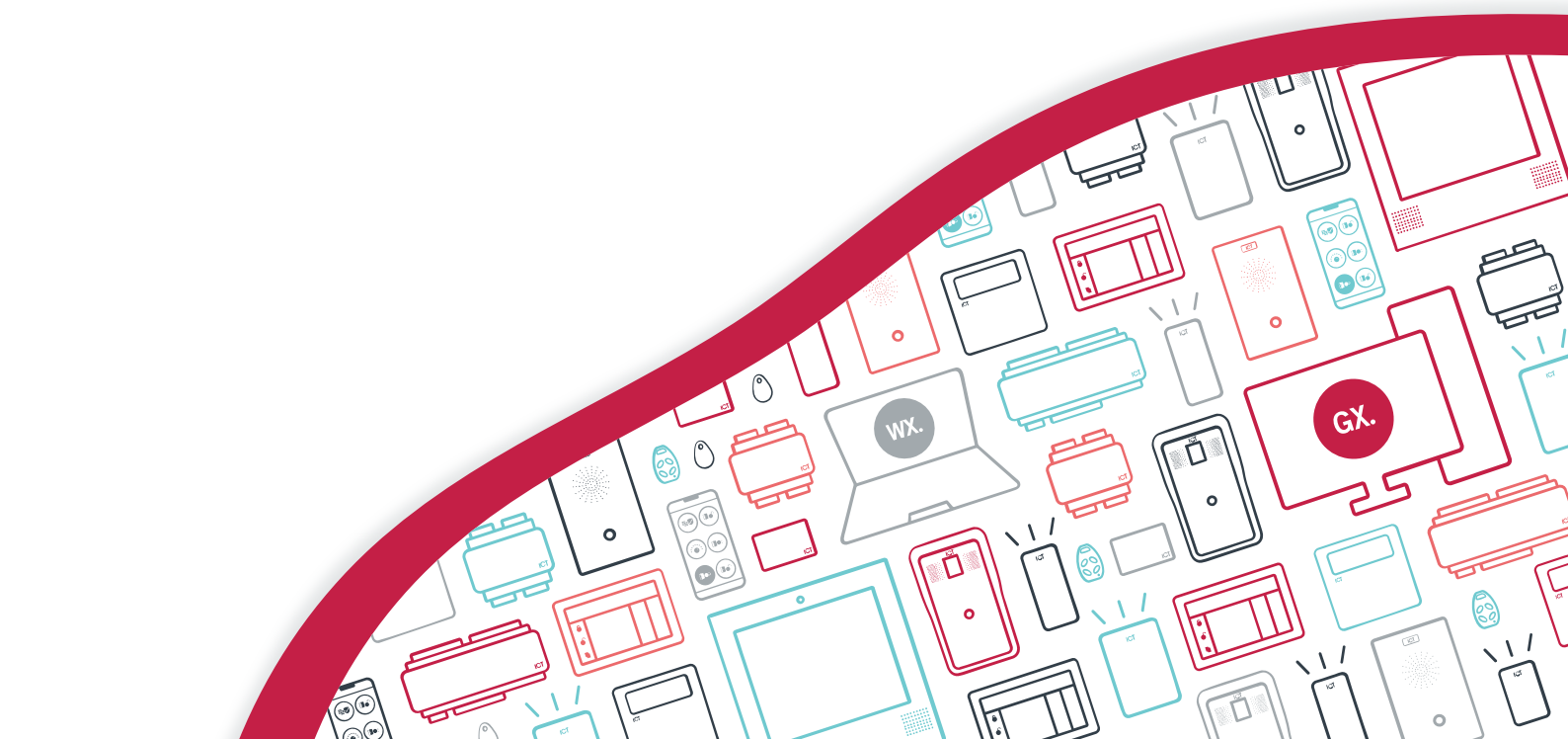
PRT-GX-SRVR

Système Protege GX

Manuel de référence de l'opérateur



Dernière publication en 01-juin-23 08:32.

Contenu

Référence de l'opérateur Protege GX

Bienvenue dans la référence de l'opérateur Protege GX, une documentation conçue pour vous donner les informations dont vous avez besoin lors de la programmation et de la maintenance de Protege GX. Ce manuel PDF constitue une référence complète pour le système Protege GX, et peut être imprimé ou consulté sur un PC ou une tablette. La documentation est également disponible sous forme de système d'aide au sein même de Protege GX.

Il existe plusieurs façons d'utiliser cette documentation :

- **Introduction à Protege GX** : Les deux premières sections fournissent des informations sur la façon de naviguer dans l'interface utilisateur Protege GX (consultez page suivante), ainsi que des conseils généraux de programmation et de dépannage (consultez la page 23).
- **Référence de la page de programmation** : La deuxième partie de la documentation comprend des informations de référence complètes pour chaque page du logiciel. Vous pouvez utiliser la table des matières (consultez la page 3) ou le volet **Signets** de votre visionneur de PDF pour naviguer dans la documentation, qui est organisée selon la même structure que le menu principal de Protege GX.

  Par exemple, si vous avez besoin de trouver de l'information à propos de l'onglet **Options** dans la programmation des portes, développez le menu Programmation et localisez Portes | Options.
- **Référence du champ de programmation** : Presque tous les champs du logiciel sont décrits dans cette documentation. Pour trouver rapidement des informations sur un champ particulier du logiciel, appuyer sur Contrôle + F et saisir le nom du champ dans la barre de recherche, puis appuyer sur Entrée.

  Par exemple, vous pouvez rechercher **Toujours vérifier horaire de déverrouillage** pour en apprendre davantage sur les fonctions de cette option.

Cette documentation est destinée aux opérateurs qui utiliseront et programmeront le logiciel. Pour obtenir des instructions sur l'installation du logiciel Protege GX, veuillez consulter le Manuel d'installation Protege GX distinct. Le Guide de l'utilisateur final Protege GX fournit une introduction aux fonctions clés pour les utilisateurs finaux tels que les gestionnaires de bâtiments, le personnel des RH et les gardes.

Veuillez tenir compte de l'environnement avant d'imprimer cette documentation.

L’interface utilisateur Protege GX

Cette section fournit un guide des sections et des caractéristiques de l’interface utilisateur Protege GX.

Le niveau de sécurité de votre opérateur détermine les fonctions qui vous sont accessibles lorsque vous êtes enregistré. L'accès à la visualisation et à la modification de certains types d'enregistrements peut avoir été restreint par l'administrateur de votre site.

