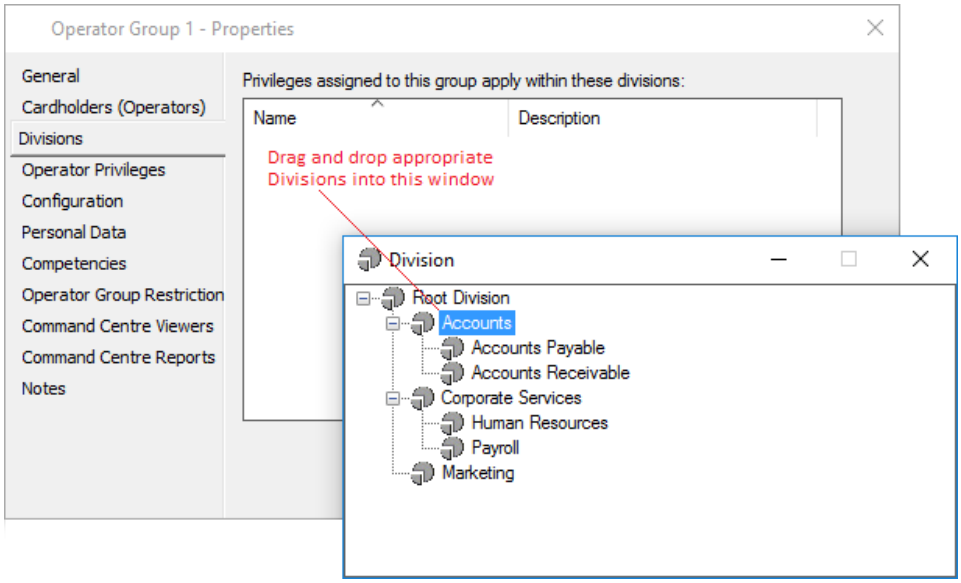
9. Fermez la fenêtre Liste principale des **détenteurs de** carte.
10. Cliquez sur l'onglet **Divisions**.
    Cet onglet indique où vous pouvez utiliser les privilèges d'opérateur que vous sélectionnez pour ce groupe (à l'étape 15). Par défaut, la division automatiquement affectée dans l'onglet **Général** est affectée à cet onglet également.



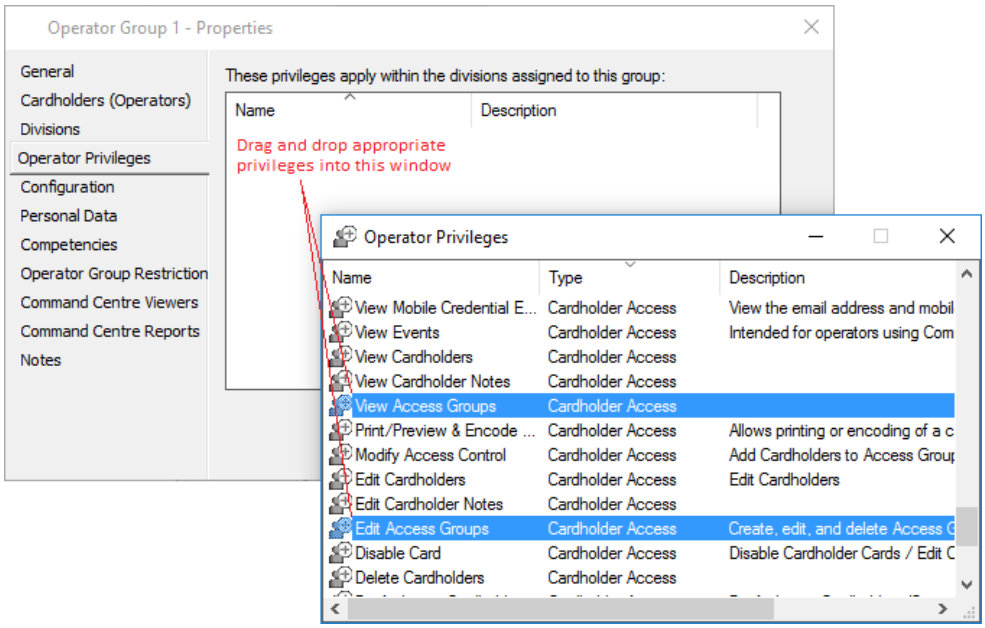
11. Avez-vous besoin des privilèges attribués à ce groupe pour s'appliquer à tous Divisions ?

Si...	**alors...**
oui	laissez la "division racine" dans la grille, car toutes les autres divisions seront incluses avec celle-ci. Passez à l'étape 15.
non	cliquez avec le bouton droit sur la "Division Racine" et sélectionnez Supprimer **de la liste**.

12. Cliquez sur **Configurer** dans la barre de menus, puis sur **Divisions**.
    La fenêtre Liste principale des divisions s'ouvre.
13. Sélectionnez les divisions pour lesquelles ce groupe d'opérateurs transmet des privilèges. Faites glisser et déposez-les dans l'onglet Divisions.
    Remarque :
    Si une division est sélectionnée, ses divisions enfant(s) sont automatiquement incluses également.

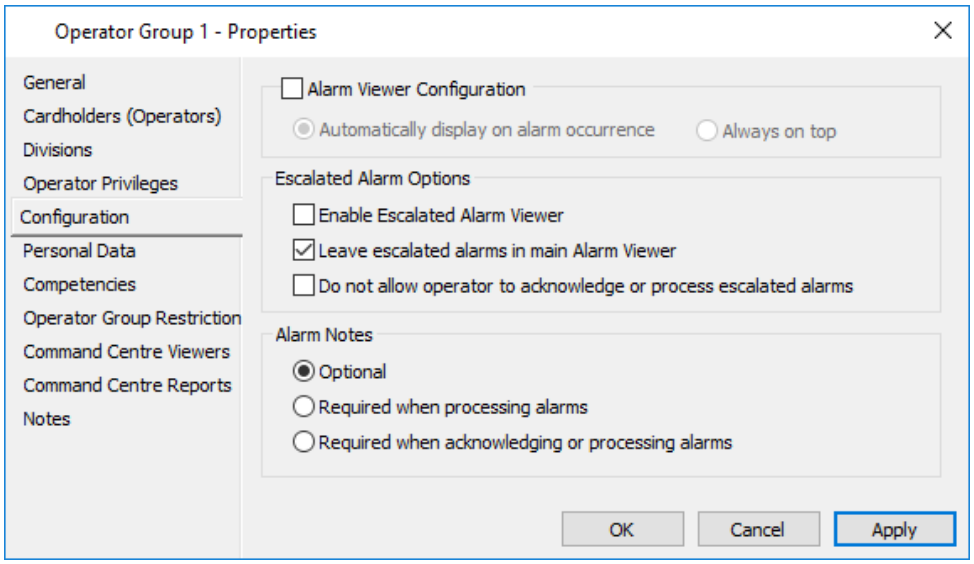


14. Fermez la fenêtre Liste principale **des** divisions.
15. Cliquez sur l'onglet **Privilèges de l'opérateur**.
16. Cliquez sur **Gérer** dans la barre de menus, puis sur **Privilèges opérateur**.
    La fenêtre Liste principale des privilèges opérateur s'ouvre.
    Sélectionnez les privilèges appropriés pour ce groupe d'opérateurs.
    Faites-les glisser et déposez-les dans l'**onglet Privilèges de l'opérateur**.



Remarque : Les opérateurs peuvent se retrouver sans les privilèges requis pour voir leurs propres événements. Cela se produit lorsque la division utilisée pour les événements est différente de la division utilisée pour modifier les éléments.

17. Fermez la fenêtre Liste principale des privilèges opérateur.
18. Cliquez sur l'onglet **Configuration (Configuration)**.



19. Souhaitez-vous modifier le comportement de la fenêtre de visionneuse d'alarme?

Si...	alors...
oui	Cochez la case **Configuration** de visionneuse **d'alarme**. Passez à l'étape 20.
non	Ne cochez pas la case **Configuration de visionneuse d'**alarme. Passez à l'étape 21. **Remarque :** Si la case à cocher n'est pas cochée, la visionneuse d'alarme reste à l'endroit où il est placé par l'opérateur actuellement connecté et ne s'affiche pas automatiquement à l'avant des autres fenêtres.

20. Cliquez sur le bouton radio approprié pour l'option que vous préférez.

    Affiche automatiquement l'occurrence de l'alarme
    La visionneuse d'alarme sera ouvert, rendu visible et placé à l'avant de toutes les autres fenêtres sur la survenue de toute nouvelle alarme.
    Avec cette option activée, vous ne pouvez pas localiser la visionneuse d'alarme hors de l'écran et l'ensemble de visionneuse d'alarme sera visible à tout moment.

    Toujours en haut
    La visionneuse d'alarme sera toujours en face de toutes les autres fenêtres.
    Lorsque cette option est activée, l'ensemble de visionneuse d'alarme est visible en tout temps et vous ne pouvez pas :
    - réduire ou réduire la visionneuse d'alarme, ou
    - localisez l'écran de visionneuse d'alarme.

21. La section **Options d'alarme escaladée** de cet écran vous permet de définir ce qui arrivera aux alarmes escaladées.
    Remarque : Les privilèges visionneuse alarme escaladé sont transmis via un groupe d'opérateurs, mais ils sont destinés à être appliqués à l'échelle du système pour un opérateur (c'est-à-dire qu'ils ne sont pas basés sur une division comme la plupart des autres privilèges transmis via un groupe d'opérateurs). Par conséquent, la désactivation du groupe d'opérateurs à partir de la vue système n'affecte pas ces paramètres (par exemple, un opérateur appartient à plusieurs groupes d'opérateurs, tous avec des paramètres d'option d'alarme escaladée différents). Si l'opérateur réduit leur vue système à un groupe d'opérateurs dont les paramètres n'activent pas la visionneuse d'alarme escaladé, il ignorera ce paramètre et affichera toujours la visionneuse d'alarme escaladé si l'un des groupes d'opérateurs a ce paramètre activé).

    Voulez-vous que les alarmes reportées s'affichent dans une fenêtre distincte de la Visionneuse d'alarmes principale ?

Si...	puis vérifiez...
oui	**Activez la** case à cocher **Visionneuse d'alarme escaladée**. La visionneuse d'alarme escaladé sera accessible à partir du menu **Moniteur**, ainsi que la visionneuse d'alarme principal.
non	**Laissez les alarmes reportées dans la** case **principale de visionneuse d'alarmes**. Toute alarme montée en puissance reste dans la visionneuse d'alarme principal avec des alarmes non remontées.

    Remarque : En cochant les deux options, vous pouvez faire apparaître les alarmes reportées dans la visionneuse d'alarme principale ainsi que la visionneuse d'alarme remontée.

22. Cochez la case **Ne pas autoriser l'opérateur à accuser réception ou à traiter les alarmes escaladées** si nécessaire pour les opérateurs de ce groupe.
    Remarque : Si cette option est activée, les boutons Accuser réception et Traiter seront désactivés sur la page de propriétés Détails de l'alarme pour les alarmes reportées.

23. Voulez-vous configurer les options de la note d'alarme ?
    Si **non**, passez à l'étape 24.
    Si **oui**, cliquez sur le bouton radio approprié pour l'option souhaitée.

    Facultatif *(Option A)*
    L'opérateur privilégié peut éventuellement sélectionner une ou plusieurs notes d'alarme avant le traitement ou l'accusé de réception d'une alarme.

    Obligatoire lors du traitement des alarmes *(Option B)*
    L'opérateur privilégié doit sélectionner une ou plusieurs notes d'alarme afin de traiter ou de traiter en bloc les alarmes à un niveau de priorité égal ou supérieur au seuil de priorité des notes d'alarme.

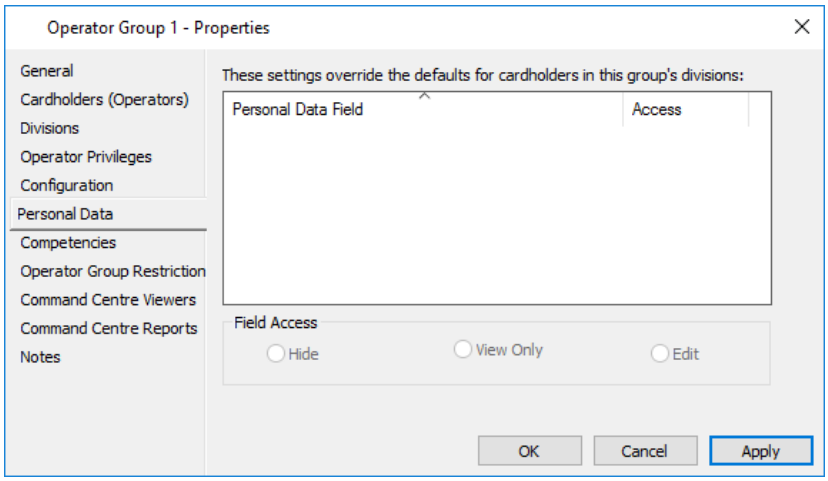
    Obligatoire lors de la reconnaissance ou du traitement des alarmes *(Option C)*
    L'opérateur privilégié doit sélectionner une ou plusieurs notes d'alarme afin de reconnaître, traiter ou traiter des alarmes de processus en bloc à un niveau de priorité égal à ou supérieur au seuil de priorité des notes d'alarme.

Remarques :

- Lorsqu'un opérateur de surveillance d'alarme est membre de plusieurs groupes d'opérateurs, les règles suivantes s'appliquent :
  1. SI au moins un groupe d'opérateurs auquel l'opérateur appartient est défini à l'*option A*, les notes d'alarme THEN sont facultatives pour Accuser réception, Processus ou Processus en vrac.
  2. SI au moins un groupe d'opérateurs auquel appartient l'opérateur est défini sur l'*option B*, ALORS les notes d'alarme sont obligatoires pour le processus ou le processus en vrac et facultatives pour l'accusé de réception.
  3. SI tous les groupes d'opérateurs auxquels l'opérateur appartient sont définis sur l'*option C*, ALORS les notes d'alarme sont obligatoires pour Accuser réception, Processus ou Processus en vrac.

  Ces règles sont données par ordre de priorité. Par conséquent, un opérateur appartenant à trois groupes d'opérateurs dont chacun a une option différente (A, B, C) ne sera pas obligé d'entrer des notes d'alarme pour les alarmes puisque la règle 1 a priorité sur la règle 2 et la règle 3. Ceci est basé sur l'hypothèse qu'un opérateur qui est forcé d'entrer des notes d'alarme est susceptible d'avoir reçu cette restriction parce qu'ils sont considérés comme moins fiables que ceux qui ne sont pas forcés.
- Si aucune ou une seule note d'alarme n'a été configurée dans les propriétés du serveur, l'option "Alarm Notes" ne sera pas activée.

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



Par défaut, cet onglet ne contient aucun champ de données personnelles (PDF). À la place, ce groupe d'opérateurs obtiendra les privilèges pour les fichiers PDF qui sont attribués au niveau PDF. Si vous souhaitez remplacer le privilège par défaut par un autre privilège, vous pouvez faire glisser les fichiers PDF sur cet onglet. Le niveau de privilège de l'opérateur pour afficher ou modifier les informations sur le titulaire de la carte stockées dans les données personnelles d'un titulaire de carte est déterminé pour chaque fichier PDF. Les privilèges PDF ne s'appliquent qu'aux détenteurs de cartes dans les divisions du groupe d'opérateurs (configurés sur l'onglet **Divisions**).

Le privilège d'opérateur par défaut pour chaque fichier PDF est déterminé lorsque les propriétés du fichier PDF sont configurées. Le privilège opérateur par défaut peut être remplacé pour chaque fichier PDF en sélectionnant une nouvelle option.

25. Pour déterminer le niveau de privilège de l'opérateur pour chacun des fichiers PDF, sélectionnez le fichier PDF et cliquez sur le bouton d'option correspondant.

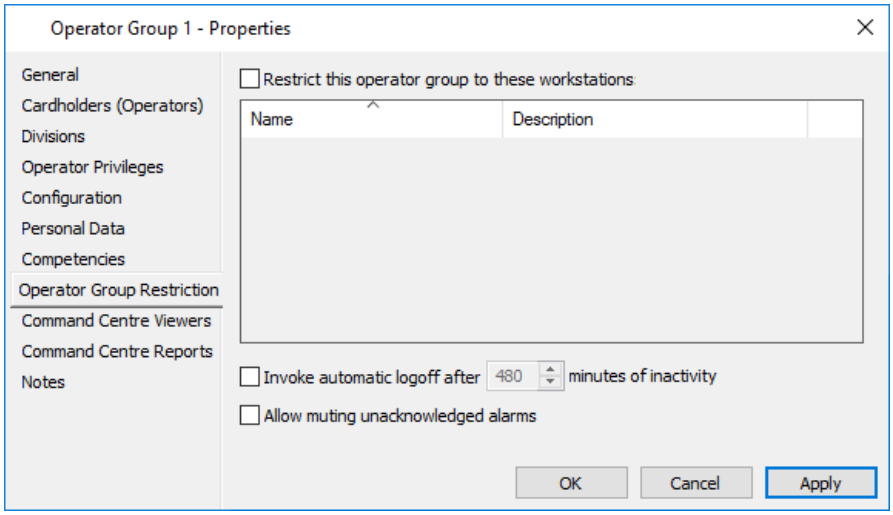
Pour attribuer un privilège à un fichier PDF, faites glisser le fichier PDF dans l'onglet **Données personnelles (Personal Data)**. Cliquez sur le PDF pour le sélectionner, puis choisissez l'un des privilèges suivants.

Privilège	Description
Masquer	Les opérateurs ne verront pas les informations enregistrées dans les divisions de ce groupe pour les titulaires de carte.
Afficher uniquement	Les opérateurs pourront consulter les informations sur les titulaires de carte pour ce PDF, pour les détenteurs de carte dans les divisions de ce groupe.
Modifier	Les opérateurs pourront saisir, afficher, modifier et supprimer les informations sur le détenteur de la carte pour ce fichier PDF, pour les détenteurs de la carte dans les divisions de ce groupe.

Remarques :

- Il existe des privilèges d'opérateur distincts pour afficher et modifier les propriétés des fichiers PDF. Si les opérateurs n'ont pas le privilège opérateur "Afficher le champ de données personnelles" ou "Modifier le champ de données personnelles" (comme indiqué dans l'onglet **Privilèges de l'opérateur**), et qu'un fichier PDF individuel est "masqué" de leur vue, ils ne seront pas même conscients de son existence.
- Si des groupes d'opérateurs et des fichiers PDF sont créés en même temps, la liste des fichiers PDF qui seront enregistrés dans le nouveau groupe d'opérateurs n'inclura que ceux qui ont été "appliqués" avant la création du groupe d'opérateurs. Pour vous assurer que tous les fichiers PDF sont inclus dans la liste, créez d'abord tous les fichiers PDF ou cochez la case Groupes d'opérateurs au fur et à mesure de leur création, puis faites glisser les nouveaux fichiers PDF dans.
- Pour supprimer un privilège PDF affecté à ce groupe d'opérateurs, cliquez avec le bouton droit de la souris dans le document **PDF**, puis **Supprimer**.

26. Voulez-vous remplacer l'accès par défaut d'une compétence pour les opérateurs de ce groupe d'opérateurs ?
    Si **oui**, consultez la section ***Remplacement des compétences des groupes d'opérateurs*** (page 53-17) pour la procédure.
    Si **non**, passez à l'étape 27.
27. Cliquez sur l'onglet **Restriction de groupe d'opérateurs** (**Operator Group Restriction**).



Remarque : Par défaut, la case **à** cocher **Restreindre ce groupe d'opérateurs à ces postes de travail** est désactivée et la grille est désactivée. Cela signifie que le groupe d'opérateurs est illimité et que ses privilèges sont donc disponibles pour une utilisation sur n'importe quel poste de travail.

28. Voulez-vous restreindre les postes de travail accessibles à ce groupe d'opérateurs? Si **oui**, passez à l'étape 29.
    Si **non**, passez à l'étape 33.
29. Cochez la case Restreindre ce groupe d'opérateurs à ces postes de travail. La grille est activée. **Remarques :**
    - Une fois cette case cochée, au moins un poste de travail doit être affecté à la grille avant que vous puissiez appliquer et enregistrer les modifications.
    - L'authentification client vérifie qu'une station de travail est ce qu'elle prétend être, à l'aide d'un certificat client installé sur la machine de la station de travail. L'activation des restrictions de station de travail signifie que toutes les stations de travail, à l'exception de la station de travail serveur, doivent être enregistrées avec un code d'enregistrement. Reportez-vous à l'"Annexe sur l'authentification du client" dans la *Note de publication du Centre de commandes*.
30. Cliquez sur **Configurer** dans la barre de menus, puis sur **Services et stations de travail**. La fenêtre **Services et stations de travail** Liste principale s'ouvre.
31. Sélectionnez les postes de travail auxquels vous souhaitez restreindre ce groupe d'opérateurs.
    Faites-les glisser et déposez-les dans l'**onglet Restriction de groupe d'opérateurs**.
32. Fermez la fenêtre Liste principale des stations de travail et des services.
33. Voulez-vous que les membres de ce groupe d'opérateurs soient automatiquement déconnectés après une période d'inactivité spécifiée ?

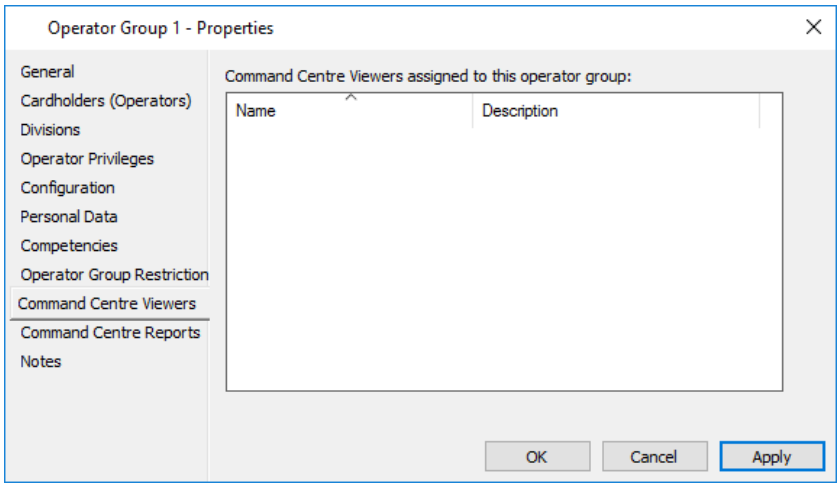
Si...	alors...
oui	cochez la case **Invoquer** la **déconnexion automatique** et indiquez la période d'inactivité dans la case à cocher. (Valeur par défaut = 60 minutes. Plage = 1 minute - 1440 minutes, soit 24heures) Voir ***Automatique*** (page 2-12) pour une explication complète.
non	allez à l'étape 34. **Remarque :** En laissant l'heure de fermeture de session automatique désactivée, l'heure de fermeture de session automatique du groupe d'opérateurs est identique à la valeur du serveur (c'est-à-dire sur l'onglet **Opérateurs par défaut** des propriétés du serveur).

34. Souhaitez-vous que les membres de ce groupe d'opérateurs voient leur connexion opérateur automatiquement désactivée après un certain nombre de jours d'inactivité ?

Si...	alors...
non	passez à l'étape suivante.
oui	cochez la case Désactiver la connexion de l'opérateur et indiquez le nombre de jours avant la désactivation de la connexion dans la boîte temporelle. (Valeur par défaut = 90 jours. Plage = 1 jour à 999 jours) **Remarques :** • Si un opérateur est affecté à plusieurs groupes d'opérateurs, le plus grand nombre de jours affectés à ces groupes d'opérateurs sera le temps utilisé, ce qui signifie que si l'un de ces groupes d'opérateurs n'a pas cette restriction activée, la connexion de l'opérateur ne sera pas désactivée parce qu'il ne s'est pas connecté.

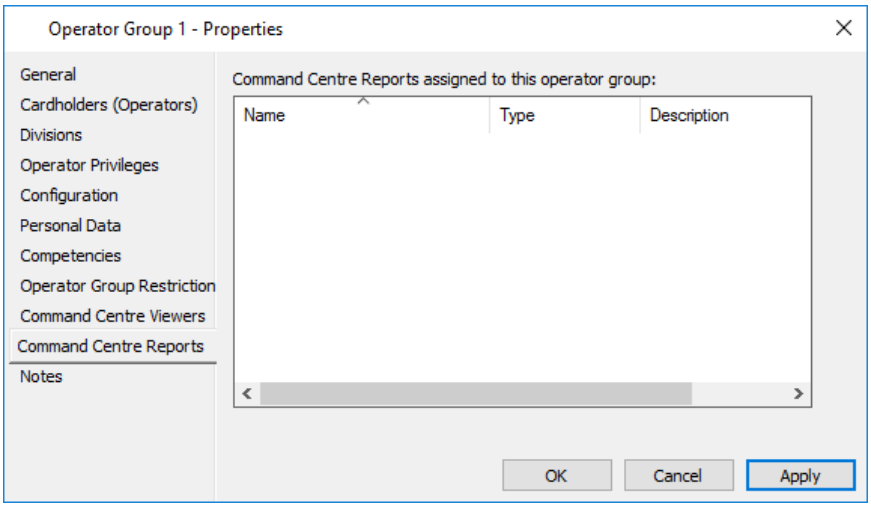
Si...	alors...
	• Il est recommandé que seuls les groupes d'opérateurs non administratifs soient configurés pour être désactivés pour cause d'inactivité. Si tous les opérateurs disposant du privilège "Modifier les opérateurs" peuvent être désactivés pour cause d'inactivité et que l'opérateur système est désactivé (comme cela est recommandé), la capacité de gérer correctement le site risque d'être perdue. • Les macros ou rapports programmés utilisent les informations d'identification de l'opérateur qui les a modifiés en dernier. Lorsque ces macros ou rapports sont exécutés, ils sont considérés comme une activité. De même, si cet opérateur est bloqué pour cause d'inactivité, la macro ou le rapport programmé ne s'exécutera pas.

35. Si vous souhaitez que les opérateurs du centre de commande puissent mettre en sourdine les alarmes non acquittées (en appuyant sur la touche <**F9**>), activez la case à cocher Autoriser la sourdine des alarmes non acquitté. Pour empêcher les opérateurs de mettre en sourdine les alarmes non acquittées, désactivez la case à cocher. **Remarques :**
    - Un opérateur ne doit appartenir qu'à un seul groupe d'opérateurs lorsque cette case est cochée pour mettre en sourdine les alarmes non acquittées.
    - Cette case à cocher n'empêche pas les opérateurs de mettre en sourdine les alarmes par d'autres méthodes, telles que la réduction du volume de leur station de travail.
36. La case à cocher Enforce FIDO2 connexion multi-facteurs sera désactivée (grisée) si les données FIDO2 n'ont pas été enrôlés contre les détenteurs de cartes. La configuration des données FIDO2 est effectuée dans le Command Centre Client. Pour plus d'informations, voir la section "FIDO2 Données " dans le fichier d'aide de Command Centre Client.
    Remarque : Si un groupe d'opérateurs a activé la fonction de connexion à plusieurs facteurs Enforce FIDO2, le centre de commande veillera à ce qu'il y ait au moins un opérateur qui puisse se connecter au centre de commande à l'aide d'un identifiant FIDO2. Cela signifie que le dernier opérateur ne sera pas désactivé pour cause d'inactivité.
37. Cliquez sur l'onglet **Afficheurs du Centre de commandes** (Command Center Viewers).



Cet onglet est en lecture seule et affiche tous les visionneuses du client du centre de commande qui sont affectés au groupe d'opérateurs dans l'ordre alphabétique.

38. Cliquez sur l'onglet **Rapports du centre de commandes**.



Cet onglet est en lecture seule et affiche tous les rapports du client du centre de commande qui sont affectés au groupe d'opérateurs dans l'ordre alphabétique.

39. Cliquez sur l'onglet **Remarques** si vous souhaitez ajouter une ou plusieurs remarques sur ce groupe d'opérateurs.
    Pour plus de détails concernant l'**onglet Notes,** voir ***Notes*** (page 6-81).
40. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications. Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Un groupe d'opérateurs est créé.

Conseils

Modification et suppression des groupes d'opérateurs
Reportez-vous à la section ***Modification d'éléments*** (page 3-26) et ***Suppression d'éléments*** (page 3-27) pour connaître les procédures sur la façon de modifier et de supprimer les groupes d'opérateurs.
Remarque : Le système n'autorise la suppression d'un groupe d'opérateurs que si tous les opérateurs (répertoriés dans l'onglet **Titulaires de carte (Opérateurs**)) sont supprimés du groupe d'opérateurs en premier.

Copier et coller
Une alternative à la méthode glisser-déplacer consiste à utiliser la méthode copier-coller.

Détail du titulaire de la carte (opérateurs)
Les titulaires de carte que vous avez ajoutés à ce groupe d'opérateurs (à l'étape 10) verront maintenant les détails s'afficher dans l'onglet Configuration de l'opérateur de l'écran Propriétés du détenteur de carte (c'est-à-dire le nom de connexion et les détails d'appartenance au groupe d'opérateurs).

Configuration des opérateurs

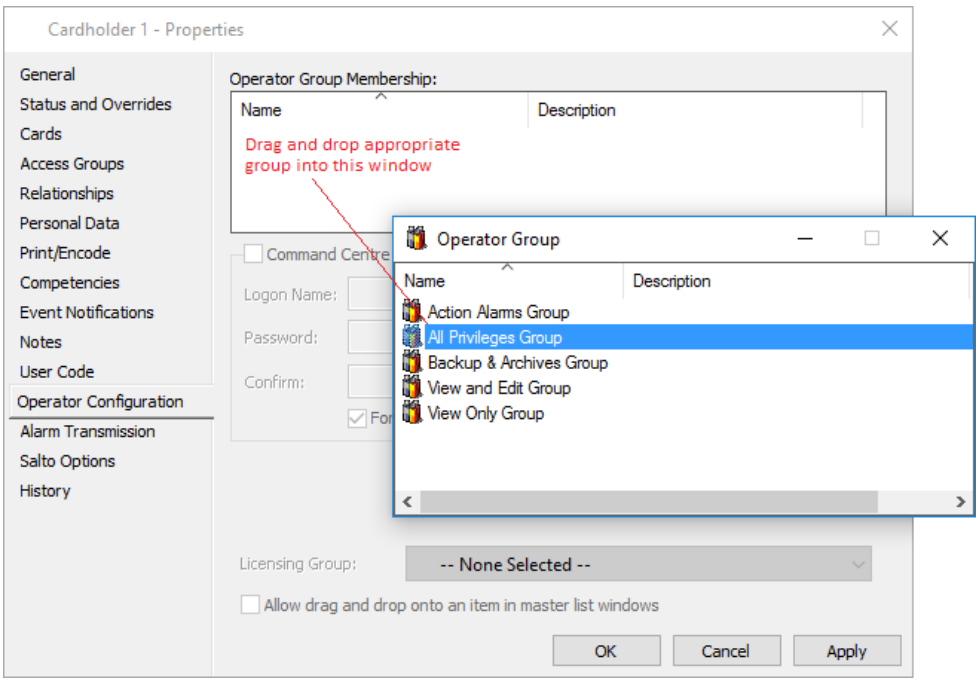
Introduction

Les administrateurs système peuvent configurer les détenteurs de cartes en tant qu'opérateurs dans Command Center en suivant la procédure suivante.

Remarque : Chaque personne est unique dans le système du Centre de commandement. Bien qu'il soit possible pour les personnes d'avoir le même nom, le Centre de commande s'assure que chaque entité doit avoir un nom d'utilisateur et un mot de passe uniques.

Procédure

1. Cliquez sur **Gérer** dans la barre de menu, puis sur Titulaires de carte.
   La fenêtre Liste principale des titulaires de carte s'ouvre (en mode grille).
2. Localisez et mettez en surbrillance le détenteur de carte à modifier.
3. Cliquez avec le bouton droit de la souris et sélectionnez Propriétés.
4. Cliquez sur l'onglet Operator Configuration (Configuration de l'opérateur).
5. Est-ce que le groupe dont l'opérateur a besoin pour être membre apparaît dans **Opérateur Groupe** Grille **d'adhésion** ?
   Si **oui**, cochez la case Ouverture de session du Centre de commandes et passez à l'étape 9.
   Si **non**, passez à l'étape 6.
6. Cliquez sur **Gérer** dans la barre de menus, puis sur **Groupes d'opérateurs**.
   La fenêtre **Liste** principale **du groupe d'opérateurs** s'ouvre.
7. Sélectionnez le groupe d'opérateurs approprié pour ce détenteur de carte, puis faites-le glisser et déposez-le dans l'onglet Configuration de l'opérateur.



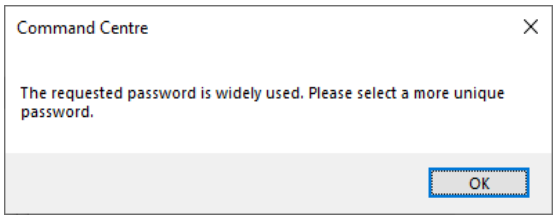
8. Fermez la fenêtre Liste principale **du groupe d'opérateurs**.
9. La section d'**ouverture de session du Centre de commandes** devient activée et le champ **Logon Name** est renseigné.

Le nom d'ouverture de session est composé de la première lettre des opérateurs Prénom et leur nom complet.

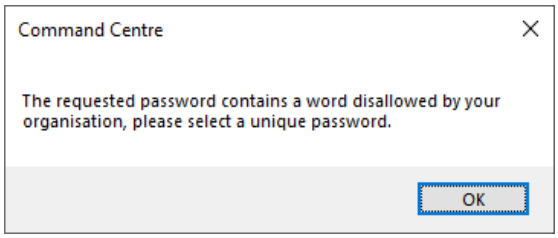
10. Générer un mot de passe pour l'opérateur :
    - saisir manuellement un mot de passe dans le champ **Mot** de **passe** et le saisir à nouveau dans le champ **Confirmer**, OU
    - cliquez sur le bouton **Générer** pour générer un mot de passe aléatoire. Un mot de passe généré par le système remplit le champ Mot de passe.

    Remarques :
    - La case à cocher **Forcer la modification du mot de passe à la prochaine ouverture de session** est activée par défaut. Cela signifie que lorsque l'opérateur ouvre une session pour la première fois, la boîte de dialogue "Mot de passe arrivé à expiration" s'affiche, ce qui les oblige à modifier leur mot de passe. Une fois la modification forcée, la case à cocher Forcer la modification du mot de passe **à la prochaine ouverture de session** redevient désactivée, sauf si la **case Conformité EN50131** ou **Conformité SSF1014** est activée dans l'onglet **Normes** des propriétés du serveur.
    - 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 s'affiche :

    Pour plus d'informations, consultez ***Empêcher les mots de passe spécifiques au contexte*** (page 2-22).

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.
12. Aviser l'opérateur de ce que sont leur nom de connexion et leur mot de passe.

Résultat

Un opérateur a été configuré.
La première fois que l'opérateur ouvre une session, il est obligé de modifier son mot de passe.

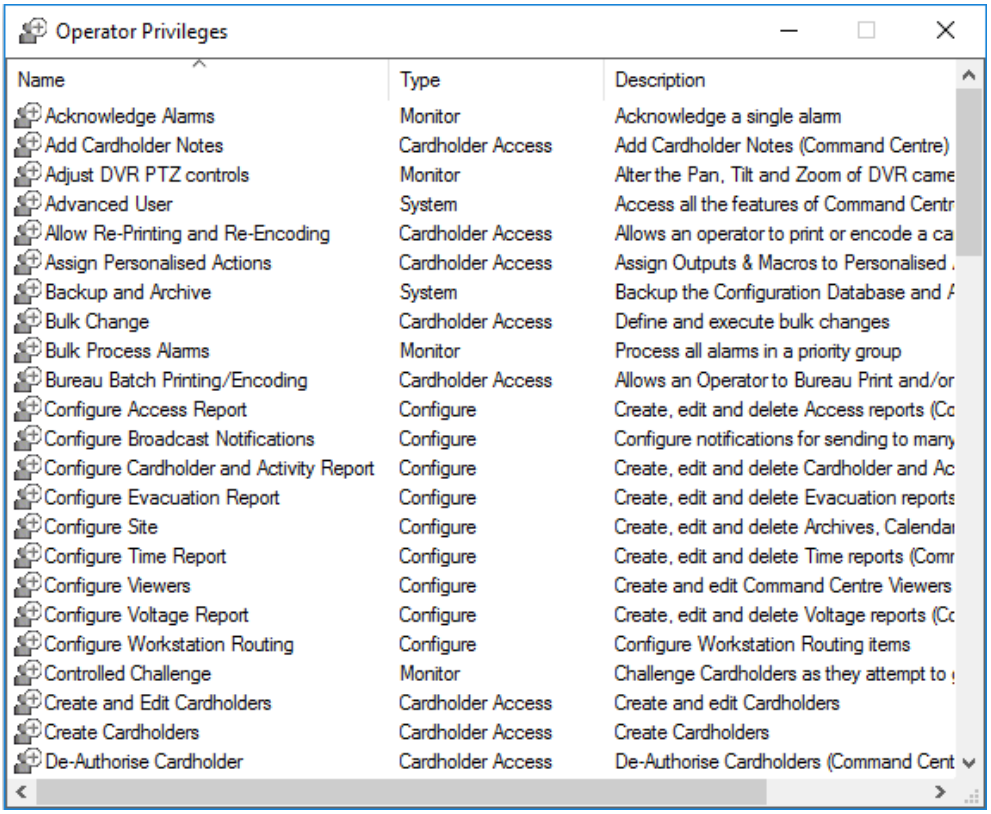
Chapitre 37 : Privilèges d'opérateur

Introduction

Les privilèges de l'opérateur restreignent les fonctionnalités disponibles pour les opérateurs (par exemple, un réceptionniste aura accès à moins de fonctionnalités qu'une personne responsable de la configuration et de la maintenance du système).

Fenêtre Liste principale des privilèges d'opérateur

La fenêtre **Privilèges opérateur** de la liste principale s'ouvre en mode grille.



Chaque privilège opérateur a un privilège "Type". Les types de privilèges correspondent à un rôle d'opérateur particulier et les privilèges associés ont le même type.

Cette fenêtre peut être triée par type de privilège, ce qui permet de trier les privilèges de l'opérateur en groupes logiques. Cela facilite la configuration des groupes d'opérateurs de réseau.

Quels privilèges d'opérateur vous devez

Introduction

Les listes suivantes de privilèges d'opérateur sont triées par privilège "Type". Les types de privilèges permettent de trier les privilèges de l'opérateur en groupes logiques, ce qui peut être utile lors de la configuration des groupes d'opérateurs. Ces listes indiquent ce que chaque privilège vous permettra de faire, ou vous donnera accès à.

Remarques :

- **Affichage** signifie qu'un utilisateur peut ouvrir la fenêtre de la liste principale et consulter les pages de propriétés, mais ne peut pas les modifier.
- **Modifier** signifie qu'un utilisateur peut modifier les propriétés des éléments associés, en créer de nouveaux et en supprimer d'anciens.
- **Aucune propriété signifie que, bien qu'un opérateur puisse voir** quelque chose dans une fenêtre de liste principale, il ne peut pas réellement "afficher" les propriétés de celle-ci (par exemple, tous les opérateurs peuvent voir la fenêtre de liste **principale de la description de l'état**, et s'il y a des rapports de titulaire de carte en existence, ils pourront les voir répertoriés là, mais ils ne pourront pas ouvrir les propriétés pour afficher réellement ces rapports à moins qu'ils n'aient le privilège "Afficher les titulaires de carte").

Cette rubrique couvre :

- ***Accès aux titulaires*** de ***carte*** (page 37-3)
- ***Configurer*** (page 37-11)
- ***Gérer*** (page 37-24)
- ***Moniteur*** (page 37-26)
- ***Remplacer*** (page 37-30)
- ***Système*** (page 37-33)

Accès aux titulaires de carte

Ajouter une carte ou des informations d'identification

Un opérateur disposant du privilège "Ajouter une carte ou des informations d'identification" dans une division peut ajouter une carte, des informations d'identification mobiles ou des informations d'identification FIDO2 à un titulaire de carte dans cette division à la fois dans le client Command Center et dans le client de configuration de la division. **Remarques :**

- Ce privilège inclut "Afficher les détenteurs de cartes" (c'est-à-dire qu'il peut afficher les propriétés des détenteurs de cartes, à l'exception des notes des détenteurs de cartes et des détails de configuration de l'opérateur, pour tout détenteur de cartes dans cette division).
- "Modifier les titulaires de carte" conserve la capacité d'exécuter cette action.
- Ne permet pas la suppression de la carte ou des informations d'identification (c'est-à-dire que le privilège "Supprimer la carte ou les informations d'identification" est nécessaire pour faire cela).
- Ne permet pas la modification d'une carte ou d'informations d'identification existantes (c'est-à-dire que l'option "Modifier la carte ou l'attribut des informations d'identification" est nécessaire pour cela).

Ajouter des notes de titulaire

Un opérateur avec le privilège "Ajouter des notes de titulaire de carte" dans une division peut effectuer les opérations suivantes dans Command Center :

- Affichez et ajoutez des notes de titulaire de carte, mais ne pouvez pas modifier ou supprimer des notes existantes (Centre de commandes client uniquement).
- Afficher les notes sur les titulaires de carte uniquement (client de configuration uniquement).
- Rechercher les titulaires de carte et afficher uniquement toutes les propriétés du titulaire de carte **Opérateur,** onglet **Configuration**.
- Voir les modifications apportées aux notes sous l'onglet **Historique**.
- Voir l'option PhotoID dans le menu **Configurer** mais ne peut pas modifier.

Autoriser la réimpression et le recodage

Un opérateur avec le privilège "Autorise la réimpression et le recodage" dans une division peut effectuer les opérations suivantes :

- Tout ce que permet le privilège "Imprimer et encoder la carte".
- Imprimez et/ou codez une carte qui a déjà été imprimée/codée sur une carte auparavant avec les mêmes détails d'identification (c'est-à-dire le code d'installation, le numéro de la carte et le niveau d'émission).
  Remarque : Sans cela, les cartes privilèges ne peuvent être imprimées et encodées qu'une seule fois.

Affecter des actions personnalisées

Ce privilège s'applique uniquement à la mosaïque Actions personnalisées du titulaire de carte dans le client Command Center.

Un opérateur a besoin du privilège "Affecter des actions personnalisées" dans la division de la sortie ou de la macro, pour pouvoir affecter cet élément à la vignette Actions personnalisées du titulaire de carte.
Remarque : L'opérateur a besoin de "Visualiser le site" ou "Modifier le site" dans la division de la zone d'accès pour l'attribuer à la tuile.

Modification en bloc

Un opérateur disposant du privilège "Modification en bloc" dans une division peut effectuer les opérations suivantes :

- Ajouter ou supprimer une modification en vrac.
- Affichez et configurez les propriétés de toute modification globale dans cette division.
- Enregistrer une modification en masse dans cette division.
- Effectuez un changement en bloc dans cette division. [Une modification en bloc ne modifie que les éléments que l'opérateur aurait suffisamment de privilèges pour modifier via l'interface utilisateur standard du Centre de commandes (c'est-à-dire en dehors de la modification en bloc).]

Bureau Impression/codage par lots

Un opérateur disposant du privilège "Impression/encodage par lots Bureau" dans une division peut effectuer les opérations suivantes :

- Affichez les propriétés des types de cartes de cette division.
- Encodez, ou imprimez et encodez plusieurs cartes d'un type de carte.

Créer et modifier les titulaires

Un opérateur disposant du privilège "Créer et modifier des titulaires de carte" dans une division peut effectuer les opérations suivantes :

- Affichez et modifiez les propriétés de la description d'un rapport Titulaire de carte ou de la description d'un rapport Time & Attendance dans cette division.
- Créez de nouvelles descriptions de rapport de titulaire de carte ou de rapport de temps et de présence descriptions dans cette division.
- Affichez et modifiez les propriétés des titulaires de cartes pour tous les titulaires de cartes de cette division, à l'EXCEPTION des onglets **Notes** et **Configuration de l'opérateur des titulaires de cartes** (aucun des onglets n'est visible).
- Pardonnez à un détenteur de carte dans cette division les violations anti-passback pour une zone d'accès sélectionnée (doit également avoir le privilège "Override" dans la division de la zone d'accès).
- Ajoutez de nouveaux détenteurs de cartes dans cette division.

- Exécuter les Assistants Inscription dans cette division. [Peut modifier les données des titulaires de carte dans un Assistant Inscription uniquement en fonction de leurs privilèges de modification habituels pour ce titulaire de carte.]
- Utilisez l'utilitaire de **lecture de carte MIFARE** pour lire les données de la carte.

Créer des titulaires

Un opérateur disposant du privilège "Créer des titulaires de carte" dans une division peut créer des titulaires de carte, mais ne peut pas éditer des titulaires de carte.

Désautoriser le titulaire de la carte

Un opérateur disposant du privilège "Désautoriser le détenteur de la carte" dans une division peut effectuer les opérations suivantes dans le Centre de commandement :

- Tout ce que permet le privilège "Voir les détenteurs de cartes", ET
- Non applicable au client de configuration :
  Désautoriser un détenteur de carte (Centre de commande), mais ne peut pas les activer ou modifier d'autres entrées sur la vignette Cartes.

Supprimer les titulaires

Un opérateur disposant du privilège "Supprimer le détenteur de la carte" dans une division peut supprimer n'importe quel détenteur de la carte dans cette division.

Désactiver la carte

Un opérateur disposant du privilège "Désactiver la carte" dans une division peut effectuer les opérations suivantes dans le client du centre de commande :

- Tout ce que permet le privilège "Voir les détenteurs de cartes", ET
- Non applicable au client de configuration :
  Désactivez une carte Titulaire de carte ou modifiez ses dates de début et de fin pour une carte activée, mais ne pouvez pas activer une carte Titulaire de carte Card ou modifier d'autres entrées sur la vignette **Titulaire de carte**.

Modifier les groupes d'accès

Un opérateur disposant du privilège "Modifier les groupes d'accès" dans une division peut effectuer les opérations suivantes :

- Affichez et modifiez les propriétés des groupes d'accès dans cette division, SAUF l'ajout ou la suppression de détenteurs de cartes dans le groupe d'accès (vous pouvez toujours "afficher" les noms des détenteurs de cartes).
- Ajouter ou supprimer des groupes Access.
- Affichez et modifiez les propriétés d'une description de rapport de groupe d'accès, dans cette division.
- Ajouter ou supprimer dans cette division les descriptions de rapport Access Group.
- Exécuter les descriptions d'état du groupe d'accès dans cette division. Dans ce

cas, l'état Groupe d'accès inclut uniquement les groupes d'accès auxquels l'opérateur a le privilège "Afficher les groupes d'accès" ou "Modifier les groupes d'accès".

Modifier donnés biométrique

- Un opérateur disposant du privilège "Modifier les données biométriques" dans une division peut saisir/inscrire des données biométriques pour les lecteurs de Morpho à l'aide de Finger/Vein/Wave.
  Remarques :
- Ce privilège inclura "Afficher les détenteurs de cartes" (c.-à-d. peut afficher les propriétés des détenteurs de cartes, à l'exception des notes des détenteurs de cartes et des détails de configuration de l'opérateur, pour tous les détenteurs de cartes de cette division).
- "Modifier les titulaires de carte" conservera la possibilité d'effectuer cette action.

Modifier la carte ou les informations d'identification

Un opérateur disposant du privilège "Modifier la carte ou les informations d'identification" dans une division peut ajouter, supprimer ou modifier les attributs (statut, niveau d'émission, dates d'activation et d'expiration) d'une carte ou des informations d'identification mobiles de tout détenteur de carte dans cette division, à la fois sur le client Command Center et sur le client Command Center.
Le privilège comprend les éléments suivants :

- privilège "Ajouter une carte ou des informations d'identification"
- privilège "Supprimer la carte ou les informations d'identification"
- privilège "Modifier la carte ou l'attribut d'informations d'identification"

Remarques :

- Ce privilège inclut "Afficher les détenteurs de cartes" (c.-à-d. peut afficher les propriétés des détenteurs de cartes, à l'exception des notes des détenteurs de cartes et des détails de configuration de l'opérateur, pour tout détenteur de cartes dans cette division).
- "Modifier les titulaires de carte" conserve la capacité d'exécuter ces actions.

Modifier l'attribut de carte ou d'identification

Un opérateur disposant du privilège "Modifier la carte ou l'attribut d'informations d'identification" dans une division peut modifier les attributs suivants d'une carte ou d'informations d'identification mobiles existantes d'un titulaire de carte dans cette division, à la fois dans le client du Centre de commandes et dans le client de configuration.
Les attributs modifiables sont les suivants :

- État
- Niveau de problème
- Date d'activation (De)
- Date d'expiration (Jusqu'au)

Exclusions :

- Le privilège n'autorise pas la fonctionnalité Imprimer et encoder ni Afficher les broches. Ces fonctions ont leurs privilèges.
- Les numéros de carte, les numéros de téléphone mobile, les adresses de messagerie et les descriptions de modèle mobile ne sont pas modifiables (pour les cartes existantes et les informations d'identification, elles ne sont pas modifiables par un privilège quelconque).

Remarques :

- Ce privilège inclut "Afficher les détenteurs de cartes" (c.-à-d. peut afficher les propriétés des détenteurs de cartes, à l'exception des notes des détenteurs de cartes et des détails de configuration de l'opérateur, pour tout détenteur de cartes dans cette division).
- "Modifier les titulaires de carte" conserve la capacité d'exécuter cette action.

Modifier le nom du détenteur de la carte

Un opérateur disposant du privilège "Modifier le nom du détenteur de carte" dans une division peut modifier le prénom, le nom et le nom abrégé d'un détenteur de carte dans cette division à la fois dans le client Command Center et dans le client de configuration. **Remarques** :

- Ce privilège inclut "Afficher les détenteurs de cartes" (c'est-à-dire qu'il peut afficher les propriétés des détenteurs de cartes, à l'exception des notes des détenteurs de cartes et des détails de configuration de l'opérateur, pour tout détenteur de cartes dans cette division).
- "Modifier les titulaires de carte" conserve la capacité d'exécuter cette action.

Modifier les notes du titulaire de carte

Un opérateur disposant du privilège "Modifier les notes du titulaire de carte" dans une division peut effectuer les opérations suivantes :

- Affichez, ajoutez ou supprimez des notes pour les détenteurs de cartes dans cette division.
- Afficher toutes les propriétés des titulaires de carte dans cette division, SAUF **Opérateur**, onglet **Configuration**.

Modifier les données personnelles du titulaire de la carte

Un opérateur disposant du privilège "Modifier les données personnelles d'un titulaire de carte" dans une division peut modifier les valeurs de champ de données personnelles d'un titulaire de carte dans cette division à la fois dans le client Command Center et le client de configuration.
Remarques :

- Ce privilège inclut "Afficher les détenteurs de cartes" (c'est-à-dire qu'il peut afficher les propriétés des détenteurs de cartes, à l'exception des notes des détenteurs de cartes et des détails de configuration de l'opérateur, pour tout détenteur de cartes dans cette division).

- "Modifier les titulaires de carte" conserve la capacité d'exécuter ces actions.
- Ce privilège complète le privilège de groupe d'opérateurs existant relatif aux données personnelles pour permettre aux fichiers PDF d'être modifiés, seulement affichés ou masqués. *Par exemple*, un opérateur disposant du privilège "Modifier les données personnelles du titulaire de carte" ne peut pas modifier un fichier PDF qui en est masqué ou qui est affiché uniquement.

Modifier les titulaires

Un opérateur disposant du privilège "Modifier les titulaires de carte" dans une division peut modifier tous les champs des titulaires de carte, SAUF la **division**, et empêche ces opérateurs de créer de nouveaux titulaires de carte.

Modifier détails passager

Un opérateur disposant du privilège "Modifier les détails des passagers" dans une division peut ajouter/modifier/supprimer un étage par défaut pour un système d'ascenseur ThyssenKrupp. Cela permet à l'opérateur d'afficher une liste de groupes d'ascenseurs et, à partir de cette liste, d'afficher les zones d'accès par défaut admissibles et de les affecter.

Modifier le contrôle d'accès

Un opérateur avec le privilège "Modifier le contrôle d'accès" dans une division peut effectuer les opérations suivantes :

- Affichez les propriétés des groupes Access de cette division.
- Ajoutez ou supprimez les détenteurs de cartes (auxquels ils doivent avoir le privilège "Afficher") des groupes d'accès de cette division.

Imprimer/Aperçu & Encoder la carte

Un opérateur avec le privilège "Imprimer/Aperçu et encoder" dans une division peut effectuer les opérations suivantes :

- Afficher un aperçu ou imprimer les cartes des titulaires de cette division.
- Encoder ou imprimer et coder les cartes pour les titulaires de carte de cette division, avec la possibilité d'entrer des NIP définis par l'utilisateur ou de générer des NIP aléatoires, mais pas de voir les NIP (car ils seront masqués).
  Remarque : Le type de carte de la carte n'a pas besoin de se trouver dans cette division.
- Affichez les propriétés du détenteur de la carte de cette division.
- Affichez les propriétés des détenteurs de cartes pour tous les détenteurs de cartes de cette division, à l'exception des notes des détenteurs de cartes et de l'onglet Configuration de l'opérateur.
- Exécutez les Assistants Inscription dans cette division, mais en mode Affichage seul (impossible de modifier les données des titulaires de cartes ou de créer de nouvelles cartes pour un titulaire de cartes).
- Exécutez les Assistants Inscription dans cette division avec la possibilité

d'imprimer ou d'encoder des cartes pour les détenteurs de cartes dans cette division. Entrez des NIP définis par l'utilisateur ou générez des NIP aléatoires lors du codage des cartes mais ne les affichez pas (car elles sont masquées). **Remarque :** Le type de carte n'a pas besoin d'être dans cette division.

Supprimer la carte ou les informations d'identification

Un opérateur disposant du privilège "Supprimer la carte ou les informations d'identification" dans une division peut supprimer une carte, des informations d'identification mobiles ou des informations d'identification FIDO2 d'un détenteur de carte dans cette division à la fois dans le client et le client de configuration Command Center. **Remarques :**

- Ce privilège inclut "Afficher les détenteurs de cartes" (c'est-à-dire qu'il peut afficher les propriétés des détenteurs de cartes, à l'exception des notes des détenteurs de cartes et des détails de configuration de l'opérateur, pour tout détenteur de cartes dans cette division).
- N'autorise pas l'ajout de cartes ou d'informations d'identification.
- N'autorise pas la modification des cartes ou des informations d'identification.
- "Modifier les titulaires de carte" conserve la capacité d'exécuter cette action.

Afficher les groupes d'accès

Un opérateur disposant du privilège "Afficher les groupes d'accès" dans une division peut effectuer les opérations suivantes :

- Affichez les propriétés des groupes d'accès dans cette division, y compris les noms de tous les titulaires de carte qui appartiennent au groupe d'accès à.
- Affichez et modifiez les propriétés d'une description de rapport de groupe d'accès, dans cette division.
- Exécuter les rapports Access Group dans cette division. Dans ce cas, l'état Groupe d'accès n'inclura que les groupes d'accès pour lesquels l'opérateur dispose du privilège "Afficher les groupes d'accès".
- Ajouter ou supprimer des descriptions d'état Groupe Access dans cette division.

Afficher les notes des titulaires de carte

Un opérateur disposant du privilège "Afficher les notes du titulaire de carte" dans une division peut effectuer les opérations suivantes :

- Afficher les notes des titulaires de carte de cette division.
- Afficher toutes les propriétés des titulaires de carte dans cette division, SAUF **Opérateur,** onglet **Configuration**.

Afficher les titulaires de carte

Un opérateur disposant du privilège "Afficher les détenteurs de cartes" dans une division peut effectuer les opérations suivantes :

- Affichez et modifiez les propriétés de la description d'un rapport Titulaire de carte ou de la description d'un rapport Time & Attendance dans cette division.
- Créez de nouvelles descriptions de rapport de titulaire de carte ou de rapport de temps et de présence descriptions dans cette division.

- Afficher les propriétés de tous les détenteurs de cartes **Notes** et onglets **Configuration** de l'**opérateur**.
- Exécutez les Assistants Inscription dans cette division, mais en mode Affichage seul (aucune possibilité de modifier les données des titulaires de carte, de créer, d'imprimer ou d'encoder des cartes).
- Utilisez l'utilitaire de **lecture de carte MIFARE** pour lire les données de la carte.

Afficher les codes utilisateur des titulaires de cartes chiffrés (API uniquement)

Un opérateur disposant du privilège « Afficher les codes d'utilisateur de titulaire de carte chiffrés » peut afficher les codes d'utilisateur de titulaire de carte chiffrés (API REST uniquement).
Remarque : Le privilège « Utilisateur avancé » ne transmet pas automatiquement ce privilège.

Afficher les événements

Remarque : Le but de ce privilège est de permettre aux opérateurs qui n'ont pas (et ne devraient pas) le privilège "Afficher les événements et les alarmes" et dont le rôle n'implique pas la surveillance/gestion des alarmes, d'afficher les événements dans le client du centre de commande (en particulier, mais pas exclusivement, les événements sur la vignette de la piste d'événements) et de voir l'état d'alarme d'un élément dans l'un des clients. Il ne sera pas possible de voir les détails de l'alarme.

Un opérateur disposant du privilège "Afficher les événements" dans une division peut effectuer les opérations suivantes :

- Afficher les événements dans cette division à l'aide du client du centre de commandement.
- À l'exception de ce qui précède, ne sera PAS en mesure de faire les autres choses que le privilège "Voir les événements et les alarmes" permet.

Afficher les codes confidentiels

Il existe deux types de NIP (numéros d'identification personnels); PIN générés par le système et PIN définis par l'utilisateur. Un opérateur disposant du privilège "Afficher les NIP" peut afficher les NIP attribués aux cartes selon les règles suivantes :

- Un opérateur ne peut voir un code NIP généré par le système que s'il dispose du privilège "Voir les codes NIP" ET si le code NIP n'a pas été modifié. S'il est modifié, il devient alors un code NIP défini par l'utilisateur et les règles suivantes s'appliquent.
- Un opérateur ne peut voir les codes NIP définis par l'utilisateur que s'il dispose du privilège "Voir les codes NIP" ET si la case Stocker les codes NIP pour les consulter ultérieurement a été cochée dans l'onglet Sécurité des cartes des propriétés du serveur au moment où le code PIN a été défini.
- Les NIP définis par l'utilisateur modifiés avant la **case** à cocher **Stocker les NIP pour consultation ultérieure** (onglet **Sécurité de la carte de** propriétés du serveur) ne peuvent pas être récupérés et doivent être réaffectés si le détenteur de la carte les a oubliés.

Remarque : La fonctionnalité "Afficher les NIP" n'est pas prise en charge pour les cartes PIV.

Configurer

Configurer le rapport d'accès

Un opérateur disposant du privilège "Configurer le rapport d'accès" dans une division peut enregistrer ou supprimer n'importe quel rapport d'accès dans le client du centre de commande, pour la division du rapport, mais uniquement si l'opérateur a également le privilège d'afficher les rapports.

Configurer les notifications de diffusion

Un opérateur d'un site disposant de "Notifications" incluses dans le fichier de licence et du privilège "Configurer les notifications de diffusion" dans une division peut afficher, enregistrer, modifier et supprimer les éléments de notification de diffusion dans le client du centre de commande.

Configurer le rapport des titulaires de carte et des activités

Un opérateur disposant du privilège "Configurer le détenteur de carte et le rapport d'activité" dans une division peut enregistrer ou supprimer tout détenteur de carte et rapport d'activité dans le client du centre de commande, pour la division du rapport, mais uniquement si l'opérateur a également le privilège de consulter les rapports.

Configurer le rapport d'évacuation

Un opérateur disposant du privilège "Configurer le rapport d'évacuation" dans une division peut effectuer les opérations suivantes dans le client du centre de commande:

- Créer un rapport d'évacuation.
- Supprimer un rapport d'évacuation dans cette division.
- Modifiez les propriétés d'un rapport d'évacuation dans cette division.

Remarque : Pour afficher les propriétés d'un rapport d'évacuation enregistré existant et/ou l'exécuter, un opérateur doit disposer du privilège "Afficher les événements et les alarmes" dans la division du rapport d'évacuation. Disposer de privilèges différents pour la création et l'exécution de rapports d'évacuation permet d'empêcher les opérateurs qui sont en mesure d'exécuter et d'imprimer des rapports d'évacuation préconfigurés (en cas d'urgence) de modifier leur configuration.

Configurer le site

Un opérateur disposant du privilège "Configurer le site" dans une division peut ajouter ou supprimer des éléments du Centre de commandes ou afficher et modifier leurs propriétés (c'est-à-dire utiliser les options de menu contextuel "Nouveau", "Supprimer", "Propriétés") pour tous les éléments du Centre de commandes au sein de cette division et des types suivants :
- Archives
- CardType, y compris la modification de la disposition de la carte
- Format de carte universel
- Division
- Jour Catégorie *
- Calendrier

- Calendrier spécial
- Morpho Type biométrique
- Compétences
- Filtre de notification

* Les catégories de jours sont sans division, donc le fait d'avoir "Configurer le site" dans n'importe quelle division permet à un opérateur de configurer n'importe quelle catégorie de jours.

Exclusions: Les actions suivantes, précédemment incluses dans ce privilège, sont explicitement exclues de ce privilège et requièrent le privilège "Modifier le site" pour effectuer les opérations suivantes:
- Arrêt FTP
- Début FTP
- Resynchroniser les bases de données

Configurer le rapport de temps

Un opérateur disposant du privilège "Configurer le rapport temporel" dans une division peut enregistrer ou supprimer n'importe quel rapport temporel dans le client du centre de commande, pour la division du rapport, mais uniquement si l'opérateur a également le privilège d'afficher les rapports.

Configurer les visionneuses

Un opérateur disposant du privilège "Configurer les visionneuses" dans une division peut créer, modifier et supprimer des visionneuses dans cette division, dans le client Command Center.
Remarque : Ce privilège n'accorde pas automatiquement d'autres privilèges, ce qui signifie que l'Opérateur aura besoin de privilèges supplémentaires pour pouvoir voir les éléments (y compris les détenteurs de cartes) à inclure dans la configuration.

Configurer le rapport de tension

Un opérateur disposant du privilège "Configurer le rapport de tension" dans une division peut enregistrer ou supprimer n'importe quel rapport de tension dans le client du centre de commande, pour la division du rapport, mais uniquement si l'opérateur a également le privilège d'afficher les rapports.

Configurer le routage de station de travail

Un opérateur disposant du privilège "Configurer le routage de station de travail" dans une division, peut créer, modifier et supprimer des éléments de routage de station de travail dans cette division, dans le client du Centre de commandes.

Modifier la configuration d'alarme

Un opérateur disposant du privilège "Modifier la configuration d'alarme" dans une division peut effectuer les opérations suivantes :

- Créer ou supprimer des plans d'action dans cette division.
- Affichez et modifiez les propriétés des plans d'action de cette division.
- Créer ou supprimer des balises d'insertion.

- Affichez et modifiez les propriétés des balises d'insertion dans cette division.
- Créer ou supprimer des instructions d'alarme dans cette division.
- Afficher et modifier les propriétés des instructions d'alarme.

Modifier les définitions de compétences

Un opérateur disposant du privilège « Modifier les définitions de compét-ences » dans une division peut effectuer les opérations suivantes :

- Ajouter ou supprimer une compétence dans cette division.
- Afficher ou modifier une compétence dans cette division.

Modifier les divisions

Un opérateur disposant du privilège « Modifier les divisions » peut effectuer les opérations suivantes :

- Ajouter ou supprimer une division.
- Afficher ou modifier une division.

Modifier les ensembles d'états de carte

Un opérateur disposant du privilège "Modifier les jeux d'états de carte" dans une division peut créer, modifier et supprimer des jeux d'états de carte dans cette division, dans le client du centre de commande.
Remarque : Les opérateurs doivent disposer de ce privilège dans au moins une division afin de voir l'icône État de la carte dans la barre d'outils **Administration** du client du centre de commande.

Modifier les types de cartes

Un opérateur disposant du privilège « Modifier les types de cartes » dans une division peut effectuer les opérations suivantes :

- Modifiez les propriétés des types de cartes dans cette division, à l’exception des propriétés qui ne sont pas modifiables.
- Ajouter ou supprimer des types de cartes dans cette division.
- Modifiez les mises en page des cartes dans cette division.

Modifier la notification du détenteur de la carte

Un opérateur disposant du privilège "Modifier la notification du titulaire de carte" dans une division peut effectuer les opérations suivantes :

- Activez/désactivez les notifications dans l'onglet **Notifications d'événements** d'un enregistrement du détenteur de la carte.
- Modifier la méthode de notification affectée à chaque filtre de notification sur **Onglet Notifications d'**événements d'un enregistrement de titulaire de carte.
- Modifiez le calendrier attribué à un détenteur de carte en le remplaçant par le calendrier par défaut ou par un calendrier spécial spécifique.
- Les fonctions suivantes requièrent un privilège supplémentaire ainsi que le privilège "Edit Titulaire de carte Notification" :

Pour pouvoir...	un opérateur doit également...
ajouter ou supprimer un filtre d'un titulaire de carte,	Privilège "Afficher le site" dans la division du filtre de notification.
ajouter un calendrier à la page de notification d'un titulaire de carte,	Privilège "Afficher les annexes" dans la division de l'annexe.
mettre à jour les onglets Titulaire de carte autres que l'onglet **Notification d'événement,**	le privilège approprié du détenteur de la carte (p. ex. "Edit Titulaire de carte", "Delete Titulaire de carte", "Edit Titulaire de carte Notes").

Le privilège "Modifier la notification du titulaire de carte" reçoit en soi le privilège de "Afficher les titulaires de carte".

Modifier les modèles d'inscription

Un opérateur disposant du privilège "Modifier les modèles d'inscription" dans une division peut effectuer les opérations suivantes :

- Créer un modèle d'inscription dans cette division.
- Supprimer un modèle d'inscription dans cette division.
- Affichez les propriétés des modèles d'inscription de cette division.
- Modifiez les propriétés des modèles d'inscription de cette division.

Remarque : Certaines propriétés de modèle d'inscription nécessitent des privilèges supplémentaires pour être configurées (p. ex. "Visualiser le site" est nécessaire dans la division Type de carte pour sélectionner le type de carte, et "Visualiser les définitions de données personnelles" est nécessaire dans la division PDF pour sélectionner ce PDF dans le modèle d'inscription).

Modifier les interfaces de données d'entreprise

Un opérateur disposant du privilège "Modifier les interfaces de données d'entreprise" peut effectuer les opérations suivantes :

- Créer une interface de données d'entreprise (EDI)
- Enregistrer un EDI
- Modifier un EDI
- Exécuter un EDI
- Activer/désactiver un EDI.

Modifier le rapport d'évacuation

Un opérateur disposant du privilège "Modifier le rapport d'évacuation" dans une division peut modifier les propriétés d'un rapport d'évacuation dans cette division, dans le client de configuration.

Remarque : Pour afficher les propriétés d'un rapport d'évacuation enregistré existant et/ou l'exécuter, un opérateur doit disposer du privilège "Afficher les événements et les alarmes" dans la division du rapport d'évacuation. Disposer de privilèges différents pour la création et l'exécution de rapports d'évacuation permet d'empêcher les opérateurs qui sont en mesure d'exécuter et d'imprimer des rapports d'évacuation préconfigurés (en cas d'urgence) de modifier leur configuration.

Modifier Guard Tours

Un opérateur disposant du privilège "Edit Guard Tours" dans une division peut effectuer les opérations suivantes :

- Modifiez les propriétés de Guard Tours dans cette division, y compris la liste des points de contrôle qui sont configurés pour la visite.
- Ajouter ou supprimer Guard Tours dans cette division.

Modifier les jeux d'icônes

Un opérateur disposant du privilège "Modifier les jeux d'icônes" peut exécuter les opérations suivantes :

- Ajouter ou supprimer un jeu d'icônes dans n'importe quelle division.
- Affichez et modifiez les propriétés de n'importe quel jeu d'icônes dans n'importe quelle division.

Remarque : Les jeux d'icônes sont sans division, ce privilège s'applique à l'échelle du système.

Modifier les casiers

Un opérateur disposant du privilège "Modifier les casiers" dans une division peut créer, modifier et supprimer des casiers et des banques de casiers.

Modifier les macros

Un opérateur disposant du privilège "Modifier les macros" dans une division peut effectuer les opérations suivantes :

- Affichez et modifiez les propriétés des macros de cette division (à l'exception de la planification de la macro).
- Ajouter ou supprimer des macros dans cette division (à l'exception de la planification de la macro).
- Dupliquer une macro dans cette division (à l'exception de la planification de la macro).

Modifier les opérateurs

Un opérateur disposant du privilège "Modifier les opérateurs" dans une division peut effectuer les opérations suivantes :

- Afficher tous les privilèges opérateur (leur nom et description).
- Affichez et modifiez les propriétés des groupes d'opérateurs de cette division (y compris l'ajout de privilèges à ces groupes d'opérateurs, à condition que l'opérateur ait le privilège "Modifier les opérateurs" dans chaque division à laquelle ces privilèges s'appliquent).
- Ajouter ou supprimer des groupes d'opérateurs dans cette division.
- Affichez l'onglet **Configuration de l'opérateur** sur les propriétés d'un titulaire de carte pour les titulaires de carte de cette division, si l'opérateur dispose également du privilège "Afficher les titulaires de carte" dans cette division.
  Affichez et modifiez l'onglet **Configuration de l'opérateur** sur les propriétés d'un titulaire de carte pour les titulaires de carte de cette division, si l'opérateur dispose également du privilège "Modifier les titulaires de carte" dans cette division.

Modifier les définitions de données personnelles

Un opérateur disposant du privilège "Modifier les définitions de données personnelles" dans une division peut effectuer les opérations suivantes :

- Ajouter ou supprimer les champs Données personnelles.
- Afficher ou modifier les propriétés des définitions de champs de données personnelles dans cette division.

Modifier les descriptions de rapport

Un opérateur disposant du privilège "Modifier les descriptions de rapport" dans une division peut enregistrer ou supprimer tout type de description de rapport (à l'exception du rapport d'évacuation) dans le client de configuration, pour la division Description du rapport, mais uniquement si l'opérateur a également le privilège d'afficher les rapports.
Remarque : Cela s'applique à tous les rapports, à l'exception du rapport d'évacuation qui est contrôlé par le privilège "Modifier le rapport d'évacuation".

Modifier les définitions de rôle

Un opérateur disposant du privilège "Modifier les rôles" dans une division peut effectuer les opérations suivantes :

- Affichez et modifiez les propriétés des rôles dans cette division.
- Ajouter ou supprimer des rôles dans cette division.

Modifier les éléments Salto

Un opérateur disposant du privilège "Modifier les articles vendeur" dans une division peut effectuer les opérations suivantes :

- Supprimer ou modifier les noms, les descriptions et les relations de zone de porte de Salto Doors and Zones.
- Resynchronisez avec l'application Salto.

Remarque : Les noms, descriptions ou relations de zone de porte des chambres, des casiers ou des suites ne peuvent pas être supprimés ou modifiés. Ceux-ci ne sont modifiés que par le biais d'une resynchronisation, puis uniquement du côté de Salto.

Modifier les calendriers

Un opérateur disposant du privilège "Modifier les calendriers" dans une division peut effectuer les opérations suivantes :

- Affichez et modifiez les propriétés des planifications dans cette division.
- Ajouter ou supprimer des calendriers dans cette division.
- Dupliquer des calendriers.

Modifier le site

Un opérateur disposant du privilège "Modifier le site" dans la division racine peut modifier la liste des raisons de l'impression ou du codage d'une carte.

Un opérateur disposant du privilège "Modifier le site" dans une division peut effectuer les opérations suivantes :

- Créer et supprimer des postes de travail.
- Affichez l'afficheur d'état.
- Afficher les jeux d'icônes et modifier les icônes des éléments du centre de commande.
- Affichez et modifiez les propriétés de l'un des éléments suivants du Centre de commandes dans cette division (par exemple, vous pouvez utiliser l'option de menu contextuel **Propriétés** dans la fenêtre de liste principale appropriée).
- Ajoutez ou supprimez l'un des éléments suivants du Centre de commandes de cette division, à l'exception du serveur (vous pouvez utiliser les options de menu **contextuel** Nouveau ou Supprimer dans la fenêtre de liste principale appropriée).
- Consultez les visionneuses de site du client Command Center de cette division.
- Affichez les filtres et les compétences de notification, mais ne les créez pas.
- Utilisez le remplacement "Identifier le périphérique".

Contrôleurs matériels :
- Contrôleur 6000

Matériel - bus hôte :
- Lecteur HBUS
- Terminal HBUS
- Terminal d'alarmes HBUS uniquement
- Clôture HBUS F31/F32/F41/F42 Contrôleur
- Contrôleur de clôture HBUS F22
- Interface d'E/S HBUS
- Groupe de capteurs de tension HBUSZ10

Matériel - Capteur :
- Capteur de fil tendu D10
- Capteur de perturbation Z20

Matériel - **Aperio :**
- Aperio Door

Logiciel du périphérique :
- Logiciel de contrôleur
- Logiciel RIO
- Logiciel de personnalisation du contrôleur

Matériel - Autre :
- Entrée
- Sortie (virtuelle ou physique)
- Lecteur tiers (Tiers)
- Morpho Biometric Reader (troisième Lecteur de fête)
- Numéroteur d'alarme
- Ascenseur HLI
- Système DVR
- Caméra DVR

Autres éléments :
- Serveur **
- Station de travail
- Zone d'accès
- Zone d'alarme
- Porte
- Plan du site
- Voiture d'ascenseur
- Salto Server **
- Salto Access Zone
- Ascenseur Voiture HLI
- Intercom
- Système Intercom
- Groupe Interlock
- Système externe
- Élément système externe
- Bloc logique
- Salto Door
- Réceptions
- Émetteur d'alarme IP

** Cet élément NE PEUT PAS être ajouté ou supprimé avec le privilège "Modifier le site".

Un opérateur disposant du privilège "Modifier le site" dans une division peut afficher et modifier les propriétés de l'un des éléments Services et postes de travail suivants de cette division, ainsi que supprimer les éléments Services et postes de travail (**élément** Services et **postes de travail** > **Supprimer ou,** > **Propriétés)**.
- Service de contrôleur FT (FT Controller)
- Service FT Import-Export
- Service FT Bootstrap Protocol
- Service FT Intercom

Un opérateur disposant du privilège "Modifier le site" dans une division peut effectuer les opérations suivantes :

- Resynchronisez les bases de données entre le serveur et tout contrôleur de cette division.
- Resynchronisez les bases de données entre le serveur et n'importe quel Morpho Biometric Reader de cette division.
- Resynchronisez avec l'application Salto.
- Accepter un nouveau certificat pour un serveur distant.
- Créer une nouvelle voiture d'ascenseur dans cette division en dupliquant (ou copiant) les propriétés d'une autre voiture d'ascenseur (à laquelle l'opérateur a également le privilège "Modifier le site").
- Créez un nouveau système externe dans cette division en dupliquant (ou en copiant) les propriétés d'un autre système externe (auquel l'opérateur a également le privilège "Modifier le site").
- Créez un nouvel élément de système externe dans cette division en dupliquant (ou en copiant) les propriétés d'un autre élément de système externe (auquel l'opérateur a également le privilège "Modifier le site").

Un opérateur disposant du privilège "Modifier le site" dans une division peut transmettre la configuration de cet élément au contrôleur qui héberge l'élément pour l'un des éléments suivants du Centre de commandes dans cette division (l'option de menu contextuel est l'**élément Centre de commandes** > **Envoyer la configuration**).

Contrôleur 6000	Lecteur HBUS	Terminal HBUS	Terminal d'alarmes HBUS uniquement
HBUS F31/F32/F41/F42 Contrôleur de clôture	Contrôleur de clôture HBUS F22	Ascenseur HLI	Ascenseur voiture HLI
Voiture d'ascenseur	Porte	Groupe Interlock	Entrée
Sortie	Système externe	Élément système externe	Système DVR
Caméra DVR	Zone de clôture	Zone d'accès	Zone d'alarme
Numéroteur d'alarme	Lecteur Cardax IV	Interface d'E/S HBUS	Lecteur tiers (Tiers)

Rapport de configuration du site :
Un opérateur disposant du privilège "Modifier le site" dans une division peut ajouter, supprimer, générer, afficher et modifier les propriétés d'une description de rapport de configuration de site dans cette division. Lors de l'exécution, le rapport de configuration

de site ne signale que les propriétés des éléments du centre de commande pour lesquels l'opérateur dispose du privilège "Affichage".

Rapport Contact ID : Un opérateur disposant du privilège "Modifier le site" dans une division peut ajouter, supprimer, générer, afficher et modifier les propriétés d'une description de rapport Contact ID dans cette division. Le rapport Contact Id inclut uniquement les éléments du Centre de commandes auxquels l'opérateur a le privilège "Afficher".

Rapport d'accès: Un opérateur disposant du privilège "Modifier le site" dans une division peut ajouter, supprimer, générer, afficher et modifier les propriétés d'une description de rapport d'accès (Résumé ou Détaillé) dans cette division. Les règles ci-après s'appliquent :

- Lorsque l'état d'accès est exécuté, il ne fait état que des zones d'accès ou des zones d'accès Salto auxquelles l'opérateur a le privilège "Afficher le site".
- Si une porte plutôt qu'une zone d'accès est configurée dans la description de l'état, la zone d'accès à laquelle la porte fournit une entrée est la zone d'accès effective sur laquelle est généré l'état. Il n'en va pas de même pour Salto Doors, car celles-ci peuvent être signalées directement.

Rapport détaillé d'accès :
Si l'opérateur a le privilège d'afficher les propriétés d'une zone d'accès, d'une zone d'accès Salto ou d'une porte Salto incluses dans l'état, tous les détenteurs de carte qui ont accès à cet élément (leur nom uniquement) à l'heure configurée dans la description de l'état (ou pour la catégorie de jour configurée) seront affichés dans l'état d'accès détaillé. Cela s'applique indépendamment des privilèges de l'opérateur, ou de l'absence de ceux-ci, à ce détenteur de carte.

Le contenu d'un fichier PDF n'est affiché dans le rapport d'accès détaillé, pour chaque titulaire de carte, que si l'opérateur a le privilège de consulter le contenu de ce fichier PDF pour ce titulaire de carte.

Le numéro de carte du titulaire de carte n'est affiché dans le rapport d'accès détaillé que si l'opérateur dispose du privilège "Afficher le titulaire de carte" pour ce titulaire de carte.

Rapport d'accès de synthèse : Lors de l'exécution de l'état d'accès récapitulatif, il affiche les noms des groupes d'accès, ainsi que d'autres informations sur ce groupe d'accès, pour tous les groupes d'accès qui fournissent l'accès à cet élément au moment configuré dans la description de l'état (ou pour la catégorie de jour configurée). Cela s'applique indépendamment des privilèges de l'opérateur, ou de leur absence, à ces groupes d'accès.

Rapport de tension de clôture : Un opérateur disposant du privilège "Modifier le site" dans une division peut ajouter, supprimer, générer, afficher et modifier les propriétés d'une description de rapport de tension de clôture dans cette division. Le rapport de tension de clôture ne doit inclure que les éléments du Centre de commandes auxquels l'opérateur a le privilège "Affichage".

Modifier les visites

Un opérateur disposant du privilège "Modifier les visites" peut effectuer les opérations suivantes dans le système de gestion des visiteurs :

- Créer et modifier des visites, y compris ajouter et supprimer des visiteurs de la visite.

- Effectuez l'une des actions, toutes mettant à jour le statut du visiteur pour la visite et conservant un enregistrement des actions effectuées.
- Pour envoyer une notification d'arrivée ou générale.

Activer/désactiver l'opérateur

Un opérateur avec le privilège "Activer/désactiver l'opérateur" dans une division peut activer et désactiver l'ouverture de session du centre de commandes pour les opérateurs via :

- l'onglet **Configuration de l'opérateur** des propriétés Titulaire de carte dans le client de configuration, OU
- Cliquez sur le bouton Détails de connexion sur la vignette Groupes d'opérateurs de cartes de visionneuse de détenteurs de cartes dans le client Command Center.

Gérer les clés

Un opérateur disposant du privilège "Gérer les clés" dans la division racine peut effectuer les opérations suivantes :

- Modifier/importer/exporter les clés du site
- Démarrer/arrêter la migration
- Encoder les cartes d'administration
- Changer/importer/exporter clés de type biométrique Morpho
- Modifier le jeu de clés Salto et configurer le remplacement du chiffrement

Les opérations ci-dessus ne seront pas disponibles pour tout opérateur qui n'a pas le privilège "Gérer les clés" ou l'équivalent, (i.e. "Utilisateur avancé" dans la même division ou opérateur de système).

Gérer les affectations du casier

Un opérateur disposant du privilège "Gérer les affectations de casiers" dans une division peut affecter (allouer), modifier et/ou supprimer manuellement des casiers des titulaires de carte.
Remarque : Il n'inclut toutefois pas le privilège "Afficher le détenteur de la carte". Le privilège "Afficher le détenteur de carte" n'est pas requis pour afficher les affectations de casier existantes dans la visionneuse du casier.

Gérer les paramètres de conservation des données

Un opérateur disposant du privilège « Gérer les paramètres de conservation des données » peut gérer les paramètres liés à la politique de conservation des données et à la rédaction des informations personnelles identifiables du titulaire de la carte.

Modifier l'appartenance au groupe d'opérateurs

Un opérateur avec le privilège "Modifier l'appartenance au groupe d'opérateurs" (mais sans le privilège "Modifier les opérateurs") pourra ajouter et supprimer des détenteurs de cartes de groupes d'opérateurs, mais ne pourra pas modifier le groupe d'opérateurs de toute autre manière.

Planifier la zone d'accès

Un opérateur disposant du privilège "Zone d'accès de planification" dans une division peut modifier une planification dans une zone d'accès en une autre qui a déjà été créée.

Sélectionner la vue système

Un opérateur disposant du privilège "Sélectionner la vue système" au sein d'une division peut restreindre sa vue système au sein du Centre de commande à un ou plusieurs des groupes d'opérateurs auxquels ils appartiennent.
Cela rend la boîte de dialogue de sélection **de la vue système** disponible pour eux.

Afficher la configuration des alarmes

Un opérateur disposant du privilège "Afficher la configuration d'alarme" dans une division peut effectuer les opérations suivantes :

- Affichez les propriétés des plans d'action de cette division.
- Affichez les propriétés des balises d'insertion dans cette division.
- Affichez les propriétés des instructions d'alarme de cette division.

Afficher les casiers

Un opérateur disposant du privilège "Afficher les casiers et les affectations" dans une division peut afficher les casiers, les casiers et les affectations de casiers.

Afficher les opérateurs

Un opérateur disposant du privilège "Afficher les opérateurs" dans une division peut effectuer les opérations suivantes :

- Afficher tous les privilèges d'opérateur et description.
- Affichez les propriétés des groupes d'opérateurs de cette division.
- Affichez l'onglet Configuration de l'opérateur sur les propriétés d'un titulaire de carte pour les titulaires de carte dans cette division, mais uniquement si l'opérateur a également le privilège "Afficher les titulaires de carte" ou "Modifier les titulaires de carte" dans cette division.

Afficher les définitions de données personnelles

Un opérateur disposant du privilège "Afficher les définitions de données personnelles" dans une division peut afficher les propriétés des champs de données personnelles dans cette division.

Afficher les programmes

Un opérateur disposant du privilège "Afficher les plannings" dans une division peut afficher les propriétés des plannings dans cette division.

Afficher le site

Un opérateur disposant du privilège "Visualiser le site" dans une division peut afficher les propriétés de l'un des éléments suivants du centre de commande de cette division (c'est-à-dire utiliser l'option de menu contextuel **Propriétés** pour l'élément du centre de commande approprié).