Se connecter

1. Double-cliquez sur l'icône Protege GX sur votre bureau ou accédez au programme à partir de votre menu Démarrer de Windows :

   La fenêtre de connexion s'affiche.
2. Saisissez vos coordonnées telles que fournies par votre administrateur système ou votre intégrateur Protege GX :
   - **Nom d’utilisateur** : Votre nom d’utilisateur d’opérateur Protege GX.
   - **Mot de passe** : Votre mot de passe d’opérateur Protege GX.
   - **Langue** : Définit la langue de l’interface utilisateur.

     Les deux options de langue disponibles sont définies par votre installation.
   - **Serveur** : Saisissez le nom ou l’adresse IP du serveur Protege GX auquel vous vous connectez, ou sélectionnez un serveur précédemment utilisé dans la liste déroulante. Si vous vous connectez à un serveur sur la machine locale, ce champ peut être vide.

     Vous pouvez utiliser le bouton **Effacer** pour supprimer le serveur actuellement sélectionné dans la liste déroulante.
3. **Utiliser l’authentification Windows :** Si votre installation utilise l’intégration Répertoire actif, sélectionnez cette option pour vous connecter à l’aide de votre compte Windows.

   Si vous utilisez l’authentification Windows, vous n’avez pas besoin de saisir les détails de l’utilisateur. Dans le champ **Serveur**, saisir le nom de l’ordinateur ou l’adresse IP du serveur Protege GX. Si vous vous connectez au serveur depuis l’extérieur du domaine du réseau, vous devez saisir un nom de domaine complet qualifié.
4. Cliquer sur **Se connecter**.

Lorsque vous vous connectez pour la première fois, vous serez invité à ajouter un nouveau site et un nouveau contrôleur. Vous devez terminer ce processus avant de fermer l’application client, sinon les registres par défaut importants ne seront pas créés.

L’identifiant de connexion par défaut de l’opérateur est admin avec un mot de passe vide. Pour des raisons de sécurité, il est fortement recommandé de remplacer immédiatement le mot de passe administrateur par un mot de passe robuste.

Page d’accueil

La **Page d’accueil** est affichée lorsque vous vous connectez pour la première fois.

D’ici, vous pouvez :

- Afficher les **détails de l’opérateur** concernant l’opérateur actuellement connecté.
- Changez le **site actuel** que vous souhaitez visualiser (si vous avez plusieurs sites).
- Définir le **thème de l’affichage** (clair ou foncé) et la **couleur de l’affichage** pour l’opérateur.
- **Se déconnecter** pour fermer Protege GX et revenir à l’écran de connexion.
- Utilisez la fonction **Changer le mot de passe** pour changer votre mot de passe opérateur.

  Cette option n’est pas accessible lors de l’utilisation de l’authentification Windows.

Le menu principal en haut de l'écran permet d'accéder à toutes les fonctions disponibles pour travailler dans le système. Vous pouvez revenir à la page d'accueil à tout moment en visitant **Global | Accueil** dans le menu principal.

Résolutions d'écran prises en charge

L'interface utilisateur Protege GX prend en charge les résolutions d'écran standard suivantes :

- 1280 x 1024
- 1400 x 1050
- 1600 x 1200
- 1680 x 1050
- 1920 x 1080

La sélection d'autres résolutions d'écran peut produire des résultats d'affichage inattendus.

Modification du mot de passe de l'opérateur

1. Pour modifier votre mot de passe opérateur, cliquez sur le bouton **Modifier le mot de passe** sur la page d'accueil. Cela ouvre la fenêtre **Modifier le mot de passe**.
2. Saisissez le mot de passe opérateur existant dans le champ **Ancien mot de passe**.
3. Saisissez un **nouveau mot de passe**, puis répétez le même mot de passe dans le champ **Confirmer le nouveau mot de passe**.

   Il est recommandé de créer un mot de passe très sûr, en particulier pour l'opérateur admin. Pour plus d'informations, consultez la section Création d'un mot de passe sûr (ci-dessous).
4. Cliquez sur **OK**.

Pour réinitialiser le mot de passe d'un autre opérateur, naviguez dans **Global | Opérateurs** et cliquez sur le bouton ellipsis **[...]** à côté du champ **Mot de passe**.

Création d'un mot de passe sûr

Lorsque vous créez ou modifiez le mot de passe de l'opérateur administrateur, il est **vivement recommandé** de créer un mot de passe très sûr.

À titre indicatif, un mot de passe sécurisé doit inclure les caractéristiques suivantes :

- Minimum huit caractères de longueur
- Combinaison de lettres majuscules et minuscules
- Combinaison de chiffres et de lettres
- Inclusion de caractères spéciaux

Les mots de passe doivent être conformes aux exigences de la politique de mot de passe.

Naviguer dans l'interface utilisateur

Il existe deux méthodes pour naviguer dans l'interface utilisateur : le menu principal et le navigateur du système.

Menu principal

Le menu principal est situé en haut de l'écran et permet d'accéder à toutes les pages du logiciel.

Les items du menu sont organisés en groupes logiques correspondant à leurs fonctions. Par exemple, le menu **Surveillance** permet d'accéder aux fonctions de surveillance du site (p. ex. pages des statuts, plans d'étage, caméras), tandis que le menu **Utilisateurs** vous permet de programmer les utilisateurs et les éléments connexes tels que les niveaux d'accès.

Pour ouvrir une fenêtre de programmation spécifique, cliquez sur l'élément du menu principal correspondant pour le développer, puis sélectionner l'élément souhaité dans le menu déroulant pour ouvrir la fenêtre de programmation.

Certains menus et pages peuvent ne pas être disponibles sans la licence correspondante ou des autorisations suffisantes de l'opérateur.

Navigateur système

Le navigateur système offre un moyen rapide d'accéder à des appareils spécifiques et à des enregistrements programmés.

Vous pouvez ouvrir le navigateur système en cliquant sur l'icône hamburger ≡ en haut à gauche de la fenêtre. La flèche de retour en arrière permet de fermer le navigateur système.

La barre de navigation s'ouvre sur le côté gauche de l'écran, affichant les catégories disponibles. Les enregistrements sont classés dans un ordre relationnel, de sorte que vous pouvez localiser les enregistrements en développant les catégories pertinentes.

Le navigateur système n'affiche que les enregistrements du **site** actuellement sélectionné sur la page d'accueil.