Contrôleurs matériels :
- Contrôleur 6000

Matériel - bus hôte :
- Lecteur HBUS
- Terminal HBUS

Autres éléments : (ces éléments ont été modifiés avec les options "Configurer le site", "Modifier les jeux d'icônes" ou "Modifier les macros")
- Archive

- Terminal d'alarmes HBUS uniquement
- Clôture HBUS F31/F32/F41/F42 Contrôleur
- Contrôleur de clôture HBUS F22
- Interface d'E/S HBUS
- Groupe de capteurs de tension HBUS Z10

Matériel-Capteur :
- Capteur de fil tendu D10
- Capteur de perturbation Z20

Matériel - **Aperio:**
- Aperio Door

Matériel - Autre :
- Entrée
- Sortie (virtuelle ou physique)
- Lecteur tiers (Tiers)
- Lecteur biométrique Morpho (Lecteur Tiers)
- Numéroteur d'alarme
- Ascenseur HLI
- Système DVR
- Caméra DVR

Autres éléments : (ces éléments ont été modifiés avec "Modifier le site")
- Serveur **
- Station de travail
- Zone d'accès
- Zone d'alarme
- Porte
- Plan du site
- Voiture d'ascenseur
- Ascenseur Voiture HLI
- Intercom
- Réceptions
- Groupe Interlock
- Système externe
- Élément système externe
- Contrôleur de clôture
- Zone de clôture
- Salto Server **
- Salto Door
- Salto Access Zone
- Compétences
- Calendrier
- Calendrier spécial
- Type de carte
- Jour *
- Division
- Formats universels de cartes
- Filtres de notification
- Macro
- Jeux d'icônes *

* Cet élément est sans division, donc avoir "Voir le site" dans n'importe quelle division permet à un opérateur de voir les propriétés de cet élément.

** Cet élément NE PEUT PAS être ajouté ou supprimé avec le privilège "Modifier le site".

Un opérateur disposant du privilège "Visualiser le site" dans une division peut afficher les propriétés de n'importe quel des éléments suivants du logiciel périphérique, dans cette division.
- Service de contrôleur FT (FT Controller)
- Service FT Import-Export
- Service FT Bootstrap Protocol
- Service FT Intercom
- Serveur distant

Un opérateur disposant du privilège "Visualiser le site" dans une division peut voir les visionneuses de site du client du centre de commande de cette division.

Rapports : Un opérateur disposant du privilège "Visualiser le site" dans une division peut ajouter, supprimer, générer, afficher et modifier les propriétés d'une description de rapport de configuration de site dans cette division. Lors de l'exécution, le rapport

de configuration de site ne signale que les propriétés des éléments du centre de commande pour lesquels l'opérateur dispose du privilège "Affichage".

Un opérateur disposant du privilège "Afficher le site" dans une division peut ajouter, supprimer, générer, afficher et modifier les propriétés d'une description de rapport Contact ID dans cette division. Le rapport Contact ID inclut uniquement les éléments du Centre de commandes auxquels l'opérateur a le privilège "Afficher".

Un opérateur disposant du privilège "Visualiser le site" dans une division peut ajouter, supprimer, générer, afficher et modifier les propriétés d'une description de rapport d'accès (Résumé ou Détaillé) dans cette division. Les règles suivantes s'appliquent :

- Lorsque l'état d'accès est exécuté, il ne fait état que des zones d'accès ou des zones d'accès Salto auxquelles l'opérateur a le privilège d'afficher les propriétés de la zone d'accès.
- Si une porte plutôt qu'une zone d'accès est configurée dans la description de l'état, la zone d'accès à laquelle la porte fournit une entrée est la zone d'accès effective sur laquelle est généré l'état. Il n'en va pas de même pour Salto Doors, car celles-ci peuvent être signalées directement.

Rapport détaillé d'accès : Si l'opérateur a le privilège d'afficher les propriétés d'une zone d'accès, d'une zone d'accès Salto ou d'une porte Salto incluses dans l'état, tous les détenteurs de carte qui ont accès à cet élément (leur nom seulement) à l'heure configurée dans la description de l'état (ou pour la catégorie de jour configurée) seront affichés dans l'état d'accès détaillé. Cela s'applique indépendamment des privilèges de l'opérateur, ou de l'absence de ceux-ci, à ce détenteur de carte.

Le contenu d'un fichier PDF n'est affiché dans le rapport d'accès détaillé, pour chaque titulaire de carte, que si l'opérateur a le privilège de consulter le contenu de ce fichier PDF pour ce titulaire de carte.

Le numéro de carte du titulaire de carte n'est affiché dans le rapport d'accès détaillé que si l'opérateur a le privilège de voir le numéro de carte pour ce titulaire de carte.

Rapport d'accès de synthèse : Lors de l'exécution de l'état d'accès récapitulatif, il affiche les noms des groupes d'accès, ainsi que d'autres informations sur ce groupe d'accès, pour tous les groupes d'accès qui fournissent l'accès à cet élément au moment configuré dans la description de l'état (ou pour la catégorie de jour configurée). Cela s'applique indépendamment des privilèges de l'opérateur, ou de leur absence, à ces groupes d'accès.

Rapport de tension de clôture : Un opérateur disposant du privilège "Visualiser le site" dans une division peut ajouter, supprimer, générer, afficher et modifier les propriétés d'une description de rapport de tension de clôture dans cette division. Le rapport de tension de clôture ne doit inclure que les éléments du Centre de commandes auxquels l'opérateur a le privilège "Affichage".

Afficher les visites

Un opérateur disposant du privilège "Visite de la vue" peut effectuer les opérations suivantes dans le système de gestion des visiteurs :

- Afficher les visites pour une réception pour laquelle la réceptionniste ne dispose pas de droits de modification. Les gardes peuvent avoir accès en "vue".
- Imprimer les rapports de gestion des visiteurs (à l'exception du rapport d'évacuation).

Remarque : Ce privilège n'est pas requis si le privilège "Modifier les visites" est accordé.

Gérer

Gérer l'emplacement du titulaire de carte

L'option "Gérer l'emplacement du détenteur de carte" concerne les fonctionnalités suivantes du client Command Center :
- Évacuation mobile,
- Tableaux, et
- Action "Déplacer vers l'emplacement" depuis la visionneuse du détenteur de carte

- Pour déplacer un ou plusieurs titulaires de carte d'une zone d'accès à une autre zone, un opérateur doit disposer du privilège "Gérer l'emplacement du titulaire de carte" dans la division de la zone d'accès cible.
- Pour déplacer un titulaire de carte à l'extérieur du système, un opérateur doit disposer du privilège "Gérer l'emplacement du titulaire de carte" dans n'importe quelle division et l'option Autoriser le **déplacement des titulaires de carte à l'extérieur du système** doit également être activée sur l'onglet **Général** de la fenêtre de visualisation mobile Paramètres globaux.

Gérer Guard Tours

Un opérateur disposant du privilège "Gérer les visites de garde" dans une division peut effectuer les opérations suivantes :

- Remplacez par "Démarrer" ou "Arrêter" toute visite guidée dans cette division, dans le client de configuration.
- Affichez les propriétés de Guard Tours dans cette division, y compris la liste des points de contrôle qui sont configurés pour la visite, dans le client de configuration.
- Reportez-vous à une visite guidée dans l'outil de navigation lors de la configuration d'une vignette de visite guidée dans le client du Centre de commande. Seuls les circuits dans cette division où le privilège (ou un des autres privilèges qualifiants) est détenu seront disponibles.
- Consultez une division dans l'outil Parcourir lors de la configuration d'une mosaïque de visite de garde, dans le client du Centre de commande. Seules les divisions dans lesquelles le privilège (ou l'un des autres privilèges admissibles) est détenu seront disponibles.
- En mode opérationnel dans le client du centre de commande, pour afficher une visite guidée, sélectionnez la Garde, démarrez et arrêtez les visites guidées configurées (dans cette division) sur une vignette de visite guidée de la Garde.

Remarque : Des privilèges supplémentaires sont requis pour configurer les mosaïques dans le client Command Center.

Gérer les réceptions

Un opérateur disposant du privilège "Gérer les réceptions" dans une division peut effectuer les opérations suivantes :

- Déterminez si un utilisateur est un réceptionniste pour une réception particulière.
- Visualiser les données de type de carte qui sont utilisées pour valider une carte d'accès lors de l'attribution à un visiteur.

Gérer les attributs des visiteurs

Un Réceptionniste utilisant le système de gestion des visiteurs avec le privilège "Gérer les attributs des visiteurs" peut assigner une escorte à un titulaire de carte dans une division pour laquelle il n'a pas de privilèges "Modifier le titulaire de carte".

Disposition de plusieurs moniteurs

Un opérateur disposant du privilège "Disposition de plusieurs moniteurs" est une division qui peut déplacer des visionneuses entre des fenêtres existantes ou créer de nouvelles fenêtres de visionneuses dans le client Command Center.

Moniteur

Acquitter les alarmes

Un opérateur disposant du privilège "Accuser réception des alarmes" dans une division peut exécuter les actions suivantes sur une seule alarme :

- Reconnaître et modifier les propriétés des alarmes dont la source est un élément du Centre de commande au sein de cette division. Cela inclut l'ajout d'une note ou d'un commentaire à l'alarme.
- Afficher les événements et les alarmes dont la source est un élément du Centre de commande au sein de cette division.
- Affichez une séquence d'images dans cette division.
- Rafraîchir les alarmes d'un contrôleur dans cette division, mais uniquement avec le privilège "Voir le site" dans cette division.
- Ajoutez, supprimez, modifiez les propriétés ou exécutez une description de rapport d'activité ou d'exception dans cette division. Si l'état contient des éléments pour lesquels l'opérateur ne dispose pas du privilège "Afficher", ils sont exclus de l'état.
- Affichez les propriétés d'un rapport d'évacuation dans cette division ou exécutez une description de rapport d'évacuation dans cette division.

Ajuster les contrôles DVR PTZ

Un opérateur disposant du privilège "Ajuster les commandes DVR PTZ" dans une division peut modifier le panoramique, l'inclinaison ou le zoom (ou d'autres contrôles fournis par l'intégrateur DVR) d'une caméra DVR dans cette division, tout en regardant des séquences d'images en direct de cette caméra DVR.

Traiter des alarme en bloc

Un opérateur disposant du privilège "Bulk Process Alarms" dans une ou plusieurs divisions peut effectuer les opérations suivantes :

- Traitement en bloc de toutes les alarmes inactives au sein d'un groupe d'alarmes prioritaires. Cela traite toutes les alarmes, pas seulement celles de la division dans laquelle le privilège est détenu.
  Remarques :
  - Le privilège "Modifier les alarmes" dans une division est également nécessaire pour traiter en bloc les alarmes dont la source est un élément de cette division.
  - Pour les alarmes escaladées, l'opérateur doit également appartenir à un groupe d'opérateurs qui leur permet d'accuser réception ou de traiter les alarmes escaladées (configuré via les propriétés du groupe d'opérateurs, onglet Configuration).

Défi contrôlé

Un opérateur disposant du privilège "Défi contrôlé" peut ouvrir la visionneuse de défi en mode "Contrôlé" et accorder ou refuser l'accès aux détenteurs de cartes qui entrent par une porte de cette division. L'opérateur doit également avoir le privilège "Afficher les événements et les alarmes" dans la division de la porte, pour utiliser la visionneuse de défi et le privilège "Afficher la caméra numérique" s'il utilise des caméras DVR.

Modifier les alarmes

Un opérateur disposant du privilège "Modifier les alarmes" dans une division peut effectuer les opérations suivantes :

- Reconnaître, modifier les propriétés et traiter les alarmes dont la source est un élément du Centre de commande de cette division.
- Afficher les événements et les alarmes dont la source est un élément du Centre de commande au sein de cette division.
- Visualiser une séquence d'images dans cette division.
- Ajouter, supprimer, modifier les propriétés ou exécuter une description de rapport d'activité dans cette division. Si l'état contient des éléments pour lesquels l'opérateur n'a pas le privilège "Afficher", ils sont exclus de l'état.
- Ajouter, supprimer, modifier les propriétés ou exécuter une description de rapport d'exception dans cette division. Si l'état contient des éléments pour lesquels l'opérateur ne dispose pas du privilège "Afficher", ils sont exclus de l'état.
- Affichez les propriétés d'une description de rapport d'évacuation dans cette division ou exécutez une description de rapport d'évacuation dans cette division. **Remarque :** Il s'agit du seul état qui inclut toutes les zones d'accès configurées dans la description de l'état, quels que soient les privilèges de l'opérateur (générateur) (ou l'absence de ces privilèges) sur ces zones d'accès.
- "Traitement rapide" une alarme dont la source est un élément du Centre de commande au sein de cette division.

Modifier les alarmes en dessous de la haute priorité

Un opérateur disposant du privilège "Modifier les alarmes en dessous de la priorité élevée" ne peut reconnaître et traiter les alarmes que des priorités suivantes :
- Moyen-haut,
- Moyen,
- Moyennement bas,
- Faible, et
- Très faible

Forcer le processus

Un opérateur disposant du privilège "Forcer le processus" dans une division et des privilèges "Afficher le site" et "Modifier les alarmes" peut forcer le traitement des alarmes actives.

Lancer le client de configuration

Un opérateur disposant du privilège "Lancer le client de configuration" dans une ou plusieurs divisions peut exécuter les opérations suivantes :

- Connexion au client de configuration via CCFT.exe
- Reportez-vous au bouton **Configuration Client** de l'onglet Administration du client Command Center (Centre de commandes).
- Cliquez une fois sur le bouton **Configuration Client** pour lancer Configuration Client à partir de cette icône.

Enregistrer le flux DVR en direct

Un opérateur avec le privilège "Enregistrer le flux DVR en direct" dans une division peut enregistrer les séquences d'images DVR en direct, tout en les regardant depuis une caméra DVR dans cette division.

Utiliser Intercom

Un opérateur disposant du privilège "Utiliser l'interphone" dans une division peut effectuer les opérations suivantes :
Remarque : L'opérateur a également besoin de "View Site" dans la division Intercom, pour voir l'article Intercom Command Center, et de "View Events & Alarms" dans la division Intercom pour recevoir un appel de l'Intercom.

- Appelez un interphone de cette division.
- Répondez à un appel ou terminez un appel d'un interphone de cette division.
- Mettre un appel en attente ou transmettre un appel d'un interphone de cette division.

Afficher le défi

Un opérateur disposant du privilège "Afficher défi" dans une division peut effectuer les opérations suivantes :

- Ouvrez la visionneuse de défi en mode "Affichage seulement" et utilisez la visionneuse de défi pour toutes les portes de cette division.
- Affichez les propriétés de toutes les portes de cette division.
- L'opérateur doit également avoir le privilège "Afficher les événements et les alarmes" dans la division de la porte, pour utiliser la visionneuse de défi.

Afficher la caméra numérique

Un opérateur disposant du privilège "View Digital Camera" pour la division Caméra numérique ou Caméra DVR peut voir les propriétés de cette caméra.

Afficher les événements des titulaires de carte (API uniquement)

Ce privilège s'applique uniquement aux opérateurs utilisés en tant qu'opérateur client REST pour un élément client REST. Un opérateur client REST disposant du privilège « Afficher les événements des titulaires de carte (API uniquement) » peut afficher les événements des titulaires de carte (par exemple, l'accès à la porte accordé) via l'API REST. Cela peut permettre à un client REST de surveiller les mouvements des titulaires de carte sans pouvoir afficher les événements des non-titulaires de carte.

Afficher les événements et les alarmes

Un opérateur disposant du privilège "Afficher les événements et les alarmes" dans une division peut effectuer les opérations suivantes :

- Afficher les événements et les alarmes dont la source est un élément du Centre de commande au sein de cette division.
- Visualiser une séquence d'images dans cette division.
- Actualiser les alarmes d'un contrôleur (tous types) dans cette division, mais uniquement avec le privilège "Voir le site" dans cette division également.
- Ajouter, supprimer, modifier les propriétés ou exécuter une description de rapport d'activité dans cette division. Si l'état contient des éléments pour lesquels l'opérateur n'a pas le privilège "Afficher", ils sont exclus de l'état.
- Ajoutez, supprimez, affichez et modifiez les propriétés ou exécutez une description de rapport d'exception dans cette division. Si le rapport contient des alarmes dont la source est un élément du Centre de commande dans une division dans laquelle l'opérateur ne dispose pas du privilège "Afficher les événements et les alarmes", elles sont exclues du rapport.
- Affichez les propriétés d'un rapport d'évacuation dans cette division ou exécutez une description d'un rapport d'évacuation dans cette division.
- Voir les visionneuses d'alarme stockés dans cette division qui ont été configurés pour être utilisés dans le client Command Center.

Afficher les tour de gardes

Un opérateur disposant du privilège "Visualiser les tour de gardes" dans une division peut visualiser les propriétés des tours de garde dans cette division, y compris la liste des points de contrôle qui sont configurés pour le tour.

Contourner/Remplacer

Désactiver le routage de station de travail

Un opérateur disposant du privilège "Désactiver le routage de station de travail" dans une division peut effectuer les opérations suivantes dans le client du centre de commande :

- Déplacer tout élément de routage de poste de travail de cette division vers l'état "Désactivé", et
- Déplacer tout élément de routage de poste de travail de cette division de l'état "Désactivé" vers l'un des autres états.

Remplacement de la maintenance

Un opérateur disposant du privilège "Maintenance Override" dans une division peut effectuer les opérations suivantes :

- Remplacez par "Shunt", "Unshunt", "Isolate" ou "Dé-isolate" toute entrée dans cette division.
- Remplacez par "Shunt" ou "Unshunt" toute zone de clôture dans cette division (c'est-à-dire que la force de dissuasion est toujours active et répondra aux commandes, mais tous les événements d'alerte ou d'alarme sont ignorés).
- Remplacez par "On" ou "Off" toute zone de clôture dans cette division.
- Remplacez par "Haute tension" ou "Faible sensation" pour toute zone de clôture connectée à un contrôleur de clôture F31, F32, F41, F42 ou F22 dans cette division.
- Remplacez par "Mode Maintenance" ou "Mode d'essai de marche" tout groupe de capteurs de tension Z10 de cette division.
- Remplacez par les éléments spécifiques du centre de commande du matériel "Reset", "Shunt" ou "Unshunt"* dans cette division.
- Remplacez par les éléments matériels spécifiques** du centre de commande "Shunt" ou "Unshunt" dans cette division.
- Remplacez par "Réinitialiser", "Désactiver la communication", "Activer la communication", "Activer les connexions WWW" ou "Annuler le remplacement WWW" de tout contrôleur dans cette division.
- Remplacez par "Renew DHCP Settings", "Revalidate Certificate" Contrôleur 6000 dans cette division.
- Remplacez par "Utiliser l'Ethernet secondaire" ou "Annuler l'utilisation de l'Ethernet secondaire" Contrôleur 6000 uniquement (si le double Ethernet est activé).
- Remplacez par "Réinitialiser les clés du lecteur" pour les lecteurs Cardax IV, avec le privilège "Afficher le site" ou "Modifier le site" également.
- Remplacez tout bloc logique de cette division par "Activé", "Désactivé" ou "Réinitialiser la logique".
- Désactiver ou activer la communication avec un serveur distant.
- Réinitialiser la réplication avec un serveur distant.
- Annuler remplace ce privilège qui peut être établi.

L'opérateur doit pouvoir "afficher" les éléments qu'il souhaite remplacer afin de pouvoir accéder à l'**onglet** Statut **et Remplacements** sur la page des propriétés afin d'effectuer le remplacement/shunt.

* Remplacez par "Reset", "Shunt" ou "Unshunt" les éléments matériels suivants du centre de commande du matériel de cette division :

HBUS-8-Entrée Module de porte	HBUS - Carte 8Po	HBUS 4 Entrées 4 Sorties Conseil	HBUS 16Po 16 Po Conseil
Terminal HBUS	Terminal d'alarmes HBUS uniquement	Contrôleur de clôture HBUS F22	HBUS F31/F32/F41/F42 Contrôleur de clôture

** Remplacer par "Shunt" ou "Unshunt" les éléments suivants du centre de commande dans cette division :

Groupe de capteurs de tension Z10	Ascenseur HLI

Remplacer

Un opérateur disposant du privilège "Remplacer" dans une division peut effectuer les opérations suivantes :

- Remplacer l'état de la zone d'accès pour une durée spécifiée ou jusqu'à la prochaine modification programmée ou jusqu'à ce que le remplacement soit annulé, pour toute zone d'accès de cette division pour l'un des douze états de zone d'accès possibles.
- Pardonnez aux titulaires de carte de cette division (à qui ils ont également le privilège "Afficher le titulaire de la carte", ou tout autre privilège supérieur qui leur permet de voir les propriétés du titulaire de la carte) les violations de protection contre les droits de retour, pour toute zone d'accès dans cette division.
- Pardonnez à tous les détenteurs de carte les violations anti-passback pour toute zone d'accès dans cette division.
- Effectuez un verrouillage ou annulez un verrouillage sur une zone d'accès de cette division.
- Remplacez le nombre de zones pour toute zone d'accès de cette division.
- Remplacer une sortie (par "On", "Off" ou "Pulse") pour une durée spécifiée ou jusqu'à la prochaine modification programmée, pour toute sortie dans cette division.
- Remplacer l'état d'une zone d'alarme (par "Armé", "Désarmé", "Utilisateur1" ou "Utilisateur2"), pour toute zone d'alarme de cette division.
- Remplacer un groupe Interlock dans cette division ("Activer" ou "Désactiver" le groupe Interlock).
- Remplacez une voiture d’ascenseur.
- Annuler les remplacements avec état qui peuvent être établis avec ce privilège. **Remarque :** Si un remplacement ne peut pas être annulé (shunt ou unshunt) est sélectionné, alors il n'est pas possible pour l'utilisateur d'annuler le remplacement.

Ce privilège permet également à un opérateur d'afficher tous les éléments qu'il peut remplacer avec ce privilège (à l'exception des détenteurs de carte).

Remplacer la priorité supérieure à moyenne

Le privilège "Remplacer par une priorité moyenne" autorise le même jeu de privilèges que le privilège "Remplacer" (voir ci-dessus), mais l'opérateur ne peut remplacer que les alarmes actives jusqu'à (et y compris) "Priorité moyenne" (tant que cela ne provoque pas d'alarmes).

Remplacer - Ouvrir la porte

Un opérateur avec le privilège "Override Open Door" dans une division peut déverrouiller une porte verrouillée pour un court temps, pour n'importe quelle porte de contrôleur dans cette division.

Remplacer - Ouvrir le casier

Un opérateur disposant du privilège "Remplacer - Ouvrir le casier" dans une division peut ouvrir et/ou isoler les casiers.

Remplacer l'état de la carte

Un opérateur disposant du privilège "Remplacer le statut de la carte" dans une division peut effectuer les opérations suivantes :

- Modifiez l'état d'une carte qui est en état de désactivation permanente.
- Autoriser la création d'une carte avec les mêmes détails (numéro de carte, code de fonction, niveau de problème) qu'une carte qui est dans un état "Volé" ou dans un autre état Permanently Disabled.

Exécuter les macros

Un opérateur disposant du privilège "Exécuter les macros" dans une division peut effectuer les opérations suivantes :

- Affichez les propriétés des macros de cette division.
- Exécutez une macro dans cette division.

Planifier & exécuter des macros

Un opérateur disposant du privilège "Planifier et exécuter des macros" dans une division peut effectuer les opérations suivantes :

- Affichez les propriétés des macros de cette division.
- Modifier les heures d'exécution planifiées pour une macro de cette division (ajouter ou supprimer des heures d'exécution planifiées).
- Exécutez une macro dans cette division.

Envoyer une notification de diffusion

Lorsqu'il est ajouté à une visionneuses, un opérateur disposant du privilège "Envoyer une notification de diffusion" peut afficher, modifier avant d'envoyer et d'envoyer le même message électronique ou SMS (service de messages courts) à de nombreux titulaires de carte à la fois dans le client Command Center.

Utiliser le routage de station de travail

Un opérateur disposant du privilège "Utiliser le routage de station de travail" dans une division peut déplacer n'importe quel élément de routage de station de travail de cette division entre les états non désactivés, dans le client du centre de commande.

Système

Utilisateur avancé

Un opérateur disposant du privilège "Utilisateur avancé" au sein d'une division possède tous les privilèges au sein de cette division, à l'exception du privilège "Défi contrôlé". Cela inclut le privilège "Sélectionner la vue système", qui s'applique à l'échelle du système plutôt qu'à une division spécifique.

Un opérateur avec le privilège "Utilisateur avancé" dans une ou plusieurs divisions peut également :

- Traiter les alarmes actives (soit individuellement, soit via un processus en bloc).
  Remarque : L'option "Forcer le traitement de toutes" traite toutes les alarmes actives et inactives qui font partie du groupe de priorités des alarmes et dont la source est un élément d'une division dans laquelle le privilège "Utilisateur avancé" est détenu. Il traite également toutes les alarmes inactives du groupe de priorités d'alarme dont la source est un élément d'une division dans laquelle le privilège "Modifier l'alarme" est détenu.
- Configurez les événements et/ou les séquences d'images à détecter à partir de la base de données des événements au lieu d'être archivés. Une fois configurés, les événements et/ou les séquences d'images sont supprimés au lieu d'être archivés lorsque l'archive est exécutée par un opérateur.
- Affichez et modifiez le contenu de tous les fichiers PDF pour tous les détenteurs de cartes de cette division (c'est-à-dire que l'opérateur n'est pas limité par les privilèges PDF normaux définis dans la définition de PDF ou dans les groupes d'opérateurs auxquels ils appartiennent).
- Exécutez les Assistants Quickstart.
- Créez des serveurs distants et effectuez des remplacements "Accepter le certificat" des serveurs distants.

Sauvegarde et archivage

Un opérateur disposant du privilège "Sauvegarde et archivage" dans une division peut effectuer les opérations suivantes :

- Afficher les propriétés d'une archive de cette division.
- Démarrer (exécuter) une archive ou arrêter une archive en cours d'exécution, au sein de cette division.
  Remarque : La division Archive contrôle les opérateurs qui peuvent voir l'archive, et démarrer ou arrêter l'exécution de l'archive. Il ne contrôle pas les événements qu'il contient. Chaque Archive archive toujours tous les événements de toutes les divisions.
- Configurer et exécuter une sauvegarde.

Chapitre 38 : Modifications en bloc

Présentation des modifications en bloc

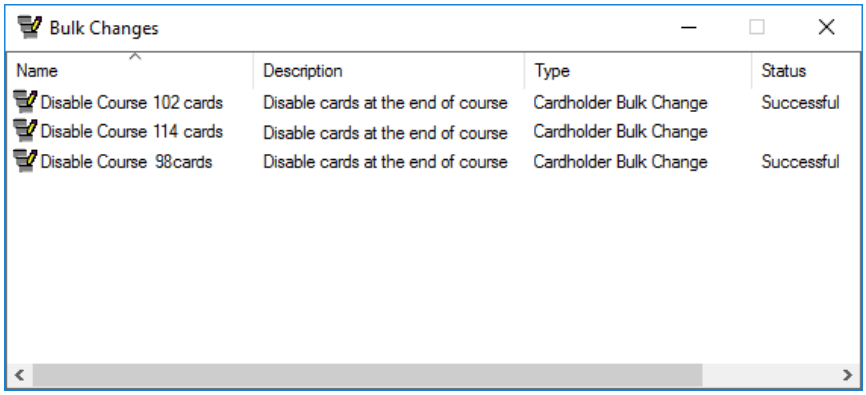
La fonction de modifications en bloc fournit une méthode automatisée de modification d'un ensemble commun de propriétés sur un groupe d'éléments dans le Centre de commandes. Il est possible de planifier l'exécution des modifications en masse à des moments précis. Ceci est réalisé à l'aide de la fonctionnalité Macro. Voir ***Macros*** (page 20-1) pour plus de détails.

Une seule modification en bloc peut être exécutée à la fois. Si un opérateur tente de démarrer une modification en bloc alors qu'il en existe déjà une en cours d'exécution, la seconde sera mise en file d'attente et exécutée une fois la première terminée. De même, si des modifications en bloc sont programmées pour s'exécuter (via des macros), elles seront mises en file d'attente et exécutées dans l'ordre planifié, avec une seule exécution à la fois.

IMPORTANT:
Comme les autorisations ne seront pas vérifiées avant l'exécution d'une modification en bloc, un opérateur disposant du privilège d'opérateur "Modification en bloc" pourra voir toutes les données contenues dans une modification en bloc qui a été enregistrée. Même s'ils n'ont pas le privilège d'afficher les données autrement, ils seront en mesure de le voir dans le changement en bloc.
Par exemple:
Une modification en bloc peut contenir un certain nombre de détenteurs de cartes ou de groupes d'accès auxquels l'éditeur de modifications en bloc n'a pas accès. Cependant, dans le changement en bloc, ils pourront voir cette information.

Fenêtre Liste principale des modifications en masse

La **fenêtre Modifications en** masse de la liste s'ouvre en mode grille.



Toutes les modifications en bloc enregistrées sont répertoriées dans cette fenêtre. Pour chaque modification en bloc, l'opérateur qui l'a modifiée pour la dernière fois, la date et l'heure de la dernière modification et l'état de la modification en bloc sont indiqués. Si une modification en bloc a été enregistrée mais non exécutée, l'état sera vide. Un changement en masse qui a été achevé avec succès reste sur le statut "Réussi" jusqu'à la prochaine fois qu'il est édité, auquel moment il reviendra à vide.

Statut	Modification en bloc...
Blank	n'a pas de statut. La modification en bloc n'a pas été exécutée ou a été redéfinie/enregistrée depuis la dernière exécution.
Actif	est en cours d'exécution. **Remarque :** Les modifications en bloc sont exécutées deux fois pour vérifier si les éléments qui étaient verrouillés lors de la première exécution sont maintenant déverrouillés.
L'annulation	est inactive, ayant été arrêtée en raison de l'annulation de l'opération par un opérateur.
La file d'attente	est en attente d'une autre modification en bloc en cours d'exécution, à terminer.
Réussite	est inactif, ayant accompli 100 % de réussite.
Échec	est inactif, ayant terminé avec moins de 100 % de réussite.
Échec — Interruption du serveur	a échoué en raison d'une défaillance du serveur alors que la modification en bloc est active ou en file d'attente.

Remarque : Les modifications en masse enregistrées peuvent être ajoutées à l'afficheur d'état.

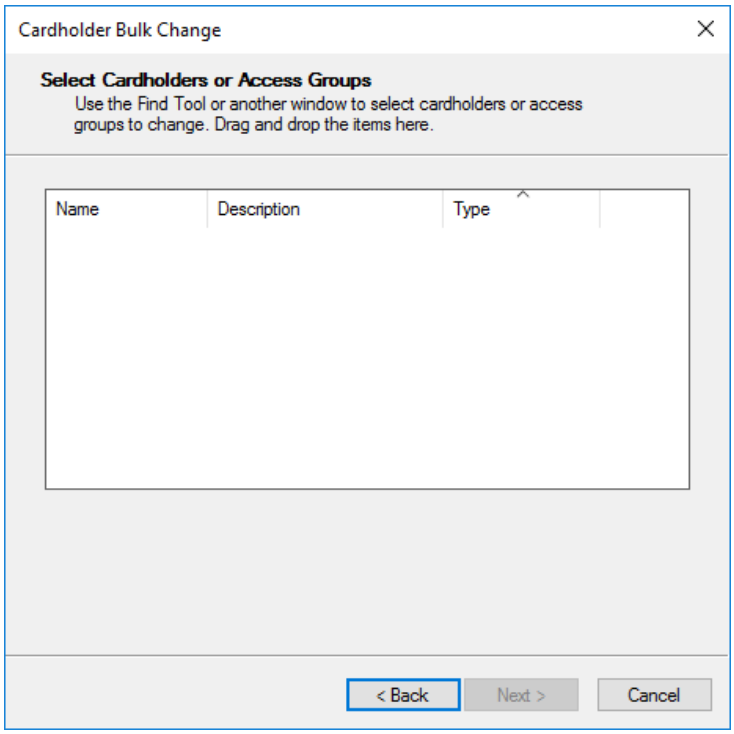
Lancement d'une modification en bloc de titulaire de carte

Introduction

Cette procédure décrit comment initier un nouveau changement de titulaire de carte en bloc dans le Centre de commande. Pour exécuter cette procédure, l'opérateur doit disposer des privilèges d'opérateur "Bulk Change" et "Edit Titulaire de cartes". En outre, l'exploitant a besoin de privilèges divisionnaires et autres suffisants pour effectuer chaque changement individuel énuméré dans un changement global.

Procédure

1. Cliquez sur **Gérer** dans la barre de menus, puis sur **Modifications en bloc.**
   La fenêtre Liste principale **des** modifications en **masse** s'affiche.
2. **Cliquez avec le bouton droit** de la souris **et sélectionnez...Titulaire de carte Bulk Change**.
   L'écran "Sélectionner les titulaires de carte ou les groupes d'accès" de l'Assistant de modification en bloc des titulaires de carte s'affiche.



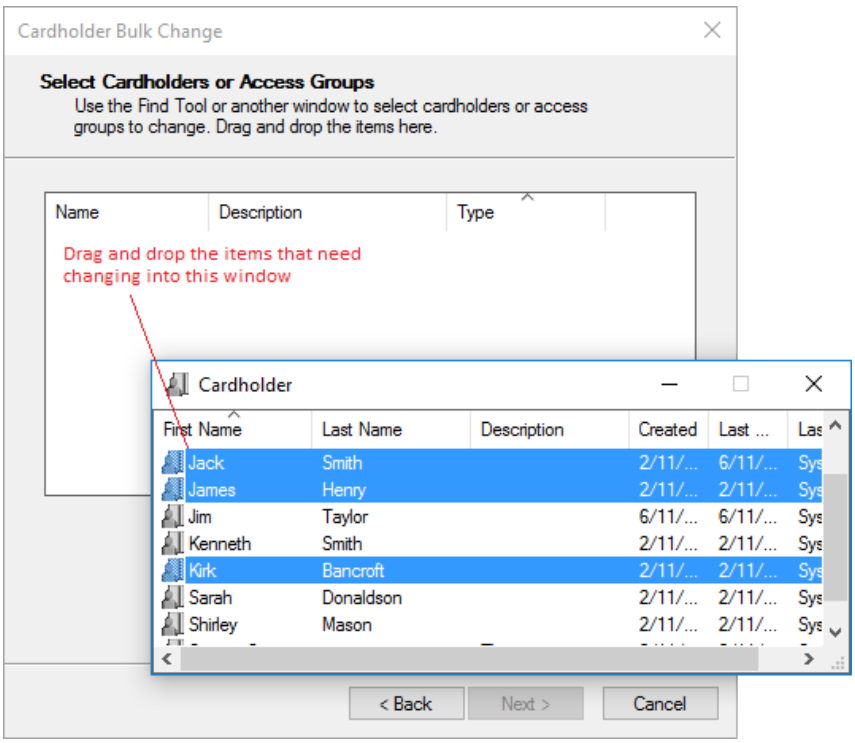
Tous les détenteurs de cartes ou groupes d'accès qui nécessitent une modification doivent être placés sur cet écran, en les faisant glisser et en les déposant de la fenêtre Liste principale des **détenteurs de cartes** ou de la fenêtre Liste principale des **groupes d'accès**, selon le cas, ou de l'outil de recherche. Dans cette procédure, la fenêtre de la liste principale des **titulaires de carte** a été utilisée.

Remarques :

- Vous pouvez sélectionner des titulaires de carte individuels ou un groupe d'accès si tous les titulaires appartenant au groupe doivent être modifiés.

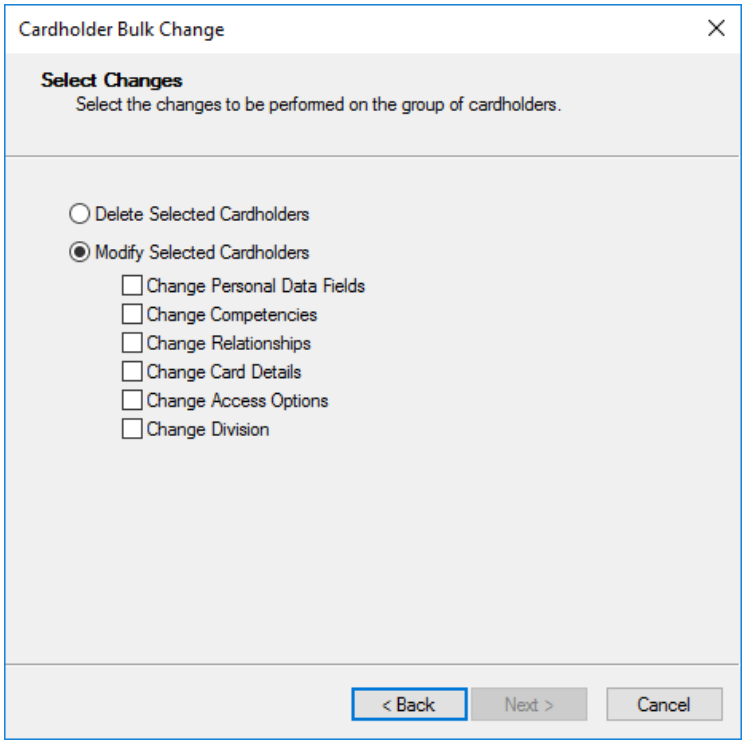
- Si une modification en bloc de division est créée et qu'un groupe d'accès est déplacé pour être modifié, seule la division du groupe d'accès est modifiée. Pour modifier les détenteurs de cartes dans la division, faites glisser le groupe d'accès dans un changement en bloc de détenteurs de cartes et modifiez la division, ou faites glisser les détenteurs de cartes individuellement dans le changement de division.

3. Cliquez sur **Gérer** dans la barre de menus, puis sur **Titulaires de carte**.
   La fenêtre Liste principale des titulaires de carte s'ouvre.
   Sélectionnez les détenteurs de carte à modifier, puis faites-les glisser dans cet écran de l'assistant.



4. Fermez la fenêtre Liste principale des **détenteurs de** carte.

5. Cliquez sur le bouton **Suivant**.
   L'écran "Sélectionner les modifications" de l'Assistant Modifications en bloc des titulaires de carte s'affiche.



6. Cliquez sur la case d'option correspondant à l'option souhaitée (par exemple, **Supprimer les titulaires de carte sélectionnés** ou **Modifier les titulaires de carte sélectionnés**). Seule une de ces options peut être sélectionnée.

7. Si l'option **Modifier les titulaires de carte sélectionnés** est sélectionnée, cochez les cases des éléments que vous souhaitez modifier.
   Vous pouvez sélectionner une ou plusieurs de ces options.
   Remarque : Si votre site possède une licence à la fois pour la gestion des visiteurs et les notifications, une case à cocher **Modifier les notifications de gestion des visiteurs** sera également disponible.

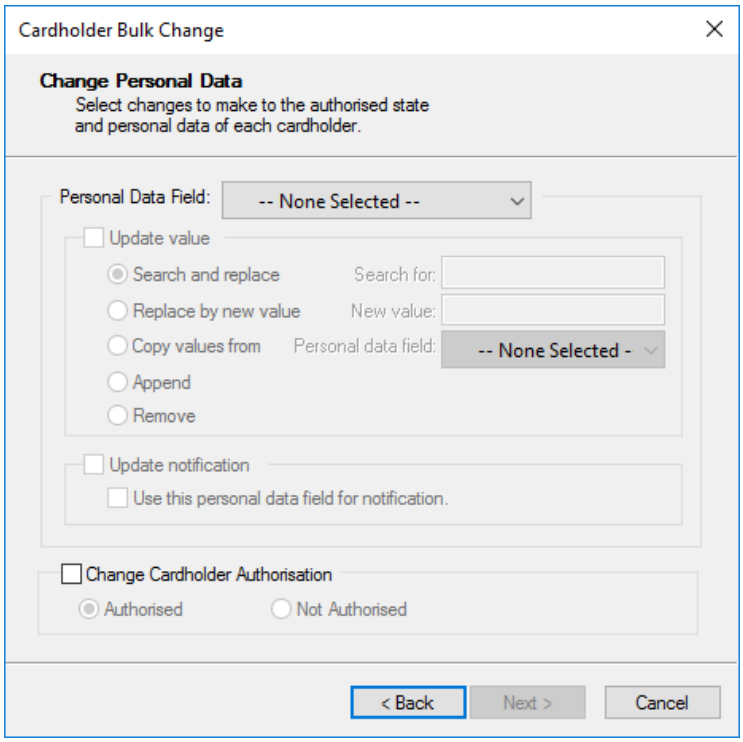
   L'écran qui s'affiche ensuite dépend des sélections effectuées sur l'écran "Sélectionner les modifications".

Si vous avez cliqué sur...	alors...
Supprimer les titulaires sélectionnés	cliquez sur le bouton **Suivant** et passez à l'étape 31.
Modifier les titulaires de carte sélectionnés	allez à l'étape 8.

8. Cliquez sur le bouton **Suivant**.
   Les écrans individuels s'affichent pour chacun des éléments que vous avez cochés pour les modifier.

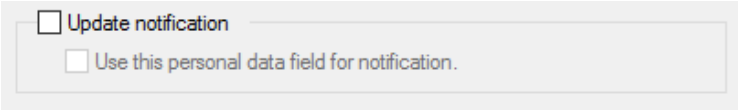
   Remarque : Si vous avez coché la case Modifier les compétences, consultez ***Modifications en masse des compétences*** (page 53-28) pour plus de détails.
   Si vous avez coché la case Modifier les relations, reportez-vous à la section Affectation de ***titulaires de carte à des rôles via la modification en bloc*** (page 35-19) pour plus de détails.

9. L'écran "Modifier les données personnelles" ne s'affiche que si la case à cocher **Modifier les champs de données personnelles** a été cochée sur l'écran "Sélectionner les modifications". Sinon, passez à l'étape 14.
   Cet écran vous permet de sélectionner les modifications à apporter à l'état autorisé et aux données personnelles de chaque détenteur de carte.



10. Si vous souhaitez apporter des modifications aux données personnelles, sélectionnez le champ Données personnelles (PDF) dans la liste déroulante. Les autres options de la section Champ de données personnelles de cet écran sont activées.
    Remarques :

    - Ce champ de données personnelles est le PDF cible.
    - Les images PDF et les fichiers PDF uniques ne peuvent pas être modifiés en bloc. Par conséquent, ces types de PDF n'apparaissent pas dans la liste déroulante.
    - Si le PDF est un PDF de type "Email" ou "Mobile", une case à cocher **Mettre à jour la notification** devient disponible, ainsi qu'une **case à cocher Utiliser ce champ de données personnelles pour la notification**.

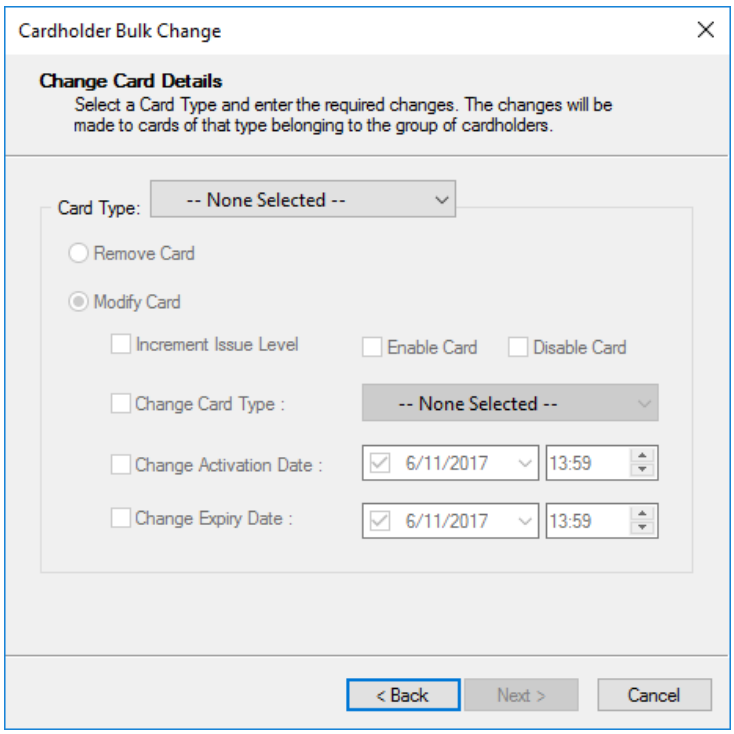
      Ces cases à cocher peuvent être activées en conjonction avec l'un des boutons radio de la section **Mettre à jour** la **valeur** ci-dessus, à l'exception du bouton d'option **Supprimer**.

11. Cliquez sur le bouton d'option du type de modification que vous souhaitez apporter.

Bouton/Champ	Description
Rechercher et remplacer	Lorsque vous cliquez dessus, les champs **Rechercher** et **Nouvelle valeur** sont activés pour vous permettre de remplacer une valeur sélectionnée par une nouvelle.
Remplacer par nouvelle valeur	Lorsque vous cliquez dessus, le champ **Nouvelle valeur** est activé, ce qui vous permet de remplacer une valeur.
Copier les valeurs de	Lorsque vous cliquez dessus, la liste déroulante **Champ de données personnelles** située à côté est activée, ce qui vous permet de remplacer les données PDF cibles par les données existantes dans le PDF source.
Ajouter	Lorsque vous cliquez sur ce bouton, le champ **Nouvelle valeur** est activé, ce qui vous permet d'ajouter une nouvelle valeur aux données existantes. **Remarque :** Si le champ de données personnelles sélectionné est un fichier PDF "Numérique", "Texte - liste" ou "Date", ce champ ne sera pas activé car il n'est pas possible d'ajouter ces types de fichiers PDF.
Supprimer	Lorsque vous cliquez dessus, aucun champ supplémentaire n'est activé, mais cela vous permet de supprimer des données. **Remarque :** Si le PDF est requis pour avoir des données (c'est-à-dire qu'il est obligatoire), l'option Supprimer ne sera pas disponible.
Recherche de	Le texte à rechercher est entré (limité à 200 caractères) et remplacé par ce qui est entré dans le champ Nouvelle valeur où qu'il figure dans le fichier PDF des détenteurs de cartes sélectionnés. **Remarques :** • Si le champ de données personnelles sélectionné est un PDF "Texte -liste", le champ **Rechercher** devient une liste déroulante contenant les chaînes de texte facultatives disponibles. • " Pour les PDF "Date", la **recherche de** modifications de champ pour un contrôle Date/Heure et une case à cocher est incluse pour représenter "aucune valeur", mais seulement pour les PDF non requis.
Nouvelle valeur	Entrez une nouvelle valeur (limitée à 200 caractères) pour le PDF. Ceci est vérifié pour s'assurer qu'il contient des données valides. **Remarques :** • Si le champ de données personnelles sélectionné est un fichier PDF "Texte -liste", le champ **Nouvelle valeur** devient une liste déroulante contenant les chaînes de texte facultatives disponibles. • Pour les PDF "Date", le champ **Nouvelle valeur** change en un contrôle Date/Heure et une case à cocher est incluse pour représenter "aucune valeur", mais uniquement pour les PDF non requis.

Bouton/Champ	Description
Champ de données personnelles (source)	Voici le PDF source. Lorsque vous sélectionnez l'option **Copier les valeurs de**, les données de ce fichier PDF source seront "copiées" vers le fichier PDF cible. **Remarque :** Le PDF source doit être du même type de données que le PDF cible. Cependant, les fichiers PDF de type "Texte", "Liste de texte", "Courriel", "Mobile", "Adresse" et "Téléphone" peuvent être utilisés de façon interchangeable puisque le sous-jacent Le type est "Texte" pour tous ces éléments.

12. Si vous souhaitez modifier l'état autorisé de chaque titulaire de carte, cochez la **case Modifier le titulaire de carte autorisé**.
    Les boutons de cette section sont activés.
13. Cliquez sur le bouton radio correspondant à l'état requis (Autorisé active une carte pour l'utilisation et **Non autorisé** désactive une carte), puis cliquez sur le bouton **Suivant**.
14. L'écran "Modifier les détails de la carte" ne s'affiche que si la case à cocher **Modifier les détails de la carte** a été cochée sur l'écran "Sélectionner les modifications". Sinon, passez à l'étape 17.
    Cet écran vous permet de sélectionner les modifications à apporter au type de carte.



15. Sélectionnez le Type de carte dans la liste déroulante.
    Les champs de cet écran sont activés.
16. Voulez-vous supprimer ou modifier le type de carte sélectionné pour les détenteurs de carte ?

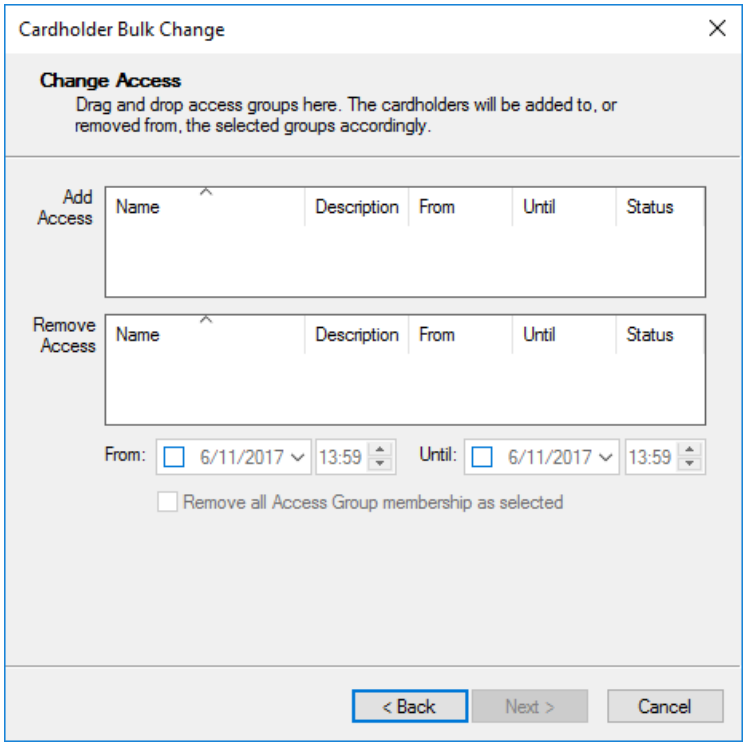
Si...	alors...
supprimer,	cliquez sur le bouton **Enlever** la carte et passez à l'étape 18.
modifier,	cliquez sur le bouton **Modifier la carte (Modify Card)**.

17. Configurez les modifications que vous souhaitez apporter si nécessaire, puis cliquez sur le bouton **Suivant** s'affiche.
Vous pouvez sélectionner une ou plusieurs de ces options.

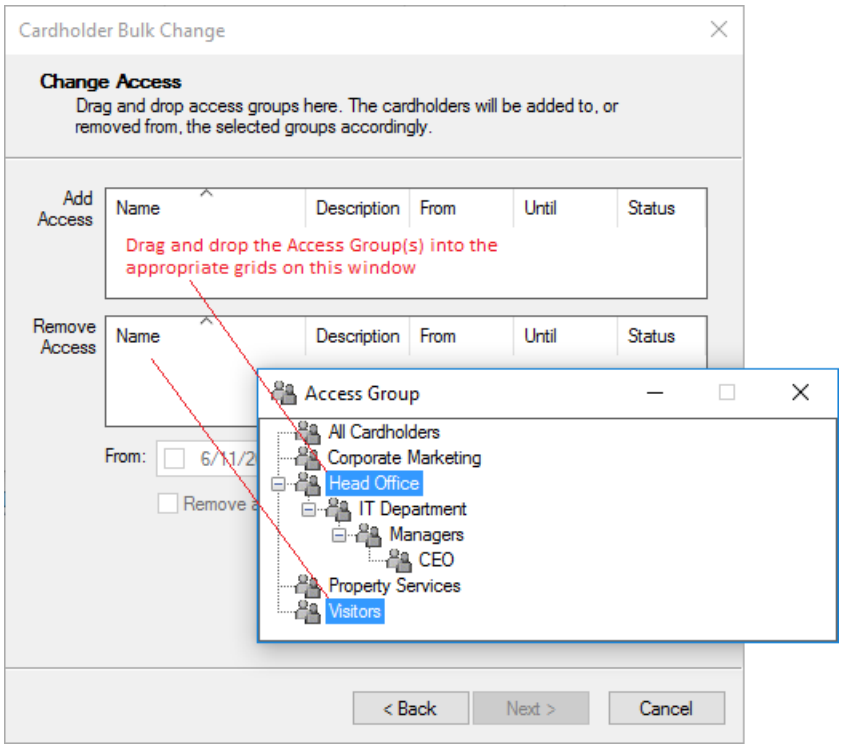
Case à cocher	Description
Incrémenter le niveau d'émission	Cochez cette case si les titulaires de carte sélectionnés nécessitent une incrémentation en masse du niveau de délivrance de la carte.
Activer/Désactiver la carte	Activez ou désactivez la carte en cochant la case appropriée.
Modifier le type de carte	Cochez cette case si le type de carte du titulaire de la carte sélectionné doit être modifié. Lorsque cette option est cochée, le champ déroulant est activé, ce qui vous permet de sélectionner un type de carte différent. **Remarques :** • Seuls les types de cartes ayant les mêmes formats de numéro de carte peuvent être échangés. • Seuls les types de carte pour lesquels vous disposez de privilèges d'affichage s'affichent dans la liste déroulante. • Si un titulaire de carte possède plusieurs cartes de type Carte, elles seront toutes modifiées, à moins qu'une carte ne soit pas mise à jour. Lorsqu'une carte n'est pas mise à jour, aucune carte pour ce titulaire de carte particulier ne sera mise à jour. • Seules les cartes dans un état de carte non personnalisé au moment de l'exécution de la modification en bloc pourront changer de type de carte (c'est-à-dire que les cartes dans n'importe quel état y compris Perdu, Volé et Endommagé peuvent être modifiées, mais pas les cartes dans un état de carte qui est ajouté manuellement par un opérateur.
Modifier la date d'activation	Cochez cette case si la date de début d'accès doit être modifiée. Lorsque cette case est cochée, les champs date et heure sont activés vous permettant de sélectionner une nouvelle date d'activation.
Modifier la date d'expiration	Cochez cette case si la date de fin d'accès doit être modifiée. Lorsque cette case est cochée, les champs date et heure sont activés vous permettant de sélectionner une nouvelle date d'expiration.

18. L'écran "Modifier l'accès" ne s'affiche que si les **options** Modifier **l'accès** a été cochée sur l'écran "Sélectionner les modifications". Si ce n'est pas le cas, passez à l'étape 26.

Cet écran vous permet de modifier les options d'accès pour les groupes d'accès si nécessaire.



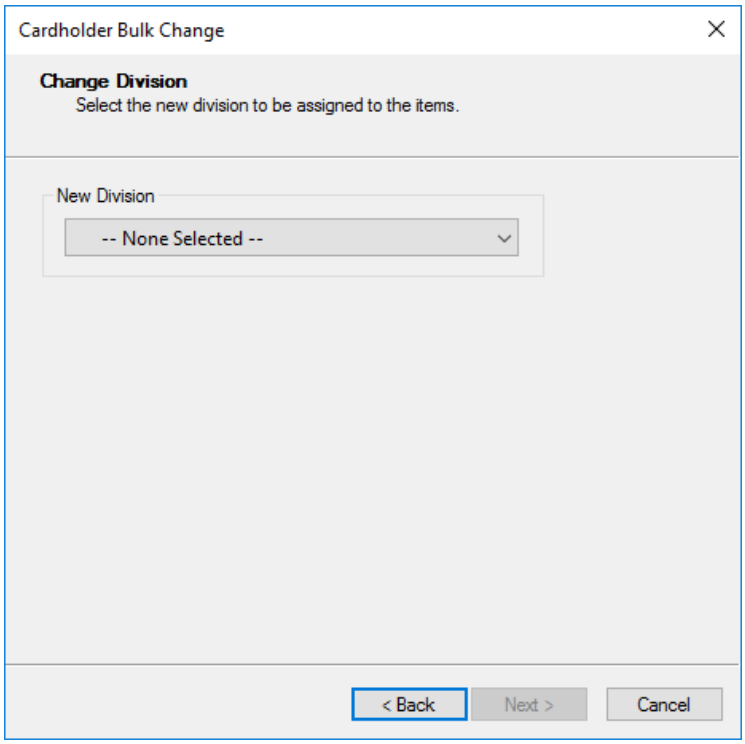
19. Cliquez sur **Gérer** dans la barre de menus, puis sur **Groupes d'accès**.
La fenêtre **Liste** principale **du groupe Access** s'ouvre.
Sélectionnez les groupes d'accès que les détenteurs de carte doivent ajouter et/ou supprimer, puis faites-les glisser dans les grilles appropriées sur cet écran de l'Assistant, puis fermez la **fenêtre Liste principale des groupes d'accès**.



20. Les champs de date/heure "Du" et "Jusqu'au" de cet écran permettent l'appartenance temporaire à un groupe Access pour être configuré si nécessaire.
    Si un accès temporaire est requis, passez à l'étape 21.
    Si un accès permanent est requis, passez à l'étape 25.
21. Mettez en surbrillance le groupe d'accès (sur l'écran **Modifier l'accès** de l'Assistant) dont les détenteurs de carte ont besoin pour accéder temporairement à.
    Les champs Date de début et Date de fin sont activés.
22. Cliquez sur la zone de liste déroulante "De" et sélectionnez la date à laquelle les détenteurs de carte doivent avoir accès à ce groupe d'accès.
    La case à cocher Heure de début est activée et la date de début s'affiche désormais dans la grille à côté du nom du groupe d'accès.
23. Sélectionnez l'heure dans la case "De" à laquelle les titulaires de carte doivent avoir accès à partir de cette date.
24. Répétez les étapes 21 et 22 pour les champs "Jusqu'à" (c'est-à-dire la date et l'heure du dernier jour auquel les détenteurs de carte doivent avoir accès).
    La date "Jusqu'au" s'affiche désormais dans la grille à côté du nom du groupe Access.
25. Cochez la case **Supprimer tous les membres du groupe d'accès comme sélectionné** si nécessaire.

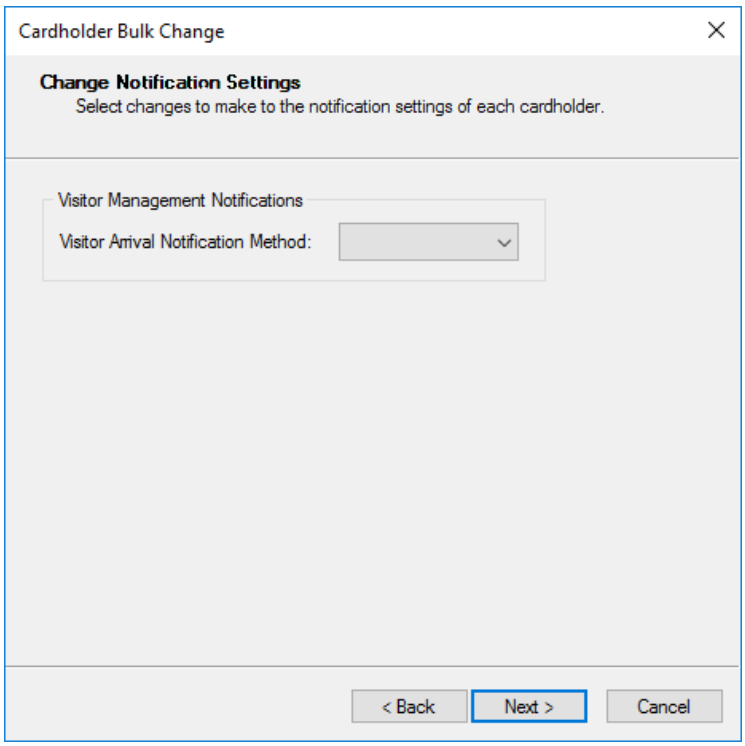
Si...	**alors...**
coché	tous les groupes d'accès répertoriés dans la grille "Supprimer l'accès" seront supprimés des titulaires de carte nommés indépendamment des dates/ heures "De" et "Jusqu'à", qui peuvent ou non avoir été saisies pour chaque sélection de groupe d'accès.
non coché et aucune date/ heure "Du" n'est saisie	seul l'accès permanent sera supprimé.
non cochée et une date/ heure "De" est entrée	un seul accès temporaire pour cette période précise sera supprimé.

26. Cliquez sur le bouton **Suivant**.
27. L'écran "Modifier la division" ne s'affiche que si la **case à** cocher **Modifier la division** a été cochée sur l'écran "Sélectionner les modifications". Si ce n'est pas le cas, passez à l'étape 29.
    Cet écran vous permet de sélectionner une nouvelle division dans laquelle ces détenteurs de carte seront changés.

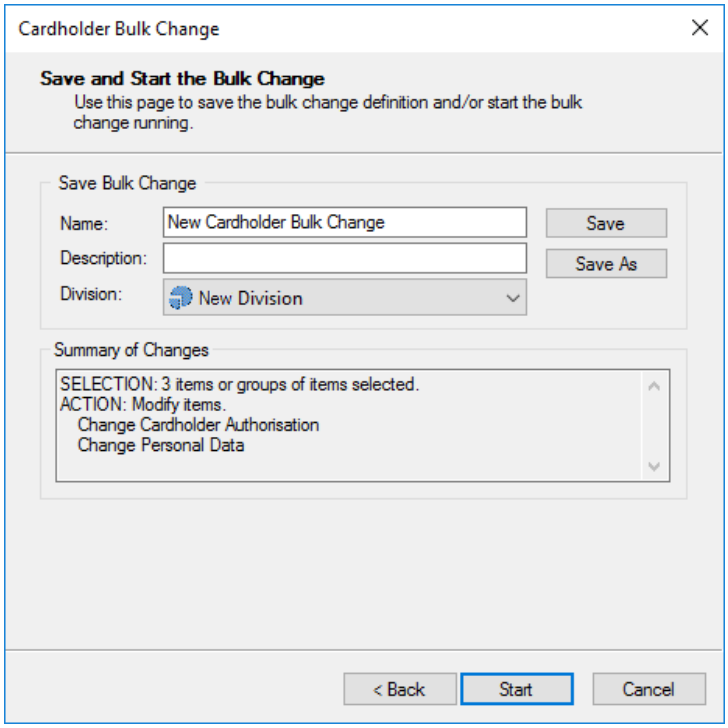


28. Sélectionnez une division dans la liste déroulante.
    Remarque : Seules les divisions auxquelles vous avez le privilège d'opérateur "Modifier le titulaire de carte" s'afficheront dans la liste déroulante.

29. L'écran "Modifier les paramètres de notification" ne s'affiche que si la case à cocher **Modifier les notifications de gestion des visiteurs** a été cochée sur l'écran "Sélectionner les modifications". Sinon, passez à l'étape 30.
    Cet écran vous permet de sélectionner la méthode de notification qui sera attribuée à chaque titulaire de carte pour indiquer l'arrivée d'un visiteur.



30. Sélectionnez une méthode de notification dans la liste déroulante (i.e. "Aucun", "Email", "SMS" ou "Email et SMS").
31. L'écran "Enregistrer et démarrer la modification en bloc" de l'Assistant de modification en bloc du titulaire de carte s'affiche.

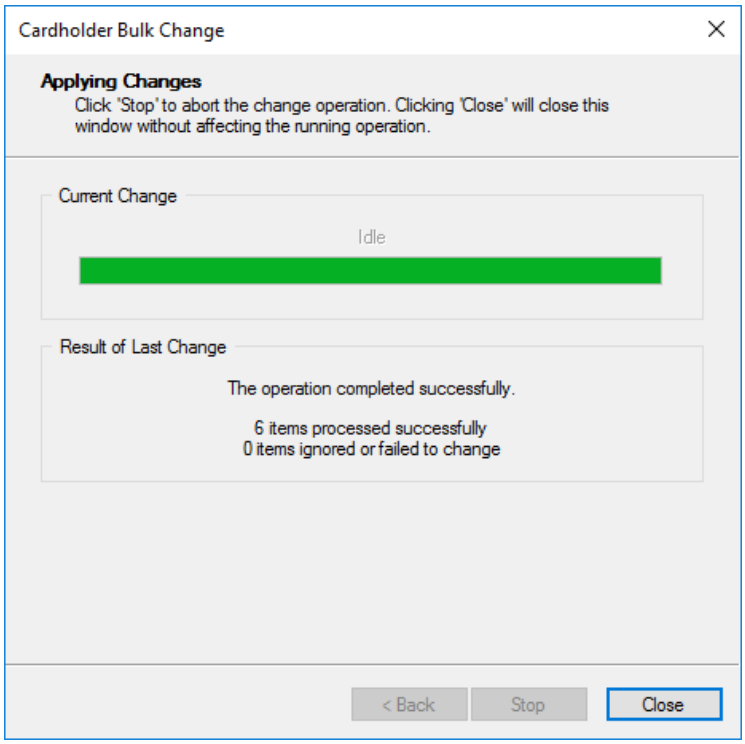


La section **Résumé des modifications** fournit un résumé des modifications que vous devez vérifier avant de continuer.

32. Voulez-vous enregistrer cette modification en bloc et ses paramètres avant de l'exécuter ?

Si...	alors...
non	allez à l'étape 34.
oui	type dans un nom et une description. **Remarque :** Le **champ Nom** est limité à 60 caractères et la **Le** champ Description est limité à 200 caractères.

33. Cliquez sur le bouton **Enregistrer**.
Cette modification en bloc et ses paramètres sont enregistrés et s'affiche désormais dans la fenêtre principale de la liste principale des **modifications en bloc**.
Remarque : Le bouton **Enregistrer sous** vous permet de modifier une modification en bloc existante et de la réenregistrer sous un nouveau nom. Si vous ouvrez une modification en bloc enregistrée existante et cliquez sur le bouton **Enregistrer sous** sans modifier le nom, un message s'affiche indiquant qu'une modification en bloc portant ce nom existe déjà.
34. Cliquez sur le bouton **Démarrer**.
L'écran "Application des modifications" de l'Assistant Modifications en bloc des titulaires de carte s'affiche.



Cet écran montre la progression de la modification en bloc. En cours, l'état de ce changement en bloc s'affiche comme "Actif" dans la fenêtre de la liste principale des **modifications en bloc**, et s'il se termine avec succès, (c'est-à-dire que la barre de progression atteint 100 %), l'état devient "Réussi". Une fois qu'il a terminé, le nombre de détenteurs de carte a changé s'affiche.?

Remarques :

- Si vous n'avez pas nommé et enregistré la modification en bloc avant de cliquer sur le bouton **Démarrer**, tandis que l'écran "Application des modifications" s'affiche, la modification en bloc apparaîtra dans la fenêtre Liste principale des **modifications en bloc** avec un nom généré par le système, jusqu'à ce qu'elle soit terminée avec succès, à ce moment le système la supprimera. Lorsqu'il est actif ou en cas d'échec, il reste dans la fenêtre **Liste principale des modifications en bloc** jusqu'à ce qu'un opérateur le supprime.
- Si vous cliquez sur le bouton **Arrêter** alors que la modification en bloc est en cours, les modifications déjà apportées lors de l'arrêt ne peuvent pas être annulées, mais elles sont terminées. Si vous cliquez sur le bouton Arrêter, vous avez la possibilité d'arrêter la modification en bloc ou de revenir en arrière et de la modifier.

Résultat

Un changement en bloc de titulaire de carte a été initié.

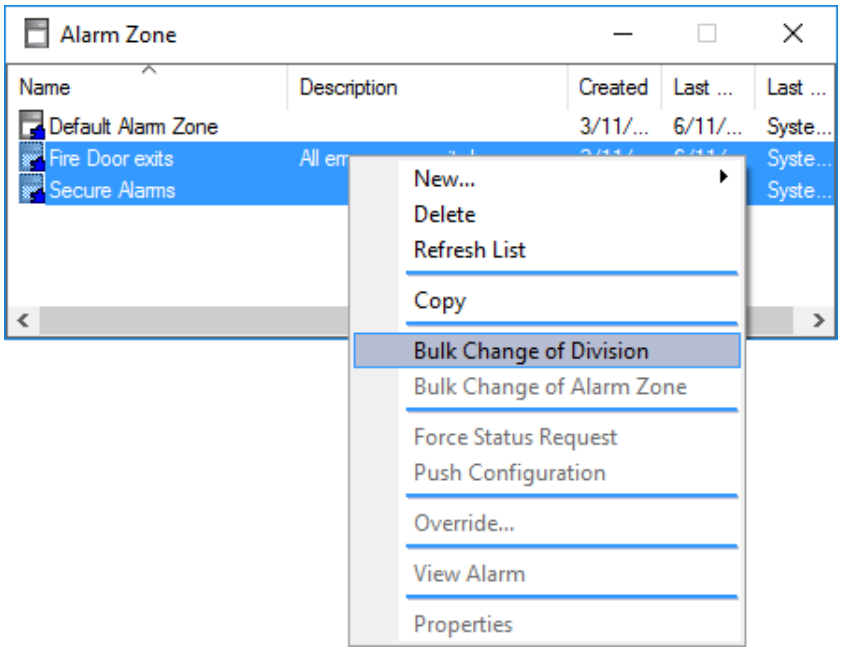
Lancement d'une nouvelle division

Introduction

Cette procédure décrit comment initier une nouvelle modification en bloc de division dans le Centre de commande. Les modifications en bloc des divisions peuvent être effectuées sur n'importe quel élément du Centre de commande qui vous permet de sélectionner plusieurs éléments, et a pour champ "Division" (par exemple, les types de cartes, les champs de données personnelles, les portes, les zones d'alarme, les zones d'accès, etc.).
Pour exécuter cette procédure, l'opérateur doit disposer à la fois du privilège opérateur "Modification en bloc" et du privilège de modification d'élément approprié.

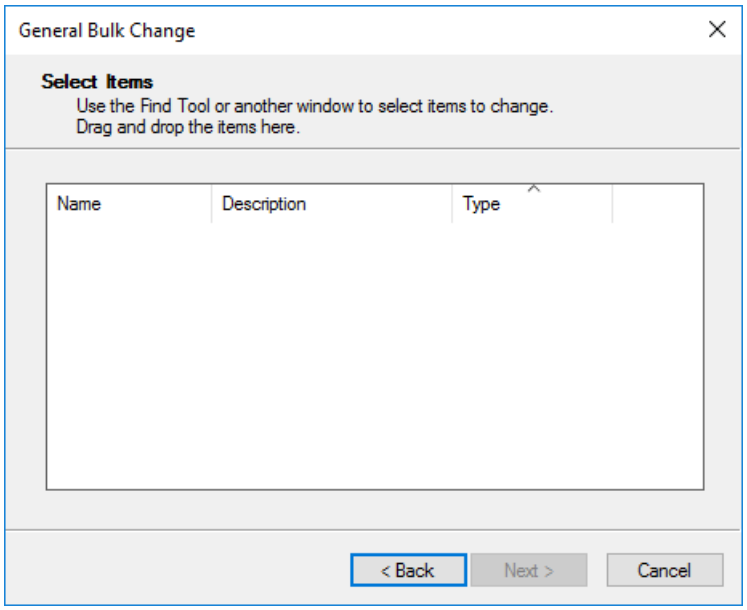
Il existe deux méthodes pour exécuter cette procédure. Vous pouvez utiliser :

- l'Assistant Modification générale, ou
- l'option de menu contextuel disponible à partir d'une fenêtre de liste principale d'éléments. En utilisant cette méthode, vous sélectionnez les éléments qui doivent changer de division, **cliquez avec le bouton droit** et sélectionnez **Bulk Change of Division** dans le menu contextuel.
  L'écran "Division des modifications" de l'assistant Modifications en bloc de la division s'affiche. Remplissez les étapes 7 et 8 de la procédure suivante pour effectuer un changement global de division.



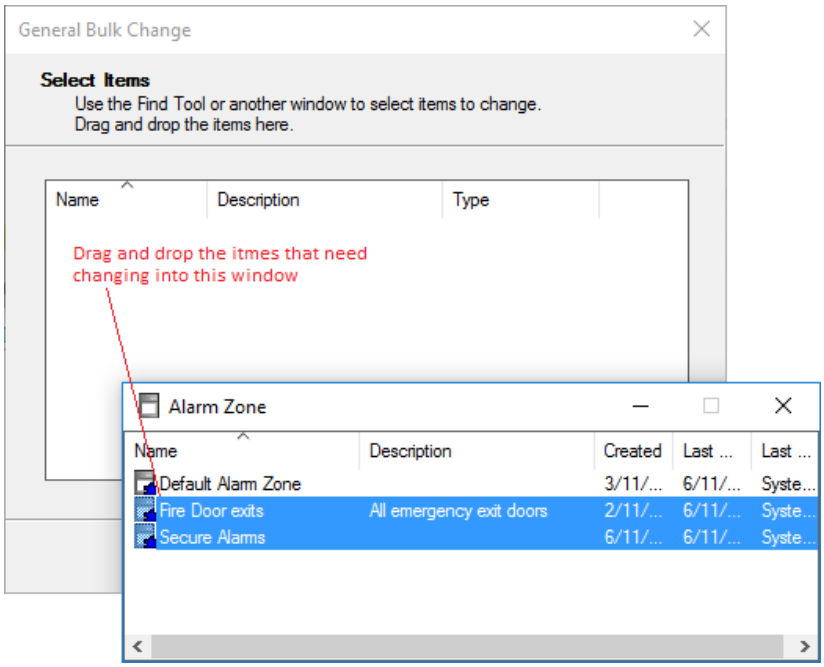
Procédure (à l'aide de l'assistant)

1. Cliquez sur **Gérer** dans la barre de menus, puis sur **Modifications en bloc**.
   La fenêtre Liste principale des modifications en **masse** s'affiche.
2. **Cliquez avec le bouton droit** de la souris et **sélectionnez ... Général Modification en bloc**.
   L'écran "Sélectionner les éléments" de l'assistant Général de modification en bloc s'affiche.

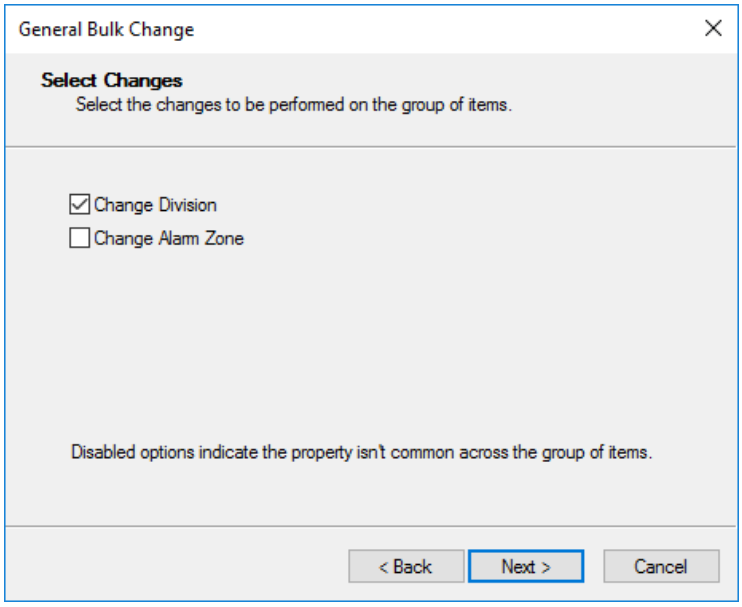


Tous les éléments à modifier doivent être placés sur cet écran, en les faisant glisser et en les déposant depuis la fenêtre de liste principale appropriée, ou l'outil de recherche peut être utilisé. Par exemple, dans cette procédure, les zones d'alarme nécessitent des modifications de division.

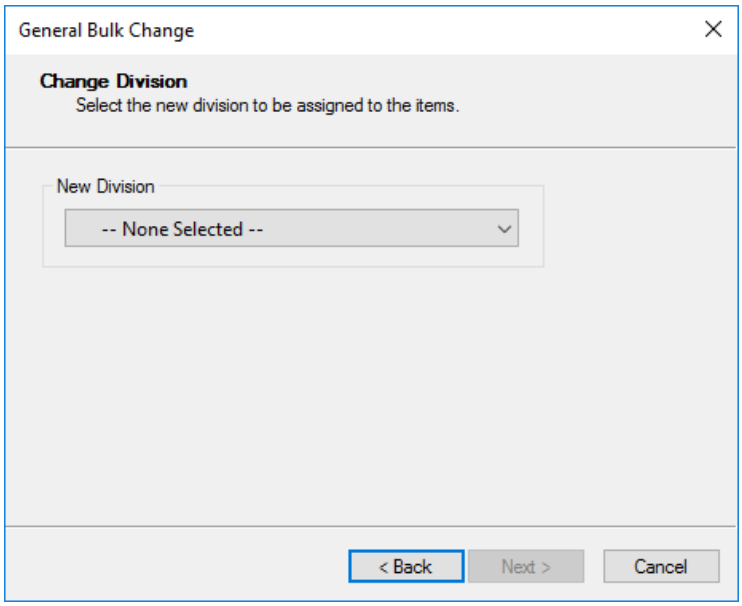
3. Ouvrez la fenêtre Liste principale des éléments du Centre de commandes et sélectionnez les éléments à modifier.
   Faites glisser et déposez-les dans cet écran de l'assistant.



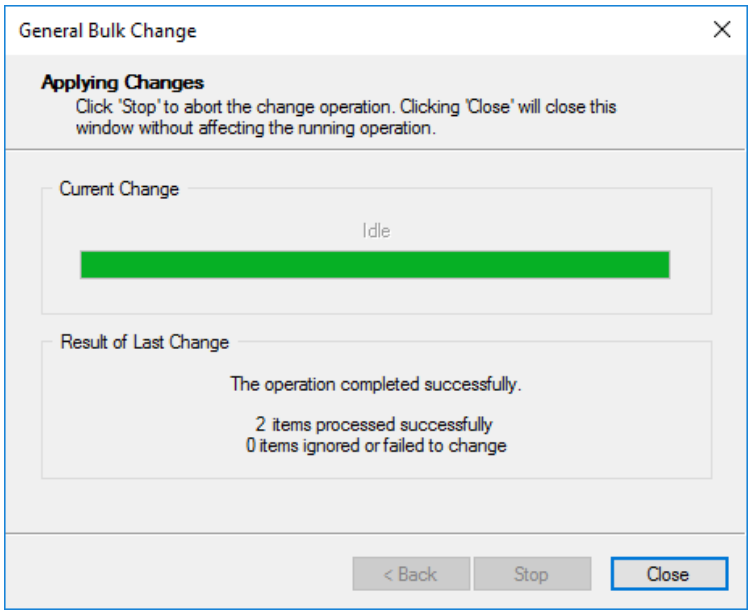
4. Fermez la fenêtre Liste principale des éléments du centre de commandes.
5. Cliquez sur le bouton **Suivant**.
   L'écran "Sélectionner les modifications" de l'assistant Général de modification en bloc s'affiche.



6. Assurez-vous que la **case** Modifier **la division** est cochée et cliquez sur le bouton **Suivant** s'affiche.
   L'écran "Division de modification" de l'assistant de modification en masse générale s'affiche.



7. Sélectionnez une nouvelle division à affecter à ces éléments dans la liste déroulante.
   Remarque : Seules les divisions pour lesquelles vous disposez du privilège de modification approprié s'affichent dans la liste déroulante.
8. Cliquez sur le bouton **Démarrer**.
   L'écran "Application des modifications" de l'assistant Général de modification en bloc s'affiche.



Cet écran affiche la progression de la modification en masse.
Pendant l'affichage de cet écran, la modification en bloc apparaît dans la fenêtre **Bulk Changes** List (Liste principale des **modifications en bloc)** avec un nom généré par le système. En cours de réalisation, l'état de cette modification en bloc s'affichera comme "Actif" dans la **fenêtre Liste principale des** modifications en bloc**, et s'il s'achève avec succès, il s'affichera comme** "Réussi", auquel moment le système la supprimera.

Remarque :
Alors qu'un changement de division en masse est actif, ou si il échoue, il restera dans le **Bulk Changes** List Window jusqu'à ce qu'un opérateur le supprime.

Résultat

Un changement de division en bloc a été initié, et les éléments sélectionnés ont fait changer leur division.

Lancement d'une purge en masse de détenteurs de cartes inactifs

Introduction

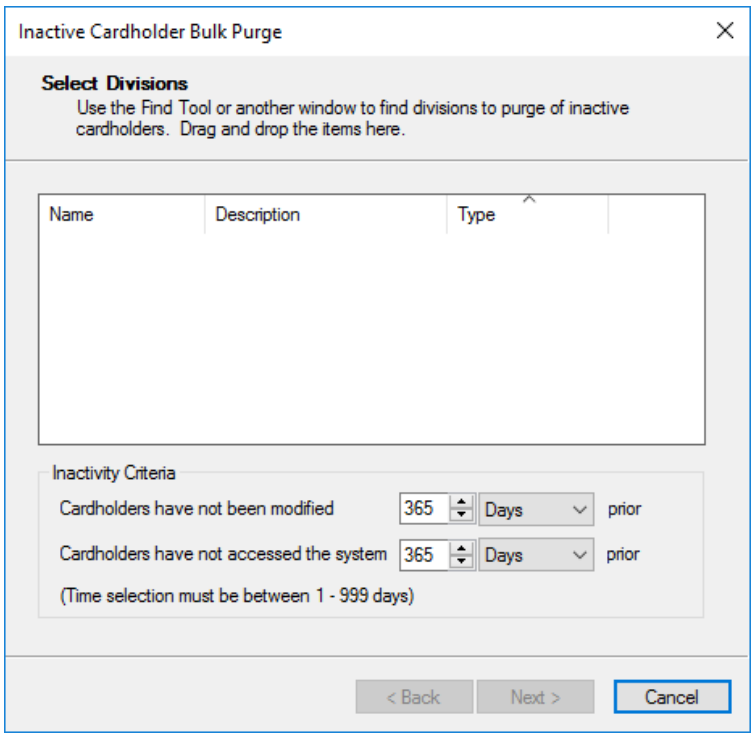
Cette procédure décrit comment purger tous les détenteurs de cartes stockés dans l'une des divisions d'une liste spécifiée, où :

- l'activité la plus récente sur le détenteur de la carte dépasse un nombre de jours spécifié, et
- le titulaire de la carte n'est pas un visiteur ou un hôte lors d'une visite active (c'est-à-dire une visite ayant le statut "Planifié" ou "En cours"), aux fins de la gestion des visiteurs (une fonctionnalité pouvant faire l'objet d'une licence).

Pour exécuter cette procédure, l'opérateur doit disposer des privilèges d'opérateur "Modification en bloc" et "Modification des titulaires de carte". En outre, l'opérateur a besoin de privilèges suffisants divisionnaires et autres pour effectuer chaque changement individuel répertorié dans une purge en bloc.
Remarque : Une purge en bloc des titulaires de carte inactifs peut être planifiée pour s'exécuter à des heures précises, via une macro. Voir ***Macros*** (à la page 20-1).

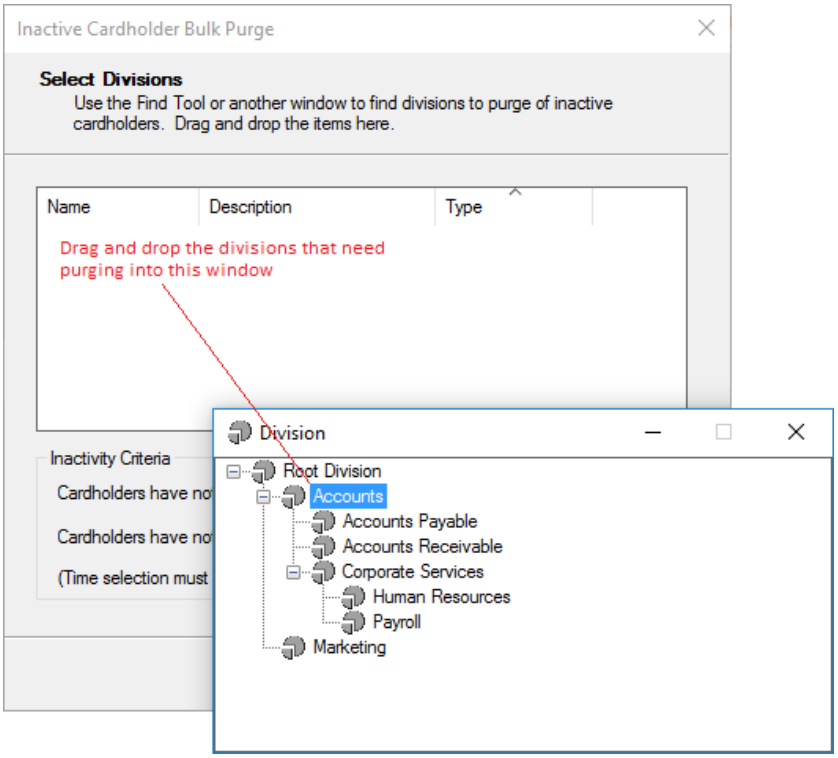
Procédure

1. Cliquez sur **Gérer** dans la barre de menus, puis sur **Modifications en bloc**.
   La fenêtre Liste principale des modifications en **masse** s'affiche.
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau... Titulaire de carte Bulk Purge**.
   L'écran "Sélectionner les divisions" de l'Assistant Inactive Titulaire de carte Bulk Purges s'affiche.