Pour naviguer dans le système :

- Cliquez sur la flèche à côté d'une catégorie pour afficher les enregistrements inclus dans cette catégorie. Par exemple, développez la catégorie **Contrôleurs** pour afficher les contrôleurs du site.
- Cliquez sur la flèche située à côté d'un enregistrement pour voir les catégories associées à cet enregistrement. Par exemple, développez un enregistrement de contrôleur spécifique pour voir les catégories des modules d'expansion, des entrées et des sorties qui peuvent être connectés au contrôleur.
- Cliquez avec le bouton gauche sur une catégorie ou un enregistrement pour ouvrir la fenêtre de programmation de cet élément. Par exemple, cliquez sur un enregistrement de partition spécifique pour ouvrir la fenêtre de programmation **Programmation | Partitions** et mettre en évidence cet enregistrement.
- Un clic droit sur un enregistrement ouvre le menu contextuel de cet élément, ainsi que la fenêtre de programmation. Par exemple, cliquez avec le bouton droit de la souris sur un enregistrement de partition spécifique pour ouvrir le menu des commandes manuelles de la partition, ce qui vous permet d'armer et de désarmer la partition.

Les entrées trouble dont le type de module est Porte (DR) ne sont pas affichées dans le navigateur du système. Il s'agit d'une limitation connue des catégories du navigateur. Pour visualiser toutes les entrées trouble, y compris celles affectées aux enregistrements de porte, cliquez sur une catégorie **Entrées trouble** pour ouvrir la fenêtre de programmation.

Barre d'état

La barre d'état est située au bas de l'écran et indique l'état de la communication, l'état de l'alarme et les détails de connexion actuels.

- **Icône de la personne** : Cliquez sur cette icône pour afficher l'opérateur qui est actuellement connecté, ainsi que le nom du serveur.
- **Icône du serveur** : Cette icône affiche l'état actuel des contrôleurs connectés. Les statuts possibles sont les suivants :
  - **OK** : Aucun problème avec les contrôleurs.
  - **Contrôleurs hors ligne** : Le nombre de contrôleurs qui sont hors ligne est indiqué par un drapeau rouge.
  - **Obtenir le statut de santé** : Le nombre de problèmes liés au statut de santé que les contrôleurs signalent actuellement.

    Pour afficher le statut de santé d'un contrôleur, naviguez vers **Sites | Contrôleurs**, faites un clic droit sur l'enregistrement du contrôleur et cliquez sur **Obtenir le statut de santé**.
- **Icône de la sirène** : Cette icône affiche le nombre d'alarmes opérateur qui n'ont pas encore été reconnues. Cliquez sur l'icône pour ouvrir la page de statut des alarmes, qui vous permet de visualiser et de reconnaître toutes les alarmes.

Certaines intégrations tierces affichent également des icônes dans la barre d'état indiquant l'état de connexion de l'intégration.

Fenêtre de programmation

La fenêtre de programmation est l'endroit où vous programmez les éléments du système. Elle est divisée en trois parties :

- **Barre d'outils** : La barre d'outils de programmation située en haut de la fenêtre fournit des boutons pour diverses fonctions, telles que l'ajout, la sauvegarde, la recherche, l'exportation et la suppression de registres.
- **Liste des registres** : La liste des registres, à gauche de la fenêtre, affiche les registres qui peuvent être programmés. Les colonnes indiquent les détails clés de chaque registre, tels que le **contrôleur**, l'**ID base de données** et la date de **dernière modification**.

  Un certain nombre de fonctionnalités vous aident à trouver les documents dont vous avez besoin :
  - Dans la barre d'outils, vous pouvez sélectionner le **site** et le **contrôleur** pour lesquels vous souhaitez afficher les registres.
  - Les registres peuvent être triés par n'importe quelle colonne, par exemple par nom ou par ID base de données. Cliquez une fois sur l'un des en-têtes de colonne pour trier les registres dans un ordre décroissant, et une autre fois pour les trier dans un ordre croissant.
  - Le bouton **Trouver** vous permet de filtrer les registres affichés par n'importe quel champ. Par exemple, vous pouvez filtrer les registres de portes pour trouver les portes dont le nom contient Entrée. Pour plus d'informations, consultez la section Utiliser l'outil de recherche (page suivante).

  En outre, vous pouvez cliquer avec le bouton droit de la souris sur certains registres pour ouvrir un menu contextuel contenant des commandes manuelles. Par exemple, cela vous permet de verrouiller ou de déverrouiller une porte.
- **Onglets de programmation** : Le volet de programmation situé à droite de la fenêtre vous permet de configurer les paramètres. Les options disponibles sont regroupées dans des onglets, affichés en haut du volet de programmation. Par exemple, la programmation de portes a des onglets **Entrées** et **Sorties** pour configurer les paramètres relatifs aux entrées et aux sorties respectivement.

  Chaque onglet est à son tour divisé en plusieurs sections. Cliquer sur l'en-tête d'une section pour développer ou masquer les options de cette section.

Barre d'outils

La barre d'outils de programmation est affichée à chaque fois qu'une fenêtre de programmation est ouverte. Elle contient des boutons utiles relatifs à la fonction sélectionnée. Les boutons les plus courants sont décrits ci-dessous.

Bouton	Fonction
Mode de programmation	Sélectionnez si vous programmez en mode local (ce contrôleur uniquement) ou global (contrôleur croisé). Disponible uniquement pour les portes et les fonctions programmables.
Contrôleur	Sélectionnez le contrôleur pour lequel vous souhaitez afficher les enregistrements.
Site	Sélectionnez le site pour lequel vous souhaitez afficher les enregistrements.
Ajouter	Créez un nouvel enregistrement avec les paramètres par défaut.
Sauvegarder	Sauvegardez les changements apportés à l'enregistrement actuel. Après la sauvegarde d'un enregistrement, les modifications peuvent être téléchargées sur le contrôleur.
Trouver	Ouvrez l'outil de recherche pour filtrer la liste des enregistrements. Pour plus d'informations, consultez la section Utiliser l'outil de recherche (page suivante).
Actualiser	Actualisez l'enregistrement actuel pour voir les mises à jour éventuelles.
Exporter	Exportez les enregistrements affichés dans la liste des enregistrements, y compris les informations des colonnes spécifiées. Vous pouvez exporter les données vers un fichier CSV ou vers le presse-papiers.

Bouton	Fonction
Copier	Copiez la configuration d'un enregistrement spécifié sur l'enregistrement actuel. Cette fonction ne crée pas de copie de l'enregistrement actuellement sélectionné. Au lieu de cela, il écrase l'enregistrement actuellement sélectionné avec les paramètres d'un autre enregistrement.
Effacer	Effacez l'enregistrement de la base de données de programmation. Cela effacera également tous les enregistrements qui dépendent de cet enregistrement. Par exemple, si vous effacez un Module d'expansion d'entrée, les entrées qui lui sont connectées seront également supprimées.
Dépannage	Ouvrez la fenêtre de programmation actuelle dans une nouvelle fenêtre de dépannage. Pour plus d'informations, consultez la section Ouvrir plusieurs fenêtres (page suivante).

Sélection de plusieurs registres

Dans Protege GX, vous pouvez sélectionner plusieurs registres dans la liste des registres. Cela permet d'appliquer des changements de programmation à un certain nombre d'enregistrements simultanément.

- Pour sélectionner plusieurs enregistrements dans un intervalle continu, cliquez sur le premier registre que vous souhaitez sélectionner, puis maintenez la touche **Maj** enfoncée et cliquez sur le dernier registre de l'intervalle.
- Pour sélectionner plusieurs registres discontinus, cliquez sur le premier registre que vous souhaitez sélectionner, puis maintenez la touche **Contrôle** enfoncée et cliquez sur chaque registre supplémentaire à inclure.
- Pour sélectionner tous les registres de la liste des registres, appuyer sur **Contrôle + A**.

Une fois que vous avez sélectionné plusieurs registres, vous pouvez les programmer tous collectivement. Par exemple, vous pourriez vouloir définir le même horaire sur un certain nombre de niveaux d'accès. Utiliser **Contrôle + Clic** pour sélectionner les niveaux d'accès requis, puis définir l'**horaire de fonctionnement** et cliquer sur **Sauvegarder**.

Vous pouvez également exporter les registres sélectionnés. Cliquer sur **Exporter** dans la barre d'outils et définir le **type d'exportation** sur Registres sélectionnés.

Utiliser l'outil de recherche

L'outil de recherche est une méthode pratique pour localiser des registres dans une liste. Il fonctionne en filtrant la liste des registres pour n'inclure que les registres ayant des propriétés de champ spécifiées. Par exemple, vous pourriez vouloir trouver tous les utilisateurs auxquels un niveau d'accès spécifique a été assigné, ou toutes les portes pour lesquelles une certaine fonction est activée.

L'utilisation efficace de l'outil de recherche est essentielle pour la gestion des systèmes Protege GX importants. Pour utiliser l'outil de recherche :

1. Naviguez vers la fenêtre de programmation concernée et cliquez sur le bouton **Trouver** dans la barre d'outils. L'outil de recherche s'ouvre.
2. Sélectionnez le **Champ** que vous utiliserez pour filtrer la liste des registres. Par exemple, vous pouvez filtrer en fonction du **Nom de famille**, du **Groupe de registres** ou du **Niveau d'accès** dans la programmation de l'utilisateur.
3. Configurez les conditions du filtre dans la section **Valeurs**. Les valeurs disponibles dépendent du type de champ sélectionné :
   - Pour les champs de texte, vous pouvez inclure ou exclure un segment de texte (**Étiqueter**).
   - Pour les champs déroulants, vous pouvez sélectionner les options qui seront incluses ou exclues par le filtre.
   - Pour les champs de case à cocher, vous pouvez régler le filtre sur **Actif** (case à cocher activée) ou **Inactif** (case à cocher désactivée).

- Pour les champs numériques, vous pouvez définir des valeurs minimales et maximales, et inclure ou exclure les registres compris dans cette plage.

Il se peut que vous deviez agrandir la fenêtre en cliquant et en faisant glisser le curseur depuis le coin inférieur droit.

4. Cliquez sur **OK**. La liste des registres affiche maintenant tous les registres qui correspondent aux critères que vous avez saisis.
5. Pour effacer le filtre et afficher tous les registres, cliquez sur **Actualiser** dans la barre d'outils.

Ouvrir plusieurs fenêtres

Protege GX permet d'afficher et de travailler sur plusieurs fenêtres d'application (fenêtres en incrustation) avec une seule connexion client. Cela vous permet de programmer efficacement, ainsi que de visualiser plusieurs plans d'étage graphiques ou pages des statuts à la fois lorsque vous surveillez un bâtiment.

Les fenêtres en incrustation comprennent la barre d'outils, la liste des registres et les onglets de programmation, mais pas le menu principal. Vous pouvez donc visualiser et programmer des registres dans les fenêtres en incrustation, mais vous ne pouvez que naviguer dans la fenêtre principale.

Bouton d'incrustation

Le bouton **Incrustation** dans la barre d'outils ouvre une nouvelle fenêtre en incrustation contenant la page de programmation que vous êtes en train de consulter. Cela vous permet de garder la fenêtre actuelle ouverte tout en naviguant vers une nouvelle page de programmation.

Cette fonction est particulièrement utile pour surveiller le système à l'aide de pages des statuts ou de plans d'étage. Ouvrez la page du statut ou le plan d'étage souhaité, puis cliquez sur **Incrustation** pour l'ouvrir dans une nouvelle fenêtre. Vous pouvez placer une ou plusieurs fenêtres en incrustation sur un deuxième écran pour garder un œil sur l'ensemble du système en même temps.

Bouton d'ellipse

De nombreux champs dans les fenêtres de programmation Protege GX disposent d'un **bouton d'ellipse[...]** à droite du champ. En cliquant sur le bouton d'ellipse, vous ouvrez une nouvelle fenêtre en incrustation contenant les registres qui peuvent être programmés dans ce champ. Cette fonction est pratique pour modifier ou créer des registres connexes au fur et à mesure que vous travaillez.

Par exemple, vous pouvez être amené à créer un nouvel horaire lors de la programmation d'un niveau d'accès. Cliquez sur l'ellipse **[...]** à droite du champ **Horaire d'opération**. La programmation de l'horaire s'ouvre dans une fenêtre en incrustation, vous permettant de programmer et de sauvegarder le nouvel horaire. Vous pouvez ensuite fermer la fenêtre en incrustation et définir immédiatement **l'Horaire d'opération** dans la programmation du niveau d'accès.

Onglets Historique, Utilisation et Événements

Les onglets Historique, Utilisation et Événements sont disponibles sur la plupart des pages de programmation du système. Ils vous aident à garder la trace des caractéristiques et des activités importantes pour chaque enregistrement individuel.

- **Onglet Historique** : Affiche l'historique d'audit de l'enregistrement, vous permettant de voir quand l'enregistrement a été créé et modifié, et par quels opérateurs. Chaque fois que l'enregistrement est sauvegardé, les détails de la modification sont enregistrés dans cet onglet.