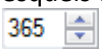


Toutes les divisions qui doivent être placées sur cet écran peuvent être glissées et supprimées de la fenêtre Liste principale de **division** ou de l'outil de recherche peuvent être utilisées. Dans cette procédure, la fenêtre Liste principale des divisions a été utilisée.

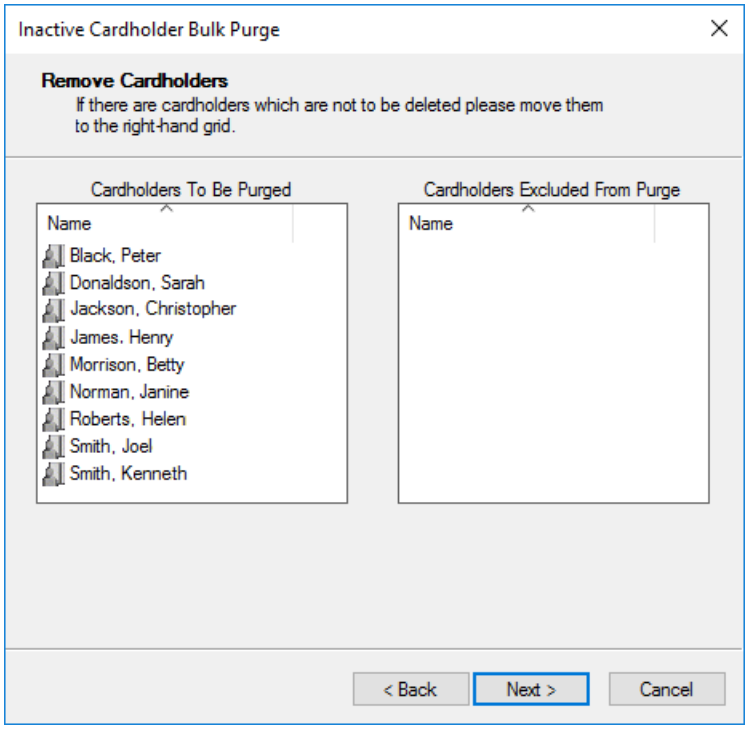
3. Cliquez sur **Configurer** dans la barre de menus, puis sur **Divisions**.
   La fenêtre Liste principale des divisions s'ouvre.
   Sélectionnez les divisions dont les titulaires de carte inactifs doivent être purgés, et faites-les glisser dans cet écran de l'assistant.



Remarque : Lorsqu'une division est déplacée, c'est toute la hiérarchie enfant qui est également déplacée. Dans l'exemple d'écran ci-dessus, si la division "Comptes" est déplacée sur l'assistant, les divisions "Comptes fournisseurs" et "Comptes clients" seront également déplacées.

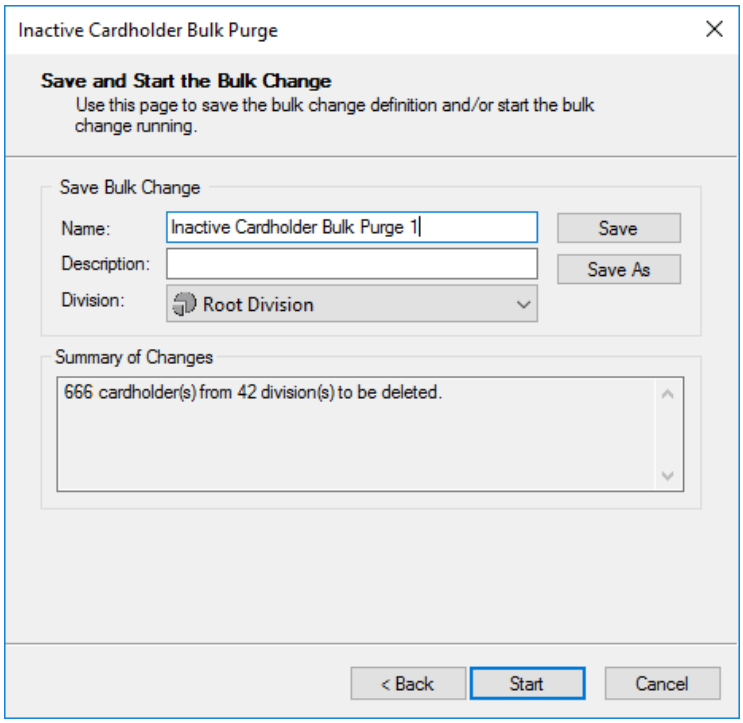
4. Indiquez le nombre de jours pendant lesquels un détenteur de carte est classé comme inactif, en entrant un nombre 

dans le champ.
   (Par défaut = 365 jours ; Limite = 1 -999 jours)
5. Fermez la fenêtre Liste principale des divisions.
6. Cliquez sur le bouton **Suivant**.
   L'écran "Retirer les titulaires de carte" de l'Assistant Inactif de purge en bloc de titulaire de carte s'affiche.



La grille **des titulaires de carte à presser** sur la gauche est remplie de détenteurs de cartes inactifs des divisions choisies.
Remarque : Un détenteur de carte inactif est un détenteur de carte dont la dernière carte a été badgée plus que le nombre de jours spécifié auparavant et qui n'a pas non plus été modifié à ce moment-là. S'ils sont associés à une visite d'une manière ou d'une autre, ils ne pourront pas être supprimés.

7. Faites glisser les détenteurs de carte que vous ne souhaitez pas supprimer de la grille **Titulaire de cartes To Be Purged** (à gauche) vers la grille **Titulaire de cartes Excluded From Purge** (à droite).
8. Cliquez sur le bouton **Suivant**.
   L'écran "Enregistrer et démarrer la modification en bloc" de l'Assistant Inactive Titulaire de carte Bulk Purges (Purge en bloc) s'affiche.



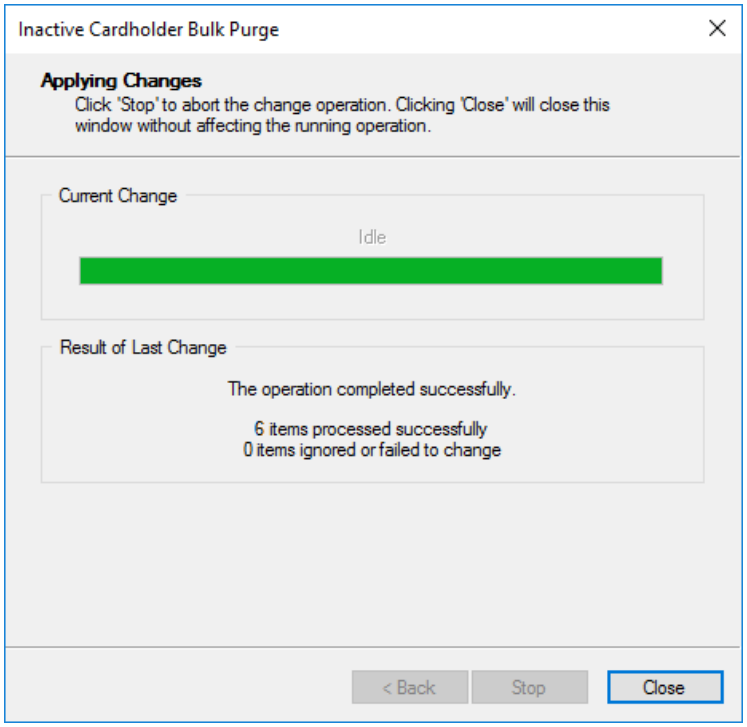
La section **Résumé des modifications** fournit un résumé des modifications que vous devez vérifier avant de continuer.

9. Voulez-vous enregistrer cette modification en bloc et ses paramètres avant de l'exécuter ?

Si...	alors...
non	allez à l'étape 11.
oui	tapez un nom et une description. **Remarque :** Le champ **Nom** est limité à 60 caractères et la description est limité à 200 caractères.

10. Cliquez sur le bouton **Enregistrer**.
Cette purge en bloc et ses paramètres sont enregistrés et s'affichent maintenant dans la fenêtre principale de la liste principale des **modifications en** bloc.
Remarque :
Le bouton **Enregistrer sous** vous permet de modifier une purge en bloc existante et de l'enregistrer à nouveau sous un nouveau nom de purge en bloc. Si vous ouvrez une purge en bloc enregistrée existante et cliquez sur le bouton **Enregistrer sous** sans modifier le nom, un message s'affiche indiquant qu'une purge en bloc portant ce nom existe déjà.

11. Cliquez sur le bouton **Démarrer**.
L'écran "Application des modifications" de l'Assistant Inactive Titulaire de carte Bulk Purges s'affiche.



Cet écran affiche la progression de la purge en bloc. En cours, l'état de cette purge en bloc s'affichera sous la forme "Actif" dans la fenêtre Liste principale des **modifications en bloc**, et s'il s'achève avec succès (la barre de progression atteint 100 %), l'état passera à "Réussi". Une fois qu'il a terminé, le nombre de détenteurs de carte a changé s'affiche.

Remarques :

- Si vous n'avez pas nommé et enregistré la modification en bloc avant de cliquer sur le bouton **Démarrer**, tandis que l'écran "Application des modifications" s'affiche, la modification en bloc apparaîtra dans la fenêtre Liste principale des **modifications en bloc** avec un nom généré par le système, jusqu'à ce qu'elle soit terminée avec succès, à ce moment le système la supprimera. Lorsqu'il est actif ou en cas d'échec, il reste dans la fenêtre **Liste principale des modifications en bloc** jusqu'à ce qu'un opérateur le supprime.
- Si vous cliquez sur le bouton **Arrêter** alors que la modification en bloc est en cours, les modifications déjà apportées lors de l'arrêt ne peuvent pas être annulées, mais elles sont terminées. Si vous cliquez sur le bouton Arrêter, vous avez la possibilité d'arrêter la purge en bloc ou de revenir en arrière et de la modifier.

Résultat

Certains détenteurs ont été supprimés du système.

Modification et exécution d'une modification en bloc enregistrée

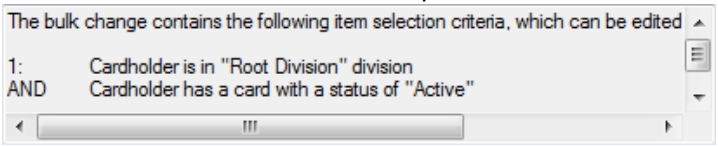
Introduction

Cette procédure décrit comment modifier et exécuter une modification en bloc existante dans le Centre de commandes. Pour exécuter cette procédure, l'opérateur doit disposer à la fois du privilège d'opérateur "Modification en bloc" et du privilège de modification d'élément approprié.
Remarques :

- Lorsqu'une modification en bloc est exécutée, elle utilise TOUS les privilèges d'un opérateur, quelle que soit la vue système sélectionnée. Par exemple, un opérateur peut exclure un privilège d'opérateur de sa vue système actuelle, mais si une modification en bloc est exécutée, ce privilège fera partie des privilèges d'opérateur sous lesquels la modification en masse sera exécutée.
- Les modifications en bloc sont soumises à toutes les restrictions de station de travail en vigueur sur la station de travail à laquelle elle est exécutée.

Procédure

1. Cliquez sur **Gérer** dans la barre de menus, puis sur **Modifications en bloc**.
   La fenêtre Liste principale des modifications en **masse** s'affiche.
2. Sélectionnez la modification en bloc que vous souhaitez modifier et exécuter, puis double-cliquez sur le bouton de la souris.
3. La modification en masse a-t-elle déjà été exécutée ?

Si...	puis s'ouvre l'assistant...
non, (c'est-à-dire qu'il n'a pas d'état dans la fenêtre **Bulk Changes** List)	Écran "Sélectionner les titulaires de carte ou les groupes d'accès". a) À l'aide du bouton **Suivant**, parcourez l'assistant en apportant les modifications nécessaires. b) Lorsque vous accédez à l'écran "Enregistrer et démarrer le changement en bloc", passez à l'étape 4. **Remarque :** Si le changement de titulaire de carte en bloc a été configuré dans le client du centre de commande plutôt que dans le client de configuration, ET qu'il a été configuré avec des critères (par exemple, des règles de recherche avancées), le message suivant s'affiche en bas de l'écran de l'assistant : *"La modification en bloc contient les critères de sélection d'éléments suivants, qui peuvent être modifiés dans le client Command Center uniquement".* 

Si...	puis s'ouvre l'assistant...
oui, (c'est-à-dire qu'il a un statut dans la fenêtre **Liste** principale des modifications en **vrac**)	écran "Application des modifications". Cela vous permet d'afficher les résultats de la dernière exécution. a) À l'aide du bouton Précédent, effectuez votre retour à l'aide de l'Assistant pour apporter des modifications si nécessaire, ou simplement revenez à l'écran "Enregistrer et démarrer la modification en bloc" pour l'exécuter. b) Passez à l'étape 4.

4. Sur l'écran "Enregistrer et démarrer la modification en bloc", le nom et la description de la modification en bloc existante remplissent les **champs** Nom **et** Description. Voulez-vous enregistrer les modifications apportées à la modification en bloc existante ou souhaitez-vous enregistrer ces modifications en tant que nouvelle modification en bloc ?

Si tu veux...	alors...
enregistrer les modifications apportées à la modification globale existante	cliquez sur le bouton **Enregistrer**. La modification en bloc sera de nouveau enregistrée lorsque vos modifications seront effectuées.
enregistrer comme nouvelle modification en bloc	modifiez le nom et la description, puis cliquez sur Bouton **Enregistrer sous**. La modification en bloc d'origine et la modification en bloc nouvellement nommée s'affichent dans la fenêtre **Liste** principale des modifications en bloc. **Remarque :** Si vous cliquez sur le bouton **Enregistrer sous** si vous modifiez le nom, un message d'erreur s'affiche indiquant que le nom doit être modifié.

5. Cliquez sur le bouton **Démarrer**.
   L'écran "Application des modifications" de l'Assistant Modifications en bloc des titulaires de carte s'affiche. Cet écran montre la progression de la modification en bloc. En cours, l'état de cette modification en bloc s'affichera comme "Actif" dans la fenêtre Liste principale des **modifications en bloc**, et s'il s'achève avec succès, (c'est-à-dire que la barre de progression atteint 100 %), l'état passera à "Réussi". Une fois qu'il a terminé, le nombre de détenteurs de cartes a changé d'affichage.
   Remarque : Si vous cliquez sur le bouton Arrêter alors que la modification en bloc est en cours, les modifications déjà apportées lorsqu'elle est arrêtée ne peuvent pas être annulées, mais elles sont terminées. Si vous cliquez sur le bouton Arrêter, vous avez la possibilité d'arrêter la modification en bloc ou de revenir en arrière et de la modifier.

Résultat

Une modification en masse (enregistrée) existante a été modifiée et exécutée.

Indication

Suppression des modifications en bloc enregistrées
Reportez-vous à ***Suppression d'éléments*** (page 3-27) pour la procédure de suppression d'un changement en bloc de titulaire de carte enregistré.
Remarque : Une modification en bloc ne peut pas être supprimée si elle est incluse dans une macro.

Lancement d'un changement en bloc de zone d'alarme

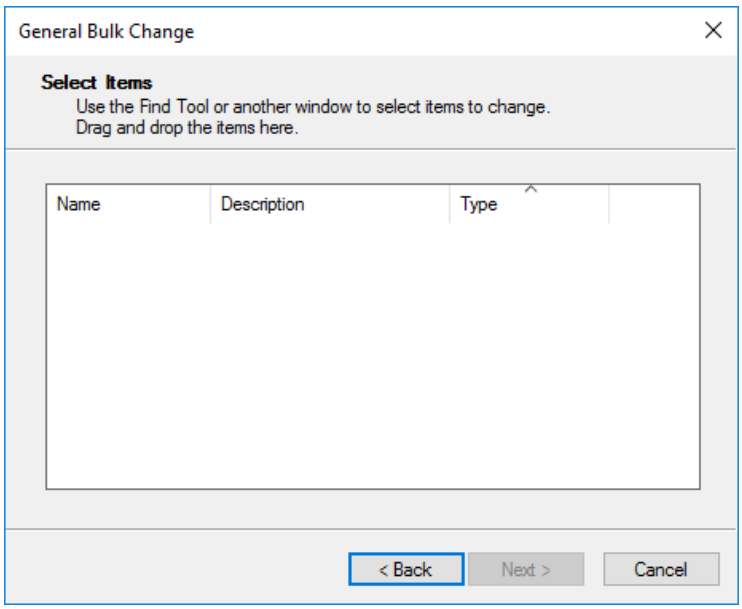
Introduction

Cette procédure décrit comment ajouter plusieurs éléments du Centre de commandes à une zone d'alarme. Les modifications en bloc des zones d'alarme peuvent être effectuées sur n'importe quel élément du centre de commande qui vous permet de sélectionner plusieurs éléments (par exemple, types de carte, champs de données personnelles, portes, zones d'accès, etc.). Pour exécuter cette procédure, l'opérateur doit disposer à la fois du privilège d'opérateur "Modification en bloc" et du privilège de modification d'élément approprié.

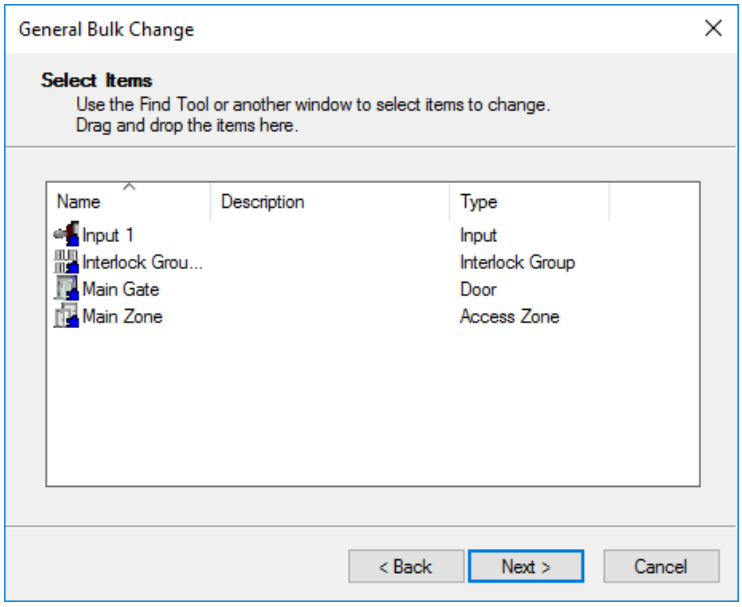
Il existe trois méthodes pour ajouter plusieurs éléments du Centre de commande à une zone d'alarme. Cette procédure décrit l'utilisation de l'Assistant Modification générale. Pour les autres méthodes, reportez-vous à ***Ajout de plusieurs éléments aux zones d'alarme*** (page 14-18).

Procédure (à l'aide de l'assistant)

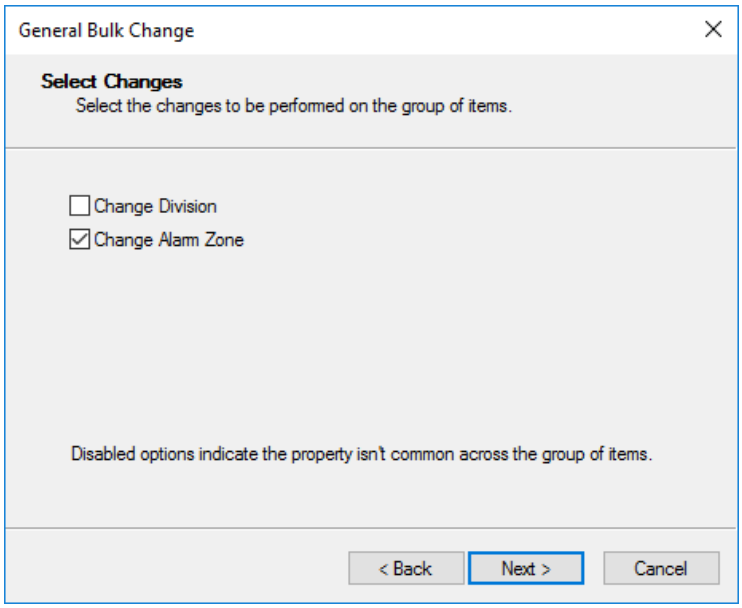
1. Cliquez sur **Gérer** dans la barre de menus, puis sur **Modifications en bloc**.
   La fenêtre Liste principale des modifications en **masse** s'affiche.
2. **Cliquez avec le bouton droit** de la souris et **sélectionnez ... Général Modification en bloc**.
   L'écran "Sélectionner les éléments" de l'assistant Général de modification en bloc s'affiche.



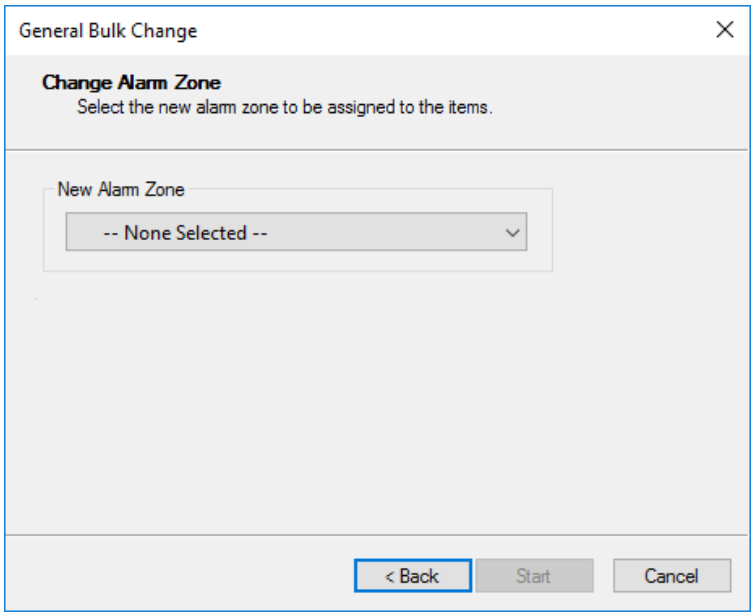
3. Placez tous les éléments à ajouter à la zone d'alarme sur cet écran, en les faisant glisser et en les déposant depuis la fenêtre de liste principale appropriée ou en utilisant l'outil de recherche.



4. Cliquez sur le bouton **Suivant**.
   L'écran "Sélectionner les modifications" de l'assistant Général de modification en bloc s'affiche.

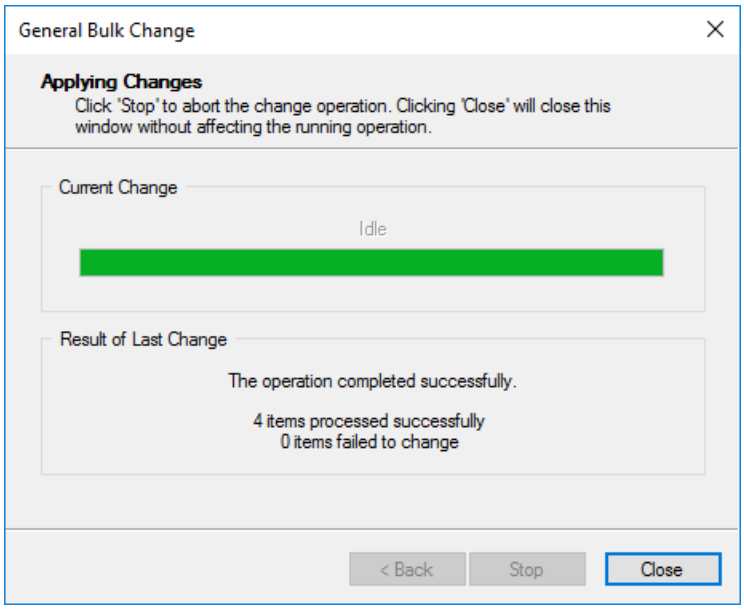


5. Vérifiez que la case **Modifier la zone d'alarme** est cochée, puis cliquez sur le bouton **Suivant** s'affiche.
   L'écran "Modifier la zone d'alarme" de l'assistant général de modification en bloc s'affiche.



6. Sélectionnez une nouvelle zone d'alarme à affecter à ces éléments dans la liste déroulante.
   Remarque : Seules les zones d'alarme pour lesquelles vous disposez du privilège de modification approprié s'affichent dans la liste déroulante.

7. Cliquez sur le bouton **Démarrer**.
   L'écran "Application des modifications" de l'assistant Général de modification en bloc s'affiche.



   Cet écran affiche la progression de la modification en masse.
   Pendant l'affichage de cet écran, la modification en bloc apparaît dans la fenêtre **Bulk Changes** List (Liste principale des **modifications en bloc)** avec un nom généré par le système. En cours de réalisation, l'état de cette modification en bloc s'affichera comme "Actif" dans la **fenêtre Liste principale des** modifications en bloc**, et s'il s'achève avec succès, il s'affichera comme** "Réussi", auquel moment le système la supprimera.

Remarque :
Lorsqu'une modification en bloc de la zone d'alarme est active ou en cas d'échec, elle reste dans la fenêtre de liste principale des **modifications en bloc** jusqu'à ce qu'un opérateur la supprime.

Résultat

Un changement en bloc des zones d'alarme a été initié et les éléments sélectionnés ont été ajoutés à la zone d'alarme.

Lancement d'un changement en bloc de contrôleur 6000

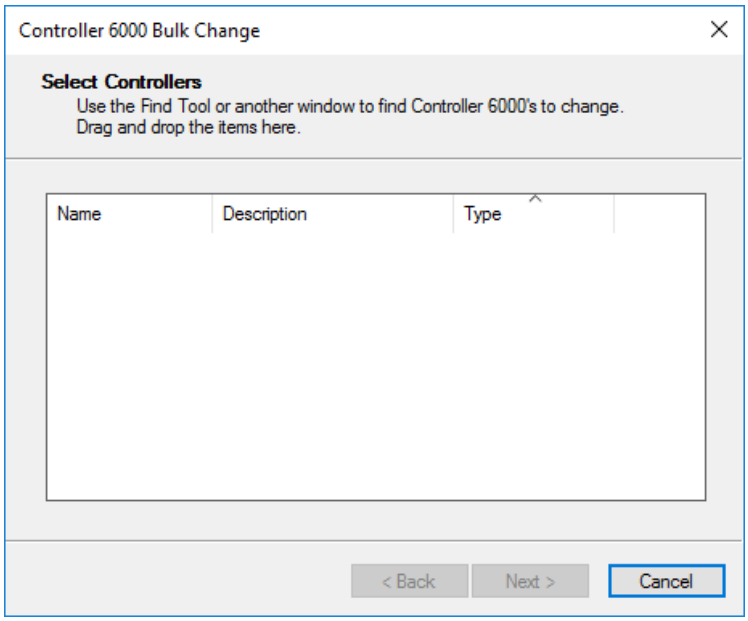
Introduction

Cette procédure décrit comment initier une nouvelle modification en bloc du contrôleur 6000 dans le centre de commandes. Pour exécuter cette procédure, l'opérateur a besoin du privilège "Bulk Change" (Modification en bloc).

Remarque : Il est recommandé de ne **PAS** exécuter plusieurs modifications en bloc de contrôleur à la fois. Cela peut signifier que les modifications en bloc du contrôleur sont exécutées après les heures. Si tel est le cas, il est important que quelqu'un soit sur place lorsqu'il fonctionne au cas où il y a un problème qui doit être résolu.

Procédure (à l'aide de l'assistant)

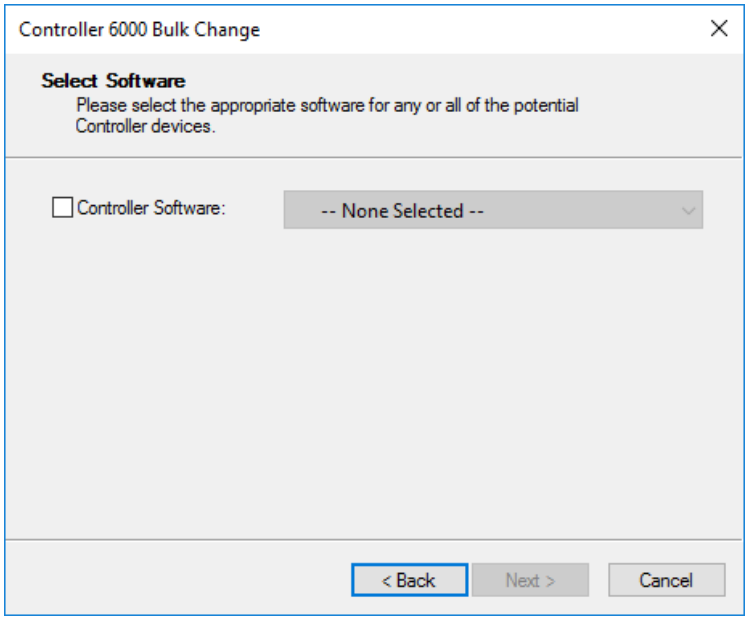
1. Cliquez sur **Gérer** dans la barre de menus, puis sur **Modifications en bloc**.
   La fenêtre Liste principale des modifications en **masse** s'affiche.
2. **Faites un clic droit** et sélectionnez **New...Controller 6000 Bulk Change**.
   L'écran "Sélectionner les contrôleurs" de l'Assistant Modification en bloc du contrôleur 6000 s'affiche.



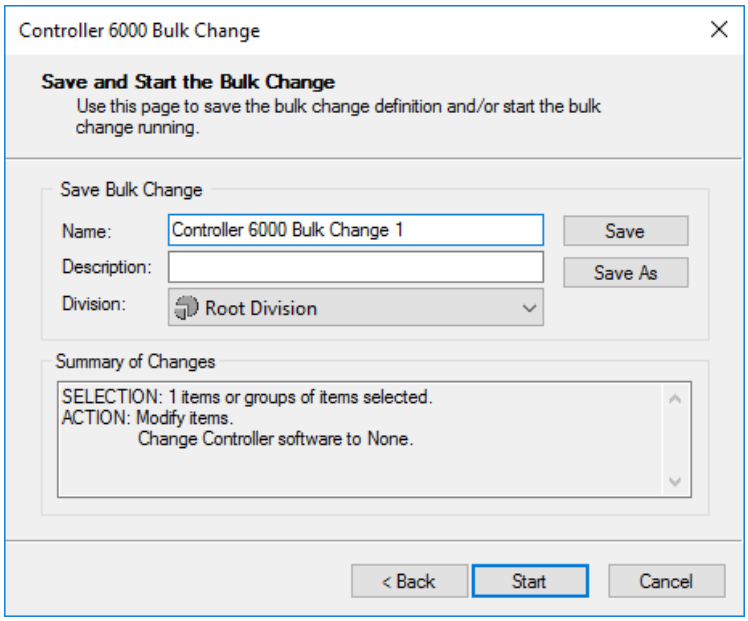
Tous les contrôleurs 6000 qui nécessitent des modifications doivent être placés sur cet écran, en les faisant glisser et en les déposant depuis la fenêtre de liste principale du matériel, ou l'outil de recherche peut être utilisé.
Remarques :

- Seul le contrôleur 6000 peut être placé sur cette grille.
- Jusqu'à 20 Contrôleurs peuvent être modifiés à un moment dans une modification en bloc, donc si le nombre de Contrôleurs dans la grille dépasse 20, le bouton Suivant restera désactivé jusqu'à ce qu'il y ait moins de 20 Contrôleurs dans la grille.

3. Sélectionnez les contrôleurs à modifier (à partir de la fenêtre Liste principale du matériel ou de l'outil de recherche), puis faites-les glisser dans cet écran de l'assistant.
4. Cliquez sur le bouton **Suivant**.
   L'écran "Select Software" (Sélectionner le logiciel) de l'assistant de modification en bloc du contrôleur 6000 s'affiche.



   Si vous cochez la case **Logiciel** du **contrôleur,** le logiciel sera modifié sur le ou les contrôleurs. Il sera possible de changer le logiciel en — None Selected —, qui définira le ou les contrôleurs de sorte qu'ils n'aient pas de logiciel spécifique de ce type, comme s'il avait été choisi à partir de la page de propriétés Controllers **Software**.
5. Cochez la case appropriée et sélectionnez le logiciel dans la liste déroulante si nécessaire.
6. Cliquez sur le bouton **Suivant**.
   L'écran "Enregistrer et démarrer la modification en bloc" de l'assistant de modification en bloc du contrôleur 6000 s'affiche.

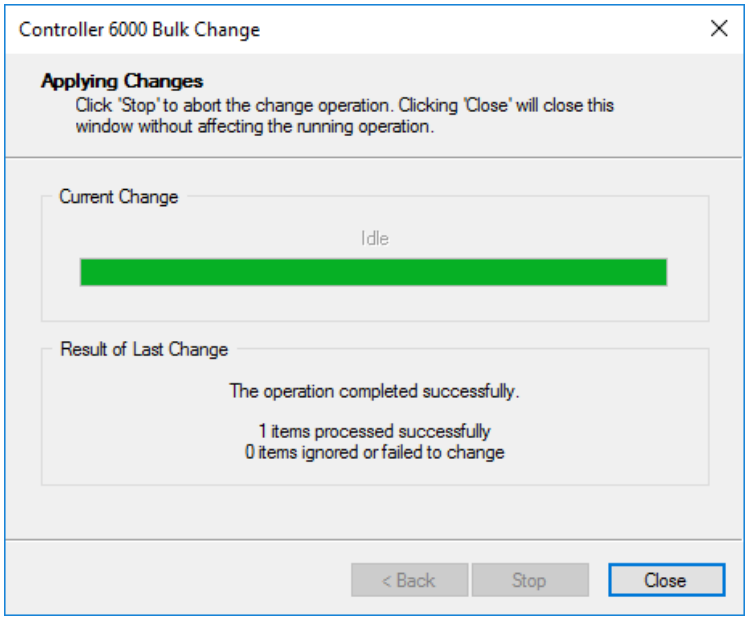


La section **Résumé des modifications** fournit un résumé des modifications que vous devez vérifier avant de continuer.

7. Voulez-vous enregistrer cette modification en bloc et ses paramètres avant de l'exécuter ?

Si...	alors...
non	allez à l'étape 9.
oui	tapez un nom et une description. **Remarque :** Le champ **Nom** est limité à 60 caractères et le champ Description est limité à 200 caractères.

8. Cliquez sur le bouton **Enregistrer**.
   Cette modification en bloc et ses paramètres sont enregistrés et s'affiche désormais dans la fenêtre principale de la liste principale des **modifications en bloc**.
   Remarque : Le bouton **Enregistrer sous** vous permet de modifier une modification en bloc existante et de la réenregistrer sous un nouveau nom. Si vous ouvrez une modification en bloc enregistrée existante et cliquez sur le bouton **Enregistrer sous** sans modifier le nom, un message s'affiche indiquant qu'une modification en bloc portant ce nom existe déjà.
9. Cliquez sur le bouton **Démarrer**.
   L'écran "Application des modifications" de l'Assistant Modification en bloc du contrôleur 6000 s'affiche.



Cet écran affiche la progression de la modification en masse.
Pendant l'affichage de cet écran, la modification en bloc apparaît dans la fenêtre **Bulk Changes** List (Liste principale des **modifications en bloc)** avec un nom généré par le système. En cours de réalisation, l'état de cette modification en bloc s'affichera comme "Actif" dans la **fenêtre Liste principale des** modifications en bloc**, et s'il s'achève avec succès, il s'affichera comme** "Réussi", auquel moment le système la supprimera.

Remarque :
Lorsqu'une modification en bloc du contrôleur 6000 est active ou en cas d'échec, elle reste dans la fenêtre Liste principale des **modifications** en bloc jusqu'à ce qu'un opérateur la supprime.

Résultat

Un changement en bloc du contrôleur 6000 a été initié.
Remarque : Si la modification en bloc a déjà été exécutée avec succès, alors lorsque la modification en bloc est ouverte de nouveau, elle sera par défaut affichée à l'écran Sélectionner le logiciel.

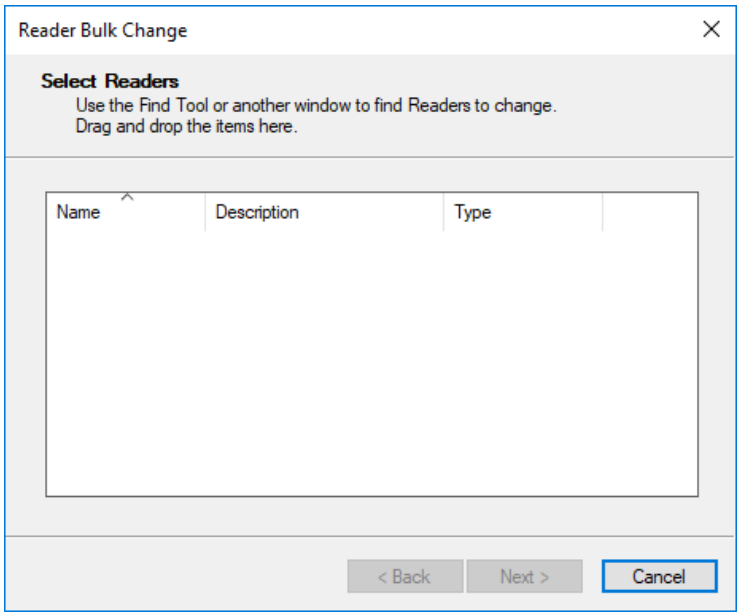
Lancement d'un changement en masse de lecteur

Introduction

Cette procédure décrit comment initier une nouvelle modification en bloc du lecteur dans le Centre de commandes. Un changement en bloc de lecteur peut être effectué pour changer les technologies de carte acceptées aux lecteurs.

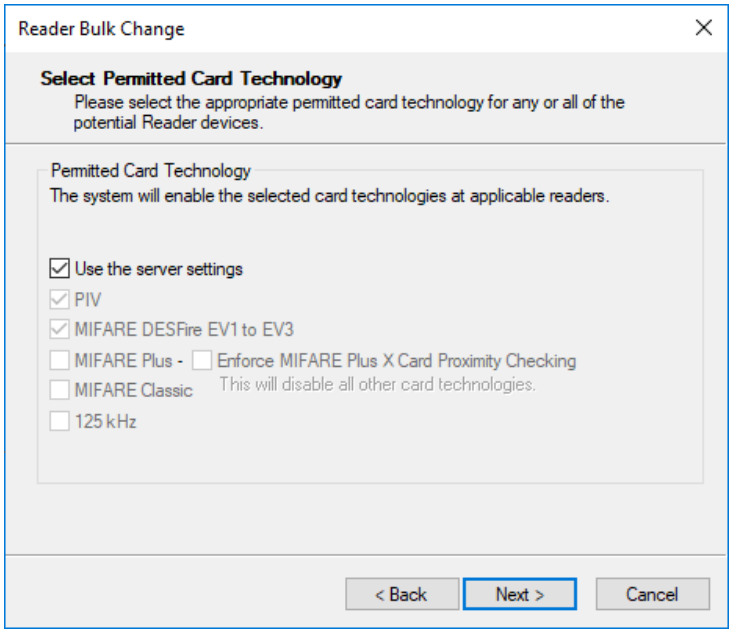
Procédure

1. Cliquez sur **Gérer** dans la barre de menus, puis sur **Modifications en bloc**.
   La fenêtre **Bulk Changes** List (Liste principale des modifications en masse) s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris et **sélectionnez Nouveau... Lecteur Changement en bloc**.
   L'écran "Sélectionner les lecteurs" de l'assistant de modification en bloc du lecteur s'affiche.

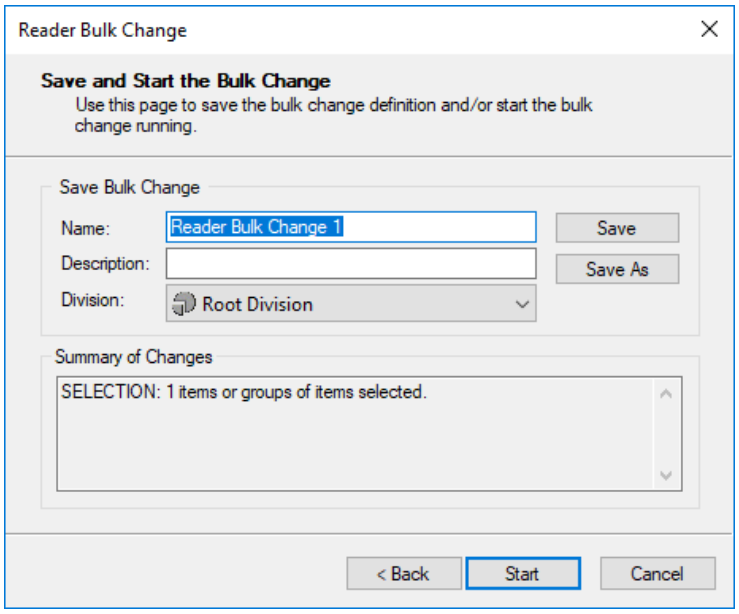


   Tous les lecteurs qui nécessitent des modifications doivent être placés sur cet écran, en les faisant glisser et en les faisant glisser depuis la fenêtre de liste principale appropriée ou l'outil de recherche peut être utilisé.

   Remarque : Vous pouvez utiliser l'outil de recherche pour localiser tous les lecteurs pour lesquels vous souhaitez modifier les technologies de la carte, puis faire glisser les résultats de la recherche sur cet écran. Voir **Exemple 4 : Avancé** (Exemple 4-D) pour plus de détails.
3. Cliquez sur le bouton **Suivant**.
   L'écran "Select Permitted Card Technology" (Sélectionner la technologie de carte autorisée) de l'assistant Reader Bulk Change Wizard s'affiche alors.



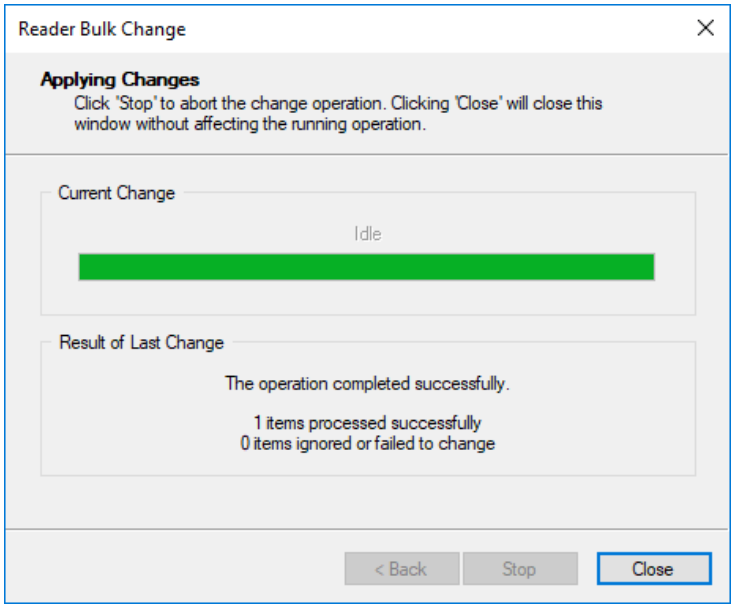
4. Dans la section Permitted Card Technology (Technologie de carte autorisée), **l'option Utiliser les paramètres du serveur** est sélectionnée par défaut. Si vous souhaitez sélectionner d'autres types de cartes à accepter au lecteur, désactivez la case à cocher **Utiliser les paramètres du serveur** et activez les cases à cocher appropriées.
5. Si votre site utilise des cartes MIFARE Plus avec l'ensemble de fonctionnalités « X » et que vous souhaitez empêcher les attaques de relais de se produire sur HBUS, cochez la case **MIFARE Plus** pour activer la case à cocher **Appliquer la vérification de proximité de la carte MIFARE Plus X**.
6. Cochez la case **Appliquer la vérification de proximité de la carte MIFARE Plus X**. Le terminal effectuera des contrôles de proximité lors de la lecture d'une carte MIFARE Plus XLe terminal effectuera des contrôles de proximité lors de la lecture d'une carte MIFARE Plus X.
   Remarques :
   - Si vous cochez cette option, toutes les autres technologies de carte sont désactivées.
   - La fonction de vérification de proximité de la carte MIFARE Plus X ne fonctionnera que si le site qui a émis la carte utilise la même graine de clé MIFARE Plus/DESFire que votre site.
   - Les opérateurs ont besoin du privilège « Modifier le site » pour pouvoir modifier ce paramètre.
7. Cliquez sur le bouton **Suivant**.
   L'écran "Enregistrer et démarrer la modification en bloc" de l'Assistant de modification en bloc du lecteur s'affiche.



8. Voulez-vous enregistrer cette modification en bloc et c'est les paramètres avant l'exécution ?

Si...	alors...
non	allez à l'étape 8.
oui	tapez un nom et une description **Remarque :** Le champ **Nom** est limité à 60 caractères et le champ Description est limité à 200 caractères.

9. Cliquez sur le bouton **Enregistrer**.
   Cette modification en bloc et ses paramètres sont enregistrés et s'affiche désormais dans la fenêtre principale de la liste principale des **modifications en bloc**.
   Remarque : Le bouton **Enregistrer sous** vous permet de modifier une modification en bloc existante et de la réenregistrer sous un nouveau nom. Si vous ouvrez une modification en bloc enregistrée existante et cliquez sur le bouton **Enregistrer sous** sans modifier le nom, un message s'affiche indiquant qu'une modification en bloc portant ce nom existe déjà.
10. Cliquez sur le bouton **Démarrer**.
    L'écran "Application des modifications" de l'Assistant Modification en bloc du lecteur s'affiche.



Cet écran affiche la progression du changement global.
Lorsque cet écran s'affiche, la modification en bloc apparaît dans la fenêtre Liste principale des **modifications en bloc** avec un nom généré par le système. En cours, l'état de cette modification en bloc s'affichera comme "Actif" dans la fenêtre Liste principale des modifications en bloc, et s'il s'achève avec succès, il s'affichera comme "Réussi", à quel moment le système le supprimera.

Remarque : Lorsqu'un changement de lecteur en bloc est actif ou en cas d'échec, il reste dans la fenêtre de liste principale des **modifications** en bloc jusqu'à ce qu'un opérateur le supprime.

Résultat

Un changement massif de lecteurs a été initié, et les lecteurs sélectionnés ont eu les technologies de carte qui sont acceptés à eux changé.

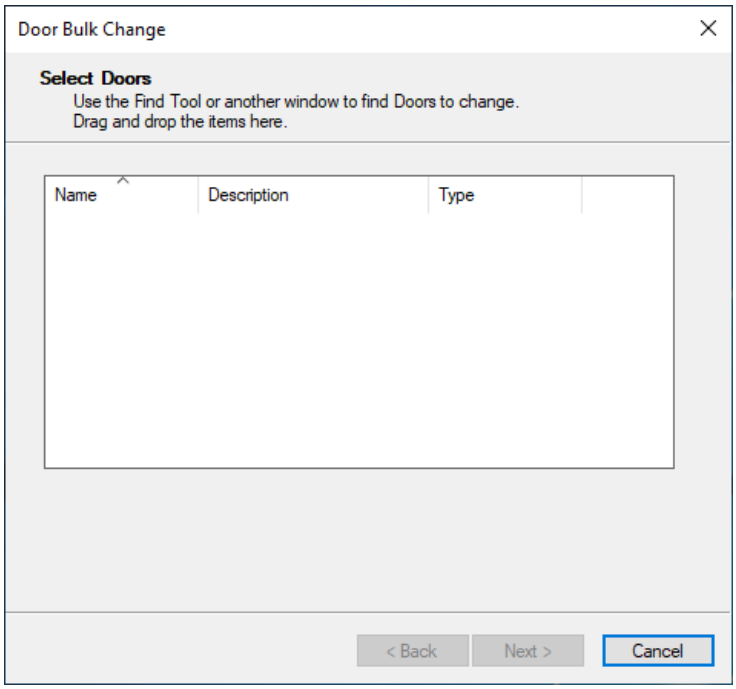
Lancement d'un nouveau changement de porte en bloc

Introduction

Cette procédure décrit comment initier un nouveau changement de porte en bloc dans le Centre de commandes. Un changement de porte en bloc peut être effectué pour modifier les messages d'affichage du terminal personnalisés utilisés pour l'accès accordé, l'accès refusé et l'accès refusé pour l'anti-talonnage/anti-retour à des portes spécifiques.

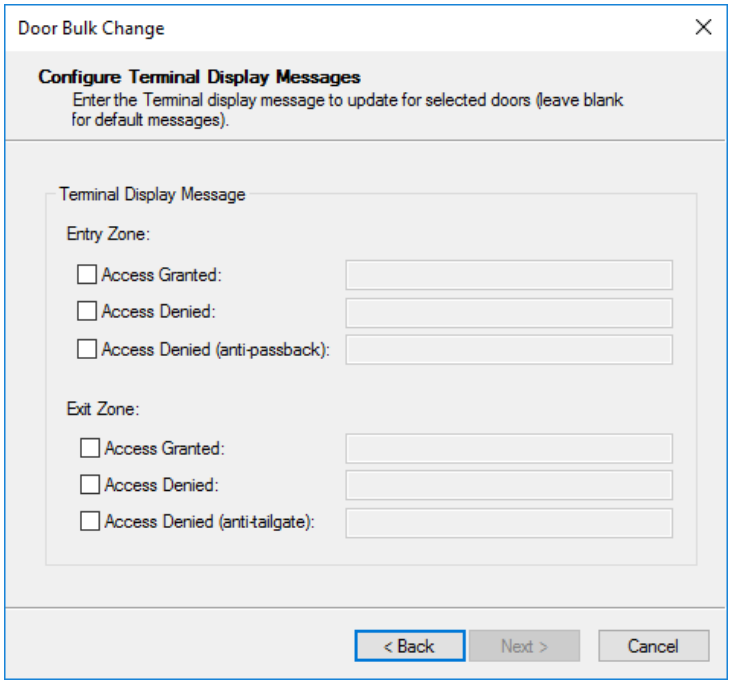
Procédure

1. Cliquez sur **Gérer** dans la barre de menus, puis sur **Modifications en bloc**.
   La fenêtre Modifications en bloc s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris et **sélectionnez Nouveau... Changement de porte en bloc**.
   L'écran "Sélectionner portes" de l'assistant de changement de porte en bloc s'affiche.



   Ajoutez toutes les portes qui nécessitent une modification à cet écran en les faisant glisser depuis la fenêtre Porte ou depuis l'outil de recherche.

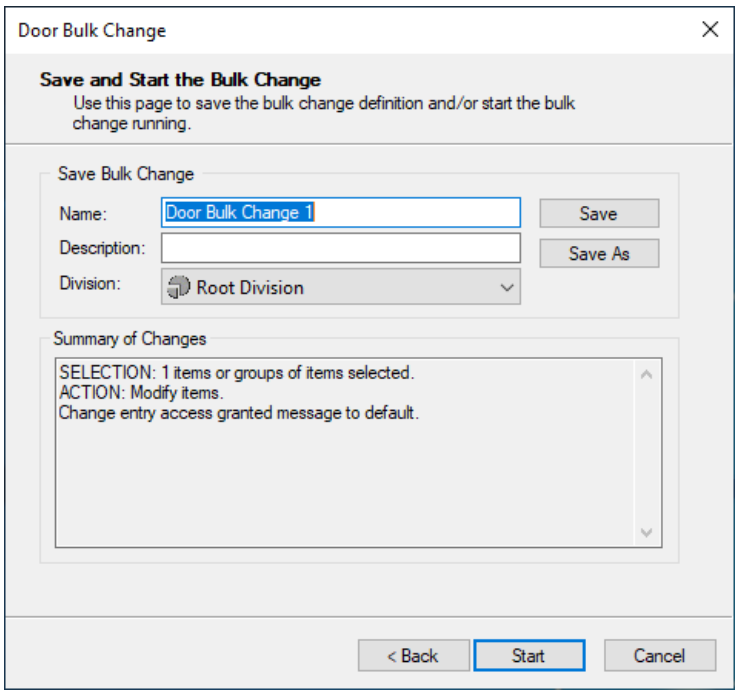
   Remarque : Vous pouvez utiliser l'outil de recherche pour localiser toutes les portes pour lesquelles vous souhaitez modifier les messages d'affichage du terminal, puis faire glisser les résultats de la recherche sur cet écran.
3. Cliquez sur le bouton **Suivant**.
   L'écran "Configurer les messages d'affichage du terminal" de l'Assistant Modificat ion en bloc de la porte s'affiche.



4. Définissez les messages des zones d'accès en entrée et en sortie pour tous les terminaux HBUS utilisés par les portes que vous avez sélectionnées pour ce changement en bloc.

   Remarque : Pour réinitialiser un message d'accès au message par défaut, activez l a case à cocher et laissez le champ de texte vide.

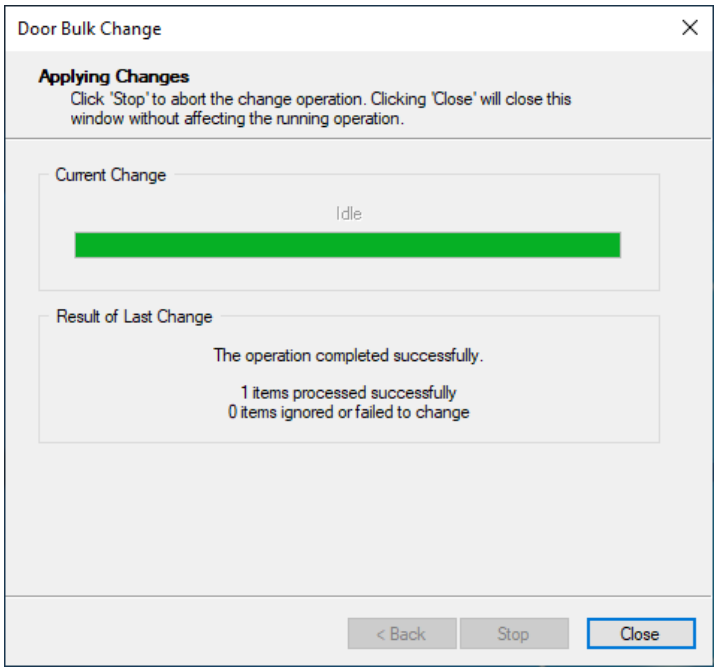
5. Cliquez sur le bouton **Suivant**.
   L'écran "Enregistrer et démarrer la modification en bloc" de l'assistant de modific ation en bloc de porte s'affiche.



6. Voulez- vous enregistrer cette modification en bloc et ses paramètres avant de l'exécuter ?

Si...	alors...
non	allez à l'étape 8.
oui	tapez un nom et une description **Remarque :** Le champ **Nom** est limité à 60 caractères et le champ Description est limité à 200 caractères.

7. Cliquez sur le bouton **Enregistrer**.
   Cette modification en bloc et ses paramètres sont enregistrés et s'affiche mainte nant dans la fenêtre Modifications en bloc.
   Remarque : Le bouton Enregistrer sous vous permet de modifier une modificatio nen bloc existante et de la réenregistrer sous un nouveau nom. Si vous ouvrez un e modification en bloc enregistrée existante et cliquez sur le bouton Enregistrer s ous sans modifier le nom, un message s'affiche indiquant qu'une modification en bloc portant ce nom existe déjà.
8. Cliquez sur le bouton **Démarrer**.
   L'écran "Application des modifications" de l'assistant de modification en bloc de porte s'affiche.



   Cet écran montre la progression de la modification en bloc.
   Si vous n'avez pas choisi d'enregistrer cette modification en bloc, la modification en bloc apparaît dans la fenêtre Modifications en bloc avec un nom généré par le système en cours. Le changement en bloc en cours aura un 'Actif' dans la fenêtre Modifications en bloc. S'il se termine correctement, il va brièvement afficher "Réussie", puis le système va le supprimer.
   Remarque : Lorsqu'une modification en bloc de porte est active ou en cas d'échec, elle reste dans la fenêtre Modifications en bloc jusqu'à ce qu'un opérateur la supprime.

Résultat

Un changement de porte en bloc a été effectué et les messages d'affichage de terminal des portes sélectionnées ont été modifiés.

Chapitre 39 : Rapports

Le Centre de commandes vous permet de créer et d'imprimer une sélection d'états, répertoriée ci-dessous, à condition que vous disposiez des privilèges d'opérateur appropriés (voir ***Privilèges d'opérateur à la*** page 37-1 pour vérifier) :

- Rapport du titulaire de carte (client de configuration)
- Rapport d'activité (client de configuration)
- Rapport d'évacuation (client de configuration)
- Rapport groupe d'accès
- Rapport d'accès
- Rapport des exceptions
- Rapport de présence et de temps (client de configuration)
- Rapport de configuration de site
- Rapport d'affectation Contact ID
- Rapport de tension
  Remarque : Le rapport de tension ne sera disponible dans la liste déroulante des types de rapport (à partir de la fenêtre Liste principale de **description de rapport**) que si votre site est sous licence pour les contrôleurs de clôture. Pour plus de détails, consultez ***Création d'un rapport de tension (client de configuration)*** (page 49-40).
- Rapport de câblage
- Rapport de visite
  Remarque : Le rapport de visite guidée de la Garde ne sera disponible dans la liste déroulante des types de rapport (à partir de la fenêtre de la liste principale de la **description du rapport**) que si votre site est autorisé à effectuer des visites guidées de la Garde. Pour plus de détails, consultez Création d'un rapport de visite de garde.
- Rapport de température
  Remarque : Le rapport de température ne sera disponible dans la liste déroulante des types de rapport (à partir de la fenêtre Liste principale de **description de rapport**) que si votre site est autorisé pour les contrôleurs de clôture F22. Pour de plus amples détails, voir ***Créer un rapport de température*** (page 49-42).

Lorsque vous créez un rapport, un Assistant s'affiche pour vous permettre de spécifier les informations particulières que vous souhaitez inclure dans l'état et l'endroit où l'état doit être imprimé.
Remarque : Les rapports qui permettent la sélection des titulaires de carte en tant que critères appuient uniquement la sélection de 10 000 détenteurs de carte au maximum.
La fenêtre **Description de l'état** - Liste principale est l'endroit où vous lancez la gestion de vos états.

Creating a new report

Introduction

La création d'un nouveau rapport est simple à l'aide de l'Assistant Rapports. Vous passez en revue le processus de création de rapports à l'aide du bouton **Suivant** pour accéder à chaque page de l'Assistant, accepter les paramètres/valeurs par défaut ou faire des choix personnalisés. À tout moment, vous pouvez effectuer un retour arrière via le bouton **Précédent** ou arrêter le processus de génération de rapports en choisissant le bouton **Annuler** (qui quitte également l'assistant sans proposer d'enregistrer les modifications).

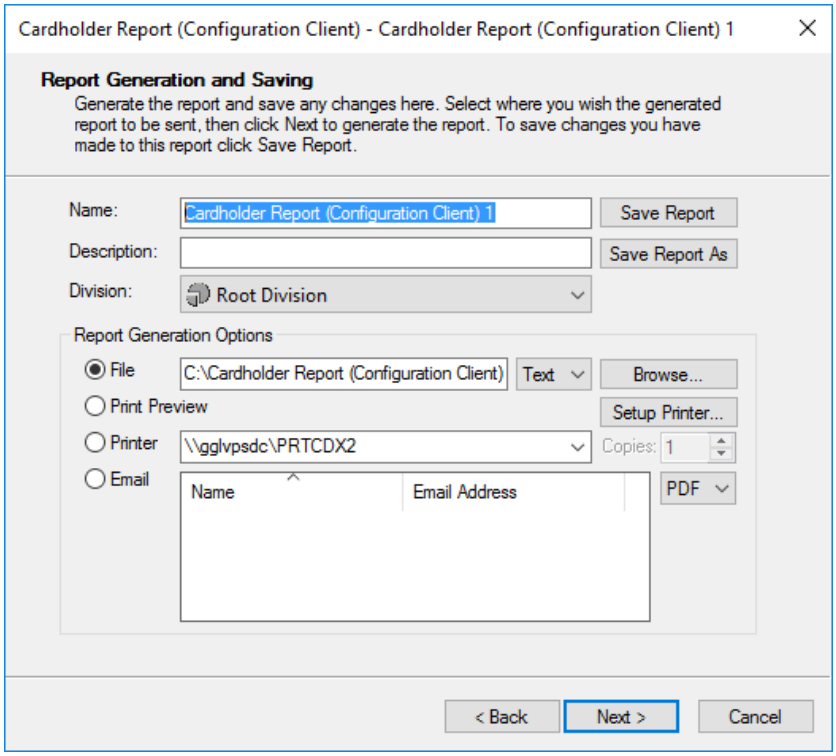
Les informations affichées lors de l'exécution de l'Assistant Rapport varient en fonction du type de rapport que vous créez.

Vous avez la possibilité d'enregistrer le rapport. Cela signifie qu'il est disponible dans la fenêtre **Description du** rapport Liste pour être utilisé à plusieurs reprises.

Procédure

1. Cliquez sur **Rapport dans** la barre de menus, puis sur **Rapport Descriptions**.
   La **fenêtre Description** de l'état Liste s'ouvre (en mode grille). **Remarque :** Tous les rapports que votre site a configurés sont affichés dans cette fenêtre.
2. Cliquez avec le bouton droit de la souris et sélectionnez Nouveau.
3. Dans le sous-menu affiché, sélectionnez le **type de rapport** que vous souhaitez créer.
4. Le premier écran de l'assistant de rapport approprié s'affiche.
   Cliquez sur les **touches** Suivant **et** Précédent **pour** parcourir l'assistant.
5. Reportez-vous à la rubrique pertinente pour plus de détails sur le type de rapport particulier vous avez sélectionné.
   Remarque : Les rapports avec "(Configuration Client)" après le nom indiquent qu'il existe un rapport équivalent dans le client du centre de commande. ***Rapport du titulaire de carte (client de configuration)*** (page 39-7)
   Rapport d'activité (client de configuration) (page 39-15)
   Rapport d'évacuation (client de configuration) (page 39-23)
   Rapport du groupe d'accès (page 39-31)
   Rapport d'accès (page 39-33)
   Rapport d'exception (page 39-35)
   Rapport sur le temps et la présence (client de configuration) (page 39-40)
   Rapport de configuration du site (page 39-55)
   Rapport d'attribution des identifiants de contact (page 39-58)
   Rapport de câblage (page 39-61)

Génération et enregistrement de rapports



La dernière page de l'Assistant (pour tous les types de rapport) est intitulée "Génération et enregistrement de rapports".
Remarque : La section "Options de génération de rapports" de cette page diffère légèrement de celle affichée pour certains types de rapports :

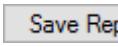
- Les *rapports Access* disposent d'une zone de liste déroulante pour sélectionner un type de fichier en regard de l'option **Fichier**.
- *Les rapports des titulaires de carte, des activités, des évacuations et des exceptions comportent une* zone *déroulante* permettant de sélectionner un type de fichier à côté de l'**option Fichier** et ils disposent également d'une option de sortie de courrier électronique supplémentaire.

6. Tapez le nom de l'état.
7. Tapez la **description** du rapport. Par exemple, vous pouvez mentionner que le rapport est imprimé à l'écran.
8. Sélectionnez la **division** dans la liste déroulante dans laquelle vous souhaitez enregistrer l'état (c'est-à-dire que seuls les opérateurs ayant accès à la division que vous sélectionnez pourront voir l'état).
9. Cliquez sur la case d'option correspondant à l'endroit où vous souhaitez que le rapport soit généré :

Cliquez sur la...	**à...**
◉ File case d'option	enregistrer les informations **dans un fichier**, et taper l'emplacement et le nom du fichier. Vous pouvez également cliquer sur le bouton **Parcourir** pour sélectionner les chemins d'accès

Cliquez sur la...	à...
	aux répertoires existants saisissez le nom du fichier. **Remarque :** Lorsque les rapports sont enregistrés dans un fichier, ils sont enregistrés sous forme de fichiers **texte** à l'exception des éléments suivants : • Access Reports, car il existe l'option permettant d'enregistrer ces rapports en tant que types de fichiers **texte** ou **XML**. **La** sortie **XML** vous permet d'analyser les données à l'aide d'une variété d'outils (par exemple Excel 2003). • Rapports des titulaires de carte, des activités, des évacuations et des exceptions, car il existe l'option d'enregistrer ces derniers sous forme de types de fichiers **texte** ou **PDF**.
Print Preview case d'option	afficher un aperçu des informations **à l'écran**.
Printer case d'option	imprimez les informations sur l'**imprimante** sélectionnée et sélectionnez une imprimante dans la liste déroulante des imprimantes disponibles ou tapez le nom de l'imprimante.xsql. **Remarques :** • Dans le cas des rapports d'évacuation automatique, si l'opérateur n'a pas accès à l'imprimante sur laquelle le rapport doit être imprimé, il n'apparaîtra pas dans la liste des imprimantes disponibles. À la place, l'opérateur peut taper le chemin d'accès à l'imprimante, auquel cas les boutons **Configurer** l'**imprimante** et **Suivant** deviennent désactivés. Les rapports d'évacuation automatique sont exécutés via le serveur, de sorte qu'ils ne peuvent pas être testés à partir de postes de travail individuels. • Via le bouton **Setup Printer (Configurer l'imprimante)** vous pouvez définir des informations sur l'imprimante (par exemple ; format de papier et orientation du papier). L'orientation du papier par défaut pour les rapports est Portrait. Vous pouvez toutefois modifier l'orientation du rapport, ce qui peut être utile pour les noms longs (par exemple, les noms des titulaires de carte dans le rapport d'évacuation). Voir ***Personnalisation des impressions de rapports*** (page 39-75) si vous souhaitez produire un rapport de cette façon.

Cliquez sur la...	à...
	• Par défaut, une seule copie du rapport va imprimer sur l'imprimante, mais vous pouvez définir ce montant sur un autre montant si vous avez besoin de copies supplémentaires.
 case d'option **Remarque :** Cette option n'est disponible que dans les rapports des titulaires de carte, des activités, des évacuations et des exceptions.	sélectionnez les titulaires de carte pour lesquels le rapport doit être envoyé par courrier électronique, en les faisant glisser et en les déposant dans la grille, et en sélectionnant le type de fichier approprié pour le rapport (c'est-à-dire **Texte** ou PDF). **Remarques** : • Si un détenteur de carte sélectionné a plusieurs adresses de messagerie, la "première" s'affiche, avec la chaîne ", ..." (indiquant qu'il en a plus d'une). • Si un détenteur de carte sélectionné n'a pas d'adresse de messagerie, un message d'avertissement s'affiche lorsque **vous cliquez sur le bouton Suivant**. • Les adresses e-mail s'affichent ici en lecture seule.

10. Pour enregistrer ce rapport et ses paramètres, cliquez sur le **bouton Enregistrer le rapport** .
    Cet état s'affiche désormais dans la fenêtre **Description de l'état**, et le bouton **Enregistrer l'état** devient désactivé et passe à **État enregistré**.
    Remarque : Lorsqu'un opérateur imprime un état existant à partir de la fenêtre Liste principale de la **description des états** (c'est-à-dire un état enregistré), de nouvelles données sont extraites, car seule la requête a été enregistrée.

    Le bouton Enregistrer le rapport sous permet d'enregistrer plusieurs rapports  à l'aide de la fenêtre de l'assistant.
    En ouvrant un état enregistré existant et en cliquant sur le bouton **Enregistrer l'état sous**, le nouvel état s'affiche dans la fenêtre Liste principale de la **description de l'état** ainsi que l'état d'origine.

    Remarque : Si vous ouvrez un rapport enregistré existant et que vous cliquez sur le bouton **Enregistrer le rapport sous** sans modifier le nom du rapport, un message s'affiche pour indiquer que le rapport existe déjà et vous demander si vous souhaitez le remplacer. En cliquant sur **Oui, le rapport d'origine est remplacé et en cliquant sur Non, vous revenez à la** page "Génération et enregistrement du rapport", ce qui vous permet de modifier le nom du fichier pour le rapport.

11. Cliquez sur le bouton **Suivant**.
    Une fenêtre **Progression de la génération de rapports** s'affiche. Cela fournit des commentaires à l'opérateur pendant que les données sont récupérées du serveur et formatées. Un opérateur peut choisir d'annuler l'état en sélectionnant l'option **Annuler ou Précédent** s'affiche. Aucune autre fonctionnalité n'est disponible sur

cette page.
Remarques :

- La génération de rapports plus longs prend plus de temps.
- Deux rapports qui accèdent aux mêmes fichiers d'archive peuvent être exécutés simultanément. Cela peut être fait sur deux stations de travail distinctes, ou sur le même PC exécutant deux stations de travail.
- Vous pouvez recevoir le message d'erreur suivant lors de la restauration des fichiers :
  "La connexion au chemin d'accès spécifié <chemin d'accès> a échoué. Veuillez vérifier *:*
  - vous avez correctement entré le chemin
  - ‘e compte d'utilisateur de l'outil d'archivage dispose des autorisations appropriées pour utiliser cette ressource réseau."
  Si tel est le cas, vous devez demander à l'administrateur système qui a configuré vos archives de vérifier que le compte d'utilisateur dispose de privilèges suffisants.

12. Cliquez sur le bouton **Terminer (Finish)**.

Résultat

Le rapport est généré et envoyé à la destination spécifiée (imprimante, à l'écran ou enregistré dans un fichier).

Indication

Suppression des rapports existants
Reportez-vous à ***Suppression d'éléments*** (page 3-27) pour la procédure de suppression d'un rapport existant.

Rapports uniques
Vous devrez peut-être créer un rapport unique et l'imprimer. Comme le rapport n'est plus requis, **ne** cliquez **pas** sur le bouton "Enregistrer le rapport". Le rapport sera imprimé mais ne sera pas enregistré.

Rapport du titulaire de carte

Introduction

Le rapport du titulaire de carte permet à l'opérateur d'imprimer une liste des informations du titulaire de carte. L'opérateur spécifie un style de rapport (c'est-à-dire détaillé ou résumé) et un ensemble de détenteurs de cartes.

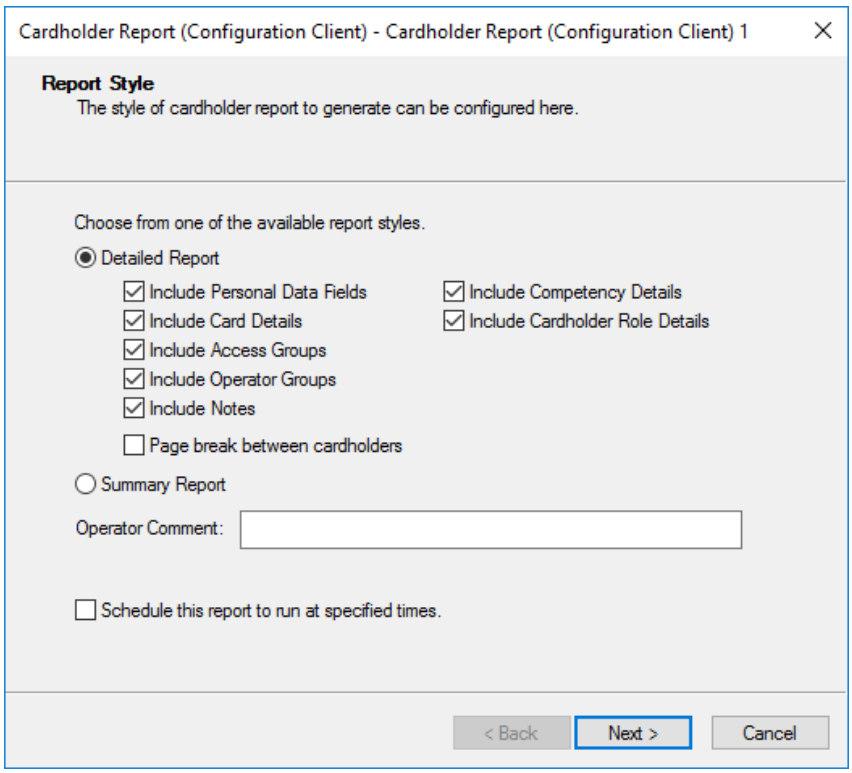
Les opérateurs doivent disposer des privilèges "Afficher les titulaires de carte" et "Modifier les descriptions de rapport" pour créer, enregistrer, modifier et supprimer les rapports des titulaires de carte.

Ce rapport peut être planifié pour s'exécuter automatiquement à des heures régulières (via des plans d'action ou des macros planifiées). Pour plus d'informations, reportez-vous à la section ***Automatic Generated Reports*** (on page 39-63) et ***Configuring Report Scheduling*** (on page 39-65).

Assistant Rapport

L'assistant Rapport des titulaires de carte contient un certain nombre de pages qui vous invitent à entrer certaines informations pour créer un rapport.
Suivez les instructions affichées.

page Style de rapport



Il s'agit de la première page de l'Assistant Rapport du titulaire de carte. Il permet à l'opérateur de sélectionner une version **détaillée** ou récapitulative de l'état.

Les **rapports détaillés** incluent le nom du titulaire de la carte, la date de création et de dernière modification, l'opérateur qui les a modifiés pour la dernière fois et éventuellement une ou plusieurs des informations suivantes :

- Champs de données personnelles
- Détails de la carte (inclut le statut de la carte, c'est-à-dire si les cartes sont actives ou non)
- Groupes d'accès
  Remarque : Si vous incluez les groupes d'accès, pour chaque groupe d'accès auquel appartient un titulaire de carte, l'état affichera les dates/heures de début et de fin de leur appartenance temporaire au groupe d'accès. S'ils restent vierges dans le rapport, le titulaire de la carte est un membre permanent du groupe d'accès. Les enregistrements d'adhésion temporaires qui ont expiré, mais qui n'ont pas été supprimés du système, apparaîtront également dans le rapport.
- Groupes d'opérateurs
- Notes, (c'est-à-dire entrées enregistrées sur l'**onglet** Notes d'un titulaire de carte).
- Détails des compétences
  Remarque : Si vous voulez inclure des détails sur les compétences des titulaires de carte dans le rapport, consultez ***Déclaration des compétences des titulaires de carte*** (à la page 53-20) pour plus de détails.
- Détails du rôle du titulaire de la carte
  Remarque : La sélection de cette option permet de répertorier les détenteurs de carte qui remplissent chaque rôle défini pour chaque détenteur de carte sélectionné dans le rapport. Il ne montrera pas la relation du point de vue du titulaire de la carte mère (c'est-à-dire qu'il ne montrera pas à tous les titulaires de la carte qu'un titulaire de la carte est "responsable"). Seul un **rapport** sommaire indiquera la relation directionnelle "responsable".

Remarques :

- Si votre site est sous licence pour l'intégration biométrique, **Cochez la case Inclure les détails biométriques (Include Biometric Details)**, qui peut être désactivée/activée selon les besoins.
- Si votre site est sous licence pour la fonctionnalité Notifications, il y aura également une case à cocher **Inclure les détails de la notification**, qui peut être désactivée/activée au besoin.
- **Des** rapports **détaillés** sur les 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 à partir d'un titulaire de carte*** (page 32-30) pour plus de détails.

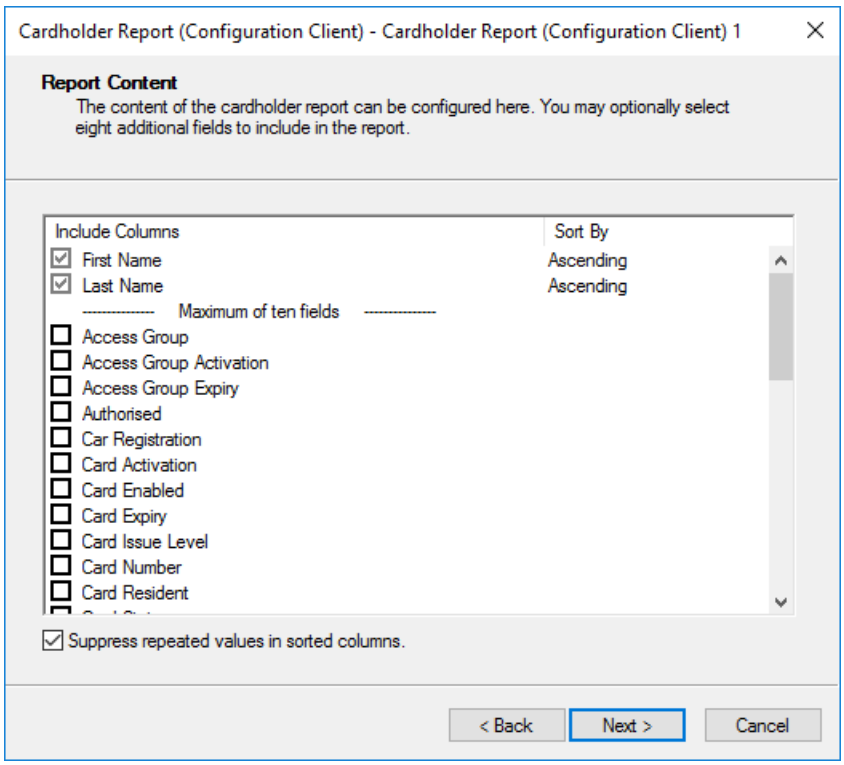
Le rapport détaillé peut être configuré pour démarrer chaque titulaire de carte sur une nouvelle page. L'ordre de tri du rapport est fixé aux derniers et aux premiers noms du titulaire de la carte.

Les rapports de synthèse ne fournissent aucune option supplémentaire sur la première page de l'assistant. Les paramètres de configuration du rapport de synthèse sont inclus dans la page de l'Assistant suivante.

Un **commentaire d'opérateur** peut être entré pour les deux styles de rapport, qui seront affichés dans l'en-tête principal du rapport. Les commentaires sont limités à un maximum de 200 caractères.

Vous pouvez éventuellement planifier l'exécution de ce rapport à des heures spécifiées pour les deux styles de rapport.

page Contenu du rapport



Cette page s'affiche uniquement si le style de rapport récapitulatif est sélectionné. **Remarque :** Si l'option Rapport détaillé est sélectionnée, l'assistant se déplace directement vers la page **Sélectionner les titulaires et les opérateurs de carte**.

Le rapport sommaire comprend toujours le prénom et le nom du titulaire de la carte, mais en plus de cela, l'exploitant peut sélectionner jusqu'à huit champs de titulaire de carte supplémentaires (en les marquant d'une coche), à partir de la liste fournie.
Remarques :

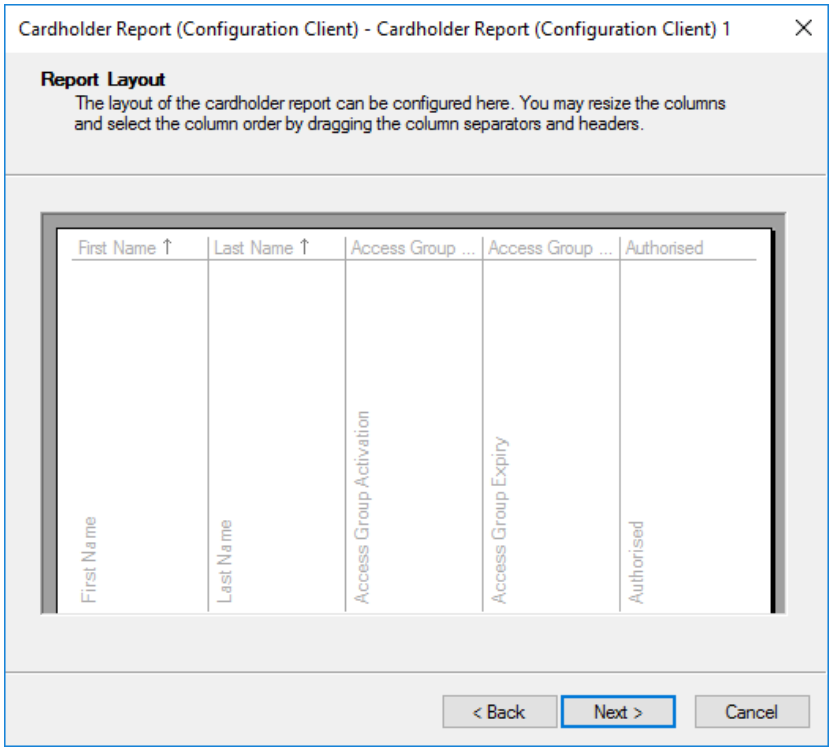
- Deux options disponibles dans la liste sont "Activation du groupe d'accès" et "Expiration du groupe d'accès". En les sélectionnant, votre rapport affichera les dates/heures de début et de fin de l'adhésion temporaire d'un titulaire de carte au groupe d'accès (Access Group). Si ces colonnes restent vides dans l'état, le titulaire de la carte est un membre permanent du groupe d'accès.
  Les enregistrements d'adhésion temporaires qui ont expiré, mais qui n'ont pas été supprimés du système, apparaîtront également dans le rapport.
- L'une des options disponibles dans cette liste est "Code utilisateur". C'est la seule façon que vous pouvez filtrer sur qui a un code utilisateur, mais les codes réels ne seront pas divulgué dans le rapport.

L'ordre des informations du rapport de synthèse peut être contrôlé par la définition

d'options de tri par rapport à un ou plusieurs des champs affichés. Un champ peut être trié dans l'ordre croissant ou décroissant, ou aucune option de tri n'est appliquée.

Cochez la case Supprimer les valeurs répétées dans les colonnes triées pour contrôler la façon dont l'état affichera les valeurs répétées dans votre état des détenteurs de carte récapitulative (par exemple, dans un état qui affiche Groupe d'accès comme première colonne, il affiche des groupes d'accès uniques comme en-têtes sans répéter le nom du groupe d'accès sur chaque ligne).

page Présentation du rapport



Cette page permet à l'opérateur de configurer la disposition de l'état.

Vous pouvez déterminer la position des colonnes horizontalement sur la page, comme suit :

1. Déplacez le pointeur de la souris sur l'en-tête de colonne à repositionner.
   Le pointeur de la souris se transforme en symbole d'une main.
2. Cliquez et maintenez le bouton de la souris enfoncé.
   La main change et s'accroche.
3. Déplacez la main (et donc l'en-tête de colonne) vers la nouvelle position souhaitée.
4. Relâchez le bouton de la souris.

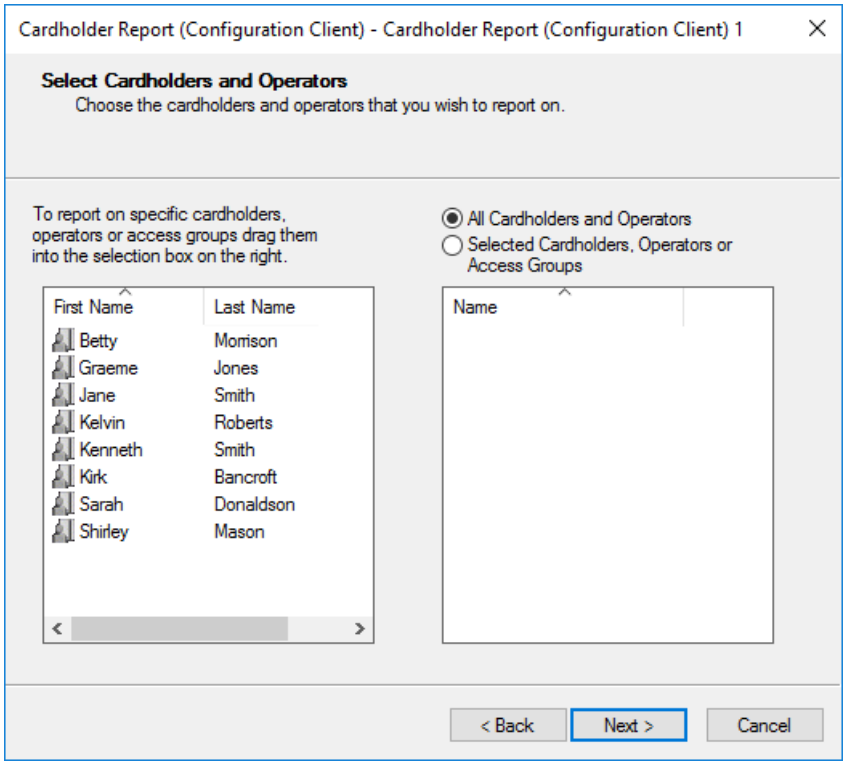
Vous pouvez également redimensionner la largeur des colonnes comme suit :

1. Déplacez le pointeur de la souris sur un séparateur de colonnes.
2. 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.

Remarque : Si les détails de la **carte**, du **groupe d'accès** ou du **groupe d'**opérateurs sont inclus comme la première colonne de l'état, les noms des titulaires de carte qui sont membres de plusieurs groupes ou qui ont plusieurs cartes apparaîtront plus d'une fois dans l'état. Alternativement, si le nom du titulaire de carte est la première colonne, alors le nom du titulaire de carte n'apparaîtra qu'une seule fois même s'il a plusieurs **cartes, groupes d'accès** ou **groupes d'opérateurs**.

page Sélectionner les titulaires de carte et les opérateurs

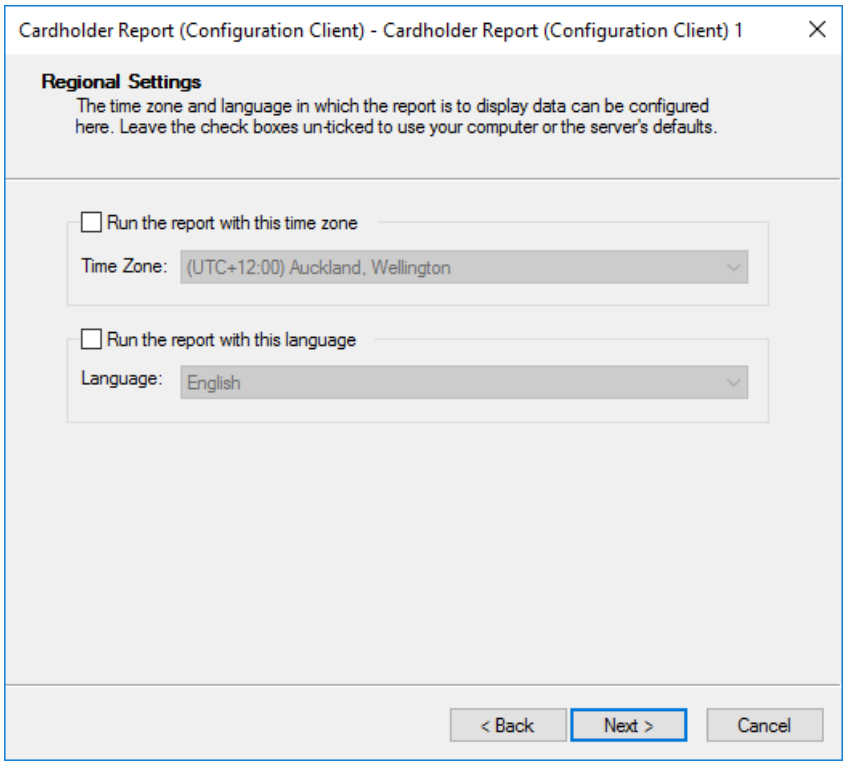


Cette page fournit une liste des titulaires de carte qu'un exploitant peut inclure dans la déclaration. Les titulaires de carte indiqués ici sont limités à ceux qui relèvent de la division de l'exploitant.

L'outil de recherche peut être utilisé pour localiser les détenteurs de cartes, 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.
Remarque : Seuls les détenteurs de carte qui sont actuellement actifs dans un groupe d'accès seront signalés. Par conséquent, si vous souhaitez que l'état inclue les membres "expirés" du groupe d'accès, vous devez sélectionner les détenteurs de carte plutôt que les groupes d'accès.
La "suppression automatique des membres expirés" des groupes d'accès modifie les informations dans l'état en fonction de l'exécution de l'état.

Si vous souhaitez supprimer un titulaire de carte ou un groupe d'accès de votre liste à droite, **cliquez** avec le bouton **droit** sur l'élément et cliquez sur **Supprimer de la liste**.

page Paramètres régionaux

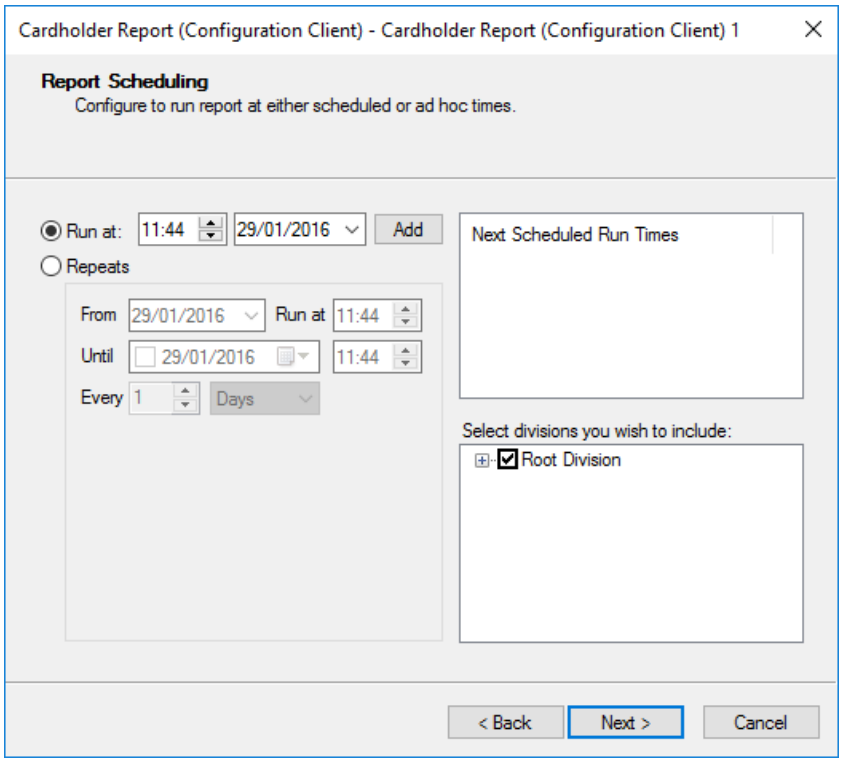


Cette page permet de sélectionner un fuseau horaire et/ou une langue pour le rapport. Ces options sont spécifiquement fournies pour prendre en charge le rapport du titulaire de carte (c'est-à-dire lorsque le rapport est exécuté via une macro sur le serveur). La sélection d'un fuseau horaire est facultative, 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, lors de l'exécution du rapport, toutes les dates et heures du rapport s'affichent dans le fuseau horaire sélectionné. Toutes les dates et heures configurées dans le rapport sont supposées être comprises dans le fuseau horaire sélectionné (plutôt que le fuseau horaire sur le poste de travail de l'opérateur de configuration).

page horaire de rapport



Cette page s'affiche uniquement si la case à cocher "Planifier l'exécution de ce rapport aux heures spécifiées" est activée sur la page **Style de rapport**. Il permet de définir les temps d'exécution et les propriétés de répétition pour le rapport. Plusieurs heures explicites d'exécution du rapport peuvent être configurées comme suit :

1. Cliquez sur le bouton d'option **Exécuter à (Run at)**.
2. Entrez une date et une heure et cliquez sur le bouton **Ajouter**.
   La date et l'heure s'affichent dans la **grille Heures d'exécution programmée suivantes**.
3. Répétez les étapes 1 à 2 pour chaque heure explicite.
   Remarque : Si vous cliquez sur le bouton radio Répéter, les ajouts explicites sont supprimés de la **grille Next Scheduled Run Times**.

Les heures de répétition du rapport à exécuter peuvent être configurées comme suit:

1. Cliquez sur le bouton d'option **Répéter (Repeats)**.
2. Sélectionnez la date et l'heure **de début** '**initiale**'.
3. Sélectionnez une date et une heure de fin si nécessaire.
   Remarque : Si aucune **date** Jusqu'à n'est entrée, le rapport se répétera indéfiniment.
4. Sélectionnez la régularité du rapport à exécuter, (c'est-à-dire **Tous** les **Heures**, **jours**, **semaines** ou **mois)**.
   Remarque : Lorsque **Semaines** est sélectionné dans la liste déroulante, les jours de la semaine s'affichent avec la possibilité de sélectionner un ou plusieurs jours (par exemple, lundi et jeudi).

Les cinq dates et heures suivantes apparaissent dans les **heures d'exécution programmées suivante** grille.

La grille de sélection de la **division** permet de programmer le rapport pour des divisions spécifiques.
Remarque : Seules les divisions pour lesquelles vous disposez du privilège de modification approprié apparaissent dans la liste.

page Génération et enregistrement de rapports

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*** (page 39-3) dans la procédure *Création d'un nouveau rapport* pour plus de détails.

Rapport d'activité

Introduction

Le rapport d'activité est un outil qui permet de signaler exactement ce qui s'est passé dans le système. Il s'agit d'un outil de requête qui ne devrait pas être utilisé pour imprimer des rapports réguliers à des fins de dépôt.

Ce rapport peut être planifié pour s'exécuter automatiquement à des heures régulières (via des plans d'action ou des macros planifiées). Pour plus d'informations, reportez-vous à la section ***Automatic Generated Reports*** (page 39-63) et ***Configuring Report Scheduling*** (page 39-65).

Remarque : Dans un environnement multi-serveur, pour tout serveur donné où l'agrégation d'événements est activée, un opérateur peut exécuter un rapport d'activité qui incorpore des événements provenant d'éléments de site distant. Le rapport d'activité peut être filtré par éléments du site distant.

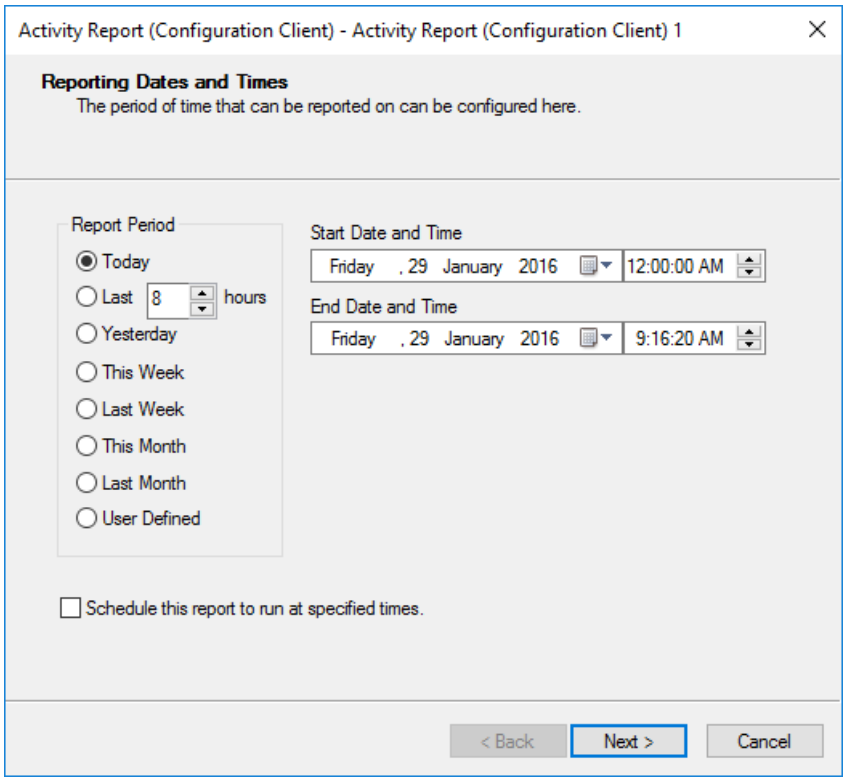
Privilèges d'opérateur

Privilège (s)	est nécessaire pour...
"Modifier la description du rapport" et "Afficher les événements et les alarmes" ou "Modifier les alarmes"	créer, afficher, modifier, imprimer, enregistrer et supprimer des rapports d'activité.
"Afficher les événements et les alarmes" ou "Modifier les alarmes"	créer, afficher, modifier et imprimer des rapports d'activité.

Assistant Rapport

L'Assistant Rapport d'activité contient un certain nombre de pages qui vous invitent à entrer certaines informations pour créer un rapport.
Suivez les instructions affichées.

page Dates et heures du rapport



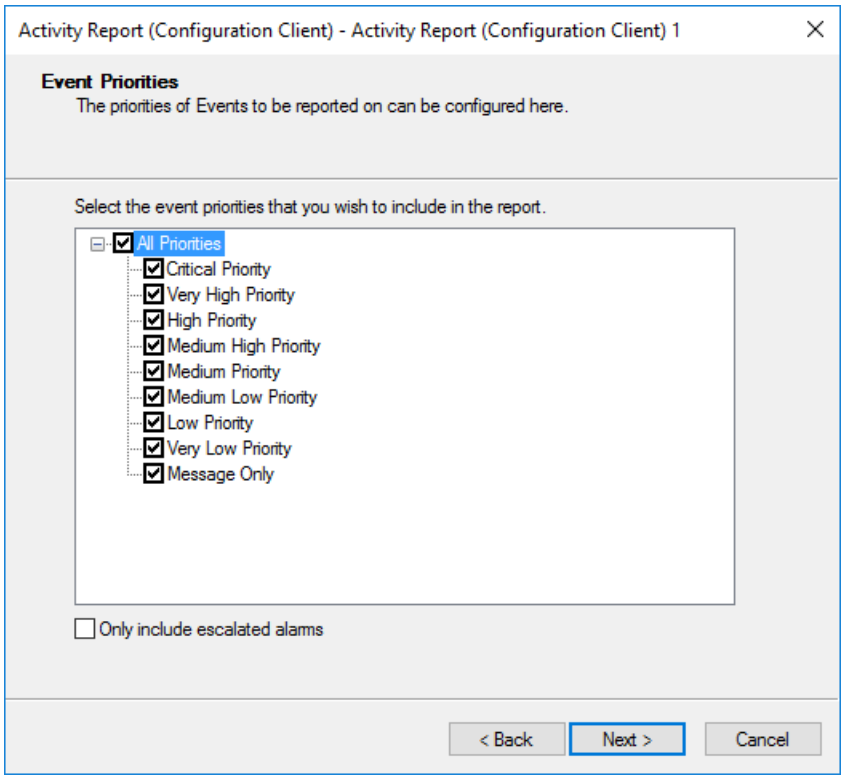
Il s'agit de la première page de l'Assistant Rapport d'activité. Cette page permet à un opérateur d'entrer les heures de début et de fin de l'état. Des périodes prédéfinies sont fournies pour plus de simplicité ou des heures de début et de fin personnalisées peuvent être entrées.

L'option par défaut est définie sur **Aujourd'hui**, la date/heure de début et de fin étant définie sur minuit et l'heure actuelle.

La valeur par défaut pour **Dernières [n] heures** est définie comme "8" heures (la plage valide est 1 - 999), avec l'idée qu'à un changement de poste un opérateur peut vouloir exécuter un rapport en fonction du nombre d'heures du dernier poste. Un décalage standard serait normalement de 8 heures, d'où le paramètre par défaut de 8 heures.

Vous pouvez éventuellement programmer cet état pour qu'il s'exécute à des heures spécifiées.

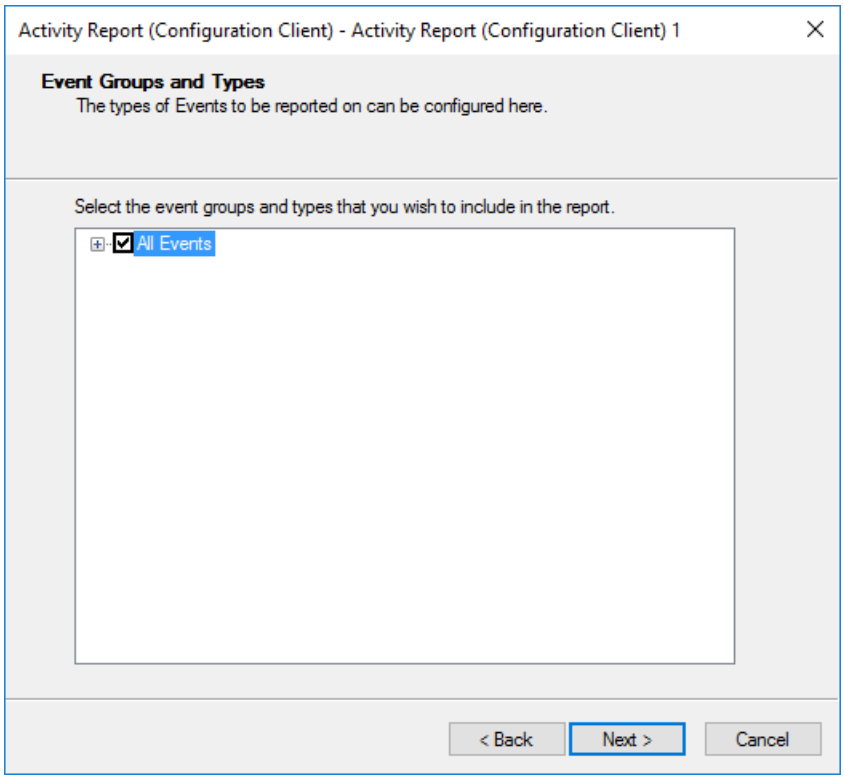
page Priorités de l'événement



Cette page fournit une représentation arborescente de toutes les priorités de l'événement et permet de sélectionner les différentes priorités à inclure dans le rapport. La sélection de la priorité est indiquée par une case à cocher et se fait en cliquant dans la case à cocher située à côté de le nom.
Remarque : Les noms de priorité sont définis par l'utilisateur (via l'onglet **Priorités des événements** des propriétés du serveur).

Cochez la case **Inclure uniquement les alarmes reportées** si vous souhaitez exécuter un rapport contenant uniquement des alarmes reportées. Un rapport d'activité ne contenant que des alarmes escaladées contiendra les détails complets de l'alarme.

page Groupes et types d'événements

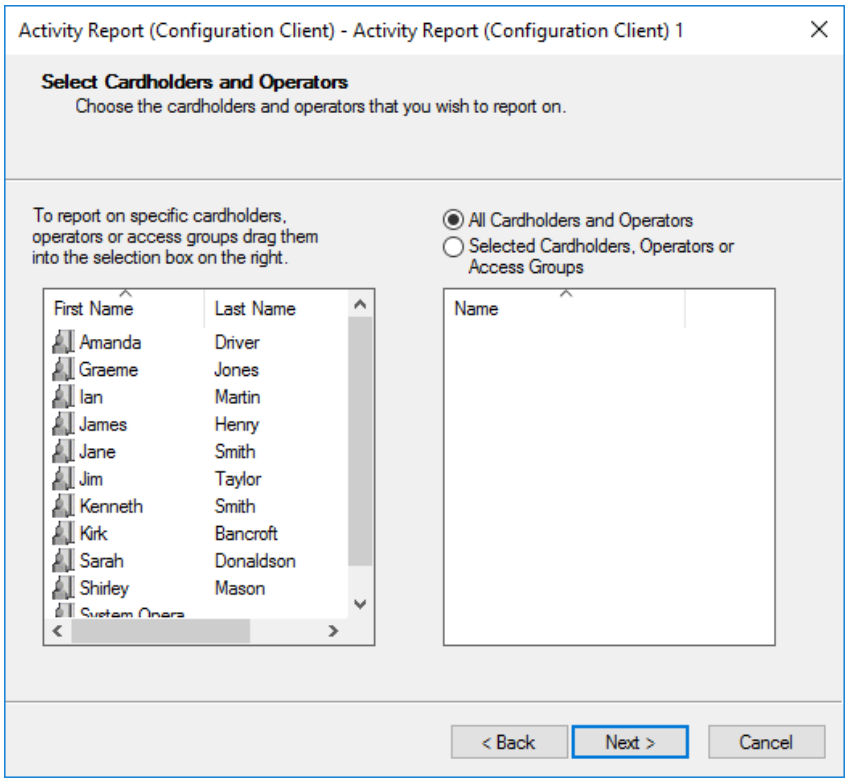


Cette page fournit une représentation arborescente des catégories et des types d'événements. La sélection du type d'événement est indiquée par une case à cocher et s'effectue en cliquant sur la case à cocher en regard du nom de l'événement. Cliquez sur l'icône pour développer ou contracter cette branche de l'arborescence.

La sélection d'une catégorie d'événements sélectionne également tous ses sous-événements. La désélection d'une catégorie d'événements désélectionne également tous ses sous-événements.

Remarque : Un fichier d'aide en ligne répertoriant tous les messages d'événement/ d'alarme est accessible via la barre de menus **Aide** du Centre de commandes et fournit des explications sur la signification de chaque message.

page Sélectionner les titulaires de carte et les opérateurs



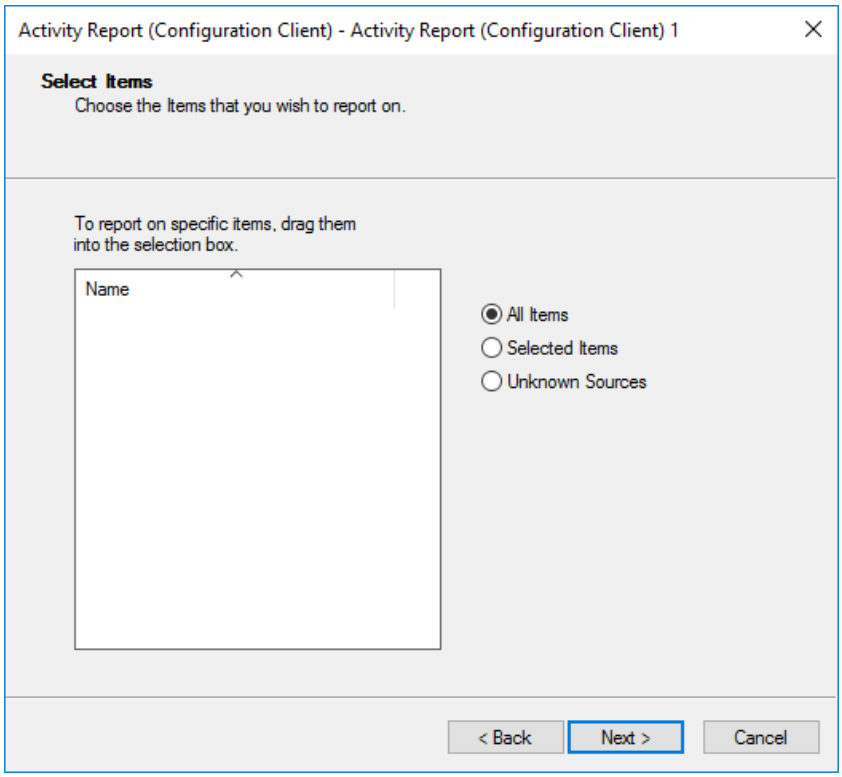
Cette page fournit une liste des titulaires de carte qu'un exploitant peut inclure dans la déclaration. Les titulaires de carte indiqués ici sont limités à ceux qui relèvent de la division de l'exploitant.

L'outil de recherche peut être utilisé pour localiser les détenteurs de cartes, 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.

Remarque :
Seuls les détenteurs de cartes actifs dans un groupe d'accès seront signalés. Par conséquent, si vous souhaitez que l'état inclue les membres "expirés" du groupe d'accès, vous devez sélectionner les détenteurs de carte plutôt que les groupes d'accès. La "suppression automatique des membres expirés" des groupes d'accès modifie les informations dans l'état en fonction de l'exécution de l'état.

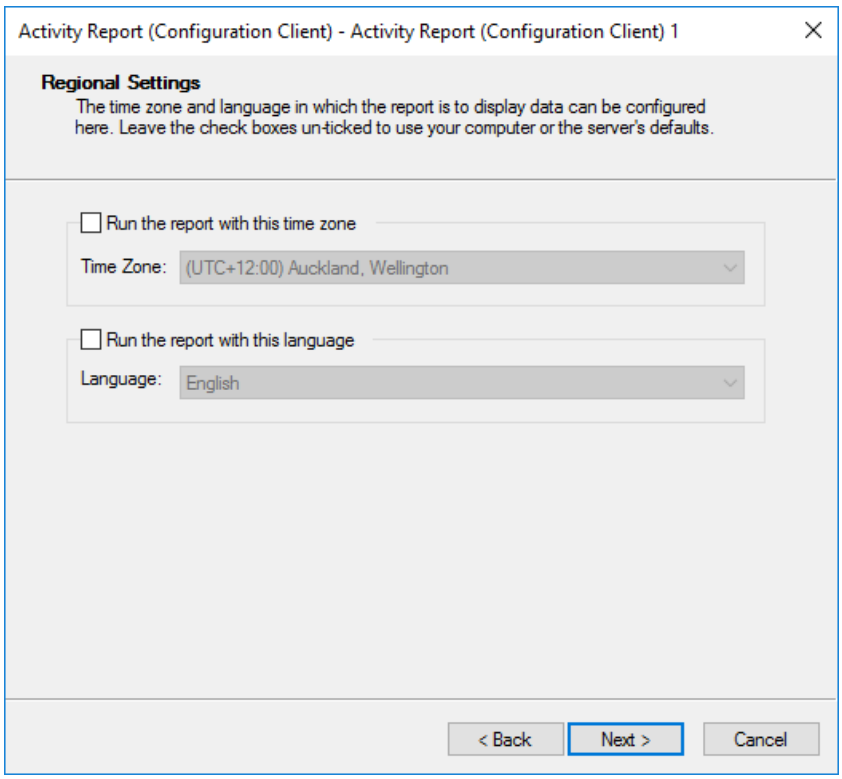
Si vous souhaitez supprimer un titulaire de carte ou un groupe d'accès de votre liste à droite, **cliquez** avec le bouton **droit** sur l'élément et cliquez sur **Supprimer de la liste**.

page Sélectionner des éléments



Cette page permet à l'opérateur de sélectionner les éléments qu'il souhaite signaler (c'est-à-dire tous les éléments ou les éléments sélectionnés par glisser-déplacer).

page Paramètres régionaux

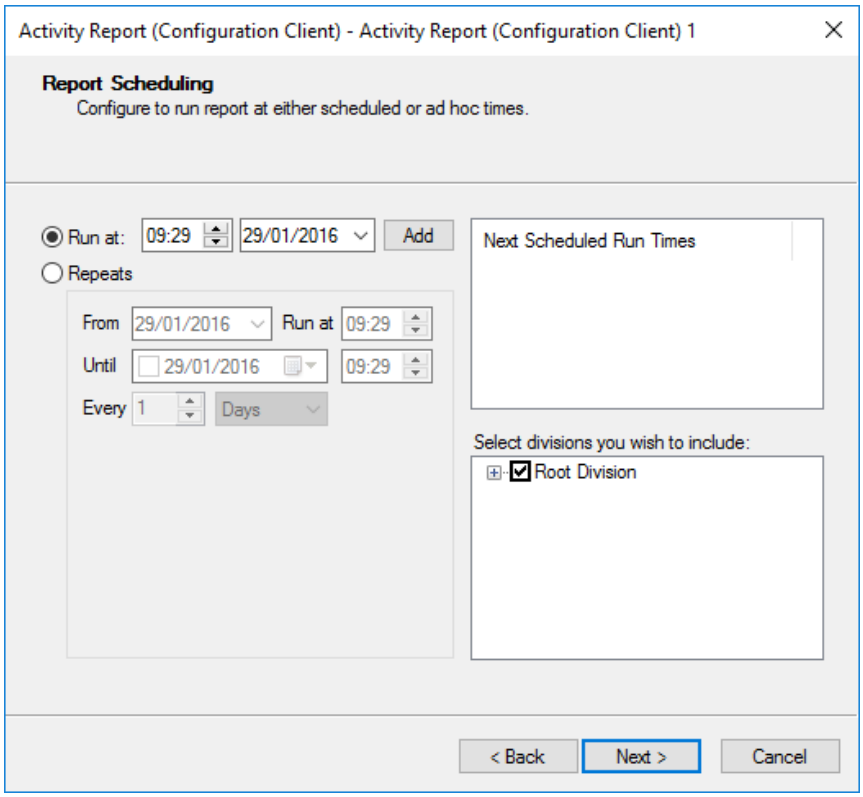


Cette page permet de sélectionner un fuseau horaire et/ou une langue pour le rapport. La sélection d'un fuseau horaire est facultative, car elle n'est requise que pour les sites du Centre de commandes qui couvrent des fuseaux horaires. La sélection d'une langue est également facultative car elle n'est 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, lors de l'exécution du rapport, toutes les dates et heures du rapport s'affichent dans le fuseau horaire sélectionné. Toutes les dates et heures configurées dans le rapport sont supposées être comprises dans le fuseau horaire sélectionné (plutôt que le fuseau horaire sur le poste de travail de l'opérateur de configuration).

page horaire rapport



Cette page s'affiche uniquement si la case à cocher "Planifier l'exécution de ce rapport à des heures spécifiées" est activée sur la page **Dates et heures du rapport**. Il permet de définir les durées d'exécution et les propriétés de répétition pour le rapport.
Plusieurs heures explicites d'exécution du rapport peuvent être configurées comme suit :

1. Cliquez sur le bouton d'option **Exécuter à (Run at)**.

2. Entrez une date et une heure et cliquez sur le bouton Ajouter.
   La date et l'heure s'affichent dans la **grille Heures d'exécution programmée suivantes**.
3. Répétez les étapes 1 à 2 pour chaque heure explicite.
   Remarque : Si vous cliquez sur le bouton radio Répéter, les ajouts explicites sont supprimés de la **grille Next Scheduled Run Times**.

Les heures de répétition du rapport à exécuter peuvent être configurées comme suit:

1. Cliquez sur le bouton d'option **Répéter (Repeats)**.
2. Sélectionnez la date et l'heure **de début** '**initiale**'.
3. Sélectionnez une date et une heure de fin si nécessaire.
   Remarque : Si aucune date Jusqu'à n'est entrée, le rapport se répétera indéfiniment.
4. Sélectionnez la régularité du rapport à exécuter, (c'est-à-dire **Tous** les **Heures**, **jours**, **semaines** ou **mois)**.
   Remarque : Lorsque **Semaines** est sélectionné dans la liste déroulante, les jours de la semaine s'affichent avec la possibilité de sélectionner un ou plusieurs jours (par exemple, lundi et jeudi).
   Les cinq dates et heures suivantes apparaissent dans les **heures d'exécution programmées suivantes** grille.

La grille de sélection de la **division** permet de programmer le rapport pour des divisions spécifiques.
Remarque : Seules les divisions pour lesquelles vous disposez du privilège de modification approprié apparaissent dans la liste.

page Génération et enregistrement de rapports

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*** (page 39-3) dans la procédure *Création d'un nouveau rapport* pour plus de détails.

Rapport d'évacuation

Introduction

Le rapport d'évacuation fournit une liste des détenteurs de cartes présents sur un site. Cela peut être utilisé dans une situation d'évacuation, comme un incendie, et permet une meilleure gestion des situations d'évacuation et une meilleure sécurité des détenteurs de cartes.
Remarque : Dans un système multi-serveurs qui utilise la gestion des visiteurs (fonction concevable sous licence), les données de visite ne sont pas répliquées entre les serveurs. Par conséquent, le rapport d'évacuation ne peut pas signaler les visiteurs éloignés.

Les rapports d'évacuation peuvent être configurés pour être générés automatiquement via un plan d'action ou une macro planifiée. Ces rapports sont appelés "rapports d'évacuation automatique" et sont déclenchés par un événement ou une alarme. Pour plus de détails, consultez ***Rapports générés automatiquement*** (page 39-63) et ***Configuration de la planification des rapports*** (page 39-65).

Prérequis

Le rapport d'évacuation se fonde sur les renseignements sur l'emplacement des détenteurs de cartes et n'est donc efficace que dans les sites où tous les détenteurs de cartes balaient leurs cartes chaque **fois** qu'ils entrent ou sortent d'une zone d'accès.

Privilèges d'opérateur

Pour créer un nouveau rapport d'évacuation, ou pour supprimer ou modifier les propriétés d'un rapport d'évacuation, un opérateur doit disposer du privilège d'opérateur "Modifier le rapport d'évacuation" dans la division du rapport d'évacuation.

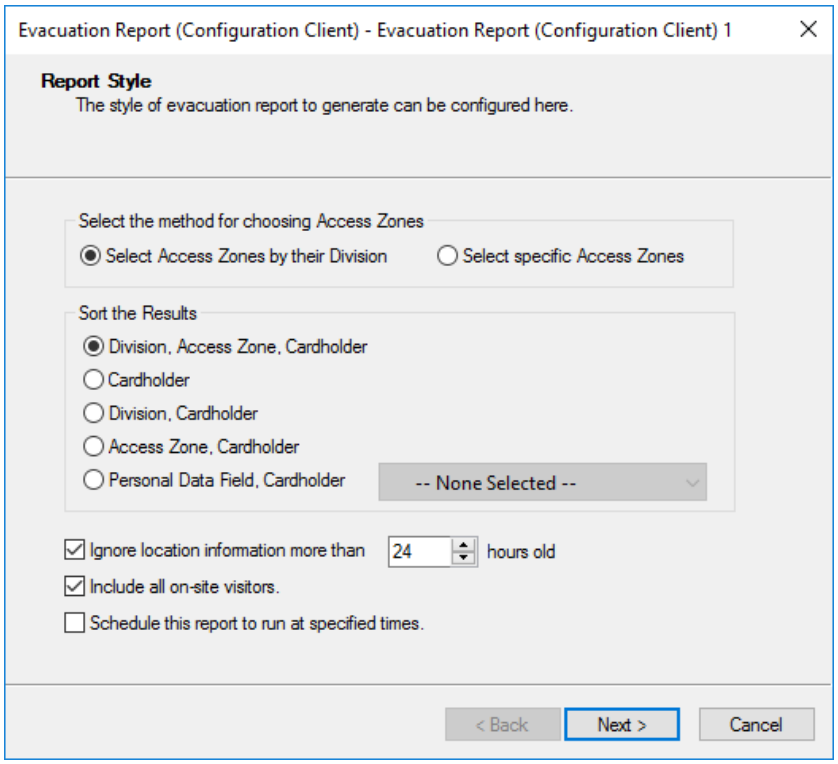
Pour afficher les propriétés d'un rapport d'évacuation enregistré existant et/ou l'exécuter, un opérateur doit disposer du privilège d'opérateur "Afficher les événements et les alarmes" dans la division du rapport d'évacuation. Un opérateur pourra toujours voir toutes les propriétés (par exemple, les éléments tels que les PDF, les zones d'accès, etc.) même si l'état contient des éléments pour lesquels l'opérateur n'a pas de privilèges.

Disposer de privilèges différents pour la création et l'exécution de rapports d'évacuation garantit que les opérateurs qui sont en mesure d'exécuter et d'imprimer des rapports d'évacuation préconfigurés (en cas d'urgence) ne sont pas autorisés à modifier leur configuration.

Assistant Rapport

L'assistant Rapport d'évacuation contient un certain nombre de pages qui vous invitent à entrer certaines informations pour créer le rapport.
Suivez les instructions affichées.

page Style de rapport



Sur cette page, vous êtes invité à :

- Choisissez la méthode de choix des zones d'accès:
  - **Sélectionner les zones d'accès par division - Cette option fournit une** méthode **rapide** et facile si vous connaissez les parties du site que vous souhaitez inclure.
  - **Sélectionner des zones d'accès spécifiques** - Cette option permet une définition plus fine que la division à laquelle la zone appartient, en sélectionnant des zones d'accès spécifiques.

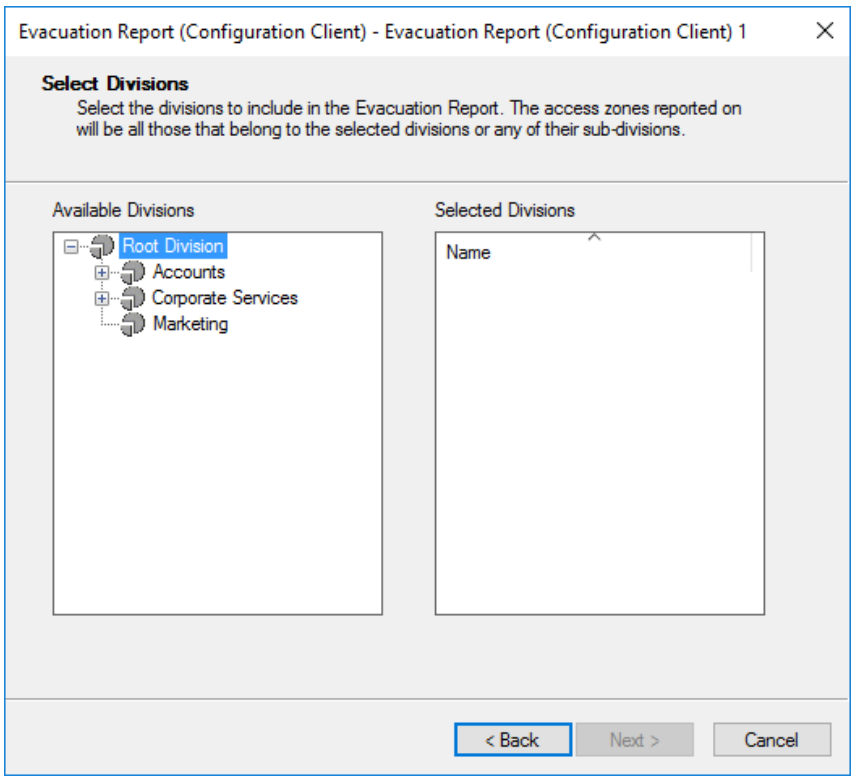
L'option que vous sélectionnez détermine la page suivante de l'assistant (soit la page "Sélectionner les divisions" ou la page "Sélectionner les zones d'accès").

- Décidez du tri des informations. Soit par :
  - Division, zone d'accès et détenteur de la carte (les dossiers seront regroupés par zone d'accès)
  - Nom du titulaire de la carte
  - Division et titulaire de la carte (les dossiers seront regroupés par division)
  - Zone d'accès et titulaire de carte (les dossiers seront regroupés par zone d'accès)
  - Champ de données personnelles et titulaire de la carte
    Remarque : La zone de liste déroulante en regard de Champ de données personnelles est activée uniquement si la case d'option **Champ de données** personnelles est sélectionnée.
    Vous pouvez choisir d'inclure ou non un champ de données personnelles dans le rapport (parce que les noms des détenteurs de cartes ne sont pas

toujours uniques, vous pouvez inclure un PDF unique pour distinguer les détenteurs de cartes avec le même nom, p.ex. 'Date de naissance' PDF) Les opérateurs peuvent sélectionner uniquement les PDF disponibles.

- Vous pouvez éventuellement définir l'état de manière à ignorer les informations d'emplacement antérieures à une certaine âge.
  (Valeur par défaut = définie pour ignorer les informations d'emplacement datant de plus de 24 heures. Le maximum autorisé est de 999 heures.)
- Vous pouvez éventuellement **programmer cet état pour qu'il s'exécute à des heures spécifiées**.
- Si votre site est sous licence pour la fonction de gestion des visiteurs, il existe également une option permettant d'inclure tous les visiteurs sur le site (cochée par défaut).
  Si cette option est sélectionnée, une nouvelle section est ajoutée à la fin du rapport, qui énumère tous les groupes sur place, en raison de congés et de visiteurs en retard et de visites touristiques.
  Remarque : Tous les visiteurs sont inclus dans le rapport, peu importe les divisions ou les zones d'accès sélectionnées, et les groupes de visite indiqueront le nombre de visiteurs et un nom de contact pour la visite.

page Sélectionner des divisions

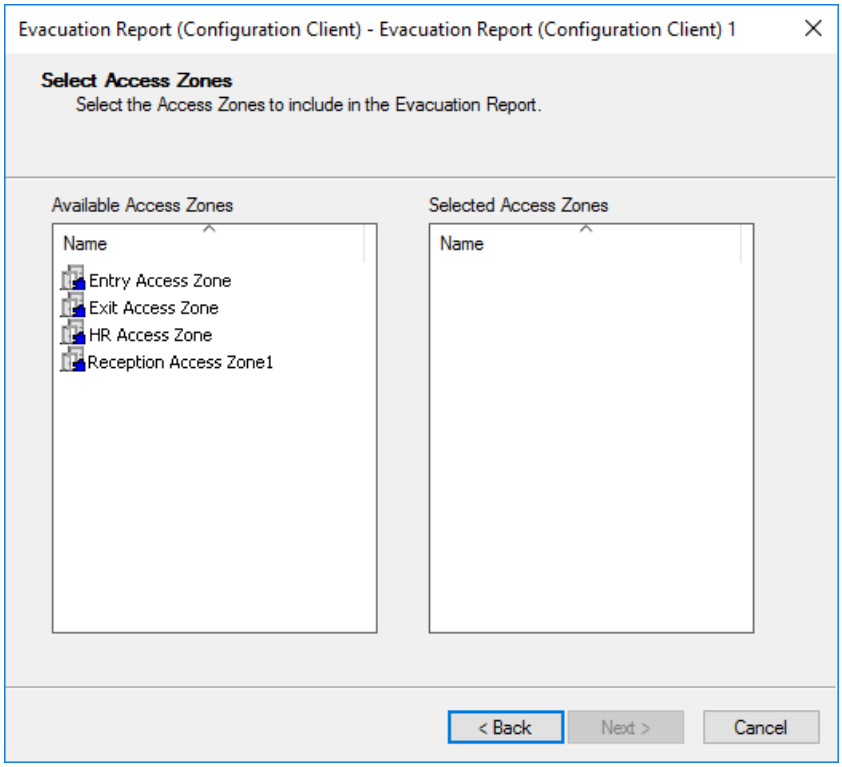


Cette page s'affiche uniquement si l'option "Sélectionner les zones d'accès par division" est sélectionnée.
La grille de gauche affiche les "Divisions disponibles" de l'opérateur actuel. Les divisions disponibles sont toutes les divisions dans lesquelles l'opérateur dispose du privilège "Afficher le site" ou "Modifier le site".

Faites glisser et déposez la ou les divisions que vous voulez inclure dans le rapport d'évacuation de la liste des divisions disponibles (la grille à gauche), vers la grille à droite.

Si vous avez ouvert un rapport d'évacuation enregistré existant, les divisions qui ont été initialement sélectionnées pour être incluses dans le rapport s'affichent dans la grille de droite. Ceux-ci s'affichent indépendamment des privilèges de l'opérateur actuel dans ces divisions. Un opérateur peut supprimer une "division sélectionnée" de la liste s'il dispose du privilège "Afficher le site" ou "Modifier le site" dans cette division.

page Sélectionner les zones d'accès

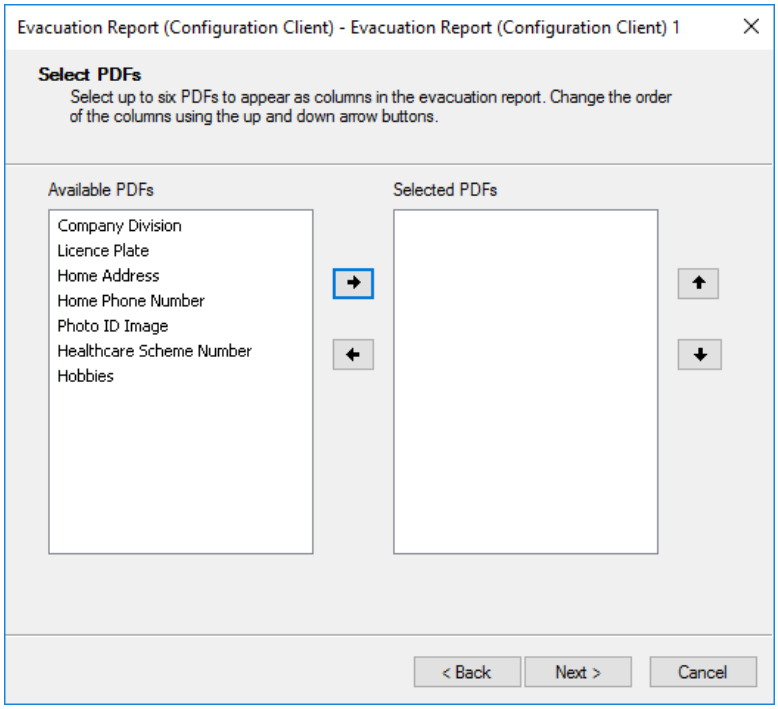


Cette page s'affiche uniquement si l'option "Sélectionner des zones d'accès spécifiques" est sélectionnée. La grille de gauche affiche les "zones d'accès disponibles" de l'opérateur actuel. Les zones d'accès disponibles sont toutes des zones d'accès dans lesquelles l'opérateur dispose du privilège "View Site".

Faites glisser et déposez les zones d'accès que vous souhaitez inclure dans le rapport d'évacuation de la liste des zones d'accès disponibles (la grille à gauche), vers la grille à droite.

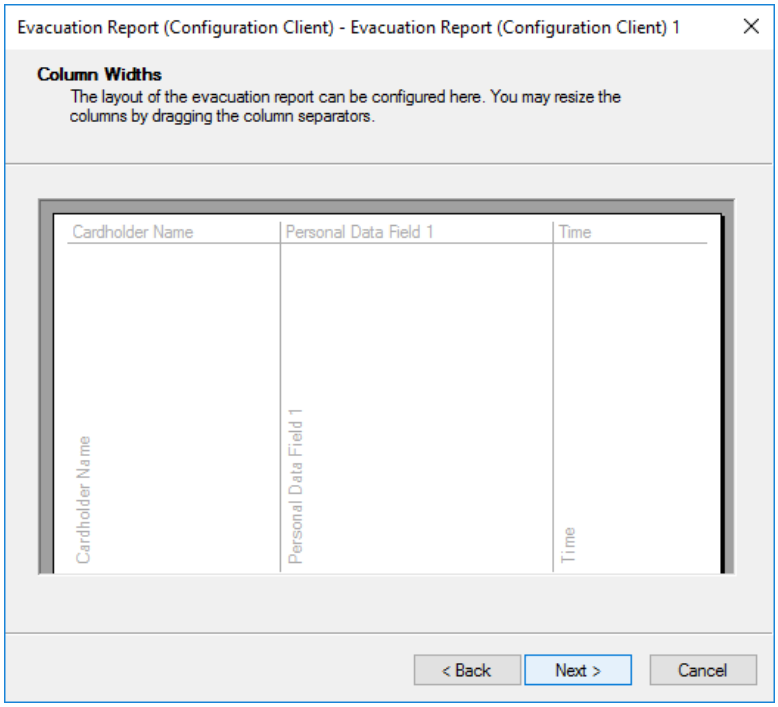
Si vous avez ouvert un rapport d'évacuation enregistré existant, les zones d'accès qui ont été initialement sélectionnées pour être incluses dans le rapport s'affichent dans la grille de droite. Ceux-ci s'affichent indépendamment des privilèges de l'opérateur actuel. Un opérateur peut supprimer une "Zone d'accès sélectionnée" de la liste s'il dispose du privilège "Voir le site" dans la division de la Zone d'accès.

Sélectionner la page PDF



Cette page vous permet d'inclure jusqu'à six champs de données personnelles dans la sortie de l'état. À l'aide des boutons fléchés, placez les champs de données personnelles dont vous avez besoin de la grille **PDF** disponible à la **grille PDF sélectionné**.
Une fois que vous avez les champs de données personnelles dont vous avez besoin dans la grille du PDF sélectionné sur la droite, les flèches vers le haut et vers le bas sur le côté peuvent être utilisées pour modifier l'ordre de ces champs (c'est-à-dire, sélectionnez le PDF que vous souhaitez déplacer et cliquez sur la flèche vers le haut ou vers le bas pour le déplacer).

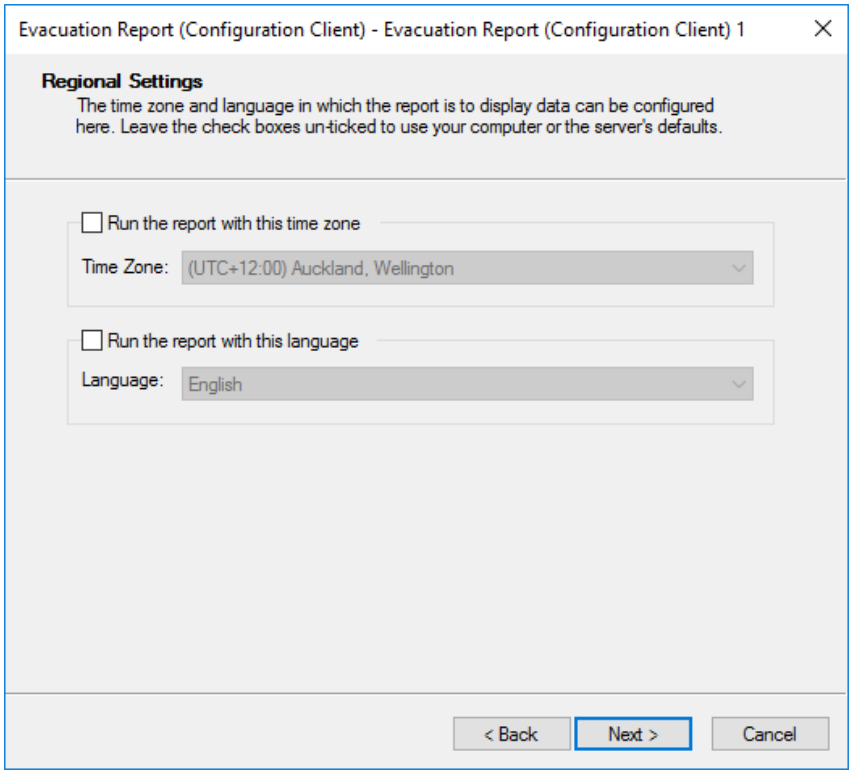
page Largeurs de colonne



Cette page permet à l'opérateur de configurer la mise en page du rapport. Vous pouvez redimensionner la largeur des colonnes comme suit :

1. Déplacez le pointeur de la souris sur un séparateur de colonnes.
2. 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.

page Paramètres régionaux

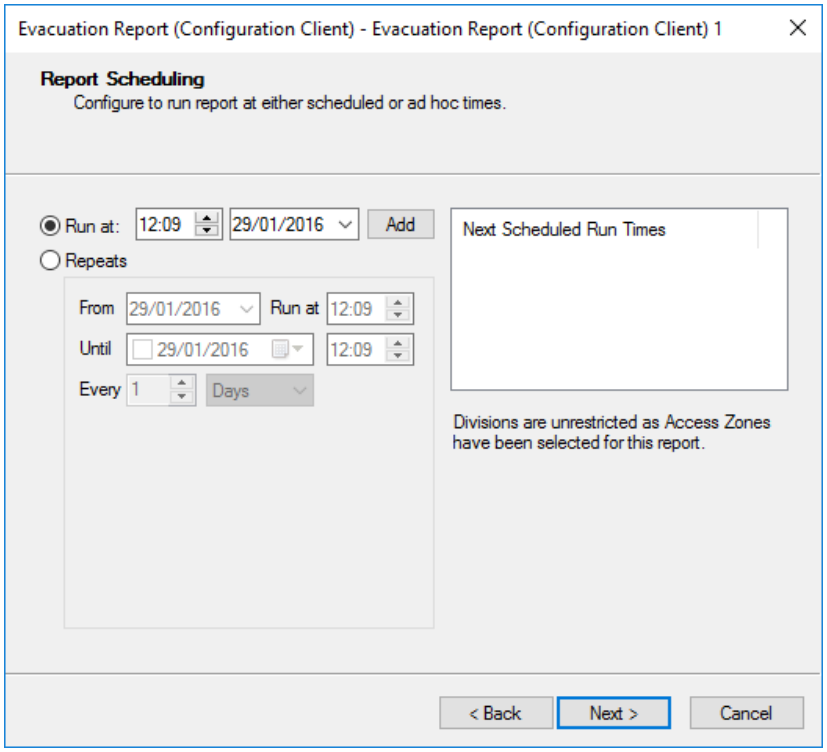


Cette page permet de sélectionner un fuseau horaire et/ou une langue pour le rapport. Ces options sont spécifiquement fournies pour prendre en charge le rapport d'évacuation automatique (c'est-à-dire lorsque le rapport est exécuté via une macro sur le serveur). La sélection d'un fuseau horaire est facultative, 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, lors de l'exécution du rapport, toutes les dates et heures du rapport s'affichent dans le fuseau horaire sélectionné. Toutes les dates et heures configurées dans le rapport sont supposées être comprises dans le fuseau horaire sélectionné (plutôt que le fuseau horaire sur le poste de travail de l'opérateur de configuration).

page horaire rapport



Cette page s'affiche uniquement si la case à cocher "Planifier l'exécution de ce rapport aux heures spécifiées" est activée sur la page **Style de rapport**. Il permet de définir les temps d'exécution et les propriétés de répétition pour le rapport. Plusieurs heures explicites d'exécution du rapport peuvent être configurées comme suit :

1. Cliquez sur le bouton d'option **Exécuter à (Run at)**.
2. Entrez une date et une heure et cliquez sur le bouton Ajouter.
   La date et l'heure s'affichent dans la **grille Heures d'exécution programmée suivantes**.
3. Répétez les étapes 1 à 2 pour chaque heure explicite.
   Remarque : Si vous cliquez sur le bouton radio Répéter, les ajouts explicites sont supprimés de la **grille Next Scheduled Run Times**.

Les heures de répétition du rapport à exécuter peuvent être configurées comme suit:

1. Cliquez sur le bouton d'option **Répéter (Repeats)**.
2. Sélectionnez la date et l'heure **de début** '**initiale**'.
3. Sélectionnez une date et une heure de fin si nécessaire.
   Remarque : Si aucune date **Jusqu'au n**'est entrée, le rapport sera répété indéfiniment.
4. Sélectionnez la régularité de l'exécution du rapport (**Tous les Heures**, **jours**, **semaines** ou **mois)**.
   Remarque : Lorsque **Semaines** est sélectionné dans la liste déroulante, les jours de la semaine s'affichent avec la possibilité de sélectionner un ou plusieurs jours (par exemple, lundi et jeudi).

Les cinq dates et heures suivantes apparaissent dans les **heures d'exécution programmées suivantes** grille.

page Génération et enregistrement de rapports

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*** (page 39-3) dans la procédure *Création d'un nouveau rapport* pour plus de détails.

Recommandation :
Il est fortement recommandé que les sites effectuent des essais du rapport d'évacuation pour s'assurer que les rapports :
- configuré correctement
- sera imprimé sur l'imprimante correcte à partir de tous les postes de travail.

Exclusion de responsabilité :
L'avertissement suivant figure dans le rapport :
"Les informations présentées dans ce rapport dépendent de la configuration du système et du rapport. Gallagher n'accepte pas la responsabilité des sites qui s'appuient sur ce rapport d'évacuation."

Méthode rapide d'impression

En cas d'urgence, les opérateurs disposant du privilège d'opérateur 'Afficher les événements et les alarmes' peuvent imprimer un rapport d'évacuation préconfiguré rapidement et facilement. Utilisez la procédure dans cette situation :

1. Cliquez sur **Rapport dans** la barre de menus, puis sur **Rapport Descriptions**.
   La **fenêtre Description** de l'état Liste s'ouvre (en mode grille).

2. Mettez en surbrillance le rapport requis.

3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Imprimer**.
   La page **Génération et enregistrement de rapports** de l'assistant de rapport s'ouvre.

4. Cliquez sur le bouton d'**option** Imprimante (s'il n'est pas déjà sélectionné) et cliquez sur Suivant s'affiche.
   Le rapport d'évacuation imprime l'imprimante préconfigurée dans le rapport. Si cette imprimante n'est pas disponible pour l'opérateur qui génère le rapport, les imprimantes disponibles pour l'opérateur sont répertoriées et l'opérateur est invité à en sélectionner une.

Rapport groupe d’accès

Introduction

Le rapport des groupes d'accès fournit une liste unifiée des groupes d'accès avec leur appartenance, leur accès et leurs propriétés.
Le rapport du groupe d'accès complète les rapports des titulaires de carte. Les rapports des titulaires de cartes contiennent des renseignements sur les titulaires de cartes, y compris des renseignements sur les champs de données personnelles (PDF), les cartes, les groupes d'accès auxquels le titulaire de carte appartient, etc. Le rapport des groupes d'accès fournit des informations spécifiques sur les groupes d'accès, notamment :

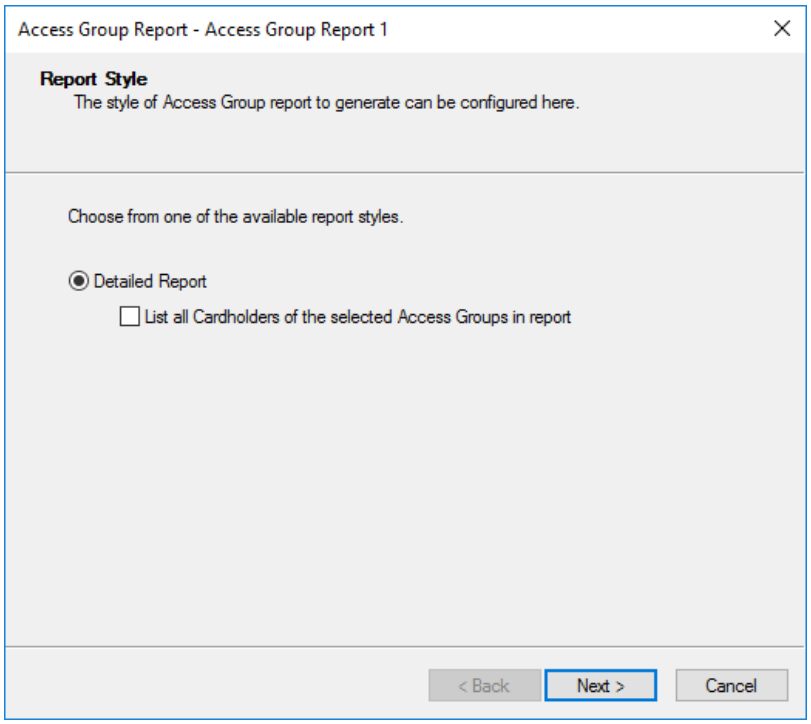
- Privilèges attribués à un groupe d'accès
- Dispositions relatives à l'accès
- La liste des champs PDF affectés à un groupe d'accès
- Une liste des titulaires de carte qui sont membres du groupe Accès

Les opérateurs doivent disposer des privilèges "Afficher les groupes d'accès" et "Modifier les descriptions de rapports" pour créer, enregistrer, modifier et supprimer les rapports de groupes d'accès.

Assistant Rapport

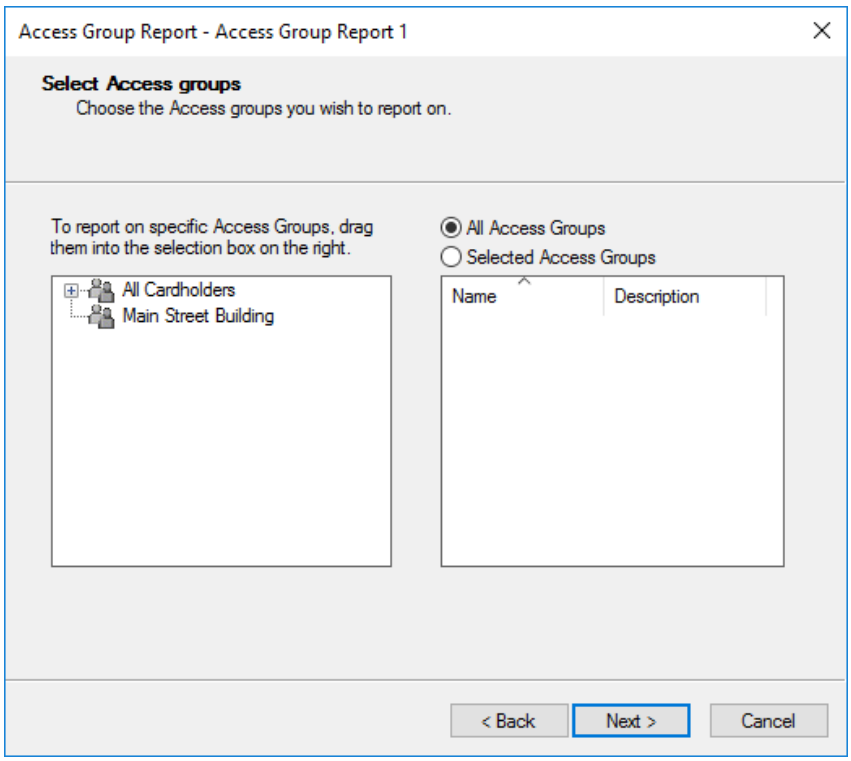
L'Assistant État de groupe d'accès contient un certain nombre de pages qui vous invitent à entrer certaines informations pour créer un état.
Suivez les instructions affichées.

page Style de rapport



Il s'agit de la première page de l'Assistant Rapport de groupe d'accès. L'opérateur a l'option ici d'inclure tous les titulaires de carte du groupe d'accès sélectionné dans le rapport. Si cette option est choisie, le rapport contiendra une section sur les membres pour chacun des groupes d'accès choisis. Cette section affichera les dates et heures de début et de fin de l'adhésion au groupe d'accès temporaire et temporaire. Les détenteurs de cartes sans date ni heure de début ni de fin sont membres permanents d'un groupe d'accès. Les enregistrements d'adhésion temporaires qui ont expiré mais n'ont pas été supprimés du système apparaissent également dans le rapport

page Sélectionner des groupes Access



Cette page permet à l'opérateur d'inclure tous les groupes d'accès ou les groupes d'accès sélectionnés, (en les faisant glisser et en les déposant), dans l'état.
Remarque :
Seuls les détenteurs de cartes actifs dans un groupe d'accès seront signalés. La "suppression automatique des membres expirés" des groupes Access modifie les informations contenues dans l'état en fonction du moment où l'état est exécuté.

Si vous souhaitez supprimer un groupe d'accès de votre liste à droite, faites un **clic** droit **sur** le groupe d'accès et cliquez **Supprimer de la liste**.

page Génération et enregistrement de rapports

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*** (page 39-3) dans la procédure *Création d'un nouveau rapport* pour plus de détails.

Rapport d'accès

Introduction

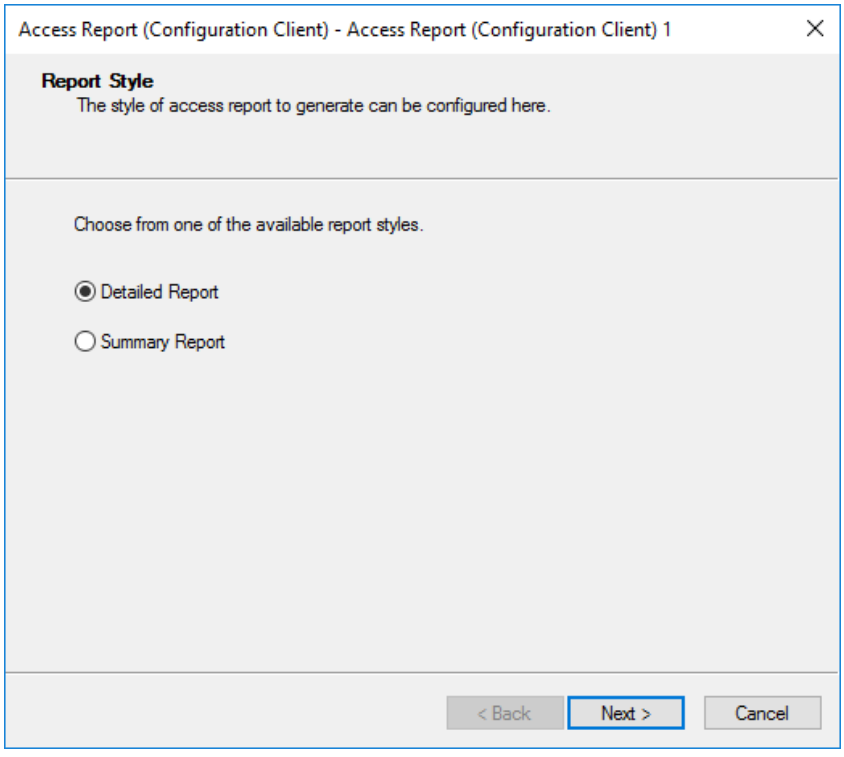
Le rapport d'accès fournit une liste des titulaires de carte qui peuvent accéder à une porte ou à une zone pendant une période de temps spécifiée.

Les opérateurs doivent disposer des privilèges d'opérateur "Modifier les titulaires de carte", "Modifier les descriptions de rapport" et "Afficher le site" pour créer, enregistrer, modifier et supprimer les rapports d'accès.

Assistant Rapport

L'Assistant État d'accès contient un certain nombre de pages qui vous invitent à entrer certaines informations pour créer un état.
Suivez les instructions affichées.

page Style de rapport

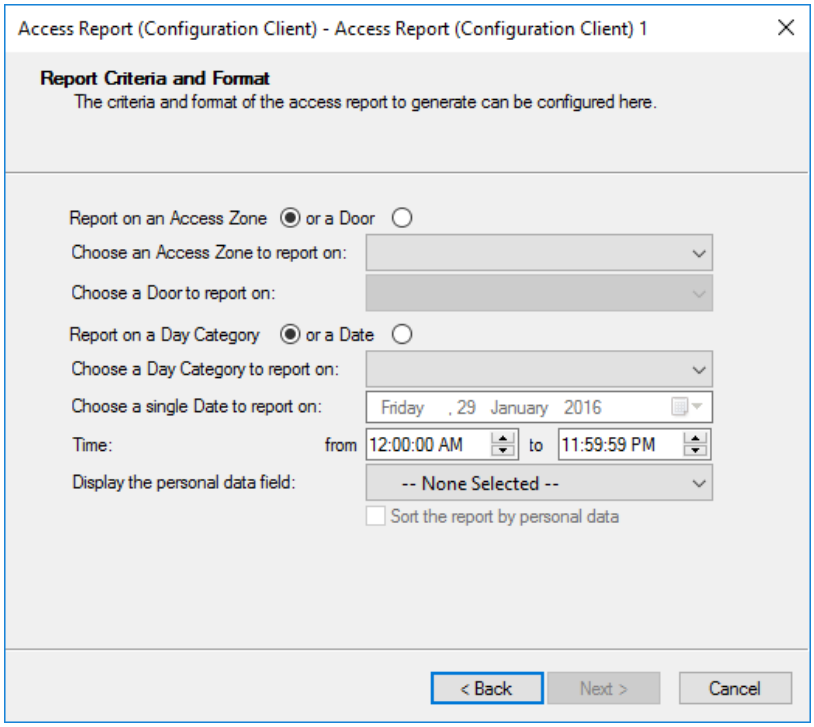


Il s'agit de la première page de l'Assistant Rapport Access. Il permet à l'opérateur de sélectionner une **version** détaillée ou **récapitulative du rapport**.

Les rapports d'accès détaillés comprennent une liste des titulaires de carte, ainsi que leurs données personnelles et les cartes attribuées. Ce style de rapport est orienté autour des titulaires de carte, avec le rapport trié par nom de titulaire de carte ou par champ de données personnelles. Ce style de rapport indique également la plage de dates à laquelle un accès des titulaires de carte s'applique, qui est déterminée à partir des heures d'activation et d'expiration de l'accès temporaire.

Les **rapports sommaires d'accès** sont axés sur les groupes d'accès et ne contiennent pas d'informations sur les titulaires de carte.

page Critères et format du rapport



Cette page permet à l'opérateur de choisir des critères pour l'état et de définir des fonctionnalités de mise en forme de base telles que l'inclusion d'un champ de données personnelles (PDF) et l'ordre de tri de l'état. Les champs **Zone d'accès** et **Porte** s'excluent mutuellement en ce que l'opérateur ne peut définir des critères que dans un champ ou dans l'autre. Les champs **Catégorie de jour** et **Date** s'excluent également mutuellement et ne peuvent pas être sélectionnés pour une date passée. Les champs d'intervalle de temps sont limités à un seul jour (c'est-à-dire qu'ils ne peuvent pas être réglés pour traverser minuit).

page Génération et enregistrement de rapports

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*** (page 39-3) dans la procédure *Création d'un nouveau rapport* pour plus de détails.

Rapport des exceptions

Introduction

Le rapport des exceptions permet aux opérateurs de générer une liste d'exceptions au fonctionnement normal du système (c'est-à-dire des problèmes en suspens tels que les alarmes non traitées).

Ce rapport peut être généré par un opérateur au début de son quart de travail, afin d'obtenir un aperçu de l'état actuel du système. Ils demandent un rapport d'exception sur la division dont ils ont la responsabilité immédiatement après s'être connectés au système.

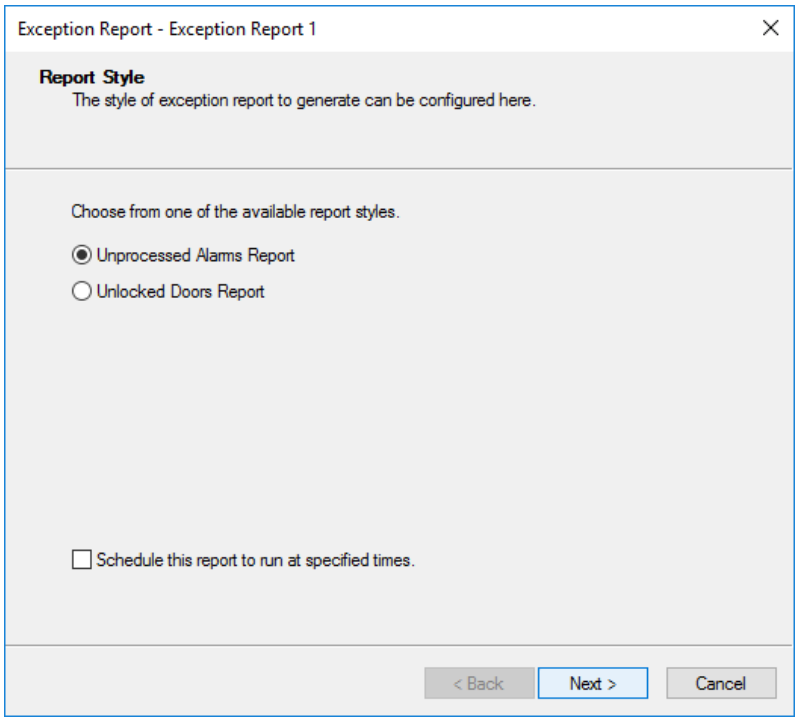
Les opérateurs doivent disposer du privilège "Modifier les descriptions de rapports" pour créer, enregistrer, modifier et supprimer les rapports d'exception.

Ce rapport peut être planifié pour s'exécuter automatiquement à des heures régulières (via des plans d'action ou des macros planifiées). Pour plus d'informations, reportez-vous à la section ***Automatic Generated Reports*** (on page 39-63) et ***Configuring Report Scheduling*** (on page 39-65).

Assistant Rapport

L'Assistant Rapport d'exceptions contient un certain nombre de pages qui vous invitent à entrer certaines informations pour créer un rapport.
Suivez les instructions affichées.

page Style de rapport



Il s'agit de la première page de l'Assistant Rapport d'exception. Il permet à

l'opérateur de sélectionner un **rapport d'alarmes non traitées** ou un rapport de portes déverrouillées.

Les rapports d'alarmes non traitées incluent toutes les alarmes non traitées, qu'elles soient reconnues ou non. Pour que cette option soit activée, un opérateur a besoin des privilèges "Afficher les événements et les alarmes" ou "Modifier les alarmes".

Portes déverrouillées Les **rapports** incluent toutes les portes dont la fermeture est prévue, mais qui sont actuellement déverrouillées en raison d'un remplacement ou d'une alarme active liée à la porte. Ce rapport est divisé en deux sections :

Remplacer la section :
Cette section du rapport répertorie les portes programmées pour être sécurisées, mais qui sont actuellement en mode "Free".
Remarque : Si une porte a deux zones (une zone d'entrée et une zone de sortie), les deux zones doivent être remplacées par "Libre", sinon la porte restera "sécurisée".

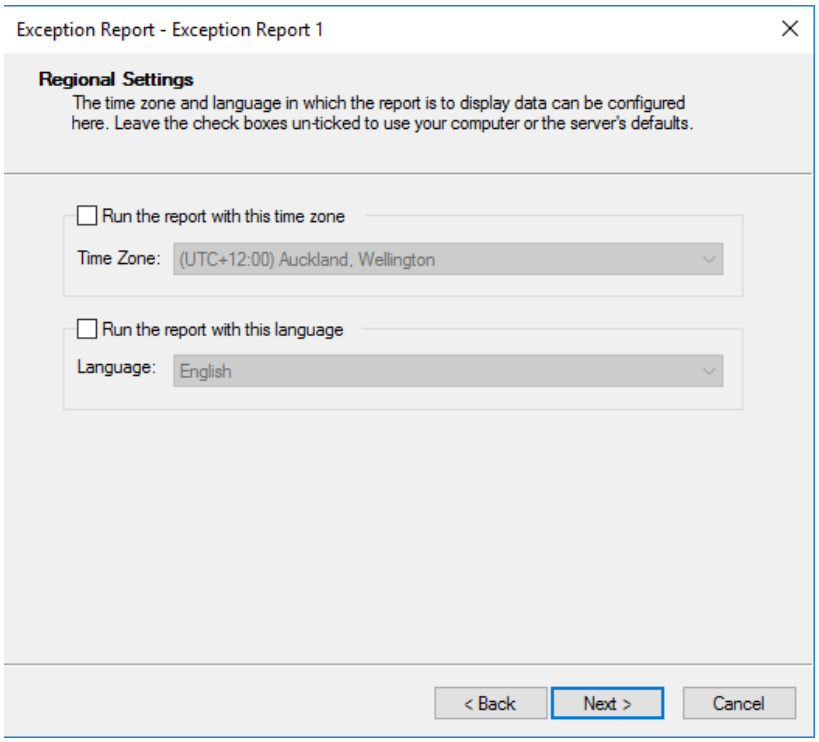
Section Alarmes actives :
Cette section du rapport énumère les portes avec l'une des alarmes actives :
- Porte forcée
- Porte non verrouillée
- Porte Ouverte
- Porte de secours

Pour que l'option "Rapport des portes déverrouillées" soit activée, un opérateur a besoin des privilèges d'opérateur "Afficher le site" ou "Modifier le site". Cela leur permet d'exécuter le rapport, mais ils ne pourront afficher que la section Remplacement. Ils requièrent également le privilège de l'opérateur "Afficher les événements et les alarmes" pour afficher la section Alarmes actives de l'état.

Remarque : Une porte sécurisée ne sera pas indiquée comme déverrouillée simplement parce qu'un titulaire de carte ouvre temporairement la porte pour y avoir accès au moment où le rapport effectue ses vérifications.

Vous pouvez éventuellement planifier l'exécution de ce rapport à des heures spécifiées pour les deux styles de rapport.

page Paramètres régionaux

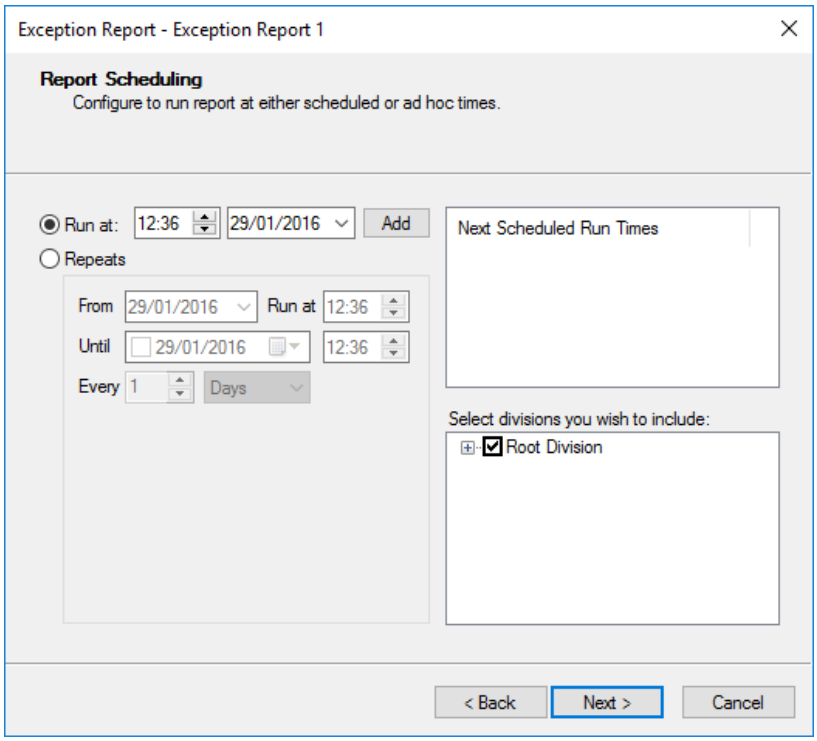


Cette page permet de sélectionner un fuseau horaire et/ou une langue pour le rapport. La sélection d'un fuseau horaire est facultative, car elle n'est requise que pour les sites du Centre de commandes qui couvrent des fuseaux horaires. La sélection d'une langue est également facultative car elle n'est 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, lors de l'exécution du rapport, toutes les dates et heures du rapport s'affichent dans le fuseau horaire sélectionné. Toutes les dates et heures configurées dans le rapport sont supposées être comprises dans le fuseau horaire sélectionné (plutôt que le fuseau horaire sur le poste de travail de l'opérateur de configuration).

page horaire rapport



Cette page s'affiche uniquement si la case à cocher "Planifier l'exécution de ce rapport aux heures spécifiées" est activée sur la page **Style de rapport**. Il permet de définir les temps d'exécution et les propriétés de répétition pour le rapport. Plusieurs heures explicites d'exécution du rapport peuvent être configurées comme suit :

1. Cliquez sur le bouton d'option **Exécuter à (Run at)**.
2. Entrez une date et une heure et cliquez sur le bouton **Ajouter**.
   La date et l'heure s'affichent dans la **grille Heures d'exécution programmée suivantes.**
3. Répétez les étapes1-2 pour chaque fois que vous en avez besoin.
   Remarque : Si vous cliquez sur le bouton radio Répéter, les ajouts explicites sont supprimés de la **grille Next Scheduled Run Times**.

Les heures de répétition du rapport à exécuter peuvent être configurées comme suit:

1. Cliquez sur le bouton d'option **Répéter (Repeats)**.
2. Sélectionnez la date et l'heure **de début** '**initiale**'.
3. Sélectionnez une date et une heure de fin si nécessaire.
   Remarque : Si aucune **date** Jusqu'à n'est entrée, le rapport se répétera indéfiniment.
4. Sélectionnez la régularité du rapport à exécuter, (c'est-à-dire **Tous** les **Heures**, **jours**, **semaines** ou **mois)**.
   Remarque : Lorsque **Semaines** est sélectionné dans la liste déroulante, les jours de la semaine s'affichent avec la possibilité de sélectionner un ou plusieurs jours (par exemple, lundi et jeudi).

Les cinq dates et heures suivantes apparaissent dans les **heures d'exécution programmées suivantes** grille.

La grille de sélection de la **division** permet de programmer le rapport pour des divisions spécifiques.
Remarque : Seules les divisions pour lesquelles vous disposez du privilège de modification approprié apparaissent dans la liste.

page Génération et enregistrement de rapports

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*** (page 39-3) dans la procédure *Création d'un nouveau rapport* pour plus de détails.

Rapport de temps et de présence

Introduction

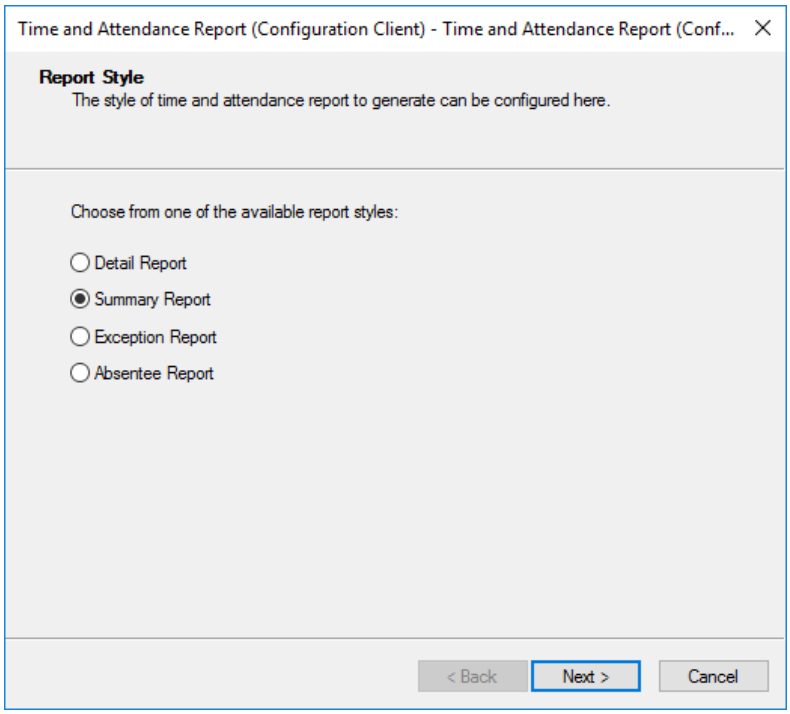
Le Rapport sur les heures et les présences permet de suivre les heures travaillées par les titulaires de carte. Les événements d'entrée et de sortie de porte sont utilisés dans le système pour calculer les heures travaillées par chaque titulaire de carte. En général, un événement d'entrée de porte est assimilé à un détenteur de carte qui effectue ou commence le travail, tandis qu'un événement de sortie de porte équivaut à un détenteur de carte qui effectue ou termine le travail.

Les opérateurs doivent disposer des privilèges "Afficher les titulaires de carte", "Modifier les descriptions de rapport" et "Afficher le site" pour créer, enregistrer, modifier et supprimer les rapports de temps et de présence. Le privilège "Visualiser le site" est requis pour afficher les lecteurs utilisés pour le rapport Temps et Présence.
Remarque : Dans un environnement multi-serveur, pour tout serveur où l'agrégation d'événements est activée, un opérateur peut exécuter un rapport de temps et de présence qui intègre des événements provenant de lecteurs distants. Le rapport de temps et de présence peut être filtré par les lecteurs distants.

Assistant Rapport

L'assistant Rapport de présence contient un certain nombre de pages qui vous invitent à entrer certaines informations pour créer un état.
Suivez les instructions affichées.

page Style de rapport



Il s'agit de la première page de l'assistant Heure et présence. Il permet la pour choisir

entre un état Détail ou Synthèse des temps et des présences, un état **des exceptions** ou un état des absents.

Les rapports détaillés indiquent les heures travaillées par les titulaires de carte sélectionnés au cours de la période définie. Ils montrent chaque fois qu'un titulaire de carte a fait son entrée ou sa sortie au cours de la période de déclaration, avec un total d'heures travaillées entre chaque paire d'horloge dans et hors événements.

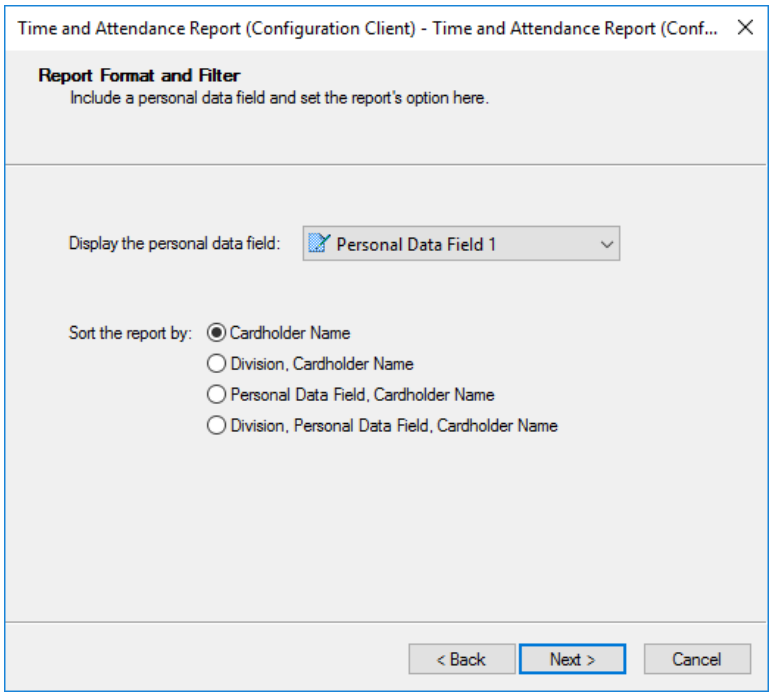
Les rapports de synthèse indiquent également les heures travaillées par chaque titulaire de carte, mais résument cette information quotidiennement. Ils montrent la première fois qu'un titulaire de carte a fait un pointage pour le travail et la dernière fois qu'il a fait un pointage à la fin de la journée, avec un total d'heures travaillées entre ces périodes.