  Pour afficher les informations complètes sur ce qui a été changé, mettez en évidence une entrée dans la liste de l'historique et cliquez sur **Détails**.
- **Onglet Utilisation** : Indique où l'enregistrement est actuellement utilisé dans le logiciel. Par exemple, pour un enregistrement de porte, vous pouvez voir où la porte est utilisée dans les groupes de portes, les niveaux d'accès et les fonctions programmables.

Ceci est utile pour déterminer quels autres enregistrements seront affectés si vous apportez une modification à l'enregistrement. Il est recommandé de vérifier cet onglet avant de supprimer un enregistrement, afin de s'assurer qu'il n'est pas utilisé ailleurs dans le système.

- **Onglet Événements** : Affiche les événements récents associés à l'enregistrement. Par exemple, pour un enregistrement de porte, vous verrez les plus récents événements d'accès autorisé, de porte ouverte et de porte forcée.

  Cliquez sur **Chargement des événements** pour charger les événements. Le bouton **Parcourir comme rapport** ouvre une fenêtre de incrustation contenant un rapport d'événement pour cet enregistrement, qui peut être exporté, imprimé ou envoyé par courriel selon les besoins. Vous pouvez également utiliser le bouton **Copier dans le presse-papiers** pour copier les événements afin de les coller dans un fichier CSV.

Fenêtre de rapport

La fenêtre des rapports s'affiche chaque fois que vous exécutez un rapport (tel qu'un rapport d'utilisateur ou un rapport d'événement) ou une recherche (recherche d'utilisateur ou recherche d'événement). La grille de rapport dispose de diverses fonctions de tri, de regroupement et de filtrage des données d'événements, ce qui vous permet de visualiser et d'exporter exactement les informations dont vous avez besoin.

Pour plus d'informations, consultez la section Visualisation des rapports (la page 171).

Conseils de programmation et dépannage

Cette section contient des conseils de programmation utiles, des informations sur l'endroit où trouver des ressources supplémentaires et des informations de dépannage.

Ressources additionnelles

Un certain nombre de ressources additionnelles sont à votre disposition lorsque vous utilisez le Protege GX système, que vous soyez en train d'apprendre le système ou que vous recherchiez des astuces de programmation avancées.

- **Les notes d'application** décrivent des applications spécifiques du système, comme la façon de programmer une fonction ou une intégration particulière. Ils comprennent généralement des instructions de programmation étape par étape.

  Cette documentation comprend des références à des notes d'application qui contiennent des informations plus détaillées sur des caractéristiques particulières.

  Les notes d'application sont disponibles sur le ICT site web de :www.ict.co/Application-Notes .
- La **Base de Connaissances ICT** est conçue pour répondre aux questions techniques les plus courantes que les opérateurs se posent sur les Protege systèmes. Il fournit des conseils de dépannage et de programmation pour vous aider à résoudre les problèmes.

  Visiter la Base de Connaissances ICT ici.
- **Les vidéos** sur la chaîne YouTube de l'ICTNZ fournissent des démonstrations visuelles et auditives. Il s'agit notamment de didacticiels sur les logiciels et le matériel, de conseils pour les techniciens, de présentations de solutions et de webinaires gratuits. De nouvelles vidéos sont ajoutées fréquemment.
- **La formation** est disponible à la fois en personne avec nos formateurs techniques qualifiés et en ligne. Les modules en ligne peuvent être revus à tout moment pour vous rafraîchir la mémoire. Contacter ICT pour plus d'informations et pour s'inscrire aux cours.
- Si tout le reste échoue, vous pouvez contacter **l'équipe d'assistance technique ICT** par courriel ou par téléphone, ou enregistrer un ticket d'assistance. Voir www.ict.co/Contact-Us pour connaître les meilleurs moyens d'entrer en contact.

Convention d'appellation

Avant de programmer un site, il est important de définir une convention d'appellation qui sera utilisée dans tout le système. Plus la convention d'appellation est cohérente, plus la maintenance du site sera facile, car les registres pourront toujours être identifiés facilement et précisément.

Les noms descriptifs des registres sont utiles pour rechercher des registres spécifiques à l'aide de l'outil de recherche (consultez la page 20). Il est recommandé de donner aux registres similaires un élément de dénomination commun afin de pouvoir les retrouver facilement.

Une bonne convention d'appellation est également importante pour aider les installateurs et les techniciens à identifier rapidement et précisément les appareils physiques, qu'ils utilisent le logiciel ou un clavier sur site. Un nom utile contient des informations sur l'emplacement physique de l'appareil, son adresse réseau et sa fonction.

Trois champs d'appellation sont disponibles pour les appareils :

- **Nom** : Il s'agit du nom qui apparaît dans la version anglaise du logiciel Protege GX et dans les journaux des événements. Il doit identifier les principales caractéristiques du registre, comme sa fonction dans le système, l'adresse de son module et le contrôleur auquel il est connecté.
- **Nom (deuxième langue)** : Le nom qui apparaît dans la version du logiciel de la deuxième langue et dans les journaux des événements. Si le site n'utilise pas une deuxième langue, ce champ peut être utilisé pour des informations supplémentaires sur le registre.

- **Nom d'affichage du clavier** : Le nom qui est affiché sur le clavier (pour les partitions, les portes, les entrées, etc.) et dans les signalements destinés à une station de surveillance IP. Ce nom doit être reconnaissable par les utilisateurs finaux. Par exemple, si l'utilisateur final arme une partition et que certaines entrées sont ouvertes, il doit être en mesure d'identifier facilement les entrées qu'il doit vérifier avant de quitter les lieux.

  Le clavier ne peut afficher que les 16 premiers caractères du nom.

Exemple

Ci-dessous un exemple de convention d'appellation des entrées. Il s'agit des entrées 1 à 4 connectées au module d'expansion du lecteur 1 du contrôleur 1 :

Nom	Nom d'affichage du clavier
CTRL1 Porte de bureau Reed RD1.1	Porte de bureau
CTRL1 Porte de bureau REX RD1.2	Porte de bureau REX
CTRL1 Porte de bureau Bond RD1.3	Serrure de bureau
CTRL1 Bureau PIR RD1.4	PIR de bureau

Opérations inter-contrôleurs (programmation globale)

Pour toutes les informations concernant cette fonction, consulter la Note d'application 180 : Opérations inter-contrôleurs dans Protege GX.