Les rapports détaillés peuvent comporter deux entrées pour une journée, l'une qui ne contient pas suffisamment de données et l'autre qui est réelle (par exemple, un titulaire de carte a ouvert la porte à un lecteur d'entrée et a badgé sa carte, mais a ensuite décidé de ne pas entrer). Dix minutes plus tard, le même titulaire de carte entre à nouveau au même lecteur d'entrée et sort huit heures plus tard). Dans le rapport détaillé, l'heure serait correctement additionnée, mais dans un rapport sommaire, il serait noté ce jour-là comme ayant des données insuffisantes.
Si vous exécutez un rapport de synthèse et que vous ne disposez pas de données suffisantes pour un titulaire de carte, exécutez un rapport détaillé pour ce titulaire de carte.
Remarque :
Il est recommandé d'exécuter également un rapport d'exceptions si vous exécutez un rapport de synthèse. Ceci est dû à une sortie de rapport de synthèse ne donnant aucune indication quant à savoir si le rapport contient ou non des événements inutilisables, tandis qu'un rapport d'exception identifie les événements inutilisables.

Les rapports d'exception fournissent une analyse des événements qui influent sur la précision des rapports sur l'heure et la fréquentation (p. ex., un titulaire de carte peut oublier de se retirer à la fin de la journée ou présenter sa carte plus d'une fois au moment de commencer ou de quitter son travail). L'exactitude des informations sur les événements est essentielle au calcul des heures travaillées pour chaque titulaire de carte, ce qui vous permet d'identifier les événements incorrects lorsque les heures travaillées d'un titulaire de carte ne peuvent être calculées ou sont excessives.

Les rapports sur les absents fournissent des renseignements sur les jours où un titulaire de carte n'a pas travaillé. Ils déterminent qu'un titulaire de carte était absent un jour donné s'il n'y avait pas d'horloge dans ou hors des événements.
Remarque :
Vous devez configurer un rapport d'absentéisme pour exclure les week-ends et/ou les autres jours où un détenteur de carte ne devrait pas travailler.

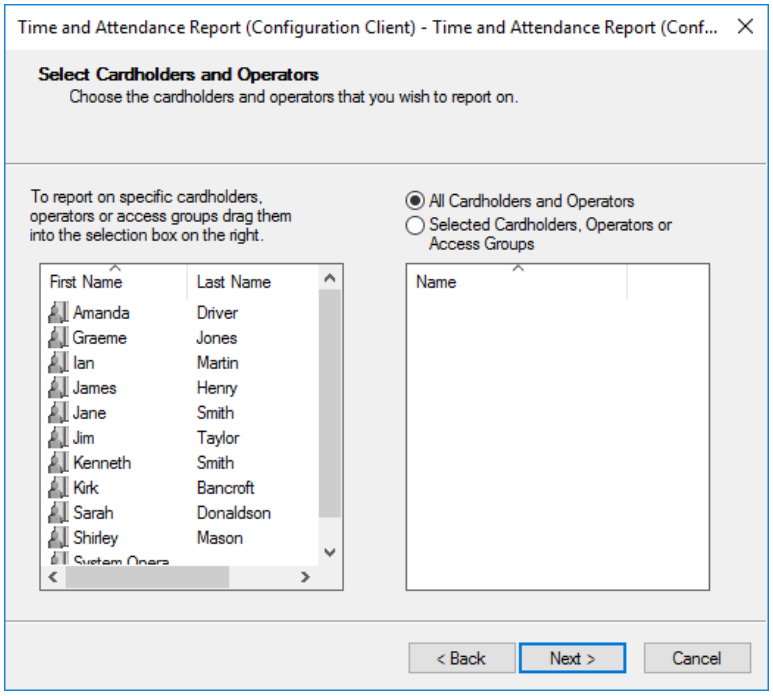
page Format de rapport et filtre



Cette page permet à l'opérateur de définir deux options comme suit :

- Un **champ** de **données personnelles** numérique ou de chaîne peut être sélectionné pour être affiché dans le rapport.
- L'opérateur peut trier l'état par nom du détenteur de la carte ou par **champ de** données personnelles, avec un niveau supérieur facultatif trié par division.

page Sélectionner les titulaires de carte et les opérateurs



Cette page fournit une liste des titulaires de carte qu'un exploitant peut inclure dans le de Les titulaires de carte indiqués ici sont limités à ceux qui relèvent de la division

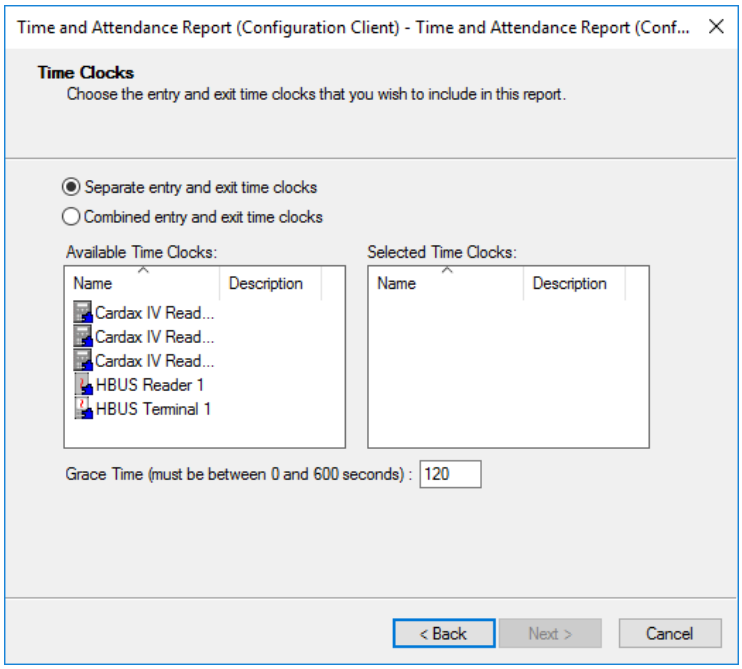
de l'exploitant.

L'outil de recherche peut être utilisé pour localiser les détenteurs de cartes, 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.
Remarque : Seuls les détenteurs de carte qui sont actuellement actifs dans un groupe d'accès seront signalés. Par conséquent, si vous souhaitez que l'état inclue les membres "expirés" du groupe d'accès, vous devez sélectionner les détenteurs de carte plutôt que les groupes d'accès. La "suppression automatique des membres expirés" des groupes d'accès modifie les informations dans l'état en fonction de la date d'exécution de l'état.

Si un opérateur sélectionne l'option **Tous les détenteurs de carte**, l'état est exécuté pour tous les détenteurs de carte dans la division actuelle de l'opérateur.

Si vous souhaitez supprimer un titulaire de carte de votre liste à droite, cliquez avec le bouton droit sur le Titulaire de carte et cliquez sur **Supprimer de la liste**.

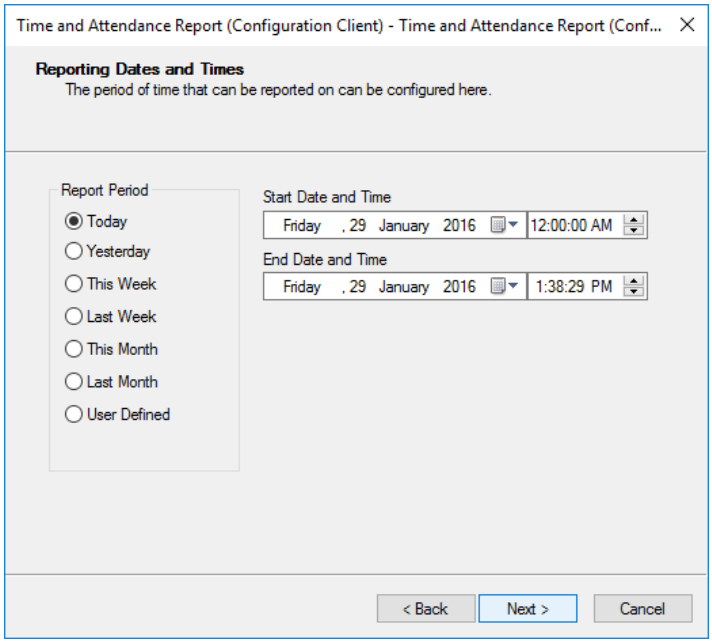
page Horloges temporelles



Cette page fournit une liste des horloges temporelles disponibles ou des lecteurs, à partir desquels un opérateur peut sélectionner celles à inclure dans le rapport. L'opérateur doit également indiquer s'il utilise des horloges de temps d'entrée et de sortie combinées ou séparées (voir les explications ci-dessous), et ajuster le temps de grâce pour les événements en double si nécessaire.
Horloges d'entrée et de sortie séparées : Un lecteur/horloge pour l'entrée et un autre lecteur/horloge pour la sortie.
Horloges d'entrée et de sortie combinées : Un titulaire de carte peut glisser sa carte sur n'importe quel lecteur (entrée ou sortie), et la PREMIÈRE lecture/badge est prise comme la lecture "Entrée" et la lecture SUIVANTE/badge est prise comme la lecture "Sortie" pour ce titulaire de carte.

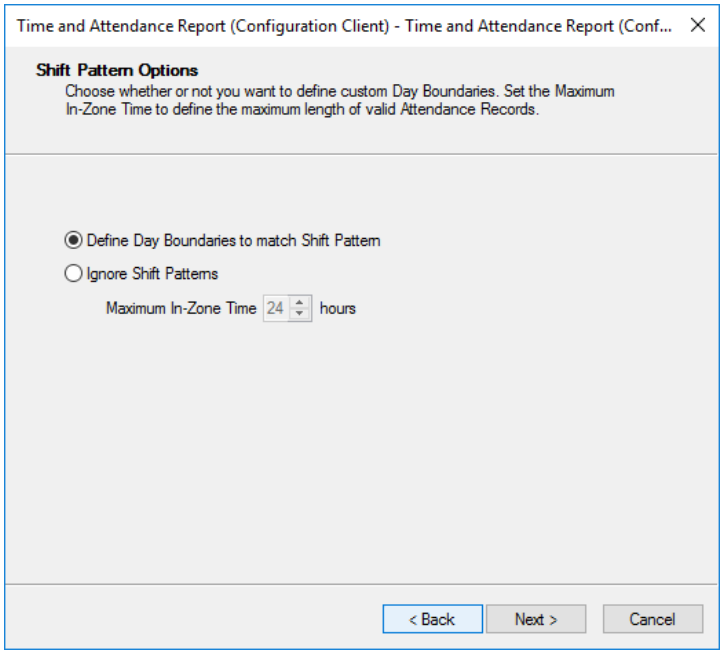
Le système ne vérifie pas non plus que l'entrée ou la sortie a été effectivement prise, car certains sites utilisent simplement les lecteurs comme horloges de temps, de sorte qu'ils ne sont pas attachés aux portes du tout

page Dates et heures de rapport



Cette page permet à un opérateur d'entrer une heure de début et de fin pour l'état. Des périodes prédéfinies sont fournies pour plus de simplicité, ou des heures de début et de fin personnalisées peuvent être entrées.

page Shift Pattern Options

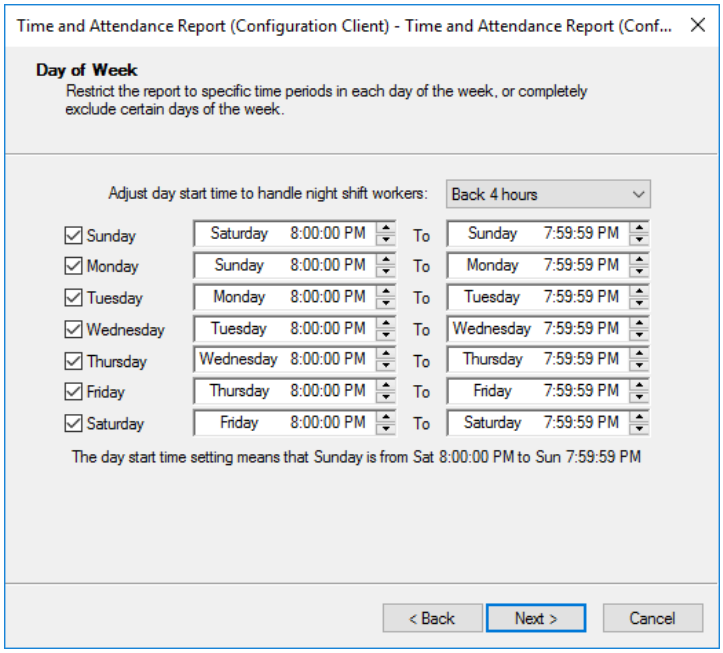


Cette page fournit des options d'opérateur permettant de déterminer les règles à appliquer lors du calcul des enregistrements de présence pour l'état. Il n'affiche que si **Détail**, **Résumé** ou **Rapport d'exception** a été sélectionné sur la première page de l'assistant, (c'est-à-dire la page Style de rapport). Elle ne s'affiche pas si l'option

Rapport d'absence est sélectionnée. Si vous cliquez sur le bouton d'option Définir les limites du jour pour correspondre au modèle de décalage et sur le bouton Suivant, la page 'Jour de la semaine' s'affiche.

Si vous cliquez sur le bouton d'option **Ignorer les modèles de décalage**, puis sur le bouton **Suivant**, la page Génération et enregistrement du rapport s'affiche (en ignorant la page Jour de la semaine). L'option Ignorer les répétitions de décalage détermine la sortie de rapport appropriée à l'aide des règles de répétition de décalage flexible. Lorsque cette option est sélectionnée, elle active également le champ **Durée maximale dans** la **zone** utilisé par les règles de répétition de décalage flexible. La figure saisie dans ce champ détermine la durée au-delà de laquelle le titulaire de la carte est sorti sans badger sa carte. Voir les ***règles*** relatives aux modèles de décalage flexibles ***(page 39-46) pour une explication complète de ces règles, et les exemples de travail*** (page 39-48) pour aider à expliquer le fonctionnement de cette option.

page Jour de la semaine



Cette page permet d'appliquer des restrictions de temps au cours de la période globale de rapport. Elle s'affiche uniquement si l'option **Rapport d'absence** a été sélectionnée sur la première page de l'assistant (c'est-à-dire la page Style de rapport) ou si le bouton d'option **Définir les limites de jour pour correspondre au modèle de décalage** a été sélectionné sur la page **Options de** modèle de décalage. Certains jours de la semaine peuvent être exclus du rapport, ou le rapport peut être limité à une tranche de temps spécifique dans certains jours de la semaine. L'opérateur peut également ajuster l'heure de début de la journée pour accommoder les travailleurs de quart de nuit (c'est-à-dire déplacer le concept de minuit).

page Génération et enregistrement de rapports

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*** (page 39-3) dans la procédure *Création d'un nouveau rapport* pour plus de détails.

Flexibilité des règles de modèle de décalage

Lorsque l'option Ignorer les motifs de décalage est sélectionnée dans la page 'Options de motif de décalage' de l'assistant Rapport de présence et de temps, les règles suivantes s'appliquent :

Événements Utilisables

1. Les événements suivants décrivent les événements qui seront utilisés pour créer des enregistrements de présence.
   - Un événement d'entrée ne sera utilisé que si son événement suivant est un événement de sortie, ou s'il n'a aucun événement ultérieur dans le délai du rapport. Un événement Entry ne sera PAS utilisé si son événement suivant est également un événement Entry.
   - Un événement Exit ne sera utilisé que si l'événement précédent est un événement Entry ou s'il n'a pas d'événement précédent dans le délai du rapport.
     Un événement Exit ne sera PAS utilisé si son événement précédent est également un événement Exit.
   - La facilité d'utilisation d'un événement dépend de la validité de l'enregistrement de présence. Voir "Enregistrements de présence valides" ci-dessous.

Création d'enregistrements de présence normaux

2. Un enregistrement de présence normal est créé en recherchant le premier événement d'entrée utilisable non utilisé pour un titulaire de carte et en le faisant correspondre avec l'événement de sortie utilisable suivant pour déterminer le temps total contigu en zone pour le titulaire de carte. Reportez-vous à la section "Événements utilisables" pour la définition des événements d'entrée et de sortie utilisables.

Créer des enregistrements de présence en utilisant des hypothèses

3. Si le premier événement du titulaire de la carte est un événement de sortie, supposez que le titulaire de la carte était en zone à la date et heure de début du rapport et créez un enregistrement de présence pour refléter cela. Utilisez la date et l'heure de début de l'état comme date et heure de début. NB : L'enregistrement de présence résultant sera soumis à la règle "enregistrements de présence valides" (voir ci-dessous).
4. Si l’événement final du titulaire de la carte est un événement d’entrée, supposez que le titulaire de la carte était dans la zone à la date de fin du rapport et à l’heure de fin du rapport et créez un enregistrement de présence pour refléter cet événement. Utilisez la date et l'heure de fin de l'état comme heure de sortie. NB : L'enregistrement de présence résultant sera soumis à la règle "enregistrements de présence valides" (voir ci-dessous).

Enregistrements de présence valides

5. Tout enregistrement de présence dont le temps de présence est supérieur au temps maximal en zone est considéré comme non valide. L'événement Entry et l'événement Exit pour cet enregistrement doivent être classés comme inutilisables et signalés en conséquence.
6. Les limites de jour ne sont pas prises en compte dans les règles de modèle de décalage flexible. Présence Les enregistrements qui s'étendent sur une frontière de jour sont considérés comme valides.

Créer des enregistrements de participation récapitulative

7. Un enregistrement de présence de synthèse est créé en combinant tous les enregistrements de présence valides (pour un titulaire de carte particulier) qui ont la même date de saisie, indépendamment de la date de fin de l'enregistrement de présence.
8. Un enregistrement de présence de synthèse est associé à une date-heure de saisie égale à la date-heure de saisie du premier enregistrement de présence dans le groupe résumé et à une date-heure de fin égale à la date-heure de fin du dernier enregistrement de présence dans le groupe résumé.
9. Le total du temps de travail de l'enregistrement de présence sommaire est égal à la somme du temps de travail de tous les enregistrements de présence du groupe résumé (à tout moment où le titulaire de la carte était absent entre la date et l'heure d'entrée de l'enregistrement de présence sommaire et la date et l'heure de fin ne sont pas incluses).

Enregistrements de présence de synthèse valides

10. Tous les enregistrements sommaires de présence calculés sont considérés comme valides, quelle que soit leur longueur.
11. Si des événements inutilisables se produisent entre la date et l'heure de début et de fin de l'enregistrement de participation sommaire, les événements inutilisables sont ignorés et cela n'invalide pas l'enregistrement de participation sommaire.
12. Le paramètre Durée maximale en zone n'est pas pris en compte lors de la création d'enregistrements de présence récapitulatifs. Le temps de travail total d'un enregistrement de présence résumé peut dépasser le paramètre Temps maximum en zone, mais aucun des enregistrements de présence individuels dans le groupe résumé ne sera utilisé.

Exemples de travail

Les exemples suivants expliquent le fonctionnement de l'option "Ignorer les modèles de décalage" dans le **rapport** de **présence et de temps**, en montrant des exemples de sortie de rapport. Quatre exemples sont fournis, les exemples 1 à 3 étant des exemples de "rapport détaillé" et l'exemple 4 étant un exemple de "rapport sommaire".

Exemple 1 : Heure maximale dans la zone (rapport détaillé)

Exemple 2 : Le premier événement est une sortie ou le dernier événement est une entrée (rapport détaillé)

Exemple 3 : Événements Entrée ou Sortie manquants (Rapport détaillé)

Exemple 4 : Rapport de synthèse

Exemple 1 : Durée maximale dans la zone (rapport détaillé)

Dans cet exemple, les données brutes contiennent un événement Entry et un événement Exit qui entraînerait un enregistrement de présence non valide. Le titulaire de la carte a quitté le travail le lundi et a reculé dans la matinée du mardi.

Données brutes

Event	Date	Time
Entry	Mon 22 Jan	8:30 a.m.
Exit	Mon 22 Jan	12:30 p.m.
Entry	Mon 22 Jan	1:00 p.m.
Exit	Tue 23 Jan	12:30 p.m.
Entry	Tue 23 Jan	1:00 p.m.
Exit	Tue 23 Jan	5:00 p.m.

Rapport scénario 1

Dans ce scénario, nous utilisons les données brutes ci-dessus et définissons les valeurs suivantes lors de l'exécution du rapport.

Date-Heure de début du rapport :	Lundi 22 janvier 2007 :00:00
Date/Heure de fin du rapport :	Mardi 23janvier 23:59:59
Maximum Dans La Zone :	24 heures

Sortie du rapport

L'événement d'entrée à 13h le lundi est jumelé à l'événement de sortie à 12h30 le mardi et un enregistrement de présence est créé pour 23.5hrs. Ceci est traité comme un enregistrement valide car sa longueur est inférieure au paramètre Maximum In-Zone Time de 24 heures.

Entry Clock	Entry Card	Entry Date/Time	Exit Clock	Exit Card	Exit Date/Time	Time Worked
Main Entry Reader	501	22/01/2007 8:30:00 a.m.	Main Exit Reader	501	22/01/2007 12:30:00 p.m.	4:00:00
Main Entry Reader	501	22/01/2007 1:00:00 p.m.	Main Exit Reader	501	23/01/2007 12:30:00 p.m.	23:30:00
Main Entry Reader	501	23/01/2007 1:00:00 p.m.	Main Exit Reader	501	23/01/2007 5:00:00 p.m.	4:00:00
					Total Working Time (Excluding insufficient Data):	31:30:00

Scénario de rapport 2

Dans ce scénario, nous utilisons les mêmes données brutes mais réduisons le paramètre Maximum In-Zone Time à 20 heures.

Rapport Date et heure de début : lundi 2007 00:00:00

Rapport Date-Heure De Fin : Mardi, 23Jan 2007 23:59:59

Durée maximale dans la zone : 20 heures

Sortie du rapport

Maintenant, l'événement d'entrée à 13h00 le lundi n'est pas jumelé à l'événement de sortie à 12h30 le mardi parce que l'enregistrement de présence résultante serait non valide parce que sa longueur (23,5hrs) dépasserait le paramètre Maximum In-Zone Time de 20hrs. Au lieu de cela, ces événements sont affichés montrant "Données insuffisantes".

Entry Clock	Entry Card	Entry Date/Time	Exit Clock	Exit Card	Exit Date/Time	Time Worked
Main Entry Reader	501	22/01/2007 8:30:00 a.m.	Main Exit Reader	501	22/01/2007 12:30:00 p.m.	4:00:00
Main Entry Reader	501	22/01/2007 1:00:00 p.m.				Insuff. D.
			Main Exit Reader	501	23/01/2007 12:30:00 p.m.	Insuff. D.
Main Entry Reader	501	23/01/2007 1:00:00 p.m.	Main Exit Reader	501	23/01/2007 5:00:00 p.m.	4:00:00
					Total Working Time (Excluding insufficient Data):	8:00:00

Exemple 2 : Le premier événement est une sortie ou le dernier événement d'entrée (rapport détaillé)

Dans cet exemple, le premier événement du titulaire de la carte dans la période de déclaration est un événement de sortie et le dernier événement du titulaire de la carte dans la période de déclaration est un événement d'entrée.

Données brutes

Event	Date	Time
Exit	Mon 22 Jan	12:30 p.m.
Entry	Mon 22 Jan	1:00 p.m.
Exit	Mon 22 Jan	5:00 p.m.
Entry	Tue 23 Jan	8:30 a.m.
Exit	Tue 23 Jan	12:30 p.m.
Entry	Tue 23 Jan	1:00 p.m.

Rapport scénario 1

Dans ce scénario, nous utilisons les données brutes ci-dessus et définissons les valeurs suivantes lors de l'exécution du rapport.

Rapport Date et heure de début : lundi 2007 00:00:00

Rapport Date-Heure De Fin : Mardi**,** 23Jan 2007 23:59:59

Durée maximale dans la zone : 24 heures

Sortie du rapport

L'intervalle entre la date et l'heure de début de l'état (22 janv.) et le premier événement (un événement de sortie) est de 12,5 heures, ce qui ne dépasse pas le paramètre Maximum In-Zone Time (24 heures). Par conséquent, un enregistrement de présence est créé à l'aide de la date et de l'heure de début de l'état comme l'heure d'entrée supposée.

De même, le temps écoulé entre le dernier événement (un événement d'entrée) et la date et l'heure de fin de l'état ne dépasse pas le paramètre Heure maximale dans la zone, de sorte qu'un enregistrement de présence est créé à l'aide de la date et de l'heure de fin de l'état comme heure de sortie supposée.

Notez que si le temps maximum dans la zone avait été fixé à 10hrs, alors les premier et dernier enregistrements de présence n'auraient PAS été créés car ils dépassent cette longueur.

Entry Clock	Entry Card	Entry Date/Time	Exit Clock	Exit Card	Exit Date/Time	Time Worked
Report Start Date-Time		22/01/2007 12:00:00 a.m.	Main Exit Reader	501	22/01/2007 12:30:00 p.m.	12:30:00
Main Entry Reader	500	22/01/2007 1:00:00 p.m.	Main Exit Reader	500	22/01/2007 5:00:00 p.m.	4:00:00
Main Entry Reader	501	23/01/2007 8:30:00 a.m.	Main Exit Reader	501	23/01/2007 12:30:00 p.m.	4:00:00
Main Entry Reader	501	23/01/2007 1:00:00 p.m.	Report End Date-Time		23/01/2007 11:59:59 p.m.	10:59:59

Total Working Time (Excluding insufficient Data): 31:29:59

Scénario de rapport 2

Dans ce scénario, nous utilisons les mêmes données brutes que dans le scénario 1, mais nous utilisons un calendrier de rapport différent. Nous ferons un rapport sur l'ensemble du mois (1er janvier - 31janvier).

Date-Heure de début du rapport :	Lundi 1er janvier 2007 00:00:00
Date/Heure de fin du rapport :	Mercredi 31 janvier 2007 23:59:59
Maximum Dans La Zone:	24 heures

Sortie du rapport

Le premier événement du titulaire de carte dans le délai de déclaration est un événement de sortie et le temps écoulé entre la date et l'heure de début du rapport et ce premier événement dépasse le temps maximum dans la zone, donc aucun enregistrement de présence n'est créé.

De même, le temps écoulé entre le dernier événement (un événement d'entrée) et la date de fin de l'état dépasse le paramètre Heure maximale dans la zone, de sorte qu'aucun enregistrement de présence n'est créé.

Entry Clock	Entry Card	Entry Date/Time	Exit Clock	Exit Card	Exit Date/Time	Time Worked
			Main Exit Reader	501	22/01/2007 12:30:00 p.m.	Insuff. D.
Main Entry Reader	500	22/01/2007 1:00:00 p.m.	Main Exit Reader	500	22/01/2007 5:00:00 p.m.	4:00:00
Main Entry Reader	501	23/01/2007 8:30:00 a.m.	Main Exit Reader	501	23/01/2007 12:30:00 p.m.	4:00:00
Main Entry Reader	501	23/01/2007 1:00:00 p.m.				Insuff. D.
					Total Working Time (Excluding insufficient Data):	8:00:00

Commentaires

Notez que les mêmes données brutes ont produit des temps de travail totaux différents dans des rapports différents. Pour minimiser cet effet, le temps maximum dans la zone doit être défini aussi bas qu'il est possible de le faire sans exclure les enregistrements de présence valides, et les délais de rapport doivent être définis sur la période minimale requise pour couvrir toutes les données brutes souhaitées.

Exemple 3 : Événements d'entrée ou de sortie manquants (rapport détaillé)

Dans cet exemple, les données brutes contiennent plusieurs événements Entry consécutifs et plusieurs événements Exit consécutifs. Le lundi, le détenteur de la carte s'est taillé pour le déjeuner. Mardi, le détenteur de la carte est rentré après le déjeuner.

Données brutes

Event	Date	Time
Entry	Mon 22 Jan	8:30 a.m.
Entry	Mon 22 Jan	1:00 p.m.
Exit	Mon 22 Jan	5:00 p.m.
Entry	Tue 23 Jan	8:30 a.m.
Exit	Tue 23 Jan	12:30 p.m.
Exit	Tue 23 Jan	5:00 p.m.

Rapport scénario 1

Dans ce scénario, nous utilisons les données brutes ci-dessus et définissons les valeurs suivantes lors de l'exécution du rapport.

Date-Heure de début du rapport : Lundi 22 janvier 2007 00:00:00

Date/Heure de fin du rapport : Mardi 23janvier 2007 23:59:59

Maximum Dans La Zone : 24 heures

Sortie du rapport

Le premier événement d'entrée est inutilisable car son événement suivant n'est pas un événement de sortie, de sorte qu'aucun enregistrement de présence n'est créé. L'événement affiche "Données insuffisantes".

De même, le dernier événement de sortie est inutilisable car son événement précédent n'est pas un événement d'entrée. Par conséquent, aucun enregistrement de présence n'est créé. L'événement s'affiche avec "Données insuffisantes".

Entry Clock	Entry Card	Entry Date/Time	Exit Clock	Exit Card	Exit Date/Time	Time Worked
Main Entry Reader	501	22/01/2007 8:30:00 a.m.				Insuff. D.
Main Entry Reader	501	22/01/2007 1:00:00 p.m.	Main Exit Reader	501	22/01/2007 5:00:00 p.m.	4:00:00
Main Entry Reader	501	23/01/2007 8:30:00 a.m.	Main Exit Reader	501	23/01/2007 12:30:00 p.m.	4:00:00
			Main Exit Reader	501	23/01/2007 5:00:00 p.m.	Insuff. D.
					Total Working Time (Excluding insufficient Data):	8:00:00

Commentaires

Dans cet exemple, l'extension de l'intervalle de temps du rapport pour qu'il commence plus tôt et/ou se termine plus tard n'affecte pas la sortie du rapport, car les dates de début et de fin du rapport ne sont pas utilisées pour créer des enregistrements de présence quelconque.

Exemple 4 : Rapport de synthèse

Dans cet exemple, les données brutes contiennent les événements Entry et Exit correspondants qui se croisent sur minuit. Le titulaire de carte travaille le lundi matin, le mardi soir, le mercredi et le jeudi après-midi, et a congé le vendredi.

Données brutes

Event	Date	Time
Entry	Mon 22 Jan	7:00 a.m.
Exit	Mon 22 Jan	11:30 a.m.
Entry	Mon 22 Jan	12:00 p.m.
Exit	Mon 22 Jan	3:30 p.m.
Entry	Tue 23 Jan	11:00 p.m.
Exit	Wed 24 Jan	3:00 a.m.
Entry	Wed 24 Jan	3:30 a.m.
Exit	Wed 24 Jan	7:30 a.m.
Entry	Wed 24 Jan	11:00 p.m.
Exit	Thu 25 Jan	3:00 a.m.
Entry	Thu 25 Jan	3:30 a.m.
Exit	Thu 25 Jan	7:30 a.m.
Entry	Thu 25 Jan	3:00 p.m.
Exit	Thu 25 Jan	7:00 p.m.
Entry	Thu 25 Jan	7:30 p.m.
Exit	Thu 25 Jan	11:30 p.m.

Rapport scénario 1

Dans ce scénario, nous utilisons les données brutes ci-dessus et définissons les valeurs suivantes lors de l'exécution du rapport.

Date-Heure de début du rapport :	Lundi 22 janvier 2007 00:00:00
Date/Heure de fin du rapport :	vendredi 26 janvier 2007 23:59:59
Maximum Dans La Zone :	20 heures

Sortie du rapport

Le titulaire de la carte a travaillé un total de 8 heures le lundi (les pauses déjeuner sont exclues).

Le mardi, le titulaire de la carte commence un quart de nuit à 11:00pm et horloges dehors pour une pause à 3:00 mercredi matin, donc le rapport montre que cela comme un total de 4 heures pour le mardi.

La deuxième moitié de l'équipe de nuit du mardi (mercredi matin) est combinée à la première moitié de l'équipe de nuit du mercredi pour donner un total de 8 heures pour le mercredi.

La deuxième moitié du quart de travail du mercredi soir (jeudi matin) est combinée avec le quart de travail du jeudi après-midi pour donner un total de 12 heures pour le jeudi.

Entry Clock Name	First Entry Date/Time	Exit Clock Name	Exit Date/Time	Time Worked
Main Entry Reader	22/01/2007 7:00:00 a.m.	Main Exit Reader	22/01/2007 3:30:00 p.m.	8:00:00
Main Entry Reader	23/01/2007 11:00:00 p.m.	Main Exit Reader	24/01/2007 3:00:00 a.m.	4:00:00
Main Entry Reader	24/01/2007 3:30:00 a.m.	Main Exit Reader	25/01/2007 3:00:00 a.m.	8:00:00
Main Entry Reader	25/01/2007 3:30:00 a.m.	Main Exit Reader	25/01/2007 7:30:00 a.m.	12:00:00
			Total Working Time (Excluding insufficient Data):	32:00:00

Commentaires

Comme le titulaire de la carte effectue des pauses de mi-quart, les heures de quart de nuit sont réparties sur différents jours - la première moitié du quart étant affichée un jour et la deuxième moitié du quart étant affichée le lendemain. Pour que l'ensemble de l'équipe de nuit du mardi soit inclus dans le total de mardi, le titulaire de la carte ne doit pas se retirer entre minuit et la fin de l'équipe.

Veuillez noter que si la date et l'heure de fin du rapport avaient été fixées au mercredi 24 janvier 2007 00:00:00, l'heure de fin du mardi ne s'afficherait qu'à 1 heure, car le rapport supposerait une sortie à la date et l'heure de fin du rapport.

Rapport de configuration de site

Introduction

Le rapport de configuration du site permet à un opérateur d'obtenir un enregistrement papier de la configuration des éléments sélectionnés. Le rapport peut être généré pour tout élément sélectionné au sein de la division de l'exploitant. Les éléments **non** signalés sont les suivants : CryptSeed, Code site, Titulaire de carte, groupe d'accès, champs Donnée personnelle, groupe opérateur et privilège opérateur.

Les opérateurs doivent disposer des privilèges "Visualiser le site" et "Modifier les descriptions de rapports" pour créer, enregistrer, modifier et supprimer des rapports de configuration de site. La division système limite le niveau d'informations sur les articles qu'un opérateur peut consulter dans le rapport.

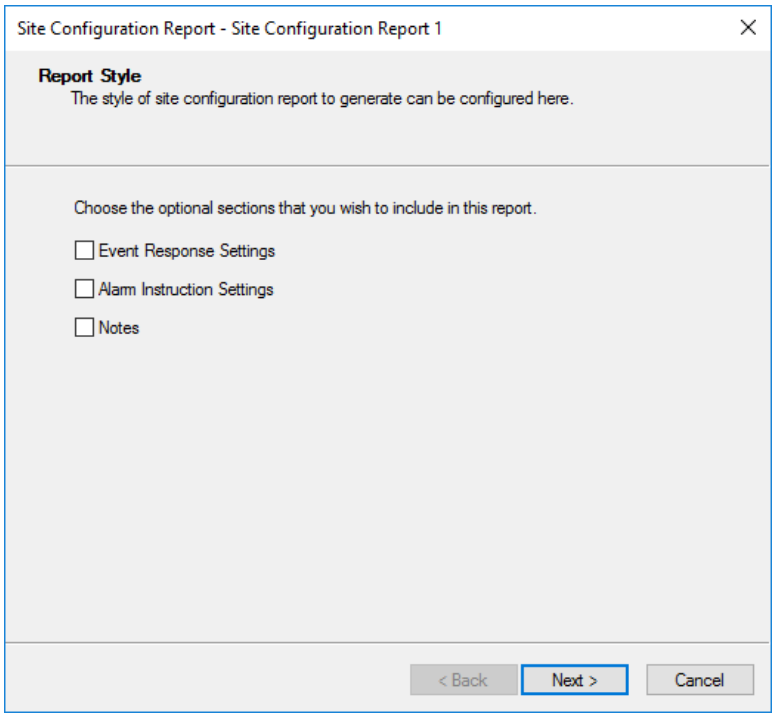
Remarque : Le rapport de configuration du site peut être utilisé pour les visites de garde (c'est-à-dire qu'il peut énumérer les points de contrôle qu'un agent de sécurité doit suivre sur un itinéraire spécifique de visite de garde et indiquer les heures permises (et les tolérances) entre les points de contrôle).
Le rapport peut être exécuté pour que :

- Le texte contenu dans l'onglet **Notes** d'une visite guidée peut être affiché sur le rapport (en cochant la case **Notes** de la page **Style de rapport**). Cela permet d'imprimer des instructions spéciales pour le gardien.
- toutes les autres données de configuration de site sont éliminées (dans la **page Sélectionner des éléments)**.

Assistant Rapport

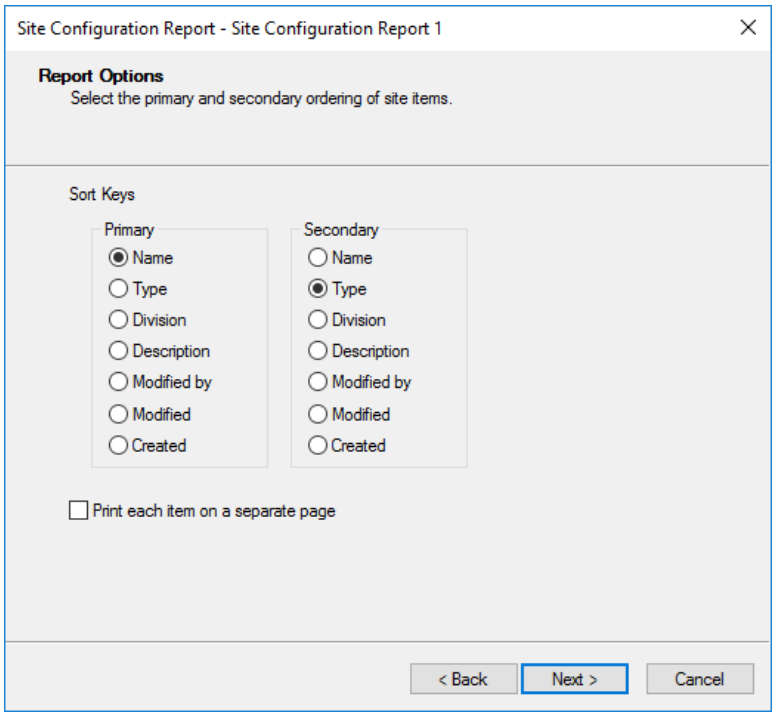
L'Assistant Rapport de configuration de site contient un certain nombre de pages qui vous invitent à créer un rapport.
Suivez les instructions affichées.

page Style de rapport



Il s'agit de la première page du rapport de configuration du site et permet à l'opérateur de choisir la ou les sections facultatives à inclure dans le rapport (c'est-à-dire qu'une ou deux options ou que les trois options peuvent être sélectionnées).

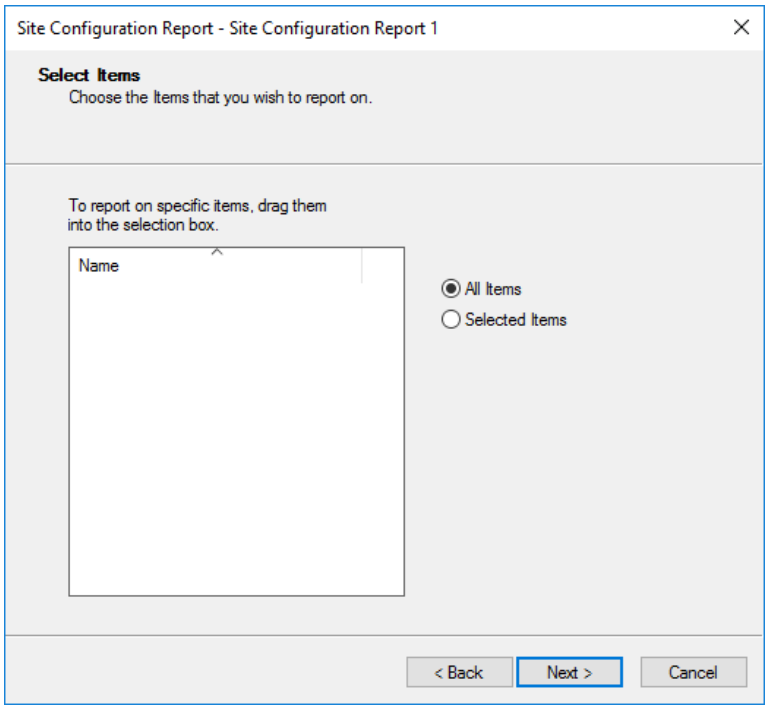
page Options du rapport



Cette page permet à l'opérateur de choisir une clé de tri primaire et secondaire pour l'état. Les clés de tri par défaut sont "Nom" pour la clé primaire et "Type" pour la clé secondaire.

L'opérateur peut également choisir d'imprimer chaque élément sur une page distincte ou de l'imprimer en continu.

page Sélectionner des éléments



Cette page permet à l'opérateur d'inclure des éléments spécifiques dans le rapport (c'est-à-dire tous les éléments ou les éléments sélectionnés). Si l'opérateur sélectionne le bouton radio pour tous les éléments, le bouton **Suivant** est activé. Toutefois, si l'opérateur sélectionne le bouton radio pour les éléments sélectionnés, le bouton **Suivant** ne sera pas activé tant que les éléments n'auront pas été placés dans la zone de sélection.

L'opérateur peut soit utiliser l'outil de recherche pour rechercher des éléments, puis les faire glisser et les déposer dans la zone de sélection en tant que critères pour ce rapport, soit faire glisser des éléments depuis les fenêtres de la liste principale.

page Génération et enregistrement de rapports

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*** (page 39-3) dans la procédure *Création d'un nouveau rapport* pour plus de détails.

Rapport d'affectation Contact ID

Introduction

Le rapport d'attribution Contact ID permet à un opérateur de produire un rapport de toutes les chaînes Contact ID possibles qui peuvent être envoyées à partir d'un numéroteur vers une station de surveillance à distance. Ce rapport est conçu pour être envoyé à la station de surveillance distante afin de les aider à interpréter les messages Contact ID pour ce site. Consultez la section Surveillance externe des alarmes pour plus de détails.
Le rapport comporte les trois sections suivantes :

Zones d'alarme : Les zones d'alarme répertoriées sont toutes celles avec une valeur GG autre que 00.

Titulaires de carte : Les titulaires de carte qui figurent sur la liste sont tous ceux dont la valeur CCC est autre que 000.

Code régional de l'ID du contact (GG) : Les éléments de cette section sont les suivants :
- un onglet **de numérotation d'alarme**,
- un CCC autre que 000, et
- une zone d'alarme affectée à l'onglet **Réponse à l'événement**.

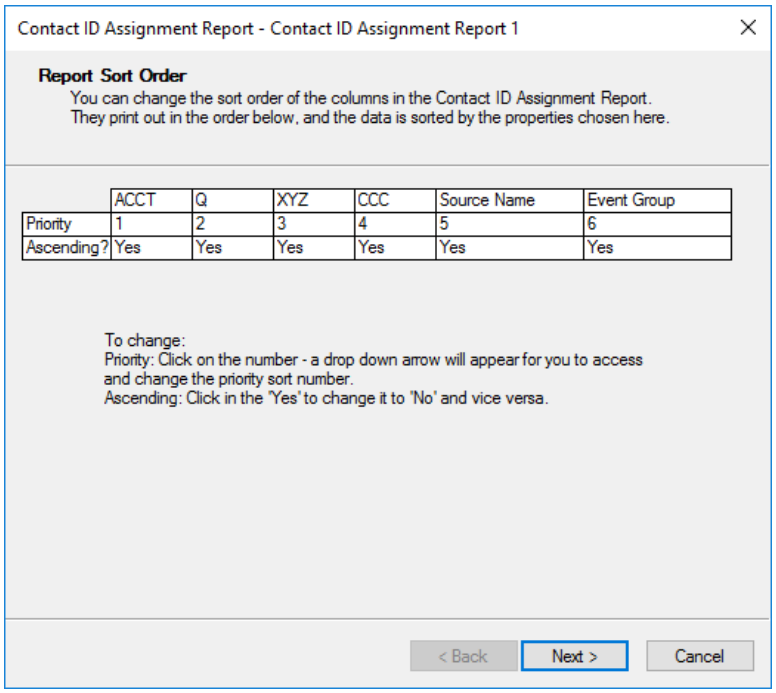
Remarque : Tous les 400 niveaux XYZ plus 121, 313 XYZ sont de type utilisateur, ils s'affichent donc sous la forme "CCC" et "Dépendant de l'utilisateur" dans le rapport plutôt que le nom réel de l'élément de site.

Les opérateurs doivent disposer des privilèges "Visualiser le site" et "Modifier les descriptions de rapports" pour créer, enregistrer, modifier et supprimer les rapports d'affectation Contact ID avec les données Contact ID relatives aux *éléments du site*. Pour créer, enregistrer, modifier et supprimer des rapports d'attribution Contact ID avec des données Contact ID relatives aux *titulaires de carte*, ils doivent disposer du privilège "Modifier les titulaires de carte". La division système restreint le niveau d'informations sur les éléments du site qu'un opérateur peut consulter dans le rapport.

Assistant Rapport

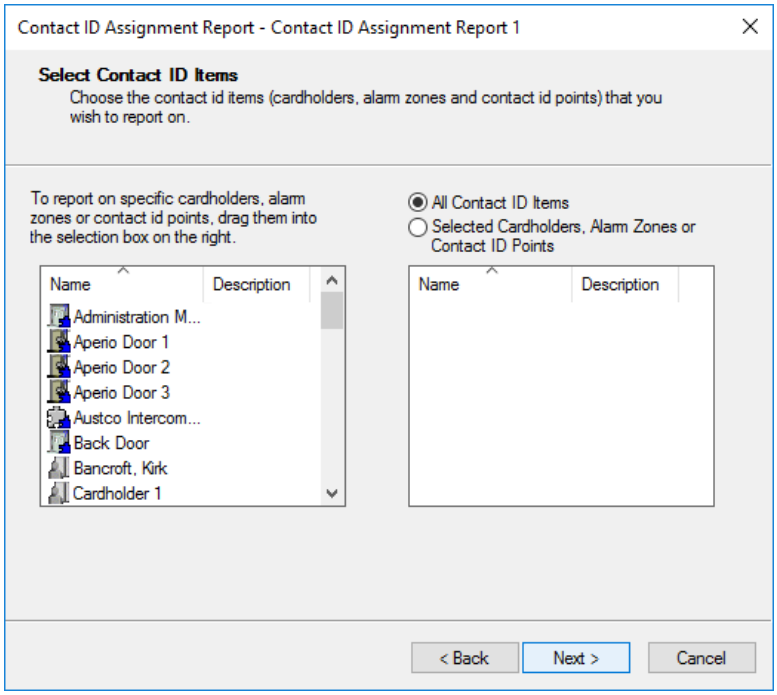
L'Assistant Rapport d'affectation Contact ID contient trois pages qui vous permettent de créer un rapport.
Suivez les instructions affichées.

page Rapport Ordre de tri



Il s'agit de la première page de l'Assistant Rapport d'affectation d'ID contact. Il permet à l'opérateur de modifier l'ordre de tri des colonnes d'un rapport d'affectation Contact ID.
En cliquant sur un numéro de priorité (1-6), une flèche vers le bas apparaîtra à partir de laquelle vous pourrez sélectionner un numéro de tri prioritaire différent. Vous pouvez également choisir de trier une colonne par ordre croissant ou décroissant, en cliquant sur **Oui, qui** passe automatiquement à **Non**, et inversement.

Sélectionner la page Éléments Contact ID



Cette page fournit une liste des éléments d'identification de contact (c'est-à-dire les titulaires de carte, les zones d'alarme et les points d'identification de contact) qu'un opérateur peut inclure dans le rapport, plutôt que d'avoir à signaler tout. Les articles indiqués ici sont réservés à ceux relevant de la division de l'exploitant.

L'outil de recherche peut être utilisé pour localiser les éléments Contact ID, qui peuvent ensuite être glissés et déposés sur cette page. Vous pouvez également ouvrir la fenêtre de liste principale appropriée et faire glisser les éléments dont vous avez besoin sur cette page.

Si vous souhaitez supprimer un élément de votre liste à droite, **faites un clic droit** sur l'élément, puis cliquez **sur Supprimer de la liste**.

Exemple de sortie :

ACCT	Q	XYZ	GG	CCC	Source Name	Event Group
0281	1	130	00	000	Input to be Triggered	Open/Off
0281	3	130	00	000	Input to be Triggered	Open/Off
0282	1	130	00	082	004 on 2.82	Open/Off
0282	1	393	00	282	Modem on 2.82	Alarm Dialling Failure
0282	1	602	00	282	Modem on 2.82	{Periodic Test}
0282	3	130	00	082	004 on 2.82	Open/Off
0282	3	393	00	282	Modem on 2.82	Alarm Dialling Failure
0283	1	393	00	283	Modem on 2.83	Alarm Dialling Failure
0283	1	602	00	283	Modem on 2.83	{Periodic Test}
0283	3	393	00	283	Modem on 2.83	Alarm Dialling Failure
0284	1	130	00	084	004 on 2.84	Open/Off
0284	3	130	00	084	004 on 2.84	Open/Off
1234	1	130	00	000	001	Open/Off
1234	1	130	00	000	002	Open/Off
1234	1	393	00	000	Cardax 3000 Modem	Alarm Dialling Failure
1234	1	602	00	000	Cardax 3000 Modem	{Periodic Test}
1234	1	602	00	000	Flooding # 2	{Periodic Test}
1234	3	130	00	000	001	Open/Off

page Génération et enregistrement de rapports

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*** (page 39-3) dans la procédure *Création d'un nouveau rapport* pour plus de détails.

Rapport de câblage

Introduction

Le rapport de câblage permet à l'opérateur de créer un nouveau rapport, ou un ensemble de rapports, qui peut être exécuté après la configuration du matériel dans le Centre de commandes. Le rapport fournit une documentation qui indique à l'installateur comment le matériel doit être câblé. Idéalement, les programmes d'installation exécuteront ce programme à la fin de l'exécution d'un Assistant pour configurer le matériel.

Les opérateurs ont besoin des privilèges d'opérateur "Visualiser le site" et "Modifier les descriptions de rapports" pour créer, enregistrer, modifier et supprimer les rapports de câblage.

Les éléments qui peuvent être signalés sont énumérés ci-dessous :

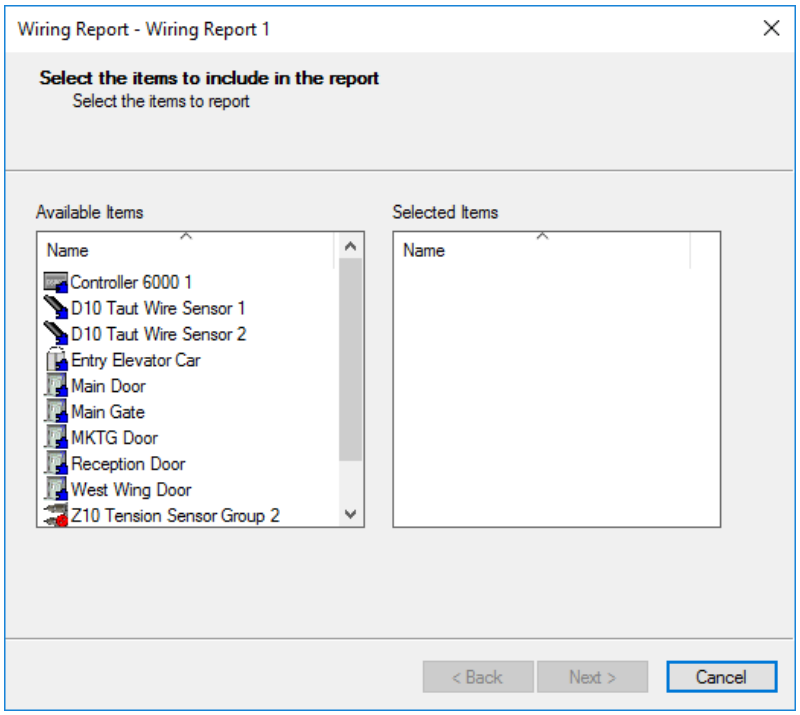
Contrôleur 6000s

Périphériques HBUS :	Contrôleur de clôture HBUS F31/F32/F41/F42 Contrôleur de clôture HBUS F22 Groupe de capteurs de tension HBUS Z10 E/S HBUS
Autres :	Portes Ascenseur Voiture

Assistant Rapport

L'Assistant Rapport de câblage ne contient que deux pages qui vous permettent de créer un rapport.
Suivez les instructions affichées.

page 'Sélection de périphériques'



Cette page fournit une liste de tous les éléments qu'un opérateur peut inclure dans le rapport. Faites glisser les éléments dont vous avez besoin de la liste Eléments disponibles, vers la colonne **Eléments sélectionnés** à droite.

Remarque : Tant que la **liste** Eléments sélectionnés sur la droite reste vide, la sera désactivé.

Si vous souhaitez supprimer un élément de la liste Éléments sélectionnés, cliquez avec le bouton droit sur l'élément et cliquez sur **Supprimer de la liste**.

page Génération et enregistrement de rapports

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*** (page 39-3) dans la procédure *Création d'un nouveau rapport* pour plus de détails.

Rapports générés automatiquement

Introduction

Les trois états suivants peuvent être définis pour être générés automatiquement :
Remarque : Il existe plusieurs façons de planifier la génération automatique de ces rapports. Pour obtenir des exemples, reportez-vous à la section ***Configuration de la planification des rapports*** (page 39-65).

Type de rapport	But
Rapport d'évacuation (appelé rapport d'évacuation automatique)	Utilisé dans les situations d'urgence (par ex. évacuation en cas d'incendie).
Rapport des exceptions	Utilisé principalement à des fins d'information (p. ex. portes actuellement déverrouillées qui étaient prévues pour être sécurisées).
Rapport d'activité	Utilisé principalement à des fins d'information (par exemple, des alarmes survenant au cours des 8 dernières heures).

Ces rapports sont pris en charge par des macros de sorte qu'ils peuvent être générés automatiquement lorsqu'un événement système spécifique se produit (par exemple, une alarme incendie dans le cas d'un rapport d'évacuation). Ils sont déclenchés par un événement ou une alarme. Pour générer automatiquement un de ces rapports, une macro qui exécute le rapport doit pouvoir être lancée à partir d'un plan d'action. Grâce à la fonction de planification des macros, ces rapports peuvent être configurés pour s'exécuter automatiquement sur une base planifiée (par exemple toutes les 8 heures à un changement de poste, pour être présentés à la garde suivante).
Remarque : Ces rapports peuvent uniquement être imprimés sur des imprimantes situées sur le même domaine que le serveur. Pour imprimer à partir d'une station de travail, l'utilisateur de la station de travail a besoin de privilèges sur cette imprimante. Voir ***Configuration des imprimantes pour les rapports générés automatiquement via les macros*** (page 39-71) pour plus de détails.

Lorsqu'une macro lance l'un de ces rapports et que le rapport est configuré pour envoyer l'état en mode Aperçu avant impression, l'état échoue car il n'y a pas d'opérateur pour afficher l'aperçu avant impression ou envoyer l'état à une imprimante. Lorsqu'une macro lance un rapport et que le rapport est configuré pour envoyer le rapport à un fichier sur un lecteur local, le rapport est placé sur le lecteur local du serveur Command Center, plutôt que sur le lecteur local de l'opérateur exécutant la macro. Cela est dû au fait qu'il n'y a pas toujours d'opérateur connecté et que le lecteur de station de travail locale peut ne pas être disponible.

Lorsqu'un rapport généré automatiquement est déclenché par une alarme, si le serveur est alors hors ligne, le rapport est généré une fois que le serveur est de nouveau en ligne. Toutefois, si le rapport est inclus dans une macro programmée, après une minute, l'action sera annulée et le rapport ne sera pas produit.

Événements de rapport générés automatiquement

Lorsqu'un rapport généré automatiquement est exécuté, un événement est généré pour indiquer qu'il a été exécuté. La réception d'un événement "Rapport terminé" indique également que le rapport a été spoulé sur l'imprimante. Si cet événement n'est pas généré, cela peut être dû à une configuration d'imprimante incorrecte.

Si l'impression échoue, il en sera ainsi pour les raisons suivantes :

Raison	Résultat
La description du rapport est configurée avec une imprimante inconnue	Une alarme sera générée avec les détails de l'imprimante inconnue.
L'imprimante est hors ligne ou hors papier	Un événement ne sera pas généré, car Command Center ne le saura pas.

Configuration de la planification des rapports

Introduction

Les rapports d'activité, de titulaire de carte, d'exception et d'évacuation peuvent être définis pour être générés automatiquement. Il existe plusieurs façons de configurer la planification des rapports, comme le montrent les deux exemples suivants.

Exemple 1 :
Un rapport d'évacuation est habituellement produit dans une situation d'urgence. Nous recommandons qu'un plan d'action soit mis en place sur l'entrée de sortie d'urgence de la porte afin qu'une alarme soit créée lorsque l'entrée est activée. Une façon de produire automatiquement le rapport d'évacuation lorsque la sortie d'urgence des portes est activée est d'ajouter une macro au plan d'action, où l'action de la macro consiste à imprimer un rapport à un endroit précis.

Exemple 2 :
Une planification peut être configurée pour indiquer à une sortie virtuelle de se mettre en marche à une date ou à une heure données. Lorsque la sortie est activée, elle utilise un plan d'action qui exécute une macro, où l'action de la macro est de produire l'état (c'est-à-dire que si vous configurez la planification pour activer la sortie toutes les 8 heures au moment du changement de poste, un état sera automatiquement produit toutes les 8 heures).

L'exemple 2 a été développé avec plus de détails et est divisé en trois parties, dans l'ordre dans lequel elles doivent être exécutées :

- Configuration d'une macro pour un rapport
- Configuration des options de planification des rapports
- Configuration des déclencheurs de macro de rapport

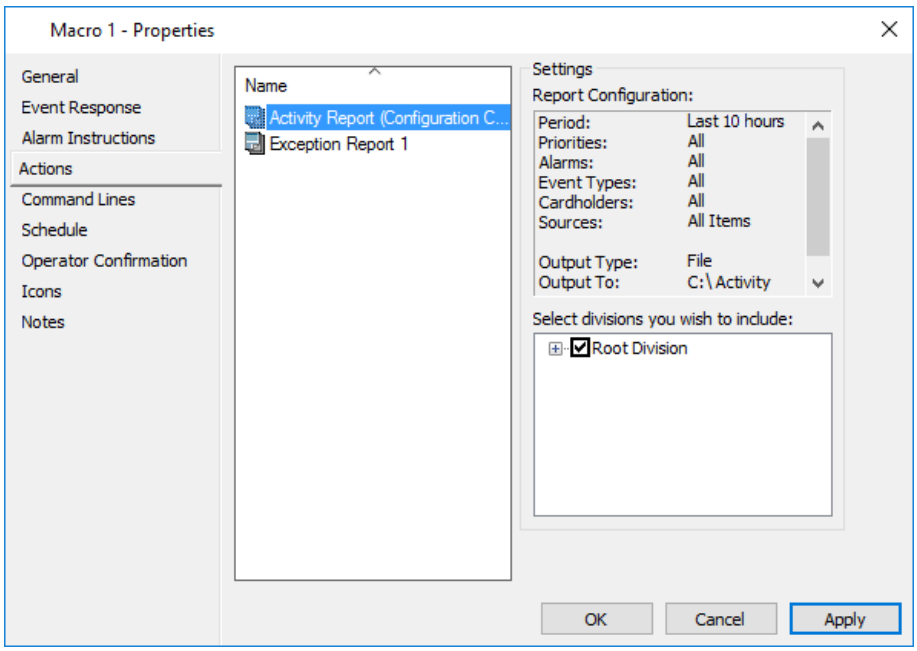
Lorsque cela est nécessaire, cette procédure fait référence à des procédures distinctes, étape par étape, qui sont détaillées ailleurs dans cette aide en ligne.

Exemple 2

Configuration d'une macro pour un rapport

1. Créez une nouvelle macro ou modifiez une macro existante à partir de la fenêtre **Macro** List (Liste principale des macros).
   Reportez-vous à la section Création d'une macro pour la procédure générique de création de macros ou **cliquez avec le bouton droit** sur une macro existante et sélectionnez **Propriétés**.
2. Cliquez sur l'onglet **Actions**.
3. Faites glisser le rapport dont vous avez besoin pour planifier à partir de la **description du rapport** Fenêtre Liste principale, et déposez-la dans la **grille Nom**.
4. Cliquez sur le rapport dans la **grille Nom**.

Les paramètres qui ont été enregistrés pour l'affichage du rapport dans un à droite de la grille Nom.



Remarques :

- Les paramètres du rapport peuvent être modifiés (si vous disposez du privilège opérateur pour modifier le rapport dans la division du rapport), en cliquant avec le bouton droit sur le rapport dans la grille **Nom** et en sélectionnant **Propriétés**.
- Pour les rapports sur les exceptions, les activités et les détenteurs de carte, une grille **Sélectionnez les divisions que vous** souhaitez **inclure**. Vous devez sélectionner l'état dans la grille de noms afin que sa division soit sélectionnée automatiquement.

5. Cliquez sur l'onglet **Planification**.
6. Une ou plusieurs entrées peuvent être ajoutées pour la planification de rapports ponctuels. Reportez-vous à la rubrique Planification d'une macro.
7. Cliquez sur le bouton **OK** pour enregistrer la macro.

Configuration des options de planification des rapports

8. Configurez les catégories de jours et le calendrier par défaut si nécessaire. Reportez-vous à Ajout d'une nouvelle catégorie de jours et Affichage/Modification du calendrier par défaut pour les procédures.
9. Créer une nouvelle planification.
   Reportez-vous à la section Création d'une nouvelle planification.
10. Ajoutez les catégories de jours appropriées pour le type de programme que vous configurez, comme indiqué ci-dessous :

Pour ...	**puis...**
Planification quotidienne, (par exemple, tous les jours h et 16h)	Catégories de jours couvrant tous les jours (semaine et fin de semaine, par exemple).

Pour ...	puis...
Horaire basé sur **le jour de la semaine** (par exemple tous les lundis à 8h et 16h)	Jour Catégorie représentant le lundi.
Jours de la semaine selon l'horaire (par exemple tous les lundis et vendredis à 8 h et 16 h)	Catégories de jour couvrant du lundi au vendredi (par exemple, jour de la semaine).

11. Cliquez sur le bouton **OK** pour enregistrer la planification.

Configuration des déclencheurs de macro Rapport

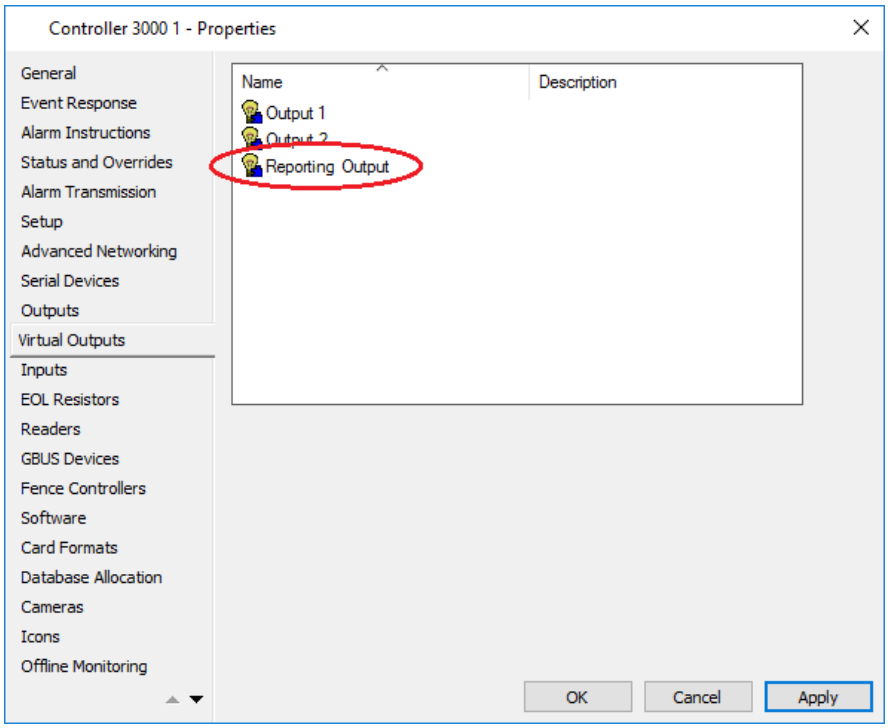
Les étapes nécessaires à la configuration des déclencheurs de macro de rapport sont les suivantes :

a) Configuration d'un déclencheur d'événement (une sortie virtuelle)
b) Liaison de la sortie virtuelle au contrôleur
c) Création d'une zone d'alarme spécifique à la sortie virtuelle
d) Configuration d'un plan d'action

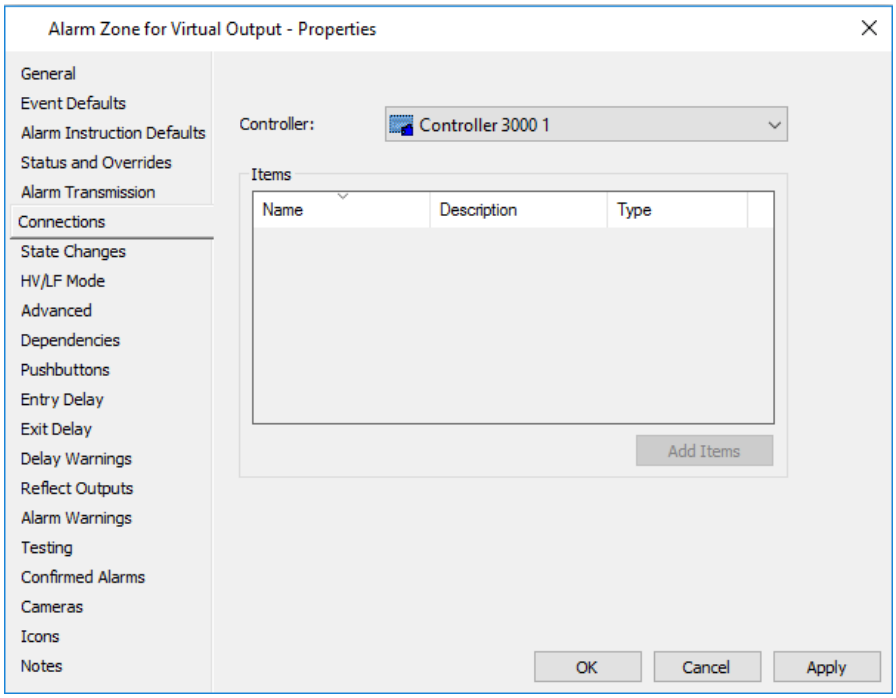
12. Configurez le déclencheur d'événement en créant une nouvelle sortie virtuelle. **Remarque :** Pour répéter la planification des rapports, il est recommandé d'utiliser les sorties virtuelles comme déclencheurs lorsque l'état de la sortie change, par exemple de **OFF à ON**.

    Reportez-vous à ***Création d'entrées et de sorties*** (page 21-44) pour la procédure générique de création de sorties.

13. Cliquez sur le bouton **OK** pour enregistrer la sortie virtuelle.
14. Dans la fenêtre Liste principale du matériel, ouvrez le contrôleur auquel la sortie virtuelle doit être liée.
15. Cliquez sur l'onglet **Sorties virtuelles**.
16. Faites glisser la sortie virtuelle (déjà configurée à l'étape 12) et déposez-la dans la grille.



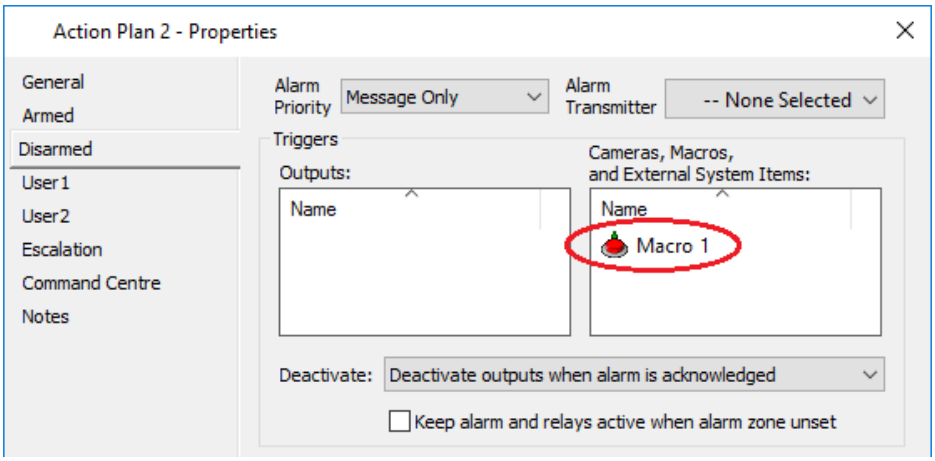
17. Cliquez sur le bouton **OK** pour enregistrer la modification sur le contrôleur.
18. Créez une nouvelle zone d'alarme pour la sortie virtuelle.
    Remarque : Une configuration minimale est nécessaire car il ne s'agit pas d'une zone réelle.
19. Cliquez sur l'onglet **Connexions (Connections)**.
20. Sélectionnez le contrôleur auquel la sortie virtuelle a été liée dans la Liste déroulante **Contrôleur**.



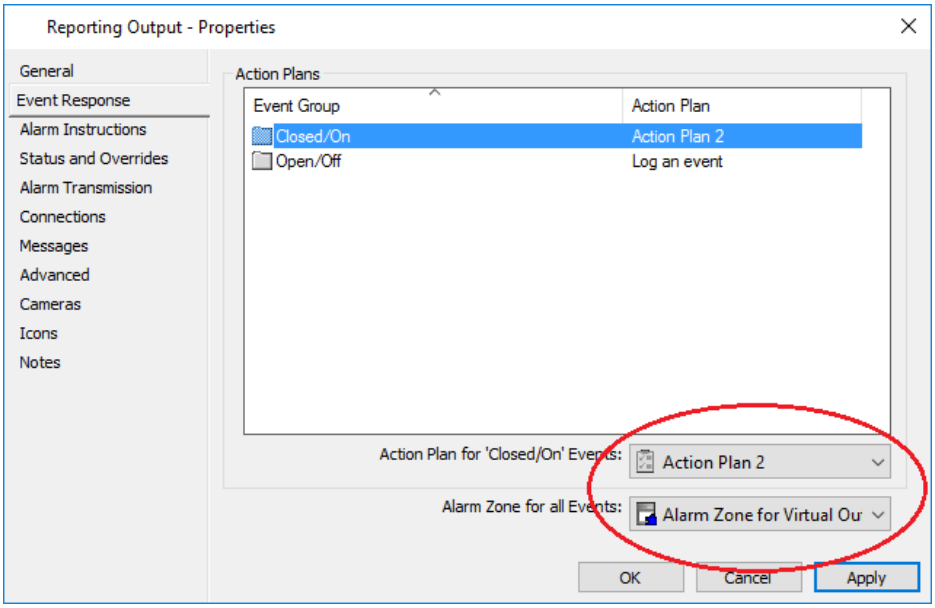
21. Cliquez sur le bouton **OK** pour enregistrer la zone d'alarme.
22. Créer un nouveau plan d'action, ou modifier un plan d'action existant Fenêtre

Liste principale du **plan d'action**.
Reportez-vous à la section Création d'un nouveau plan d'action pour la procédure générique de création de plans d'action ou **cliquez avec le bouton droit** sur un plan d'action existant et sélectionnez **Propriétés**.

23. Cliquez sur l'onglet approprié qui représente l'état de la zone d'alarme.
L'onglet **Désarmé** est sélectionné sur l'exemple ci-dessous.
24. Faites glisser la macro de rapport (déjà configurée à l'étape 1) dans la grille **Appareils photo, Macros et Éléments système externes**.

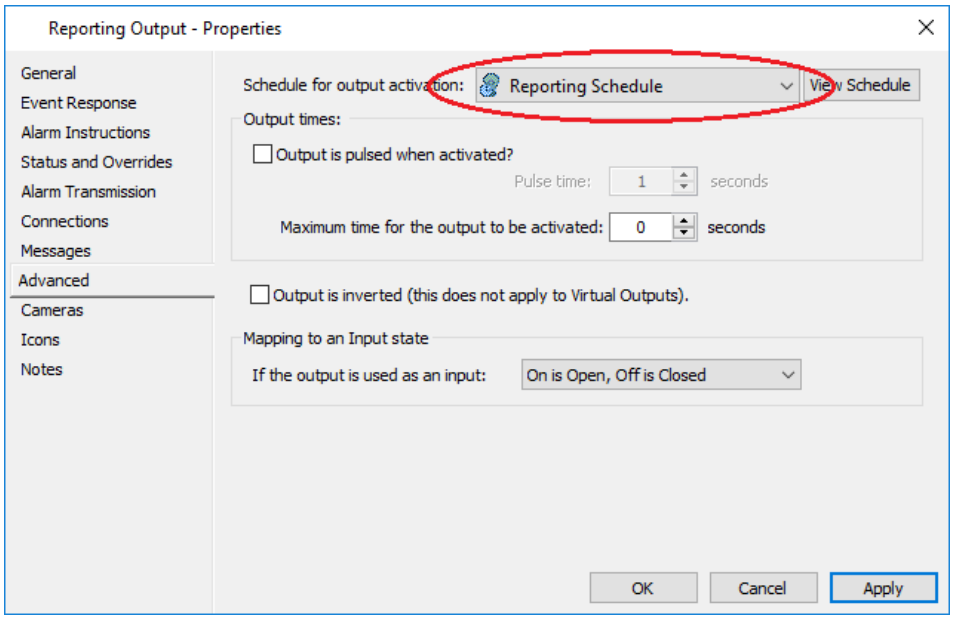


25. Cliquez sur le bouton **OK** pour enregistrer le plan d'action.
26. Rouvrez la sortie virtuelle créée à l'étape 12.
27. Cliquez sur l'onglet **Réponse aux événements**.
28. Sélectionnez le groupe d'événements "Fermé/Activé" et modifiez son plan d'action en le remplaçant par celui qui est configuré à l'étape 22 ci-dessus.
Cela déclenchera l'exécution de la macro de rapport lorsque l'état Sortie passe de **OFF** à **ON**.
29. Sélectionnez la **zone d'alarme** (déjà créée à l'étape 18) dans la liste déroulante.



30. Cliquez sur l'onglet **Avancé (Advanced)**.

31. Sélectionnez le calendrier de rapport (déjà configuré à l'étape 9) **Planification de la** liste déroulante **activation de sortie**.



32. Cliquez sur le **bouton** OK pour enregistrer les modifications apportées à la sortie virtuelle.

Configuration des imprimantes pour les rapports générés automatiquement via les macros

Introduction

Les problèmes liés à l'impression de rapports planifiés à l'aide de macros dépendent du type d'imprimante utilisée (locale ou réseau) et du système d'exploitation sur lequel s'exécute le service FT Command Center.
Détails importants à connaître :

- Les imprimantes réseau ne sont installées que pour l'utilisateur connecté, sauf si elles sont déployées à l'échelle de l'ordinateur.
- Les macros sont exécutées à partir du serveur du Centre de commandes, même si elles sont démarrées à partir d'une station de travail.
- Les macros sont exécutées à l'aide du compte d'utilisateur d'ouverture de session configuré pour le service FT Command Center.
- Si le rapport doit être configuré à partir de la station de travail, la même imprimante devra être installée sur la station de travail et le serveur. Sinon, l'imprimante ne pourra pas être sélectionnée dans la liste déroulante des rapports sur le poste de travail.
- L'authentification pourrait également devenir un problème. Le compte d'utilisateur configuré en tant qu'ouverture de session pour le service FT Command Center doit disposer de droits d'impression sur l'imprimante partagée.

C'est pourquoi un rapport peut s'imprimer correctement lorsqu'il est exécuté manuellement (à partir des propriétés du rapport du Centre de commandes, exécuté sous l'utilisateur connecté). Pour résoudre ces problèmes, suivez l'une des procédures ci-dessous appropriées pour votre système d'exploitation :

MÉTHODE 1

Pour installer une imprimante réseau à l'échelle de l'ordinateur, déployez l'imprimante à l'aide de Rundll32, PrintUI.dll, fonction comme suit :

1. Connectez-vous au serveur du Centre de commandes.
2. Ouvrez une invite de commandes, exécutez-la en tant qu'administrateur et entrez :

   RUNDLL32 PRINTUI.DLL,PrintUIEntry /ga /n\\Server_name\Printer_sharename
3. Le serveur du Centre de commandes devra être redémarré lorsque l'imprimante sera installée lors de la connexion.
4. Lorsque le serveur a redémarré, vérifiez que la nouvelle imprimante est installée en ouvrant une invite de commandes et en entrant :

   RUNDLL32 PRINTUI.DLL,PrintUIEntry /ge

Créez et configurez le rapport (voir ***Création d'un rapport*** page 39-2) et la macro (voir ***Création d'une nouvelle macro*** page 20-2).

MÉTHODE 2

Le compte d'ouverture de session sous lequel le service FT Command Center s'exécute doit être modifié en un compte d'utilisateur ou d'administrateur local.

1. Dans le menu **Démarrer**, cliquez sur **Exécuter...,** et entrez dans services.msc
2. Double-cliquez sur le service FT Command Center.
   La fenêtre des propriétés de service du centre de commandes FT s'affiche.
3. Cliquez sur l'**onglet Connexion,** et sélectionnez la **case d'option Ce compte**.
4. Cliquez sur le bouton Parcourir... pour localiser le nom du compte ou tapez le nom du compte, et entrez le mot de passe pour ce compte.
5. Cliquez sur le bouton **Appliquer (Apply)**.
   Remarque : Le service doit être relancé pour prendre effet.

Remarque : Ces étapes devront être répétées si le Centre de commandes est à nouveau mis à niveau, car l'ouverture de session du service du Centre de commandes FT reviendra au compte du système local chaque fois que le Centre de commandes sera mis à niveau.

Maintenant que le service a été modifié, l'imprimante doit être installée pour cet utilisateur. Cela peut être fait :

- connexion en tant qu'utilisateur et installation de l'imprimante réseau, et
- installation de l'imprimante réseau en tant qu'imprimante locale.
  Remarque : Les imprimantes locales sont installées pour tous les utilisateurs, pas seulement l'utilisateur connecté.

Pour installer une imprimante réseau en tant qu'imprimante locale :

1. Dans le menu **Démarrer**, cliquez sur **Imprimantes et télécopieurs**.
2. Cliquez sur **Fichier dans** la barre de menus, puis sur **Ajouter une imprimante**.
   L'écran de bienvenue de l'Assistant Ajout d'imprimante s'affiche.
3. Cliquez sur le bouton **Suivant**.
4. Cliquez sur le bouton d'option **Imprimante locale connectée à cet ordinateur**, puis désactivez l'option **Détecter et installer automatiquement mon imprimante Plug-and-Play** en dessous.
5. Cliquez sur le bouton **Suivant**.
6. Cliquez sur la case d'option **Créer un nouveau port**.
7. Dans la **liste déroulante Type de port** :
   - **Port local** si l'imprimante est partagée à partir d'un autre ordinateur sur le réseau, (i.e. \\XP_workstation_name\Printer_share_name), ou
   - **Port TCP/IP standard** si l'imprimante est une véritable imprimante réseau avec une adresse IP, (par exemple 192.168.1.200).
8. Continuez l'installation de l'imprimante comme d'habitude, en sélectionnant les pilotes de l'imprimante, un nom pour l'imprimante, les valeurs par défaut d'impression, etc.

Créez et configurez le rapport (voir Création d'un rapport page 39-2) et la macro (voir Création d'***une nouvelle macro*** page 20-2).

Impression d'un rapport existant

Introduction

Une fois qu'un rapport a été créé et enregistré, il s'affiche dans la fenêtre Liste principale **de la description de l'état**. À tout moment, vous pouvez sélectionner cet état et l'imprimer, à condition de disposer des privilèges d'opérateur appropriés. Cela dépend de l'opérateur qui a créé le rapport et de la division qu'ils occupent.

Procédure

1. Cliquez sur **Rapport dans** la barre de menus, puis sur **Rapport Descriptions**.
   La **fenêtre Description** de l'état Liste s'ouvre (en mode grille).
2. Mettez en évidence le **rapport requis**.
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
4. Cliquez sur le bouton **Suivant** sur chaque écran jusqu'à ce que vous arriviez à l'écran "Génération de rapports et enregistrement".
5. Cliquez sur le bouton radio en regard de **Printer (Imprimante)**.
6. Sélectionnez l'imprimante requise dans la liste déroulante des imprimantes disponibles.
7. Cliquez sur le bouton **Configurer l'imprimante...** si vous avez besoin de définir des informations sur l'imprimante (par exemple, la taille du papier ou l'impression de plusieurs pages sur une seule feuille de papier). Voir ***Personnalisation des impressions de rapports*** (page 39-75) si vous avez besoin de plus de détails.
   Une fois les paramètres de l'imprimante définis, cliquez sur le bouton **OK** pour revenir à l'écran "Génération de rapports et enregistrement".
8. Cliquez sur le bouton **Suivant**.
   Le rapport s'imprime sur l'imprimante indiquée.
9. Cliquez sur le bouton **Terminer** pour revenir à la fenêtre **Description** du rapport - Liste principale.

Résultat

Le rapport est imprimé.
Selon les paramètres définis lors de la création de l'état, l'état peut être imprimé vers l'une des destinations suivantes :

- à l'écran
- une copie papier est imprimée
- vers un fichier

Conseils

- Une autre méthode d'impression consiste à utiliser l'option Propriétés (clic droit). Parcourez l'assistant jusqu'à ce que l'écran "Enregistrement du rapport" s'affiche. Cette méthode vous permet d'apporter les modifications nécessaires au rapport.

  Si une imprimante sélectionnée spécifique n'est pas disponible, le rapport est dirigé vers l'imprimante par défaut.

  Si l'imprimante par défaut n'est pas disponible, le rapport est dirigé vers l'aperçu avant impression (à l'écran).

- Lorsque le rapport est enregistré dans un fichier, le fichier peut être ouvert à l'aide de Microsoft Excel ou Access. Cela permet d'utiliser divers outils de tri et d'extraction de données, comme les données Excel, les filtres, les filtres automatiques ou les requêtes d'accès.

Personnalisation des impressions de rapports

Introduction

Les paramètres de l'imprimante peuvent être modifiés, en fonction de l'imprimante que vous utilisez, pour personnaliser la façon dont un rapport sera imprimé (par exemple, l'orientation du papier, l'impression recto verso, plusieurs pages par feuille, etc.). Cela peut être réalisé pour les nouveaux rapports et les rapports qui ont déjà été créés et enregistrés.

L'exemple suivant indique comment modifier les paramètres de votre imprimante de sorte qu'un état imprime plusieurs pages sur une seule feuille de papier (pour réduire la quantité de papier utilisée).

EXEMPLE : Impression de plusieurs pages par feuille

Procédure

1. Cliquez sur **Rapport dans** la barre de menus, puis sur **Rapport Descriptions**.
   La **fenêtre Description** de l'état Liste s'ouvre (en mode grille).
2. Soit :
   - sélectionnez un rapport déjà enregistré, ou
   - **cliquez avec le bouton droit de la souris et** sélectionnez Nouveau, puis le type de rapport requis.
3. À l'aide des boutons **Suivant** et **Précédent**, passez l'étape de l'Assistant État en choisissant les paramètres de rapport appropriés sur chaque écran jusqu'à ce que vous arriviez à l'écran "Génération et enregistrement de rapports".
4. Cliquez sur le bouton radio en regard de **Printer (Imprimante)**.
5. Sélectionnez l'imprimante requise dans la liste déroulante des imprimantes disponibles.
6. Cliquez sur le bouton **Setup Printer... (Configurer l'imprimante)**.
   L'écran **Print Setup** s'affiche.
7. Cliquez sur le bouton radio correspondant à l'orientation souhaitée (Portrait ou Paysage).
8. Cliquez sur le bouton **Propriétés**.
   Par défaut, l'onglet **Papier/Sortie** des propriétés de l'imprimante s'affiche.
9. Si vous souhaitez que l'état soit imprimé recto verso (c'est-à-dire des deux côtés de chaque feuille de papier), sélectionnez "Impression recto verso" dans la liste déroulante **Impression recto verso**.
10. Cliquez sur l'onglet Disposition/filigrane et sélectionnez le nombre de pages requis par feuille à partir des options sous **Pages par feuille (N-Up)**.
11. Cliquez sur le bouton **OK**.
    L'écran Configuration de l'**impression** s'affiche à nouveau.
12. Cliquez sur le bouton **OK**.
    L'écran "Génération de rapports et enregistrement" s'affiche à nouveau.

13. Cliquez sur le **bouton** Enregistrer le **rapport si** vous souhaitez enregistrer ce rapport.
    Remarque :
    Ignorez cette étape si vous réexécutez un rapport déjà enregistré, car le bouton **Enregistrer le rapport** est désactivé.
14. Cliquez sur le bouton **Suivant**.
    Le rapport s'imprime sur l'imprimante indiquée.
15. Cliquez sur le bouton **Terminer** pour revenir à la fenêtre **Description** du rapport - Liste principale.

Résultat

Le rapport est imprimé.
Important :
Tout écart par rapport à la procédure ci-dessus peut entraîner le retour du rapport aux paramètres par défaut et l'impression attendue. Par exemple :

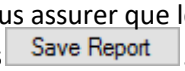
- Si vous effectuez les étapes 1 à 13, puis quittez, lorsque vous réexécutez le rapport, il utilise les paramètres par défaut (c'est-à-dire recto verso et une page par feuille).
- Si vous faites tout, mais à l'étape 4, vous cliquez sur le bouton d'option **Aperçu avant impression** au lieu du bouton d'option **Imprimante**, encore une fois, le rapport s'exécutera en utilisant les paramètres par défaut.

Modification des paramètres d'un rapport existant

Introduction

Une fois qu'un état a été créé, il s'affiche dans la fenêtre **Description de l'état -** Liste principale. Vous pouvez modifier ces rapports à tout moment. Par exemple, vous pouvez prolonger la période indiquée dans un rapport d'activité existant.

Procédure

1. Cliquez sur **Rapport dans** la barre de menus, puis sur **Rapport Descriptions**.
   La **fenêtre Description** de l'état Liste s'ouvre (en mode grille).
2. Mettez en surbrillance le rapport requis.
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**. L'Assistant Rapport s'affiche.
4. Utilisez les touches **Suivant** et **Précédent** pour parcourir les différents écrans de l'Assistant. Le cas échéant, modifiez le ou les paramètres.
5. Passez l'assistant à l'écran "Enregistrement de rapport".
   Cliquez sur le bouton **Enregistrer le rapport** pour vous assurer que les paramètres que vous avez modifiés sont enregistrés 

.

Résultat

Les modifications que vous avez apportées au rapport sont enregistrées.

La fenêtre Aperçu avant impression de l'état

Introduction

Certains rapports ont été configurés pour être imprimés à l'écran. Cela vous permet d'afficher un aperçu du rapport -essayer avant d'acheter.
Une fois que vous avez consulté le rapport, vous avez la possibilité de l'imprimer.

En restant dans la fenêtre **Aperçu de l'état**, vous pouvez imprimer l'état. Il est envoyé à l'imprimante par défaut, comme défini dans le champ suivant :

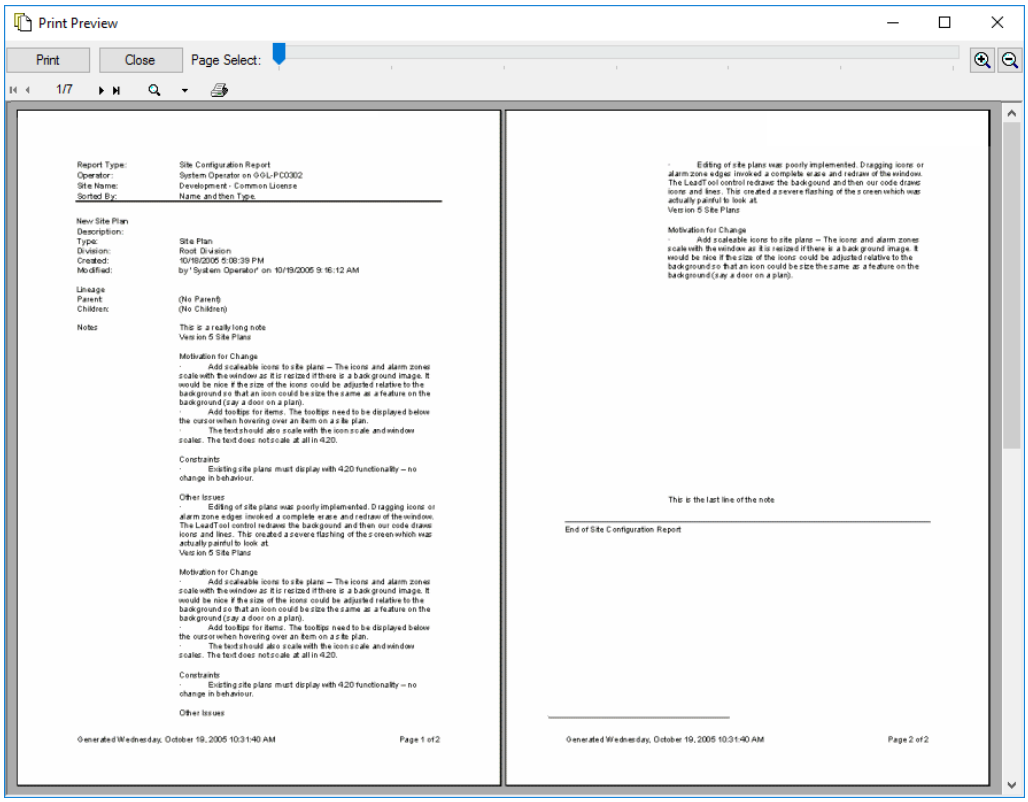


Procédure

1. Cliquez sur **Rapport dans** la barre de menus, puis sur **Rapport Descriptions**. La **fenêtre Description** de l'état Liste s'ouvre (en mode grille).
2. Dans la liste affichée**, sélectionnez et imprimez un rapport** que vous savez **imprimer à l'écran**. Le champ Description (dans la fenêtre Liste principale Description des états) peut indiquer que l'état est imprimé à l'écran.

Résultat

L'état est généré et s'affiche dans la fenêtre d'aperçu avant impression de l'état :

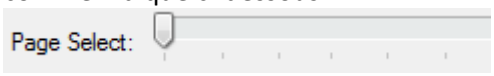


Affichage de pages spécifiques

Lorsque le rapport est généré, la première page du rapport s'affiche à l'écran. Il existe plusieurs façons d'afficher d'autres pages dans un rapport, comme suit :

- Utilisez les flèches de navigation 

(Première page, Page précédente, Page suivante et Dernière page) pour parcourir le rapport.
- L'indicateur Sélection de page vous permet de sélectionner différentes pages à afficher. Les marqueurs Page représentent les différentes pages du rapport.
  - Déplacez le pointeur de la souris vers le marqueur approprié de la page.
  - Cliquez sur le bouton de la souris pour afficher cette page sélectionnée.

  Par exemple:
  Pour afficher la page 3 du rapport, cliquez sur l'indicateur Sélection de page comme indiqué ci-dessous.
  

- Utilisez la barre de défilement verticale pour vous déplacer vers l'avant et vers l'arrière dans le rapport.

Loupe de verre

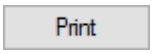
La loupe fait basculer  l'affichage entre la page entière et 100 %. Cliquez sur la flèche pour afficher un menu déroulant proposant d'autres options de dimensionnement qui vous permettent d'agrandir ou de réduire la taille du texte affiché dans la fenêtre Imprimer l'aperçu.

Impression de votre rapport

Le rapport est beau et contient toutes les informations que vous voulez.
Vous pouvez désormais imprimer le rapport.

Vous pouvez imprimer à partir de la fenêtre Aperçu avant impression ou fermer la fenêtre Aperçu avant impression, revenir à l'Assistant État et imprimer à partir de là. Utilisez l'une des méthodes suivantes :

Soit :

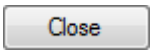
1. Cliquez sur **Imprimer** 

Le rapport s'imprime sur l'imprimante par défaut. La fenêtre Aperçu avant impression se ferme et vous revenez à l'assistant Rapport.

Ou:

1. Cliquez sur le  bouton.
2. Vérifiez/modifiez les paramètres de l'imprimante, y compris l'imprimante sur laquelle le rapport sera imprimé à.
3. Cliquez sur le bouton **OK**.

Ou:

1. Cliquez sur **Fermer** 

2. Cliquez sur le bouton **Précédent** pour revenir à l'écran Génération et enregistrement de rapports. Vérifiez/modifiez les paramètres de l'imprimante.
3. Sélectionnez le bouton d'option **Imprimante** (**Printer)**.
4. Cliquez sur le bouton **Suivant**.
5. Cliquez sur le bouton **Terminer (Finish)**.

Fermeture sans impression

Lorsque vous avez consulté votre état, vous pouvez fermer la fenêtre Aperçu avant impression sans imprimer l'état réel.

1. Cliquez sur le bouton **Fermer (Close)**.
2. Cliquez sur le bouton **Terminer (Finish)**.

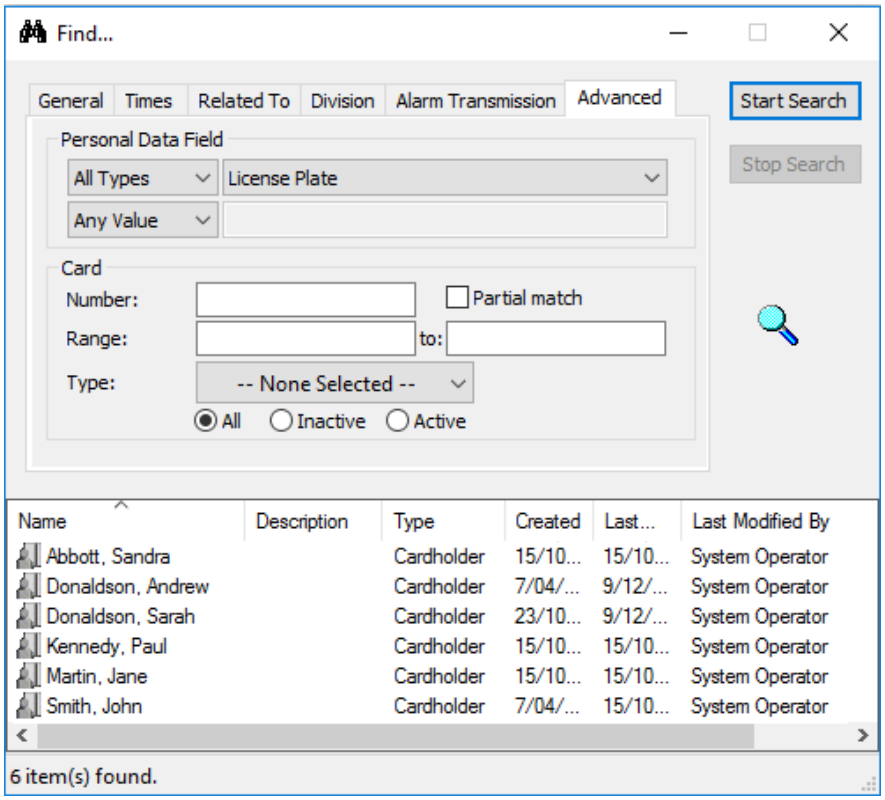
Rapports avancés

Introduction

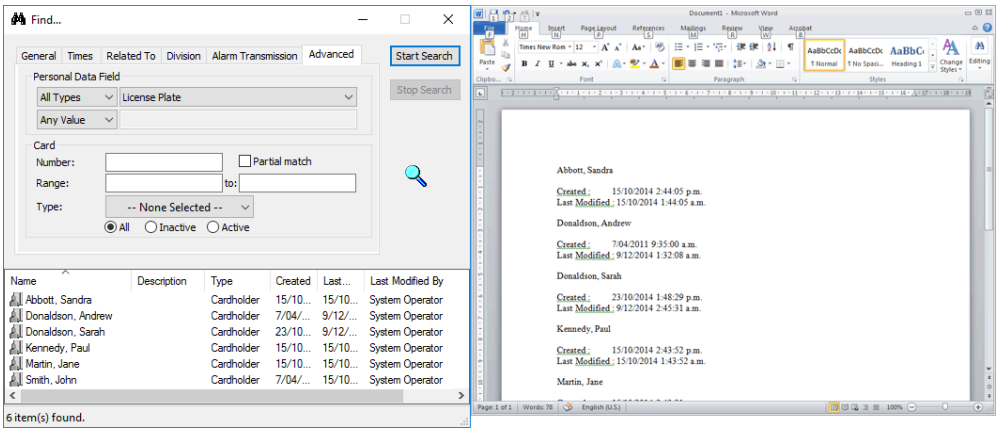
Le Centre de commande peut effectuer des rapports avancés. Vous pouvez trouver des éléments et les "glisser-déposer" dans une autre application pour des rapports rapides et ad hoc. Les rapports peuvent également être générés de façon plus conventionnelle via l'Assistant Rapport. Reportez-vous à la section Création ***d'un nouveau rapport*** (à la page 39-2).

Procédure

1. Utilisation de la recherche Outil de recherche pour un groupe d'éléments. Reportez-vous à la rubrique "Rechercher" pour plus de détails sur l'outil de recherche.
   Remarque : Il peut s'agir de n'importe quelle entité dans l'environnement du Centre de commandes.

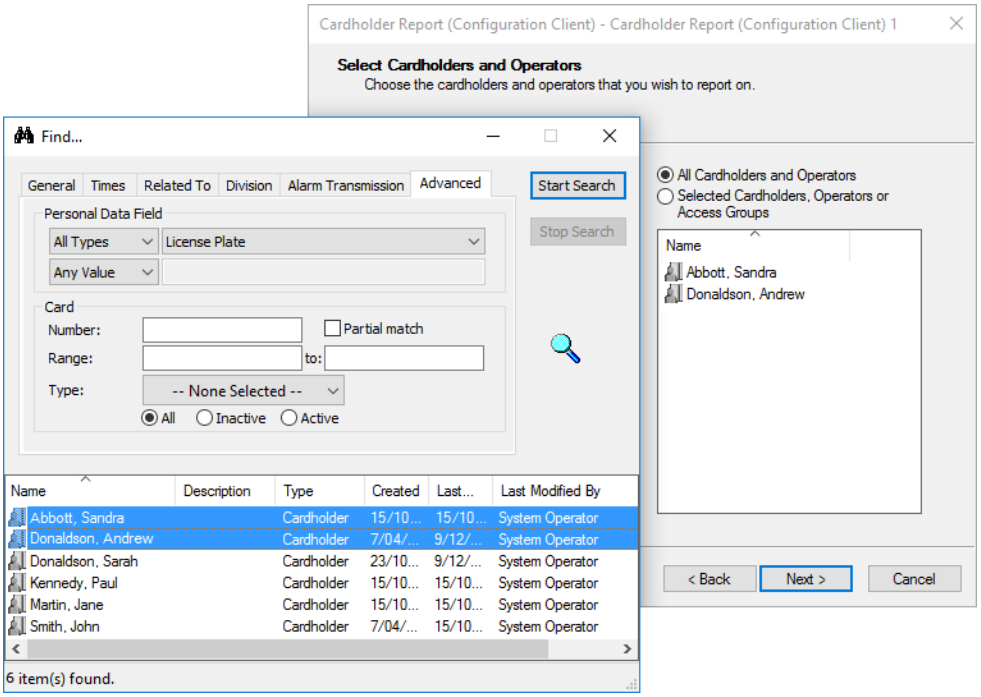


2. Sélectionnez les éléments dont vous avez besoin et "faites-les glisser" dans Microsoft Word. Affiche des données sur les entités dans un fichier Word.



Remarque : Lors de la création d'un rapport de la manière habituelle, à l'aide des "Assistants de rapport" (voir ***Création d'un rapport*** à la page 39-2), vous pouvez également utiliser la fonction "glisser-déplacer".

3. Sur l'écran Assistant de rapport intitulé "Sélectionner les titulaires et les opérateurs de carte" (c'est-à-dire l'écran qui vous permet de sélectionner les éléments à inclure dans le rapport), vous pouvez "faire glisser et déposer" des entités (dans l'exemple ci-dessous, titulaires de carte), à partir de la fenêtre **Rechercher** directement dans le panneau de sélection de l'assistant de rapport.



Chapitre 40 : Archives, sauvegardes et restaurations

Ce chapitre décrit le processus d'archivage, ainsi que le processus de sauvegarde et de restauration.

Les opérateurs doivent disposer des privilèges d'opérateur appropriés pour exécuter ces fonctions.

Archives

Chaque événement qui apparaît dans la fenêtre Événement est consigné dans la base de données Événements (CCFTEvent). Afin de limiter la taille de la base de données Event, l'archiveur manipule les données dans la base de données Event et les stocke dans un certain nombre de fichiers (un par jour) à l'emplacement spécifié par l'utilisateur. Après une archive, les événements de la période spécifiée sont supprimés de la base de données Events.

Les données archivées sont restaurées lorsqu'un opérateur exécute un rapport d'activité qui couvre une période au cours de laquelle les données résident uniquement dans des fichiers d'archive, sinon les données sont extraites de la base de données Event.

L'archiveur a trois responsabilités principales :

1. Copier et/ou déplacer l'activité de la base de données en ligne vers des fichiers externes.
2. Récupérez de l'espace en supprimant l'activité archivée de la base de données en ligne.
3. Récupère l'activité archivée à partir de fichiers externes si nécessaire pour un rapport.

Remarques :

- Si une archive et une sauvegarde sont requises, effectuez l'archive avant la sauvegarde.
- Étant donné que la génération de rapports à partir de données archivées peut être lente, il est recommandé de conserver les données sur lesquelles vous souhaitez générer des rapports dans la base de données des événements et d'archiver uniquement les données sur lesquelles vous ne générez pas de rapports régulièrement.

Sauvegardes/restaurations

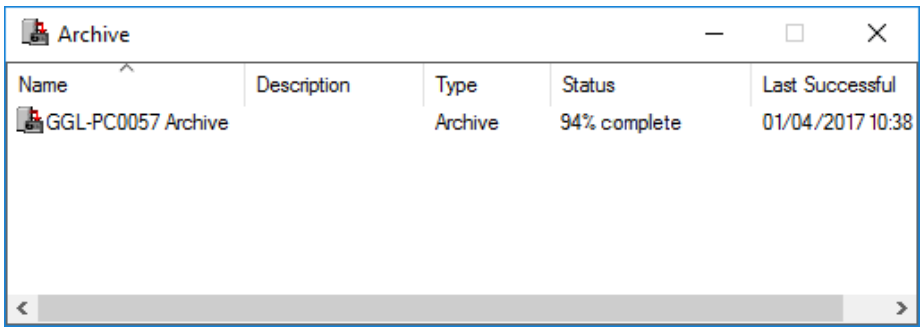
Le processus de sauvegarde/restauration enregistre l'état de la configuration des sites (CCFTCentral) à un point unique dans le temps (c'est-à-dire au moment du lancement de la sauvegarde). Après une sauvegarde, le système se comportera normalement et une restauration ne devrait être nécessaire que si quelque chose arrive à votre système.

Sauvegardes :
Vous pouvez sauvegarder les données de travail des systèmes dans un fichier. Le système peut être sauvegardé lorsqu'il est en ligne et que les opérateurs sont connectés.

Restaurations :
Vous pouvez restaurer le système de travail à partir d'un enregistrement de sauvegarde de fichier.

Fenêtre Archiver la liste principale

La fenêtre **Archiver** la liste s'ouvre en mode grille.



Cette fenêtre affiche l'état d'une archive. Si une archive est en cours d'exécution, elle affiche le pourcentage achevé. Si la dernière archive a été arrêtée ou a échoué, ou si l'archive ne peut pas démarrer, elle affiche la raison, sinon elle n'affiche rien.

Configuration des archives

Introduction

Toute la configuration de l'archive est effectuée à partir des pages de propriétés Archive. Les propriétés obligatoires pour configurer une archive sont les chemins d'archivage et le compte utilisateur. Ces propriétés sont couvertes dans les huit premières étapes de cette procédure, tandis que les étapes restantes sont des paramètres facultatifs.

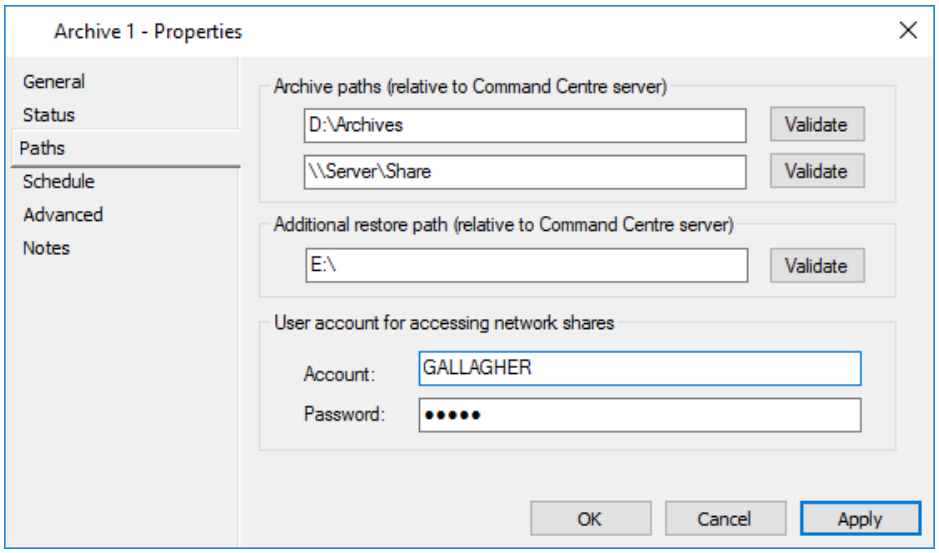
Cette procédure décrit comment configurer une archive. Pour effectuer cette procédure, vous devez disposer des privilèges d'opérateur "Afficher le site", "Configurer le site" et "Sauvegarder et archiver". Notez que le privilège de l'opérateur "Configurer le site n'est accordé qu'aux administrateurs de niveau supérieur.

Si vous souhaitez configurer une archive qui supprime les données de la base de données sans archiver les événements, vous avez besoin du privilège opérateur "Utilisateur avancé". Notez que le privilège d'opérateur "Utilisateur avancé" n'est attribué qu'aux administrateurs de niveau extrêmement élevé.

Remarque : Le système permet de configurer une archive.

Procédure

1. Cliquez sur **Fichier** dans la barre de menu, puis sur **Archives**.
   La fenêtre **Archiver la** liste s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...Archive**. Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
   Remarques :
   - La division que vous sélectionnez ici déterminera qui pourra voir les archives.
   - Toutes les données de toutes les divisions sont toujours archivées. Vous ne pouvez pas archiver séparément des divisions individuelles.
4. Cliquez sur l'onglet **Chemins d'accès**.
   Cet onglet vous permet de spécifier les emplacements d'archivage et de restauration d'un serveur.



Les champs de cet onglet sont décrits ci-dessous:

du champ	Description
Chemins d'archivage	Ceux-ci spécifient les chemins d'archivage des fichiers sera écrit. Tous les fichiers d'archive seront écrits aux deux emplacements. Assurez-vous toujours que le serveur "relatif au centre de commande" est approprié. Longueur maximale = 260 caractères. **Remarque :** Les chemins d'accès aux archives nécessitent des autorisations "Service réseau" pour écrire.
Chemin de restauration supplémentaire	Le système recherche les chemins d'archivage actuels pour les fichiers d'archive lors du reporting sur l'activité archivée. Cela permet de spécifier un chemin d'accès supplémentaire qui sera recherché pour les fichiers d'archives lors de la création de rapports, mais qui ne sera pas écrit dans, (par exemple un lecteur de CD-ROM). Longueur maximale = 260 caractères.
Compte d'utilisateur pour l'accès aux partages réseau	Nom et mot de passe du compte d'utilisateur à utiliser lors de l'accès aux emplacements d'archivage et de restauration sur les partages réseau. Si ce champ est laissé vide, les emplacements d'archivage et de restauration sont accessibles à l'aide du compte d'ouverture de session que le service FT Command Center a été configuré pour utiliser (compte du système local par défaut). Maximum = 50 caractères.

Les boutons **Valider** vérifient que l'emplacement d'archivage ou de restauration est accessible au serveur.

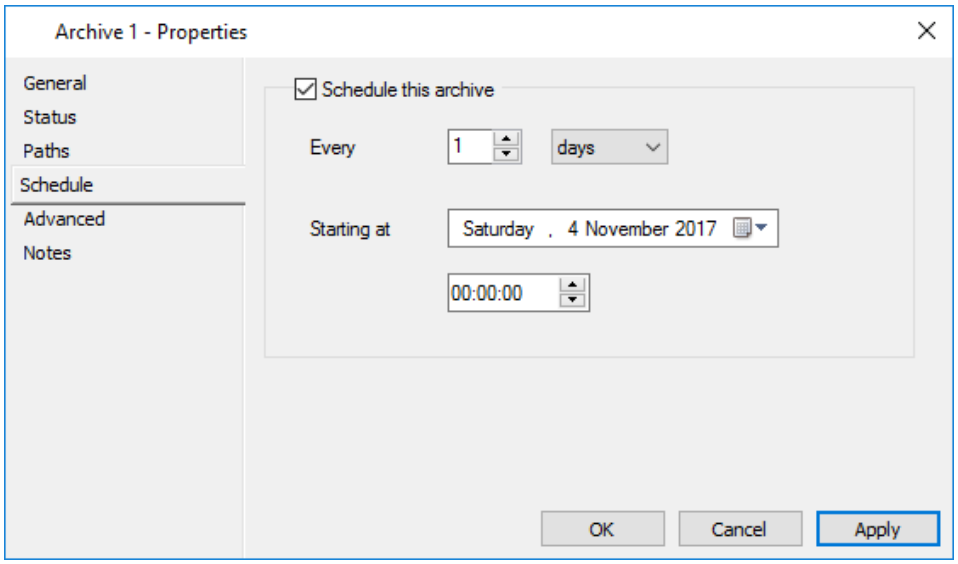
Remarque : Vous pouvez recevoir le message d'erreur suivant lors de la restauration de fichiers :
" Échec de la connexion au chemin <chemin> indiqué Veuillez vérifier :
- vous avez correctement entré le chemin
- le compte d'utilisateur de l'outil d'archivage dispose des autorisations appropriées pour utiliser cette ressource réseau."

Si vous le faites, vous devez vérifier que le compte d'utilisateur sur cet onglet a des privilèges suffisants.

5. Voulez-vous planifier cette archive pour qu'elle se produise automatiquement?

Si...	ensuite...
oui	Étape 9.
non	Étape 8.

6. Cliquez sur l'onglet **Planification (Schedule)**.
Cet onglet vous permet de spécifier un calendrier de répétition simple pour les archives automatisées.



7. Cochez la case **Planifier cette archive** pour activer les archives automatisées.
Remarque : Les autres champs de cet onglet sont désactivés jusqu'à ce que cette case à cocher soit activée. (Valeur par défaut = Désactivé)

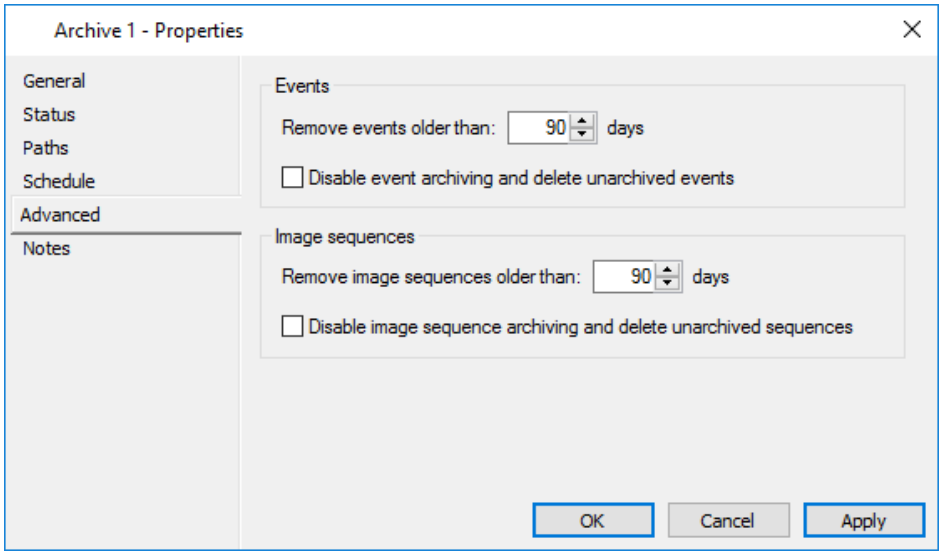
Les champs de cet onglet sont décrits ci-dessous :

du champ	Description
Every [count] [units]	Spécifie l'intervalle entre le début de chaque archive planifiée. Le nombre peut être compris entre 1 et 99, et les unités peuvent être des minutes, des heures, des jours ou des semaines. Par conséquent, le minimum est de 1 minute et le maximum est de 99 semaines. (Valeur par défaut = 1 jour)
Commençant à [date] [heure]	Indique quand la planification répétitive sera début. Valeur par défaut = Minuit du jour après la date de création de l'élément d'archive.

Remarque : La planification de l'archivage (heure de début et intervalle) est spécifiée en heure locale par rapport au serveur central. Cela signifie que l'intervalle entre les archives peut varier s'il franchit une transition d'économie d'énergie.

Exemple:
Si une archive est programmée toutes les 6 heures à partir de minuit. Les archives auront lieu à minuit, 6h, midi et 18h heure locale, même s'il n'y a que 5 heures entre minuit et 6h du matin en raison d'une transition vers l'économie de lumière du jour.

8. Cliquez sur l'onglet **Avancé (Advanced)**.
Cet onglet vous permet de spécifier si les données seront archivées et la quantité qui sera en ligne (dans la base de données).



Champ/ Case à cocher	Description
Supprimer les événements antérieurs à: ET Supprimer les séquences d'images plus anciennes que :	Le processus d'archivage ARCHIVE tous les événements/images non archivés, puis supprime les événements/images antérieurs à xxxx jours. Les événements/images non archivés NE sont PAS supprimés. Le minimum est de 0 jours et le maximum est de 9999jours. (Valeur par défaut= 90 jours)
Désactiver l'archivage des événements et supprimer les événements non archivés ET Désactiver l'archivage des séquences d'images et supprimer les séquences non archivées	Le processus d'archivage SUPPRIME tous les événements/images (archivés/non archivés) qui ont plus de xxxx jours. Le minimum est de 0 mégaoctets et le maximum est de 999 999 mégaoctets. Le privilège d'opérateur "Utilisateur avancé" est requis pour activer ce champ. (Valeur par défaut = non cochée)

IMPORTANT:
Nous ne recommandons pas la désactivation de l'archivage des événements/images. Il peut s'avérer utile si vous ne souhaitez pas conserver ou déclarer les xxxx jours.

Les normes de date UTC déterminent les données à supprimer de la base de données. Le calcul de 90 jours à l'aide de l'heure standard peut varier d'un jour.
0 jour supprime toutes les données
1 jour supprime les données actuelles
90 jours convertit le temps standard en temps UTC et supprime toutes les données 90 jours et plus anciens

	Événements et images "Archivage activé"	**Événements et images 'Archivage désactivé'**	**Événements 'Archive activée' Images 'Archive désactivée'**	**Événements 'Archive désactivée' Images 'Archive activée'**
Événements récents de xx jours	Archivé	Aucune archive	Archivé	Aucune archive
Événements antérieurs à xx jours	Archivé et supprimé	Aucune archive et supprimé	Archivé et supprimé	Aucune archive et supprimé
Images plus récentes que xx jours	Archivé	Aucune archive	Aucune archive	Archivé
Images antérieures à xx jours	Archivé et supprimé	Aucune archive et supprimé	Aucune archive et supprimé	Archivé et supprimé

9. Cliquez sur l'onglet **Remarques** si vous souhaitez ajouter une ou plusieurs remarques sur cette archive.
   Pour plus de détails concernant l'**onglet Notes,** voir ***Notes*** (page 6-81).
10. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications. Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Un élément d'archivage a été configuré.

Exécution des archives

Introduction

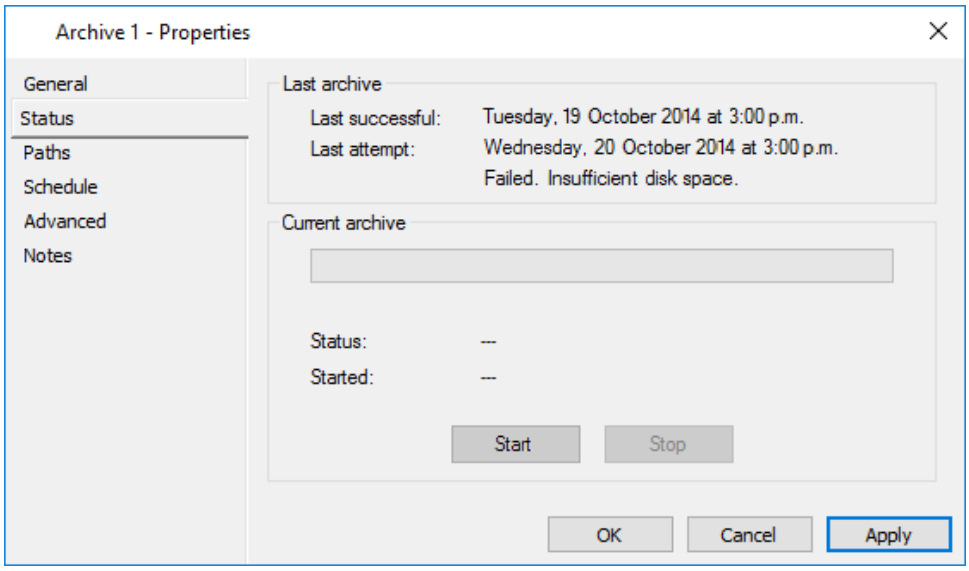
Au moins un chemin d'archivage doit être configuré avant de pouvoir démarrer une archive. Les archives peuvent être démarrées manuellement ou automatiquement en définissant une planification. Cette procédure concerne une archive manuelle. Pour plus d'informations sur la définition d'un calendrier pour une archive automatisée, reportez-vous ***à Configuration des archives*** (page 40-3).

Pour effectuer cette procédure, vous devez disposer des privilèges d'opérateur "Afficher le site" et "Sauvegarder et archiver". Ces privilèges vous permettront d'exécuter une archive, mais vous ne pourrez pas configurer ou modifier une archive.

Procédure

1. Cliquez sur **Fichier** dans la barre de menu, puis sur **Archives**.
   La fenêtre (en mode grille) de la liste principale des archives s'affiche.
2. Mettez en surbrillance l'élément d'archivage que vous souhaitez exécuter.
3. **Cliquez avec le bouton droit** de la souris sur le bouton.
4. Cliquez sur **Propriétés**.

   Remarque : Vous pouvez également cliquer sur **Démarrer l'archivage**. Bien qu'une figure de "pourcentage achevé" apparaisse dans la colonne "État" de la fenêtre de liste principale, cette méthode ne fournit pas suffisamment de détails sur la progression de l'archive.
5. Cliquez sur l'onglet **État (Status)**.



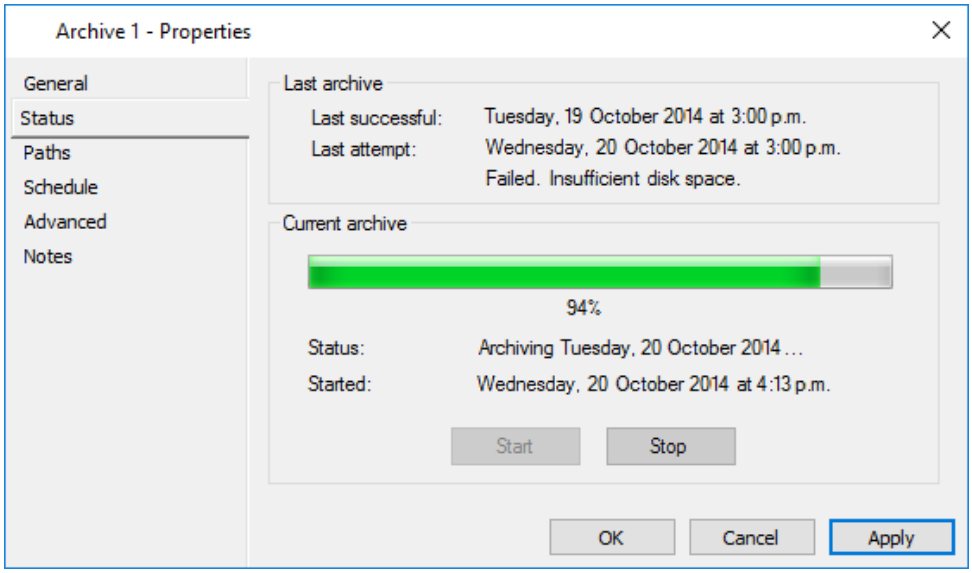
La section **Dernière archive** de cet onglet affiche les résultats de la dernière archive et la section **Archive actuelle** restera vide si une archive n'est pas en cours d'exécution.

Les champs de la section **Dernière** archive sont décrits ci-après :

du champ	Description
Dernier succès :	heure à laquelle la dernière archive a démarré.
Dernière tentative :	heure de début de la dernière tentative d'archivage. Si la dernière tentative d'archivage a réussi, elle sera la même que 'Dernière réussite'. Le résultat de la dernière tentative d'archivage sera également affiché (ex. 'Réussite', 'Arrêté par opérateur', 'Espace disque insuffisant' ou'Serveur hors connexion').

6. Cliquez sur le bouton **Démarrer** pour démarrer une archive.
Remarque : Si le bouton **Démarrer** est désactivé, ce sera pour l'une des raisons suivantes :

- l'élément d'archive n'a pas été configuré (c'est-à-dire qu'il n'a pas de serveur etau au moins un chemin d'archive),
- une archive est déjà en cours, ou
- le serveur est hors connexion.



La barre de progression indique la progression de l'archive et les champs de **La** section **Actuel** des archives est remplie comme suit :

du champ	Description
Statut :	Décrit ce que l'archiveur est en train de faire (par exemple, recherche de données à archiver, compactage de bases de données, etc.). Cela inclut généralement le jour archivé.
Démarré :	heure de démarrage de l'archive actuelle.

Remarque : Une fois l'archive terminée, il est temps d'effectuer une sauvegarde, mais pas absolument nécessaire. Reportez-vous à ***Exécution de sauvegardes*** (page 40-14) pour la procédure.

Résultat

Une archive est terminée et les fichiers d'archive sont stockés dans la ou les destinations spécifiées.

Conseils

Arrêt d'une archive
Une archive peut être arrêtée pendant son exécution, soit par :
- en cliquant sur le bouton **Arrêter** de l'onglet **État,** ou en cliquant sur,
- en cliquant avec le bouton droit de la souris sur l'archive dans la fenêtre de la liste principale, puis en cliquant sur **Arrêter l'archive** à partir du menu déroulant.

Lorsqu'une archive est arrêtée, tous les fichiers d'archive incomplets seront supprimés.

Échec de l'archivage
Si l'outil d'archivage ne parvient pas à terminer une archive pour une raison quelconque (par exemple, manque d'espace sur le disque ou arrêt de SQL Server), l'archive s'arrêtera et les fichiers d'archives seront supprimés de l'index de fichiers d'archives (si nécessaire), puis supprimés. Si les fichiers d'archive ne peuvent pas être supprimés de l'index du fichier d'archive, ils ne seront pas supprimés.

Restauration des archives

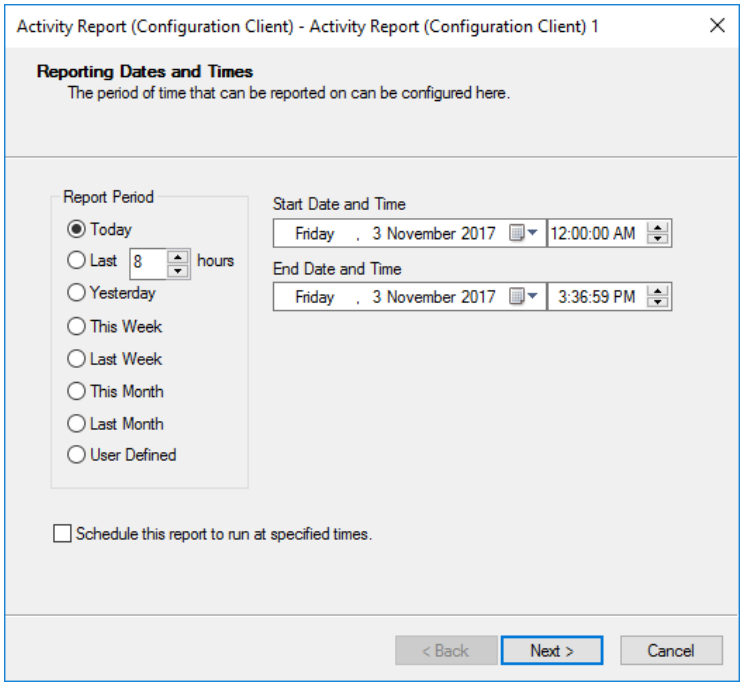
Introduction

La plupart des configurations d'archivage s'appliquent également à la restauration. Les chemins d'archive sont également des chemins de restauration et le même compte d'utilisateur sera utilisé pour accéder aux chemins de restauration sur les partages réseau. La seule propriété spécifique à la restauration est le chemin de restauration supplémentaire sous l'onglet **Chemins**. Cela permet à un site de spécifier un autre chemin de recherche de fichiers d'archive.

Les restaurations sont lancées automatiquement chaque fois qu'un événement nécessite une activité qui a été archivée et supprimée de la base de données des événements.

Procédure

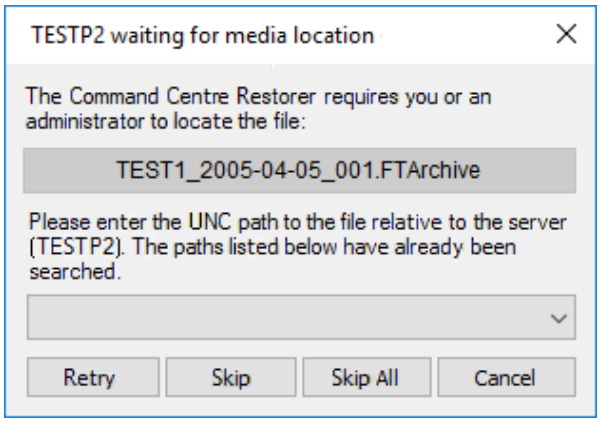
1. Cliquez sur **Rapport dans** la barre de menus, puis sur **Rapport Descriptions**.
   La **fenêtre Description** de l'état Liste s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris et **sélectionnez Nouveau rapport d'activité**.
   Le premier écran (l'écran "Dates et heures du rapport") de l'Assistant s'affiche.



3. Spécifiez la période de rapport appropriée pour l'archive à restaurer.
4. Parcourez chacun des écrans de l'assistant, en suivant les instructions affichées et en cliquant sur les boutons **Suivant** et **Précédent**.
   Lorsque le rapport est généré (c'est-à-dire après avoir cliqué sur le bouton Suivant de l'écran 'Génération et enregistrement du rapport'), une boîte de dialogue s'affiche.
5. Entrez l'emplacement des fichiers d'archive pour cette période et cliquez sur **OK** s'affiche.

Résultat

Les événements sont chargés dans la base de données restaurée (CCFTRestored) et sont inclus s'ils sont pertinents, puis supprimés après la génération du rapport pour maintenir l'espace disque libre.
Remarque : Si le restaurateur ne trouve pas de fichier d'archive dans l'un des chemins de restauration, l'écran suivant s'affiche :



Vous avez les suivantes :

1. Recommencez l'opération en cliquant sur le bouton **Réessayer**.
2. Spécifiez un nouvel emplacement de restauration.
3. Ignorer le fichier manquant en cliquant sur le bouton **Ignorer**.
   Le restaurateur ajoutera une entrée de fichier manquante à la sortie du rapport et passera au fichier suivant.
4. Ignorer tous les fichiers manquants en cliquant sur le bouton **Ignorer tout**.
   Cela a le même résultat que de cliquer sur le bouton Ignorer pour ce fichier et tous les fichiers manquants suivants.

S'il y a plus d'un serveur avec des fichiers manquants, alors vous pouvez être présenté avec plusieurs **restaurateurs en attente d'**écrans d'**emplacement des médias**, (c'est-à-dire un pour chaque serveur).

Indicatior

Arrêt d'une restauration
Une restauration peut être arrêtée en annulant la recherche à l'origine de la restauration (par exemple, en annulant le rapport ou en arrêtant l'outil de recherche).

Restauration à partir d'une station de travail distante
Si vous êtes un utilisateur sur une station de travail distante (c'est-à-dire dans une autre ville que le serveur), un certain nombre de scénarios peuvent se produire lorsque vous essayez de restaurer l'archive en exécutant un rapport d'activité.

Prendre les mesures indiquées ci-dessous :

Si...	alors...
lors de la génération du rapport, vous recevez une demande pour un fichier d'archive	contactez l'administrateur système où se trouve le serveur pour lui demander de placer les fichiers d'archives dans le PC du serveur.
les fichiers sont sur DVD	type dans la lettre de lecteur de DVD.
les fichiers se trouvent sur un lecteur réseau	spécifiez la lettre de lecteur du lecteur réseau mappé. **Remarque :** Tous les chemins d'accès sont référencés à partir du PC serveur du Centre de commande et non du PC de la station de travail.

Exécution de sauvegardes

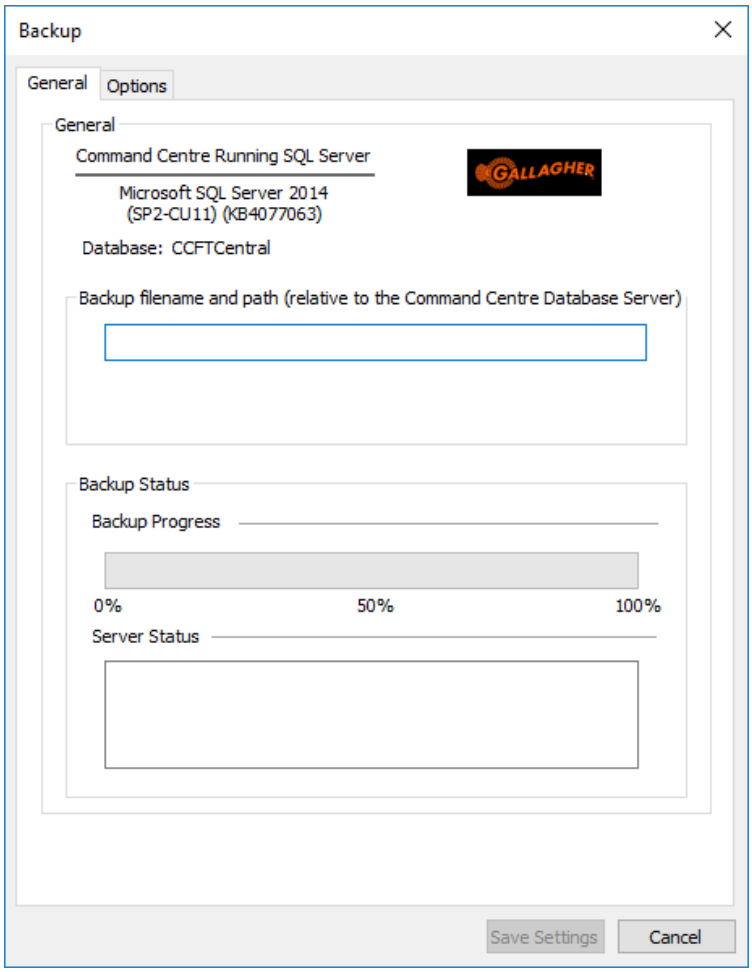
Introduction

SQL Server effectue les sauvegardes du Centre de commandes. Par conséquent, pour obtenir que SQL Server écrive à la destination que vous spécifiez et pour que la sauvegarde réussisse, vous devez exécuter le service SQL Server sous le compte d'un utilisateur qui dispose de l'autorisation de le faire.

Si votre station de travail est distante, le chemin d'accès que vous spécifiez est relatif à l'ordinateur SQL Server et non à votre ordinateur local.

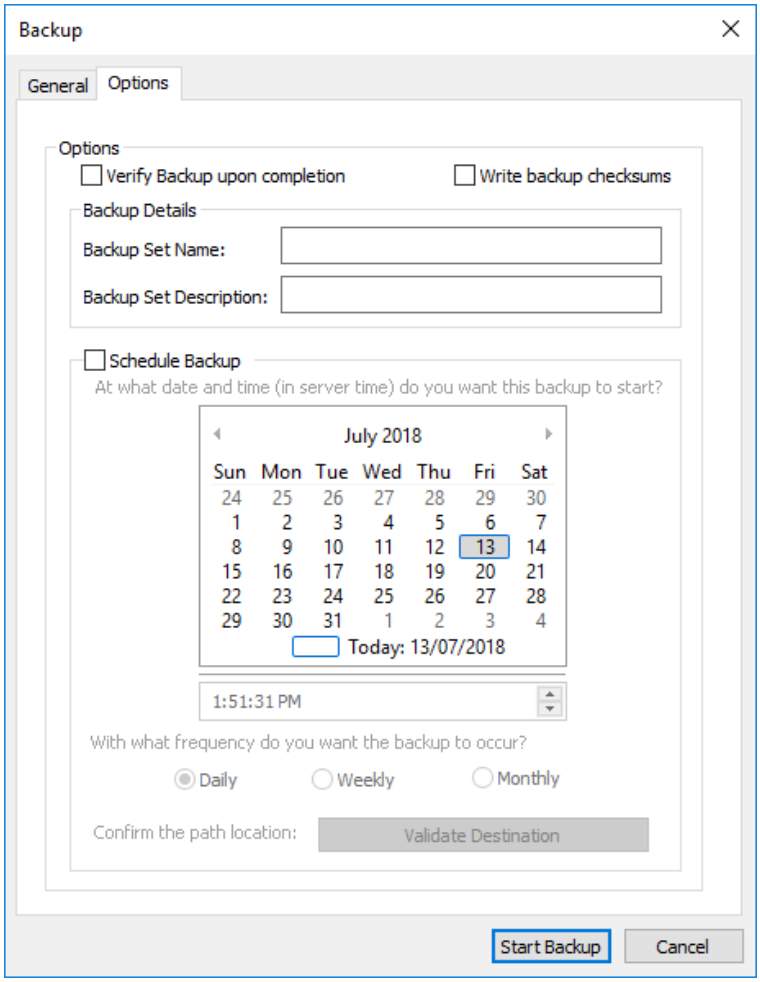
Procédure

1. Cliquez sur **Fichier** dans la barre de menus, puis sur **Sauvegarder**.
   Par défaut, l'onglet Général de la fenêtre de sauvegarde s'affiche.



2. Entrez la destination de la sauvegarde (à la fois le chemin et le nom du fichier) **Sauvegarder le** champ **nom de fichier et** chemin.
   Lorsque vous commencez à entrer des détails dans ce champ, le bouton **Enregistrer les paramètres** est activé.
3. Si vous avez besoin de l'enregistrement du nom de fichier et du chemin d'accès de sauvegarde, cliquez sur le bouton **Enregistrer les paramètres**.

4. Cliquez sur l'onglet **Options**.



5. Cochez la case **Vérifier la sauvegarde à la fin** si nécessaire.
   Remarque :
   Bien qu'elle ne soit pas obligatoire, la vérification d'une sauvegarde vérifie que la sauvegarde est intacte, physiquement, et que vous pouvez compter sur votre sauvegarde au cas où vous auriez besoin de l'utiliser. La vérification d'une sauvegarde implique :

   - Vérification du jeu de sauvegarde pour vérifier que tous les fichiers ont été écrits.
   - Vérification pour vérifier que les fichiers de la sauvegarde sont lisibles.

   La vérification d'une sauvegarde ne vérifie pas que la structure des données contenues dans le jeu de sauvegarde est correcte. Par exemple, bien que le jeu de sauvegarde ait pu être correctement écrit, il est possible qu'un certain type de problème d'intégrité de la base de données soit présent dans les fichiers de base de données qui composent le jeu de sauvegarde. Pour vérifier la structure des données avant de créer une sauvegarde, vous pouvez vérifier la cohérence de la base de données.

6. Parfois, des problèmes d'intégrité de la base de données peuvent se produire avec les fichiers de base de données qui composent un jeu de sauvegarde. Pour vérifier la structure des données, cochez la case **Write backup checksum**.

7. Saisissez le nom et la description d'un jeu de sauvegarde.

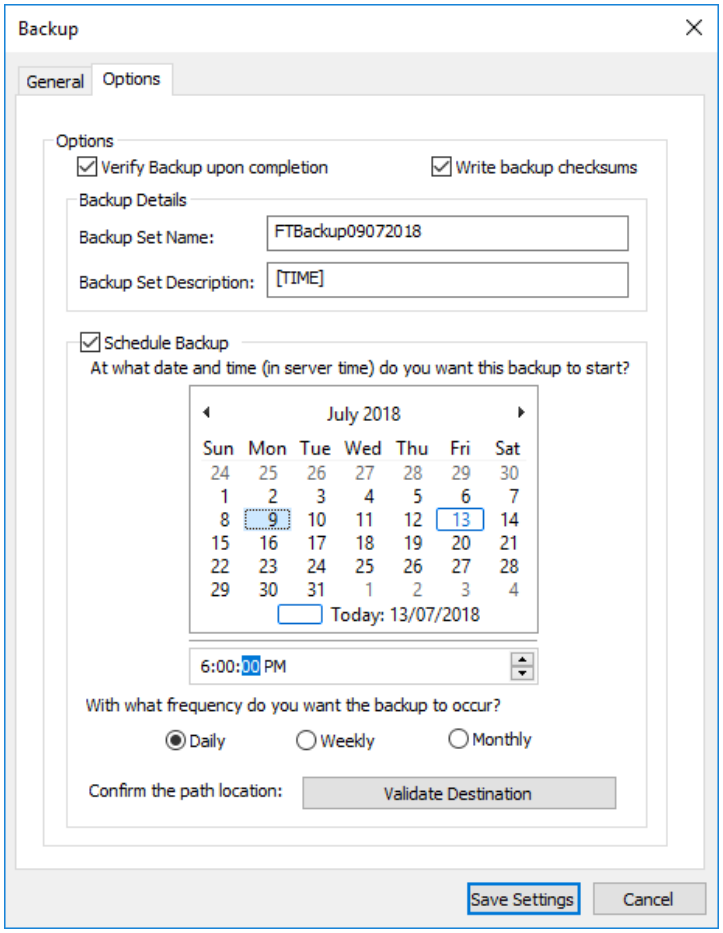
du champ	Description
Backup Set Name	Cette unité de sauvegarde.
Backup Set Description	Ce document fournit un texte descriptif ou d'identification le résultat d'une opération de sauvegarde. **Remarque :** Si vous tapez [TIME] dans le champ Description du jeu de sauvegarde, la date et l'heure réelles du serveur seront remplacées lors de la création de la sauvegarde.

Remarque :
Ces champs sont incorporés dans le fichier .FTBackup réel. Lorsque vous recherchez un jeu de sauvegarde (fichier .FTBackup) à l'aide du programme CCFTRestore, ces noms et descriptions apparaissent en bas de la fenêtre de navigation, ce qui permet à l'utilisateur d'identifier une sauvegarde même si le fichier lui-même a été renommé.

8. Souhaitez-vous exécuter la sauvegarde maintenant ou la programmer régulièrement ?

Si tu...	alors...
exécuter la sauvegarde maintenant	Cliquez sur le **bouton Démarrer la sauvegarde**. L'onglet **Général** s'affiche à nouveau et indique la progression de la sauvegarde. Lorsque la sauvegarde est terminée, le message "Sauvegarde réussie !" s'affiche dans le **champ État du serveur**. Fermez la fenêtre de sauvegarde.
planifier la sauvegarde de façon régulière	allez à l'étape 9.

9. Cochez la case **Planifier la sauvegarde**.



10. Sélectionnez la "Date de début" de votre sauvegarde dans le calendrier, en utilisant les touches pour sélectionner le mois, puis en cliquant sur le jour du mois.
11. Ajustez l'heure du jour où vous souhaitez que la sauvegarde se produise.
12. Cliquez sur le bouton radio approprié pour connaître la fréquence à laquelle la sauvegarde doit se produire.

Si...	ensuite une sauvegarde se produit...
Du quotidien	Tous les jours, à l'heure indiquée.
Chaque semaine	le jour de la semaine que vous avez sélectionné comme "Date de début", sur le calendrier (par exemple, dans l'exemple d'écran précédent, le 19 août a été sélectionné, qui est un lundi). Par conséquent, une sauvegarde se produirait toujours le lundi de la semaine.
Tous les mois	à la date sélectionnée comme "Date de début" sur le calendrier (par exemple, dans l'exemple d'écran précédent, le 19 août a été sélectionné, de sorte qu'une sauvegarde se produirait toujours le 19 du mois). **Remarque :** Si vous sélectionnez un jour qui ne se produit pas tous les mois (par exemple, le jour 31), la sauvegarde aura lieu le dernier jour de ces mois.

Remarque :
La date spécifiée est la première fois que la sauvegarde aura lieu (par exemple, un jour six mois à l'avenir pourrait être spécifié pour le démarrage des sauvegardes). Si une date/heure dépassée était spécifiée, la sauvegarde aurait besoin d'une "meilleure hypothèse" quant au moment auquel la sauvegarde devait avoir lieu (par exemple, si le 9 août 2002 était sélectionné avec un calendrier mensuel, et la date d'aujourd'hui est le 22 août 2002, alors la sauvegarde avancerait la première heure de sauvegarde au 9 septembre 2002).

13. Cliquez sur le bouton **Valider** la **destination** pour confirmer le chemin d'accès que vous avez entré. Un message d'erreur s'affiche si vous avez entré un chemin de fichier incorrect.
14. Cliquez sur le bouton **Enregistrer les paramètres**.
15. Fermez la fenêtre de sauvegarde.

Résultat

Une sauvegarde est exécutée ou planifiée pour s'exécuter de façon régulière.

Restauration des sauvegardes

Introduction

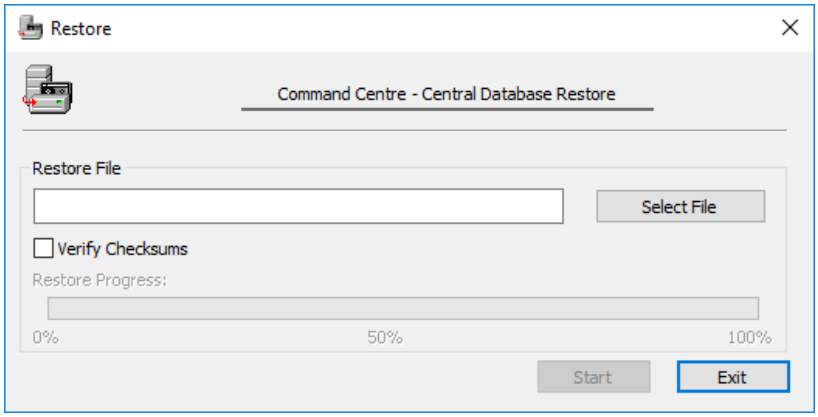
Cette procédure vous permet de restaurer le système de travail à partir d'un enregistrement de fichier de sauvegarde, par conséquent une sauvegarde doit déjà avoir été effectuée. Voir ***Exécution de sauvegardes*** (page 40-14).
IMPORTANT : Si vous restaurez une sauvegarde sur un autre ordinateur, vous aurez besoin du code de récupération de la base de données, sinon vous ne pourrez pas restaurer votre base de données.

Remarques :

- Si vous avez effectué une sauvegarde sur le réseau, la sauvegarde doit être copiée sur un lecteur non réseau avant la restauration. Une restauration ne peut être effectuée que sur le serveur.
- Certaines des captures d'écran de cette rubrique peuvent varier en fonction de votre système d'exploitation.
- La procédure ci-dessous décrit une méthode de restauration des sauvegardes. Vous pouvez également **double-cliquer** sur un fichier de sauvegarde OU sur Restaurer à partir de l'utilitaire Service Manager.
- Le certificat d'autorité de certification du centre de commande Gallagher est copié à partir de la base de données Gallagher dans le magasin de certificats Trusted Root pour les nouvelles installations, les mises à niveau et lorsque l'outil de récupération est utilisé. Le certificat d'autorité de certification du centre de commande Gallagher est utilisé pour l'authentification du client mobile et peut être supprimé en toute sécurité si le client mobile n'est pas utilisé sur le site.

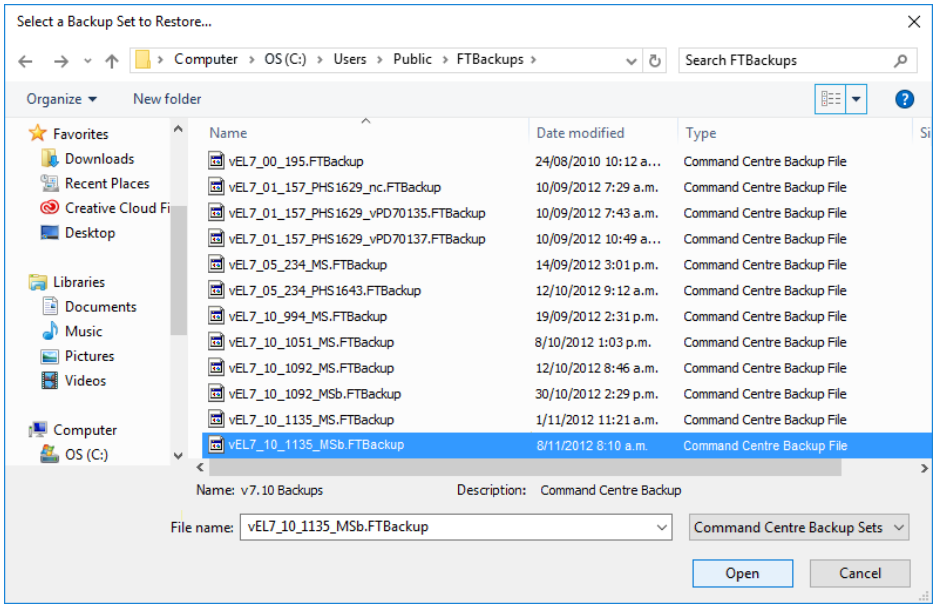
Procédure

1. Dans le menu **Démarrer**, cliquez sur **Programmes**, puis sur **Gallagher**.
2. Cliquez sur **Restauration du centre de commandes**.
   La fenêtre Restaurer s'affiche.



3. Cliquez sur le bouton Sélectionner le fichier (Select File).

4. À partir de la fenêtre contextuelle affichée, recherchez le fichier de sauvegarde que vous souhaitez utiliser pour la restauration.
   Remarque :
   Les noms que vous avez entrés dans les **champs** Nom du jeu de sauvegarde et **Description du** jeu de sauvegarde **lorsque vous avez effectué une sauvegarde apparaissent en bas de** la fenêtre de navigation, vous permettant d'identifier une sauvegarde, même si le fichier lui-même a été renommé.



5. Cliquez sur le bouton **Ouvrir (Open)**.
   Le chemin et le nom du fichier s'affichent dans le **champ** Restaurer le fichier**,** et le champ Démarrer le contrôle bouton est activé.
   L'utilitaire de restauration nécessite un accès exclusif à la base de données centrale CCFT et doit arrêter les services FT suivants pour permettre cela :
   - Service FT Command Center
   - Service de contrôleur FT (FT Controller)
   - Service FT Bootstrap Protocol
   - Service FT Import - Export
   - Service FT Intercom
   - Service de gestion des visiteurs FT

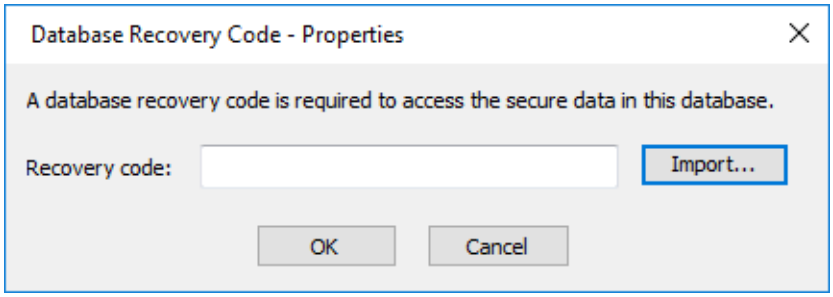
6. Si l'option "Écrire les checksum de sauvegarde" a été sélectionnée lors de l'exécution de la sauvegarde, cochez la **case Vérifier les checksum**.

   Remarque : Si vous cochez la case **Vérifier les sommes de contrôle** et que l'option "Écrire les sommes de contrôle de sauvegarde" n'a PAS été sélectionnée au moment de la sauvegarde, un message d'erreur s'affiche pour indiquer que le fichier de sauvegarde ne contient pas d'informations de total de contrôle. Si cela se produit, la désélection de **Vérifier les sommes de contrôle** vous permettra de continuer la restauration.

7. Cliquez sur le bouton **Démarrer**.
   Un message s'affiche indiquant que les services doivent être arrêtés.

8. Cliquez sur le bouton **Oui**.
   La restauration démarre. Lorsque la barre de progression de la restauration atteint 100 %, la restauration est terminée et un message contextuel *"La restauration est terminée. Voulez-vous redémarrer les services Command Center ?"* s'affiche.
9. Cliquez sur le bouton **Oui**.
   Une fois que les services FT ont redémarré, un autre message contextuel *"Restauration terminée avec succès !"* s'affiche.

   Remarque : À la fin de la restauration, le code vérifie s'il peut fonctionner avec la base de données. Si elle ne peut pas (probablement en raison de son existence d'une base de données autre système), la boîte de dialogue suivante s'affiche pour demander le code de récupération (pour la base de données source) :



10. Cliquez sur le bouton **OK**, puis sur le bouton **Quitter**.

Résultat

Une restauration d'un fichier de sauvegarde est terminée.

Indication

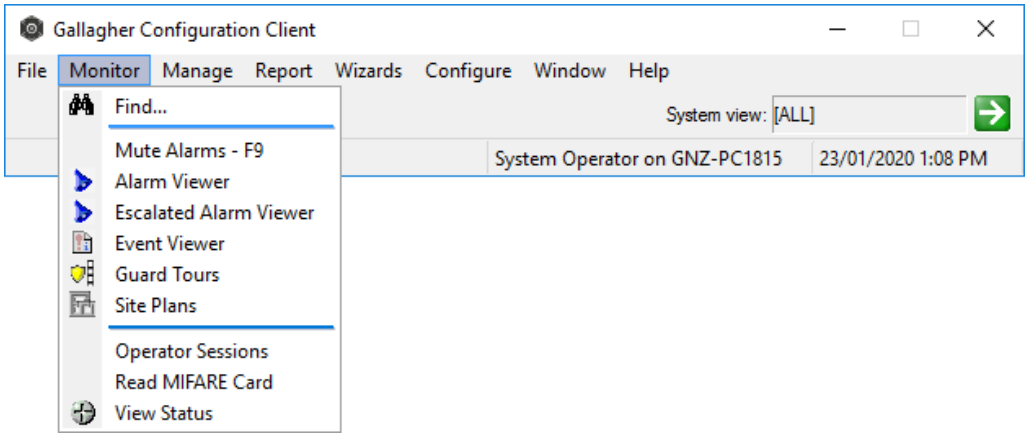
Restaurer à partir de l'Explorateur Windows
Une autre méthode de restauration d'une sauvegarde consiste à double-cliquer sur **.FTBackup,** fichier de l'Explorateur Windows sur le serveur.
La fenêtre Restauration s'affiche et vous suivez la procédure décrite précédemment, à l'exception de la sélection du fichier de sauvegarde, car le nom est déjà affiché dans le **champ Emplacement du fichier de base de données (De)**.

Partie 4 : Surveillance du site

C'est le rôle de l'opérateur, qui est souvent un agent de sécurité, de surveiller les événements et les alarmes qui se produisent sur un système. Les opérateurs sont très rarement requis pour effectuer la configuration.

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

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



Remarque :
En fonction de vos privilèges d'opérateur ou de votre vue système actuelle, certains des éléments de menu auxquels il est fait référence peuvent ne pas être visibles pour vous. Par exemple, la "fenêtre d'alarme escaladée" (pour que cet élément s'affiche, vous devez appartenir à un groupe d'opérateurs qui a l'option fenêtre d'alarme escaladée activée).

Chapitre 41 : Outil de recherche

Introduction

À l'aide de l'outil Rechercher, vous pouvez localiser des éléments dans le Centre de commandes. Chacun des onglets facilite la définition complète de vos critères de recherche.
Remarque : Un onglet **Transmission d'alarme** supplémentaire sera également disponible si votre site est sous licence pour la fonction Contact ID.

La fonction Rechercher définit la recherche en fonction des paramètres de chacun des onglets. Les résultats de la recherche incluent uniquement les éléments qui répondent à toutes les conditions définies dans tous les onglets.

Lorsque vous avez défini vos critères de recherche, assurez-vous que tous les onglets que vous ne voulez pas utiliser sont "vierges" - c'est-à-dire qu'ils ne contiennent pas de données de critères de recherche antérieurs.

Remarque : Appuyer sur **F3** sur votre clavier ouvre une nouvelle fenêtre Outil de **recherche**, sauf si une fenêtre Détails d'alarme est ouverte.

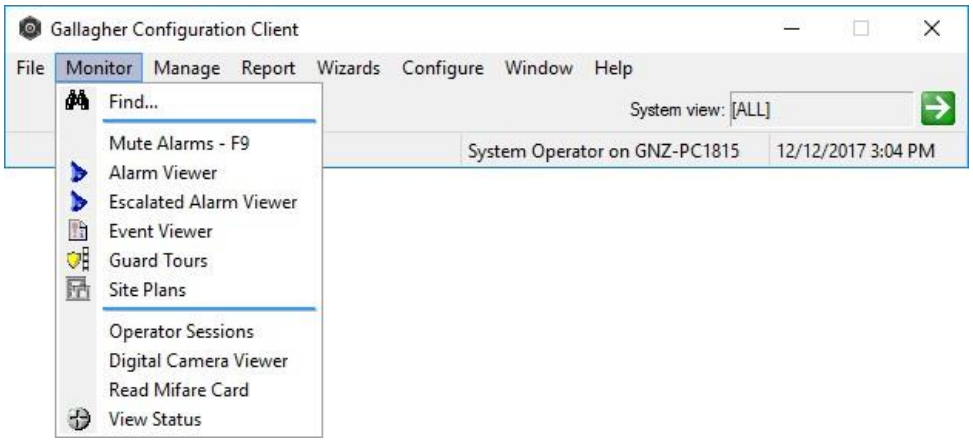
Utilisation de l'outil de recherche

Introduction

Utilisez la procédure suivante pour rechercher un élément dans le Centre de commandes, à l'aide de l'outil de recherche.

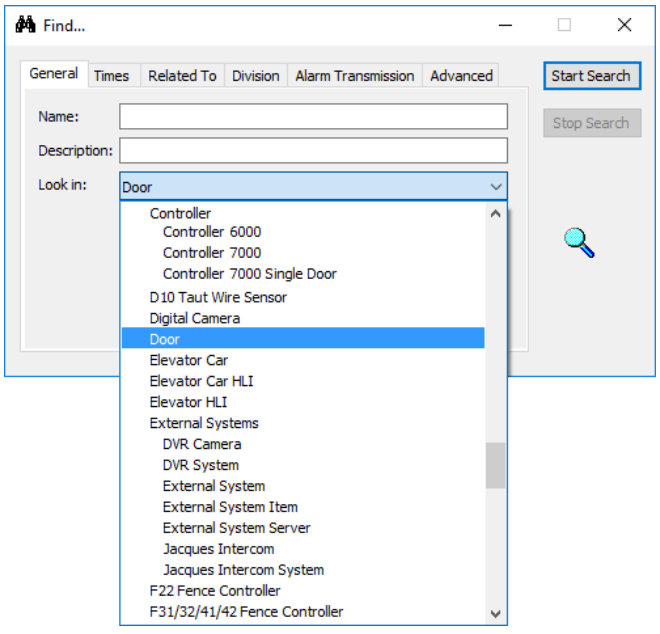
Procédure

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



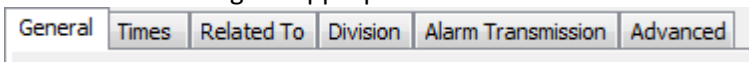
2. Entrez du texte dans les champs **Nom** et/ou **Description** pour vous aider à définir vos critères de recherche, si nécessaire.
   Remarque : Le texte partiel et les caractères génériques (%) peuvent être utilisés. Voir **Conseils** à la fin de cette rubrique pour plus de détails.

3. Cliquez sur dans le champ **Regarder dans (Look in**).
   Dans le menu déroulant affiché, cliquez sur la **zone à rechercher** dans le Centre de commandes.



Remarque : Lorsque vous recherchez des contrôleurs, vous pouvez choisir d'effectuer une recherche par différents types de contrôleurs ou par tous les contrôleurs à la fois.

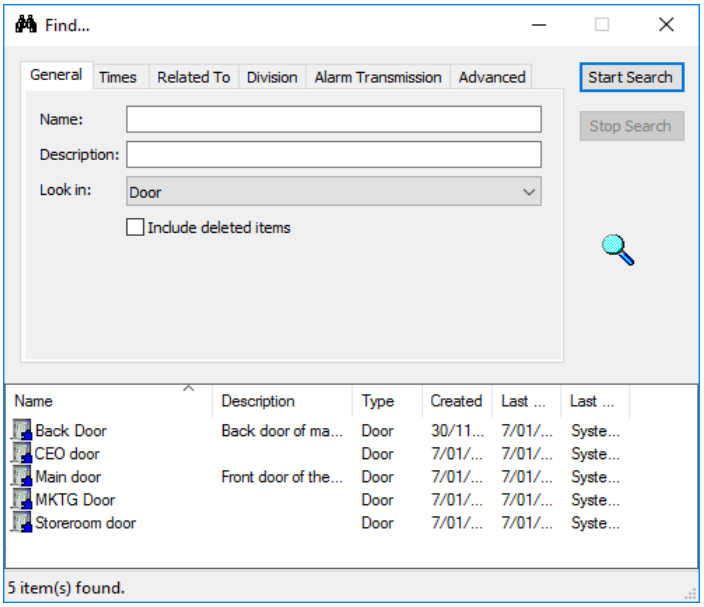
4. Cochez la case **Inclure les éléments supprimés** si vous souhaitez les inclure dans votre recherche.
   Remarque : Lorsque cette option est cochée, vous pouvez alors effectuer une recherche par "Nom" ou "Description" (dans l'onglet **Général**), ou par "Créé", "Modifié" ou "Supprimé" (dans l'onglet Heures).
5. Sélectionnez les onglets appropriés et **définissez vos critères de recherche**.



6. Voir ***Exemples*** (page 41-5), à l'aide de ces onglets, pour montrer comment vous pouvez définir vos recherches.
7. Cliquez sur le bouton **Démarrer la recherche**.

Résultat

La fenêtre Rechercher dans la liste s'ouvre et répertorie tous les éléments trouvés.



Conseils

Arrêter la recherche
Si vous cliquez sur le bouton **Arrêter la recherche**, les éléments déjà trouvés restent dans la liste affichée. Pour redémarrer la recherche à partir du début, cliquez sur le bouton **Démarrer la recherche**.

Texte partiel
Le système du Centre de commande recherche automatiquement le texte partiel saisi dans les champs **Nom** et **Description**. La recherche trouvera des correspondances qui contiennent du texte partiel recherché sur.
Par exemple, si vous entrez Will dans le champ **Nom**, les résultats de la recherche incluront dans le système n'importe quel "Williams" ou "Willis".

Caractères génériques (%)
Le symbole de pourcentage (%) peut être utilisé comme caractère générique dans le champ Nom et Champs **de description**.
Par exemple, si vous entrez du texte partiel et que vous incluez un % comme caractère générique, de sorte que vous avez co%er dans le champ Nom, les résultats de la recherche incluront les éléments avec le mot "contrôleur" ou "ordinateur" dans leur nom.
Remarque :
Si vous souhaitez rechercher le symbole %, vous devez le placer entre [%] crochets.

Respect de la casse
La recherche n'est pas sensible à la casse. Vous pouvez saisir des caractères minuscules ou majuscules.

Propriétés des éléments de la liste de recherche
Vous pouvez accéder directement à la fenêtre Propriétés de n'importe quel élément de la liste des résultats de la recherche en cliquant avec le bouton droit sur un élément, puis en sélectionnant Propriétés.

Exemples

Cliquez sur l'exemple ci-dessous qui vous demande plus de détails sur :

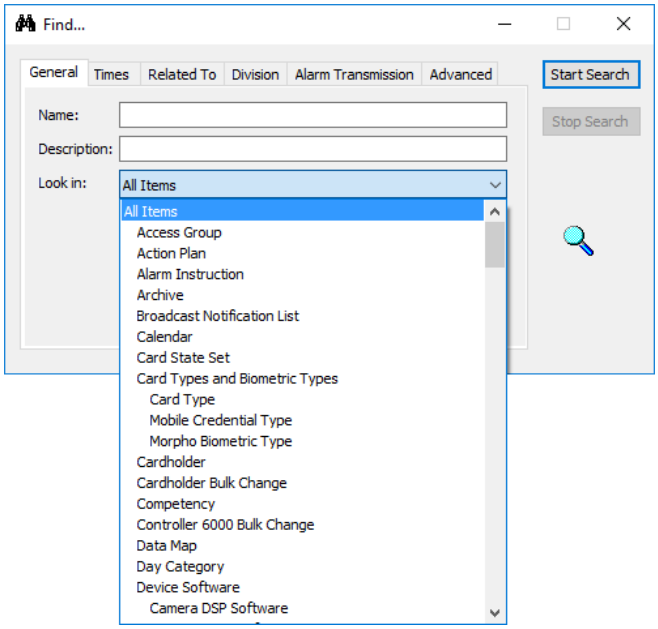
- ***Exemple 1: Recherche avec les détails généraux et temporels*** (page 41-6)
- ***Exemple 2: Recherche à l'aide de*** (page 41-8)
- ***Exemple 3: Recherche à l'aide de divisions*** (page 41-9)
- ***Exemple 4: Avancé*** (page 41-10)

Exemple 1 : Recherche à l'aide des détails généraux et temporels

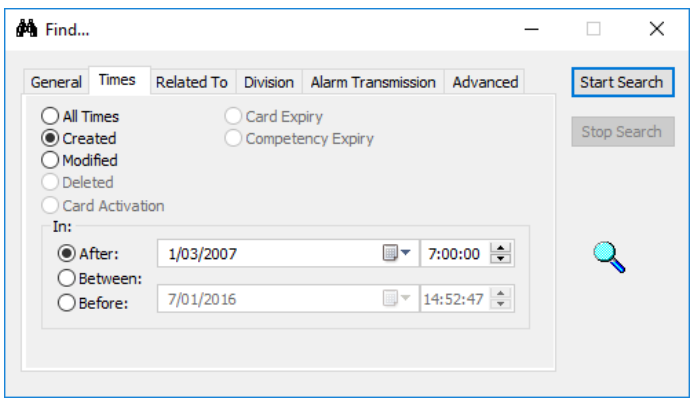
Cet exemple utilise des champs dans les onglets *Général* et *Heures* pour définir la recherche.

Suivez la procédure ci-dessous pour trouver tous les éléments qui incluent le nom du bureau et qui ont été **créés après 7h le 01/03/2007**.

1. Cliquez sur l'onglet **Général**.



2. Dans le champ Nom, tapez **office**.
3. Cliquez sur le champ **Regarder dans** et sélectionnez l'option "Tous les éléments".
4. Cliquez sur l'onglet **Times**.
   L'onglet Heures permet de rechercher des éléments en fonction des types d'événements et des critères temporels.
   Remarque :
   Dans cet exemple, les boutons radio **Activation** et Expiration de la **carte** sont désactivés. Ils ne sont activés que pour les recherches de détenteurs de cartes à cartes.



5. Sélectionnez l'option Créé, puis l'option Après.

6. Saisissez la **date** 01/03/2007 et l'**heure 07:00:00**.
7. Cliquez sur le bouton **Démarrer la recherche**.

La fenêtre Rechercher s'ouvre et affiche tous les éléments qui correspondent aux critères de recherche définis.

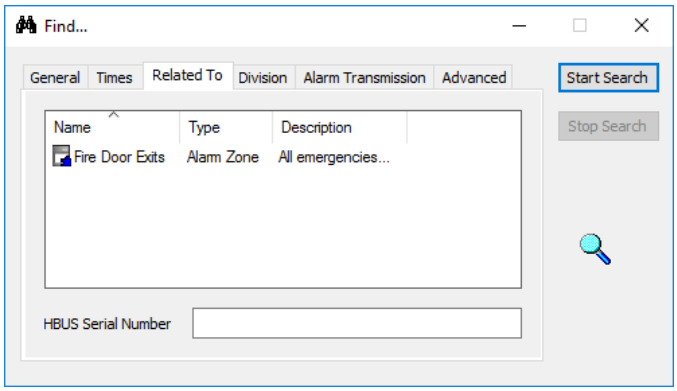
Exemple 2 : Recherche à l'aide des détails connexes

Cet exemple montre comment, à l'aide des champs des onglets *Général* et *Associé à*, vous pouvez définir votre recherche.

Remarque : Pour supprimer les critères de recherche, cliquez avec le bouton droit sur l'élément non souhaité, puis sélectionnez **Supprimer de la liste**.

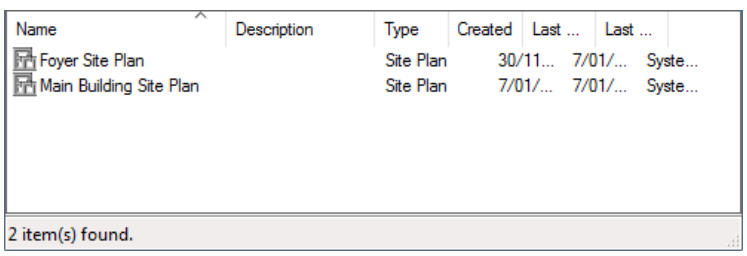
Suivez la procédure ci-dessous pour savoir sur quel(s) plan(s) de site une zone d'alarme particulière apparaît.

1. Cliquez sur l'onglet **Général**.
2. Cliquez sur le **champ** Rechercher **dans** et sélectionnez l'option "Plan de site".
3. Cliquez sur l'onglet **Associé à (Related To)**.
   L'onglet Associé à recherche les éléments du champ Rechercher dans de l'onglet Général qui sont associés à l'élément de cette fenêtre.
4. Ouvrez la fenêtre principale **de la** liste des zones d'alarme (Configurer -zones d'alarme).
5. Sélectionnez la zone d'alarme appropriée et faites-la glisser dans la fenêtre "Associé à".



Remarque : Le champ **Numéro de série HBUS** est toujours affiché, qu'un type d'élément HBUS ait été sélectionné ou non, et permet d'exécuter une recherche en fonction du numéro de série attribué à un périphérique HBUS. Cette recherche peut être basée sur un numéro de série partiel ou complet. Le champ est limité à la taille maximale du numéro de série, et seuls les caractères hexadécimaux peuvent être entrés, c'est-à-dire 0-9 et A-F.

6. Cliquez sur le bouton **Démarrer la recherche**.
   La fenêtre Rechercher s'ouvre et affiche tous les plans de site sur lesquels la zone d'alarme s'affiche.