Dans le système Protege GX, chaque contrôleur fonctionne normalement indépendamment des autres, avec son propre réseau de modules d'expansion, d'entrées et de sorties. Avec les opérations inter-contrôleurs, un certain nombre de contrôleurs Protege GX peuvent agir comme un seul système et partager les ressources matérielles. Par exemple, cela vous permet d'assigner les entrées de deux contrôleurs différents à une seule partition, ou de créer des groupes de sorties programmables qui couvrent plusieurs sections du bâtiment.

Certaines pages de programmation, telles que **Groupes | Groupes de sorties programmables**, permettent par défaut la programmation inter-contrôleurs : vous avez toujours la possibilité de sélectionner des sorties depuis n'importe quel contrôleur du site. Dans d'autres cas, tels que **Programmation | Portes** et **Programmation | Partitions**, vous pouvez régler le **mode de programmation** sur Local (ce contrôleur uniquement) ou Global (tout contrôleur sur le site) dans la barre d'outils.

Protege GX permet de relier jusqu'à 64 contrôleurs. Si cette limite est dépassée, Protege GX génère un message d'état de santé indiquant les contrôleurs qui ne peuvent pas communiquer en raison de cette limitation.

Guide des types d'événements courants

Protege GX présente des rapports d'événements complets, avec des centaines de descriptions uniques pour les différentes occurrences. En plus de fournir des données pour les rapports et les audits, la compréhension des événements Protege GX est très utile pour le dépannage. Cette section fournit un guide pour certains types d'événements courants.

Événements d'accès utilisateur

Lorsqu'un utilisateur se voit refuser l'accès pour entrer ou sortir d'une porte, il est important de savoir pourquoi cela s'est produit. Le journal événement est une ressource précieuse pour déterminer ce qui restreint l'accès de l'utilisateur.

Le tableau ci-dessous décrit un certain nombre d'événements courants qui peuvent aider à dépanner l'accès de l'utilisateur. Les causes de refus d'accès sont classées de la plus basse à la plus haute priorité.

Exemple d'événement	Causes
Lire donnée brute (1.1) au lecteur d'entrée sur la porte "Porte du bureau" (RD1 Port 1)	Le contrôleur ne reconnaît pas ce numéro de carte. Causes possibles : • La carte n'a pas été assignée à un utilisateur. Faites un clic droit sur l'événement pour assigner la carte. • Le registre de l'utilisateur n'a pas été téléchargé sur ce contrôleur. Vérifiez que l'utilisateur a accès à au moins un registre sur ce contrôleur, et attendez que le téléchargement soit terminé. • Si la carte lue a été reçue par un lecteur intelligent, il se peut que les informations d'identification ne correspondent pas à l'un des **types de correspondance des informations d'identification du lecteur**.
Utilisateur UTILISATEUR INVALIDE NIP invalide RD1 Utilisant le port Port 1 In l'Entrée du clavier	Le contrôleur ne reconnaît pas ce NIP. Causes possibles : • Le NIP n'a pas été assigné à un utilisateur. • Le registre de l'utilisateur n'a pas été téléchargé sur ce contrôleur. Vérifiez que l'utilisateur a accès à au moins un registre sur ce contrôleur, et attendez que le téléchargement soit terminé. • Le NIP ne correspond pas aux autres informations d'identification saisies par l'utilisateur (par exemple, lorsque la porte utilise l'opération carte + NIP et que l'utilisateur saisit un NIP incorrect).
Porte Porte du bureau Informations d'identification non valides fournies par Brett	La porte nécessite plusieurs informations d'identification, et les secondes informations d'identification fourni ne correspondent pas aux premières.
Utilisateur Brett Lamb Registre désactivé à RD1 Utilisant le port Port 1	Causes possibles : • Le registre utilisateur a été désactivé. • Les informations d'identification de l'utilisateur ont été désactivées.
Utilisateur Brett Lamb Registre expiré à RD1 Utilisant le port Port 1	Causes possibles : • Le registre utilisateur a expiré. • Le niveau d'accès de l'utilisateur a expiré.

Exemple d'événement	Causes
Utilisateur Brett Lamb Planification non valide au Porte du bureau Niveau d'accès Personnel	Causes possibles : • **L'horaire** défini pour ce niveau d'accès dans la programmation utilisateur n'est pas valide. • **L'horaire d'opération** défini pour ce niveau d'accès dans la programmation de niveau d'accès n'est pas valide.
Utilisateur Brett Lamb, porte non autorisée porte du bureau à l'aide du niveau d'accès de personnelUtilisateur Brett Lamb Porte non autorisée Porte du bureau Niveau d'accès Personnel	L'utilisateur n'a pas cette porte dans son niveau d'accès. Vérifiez les portes et les groupes de portes du niveau d'accès.
Utilisateur Brett Lamb Accès refusé par verrouillage de porte à Porte du bureau	La porte est en état de verrouillage et n'autorise pas l'accès dans ce sens.
Utilisateur Brett Lamb Refusé par type de porte invalide à Porte du bureau Utilisant type de porte Type de Porte (DTUnknown)	Le type de porte n'est pas configuré ou mal programmé. Causes possibles : • Aucun **Type de porte** n'est configuré dans la programmation de la porte. • Le niveau d'accès de l'utilisateur a l'option **Utiliser le type de porte de niveau d'accès** activée, mais il n'y a pas de **Type de porte de niveau d'accès** défini dans le type de porte.
Utilisateur Brett Lamb Refusé par horaire du type de porte à Port du bureau Utilisant type de porte Type de Porte	**L'horaire d'opération** pour le type de porte n'est pas valide, mais le **Type de porte secondaire** est absent ou n'est pas programmé correctement.
Utilisateur Brett Lamb Échec entrée anti-retour à la porte Porte du bureau Partition Bureau Partition requise Réception	Le type de porte est configuré pour un anti-passback dur et l'utilisateur a commis une violation de l'anti-passback. L'accès est refusé. • La première partition listée dans l'événement est la dernière partition connue où l'utilisateur a entré. La seconde partition indiquée est la partition requise pour accéder à cette porte. Dans cet exemple, Brett Lamb doit se trouver dans la partition de réception pour pouvoir franchir la porte du bureau. Cependant, il a été enregistré pour la dernière fois comme entrant dans la partition du bureau. L'accès lui est donc refusé. • Faites un clic droit sur l'événement pour réinitialiser le statut anti-passback de l'utilisateur.
Utilisateur Brett Lamb échec de l'anti-passback souple à la porte du bureau de la partition du bureau, partition de l'utilisateur réinitialisé au bureau	Le type de porte est configuré pour un anti-passback souple et l'utilisateur a commis une violation de l'anti-passback. L'accès est accordé. • La partition indiquée dans l'événement est la partition dans laquelle l'utilisateur est en train d'entrer. Le système réinitialise automatiquement la partition de l'utilisateur à cette nouvelle partition. Dans cet exemple, Brett Lamb tente par erreur d'entrer dans la partition de bureau. Le système lui accorde l'accès et réinitialise sa partition actuelle en partition de bureau.