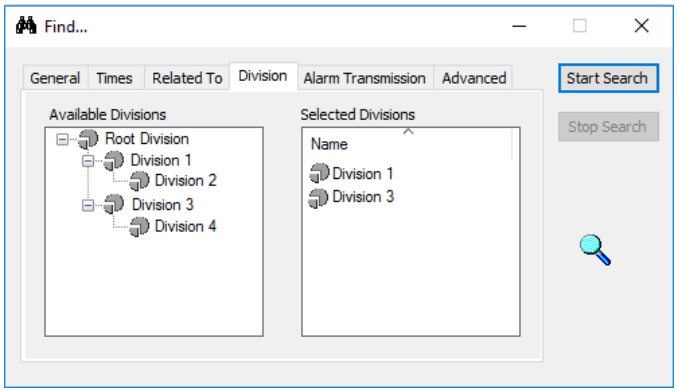


Exemple 3 : Recherche à l'aide de divisions

L'onglet Division vous permet de sélectionner directement une division dans laquelle effectuer la recherche. Les opérateurs peuvent sélectionner et rechercher plusieurs divisions à la fois. Les résultats retournés comprendront tous les renseignements provenant de toutes les divisions sélectionnées, y compris leurs sous-divisions associées.

Cet exemple montre comment utiliser des champs dans les champs **Général**, **Lié à et Onglets** de **division**, vous pouvez définir votre recherche.

1. Cliquez sur l'onglet **Général.**
2. Cliquez sur le champ **Regarder dans** et sélectionnez l'option "Tous les éléments".
3. Cliquez sur l'onglet **Associé à (Related To)**.
4. Ouvrez la fenêtre Liste principale **du groupe d'opérateurs** (Gérer - Groupes d'opérateurs).
5. Sélectionnez le groupe d'opérateurs approprié et faites-le glisser dans la fenêtre "Associé à".
6. Cliquez sur l'onglet **Division**.
   La grille **Divisions disponibles** comprend toutes les divisions dans lesquelles l'opérateur actuel peut afficher n'importe quel élément.
7. Sélectionnez "Division 1" et "Division 3" dans la grille Divisions disponibles et faites-les glisser et déposez-les dans la **grille Divisions sélectionnées**.



8. Cliquez sur le bouton **Démarrer la recherche**.
   Tous les articles associés au groupe d'opérateurs sélectionné, dans la division 1 ou la division **3**, ou dans la **division 2** ou la **division 4** s'affichent dans la fenêtre de recherche.
   Les articles des divisions 2 et 4 sont inclus dans le résultat de la recherche parce qu'ils sont des sous-divisions des divisions qui ont été sélectionnées.

Exemple 4 : Avancé

Les quatre exemples suivants montrent comment, en utilisant les champs de l'onglet Avancé, vous pouvez définir votre recherche.

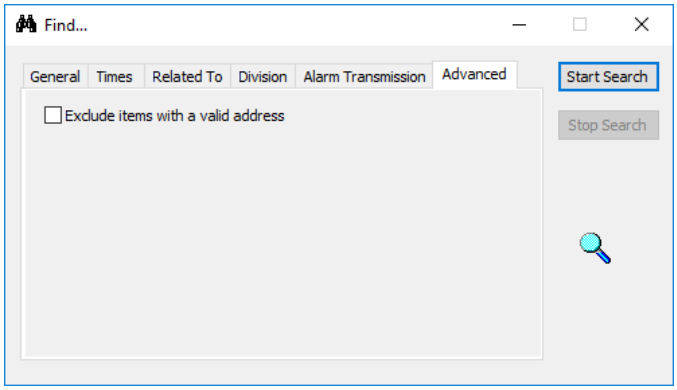
Remarque : Les informations affichées dans l'onglet Avancé varient en fonction de l'élément que vous sélectionnez dans le champ "Regarder dans" de l'onglet Général.

Par exemple, si, dans l'onglet Général, vous sélectionnez "Titulaire de carte", vous êtes invité à entrer des critères relatifs aux titulaires de carte. Ces mêmes informations ne seraient pas affichées si vous sélectionniez "E/S HBUS".

Exemple 4-A

Vous pouvez vérifier quelles interfaces d'E/S HBUS du système n'ont pas encore été configurées.

1. Cliquez sur l'onglet **Général.**
2. Dans le champ "Look in", sélectionnez "HBUS I/O".
3. Cliquez sur l'onglet **Avancé (Advanced)**.
4. **Cochez la case** pour exclure les éléments dont l'adresse est valide.



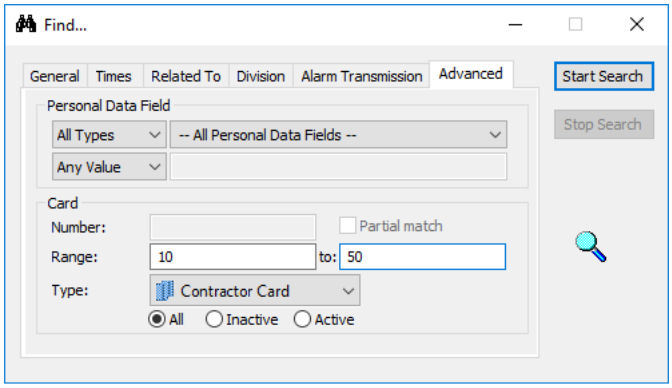
5. Cliquez sur le bouton **Démarrer la recherche**.
   Les interfaces d'E/S HBUS dont l'adresse n'est pas valide s'affichent dans la fenêtre de recherche.

Exemple 4-B

Vous voudrez peut-être savoir quels titulaires de carte dont le numéro se situe entre 10 et 50 sont des entrepreneurs.
Remarque :
Cet exemple ne serait possible que si vous aviez mis en place un type de carte pour la "carte d'entrepreneur".

1. Cliquez sur l'onglet **Général**.
2. Dans le champ "Titulaire de carte", sélectionnez "Look in".
3. Cliquez sur l'onglet **Avancé (Advanced)**.

4. Dans le champ **Plage**, tapez la plage de numéros de carte.
   Remarques :
   - "Numéro de carte" et "Plage de cartes" ne peuvent pas être définis dans votre recherche. Lorsque vous commencez à entrer des détails dans l'un de ces champs, l'autre devient désactivé.
   - Le champ Numéro accepte les caractères génériques (ex. %), s'il n **Tapez** sélectionné ou le format N'est PAS décimal.
5. Dans la liste déroulante **Type**, sélectionnez Fiche entrepreneur.



6. Cliquez sur le bouton radio approprié pour connaître l'état du type de carte à inclure dans votre recherche.

Option	Objectif
Tout	Le paramètre par défaut. Effectue une recherche de titulaire de carte en fonction des paramètres configurés où la recherche n'est pas limitée par l'état d'activation/désactivation de la carte.
Inactif	Effectue une recherche de titulaire de carte en fonction des paramètres configurés où la recherche ne renvoie que les titulaires de carte ayant au moins une carte inactive. Une carte inactive est où : a) La carte est désactivée, OU b) La date/l'heure actuelle est en dehors des limites de l'activation programmée et de la/des date/heure d'expiration.
Actif	Effectue une recherche de titulaire de carte en fonction des paramètres configurés où la recherche ne renvoie que les titulaires de carte ayant au moins une carte active. Une carte active est où : a) La carte est activée, ET b) La date/l'heure actuelle se situe entre la date/l'heure d'activation de la carte et la date/l'heure d'expiration programmée.

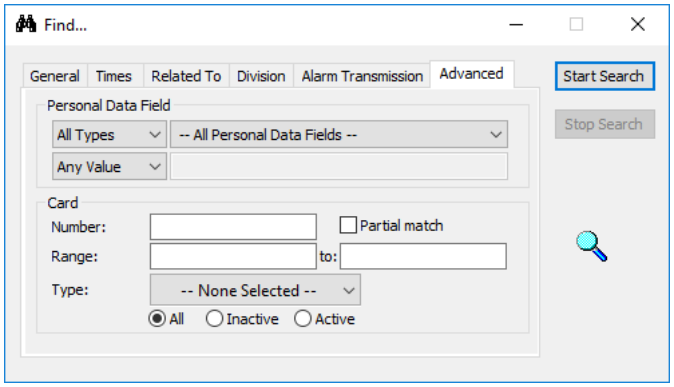
7. Cliquez sur le bouton **Démarrer la recherche**.
   Tous les titulaires de carte de l'entrepreneur dont le numéro se situe entre 10 et 50 s'affichent dans la fenêtre de recherche.

Exemple 4-C

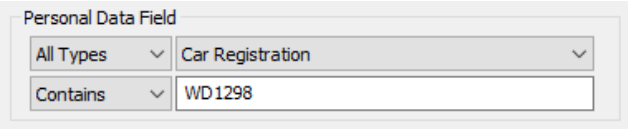
Vous devrez peut-être trouver le propriétaire d'une voiture qui doit être déplacée de l'endroit d'où elle est actuellement garée sur place.

Remarque : Cet exemple ne serait possible que si vous aviez un champ de données personnelles (PDF) configuré pour l'immatriculation des voitures.

1. Cliquez sur l'onglet **Général**.
2. Dans le champ "Titulaire de carte", sélectionnez "Look in".
3. Cliquez sur l'onglet **Avancé (Advanced)**.



4. Dans la liste déroulante Champ de données personnelles (actuellement remplie avec — **Tous les champs de données personnelles —**), sélectionnez "Enregistrement de voiture".
5. Dans le champ actuellement renseigné avec **N'importe quelle valeur**, sélectionnez "Contient" dans la liste déroulante.
   Ceci active le champ de texte libre à côté.
6. Entrez le numéro d'immatriculation de la voiture qui doit être décalée dans le champ texte libre.



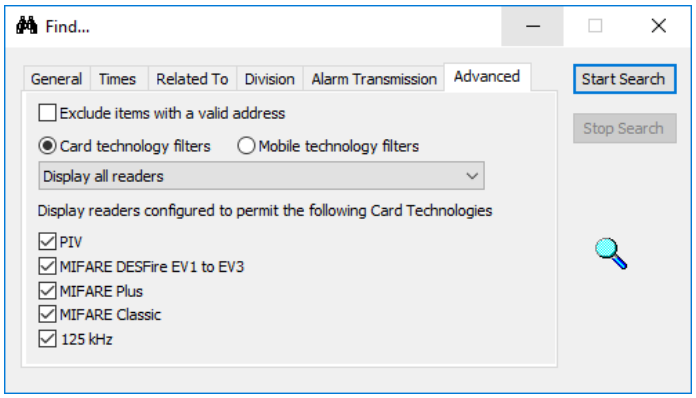
7. Cliquez sur le bouton **Démarrer la recherche**.
   Le détenteur de la carte qui possède la voiture avec le numéro d'immatriculation de la voiture saisie s'affiche dans la fenêtre de recherche.

Exemple 4-D

Il y a une option sur l'onglet **Avancé** qui permet à un site de savoir quelles technologies de cartes les lecteurs utilisent. Cet exemple montre comment savoir quels lecteurs HBUS de votre site sont configurés pour accepter les technologies de cartes MIFARE Classic ou 125 kHz.
Remarque : La technologie de carte autorisée est configurée dans l'onglet **Avancé** des propriétés des lecteurs.

1. Cliquez sur l'onglet **Général**.

2. Dans le champ Look, sélectionnez "HBUS Reader".
   Remarque : La recherche sera limitée aux lecteurs HBUS. De même, si vous avez sélectionné "Cardax IV Reader", la recherche sera limitée à Cardax IV Readers, et si vous avez sélectionné "Card Reader" la recherche inclura à la fois Cardax IV et HBUS Readers.
3. Cliquez sur l'onglet **Avancé (Advanced)**.



4. Décochez les trois premières options, laissant **MIFARE Classic** et 125 kHz coché. La case à cocher **cartes via125 kHz** devient désactivée.
5. Cliquez sur le bouton **Démarrer la recherche**.
   Les lecteurs HBUS configurés pour permettre l'accès via les cartes MIFARE Classic ou 125kHz s'affichent dans la fenêtre de recherche.

Chapitre 42 : Les visionneuses d'événements et d'alarmes

Introduction

La fenêtre Visionneuse d'événements vous permet d'afficher les événements et les alarmes se produisant sur votre site.

Tout ce qui se produit dans le système, des "changements de configuration du site" aux "contournement" en passant par les "changements de détenteur de carte", est enregistré comme activité dans le journal des événements. Lorsque de nouvelles activités se produisent, le message approprié s'affiche en haut de la fenêtre.

Les messages d'événement et d'alarme sont affichés sous forme de résumé (les messages qui vous sont affichés dépendent de votre niveau de privilège):

- Que s'est-il passé ?
- Où il a été généré
- Qui était concerné
- Quand ça s'est passé et quand ça a été enregistré
- Le type d'événement

Vous pouvez sélectionner un message individuel et afficher les détails de l'activité. À partir de là, et avec le niveau de privilège approprié, vous pouvez également reconnaître et traiter les alarmes.

Si vous souhaitez afficher tous les événements d'opérateur/de station de travail associés à un titulaire de carte, vous devez placer la station de travail dans une division pour laquelle vous disposez du privilège d'opérateur "Afficher les événements".

Remarque : Un fichier d'aide en ligne répertoriant tous les messages d'événement/d'alarme est accessible via la barre de menus **Aide** du Centre de commandes et fournit des explications sur la signification de chaque message.

Défilement dans la visionneuse d'événements

Lorsque vous faites défiler la fenêtre de l'Visionneuse d'événements pendant l'arrivée de nouveaux événements, la fenêtre de l'Visionneuse d'événements se comporte comme suit:

- Si aucun événement n'est sélectionné, la fenêtre de l'Visionneuse d'événements reviendra en haut lorsqu'un nouvel événement arrive.
- Si un événement est sélectionné, la fenêtre de l'Visionneuse d'événements conserve sa position et permet à un opérateur de faire défiler les événements de la fenêtre.
- Si l'événement sélectionné s'affiche en bas de la fenêtre de l'Visionneuse d'événements, il est désélectionné et la fenêtre de l'Visionneuse d'événements commence alors à afficher à nouveau les événements les plus récents.
- Un événement sélectionné peut être désélectionné en cliquant dessus. Effectuez cette opération si vous souhaitez afficher à nouveau les événements les plus récents.

Ouverture de la fenêtre de visionneuse d'événements

Introduction

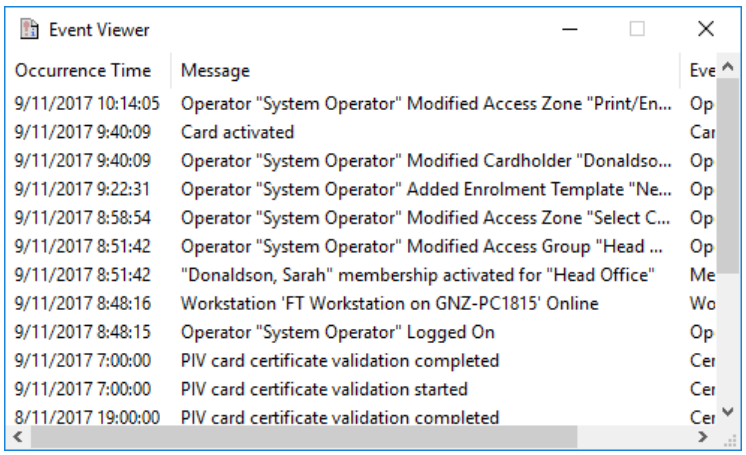
La fenêtre Visionneuse d'événements répertorie l'activité sur votre site ; messages d'événement et messages d'alarme.

Procédure

1. Cliquez sur **Surveiller** dans la barre de menus.
2. Cliquez sur **Visionneuse d'événements**.

Résultat

La fenêtre Visionneuse d'événements affiche :



Remarques :

- Si vous avez une souris avec une molette de défilement, il est possible de faire défiler (vers le haut ou vers le bas) un événement à la fois, à condition que la barre de défilement s'affiche sur le côté de la fenêtre de l'visionneuse d'événements.
- Lorsque l'Visionneuse d'événements est redimensionné ou déplacé, il conserve sa taille et sa position, même si le Centre de commandes est fermé et rouvert.

Conseils

Nouvelle activité
La fenêtre Visionneuse d'événements est mise à jour dynamiquement ; lorsque de nouvelles activités se produisent, le message d'alarme ou d'événement approprié est affiché en haut de la fenêtre.

Ancienne activité
Le système du Centre de commande a une limite quant au nombre de messages affichés (soit 500 événements). Toutefois, la génération d'un rapport d'activité vous permet d'afficher les activités antérieures.

Affichage des détails des événements

Introduction

Vous pouvez vouloir voir plus de détails sur un événement ou une alarme en particulier.

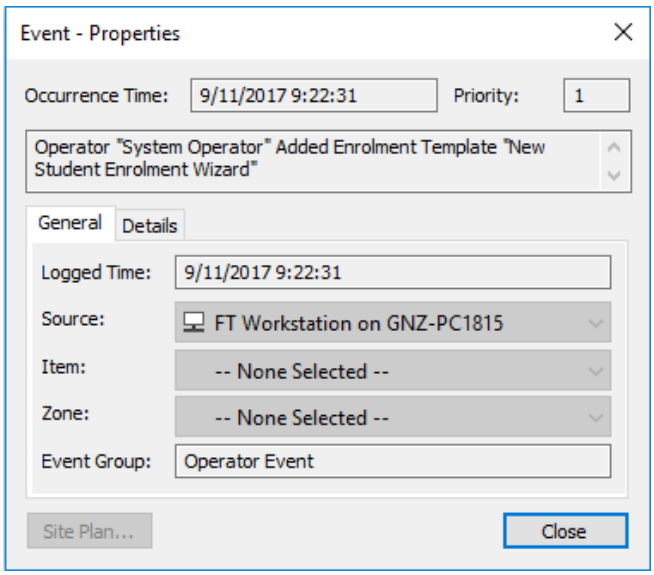
Procédure

1. Cliquez sur **Surveiller** dans la barre de menus, puis sur **Visionneuse d'événements**.
   La fenêtre **Visionneuse d'événements** s'ouvre.
2. Mettez en surbrillance le **message d'activité**.
3. Soit:
   - **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
     Remarque : Si l'événement a des séquences d'images associées, il y aura également l'option **Afficher** dans le menu contextuel. Lorsque cette option est sélectionnée, un autre menu contextuel s'affiche et vous permet de sélectionner la caméra à afficher. La visionneuse de séquences s'affiche.

   Ou:

   - **Double-cliquez sur** l'événement.

   Si vous avez sélectionné un événement, la **fenêtre Propriétés de l'événement s'affiche** :



   Si vous avez sélectionné une alarme, la fenêtre **Alarm** Properties s'affiche. Cette fenêtre est similaire à la fenêtre Événements, mais contient des informations supplémentaires spécifiques aux alarmes. Consultez la section ***Voir les détails de l'alarme*** (page 42-11).

Site Plan...

Ce bouton est activé si l'élément de site pour lequel l'événement s'est produit figure dans un plan de site. Cliquez sur ce bouton pour afficher le plan du site correspondant indiquant l'élément du site.

4. Cliquez sur les onglets si nécessaire pour afficher des détails spécifiques à l'événement.

   General

   Les détails généraux (qui, quoi, où) du message d'activité sélectionné sont affichés.

   Details

   Des détails supplémentaires sont affichés sur le message d'activité.

   Images

   Cet onglet n'apparaît sur la page Propriétés de l'événement que si une séquence d'images est associée à l'événement ; Cliquez sur ce bouton pour afficher la fenêtre de visionneuse de séquences.

5. Cliquez sur **Fermer**.

Résultat

La fenêtre Propriétés de l'événement se ferme.
Vous avez consulté les détails de l'événement, mais n'avez rien fait.

Événements avec rétablissement

Introduction

Les événements appartenant aux groupes d'événements suivants dans le Centre de commandes sont considérés comme ayant un statut et ont donc 'Retour à la normale' événements, (i.e. Restaurations). Il s'agit des événements qui peuvent avoir une icône en forme de cloche rouge dans la fenêtre de visionneuse d'alarme.

Remarque : Chacun de ces groupes d'événements peut envoyer des alarmes et des restaurations Contact ID. Voir ***Surveillance externe des alarmes*** (page 29-1) pour plus de détails.

Groupe d'événements	Type d'événement
Ouverture/Arrêt	Entrée Ouvrir Sortie Désactivée
Fermé/Activé	Entrée Sortie Fermée Activée
Tamper	Contrôleur falsifié (à l'avant) Contrôleur falsifié (à l'arrière) Saut d'entrée Entrée courte Unité Tamponnée (Avant) Unité Tamper (Arrière)
Entrée désactivée/isolée	Entrée isolée Entrée désactivée
Unité Ne Répond Plus	Unité ne répondant pas
Porte Ouverte Trop Longue	Porte Ouverte Trop Longue
Porte non verrouillée	Porte non verrouillée
Porte forcée	Porte forcée
Alimentation hors de portée	Puissance du contrôleur élevée Puissance du contrôleur faible Unité - puissance élevée Unité -puissance faible
Commandes du Centre de commandes interrompues	Échec des commandes au Centre de commandes

Visionneuses d'alarme

Les fenêtres

Il existe deux fenêtres d'affichage d'alarme disponibles dans le Centre de commande qui peuvent coexister, (c'est-à-dire qu'elles peuvent toutes deux être ouvertes sur la même station de travail). Cependant, vos privilèges d'opérateur et les options d'alarme réassignée qui ont été configurées détermineront si elles sont toutes deux accessibles à vous. Ils sont :

- la visionneuse d'**alarme principal**
- a visionneuse d'alertes escaladées (cette fenêtre affiche uniquement les alarmes escaladées, c'est-à-dire que les alarmes qui n'ont pas été confirmées dans un délai spécifié s'affichent dans la visionneuse d'alertes escaladées) **Remarque :** L'escalade est mise en place par le biais de plans d'action.

Les fenêtres de visionneuse d'alarme vous permettent de surveiller les alarmes survenant sur votre site. Les fenêtres contiennent uniquement des messages d'alarme. Cependant, ces messages d'alarme sont également inclus dans la fenêtre de l'visionneuse d'événements.

Le comportement de la fenêtre principale de visionneuse d'alarme et de la fenêtre d'alarme escaladée peut être configuré via l'onglet Configuration des propriétés d'un groupe d'opérateurs (Operator Groups). Voir ***Modification du comportement de visionneuse d'alarme*** (page 42-26) pour la procédure.

Comme la visionneuse d'alarme escaladé est essentiellement une vue filtrée de visionneuse d'alarme principal, les deux visionneuses d'alarme se conforment au même comportement que celui décrit dans ce chapitre. Par conséquent, tous les sujets abordés dans ce chapitre concernent les deux visionneuses d'alarme.

IMPORTANT :
Lorsque toutes les configurations de l'opérateur ont été définies pour supprimer les alarmes reportées de visionneuse d'alarme principal, au moins un opérateur doit avoir la visionneuse d'alarme remonté à l'échelle ouvert à tout moment, pour s'assurer que les alarmes remontées restent visibles.

Regroupement d'alarmes

Les alarmes sont regroupées en fonction de leur niveau de priorité. Lorsqu'une alarme se produit, le message d'alarme s'affiche en haut du groupe d'alarme approprié.

- Le regroupement d'alarmes ayant la priorité la plus élevée s'affiche en haut de la fenêtre.
- Le regroupement d'alarmes ayant la priorité la plus basse s'affiche en bas de la fenêtre.

Inondation d'alarme

L'inondation d'alarme se produit lorsque la même alarme est générée plusieurs fois et remplit la fenêtre de visionneuse d'alarme. Le Centre de commande permet de résumer ces alarmes en affichant une seule instance d'alarme d'inondation, avec un décompte d'inondation indiquant le nombre de fois où l'alarme s'est produite.

Le message d'alarme

Les messages d'alarme s'affichent sous forme de résumé (les messages qui vous sont affichés dépendent de votre niveau de privilège) :

- ce qui est arrivé
- où il a été généré
- qui était concerné.

La date et l'heure du message d'alarme clignotent jusqu'à ce que vous reconnaissiez l'alarme.

Actions que vous pouvez entreprendre

Vous pouvez sélectionner un message d'alarme individuel et afficher ses détails. À partir de là, et avec le niveau de privilège approprié, vous pouvez reconnaître et traiter l'alarme.

Ouverture de la fenêtre de visionneuse d'alarme

Introduction

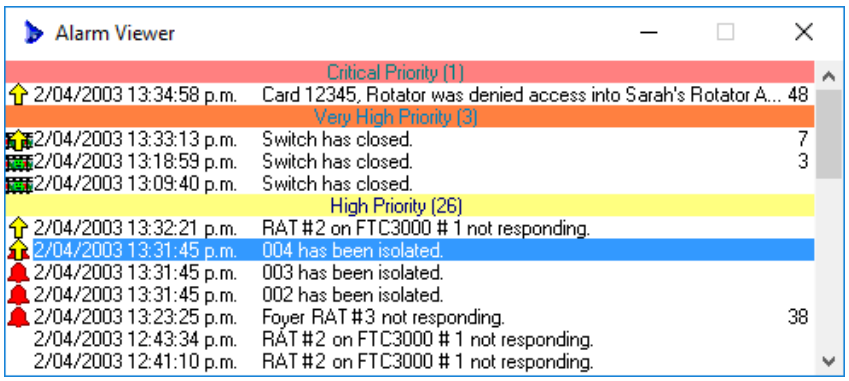
La fenêtre de visionneuse d'alarme répertorie les activités d'alarme sur votre site. Les alarmes sont regroupées selon leur niveau de priorité.

Procédure

1. Cliquez sur **Surveiller** dans la barre de menus.
2. Cliquez sur **Visionneuses d'alarme**.

Résultat

La fenêtre visionneuse alarme s'affiche :



Remarque : Si vous avez une souris avec une molette de défilement, il est possible de faire défiler (vers le haut ou vers le bas) une alarme à la fois, à condition que la barre de défilement s'affiche sur le côté de la fenêtre de visionneuse d'alarme.

Conseils

La fenêtre de visionneuse d'alarme est mise à jour dynamiquement ; lorsqu'une nouvelle alarme se produit, le message d'alarme approprié s'affiche en haut de son groupe prioritaire.

La date et l'heure d'un message d'alarme clignotent jusqu'à ce qu'il soit accusé de réception, et un message d'alarme n'est supprimé de la fenêtre de visionneuse d'alarme que lorsqu'il a été traité.

Les chiffres à l'extrême droite de la fenêtre indiquent :

- les inondations comptent pour une crue d'alarme. Une seule instance d'une crue d'alarme s'affiche, avec le nombre d'inondations pour chaque crue d'alarme, ou
- le nombre de fois qu'une alarme dynamique s'est produite.

Un opérateur doit être capable de distinguer ces deux scénarios en examinant l'historique des événements.

Les entrées d'alarme peuvent avoir différentes couleurs d'arrière-plan. Voir ***Sons d'alarme*** (page 42-23) pour plus de détails.

Diverses icônes peuvent apparaître à gauche d'une alarme. Le tableau suivant décrit ce que ces icônes sont utilisées pour indiquer :

Icône	Indique qu'une alarme....
Rouge Bell 	est actif (c'est-à-dire que le problème n'a pas encore été résolu). Vous pouvez reconnaître une alarme dans cet état, mais pas la traiter.
Film Reel 	a des images associées. Pour plus de détails, voir Voir les images ***associées à une alarme*** (page 42-15) pour plus de détails.
Flèche jaune 	est escaladé. La flèche jaune apparaît sous la forme d'une superposition sur l'icône Film Reel et l'icône Rouge Bell. **Remarque :** Tous les événements et alarmes qui correspondent à la priorité accrue seront les suivants : - **Afficheur d'alarme escaladé**, et - afficher "Escalated" dans les détails de l'alarme.
Cercle croisé	provient d'un serveur distant actuellement hors connexion, et l'opérateur ne pourra pas traiter l'alarme.

Remarque :
Les attributs affichés pour les alarmes "Notify Restoral" peuvent différer légèrement de ce qui a été mentionné ci-dessus. Veuillez consulter la section ***Aviser la restauration*** (à la page 42-29) pour plus de détails.

Réduction des groupes d'alarme

Introduction

Pour chaque groupe d'alarmes, vous pouvez masquer (réduire) ou afficher (développer) toutes les alarmes associées. Par défaut, les groupes d'alarmes sont développés.

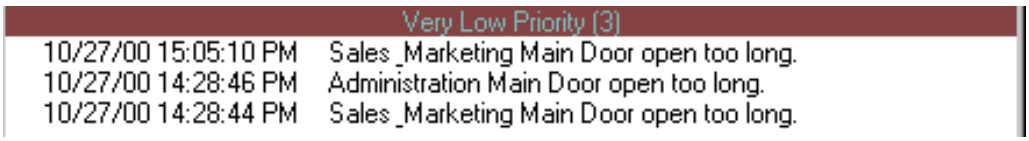
Procédure

1. Cliquez sur **Moniteur** dans la barre de menus, puis sur **Visionneuses d'alarme**. La fenêtre de visionneuse d'alarme s'ouvre.
2. **Double-cliquez** sur l'en-tête de regroupement d'alarme approprié,
   ou,
   Cliquez avec le bouton droit de la souris et sélectionnez **Réduire**.

Résultat

Les messages d'alarme sont masqués.
L'en-tête de regroupement d'alarmes indique le nombre d'alarmes entre parenthèses.

Exemple avant :



Exemple après :



Indication

Pour réafficher les alarmes associées, il vous suffit de double-cliquer de nouveau sur l'en-tête de regroupement d'alarmes ou de cliquer avec le bouton droit de la souris et de sélectionner Développer.

Affichage des détails de l'alarme

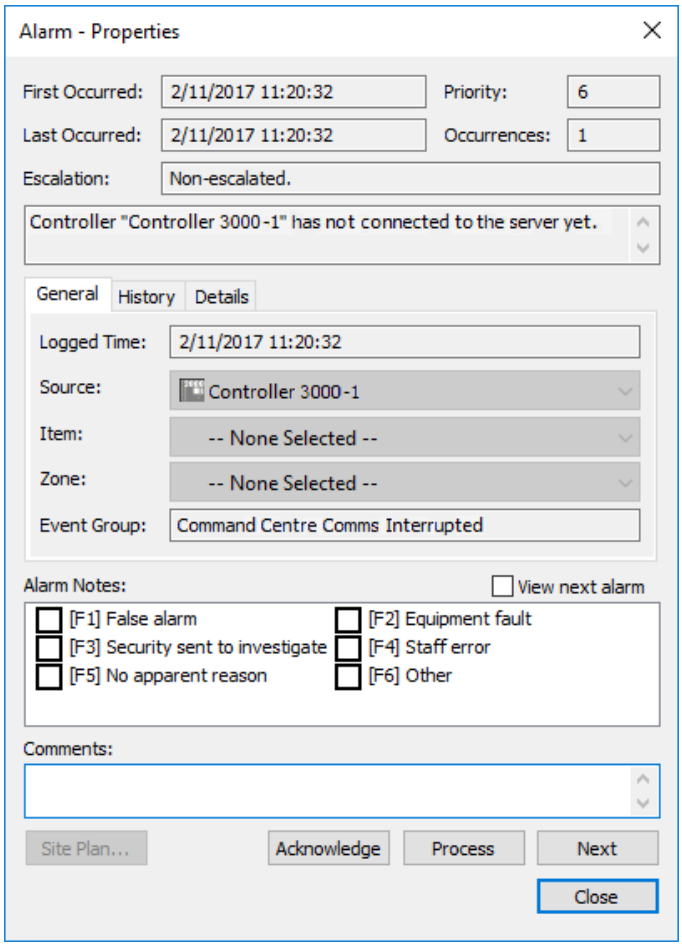
Introduction

Vous pouvez vouloir voir plus de détails sur une alarme particulière.
Remarques :

- Le privilège de l'opérateur "Modifier les alarmes" est nécessaire pour Accuser réception ou Traiter les alarmes, mais les opérateurs sans ce privilège peuvent toujours ajouter des commentaires dans le champ "Commentaires".
- Dans un système multi-serveurs, lorsqu'un serveur distant est hors ligne, un utilisateur ne peut pas accuser réception de l'alarme et elle est marquée comme hors ligne s'il tente de le faire. Toutes les autres alarmes distantes provenant de ce serveur distant apparaissent en mode hors connexion, en lecture seule et l'utilisateur ne peut pas traiter ou entrer des informations les concernant.

Procédure

1. Cliquez sur **Moniteur** dans la barre de menus, puis sur **Visionneuses d'alarme**. La fenêtre de visionneuse d'alarme s'ouvre.
2. Mettez en surbrillance le message d'alarme.
3. Soit :
   - **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**, ou
   - **Double-cliquez sur** l'alarme.
   Si une instruction d'alarme a été définie, l'onglet **Instructions** s'affiche par défaut.
   Si aucune instruction d'alarme n'est définie, l'onglet **Général** s'affiche.



La section Heure de l'événement de cette fenêtre concerne l'inondation d'alarme (voir la section Inondation d'***alarme*** à la page 42-7 pour une description de ce qu'est l'inondation d'alarme et comment la configurer). Les détails suivants sont affichés :

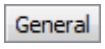
- la date/heure de la **première** apparition d'une crue d'alarme,
- la date/l'heure de l'**alarme la plus récente**,
- nombre d'**occurrences** (c.-à-d. nombre d'inondations) d'une alarme.

Le champ **Escalade** indique l'état d'escalade de l'alarme. Les États sont :

- Non escaladé
- Escaladé
- Escaladé. Accusé de réception/processus refusé.

Le champ Escalade est mis à jour dynamiquement. Si vous appartenez à un groupe d'opérateurs qui n'est pas autorisé à accuser réception ou à traiter les alarmes reportées, les **boutons Accuser réception** et Traiter deviennent désactivés à mesure qu'une alarme se déclenche.

4. Cliquez sur les autres onglets si nécessaire pour afficher les détails spécifiques relatifs à l'alarme :



Cet onglet fournit des détails généraux (qui, quoi, où) sur l'alarme. Il comprend également le "groupe d'événements" sous lequel l'alarme tombe, ce qui est utile de savoir au cas où vous souhaitez exécuter un rapport d'activité pour essayer de résoudre le problème soulevé par l'alarme.

Instructions
Cet onglet n'apparaît sur la page Propriétés de l'alarme que si une instruction d'alarme est associée à l'alarme ou à l'alarme. Il affiche les instructions d'alarme que vous devez suivre ou reconnaître l'alarme.

History
Toutes les actions passées concernant cette alarme sont affichées (par exemple, lorsqu'un opérateur entre des notes et reconnaît l'alarme, ces informations sont entrées dans l'onglet **Historique**).
Une entrée d'audit est également ajoutée à cet onglet chaque fois qu'une alarme est affichée, indiquant quel opérateur l'a vue.

Details
Des détails supplémentaires concernant cette alarme sont affichés (par exemple, la raison pour laquelle l'alarme s'est produite).

Images
Cet onglet n'apparaît sur la page Propriétés de l'alarme que s'il existe une séquence d'images associée à l'alarme. Il affiche une grille d'images. Lorsqu'un d'entre eux est sélectionné, la fenêtre de visionneuse de séquences s'affiche.

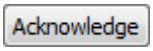
5. Le champ **Alarm Notes (Notes d'alarme)** s'affiche uniquement si des notes d'alarme ont été configurées dans le système, sous l'onglet **Alarm Notes** des propriétés du serveur. Pour de plus amples informations, ***consultez les Notes d'alarme*** (page 6-17).
   Le titre de ce champ s'affiche sous la forme de **notes d'alarme (obligatoire)** ou de **notes d'alarme**. Indique si l'opérateur doit sélectionner une ou plusieurs notes d'alarme pour traiter ou accuser l'alarme ou non.
   Lorsque la fenêtre Propriété de l'alarme est fermée, toutes les notes d'alarme sélectionnées et les commentaires facultatifs sont enregistrés. Ils peuvent ensuite être retracés à partir de l'onglet **Historique**.
   Lorsque le focus est activé sur la fenêtre de propriétés d'alarme, les notes d'alarme peuvent être sélectionnées via les touches de fonction. Par défaut, <**F1**> à <**F8**> sont affectés pour correspondre aux huit premières notes d'alarme de la série.
   Remarque : Si une touche de fonction qui n'a pas de note d'alarme correspondante est enfoncée, alors rien ne se passe.

6. La ☐ View next alarm case à cocher vous permet de parcourir la file d'attente et d'afficher chaque alarme lorsque plusieurs sont présentes. Lorsqu'elle est cochée, l'alarme suivante s'affiche automatiquement une fois que vous avez reconnu ou traité l'alarme ou que vous avez appuyé sur la touche de <**F12**> du clavier.
   La prochaine fenêtre Propriétés de l'alarme sera celle de la prochaine priorité/heure décroissante (comme affiché dans la fenêtre de visionneuse d'alarme) si vous traitez des alarmes à partir de visionneuse d'alarme, ou si entré à partir de l'élément matériel (soit via la fenêtre Matériel ou Plan de site) alors il serait plus filtre sur l'élément matériel.
   Remarque : Pour utiliser cette fonction, vous devez disposer du privilège opérateur "Modifier les alarmes".

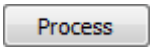
7. Cliquez sur les boutons requis :



Ce bouton est activé si l'élément de site pour lequel l'alarme s'est produite figure dans un plan de site. Cliquez sur ce bouton pour afficher le plan du site correspondant indiquant l'élément du site.

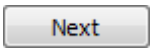


(ou appuyez sur la touche de fonction <**F10**> de votre clavier)
Cela vous permet d'accuser réception d'une alarme afin que tous les relais ou alertes déclenchés par l'alarme soient réinitialisés. Voir ***Accuser réception d'une alarme*** (page 42-16) pour plus de détails.



(ou appuyez sur la touche de fonction <**F11**> de votre clavier)
Cela vous permet de traiter une alarme une fois que la condition d'alarme a été traitée avec. Voir ***Traitement d'une alarme*** (page 42-17) pour plus de détails.

Remarque :
Les boutons **Accuser réception** et **Traiter** peuvent être désactivés pour les alarmes escaladées si vous appartenez à un groupe d'opérateurs qui n'est pas autorisé à accuser réception ou traiter les alarmes escaladées (via l'onglet Configuration du groupe d'opérateurs).



Ce bouton vous permet d'accéder aux propriétés de la prochaine alarme sans fermer la fenêtre Alarm Properties. Quand il n'y a plus d'alarmes cette fenêtre se ferme.

8. Cliquez sur **Fermer**.

Résultat

La fenêtre Propriétés de l'alarme se ferme.
Vous avez vu les détails de l'alarme (ou de l'alarme), mais n'avez rien fait.

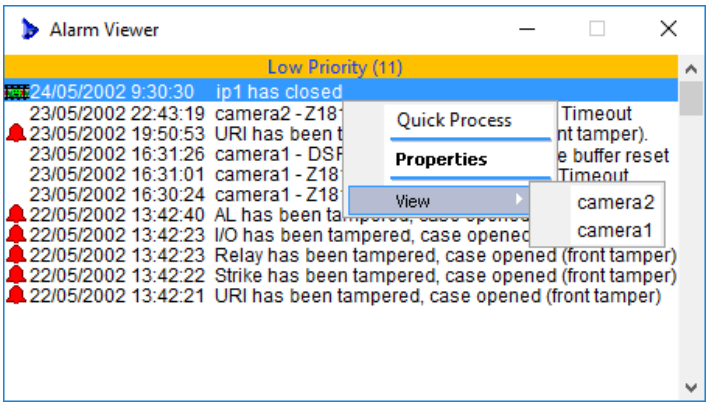
Affichage des images associées à une alarme

Introduction

Si cette option est configurée, une caméra active et enregistre les images associées à une alarme. Lorsque l'alarme s'affiche dans la fenêtre de visionneuse d'alarme, vous pouvez reconnaître qu'elle est associée à des images par l'icône de bobine de film sur le côté gauche du message d'alarme.

Procédure

1. Cliquez sur **Moniteur** dans la barre de menus, puis sur **Visionneuses d'alarme**.
   La fenêtre de visionneuse d'alarme s'ouvre.
2. Soit :
   - **Cliquez avec** le bouton **droit** sur le message d'alarme auquel une image est associée, puis sélectionnez Afficher.

     Si les alarmes associées au plan d'action ont deux caméras configurées pour la capture de séquences d'images, un autre menu contextuel s'affiche avec l'option des deux caméras.
     Sélectionnez l'appareil photo que vous souhaitez afficher.

   Ou:

   - Double-cliquez sur l'alarme.
     La fenêtre Propriétés de l'alarme s'affiche.
     Cliquez sur l'onglet **Images**.

   L'écran visionneuse de séquence s'affiche.
3. Affichez les images pré-événement et post-événement en cliquant sur le ▶ symbole pour lire la visionneuse de séquence.

Indication

Pour les alarmes d'inondation avec images associées, la méthode recommandée pour visualiser les images est d'ouvrir la fenêtre Propriétés de l'alarme et de cliquer sur l'onglet Images.

Acquitter une alarme

Introduction

C'est généralement la première action que vous entreprenez concernant une alarme. En accusant réception d'une alarme, tous les relais ou alertes déclenchés par l'alarme sont réinitialisés.

Remarque :
Le privilège de l'opérateur "Modifier l'alarme" est nécessaire pour reconnaître une alarme, mais les opérateurs dépourvus de ce privilège peuvent toujours ajouter des commentaires dans le champ "Commentaires" (limité à 1024 caractères).

Procédure

1. Cliquez sur **Moniteur** dans la barre de menus, puis sur **Visionneuses d'alarme**. La fenêtre de visionneuse d'alarme s'ouvre.
2. Mettez en surbrillance le message d'alarme.
3. Soit :
   - **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**, ou
   - **Double-cliquez sur** l'alarme.
4. Sélectionnez la ou les notes d'alarme appropriées, et entrez éventuellement les détails de l'action que vous avez entreprise dans le **champ Commentaires**.
5. Soit :
   - Cliquez sur le bouton Accuser réception ou
   - Appuyez sur la touche <**F10**> de fonction de votre clavier.

Résultat

Le message d'alarme reste dans la fenêtre de visionneuse d'alarme.
Le message d'alarme ne clignote plus alors que clignote.

Traitement d'une alarme

Introduction

Une fois que la condition d'alarme (ce qui a réellement provoqué la génération de l'alarme) a été traitée, vous pouvez traiter l'alarme.

Remarque :
Le privilège de l'opérateur "Modifier l'alarme" est nécessaire pour traiter une alarme, mais les opérateurs dépourvus de ce privilège sont toujours en mesure d'ajouter des commentaires dans le champ "Commentaires" (limité à 1024 caractères).

Procédure

1. Cliquez sur **Moniteur** dans la barre de menus, puis sur **Visionneuses d'alarme**. La fenêtre de visionneuse d'alarme s'ouvre.
2. Mettez en surbrillance le message d'alarme.
3. Soit :
   - **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**, ou
   - **Double-cliquez sur** l'alarme.
4. Si un onglet Instructions s'affiche, effectuez l'action nécessaire conformément à l'instruction d'alarme avant de traiter l'alarme.
5. Sélectionnez la ou les notes d'alarme appropriées, et entrez éventuellement les détails de l'action que vous avez entreprise dans le **champ Commentaires**.
6. Soit :
   - Cliquez sur le bouton **Processus**, ou
   - Appuyez sur la touche <**F11**> de fonction de votre clavier.

Résultat

Le message d'alarme est supprimé de la fenêtre de visionneuse d'alarme, mais il reste dans la fenêtre de l'visionneuse d'événements.

Traitement rapide d'une alarme

Introduction

Vous pouvez traiter rapidement certaines alarmes (c'est-à-dire celles qui sont configurées pour ce type de traitement), une fois que la condition d'alarme a été traitée.

Vous devez disposer du niveau de privilège correct pour traiter rapidement les alarmes. Reportez-vous à ***Opérateur*** (page 37-1).

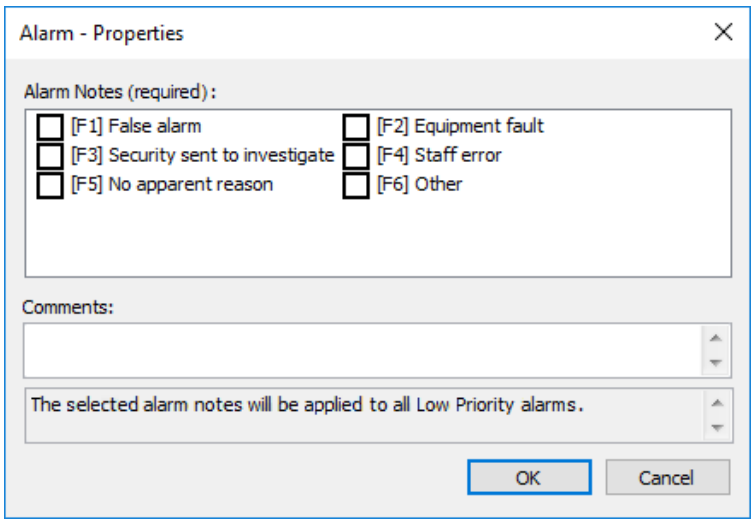
Remarque :
Pour les alarmes escaladées, vous devez appartenir à un groupe d'opérateurs autorisé à accuser réception ou à traiter les alarmes escaladées (via l'onglet **Configuration du groupe d'opérateurs**) pour disposer de la fonction "Processus rapide".

Procédure

1. Cliquez sur **Moniteur** dans la barre de menus, puis sur **Visionneuses d'alarme**. La fenêtre de visionneuse d'alarme s'ouvre.
2. Mettez en surbrillance le message d'alarme.
3. Soit :

   - Appuyez sur la touche <**Application**>  de votre clavier et sélectionnez **Quick Process**, ou
   - **Cliquez avec le bouton droit** de la souris et sélectionnez **Quick Process.**

   Remarque :
   Une boîte de dialogue Notes d'alarme s'affiche si la fonction de notes d'alarme est obligatoire.
   (Le bouton **Fermer** annule cette opération en cliquant sur ce bouton.)



   Pour traiter l'alarme :

   a) Sélectionnez les notes d'alarme appropriées.
      Ils peuvent être sélectionnés à l'aide des touches de fonction indiquées.

b) Le cas échéant, entrez les commentaires dans le champ Commentaires.

c) Cliquez sur le bouton **Processus**.

Cliquez sur le bouton **Fermer** pour enregistrer la ou les notes d'alarme et/ou les commentaires de cette alarme.

Résultat

Le message d'alarme est supprimé de la fenêtre de visionneuse d'alarme, mais il reste dans la fenêtre de l'visionneuse d'événements.

Indication

Si la condition d'alarme est toujours active, l'option Processus rapide ne sera pas disponible sur le menu contextuel, (c'est-à-dire qu'il sera grisé).

Traitement de nombreuses alarmes

Introduction

Dans certains cas (lors de la configuration d'un nouveau site, par exemple), un grand nombre d'alarmes pénètrent dans le système.

Avec le privilège d'opérateur 'Utilisateur avancé', vous pouvez :

- traiter toutes les alarmes inactives dans un groupe de priorité, ou
- traiter toutes les alarmes, actives et inactives, dans un groupe de priorités.

Avec le privilège de l'opérateur "Bulk Process Alarms", vous ne pouvez traiter que toutes les alarmes inactives dans un groupe de priorité. Reportez-vous à la page 37-1).

Remarque : Pour les alarmes escaladées, vous devez appartenir à un groupe d'opérateurs qui est autorisé à accuser réception ou à traiter les alarmes escaladées (via l'onglet **Configuration du groupe d'opérateurs**) pour que les fonctions "Traiter tout" et "Forcer - Traiter tout" soient disponibles.

Procédure

Traiter les alarmes inactives dans un groupe de priorités

1. Cliquez sur **Moniteur** dans la barre de menus, puis sur **Visionneuses d'alarme**. La fenêtre de visionneuse d'alarme s'ouvre.
2. **Cliquez avec le bouton droit** sur l'en-tête du groupe de priorité d'alarme.



3. Dans le menu contextuel affiché, sélectionnez Traiter tout.

Traiter toutes les alarmes dans un groupe prioritaire

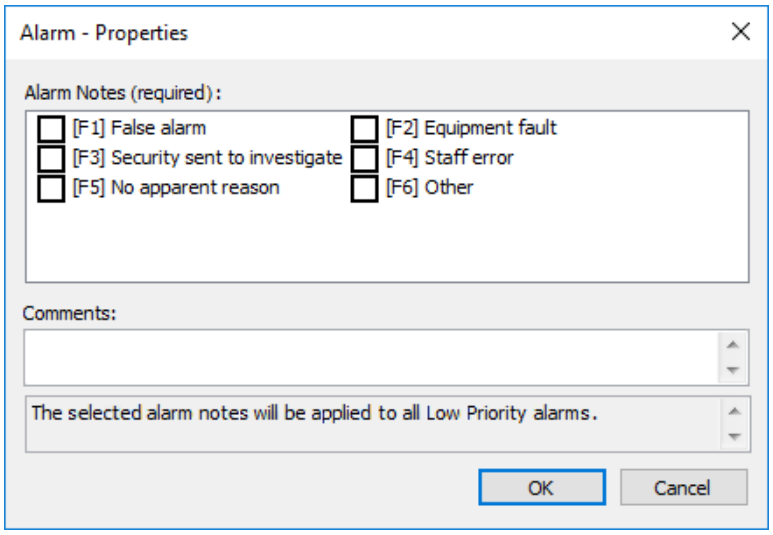
1. Cliquez sur **Moniteur** dans la barre de menus, puis sur **Visionneuses d'alarme**. La fenêtre de visionneuse d'alarme s'ouvre.
2. **Cliquez avec le bouton droit** sur un en-tête de groupe prioritaire d'alarme et appuyez en même temps sur la touche Maj.



3. Sélectionnez **Forcer-Traiter tout**.

Résultat

Une boîte de dialogue Notes d'alarme s'affiche, que la fonction de notes d'alarme soit ou non obligatoire, s'il y a des notes d'alarme configurées.

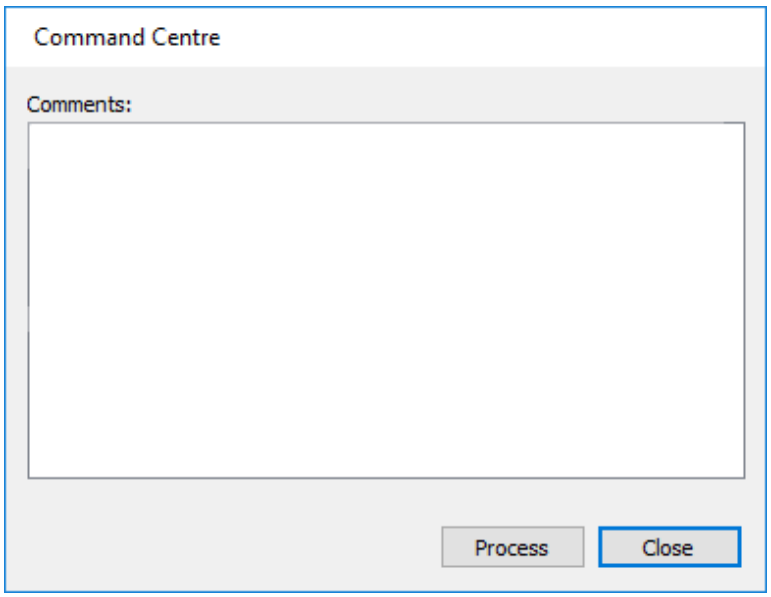


Si la fonction de notes d'alarme est obligatoire et que la priorité du groupe d'alarme est supérieure ou égale à la priorité minimale des notes d'alarme, le titre est défini comme Notes d'alarme (obligatoire), et le bouton Processus n'est activé que lorsque vous sélectionnez au moins une note d'alarme.

Si la fonction de notes d'alarme **n'**est **pas** obligatoire, le titre est défini comme **Alarm Notes**, et le bouton Process est activé.

S'il n'y a pas de notes d'alarme configurées :

- la grille **Alarm Notes** est masquée,
- la **zone de texte Commentaires** s'étend pour remplir la totalité de la zone, et
- la boîte de dialogue est renommée **Command Center**.



Si vous traitiez...	alors...
Alarmes inactives dans un groupe de priorité	toutes les alarmes inactives de ce groupe Priorité sont traitées et disparaissent de la fenêtre de visionneuse d'alarmes. Toutes les alarmes actives (c'est-à-dire les alarmes avec une icône en cloche rouge) que le groupe Priorité affichera toujours.
Toutes les alarmes d'un groupe Priorité	toutes les alarmes (actives et inactives) de ce groupe de priorité sont traitées et disparaissent de la fenêtre de l'afficheur d'alarmes.

Alarme sonore

Introduction

La rétroaction audio est une option pour la génération d'un message d'alarme. Un son (configurable via l'onglet **Événements prioritaires** des propriétés du serveur) est émis lorsqu'il y a des alarmes non reconnues dans l'afficheur d'alarme ou l'afficheur d'alarme escaladé. Reportez-vous à la section Événements prioritaires pour plus d'informations sur la configuration des sons d'alarme.

Recommandation

Si deux alarmes se produisent et que l'alarme de priorité inférieure a un son d'alarme configuré, mais que l'alarme de priorité supérieure a "Aucun son" configuré pour la priorité de l'événement, aucun son d'alarme ne sera émis. Par conséquent, nous vous recommandons de NE PAS désactiver les sons d'alarme pour une priorité d'événement si des priorités d'événement inférieures sont dotées d'un son d'alarme configuré.

Quel son d'alarme joue

Dans la visionneuse d'alarme, le son d'alarme lu est le son d'alarme sélectionné pour la priorité la plus élevée, alarme non reconnue, à condition que cette alarme se soit produite ou ait été déclenchée, depuis la dernière fois que l'opérateur a désactivé les sons d'alarme.

Une fois que l'opérateur a désactivé les sons d'alarme, aucun son d'alarme n'est émis jusqu'à ce que :

- la prochaine nouvelle alarme,
- l'alarme existante suivante est remontée, ou
- une nouvelle occurrence d'une alarme d'inondation se produit en dehors de l'"intervalle d'inondation oubliée".

Qu'est-ce qui empêche les sons d'alarme de jouer

L'une des actions suivantes empêche la lecture d'un son d'alarme sur le poste de travail de l'opérateur :

- L'opérateur éteint les alarmes (voir ***Alarme silencieuse*** à la page 42-25 pour plus de détails). Dans ce cas, aucun son d'alarme n'est émis.
- Une nouvelle alarme de priorité plus élevée se produit (que l'alarme qui est actuellement la cause de l'alarme son).
  Dans ce cas, le son d'alarme de la nouvelle alarme de priorité supérieure est émis (le cas échéant).
- Toutes les alarmes de visionneuse d'alarme de l'opérateur sont reconnues. Dans ce cas, aucun son d'alarme n'est émis.

- Toutes les alarmes non reconnues de la priorité qui déclenche actuellement le son d'alarme sont reconnues.
  Dans ce cas, les règles standard déterminent le son d'alarme (le cas échéant).

Couleurs d'arrière-plan

Différentes couleurs d'arrière-plan pour les entrées d'alarme dans la visionneuse d'alarme peuvent vous aider à déterminer quelle alarme a provoqué un son d'alarme. La couleur d'arrière-plan standard (généralement blanche, mais différente selon vos paramètres Windows), des entrées d'alarme indique les alarmes qui peuvent être la cause d'un son d'alarme, en fonction de leur priorité, tandis que les entrées d'alarme avec la couleur d'arrière-plan alternative (généralement grise), peuvent être éliminées comme causes possibles d'un son d'alarme.

Lorsqu'une nouvelle occurrence d'une alarme se produit, elle a la couleur d'arrière-plan standard et se transforme en couleur d'arrière-plan de remplacement lorsqu'elle est reconnue. Lorsqu'un opérateur met en sourdine les alarmes, la couleur d'arrière-plan de toutes les **entrées d'alarme** change en la couleur d'arrière-plan de remplacement.

Désactiver l'alarme

Introduction

Le son qui est émis en cas d'alarme non reconnue dans la visionneuse d'alarme ou la visionneuse d'alarme escaladé peut être désactivé pour les alarmes actuelles. Une fois éteint, si d'autres alarmes se produisent, le son se reproduira.

Procédure

1. Cliquez sur **Surveiller** dans la barre de menus.
2. Cliquez sur **Désactiver les alarmes - F9**.

Résultat

Le son est muet.

Conseils

Il y a une touche d'accélérateur pour cette fonction muette, comme l'indique l'élément de menu, (c'est-à-dire appuyez sur la touche **F9** pour mettre le son d'alarme en sourdine).

Modification du comportement de visionneuse d'alarme

Introduction

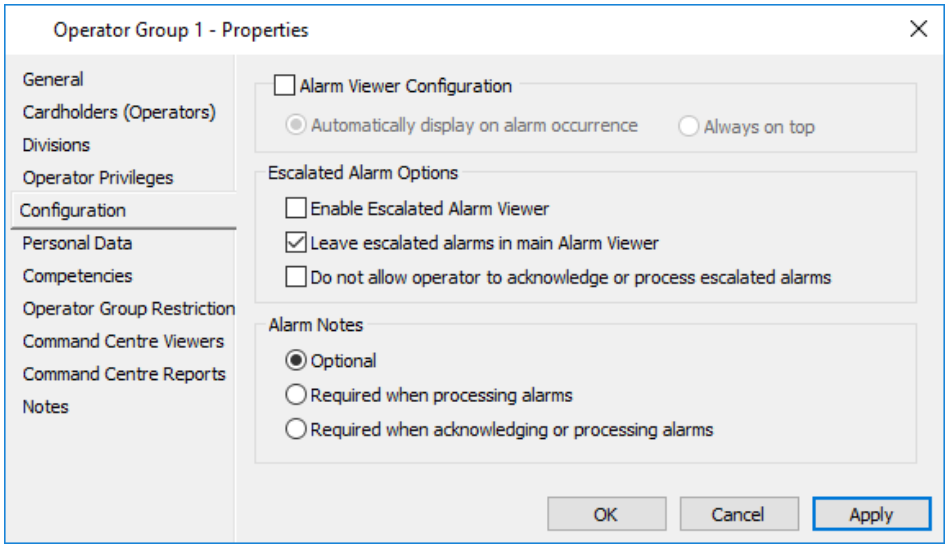
Le comportement de la fenêtre de visionneuse d'alarme peut être configuré via l'onglet **Configuration** des propriétés d'un groupe d'opérateurs. Par conséquent, la fenêtre de visionneuse d'alarme se comporte de la même façon pour tous les opérateurs d'un groupe d'opérateurs.

Les options de comportement de la fenêtre de visionneuse d'alarme sont les suivantes :

- La visionneuse d'alarme reste à l'emplacement où il est placé par l'opérateur actuellement connecté et ne s'affiche pas à l'avant des autres fenêtres.
- La visionneuse d'alarme sera toujours en face de toutes les autres fenêtres.
- La visionneuse d'alarme sera rendu visible et placé à l'avant de toutes les autres fenêtres lorsqu'une nouvelle alarme se produit.

Procédure

1. Cliquez sur **Gérer** dans la barre de menus, puis sur **Opérateur Groupes**.
   La fenêtre **Liste** principale du **groupe d'opérateurs** s'ouvre (en mode grille).
2. **Mettez en surbrillance** le groupe d'opérateurs approprié.
3. **Cliquez avec** le **bouton droit** de la souris, et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Configuration (Configuration)**.



5. Si vous souhaitez que la visionneuse d'alarme reste à l'endroit où il est placé par l'opérateur actuellement connecté et qu'il ne s'affiche pas automatiquement à l'avant des autres fenêtres, vérifiez que la case à cocher **Configuration de visionneuse d'alarme** est désactivée.
   Passez à l'étape 8.
6. Cochez la case **Alarm Viewer Configuration**.
7. Cliquez sur le bouton radio approprié pour l'option que vous préférez.

Option	Description
S'affiche automatiquement en cas d'alarme	La visionneuse d'alarme sera ouvert, rendu visible et porté à l'avant de toutes les autres fenêtres sur l'apparition de toute nouvelle alarme. Avec cette option activée, vous ne pouvez pas localiser la visionneuse d'alarme hors de l'écran et l'ensemble de visionneuse d'alarme sera visible à tout moment.
Toujours en haut	La visionneuse d'alarme sera toujours devant toutes les autres fenêtres. Lorsque cette option est activée, l'ensemble de visionneuse d'alarme sera visible à tout moment et vous ne pouvez pas : • réduire la fenêtre Alarme, ou • localisez la fenêtre d'alarme hors de l'écran.

8. Voulez-vous que les alarmes reportées s'affichent dans une fenêtre distincte de la Visionneuse d'alarmes principale ?

Si...	puis vérifiez...
oui	**Activez la** case à cocher **Visionneuse d'alarme escaladée**. La visionneuse d'alarme escaladé sera accessible à partir du menu **Moniteur**, ainsi que la visionneuse d'alarme principal.
non	**Laissez les alarmes reportées dans la** case **principale de visionneuse d'alarmes**. Toute alarme montée en puissance reste dans la visionneuse d'alarme principal avec des alarmes non remontées.

Remarque : En cochant les deux options, vous pouvez faire apparaître les alarmes reportées dans la visionneuse d'alarme principale ainsi que la visionneuse d'alarme remontée.

9. Cochez la case **Ne pas autoriser l'opérateur à accuser réception ou à traiter les alarmes reportées** si nécessaire pour ce groupe.
Remarque :
Si cette case à cocher est activée, les boutons **Accuser réception** et **Traiter** sont désactivés dans la page de propriétés Détails de l'alarme pour les alarmes reportées.

10. Voulez-vous configurer les options de la note d'alarme ?
Si **non**, passez à l'étape 11.
Si **oui**, cliquez sur le bouton radio approprié pour l'option souhaitée.

- **Facultatif**
  L'opérateur privilégié peut éventuellement sélectionner une ou plusieurs notes d'alarme avant le traitement ou l'accusé de réception d'une alarme.
- **Obligatoire lors du traitement des alarmes**
  L'opérateur privilégié doit sélectionner une ou plusieurs notes d'alarme pour pouvoir traiter ou traiter en bloc les alarmes à un niveau de priorité égal ou supérieur au seuil de priorité des notes d'alarme.

- **Obligatoire lors de la reconnaissance ou du traitement des alarmes**
  L'opérateur privilégié doit sélectionner une ou plusieurs notes d'alarme pour reconnaître, traiter ou traiter en bloc les alarmes de processus à un niveau de priorité égal à ou supérieur au seuil de priorité des notes d'alarme.

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 comportement de la fenêtre de visionneuse d'alarme a été modifié en conséquence.

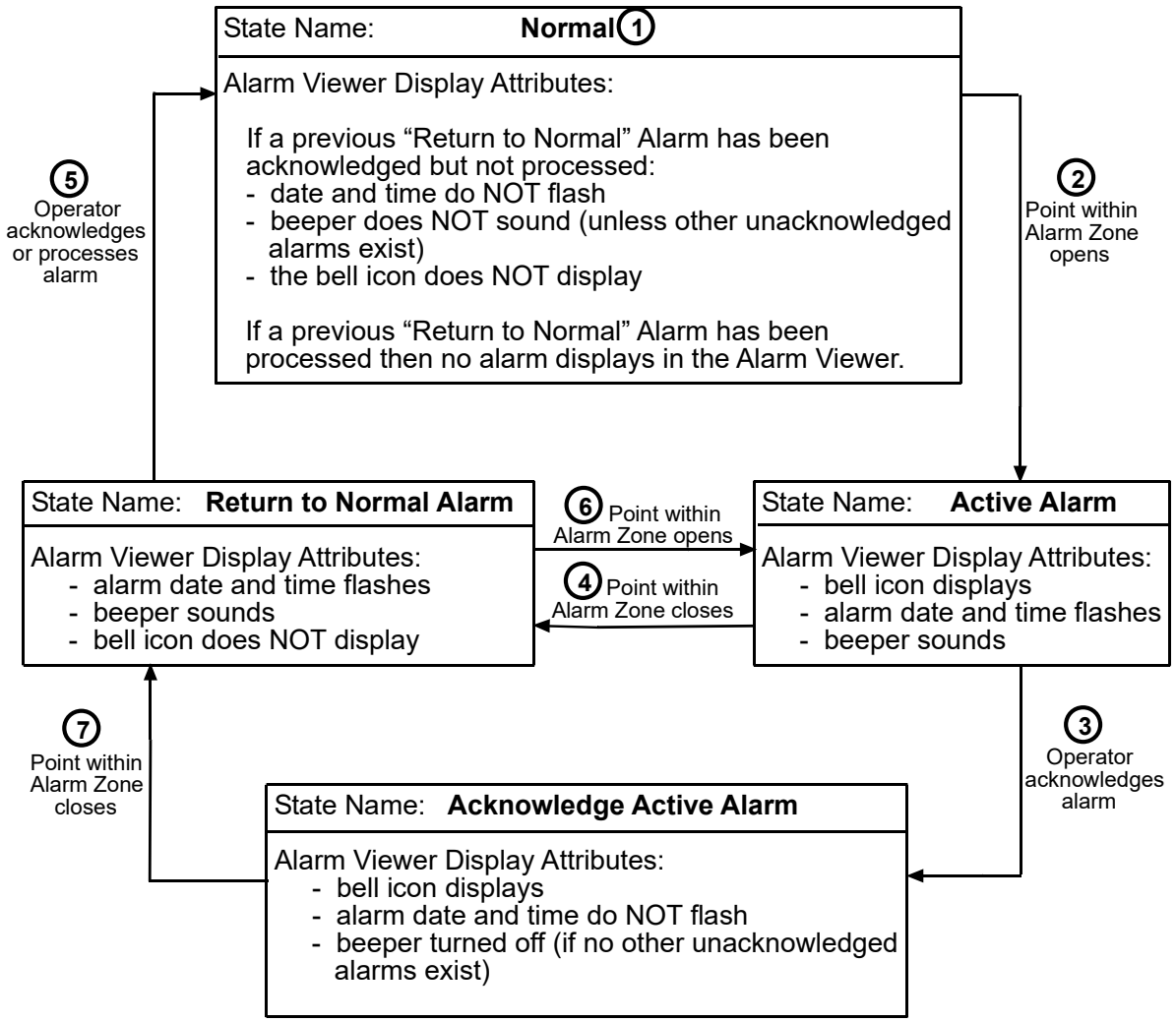
Notifier le rétablissement

Introduction

Notify Restoral ne peut être configuré que pour les événements considérés comme ayant un statut, et donc avoir des événements "Retour à la normale". Consultez la liste ***des événements avec*** des restaurations (page 42-5). Notify Restoral déclenche une alarme sur les événements ouverts et fermés d'une zone d'alarme et est configuré sous l'onglet **Avancé** d'une zone d'alarme. Le comportement Notify Restoral s'applique à tous les points d'une zone d'alarme qui peuvent entrer dans un état d'alarme (par exemple porte ouverte trop longue, porte forcée, porte forcée, etc.).

Présentation

Les points configurés en tant que points de notification et de redirection prennent en charge les états d'alarme affichés dans le diagramme suivant et s'affichent dans la visionneuse d'alarme comme décrit ci-dessous. Chaque alarme Notify Restoral sera dans un des états affichés à tout moment.



Si un utilisateur configure une zone d'alarme avec "Notify Restoral", tous les points de la zone d'alarme suivront l'alarme et tout autre comportement spécifié dans le diagramme sur la page précédente.

Exemple d'entrée Notify Restoral

① État "normal" :

Lorsque Notify Restoral est configuré pour une entrée, une nouvelle instance d'alarme est créée dans la visionneuse d'alarme dans les circonstances suivantes :

1. L'alarme s'affiche et l'entrée s'ouvre.
2. L'alarme est désactivée. Il existe une alarme de retour à la normale. Les contacts d'entrée s'ouvrent.
3. L'inondation d'alarme est activée et l'événement d'ouverture d'entrée suivant est en dehors du paramètre Tolérance.

Dans tous les autres cas, les attributs de l'alarme existante dans la fenêtre de visionneuse d'alarme sont mis à jour.

② État 'ActiveAlarm' :

Lorsqu'une alarme Notify Restoral passe de l'état Normal à l'état 'Alarme active', l'alarme s'affiche dans la visionneuse d'alarme avec les attributs suivants :
- La date et l'heure clignotent (jusqu'à ce que l'opérateur en accuse réception).
- Le bip retentit (jusqu'à ce que toutes les alarmes soient reconnues par un opérateur).
- L'icône de cloche s'affiche (tandis que les contacts d'entrée restent ouverts).

③ État de l'état de l'alarme active :

Une alarme Notify Restoral dans un état "Alarme active" peut être reconnue mais pas traitée. Cela place l'alarme dans un état Accuser réception de l'alarme active. Lorsqu'un accusé de réception d'une alarme active de notification de redirection est reçu, les attributs d'alarme de la fenêtre de visionneuse d'alarme sont mis à jour comme suit :
- La date et l'heure de l'alarme cessent de clignoter.
- Le beeper s'éteint (s'il n'y a pas d'autres alarmes non reconnues dans la visionneuse d'alarme).
- L'icône de cloche reste affichée.

'Revenir à l'état normal :

④ Lorsqu'une alarme Notify Restoral passe directement de l'état "Alarme active" à un état "Retour à la normale" Alarme (en raison de la fermeture des contacts d'entrée), et si l'opérateur n'a pas accusé réception de l'alarme, les attributs de la visionneuse d'alarme changent comme suit :
- L'alarme s'affiche à la même priorité que celle spécifiée dans le plan d'action pour l'événement "Entrée ouverte".
- La date et l'heure de l'alarme continuent de clignoter.
- Le bip continue de sonner (sauf s'il a été désactivé par l'opérateur).
- L'icône de cloche n'est PAS affichée.

Il est possible pour un opérateur de reconnaître et de traiter une alarme dans l'état "Retour à la normale". L'une ou l'autre des actions fait passer l'alarme à l'état "Normal". Lorsqu'un opérateur traite une alarme de retour à la normale, elle est retirée de visionneuse d'alarme.

Ⓢ Lorsqu'une alarme "Retour à la normale" est confirmée, les attributs d'alarme affichés dans la fenêtre de visionneuse d'alarme changent comme suit :
- L'alarme continue de s'afficher à la priorité spécifiée dans le plan d'action pour l'événement "Entrée ouverte".
- La date et l'heure de l'alarme ne clignotent PAS.
- Le signal sonore ne sonne PAS (à moins que d'autres alarmes non reconnues n'existent dans la fenêtre de visionneuse d'alarmes).
- L'icône de cloche n'est PAS affichée.

⑥ Lorsqu'une alarme Notify Restoral est à l'état "Revenir à la normale" et que les contacts d'entrée s'ouvrent, l'alarme passe à l'état "Alarme active". Si la propagation d'alarme est désactivée ou si l'événement d'ouverture d'entrée est en dehors du paramètre de tolérance pour la propagation d'alarme, une nouvelle alarme est créée et affichée dans la fenêtre de visionneuse d'alarme comme suit :
- L'alarme s'affiche à la priorité spécifiée dans le plan d'action pour l'événement "Input open".
- La date et l'heure de l'alarme.
- Le beeper retentit.
- L'icône de cloche s'affiche.

Si l'événement "Input open" est compris dans le paramètre de tolérance pour l'envahissement par alarme, le nombre d'alarmes est incrémenté de 1 et les attributs d'alarme dans la mise à jour de la fenêtre de visionneuse d'alarme comme suit :
- L'alarme continue de s'afficher à la priorité spécifiée dans le plan d'action pour l'événement "Entrée ouverte".
- La date et l'heure de l'alarme continuent de clignoter.
- Le signal sonore continue de sonner (à moins qu'il n'ait été précédemment désactivé par l'opérateur).
- L'icône de cloche s'affiche.

⑦ Lorsqu'une alarme Notify Restoral est dans l'état Accuser réception de l'alarme active et que les contacts d'entrée se ferment, l'alarme passe à l'état 'Retour à la normale'. L'alarme est retournée à un état non reconnu. Les attributs d'alarme affichés dans la fenêtre de visionneuse d'alarme changent comme suit :
- L'alarme continue de s'afficher à la priorité spécifiée dans le plan d'action pour l'événement "Entrée ouverte".
- La date et l'heure de l'alarme.
- Le beeper retentit.
- L'icône de cloche n'est PAS affichée.

Le Centre de commande gère les événements d'alarme et les interventions de l'opérateur différemment lorsque Notify Restoral est défini, par rapport à lorsque Notify Restoral n'est pas défini. Le tableau suivant compare les fonctionnalités lorsqu'un élément Input passe de l'état 'Open/Off'à l'état 'Closed/On'.

Séquence des événements	Notifier la restauration							
	Ensemble				Annuler			
	Affichage des alarmes	Afficher les flashs	Son	Icône Bell	Affichage des alarmes	Afficher les flashs	Son	Icône Bell
Ouverture/arrêt	✓	✓	✓	✓	✓	✓	✓	✓
Reconnu	✓	✗	✗	✓	✓	✗	✗	✓
Événement Fermé/activé	✓	✓	✓	✗	✓	✗	✗	✗
Reconnu	✓	✗	✗	✗	Pas possible			
Traité	✗	✗	✗	✗	✗	✗	✗	✗

Chapitre 43 : Plans de site

Ce chapitre décrit les procédures suivantes requises pour la surveillance des plans d'aménagement.

- ***Affichage d'un plan de site existant*** (page 43-2)
- ***Voir les alarmes à partir des plans du site*** (page 43-4)

Si toutefois vous avez besoin de plus d'informations sur les plans de site, reportez-vous à la section Plans de site de la partie 2 du présent manuel.

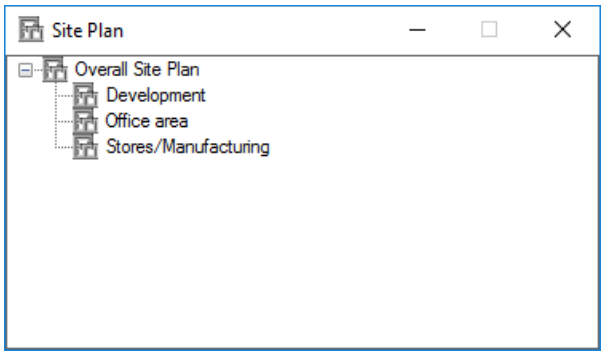
Écrans tactiles

Site Plans est la seule fonctionnalité de Gallagher à prendre en charge l'utilisation d'écrans tactiles et n'est applicable qu'en mode "Affichage" (c'est-à-dire qu'il ne fonctionne pas en mode "Edition"). L'implémentation du simple/double clic est une fonctionnalité supplémentaire pour la prise en charge de l'écran tactile.

Si le logiciel de l'écran tactile des utilisateurs "active le clic droit sur attente", ils n'ont pas besoin de faire quoi que ce soit pour activer la fonctionnalité dans Gallagher FT (clic droit sur attente signifie que s'ils maintiennent leur doigt sur l'écran, il sera le même que le clic droit sur une souris).
Si l'écran tactile de l'utilisateur n'active pas un clic droit en attente, il peut contacter le support technique Gallagher pour obtenir de l'aide.

Fenêtre Liste principale du plan de site

La fenêtre Liste principale **des plans de** site s'ouvre en mode arborescence. Cette vue de l'arborescence est réalisée via l'onglet Lignage lorsque les plans de site sont configurés.



Les plans de site contenant des éléments en alerte clignotent sur cette fenêtre. Si le plan de site qui comporte des éléments en alerte est un plan de site enfant, le plan de site parent clignote également.
Remarque : Un double-clic sur un plan de site en alarme à partir d'ici entraîne l'ouverture du plan de site tant qu'il s'agit d'un plan de site hérité (c'est-à-dire un plan de site créé dans le client de configuration). Vous pouvez ensuite double-cliquer sur l'icône clignotante dans le plan de site pour ouvrir la fenêtre Propriétés de l'alarme pour cet élément.

Si un plan de site a été créé dans le client du centre de commandes, le message suivant s'affichera lorsque vous cliquerez dessus :
"Ce plan de site est modifié ou affiché dans le client Command Center"

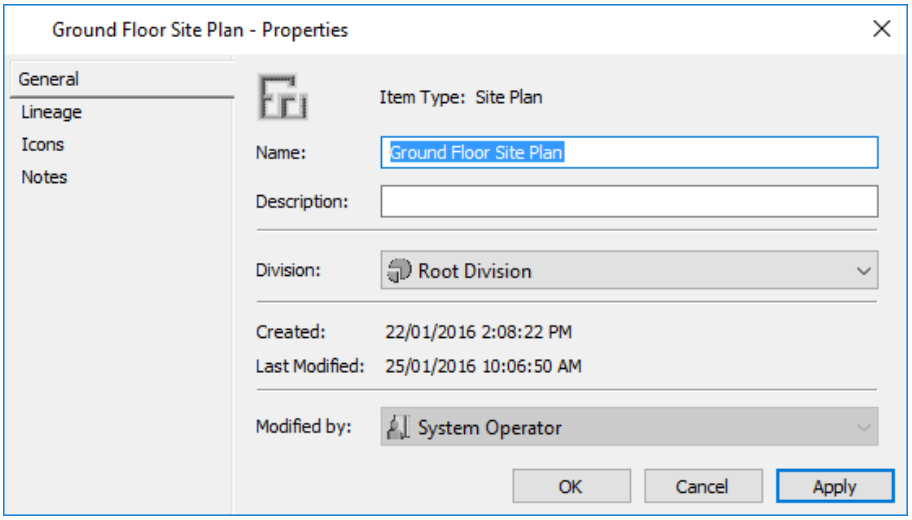
Affichage d'un plan de site existant

Introduction

Vous souhaiterez peut-être voir plus de détails sur un plan de site particulier. Cela peut être fait en ouvrant les propriétés du plan de site ou la disposition du plan de site (c'est-à-dire l'image graphique d'un site ou d'une partie d'un site).

Procédure

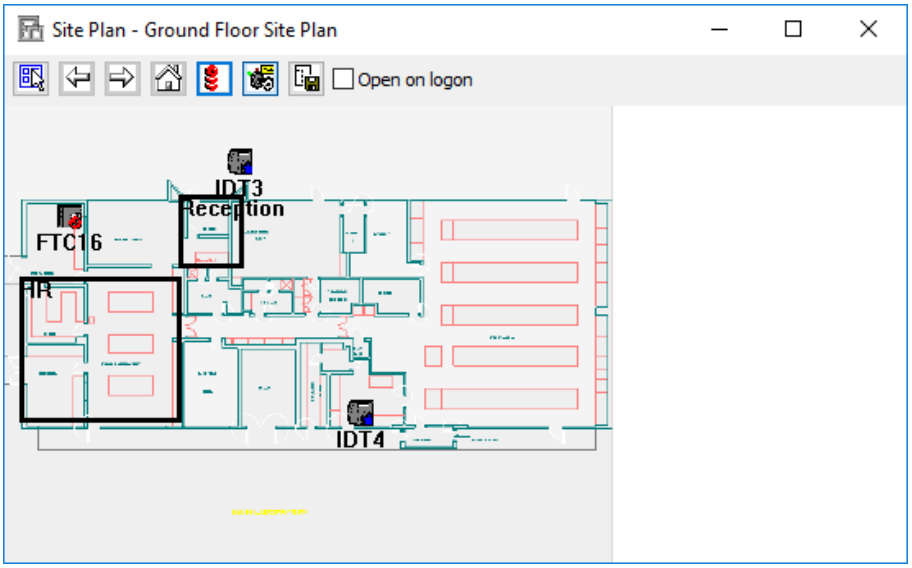
1. Cliquez sur **Surveiller** dans la barre de menus, puis sur **Plans de site**.
   La fenêtre Liste principale **des plans de site** s'ouvre (en vue arborescence).
2. Mettez en surbrillance le plan de site que vous souhaitez afficher.
3. **Cliquez avec le bouton droit** de la souris sur le bouton.
4. Dans le menu contextuel affiché, soit :
   - sélectionnez **Propriétés**.
     Les pages de propriétés Plan de site s'ouvrent. Par défaut, l'onglet **Général** s'affiche.



   ou:

   - sélectionnez **Affichage dans Nouvelle fenêtre**.
     Le plan de site s'ouvre en mode "Affichage" s'il s'agit d'un plan de site hérité (c'est-à-dire créé dans Configuration Client).

     Si le plan de site a été créé dans le client du centre de commande, le message suivant s'affiche :
     "Ce plan de site est modifié ou affiché dans le client Command Center"



Remarque :
Pour plus de détails et une description des boutons de la barre d'outils d'un plan de site, consultez les modes "Édition" et "Affichage" du plan de site.

Conseils

Mode "Edition" et "Affichage"

En cliquant sur le bouton "Mode d'édition du plan de site" vous pouvez passer d'un mode "Édition" à un mode "Affichage".

Dimensionnement et positionnement des plans de site
La taille et la position d'un plan de site peuvent être modifiées en fonction de vos besoins. Vous pouvez modifier la position d'un plan de site en cliquant sur la barre de titre, en maintenant le bouton de la souris enfoncé, puis en le faisant glisser vers la position souhaitée. Pour redimensionner une fenêtre Plan de site, consultez Dimensionnement ***des fenêtres (***page 3-9) pour la procédure.
Ces paramètres seront enregistrés par le système uniquement pour votre ouverture de session (la taille et la position d'un plan de site enregistré par un opérateur n'affecteront pas un autre opérateur).
Remarque : Le redimensionnement d'un plan de site permet de mettre à l'échelle les icônes par rapport à la taille du plan de site et le pourcentage dans le champ "Mise à l'échelle des icônes" change en conséquence.

Affichage des alarmes à partir des plans du site

Introduction

Lorsqu'un élément (par exemple, une forme, une icône, etc., indiquant un plan de site lié ou un autre élément) d'un plan de site commence à clignoter, cela indique qu'une alarme s'est produite. Lorsque cela se produit, vous pouvez consulter les alarmes directement à partir du Plan du site et les reconnaître et les traiter en conséquence.

Remarque : Si un plan de site lié dans alarme a été créé dans le client du centre de commande, le message suivant s'affiche lorsque vous essayez de l'ouvrir en utilisant cette procédure :
"Ce plan de site est modifié ou affiché dans le client Command Center"

Procédure

Affichage des plans de site liés avec alarme

Soit :

- **Cliquez avec le bouton droit** sur l'élément Plan de site lié clignotant et sélectionnez **Afficher le plan de site avec alarme**.
  La fenêtre Plan de site navigue automatiquement directement vers le plan de site contenant l'alarme la plus importante, en ignorant les plans de site intermédiaires. Vous pouvez ensuite afficher l'alarme sur l'élément du site (voir ci-dessous).

  Ou:

- **Double-cliquez** sur l'élément clignotant lié Plan de site.
  Le plan de site indiqué par le lien s'affichera, vous permettant de travailler votre chemin vers l'avant à l'alarme réelle, mais voir chacun des plans de site liés que vous allez.

Affichage des éléments du site avec alarme

Soit :

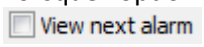
- **Faites un clic droit** sur l'élément clignotant et sélectionnez **Afficher l'alarme**.

  Ou:

- **Double-cliquez** sur l'élément clignotant.
  La plus importante page Propriétés de l'alarme pour l'élément du site s'affiche.

  Remarques :

  - Un double-clic sur une icône clignotante à partir d'ici ou de l'Afficheur d'état entraîne l'ouverture de l'élément dans la page Propriétés de l'alarme. En revanche, un double-clic sur un élément en alarme à partir d'une fenêtre de liste principale ou de l'outil de recherche entraîne l'ouverture des pages de propriétés des éléments.

- Lorsque l'option Afficher l'**alarme est** sélectionnée sur un plan de site et 

que la case à cocher est activée, l'alarme affichée est la prochaine à diminuer la priorité/le temps en rapport avec le plan de site.

Conseils

Alarmes dans la fenêtre de liste principale du plan de site
Les plans de site en alerte clignotent également sur la fenêtre **Plan de site**. Si le plan de site qui est en alerte est un plan de site enfant, le plan de site parent clignote également. Les options Afficher le plan de site avec alarme et Afficher alarme sont disponibles directement à partir de la fenêtre Liste **principale du plan de site**, en cliquant avec le bouton droit sur le plan de site dans alarme, et en sélectionnant l'option requise dans le menu contextuel.

Reconnaissance des alarmes
Les éléments du plan de site cessent de clignoter et restent en couleur une fois l'alarme confirmée.
Pour plus d'informations sur la reconnaissance et le traitement des alarmes, consultez ***Alarm Viewer*** (page 42-6).

Chapitre 44 : Sessions d'opérateurs

Les sessions opérateur peuvent être interrompues pour permettre la libération immédiate des licences de poste de travail (client de configuration ou client de centre de commande), de client mobile et de borne de gestion des visiteurs. Les seuls types de session pouvant être arrêtés sont Operator, Operator (Configuration Client), Receptionist, Visit Host et Mobile.

Remarque : Les sessions de type Opérateur (Client de configuration) sont limitées à 64 sessions par serveur.

L'affichage et la fin des sessions de l'opérateur sont contrôlés via les privilèges de l'opérateur.

- ***Ouverture de la visionneuse des sessions des opérateurs*** (page 44-2)
- ***Fin d'une session d'opérateur*** (page 44-4)

Ouverture de la visionneuse de sessions opérateur

Introduction

Cette visionneuse fournit des détails sur les opérateurs actuellement connectés au serveur Command Center Server.

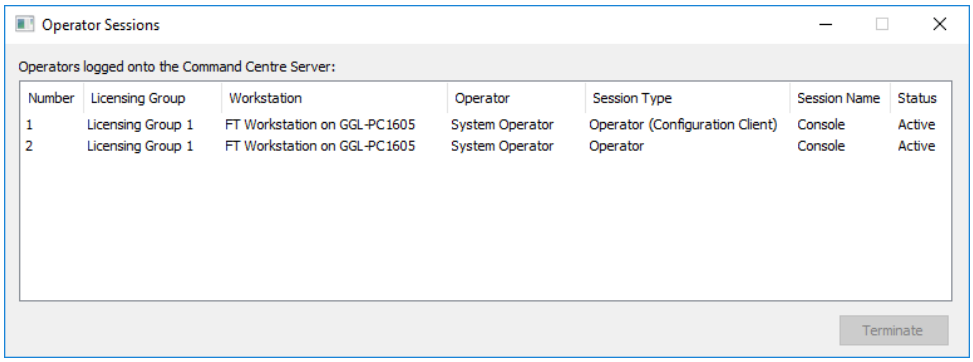
Pour afficher une session dans la visionneuse de sessions opérateur, vous avez besoin du privilège "Afficher les sessions opérateur" ou "Terminer les sessions opérateur" dans la division de la station de travail ou de l'appareil mobile associé à la session.

Procédure

1. Cliquez sur **Surveiller** dans la barre de menus.
2. Cliquez sur **Sessions d'opérateurs**.

Résultat

La liste des sessions est extraite du serveur et affichée dans la visionneuse de sessions d'opérateurs (Operator Sessions Viewer).



Les colonnes de visionneuse de sessions opérateur sont décrites dans le tableau suivant :

Si...	alors...
Nombre	Aide à compter le nombre de sessions de la liste.
Groupe de licences	Nom du groupe de licences auquel la station de travail appartient, le cas échéant.
Station de travail	Nom de l'élément FT du poste de travail associé à la session.
Opérateur	Nom du détenteur de la carte qui s'est connecté en tant qu'opérateur.

Si...	alors...
Type de session	Affiche le rôle assigné à la session à des fins de licence. L'utilisateur connecté aura l'un des rôles suivants : • Aucun (vide) • Opérateur • Opérateur (client de configuration) • Mobile • Réceptionniste • Visiter Préinscription • Importation/exportation • OPC • À distance **Remarque :** Dans un système multi-serveurs, lorsqu'un opérateur est connecté à un serveur distant (par exemple, la surveillance des alarmes distantes), elles s'affichent sous la forme d'une session "à distance".
Nom de session	Nom de la session des services Terminal Windows.
État	Chaque session a l'état "Actif" ou "Expiré". Une session **Active** est active et a envoyé un ping au serveur au cours des 50 dernières secondes. Une session **expirée** est une session orpheline qui n'a pas envoyé de ping au serveur au cours des 50 dernières secondes et qui a été déconnectée.

Fin d'une session d'opérateur

Introduction

Cette procédure décrit comment mettre fin à une session d'opérateur.

Pour autoriser la fin d'une session, vous devez disposer du privilège "Terminer les sessions de l'opérateur" dans la division du poste de travail ou de l'appareil mobile associé à la session. Le privilège "Terminer les sessions opérateur" inclut les privilèges fournis par la session de l'opérateur vue.

Procédure

1. Cliquez sur **Surveiller** dans la barre de menus, puis sur **Sessions d'opérateurs**.
   La fenêtre Opérateur Sessions Viewer s'ouvre.
2. Cliquez sur la session que vous souhaitez terminer et cliquez sur Terminer s'affiche.
   Le message de confirmation *"Êtes-vous sûr de vouloir mettre fin à cette session d'opérateur ?"* s'affiche.
3. Cliquez sur le bouton **Oui**.
   La session disparaît de la visionneuse de sessions opérateur.
4. Cliquez sur le bouton **Fermer (X)** pour fermer la Visionneuse de sessions opérateur.

Résultat

Une session opérateur est terminée et :

- le message d'échec de connexion réseau suivant s'affiche pour l'opérateur dont la session a été interrompue :
  "Votre session a été interrompue par un administrateur système"
- un événement Opérateur est généré.

Chapitre 45 : Statut et contournement

Ce chapitre fournit des informations sur l'affichage de l'état des éléments système et l'exécution de contournement pour modifier temporairement l'état des éléments.

Reportez-vous à ***Privilèges de l'opérateur*** (à la page 37-1) pour vérifier que vous disposez du niveau de privilège de l'opérateur correct pour l'activité que vous souhaitez réaliser.

Présentation du statut et des contournement

État

L'état actuel des éléments reliés à votre système du Centre de commandes peut être affiché dans l'Afficheur des états. Les informations affichées pour chaque élément dépendent du type de dispositif (par exemple, une entrée afficherait normalement si elle est ouverte ou fermée, tandis qu'une porte afficherait si elle est sécurisée, libre, etc.)

L'Afficheur d'état est mis à jour dynamiquement ; lorsque l'état d'un élément change, la visionneuse change également.

Contournement

Les contournement permettent à un opérateur/détenteur de carte de modifier temporairement le statut d'un élément connecté à votre système du Centre de commande. Ils permettent aux opérateurs de répondre à des événements aléatoires communs. Par exemple, déverrouiller temporairement la porte pour donner accès à un titulaire de carte qui a oublié sa carte.

Tous les événements de remplacement sont signalés intégralement dans le journal des événements.

Un seul remplacement peut être appliqué à un seul objet. Si un second remplacement est démarré, le premier est annulé.

Les opérateurs peuvent remplacer les horaires pour :

- Relais d'horloge
  (par exemple, changer temporairement l'heure à laquelle la climatisation est automatiquement activée)
- Mode d'accès pour une zone d'accès
  (par exemple, modifier temporairement le mode programmé d'une zone d'accès afin de permettre un accès facile aux visiteurs d'un lieu de réunion)
- État de la zone d'alarme
  (par exemple, changer temporairement le statut d'une zone d'alarme en réponse aux personnes qui font des heures supplémentaires)

Les contournement peuvent rester en vigueur jusqu'à la prochaine modification automatique (telle que programmée sur l'horaire), ou pendant une durée spécifiée entrée par l'opérateur. Les contournement mis en oeuvre pour une durée spécifiée persisteront si le serveur se réinitialise ou si une configuration du système se produit.

Ouverture de la Visionneuse d'état

Introduction

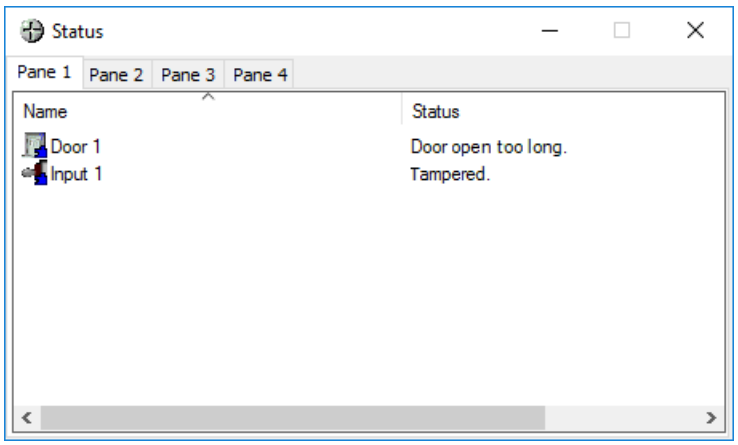
Vous pouvez ajouter et supprimer des éléments dans la Visionneuse d'état.

Procédure

1. Cliquez sur **Surveiller** dans la barre de menus.
2. Cliquez sur Afficher le statut.

Résultat

La Visionneuse d'état s'affiche.



La description du statut dépend du type d'élément sélectionné.
Par exemple ; un statut d'entrée indiquerait un sabotage, une ouverture, une fermeture, etc., tandis qu'un statut de porte indiquerait une porte ouverte trop longue, etc.

Remarque :
Les éléments en alerte clignotent sur cet écran. Un double-clic sur un élément clignotant d'ici ou d'un plan de site entraîne l'ouverture de la page Propriétés de l'alarme. En revanche, un double-clic sur un élément en alarme à partir d'une fenêtre de liste ou de l'outil de recherche entraîne l'ouverture des pages de propriétés des éléments.

Conseils

Volet onglets
Par défaut, il y a 4 volets (nommés 'Volet 1' à 'Volet 4'). Vous pouvez ainsi regrouper des articles selon vos besoins. Par exemple, dans un volet, ajoutez uniquement les éléments dont vous avez affaire. Vous pouvez ajouter ou supprimer des volets (avec une limite de 24 volets) et les renommer en fonction de vos besoins en cliquant avec le bouton droit de la souris sur un onglet et en sélectionnant l'action appropriée (par exemple **Renommer**, **Nouveau volet ou Supprimer le volet)**.

Informations enregistrées
Lorsqu'un opérateur se déconnecte, les éléments de visionneuse sont enregistrés avec les préférences (par exemple, les volets renommés). Lorsque le même opérateur se connecte à nouveau, les listes d'éléments et de préférences enregistrées sont réaffichées.

Propriétés
Une autre méthode d'affichage du statut est via la fenêtre Propriétés de l'élément requis.

Ajout d'éléments à l'afficheur d'éta

Introduction

Vous pouvez ajouter facilement des éléments à l'afficheur d'état.
Remarque : Tout élément dont les propriétés comportent un onglet Statut et Contournement peut être ajouté à la Visionneuse d'état, ainsi qu'aux archives, macros et modifications en bloc.

Procédure

Méthode Drag and Drop :

1. Cliquez sur **Moniteur** dans la barre de menus, puis sur **Afficher le statut**. L'Afficheur **des** statuts s'ouvre.
2. Ouvrez la fenêtre Liste principale qui contient l'élément dont vous souhaitez voir l'état.
   Par exemple, ouvrez la fenêtre Liste principale **du matériel**.
3. Localisez l'élément requis.
4. Faites glisser et déposez cet élément dans l'afficheur d'**état.**
   Par exemple, faites glisser l'élément matériel "H/O Controller 6000" dans l'état Visionneuse.

Méthode Copy and Paste :

1. Ouvrez la fenêtre Liste principale qui contient l'élément dont vous souhaitez voir l'état.
2. **Cliquez avec le bouton droit** de la souris sur l'élément requis.
3. Cliquez sur **Copier**.
4. Cliquez sur **Moniteur** dans la barre de menus, puis sur **Afficher le statut**. L'Afficheur **des** statuts s'ouvre.
5. Cliquez avec le bouton droit de la souris et cliquez sur Coller.

Résultat

L'élément est ajouté à la liste Statut.
Remarque : Le Centre de commandes n'enregistre que 100 éléments dans un seul volet d'état. Si vous essayez d'ajouter plus de 100, un message d'erreur s'affiche.

Indication

Vous pouvez sélectionner plusieurs éléments et les faire glisser dans la Visionneuse.
Reportez-vous à ***Sélection d'éléments d'une liste*** (page 3-7).

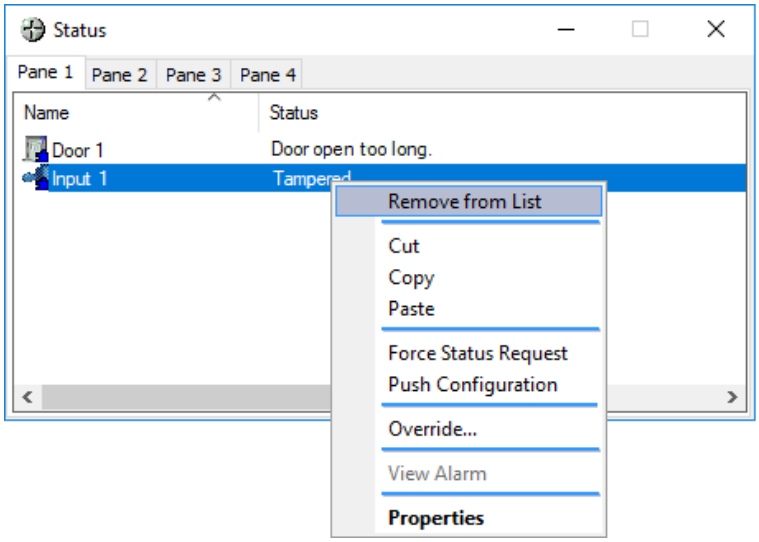
Suppression d'un élément de l'afficheur d'état

Introduction

Lorsqu'un élément n'est plus souhaité dans l'Afficheur des statuts, il s'agit d'une procédure simple pour le supprimer.

Procédure

1. Cliquez sur **Moniteur** dans la barre de menus, puis sur **Afficher le statut**. L'Afficheur **des** statuts s'ouvre.
2. Cliquez avec le bouton droit sur l'élément à supprimer.
3. Cliquez sur Supprimer de la liste.



Résultat

L'élément est supprimé de l'Afficheur des statuts.

Exécution de contournement

Introduction

Cette procédure décrit comment remplacer temporairement l'état d'un élément. Les éléments sur lesquels vous pouvez effectuer les contournement sont les suivants :

- Résultats
- Entrées
- Zones d'accès
  Remarque : Les contournement de verrouillage et de bouton-poussoir peuvent également être effectués sur les zones d'accès. Reportez-vous aux sections ***Verrouillage de la zone d'accès*** (page 10-8) et ***Configuration des contournement de boutons-poussoirs*** (page 10-32).
- Zones d'alarme
- Zones de clôture
- Blocs logiques
- Éléments matériels :
  - Contrôleur 6000
  - Lecteur HBUS
  - Terminal HBUS
  - Terminal d'alarmes HBUS uniquement
  - Lecteur de carte de contact HBUS
  - E/S HBUS
  - Contrôleur de clôture HBUSF31/F32/F41/F42
  - Contrôleur de clôture HBUS F22
  - Groupe de capteurs de tension HBUSZ10
- Interfaces d'ascenseur de haut niveau (HLI d'ascenseur)
- Guard Tours
  Remarque : Reportez-vous à ***Exécution d'un tour de garde*** (page 54-6) pour des détails sur la substitution, (c'est-à-dire l'arrêt et le démarrage) Garde Tours.
- Portes (y compris les groupes de verrouillage)
  Il existe deux options de remplacement des portes, comme suit :

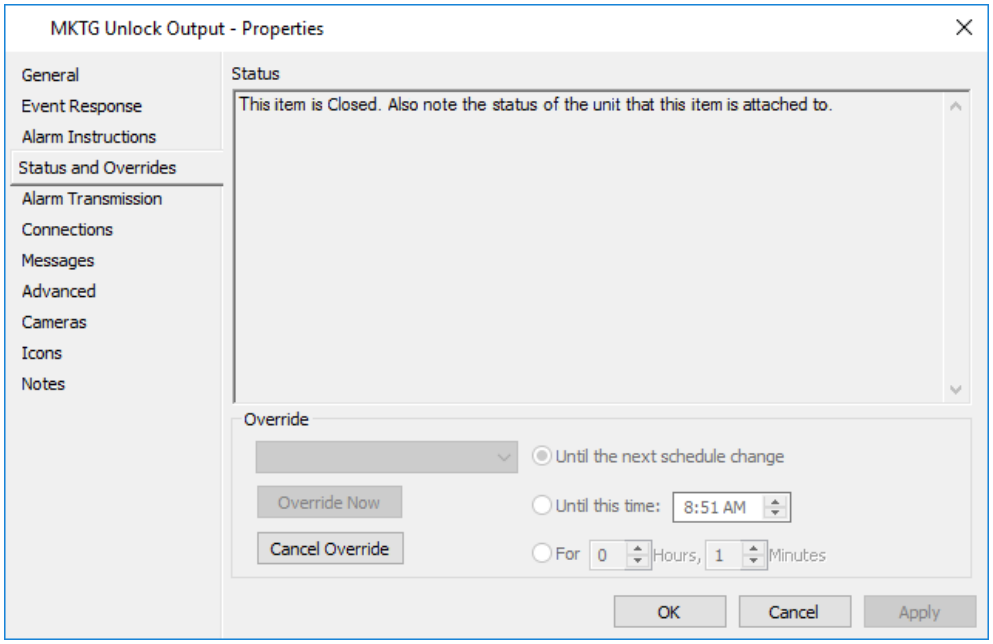
Option de menu	Fonction
Ouvrir la porte	Cette option libère une porte pour permettre à une personne de passer à travers. Veuillez consulter la ***section Ouvrir une porte*** (page 45-13) pour connaître la procédure distincte.
Remplacer l'accès d'entrée	Cette option ouvre l'onglet "Statut et remplacement" de la zone d'accès (c'est-à-dire la zone d'entrée) qui est attachée à la porte. S'il n'y a pas de zone d'entrée, cette option est grisée. **Remarque :** Le remplacement d'une zone d'entrée remplace TOUTES les portes de cette zone.

Reportez-vous à la rubrique ***Remplacement*** (page 37-26) pour afficher les privilèges requis pour effectuer un remplacement dans le Centre de commandes.

Procédure

Remarque : Vous ne pourrez peut-être pas démarrer un remplacement si l'élément cible est hors ligne, car le remplacement ne sera pas immédiatement appliqué et pourrait être perdu si la cible n'est pas en ligne pendant plus d'une minute.

1. Ouvrez la fenêtre Liste de l'élément à remplacer.
2. **Cliquez avec** le bouton **droit** sur l'élément concerné, puis cliquez sur **Remplacer...** dans le menu déroulant.
   L'onglet **Statut et remplacement** de la fenêtre Propriétés de cet élément s'affiche.



   Remarque : Si vous souhaitez remplacer l'entrée d'accès d'une porte, cliquez sur **Remplacer l'entrée (Override Entry Access)** dans le menu déroulant.
   L'onglet **Statut et remplacement** de la fenêtre Propriétés de la zone d'accès s'affiche.
3. Cliquez dans le champ **Remplacer (Override)** et sélectionnez le statut approprié dans la liste déroulante.

Si vous l'êtes remplacement...	**alors...**
une sortie, une zone d'accès ou une zone d'alarme	définissez la durée de la substitution à implémenter. Vous pouvez soit : • sélectionnez le bouton d'option Jusqu'à la prochaine modification de la planification, ou • sélectionnez le bouton radio Jusqu'à ce moment, puis entrez l'heure du jour où le remplacement doit avoir lieu, ou • sélectionnez la case d'option Pour xx heures, xx

Si vous l'êtes remplacement...	alors...
	minutes et entrez les heures et/ou les minutes (cette limite est limitée à un maximum de 23 heures et 59 minutes). **Remarques :** • Si vous ne sélectionnez pas d'option, elle sera définie par défaut jusqu'à la modification de la planification suivante. • Lors de l'affichage du journal des événements, il n'est pas possible de faire la différence entre un remplacement basé sur l'heure de la journée (par exemple jusqu'à 16h) et un remplacement basé sur la durée (par exemple, un remplacement pendant 4 minutes). Toutefois, il est possible de calculer l'heure de fin d'un remplacement en ajoutant la durée du remplacement à l'heure à laquelle l'événement de remplacement s'est produit. ***ZONES D'ALARME UNIQUEMENT*** Si une zone d'alarme ne parvient pas à s'armer en raison d'alarmes actives et que l'opérateur dispose du privilège "Override" ou "Override up to Medium Priority", une **option Armé (avec alarmes actives) est disponible dans la** liste déroulante Override au lieu d'une option Armé. Les règles de privilège s'appliquent (c'est-à-dire que si l'opérateur a le privilège "Remplacer par priorité moyenne", le remplacement ne fonctionne que sur les alarmes actives jusqu'à et y compris la priorité moyenne, et si l'opérateur a le privilège "Remplacer", il peut remplacer les alarmes actives de toute priorité).
une entrée	**Shunt :** Cela arrête la communication avec l'entrée et restera ainsi jusqu'à ce que vous "Déshunt". **Déshunt :** Ceci commence l'interrogation de l'entrée. **Isoler :** Isolera l'entrée de sorte que la zone d'alarme puisse être armée. Les alarmes de l'entrée ne seront plus déclenchées. **Désisoler :** L'entrée n'est plus isolée.

Si vous l'êtes remplacement...	alors...
une zone de clôture	**Shunt :** Cela arrête la communication avec la zone de clôture et restera ainsi jusqu'à ce que vous "Déshunt". **Déshunt :** Ceci commence le vote de la zone de clôture. **Activé :** Cela entraîne l'activation de la zone de clôture (c'est-à-dire la pulsation). **Désactivé :** Cela entraîne l'inactivité de la zone de clôture (c'est-à-dire qu'elle n'est pas en train de pulser). **Haute tension :** Cela changera le mode HV/LF à haute tension pour cette zone de clôture. Ce remplacement est uniquement compatible avec les contrôleurs de clôture F31, F32, F41, F42 et F22. **Sensation faible :** Cela changera le mode HV/LF à faible sensation pour cette zone de clôture. Ce remplacement est compatible avec les contrôleurs de clôture F31, F32, F41, F42 et F22.
un élément matériel	**Réinitialiser :** Cette opération réinitialise le logiciel sur l'élément matériel. (Remarque : Il est recommandé de vérifier l'état du commutateur DIP 2 avant d'effectuer une "réinitialisation" sur un contrôleur.) **Shunt (pas pour les contrôleurs) :** Cela arrête la communication avec le périphérique, et toutes les entrées et sorties sur ce périphérique ne seront plus disponibles par le système. Il restera ainsi jusqu'à ce que vous "Déshunt". ***LECTEURS HBUS, TERMINAUX HBUS, ALARMES HBUS UNIQUEMENT TERMINAUX ET INTERFACES D'E/S HBUS*** **Commencer l'identification du périphérique :** *Lecteurs HBUS, terminaux HBUS, terminaux HBUS Alarms Only et lecteur de carte de contact HBUS :* Le lecteur/terminal clignote ainsi cinq fois en jaune et émet un bip sonore cinq fois à plusieurs reprises, espacé d'environ trois secondes. *Interfaces E/S HBUS :* Le voyant d'état de la carte reste allumé jusqu'à ce que le remplacement soit annulé. Cela permet à un installateur d'identifier la carte dans une armoire. **Arrêter l'identification du périphérique :** Lecteurs HBUS, terminaux HBUS, terminaux HBUS Alarms Only et lecteurs de cartes de contact HBUS : Le lecteur/terminal cesse ainsi de s'identifier. *Interfaces E/S HBUS :* Cela fait cesser l'identification de la commission.

Si vous l'êtes remplacement...	alors...
	CONTRÔLEURS UNIQUEMENT **Désactiver la communication :** Ceci empêche un serveur de communiquer avec le contrôleur et reste ainsi jusqu'à ce que vous "Activer la communication". Il empêche le serveur de tenter de se connecter au contrôleur, ou le serveur d'accepter un contact de la part du contrôleur. **Activer la communication :** Cela permet à un serveur de commencer à communiquer avec le contrôleur. **Activer les connexions WWW :** Il s'agit d'un remplacement temporel qui permet l'accès Web au contrôleur jusqu'à l'expiration donnée, indépendamment des paramètres du commutateur DIP 1. **Annuler le remplacement WWW :** Ceci expire une "Activer les connexions WWW" override, et l'accès web une fois de plus sera contrôlé par les paramètres de commutateur DIP 1. **Revalider le certificat :** Cela indique au serveur d'oublier l'identité stockée précédente du contrôleur et de réinitialiser le contrôleur la prochaine fois qu'il établit une connexion au serveur. Après avoir effectué le remplace-ment, le message d'état du contrôleur affiche "Contrôleur utilisant le chiffrement hérité", jusqu'à ce que le contrôleur se reconnecte. Ce message d'état reste toutefois actif si le contrôleur exécute un microprogramme antérieur à v7.80. **Envoyer adresse du serveur :** Si un contrôleur ne peut pas se connecter au serveur (et est donc "hors ligne"), ce remplacement permet au contrôleur d'établir une communication avec le serveur. Il établira une connexion au contrôleur et utilisera ensuite cette connexion pour envoyer l'adresse du serveur. En cas de réussite, le contrôleur se connectera au serveur et reviendra "en ligne". **Remarque :** Ce contournement ne sera pas visible si le message d'état du contrôleur affiche "Contrôleur utilisant le chiffrement hérité", sur la page de propriétés **État et Contournement** du contrôleur. ***CONTRÔLEURS UNIQUEMENT (lorsqu'il est configuré pour 'Activer la liaison Ethernet secondaire')*** **Utiliser Ethernet secondaire :** Il s'agit d'un remplacement temporel qui demande au contrôleur de basculer la liaison Ethernet qu'il utilise. **Annuler l'utilisation de l'Ethernet secondaire :** Ceci expire une substitution "Utiliser l'Ethernet secondaire" et revient à la liaison Ethernet originale qu'il utilise.

Si vous l'êtes remplacement...	alors...
un ascenseur HLI	**Shunt :** Cela arrête la communication avec le système d'ascenseur et reste ainsi jusqu'à ce que vous "Unshunt". Une fois que le système d'ascenseur a détecté que la communication a été perdue, il appliquera le mode d'accès par défaut. Normalement, cela signifie que l'accès à n'importe quel étage à partir d'une voiture d'ascenseur est autorisé. (Certains systèmes d'ascenseurs, cependant, permettront d'appliquer un mode d'accès configurable en cas de perte de communication.) **Déshunt :** Ceci commence le système d'ascenseur. L'accès aux planchers des ascenseurs sera maintenant contrôlé par le Centre de commandement.
un groupe Interlock	**Désactiver le groupe :** Cela désactive la fonctionnalité de verrouillage en ignorant toutes les règles de verrouillage. Les portes du groupe fonctionnent comme si elles n'appartenaient pas à un groupe de verrouillage. **Activer le groupe :** Ceci applique les règles d'imbrication définies pour le groupe. **Remarque :** Les éléments autres que les portes d'un groupe Interlock, donnent un statut trompeur (c'est-à-dire un message d'état empêchant XXX d'ouvrir uniquement lorsque XXX est une porte).
un bloc logique	**Activé :** Cela désactive les règles et les options de minutage du bloc logique, et définit "on" sa sortie. **Désactivé :** Cela désactive les règles et les options de minutage du bloc logique, et désactive sa sortie. **Réinitialiser la logique :** Cela restaure la logique à un état connu et annule les longs délais ou les temps d'impulsion si ceux-ci sont indésirables.

Remarque : Vous ne pouvez pas spécifier la durée de la substitution sur les entrées, les éléments matériels et les HLI de l'ascenseur (c'est-à-dire jusqu'à la prochaine modification de la planification ou pour une durée spécifiée).

4. Cliquez sur le bouton **Remplacer maintenant (Override Now)**.
   À partir de cet écran, vous pouvez voir le changement d'état à la suite de la substitution.
5. Cliquez sur le bouton **OK**.

Résultat

L'élément est remplacé pendant la durée spécifiée.

Tant que le remplacement "Shunt" est en place, le système ne surveille pas l'élément, et l'élément ne génère pas d'alertes ou ne provoque pas d'événements.

Ouvrir une demande de porte

Introduction

Cette procédure permet à un opérateur disposant du privilège "Override - Open Door" d'ouvrir une porte spécifique pendant quelques secondes pour permettre à une personne de passer.

Procédure

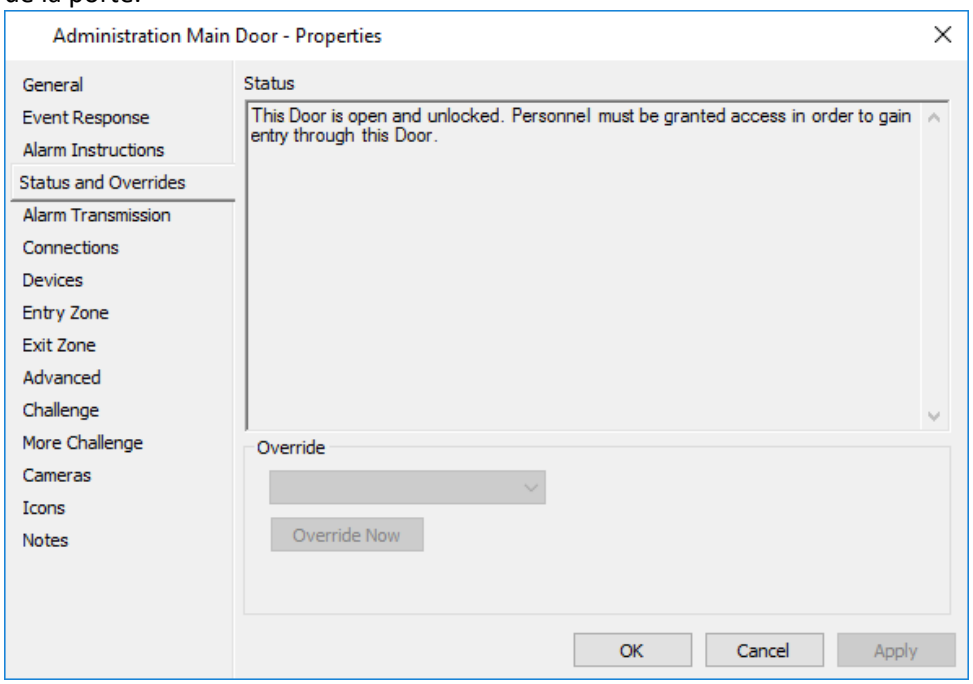
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Portes**.
   La fenêtre Liste principale de **porte** s'ouvre (en mode grille).
2. **Faites un clic droit** sur la porte que vous souhaitez ouvrir et cliquez sur **Ouvrir** la **porte** dans le menu déroulant.

Résultat

La porte est brièvement déverrouillée (pour une durée définie par le système), et la personne peut ouvrir la porte et passer à travers.

Indication

Sinon, au lieu de cliquer sur Ouvrir la porte dans le menu déroulant, vous pouvez "ouvrir la porte" à partir de l'onglet **Statut et remplacement de** la fenêtre Propriétés de la porte.



Cliquez dans le champ Override et sélectionnez "Open Door", puis cliquez sur le **bouton** Override **Now** pour ouvrir la porte.
À partir de cet écran, vous pouvez voir le changement d'état à la suite de la substitution.
Remarque : Vous ne pouvez pas spécifier qu'un remplacement pour ouvrir une porte doit être mis en oeuvre jusqu'à ce que la prochaine planification change ou pour une période spécifiée.

Configuration des contournement locaux sur les lecteurs de carte

Introduction

Un remplacement local sur un lecteur permet aux titulaires de carte d'armer ou de désarmer la zone d'alarme associée à la zone d'accès d'un lecteur. Un remplacement local peut également être utilisé pour changer le mode d'accès (par exemple, de Sécurisé à Libre) pour la zone d'accès associée au lecteur.
Remarque : Les titulaires de carte doivent disposer des privilèges appropriés pour effectuer des contournement locaux auprès des lecteurs. Reportez-vous aux procédures ci-dessous pour plus de détails sur la configuration des privilèges appropriés pour les contournement locaux sur les lecteurs.
Il existe trois méthodes d'exécution de contournement locaux, comme suit :

1. Pour un terminal Gallagher T20 connecté en tant que terminal HBUS, appuyez sur le bouton **Arm** et connectez-vous au terminal. Les informations d'identification de connexion requises sont configurées dans l'onglet "Écran d'accueil" de l'élément HBUS Terminal.

   Pour un terminal Gallagher T20 connecté en tant que lecteur Cardax IV, appuyez sur le **bouton Bras et effectuez la ou les actions nécessaires pour accéder à** la zone (présenter votre carte par exemple) à la borne.

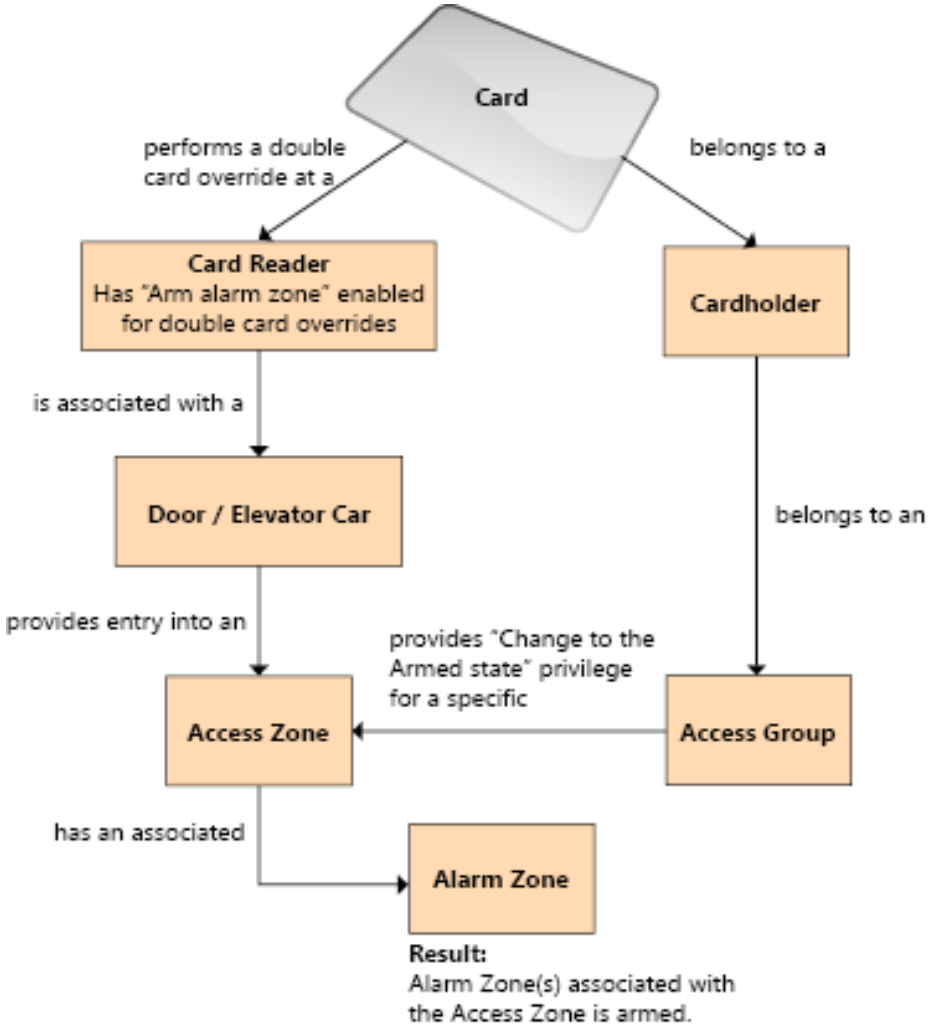
2. Pour un terminal Gallagher T20 connecté en tant que terminal HBUS, appuyez sur le bouton **Mode** et connectez-vous au terminal. Les informations d'identification de connexion requises sont configurées dans l'onglet "Écran d'accueil" de l'élément HBUS Terminal. L'écran Mode d'accès s'affiche sur le terminal. Sélectionnez le mode d'accès dont vous avez besoin.

   Pour un terminal Gallagher T20 connecté en tant que lecteur Cardax IV, appuyez sur le bouton **Mode**, puis effectuez la ou les actions nécessaires pour accéder à la zone (par exemple, présenter votre carte) du terminal. Appuyez sur le numéro (1, 2 ou 3) représentant le mode d'accès requis (mode 1, mode 2 ou planifié).

   Remarque : Vous ne pouvez pas effectuer de remplacement de zone d'accès sur un lecteur à moins que la zone d'alarme associée à la zone d'accès soit désactivée.

3. Insigne votre carte deux fois, (connu sous le nom de "double-carte override"), de n'importe quel lecteur. Selon ce qui a été configuré dans le Centre de commandes, cela remplace le mode d'une zone d'accès, alternant entre le mode 2 et planifié, ou il arme la zone d'alarme associée avec le lecteur.

   Le diagramme suivant décrit la configuration d'un remplacement de double carte pour armer la zone d'alarme associée à un lecteur.



Lecteurs dans les ascenseurs

Si un lecteur a été installé dans un ascenseur et qu'un détenteur de carte effectue une substitution au niveau du lecteur, la substitution est tentée sur toutes les zones d'accès ou zones d'alarme à tous les niveaux où le détenteur de carte a le privilège d'effectuer des contournement.

Par exemple:
Si un remplacement de la zone d'alarme est effectué au lecteur d'un ascenseur de 10 niveaux, et que le détenteur de la carte a seulement le privilège "Changement à l'état armé" à six des niveaux, alors seules les zones d'alarme sur ces six niveaux tenteront de s'armer. Selon la configuration, pour les quatre niveaux que le détenteur de la carte n'avait pas le privilège d'armer la zone d'alarme, un événement "Accès prioritaire refusé" va se produire. Cela se traduit également par une sonorité Refusé d'accès au lecteur.

Remarque : Si un terminal HBUS est assigné en tant que lecteur pour une voiture d'ascenseur, un titulaire de carte ne peut pas effectuer un remplacement en utilisant les touches de fonction (bras et mode) au terminal. Cependant, les doubles contournement de cartes peuvent toujours être effectués, bien que non recommandé.

Important:

- Cette configuration n'est pas recommandée, car des contournement doivent être effectués sur les lecteurs individuels dans chaque accès ou zone d'alarme.
- Bien que les doubles contournement de cartes puissent être effectués sur les lecteurs de voitures d'ascenseur, il n'est pas recommandé en raison du risque de remplacement accidentel de zones d'alarme multiples ou de zones d'accès.

Remplacement de la zone d'alarme sur un lecteur

Ce tableau résume l'effet de la substitution d'une zone d'alarme à un lecteur local sur une porte et les privilèges requis. Lorsque le remplacement est effectué à un lecteur de voiture d'ascenseur, les zones d'alarme à n'importe quel niveau sont armées ou désarmées comme indiqué, à condition que le titulaire de la carte ait le privilège requis pour ce niveau.

Action	Zone d'alarme (avant)	Zone d'alarme (après)	Privilèges requis
Double badge	Désarmé	Armé	Privilège "Changement à l'Etat Armé" pour la zone d'Alarme. Lecteur réglé sur "Zone d'alarme de bras" pour les contournement de double carte.
Double badge	Armé	Armé	Privilège "Changement d'état désarmé" pour la zone d'alarme. Privilège "Changement à l'Etat Armé" pour la zone d'Alarme. Lecteur réglé sur "Zone d'alarme de bras" pour les contournement de double carte.
Insigne de carte unique	Armé	Désarmé	Privilège "Changement d'état désarmé" pour la zone d'alarme.
Méthode de bras et d'accès (Cardax IV T20 Terminal) ou bras et connexion (HBUS Terminal)	Désarmé	Armé	Privilège "Changement à l'Etat Armé" pour la zone d'Alarme.

Accès Zone à un lecteur

Ce tableau résume l'effet de la substitution d'une zone d'accès à un lecteur local sur une porte et les privilèges requis. Lorsque le remplacement est effectué à un lecteur de voiture d'ascenseur, l'état de la zone d'accès pour n'importe quel niveau est modifié comme indiqué, à condition que le titulaire de la carte ait le privilège requis pour ce niveau.

Remarque : Vous ne pouvez pas effectuer de remplacement de zone d'accès sur un lecteur à moins que la zone d'alarme associée à la zone d'accès soit désactivée.

Action	Zone d'accès (avant)	Zone d'accès (après)	Privilèges requis
Double badge	Planifié	Mode 2	Privilège "Verrouiller et déverrouiller les zones d'accès" pour la zone d'accès. Lecteur réglé sur "Remplacer la zone d'accès" pour les contournement de cartes doubles.
Double badge	Mode 2	Planifié	Privilège "Verrouiller et déverrouiller les zones d'accès" pour la zone d'accès. Lecteur réglé sur "Remplacer la zone d'accès" pour les contournement de cartes doubles.
Mode et méthode d'accès (Cardax IV T20 Terminal) ou Mode et connexion (HBUS Terminal)	Tout	Mode 1, Mode 2 ou État planifié, selon le cas sélectionné par le détenteur de la carte effectuant le remplacement.	Privilège "Verrouiller et déverrouiller les zones d'accès"pour la zone d'accès.

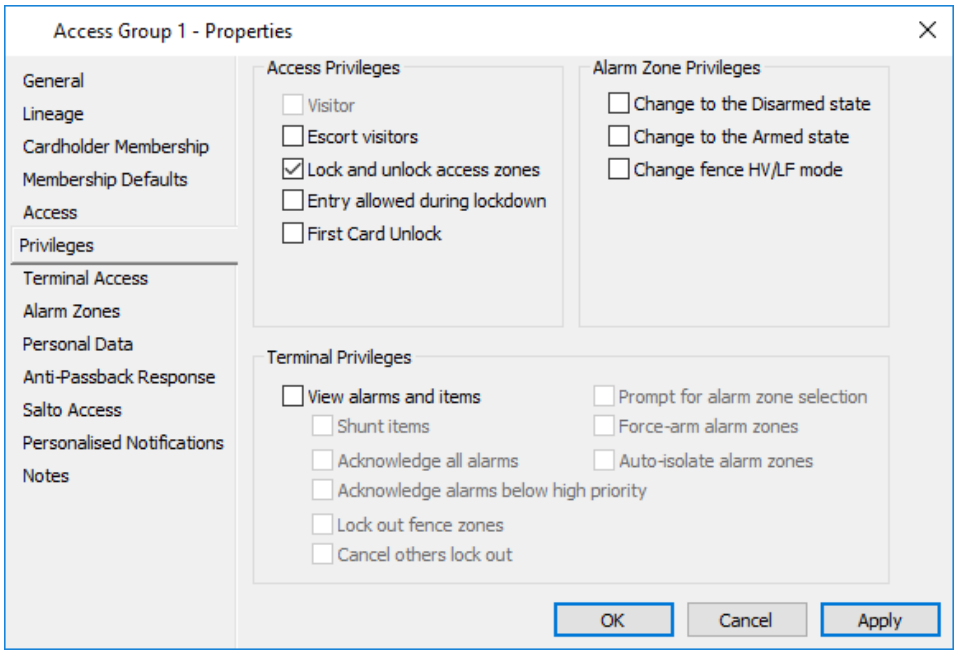
Procédure

Cette procédure a été divisée en quatre :
- Configuration d'une substitution de zone d'accès
- Configuration d'une substitution de zone d'alarme au lecteur
- Configuration du délai d'expiration du badge de carte
- Configuration des contournement de double carte au niveau d'un lecteur

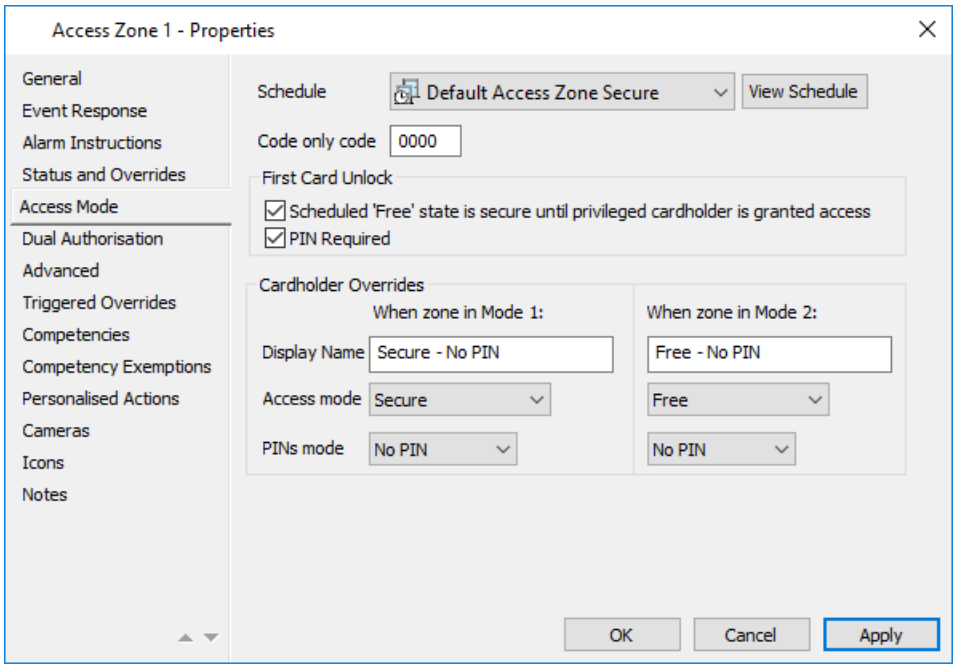
Suivez les procédures qui conviennent à la configuration dont vous avez besoin.

Configuration d'une substitution de zone d'accès

1. Cliquez sur **Gérer** dans la barre de menus, puis sur **Groupes d'accès**.
   La fenêtre Liste principale **du groupe Access** s'ouvre (en mode arborescence).
2. Ouvrez le ou les groupes d'accès pertinents pour que les personnes bénéficient de ce privilège.
3. Cliquez sur l'onglet **Privilèges**.
4. Cochez la **case à cocher Verrouiller et déverrouiller les zones d'accès**.
   Ce privilège permet aux membres de remplacer l'état d'une zone d'accès à partir d'un lecteur.
   Les zones d'accès auxquelles le privilège s'applique sont répertoriées sous l'onglet **Accès** du groupe d'accès.



5. Cliquez sur le bouton **OK**.
6. Cliquez sur **Configurer** dans la barre de menus, puis sur **Zones d'accès**.
   La fenêtre Liste principale de **la zone d'accès** s'ouvre (en mode arborescence).
7. Ouvrez la zone d'accès associée au lecteur à partir de laquelle ces contournement locaux seront effectués.
8. Cliquez sur l'onglet **Mode d'accès**.



9. La section "Contournement des titulaires de carte" de cet écran détermine ce qui se passe lorsqu'un titulaire de carte remplace cette zone d'accès.
   Sinon, le mode est déterminé par le programme.
   Lorsque vous effectuez des contournement, vous pouvez sélectionner l'état (Mode 1, Mode 2 ou Planifié) dans lequel la zone d'accès est remplacée. Lors de

l'exécution de la double carte remplace les changements d'état de la zone d'accès entre le mode 2 et l'état planifié avec chaque remplacement successif qui est appliqué.

Le nom complet est affiché sur le terminal HBUS uniquement. Le nom complet vous permet de décrire le mode d'accès (par exemple, Après les heures). Si vous utilisez un terminal HBUS, entrez le nom d'affichage pour chaque mode.

Spécifiez les modes d'accès requis pour les modes 1 et 2.

10. Cliquez sur le bouton **OK**.
11. Pour configurer le temps maximal autorisé entre les badges de carte ou entre le fait d'appuyer sur une touche de fonction et le badge de votre carte, reportez-vous à *Configuration du délai d'expiration du badge de carte (plus loin dans cette section)*.
12. Avez-vous l'intention d'utiliser des contournement de cartes doubles ?
    - Si **ce n'est pas le cas**, cette procédure est terminée.
    - Si **oui**, allez à Configuration des *contournement de cartes doubles sur un lecteur* (plus loin dans cette section).

Résultat

Les titulaires de carte appartenant à ce groupe d'accès peuvent désormais effectuer des contournement des zones d'accès attribuées à ce groupe d'accès à partir d'un lecteur local.

Indication

Si la porte a été configurée avec une zone d'accès de sortie, le remplacement est effectué avec succès sur la zone d'accès d'entrée, mais la porte reste verrouillée, si le mode d'accès de la zone d'accès de sortie est défini sur sécurisé. Pour vous assurer que l'état de verrouillage de la porte suit le mode d'accès de la zone d'entrée, cochez la **case État de** verrouillage de porte **après la zone d'entrée seulement** sur l'onglet avancé des propriétés de la porte.

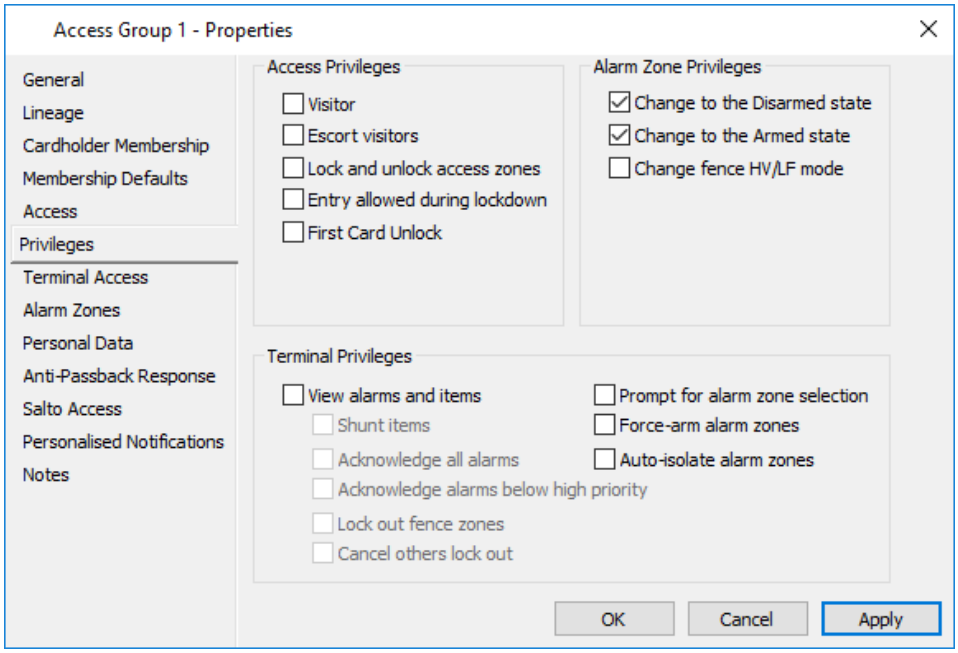
Configuration d'un remplacement de zone d'alarme

1. Cliquez sur **Gérer** dans la barre de menus, puis sur Groupes d'accès.
   La fenêtre **Liste** principale **du groupe Access** s'ouvre (en arborescence).
2. Ouvrez le(s) groupe(s) d'accès approprié(s) pour que les titulaires de carte aient ce privilège. Ce groupe d'accès doit contenir la zone d'accès associée à la zone d'alarme pour laquelle vous souhaitez accorder le privilège de remplacement.
3. Cliquez sur l'onglet **Privilèges**.

   Cochez la case **Remplacer par l'état Armé** si vous souhaitez fournir le privilège d'armer les zones d'alarme.
   Cochez la case **Remplacer par l'état Désarmé** si vous souhaitez fournir le privilège de désarmer les zones d'alarme.

   Le privilège s'applique aux zones d'alarme associées aux zones d'accès répertoriées dans l'onglet **Accès**. Il est également limité aux délais dans lesquels l'accès à la zone d'accès est autorisé, tel que spécifié dans l'annexe associée.

Remarque : Le privilège s'applique aux zones d'alarme répertoriées dans l'onglet Zones d'alarme de ce groupe d'accès, si vous effectuez la substitution sur un terminal.



4. Cliquez sur le bouton **OK**.
5. Pour configurer le délai d'expiration du badge de la carte lors de l'exécution du remplacement, reportez-vous à la section *Configuration du délai d'expiration du badge de la carte (plus loin dans* cette section). C'est le temps maximum autorisé entre les badges de carte, lors de l'exécution d'un double remplacement de carte, ou entre la pression d'une touche de fonction et le badgeage de votre carte.
6. Avez-vous l'intention d'utiliser des contournement de cartes doubles ?
   - Si **ce n'est pas le cas**, cette procédure est terminée.
   - Si **oui**, allez à *Configuration des contournement de cartes doubles dans un lecteur* (plus loin dans cette section).

Résultat

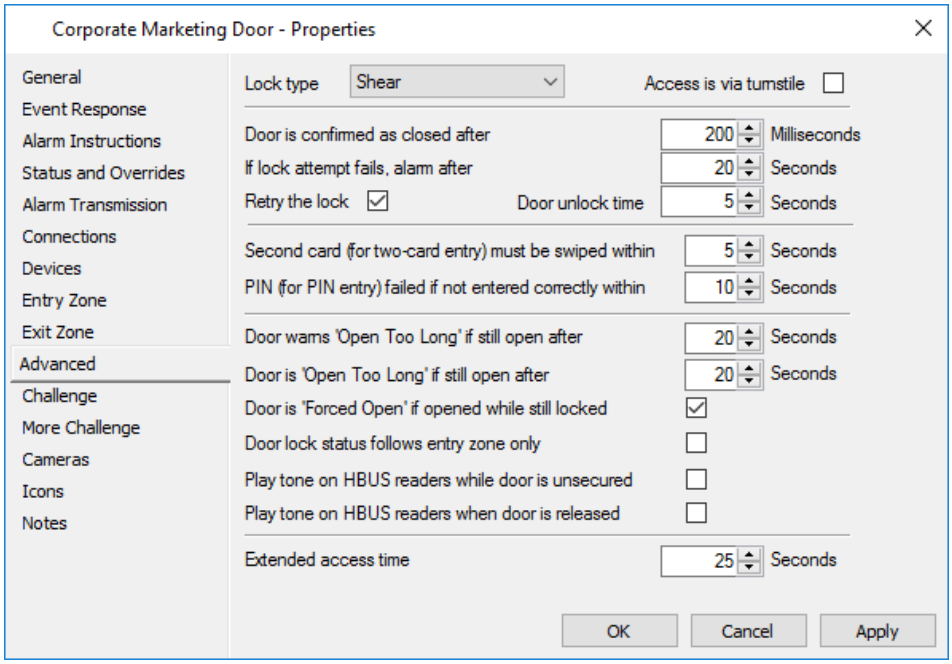
Les titulaires de carte appartenant à ce groupe d'accès peuvent désormais effectuer des contournement des zones d'alarme associées aux zones d'accès affectées à ce groupe d'accès à partir d'un lecteur local.

Configuration du délai d'expiration du badge de carte

Cette procédure configure le délai d'expiration du balayage de la carte sur un lecteur installé à une porte ou dans un ascenseur.
Remarque : Les délais d'expiration de la carte de remplacement du bras et du mode sur un terminal HBUS sont configurés sur l'**onglet** de l'**écran d'accueil** de l'élément FT du terminal HBUS.

1. Ouvrez la fenêtre principale de la **porte** (pour les portes) ou la fenêtre principale de la liste des ascenseurs (pour les ascenseurs).
2. Ouvrez la porte ou la voiture de l'ascenseur à laquelle le lecteur (c'est-à-dire le lecteur auquel le survol sera effectué) est connecté.
3. Cliquez sur l'onglet **Avancé (Advanced)**.
4. Configurez-vous le remplacement local pour une voiture porte ou ascenseur ?

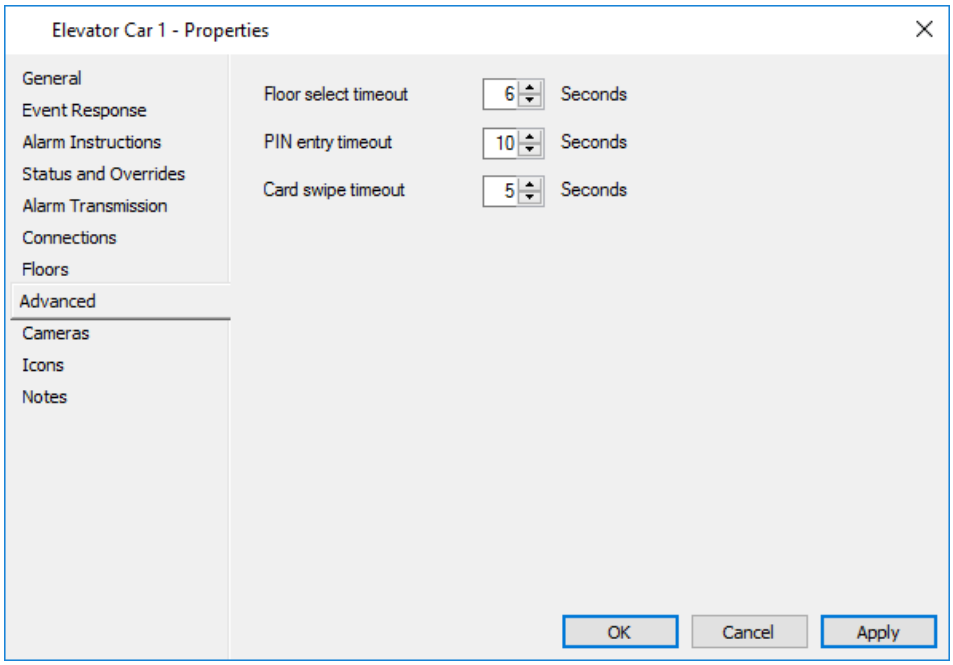
   - S'il est à une porte, reportez-vous à cette étape et sautez l'étape 5.
   - S'il est à une **voiture d'ascenseur, se référer** à l'étape 5.



   Entrez le nombre (en secondes) dans le champ Deuxième carte (pour l'entrée de deux cartes) **doit être glissé** pour le temps requis entre les deux cartes, ou entre appuyer sur une touche de fonction puis badger votre carte.

   Remarque : Cette modification modifie également le deuxième temps de balayage de la carte pour les visiteurs et le mode Double autorisation.

5. Entrez le nombre (en secondes) dans le champ Délai d'expiration du balayage de carte pour le temps requis entre les deux badges de carte, ou entre la pression d'une touche de fonction puis le marquage de votre carte.



6. Cliquez sur le bouton **OK**.

Résultat

Le délai d'expiration du badge de carte configuré sera appliqué à toutes les contournement effectués à la voiture de la porte ou de l'ascenseur.

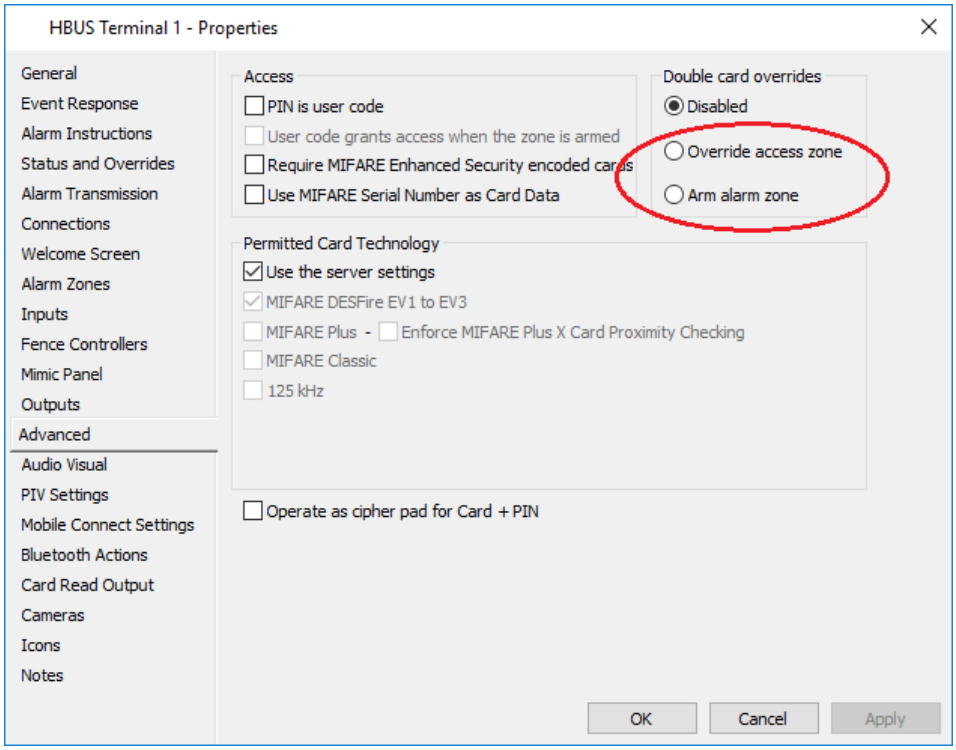
Configuration des contournement de cartes doubles sur un lecteur

1. Ouvrez la page Propriété pour le ou les lecteurs associés à la porte (c'est-à-dire comme spécifié dans les **onglets Zone d'entrée et Zone de** sortie des propriétés de la porte).

   Remarque : Si vous configurez un remplacement sur une voiture d'ascenseur, sélectionnez le lecteur associé à la voiture d'ascenseur (c'est-à-dire tel que spécifié dans l'onglet **Connexions** de la fenêtre Propriétés de la voiture d'ascenseur).

2. Cliquez sur l'onglet **Avancé (Advanced)**.

3. Cliquez sur le bouton d'option **Remplacer** la **zone d'accès** ou **Zone d'alarme** du bras, selon que vous souhaitez que le remplacement de la double carte remplace l'état de la zone d'accès ou que vous armez la zone d'alarme associée à la zone d'accès.



4. Cliquez sur le bouton **OK**.
   La fonctionnalité de remplacement de la double carte est activée.
5. Répétez cette procédure pour chaque voiture porte ou ascenseur associée à un lecteur à partir duquel vous souhaitez effectuer des contournement de carte double.

Résultat

Les titulaires de carte disposant du privilège de remplacement approprié peuvent désormais remplacer l'état de la zone d'accès ou de la zone d'alarme (selon la configuration choisie) sur ce lecteur en utilisant un remplacement par double carte.

Remarque : La fonction de remplacement de la double carte n'est pas prise en charge lorsqu'une zone d'accès est en mode autorisation double.

Chapitre 46 : Modes d'essai d'entrée d'alarme

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

(Reportez-vous à ***Privilèges de l'opérateur*** à la page 37-1 pour vérifier que vous disposez du niveau de privilège de l'opérateur correct pour l'activité que vous souhaitez effectuer.)

- ***Fonctionnalité fournie par les modes de test d'entrée d'alarme*** (page 46-2)
- ***Configuration des entrées pour les modes de test*** (page 46-5)
- ***Configuration des zones d'alarme pour les modes de test*** (page 46-7)
- ***Configuration des groupes d'accès pour les modes de test*** (page 46-9)
- ***Configuration des supports de cartes de test*** (page 46-11)
- ***Configuration des terminaux pour les modes de test*** (page 46-12)
- ***Configuration des notifications d'événement/d'alarme pour les modes de test*** (page 46-13)

Fonctionnalité fournie par les modes de test d'entrée d'alarme

La fonction Alarm Input Test Modes fournit les fonctionnalités suivantes :

Tests périodiques

Des tests périodiques sont effectués lorsqu'un membre du personnel autorisé à exécuter le mode d'essai périodique désarme le système à l'aide d'un terminal Gallagher. Le membre du personnel peut alors choisir d'entrer en mode test ou de désarmer comme d'habitude.

Il y a un délai configurable de un à trente jours pour lequel le test est optionnel. Après le temps configurable, le test n'est plus facultatif.

Le fonctionnaire doit ensuite vérifier que toutes les entrées configurées pour les tests fonctionnent correctement. Ils le font en activant chaque entrée.

À tout moment en mode test, le membre du personnel peut terminer le test manuellement à l'aide du terminal. Dans ce cas, un e-mail est envoyé au responsable pour l'informer que le test a été abandonné.

Le test doit être terminé dans un délai configurable. Le temps restant s'affiche comme un compte à rebours sur le terminal. Un avertissement sonore retentit à une minute de l'arrivée et le membre du personnel a l'occasion de prolonger le temps d'essai.

Si toutes les entrées sont activées avec succès avant le délai d'expiration, le terminal fournit une indication que toutes les entrées ont été testées avec succès. Une fois le test terminé, le système se désarme et un rapport est envoyé à la société de surveillance des alarmes et un e-mail est envoyé au responsable.

Si une ou plusieurs entrées n'ont pas pu être activées avant l'expiration du délai d'attente du test, le test est terminé et le système est désarmé. Le terminal liste toutes les entrées qui ont échoué le test, un rapport est envoyé à la société de surveillance des alarmes et un e-mail est envoyé au gestionnaire pour chaque entrée qui n'a pas réussi à s'activer pendant le test.

Test manuel

Les tests manuels permettent de tester les entrées sans modifier l'état de la zone d'alarme.

Un membre du personnel ou un technicien sera en mesure de mettre des zones du système en mode Test pendant les essais ; Le terminal indiquera si l'entrée fonctionne correctement et aucune alarme ne sera déclenchée pendant ce temps.

Test de masque

Le test de masque déclenche une alarme pour les entrées qui n'ont pas été activées dans un délai spécifié. L'objectif de cet essai est d'identifier les dispositifs qui ne fonctionnent pas (par exemple, les détecteurs de porte ou les détecteurs PIR).

Lorsqu'une entrée configurée n'a pas été activée au moins une fois au cours de la période de déclenchement d'une alarme, un message est envoyé à la société de surveillance des alarmes et un e-mail est envoyé au gestionnaire.

Essais de détection sismique

Les appareils de vibrations et les détecteurs sismiques peuvent être utilisés pour détecter les vibrations et/ou les attaques possibles (par exemple, forage ou similaire dans une chambre forte). Le contrôleur déclenchera les dispositifs de vibration qui déclencheront ensuite les détecteurs sismiques. Un test raté est un test où le contrôleur déclenche les dispositifs de vibration et où les détecteurs sismiques ne parviennent pas à le détecter. Tout échec des tests déclenchera une alarme, sera signalé à la société de surveillance des alarmes et envoyé par courriel au gestionnaire.

Les alarmes provenant des détecteurs sismiques ne seront pas déclenchées pendant les essais.

Désarmement restreint

Il est possible de configurer des groupes de membres du personnel dans les zones d'alarme qu'ils sont autorisés à désarmer et les heures auxquelles ils peuvent les désarmer (par exemple, les nettoyeurs).

Désarmement temporisé

Il est possible de configurer des groupes de membres du personnel en fonction de la période pendant laquelle ils sont autorisés à désarmer les zones d'alarme.

Armement et désarmement à distance

Il est possible que le système soit armé ou désarmé à distance par la société de surveillance des alarmes.

Traitement automatique des alarmes

Cette fonction permet au Centre de commande de traiter automatiquement toutes les alarmes qui sont inactives et accusées. Ce service peut être activé ou désactivé, au besoin. (Par défaut, le service est désactivé.)

Alarmes multiples

Il est possible pour une entrée d'envoyer une alarme à la société de surveillance d'alarme à chaque transition. Lorsque l'entrée est à nouveau scellée, un événement de restauration est envoyé.

Alternativement, il est possible de verrouiller les entrées d'alarme qui sont envoyées à la société de surveillance des alarmes. Cela signifie qu'une seule alarme sera envoyée à l'entreprise de surveillance des alarmes par entrée et que l'événement de restauration ne sera pas envoyé jusqu’à ce que l'alarme soit reconnue.

Configuration des entrées pour les modes de test

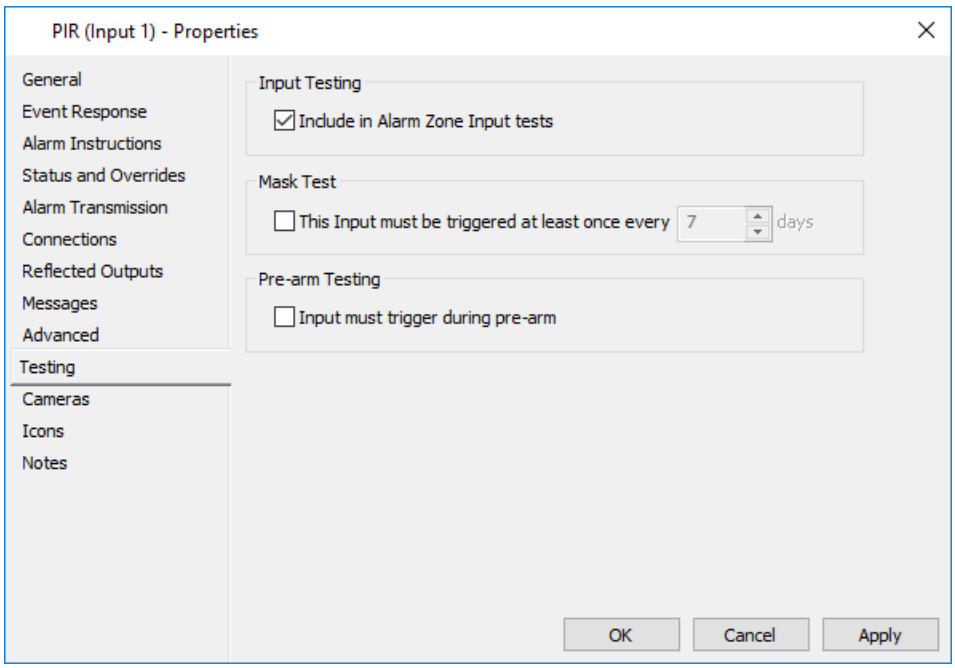
Introduction

Cette procédure décrit comment configurer chaque entrée nécessitant un test.

Remarque : L'état normal de toutes les entrées doit être "fermé". Si une entrée est "ouverte", vous devez inverser l'état de l'entrée en cochant la case Entrée inversée sur la page de propriétés avancées de l'entrée.

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'entrée appropriée et sélectionnez **Propriétés**.
3. Cliquez sur l'onglet **Réponse aux événements**.
4. Si l'entrée 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'entrée change d'état.
5. Affectez une zone d'alarme principale pour tous les événements de la liste déroulante.
6. Cliquez sur l'onglet **Test (Test)**.



7. Si l'entrée nécessite des tests périodiques ou manuels, cochez la **case Inclure dans les tests d'entrée de zone d'alarme**.
   Les données seront incluses dans tous les tests périodiques et manuels.

8. Si l'entrée 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'entrée doit être activée.
   (Valeur par défaut = 7 jours. Configurable de 1 à 30 jours.)
9. Si l'entrée est un détecteur sismique, cochez la case **Entrée doit se déclencher pendant le pré-bras**.
10. Cliquez sur le **bouton** OK pour quitter et enregistrer vos modifications.
11. Répétez cette procédure pour chaque entrée nécessitant un test.

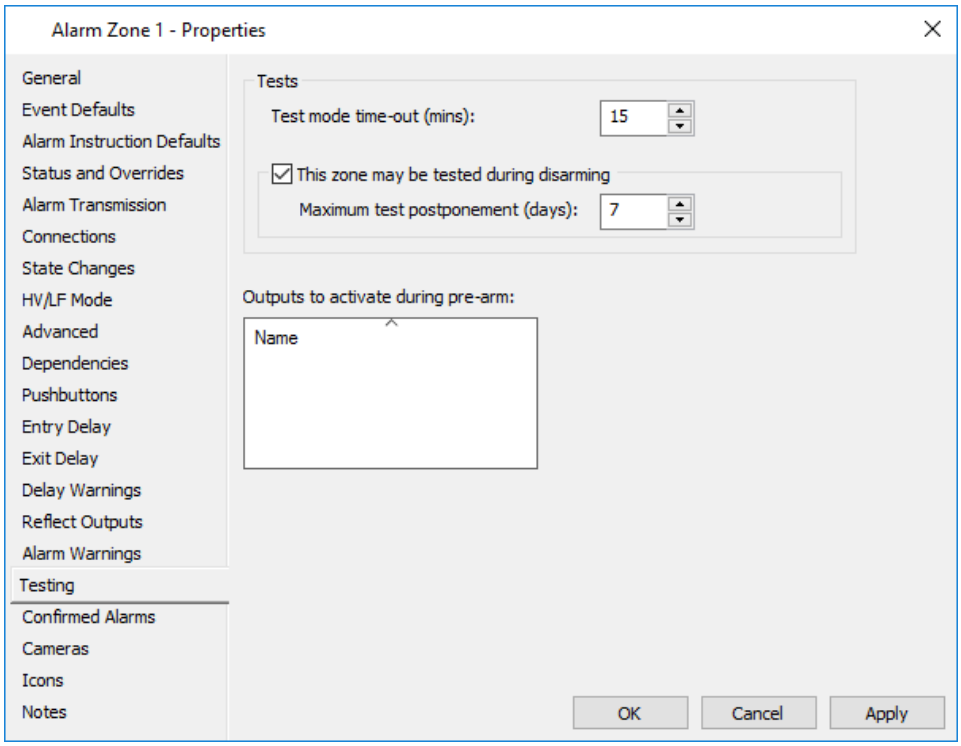
Configuration des zones d'alarme pour les modes de test

Introduction

Cette procédure décrit la configuration de chaque zone d'alarme nécessitant un test.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis **Alarme Zone**.
   La fenêtre **Alarm Zone** List s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** sur la zone d'alarme appropriée et sélectionnez **Propriétés**.
3. Cliquez sur l'onglet **Test (Test)**.



4. Dans le champ **Délai d'expiration du mode Test**, entrez le nombre de minutes nécessaires pour terminer le test.
   (Par défaut = 15 minutes. Configurable de 1 à 60 minutes.)

   Dans l'exemple ci-dessus, le test expire après 15 minutes.

   Le temps restant sera affiché comme un compte à rebours sur le terminal. Un avertissement sonore retentira dans une minute et le fonctionnaire aura l'occasion de prolonger le temps des essais.

   Lorsque le test est étendu, le temps nécessaire pour terminer le test revient à la période d'origine configurée. Le test peut être étendu plusieurs fois.
5. Cochez la case **Cette zone peut être testée lors du désarmement**.

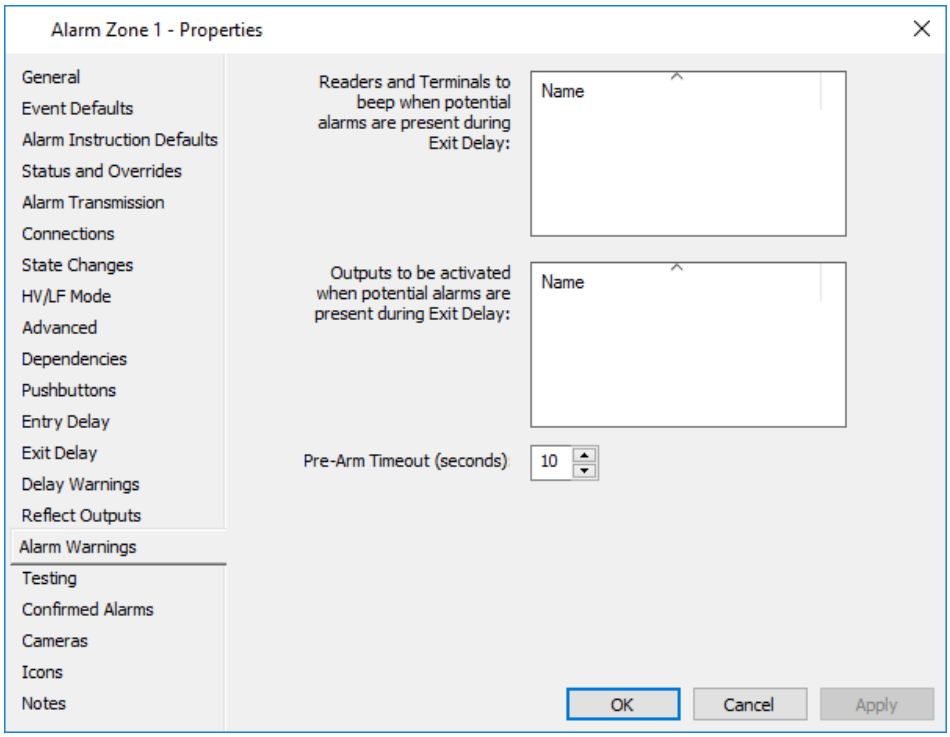
6. Dans le champ Retard maximal, entrez le nombre maximal de jours qui peuvent s'écouler avant qu'un test obligatoire soit requis.
   (Valeur par défaut = 7 jours. Configurable de 1 à 30 jours.)

   Dans l'exemple ci-dessus, après 7 jours, le test n'est plus facultatif.

7. La zone d'alarme contient-elle des dispositifs de vibration ?
   Si **oui**, passez à l'étape 8.
   Si **non**, passez à l'étape 11.

8. Glisser-déposer Faites glisser et déposez les dispositifs (sorties) dont vous avez besoin pour se déclencher pendant la période de délai d'expiration du délais dans la grille.
   Remarque : Ces sorties doivent être réglées au déclenchement.

9. Cliquez sur l'onglet **Avertissements de l'alarme (Alarm Warnings)**.



10. Dans le champ Délai d'expiration, entrez une période appropriée pour laquelle les contrôleurs doivent ignorer les alarmes (c'est-à-dire 0-60 secondes).
    Remarque : Le délai d'attente avant l'armement devra laisser suffisamment de temps pour que les dispositifs de vibration puissent se régler avant que les alarmes ne soient déclenchées. Une valeur de délai d'expiration avant le bras d'environ 10 secondes est suggérée.

11. Cliquez sur le **bouton** OK pour quitter et enregistrer vos modifications.

12. Répétez cette procédure pour chaque zone d'alarme qui nécessite un test.

Configuration des groupes d'accès pour les modes de test

Introduction

Cette procédure explique comment configurer les groupes d'accès dont vous avez besoin pour le test.

Il est possible de configurer des groupes de membres du personnel avec les zones d'alarme qu'ils sont autorisés à désarmer et les moments où ils peuvent les désarmer.

Il est également possible de configurer des groupes de membres du personnel avec la période pendant laquelle ils sont autorisés à désarmer les zones d'alarme.

Procédure

1. Assurez-vous que les informations suivantes ont déjà été configurées :

   Divisions
   Consultez la section ***Configuration de la division du système*** (page 9-3).

   Titulaires
   Reportez-vous à la section ***Ajouter un nouveau titulaire de carte*** (page 32-2).

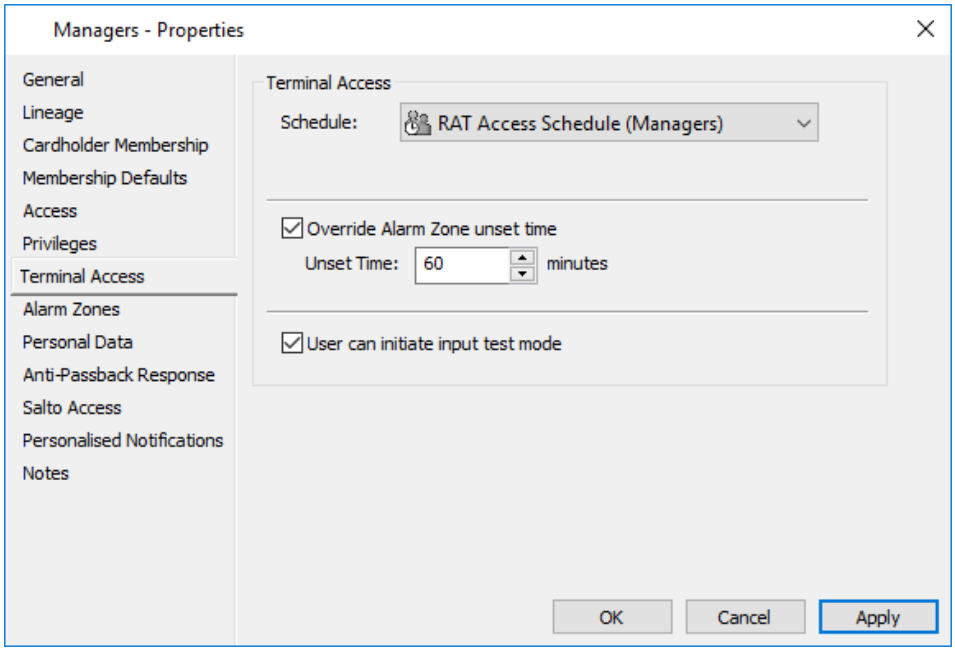
   Horaires
   Accès Horaires = relatifs aux titulaires
   Zone d'accès Horaires = se rapportant à la façon dont les portes de la zone se comportent Voir les ***Horaires*** (page 12-1).

   Zones d'accès
   Inclut une planification de zone d'accès liée
   Reportez-vous à la section ***Ajout d'une nouvelle zone d'accès*** (page 10-3).

   Champs de données personnelles
   Reportez-vous à la section ***Création d'un nouveau champ de données personnelles*** (page 33-2).

2. Cliquez sur **Gérer** dans la barre de menus, puis sur **Groupes d'accès**.
   La fenêtre Liste principale **du groupe Access** s'ouvre (en mode arborescence).
3. **Cliquez avec le bouton droit** sur le groupe d'accès approprié et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Appartenance au titulaire de la carte**.
5. Cliquez sur **Gérer** dans la barre de menus, puis sur **Titulaires de carte**.
   La fenêtre Liste principale des titulaires de carte s'ouvre.
6. Sélectionnez les titulaires de carte qui sont tenus d'effectuer des tests de saisie. Faites glisser et déposez-les dans l'onglet **Appartenance au titulaire de carte**.
7. Fermez la fenêtre Liste principale **des titulaires de carte**.
8. Cliquez sur l'onglet **Privilèges**.
9. Cochez **la case État Désarmé**.

10. Si les titulaires de carte doivent armer des zones d'alarme associées à une zone d'accès associée à ce groupe d'accès, cochez la case **Modifier l'état armé**.
11. Si les détenteurs de carte doivent sélectionner une zone d'alarme pour tester le terminal, cochez la **case Demander la sélection de la zone d'alarme**.
12. Cliquez sur l'onglet **Terminal Access (Accès aux terminaux)**.



13. Sélectionnez le calendrier d'**accès des titulaires de carte** approprié pour ce groupe d'accès. Ce calendrier détermine quand le titulaire peut accéder au terminal.
14. Cochez la case **Remplacer** l'**heure de désactivation de la zone d'alarme** et entrez la période pendant laquelle les zones d'alarme doivent être désactivées. (Valeur par défaut = 60 minutes) Cette heure remplace l'heure d'annulation de la zone d'alarme pour toutes les zones d'alarme associées à ce groupe d'accès, lorsque cette option est désactivée du terminal uniquement.
    Remarque : Si l'heure de désactivation d'une zone d'alarme est supérieure à l'heure de désactivation de la substitution configurée, la zone d'alarme est réinitialisée à l'heure spécifiée par la substitution.
15. Cochez **la case User can start input test mode**.
    Les titulaires de carte appartenant à ce groupe d'accès pourront effectuer des tests d'entrée.
16. Cliquez sur l'onglet **Alarm Zones**.
17. Cliquez sur **Configurer** dans la barre de menus, puis sur **Zones d'alarme**.
    La fenêtre Alarm Zone s'ouvre.
18. Sélectionnez les zones d'alarme que les membres de ce groupe d'accès sont autorisés à tester.
    Faites-les glisser et déposez-les dans l'onglet **Zones d'alarme**.
19. Fermez la fenêtre **de** liste principale de la zone d'alarme.
20. Cliquez sur le **bouton** OK pour quitter et enregistrer vos modifications.

Configuration des titulaires de cartes pour les modes de test

Vous devrez configurer les titulaires de carte pour qu'ils se connectent au terminal, soit en utilisant un lecteur de carte séparé ou en utilisant un code d'utilisateur.

Pour plus d'informations sur la configuration d'un code utilisateur pour un titulaire de carte, reportez-vous à la section ***Configuration des codes utilisateur pour l'accès aux lecteurs de cartes avec claviers*** (page 32-25) pour la procédure.

Configuration des terminaux pour les modes de test

Vous devrez ajouter les zones d'alarme contenant les entrées de test aux bornes. Les titulaires de carte pourront alors effectuer des tests d'entrée pour ces zones en utilisant les terminaux.

Pour plus de détails sur l'association d'une zone d'alarme à un terminal HBUS, consultez ***Configuration d'un terminal HBUS*** (page 21-54).

Pour plus d'informations sur l'association d'une zone d'alarme à un terminal HBUS Alarms Only, reportez-vous à ***Configuration d'un terminal HBUS Alarms Only*** (page 21-70).

Configuration des notifications d'événement/d'alarme pour les modes de test

Vous devez configurer les notifications d'événement/d'alarme pour le gestionnaire. Le filtre de notification affecté au gestionnaire doit inclure les groupes d'événements suivants :

- Tester les événements
- Point non testé
- Entrée non activée

Pour savoir configurer les notifications d'événement/d'alarme, reportez-vous à ***Notifications*** (page 6-47) pour la procédure.