Exemple d'événement	Causes
Utilisateur Brett Lamb a été refusé l'entrée à Porte du bureau par le statut de la région Bureau en utilisant le Niveau d'accès Personnel	L'utilisateur est empêché d'accéder à la porte car la partition située derrière la porte est armée. Causes possibles : • Par défaut, l'utilisateur n'est pas autorisé à accéder à la partition s'il n'est pas en mesure de la désarmer. Assurez-vous que cette partition est incluse dans les groupes de désarmement de partitions de l'utilisateur. • Si l'option **Refuser l'entrée si la partition intérieure/extérieure est armée** est activée dans **Programmation | Portes | Options avancées**, l'accès est refusé même si l'utilisateur peut désarmer la zone.
Entrée refusée à l'utilisateur Brett Lamb à la porte du bureau par le comptage de la partition du bureau à l'aide du niveau d'accès de personnel	Le comptage des utilisateurs est activé dans la partition dans laquelle l'utilisateur tente d'entrer (**Programmation | Partitions | Options (1)**) et contient actuellement le nombre maximum de personnes.
Utilisateur Brett Lamb Entrée refusée par interverrouillage Porte du bureau	Un groupe de portes interverrouillées est assigné à la porte (**Programmation | Portes | Général**) et une ou plusieurs des portes du groupe sont ouvertes/déverrouillées. Pour permettre l'accès, fermez et verrouillez toutes les autres portes du groupe interverrouillé.
Utilisateur Brett Lamb Entrée refuse à Porte du bureau Par erreur de mode d'entrée...	L'utilisateur a présenté un type d'informations d'identification qui n'est pas autorisé par le type de porte. La deuxième partie de l'événement apporte des détails supplémentaires sur l'erreur, par exemple : • Porte programmée pour opération par Carte seulement à l'aide de l'entrée NIP Le type de porte nécessite une carte, mais l'utilisateur a saisi un NIP. • Porte programmé pour opération avec NIP seulement à l'aide de l'entrée carte Le type de porte nécessite un NIP, mais l'utilisateur a badgé une carte. • Porte en attente du mode NIP à l'aide de l'entrée carte Le type de porte nécessite carte et NIP. L'utilisateur a badgé sa carte, puis a badgé à nouveau au lieu de saisir un NIP. • Porte en attente du mode carte à l'aide de l'entrée carte Le type de porte nécessite un identifiant biométrique ou un type d'informations d'identification, mais l'utilisateur badge une carte.
Utilisateur Brett Lamb' Accès refusé à la porte 'Porte du bureau' car l'utilisateur n'est pas un maître/fournisseur à accès double.	La porte est configurée pour l'authentification double (**Programmation | Types de portes | Options**) mais l'utilisateur n'est pas un maître de double accès ou un fournisseur de double accès (**Utilisateurs | Utilisateurs | Options**).

Événements de signalement

Lorsqu'une partition est armée ou désarmée ou qu'une entrée est ouverte, fermée, contournée ou altérée, le système enregistre généralement un événement de signalement en plus des événements normaux. Ces événements correspondent aux codes de signalement Contact ID, indiquant les informations qui seraient envoyées à la station de surveillance en utilisant le signalement Contact ID standard.

Les événements pertinents sont :

- Rapport dans <AREA_NAME> Utilisant zone <ZONE_NAME> Code spécial [<CUSTOM_REPORT_CODE>] Signale [<REPORT_FLAGS_A>]
- Rapport dans <AREA_NAME> Utilisant zone trouble <TROUBLE_ZONE_NAME> Code spécial [<CUSTOM_REPORT_CODE>] Signale [<REPORT_FLAGS_A>]
- Signaler dans <AREA_NAME> Utilisateur <USER_NAME> Rapport <AREA_REPORT_TYPE> Signale [<REPORT_FLAGS_A>]

Les définitions des différents paramètres de ces événements sont les suivantes :

Paramètre	Définition/Notes
Rapport dans <AREA_NAME>	Le nom de la partition où l'événement s'est produit. • Pour les événements d'entrée/entrée trouble, il s'agit de la partition dans laquelle l'entrée est programmée. • Pour les événements de partition, il s'agit de la partition qui a été armée/désarmée.
<ZONE_NAME> ou <TROUBLE_ZONE_NAME>	Le nom de l'entrée ou de l'entrée trouble qui a déclenché l'événement.
<USER_NAME>	Le nom de l'utilisateur qui a armé/désarmé la partition. • Si la partition n'a pas été armée/désarmée par un utilisateur, l'événement est attribué à UTILISATEUR SYSTÈME. Il s'agit d'opérateurs Protege GX, de fonctions programmables, de programmes et d'autres méthodes d'armement/désarmement.
Code spécial [<CUSTOM_REPORT_CODE>]	Basé sur le code d'événement Contact ID pour les entrées, qui décrit quel type d'entrée provoque l'événement. • Le code d'événement peut être défini comme le **code personnalisé** de signalisation dans **Programmation | Types d'entrées | Général**. Par défaut, c'est réglé sur Aucun. • Par exemple, pour un bouton de panique, le **Code personnalisé de signalisation** peut être réglé sur 12 - Alarme de panique. • Les entrées troubles utilisent des codes d'événement prédéfinis en fonction du type de condition trouble qu'elles signalent. Celles-ci sont décrites dans les manuels d'installation des modules concernés.
Rapport <AREA_REPORT_TYPE>	Basé sur le code d'événement Contact ID pour les partitions, qui décrit la méthode ou le type d'armement/désarmement. Par exemple : • Utilisateur indique que la partition a été désarmée localement par un utilisateur. • À distance indique que la partition a été désarmée à distance par le logiciel ou une fonction automatique. • Partiel indique que la partition a été armée de force. • Rester indique que la partition a été armée de séjour.

Paramètre	Définition/Notes
Signale [<REPORT_ FLAGS_A>]	Le paramètre <REPORT_FLAGS_A> consiste en deux termes. • Le premier terme est basé sur le qualificatif d'événement Contact ID. C'est soit : - [NEW] pour les nouveaux incidents (p. ex., l'entrée s'ouvre) - [RESTORE] pour la fin de l'incident (p. ex., l'entrée se ferme). • Le second terme est basé sur le code d'événement Contact ID et décrit ce qui est arrivé à l'entrée. Les options sont : - [ALARM] pour les alarmes d'entrée et restaure. - [TAMPER] pour les sabotages/courts-circuits d'entrée et restaure. - [Bypass] pour les contournements d'entrée et restaure. • Par exemple, lorsqu'une entrée est altérée, elle affiche les signes [NEW+TAMPER]. Lorsqu'une altération est restaurée, elle affiche [RESTORE+TAMPER]. • Les signalements de partition affichent toujours les signes [NEW+ALARM]

Sauvegarde et restauration de la base de données

Il est recommandé de créer régulièrement des sauvegardes des deux bases de données Protege GX. Cela garantit que la programmation et les événements ne sont pas perdus lorsqu'une base de données est corrompue ou détruite. Vous pouvez configurer des sauvegardes régulières des deux bases de données dans Protege GX, ou effectuer une sauvegarde manuelle dans Microsoft SQL Server Management Studio (SSMS). En outre, la base de données d'événements peut effectuer des sauvegardes différentielles, ce qui lui permet de purger régulièrement les anciens événements afin que la base de données ne soit pas pleine.

Le processus de restauration de la base de données doit être effectué dans SSMS, avec les services Protege GX arrêtés. La restauration d'une base de données vous permet de récupérer la programmation et les événements perdus lorsque cela est nécessaire.

Comme le serveur et les bases de données Protege GX sont complètement indépendants, toute base de données peut être restaurée sur n'importe quelle installation de serveur. Cela vous permet de restaurer des bases de données sur un serveur de test, de créer des bases de données préprogrammées qui contiennent une configuration par défaut, et de revoir les événements passés dans une installation distincte.

Compatibilité de la base de données

Lorsque vous sauvegardez ou restaurez une base de données, vous devez prendre note de la **version de la base de données**. Le numéro de version du logiciel (voir **À propos | Version**) indique la version de la base de données comme indiqué ci-dessous :

4	3	264	39
Version majeure	**Version mineure**	**La version de la base de données**	**Élaboration de logiciel**

Les sauvegardes effectuées par le logiciel Protege GX incluent toujours le numéro de version de la base de données dans le nom du fichier. C'est une bonne pratique à suivre lorsque vous effectuez vos propres sauvegardes.

Lorsque vous restaurez une base de données, vous devez vous assurer que la version de la base de données du fichier de sauvegarde est compatible avec celle du logiciel, comme indiqué ci-dessous :

La version de la base de données		Version du logiciel	
265	>	264	✖
264	=	264	✔
264	<	265	✔

- Si la version de la base de données est plus récente que la version du logiciel, il n'est pas possible de restaurer la base de données. Mettez à jour le logiciel avant de la restaurer.
- Si les numéros de version correspondent, la restauration devrait aboutir.
- Si la version de la base de données est plus ancienne que la version du logiciel, la base de données peut être restaurée mais doit être mise à niveau pour correspondre à la version du logiciel. Restaurez la base de données, puis désinstallez et réinstallez le logiciel du serveur pour mettre à niveau la version de la base de données.

Si la version de la base de données et la version du logiciel ne correspondent pas, **le service de données ne démarre pas**.

Créer des sauvegardes de la base de données

Il existe plusieurs méthodes pour sauvegarder les bases de données Protege GX, à la fois dans le logiciel Protege GX et dans SQL Server Management Studio (SSMS). Dans le logiciel, vous pouvez également configurer des sauvegardes régulières de la base de données principale, ainsi que des sauvegardes différentielles régulières et des purges de la base de données d'événements.

Effectuer des sauvegardes dans Protege GX

Dans Protege GX, naviguez vers **Global | Paramètres globaux**. Les options suivantes sont disponibles pour sauvegarder les bases de données.

Lorsque vous définissez un chemin de sauvegarde, assurez-vous que le répertoire sélectionné existe déjà sur la machine serveur. Ne sélectionnez pas un répertoire qui refuse l'accès en écriture à SQL Server, tel que Program Files, Program Data, Users, Windows, etc.

Pour sauvegarder une fois la base de données principale :

1. Saisissez un **chemin de sauvegarde**.
2. Cliquez sur **Sauvegarde maintenant**.

Le numéro de version de la base de données est ajouté au nom du fichier.

Pour sauvegarder la base de données principale chaque nuit à minuit :

1. Saisissez un **chemin de sauvegarde**.
2. Activez **Sauvegarder base de données principale tous les soirs**.
3. Vous pouvez également activer **Annexer le jour de la semaine au nom du fichier de sauvegarde**.

Les nouveaux fichiers de sauvegarde écraseront les sauvegardes existantes portant le même nom. Si plus d'une semaine de sauvegardes stockées est nécessaire, envisagez de changer régulièrement le chemin de sauvegarde.

Pour sauvegarder une fois la base de données d'événements :

1. Définissez le champ **Sélectionnez une option de sauvegarde** sur Chemin local, Chemin réseau ou FTP.
2. Saisissez le **Chemin de sauvegarde de la base de données des événements**. Si vous avez sélectionné FTP ci-dessus, vous devez saisir les paramètres FTP pertinents tels que **l'adresse IP** et le **numéro de port**.
3. Cliquez sur **Sauvegarde maintenant**.

Pour créer une sauvegarde différentielle régulière de la base de données d'événements et purger les anciens événements :

1. Définissez le champ **Sélectionnez une option de sauvegarde** sur Chemin local, Chemin réseau ou FTP.
2. Saisissez le **Chemin de sauvegarde de la base de données des événements**. Si vous avez sélectionné FTP ci-dessus, vous devez saisir les paramètres FTP pertinents tels que **l'adresse IP** et le **numéro de port**.
3. Entrez les informations de **Purger les événements plus anciens que** et d'**Heure de début de purge** pour définir la durée pendant laquelle les événements seront conservés dans la base de données avant d'être purgés.
4. Activez **Générer une sauvegarde des événements différentiels**.

Pour plus de renseignements, consulter la Note d'application 279 : Créer et restaurer des sauvegardes différentielles dans Protege GX.

Effectuer des sauvegardes dans SSMS

La procédure suivante vous permet d'effectuer une sauvegarde de l'une ou l'autre base de données dans SQL Server Management Studio (SSMS). Les instructions peuvent différer légèrement selon la version de SSMS que vous utilisez.

1. Ouvrez SSMS et connectez-vous au serveur de Protege GX.
2. Développez le nœud **Bases de données**. Faites un clic droit sur le Base de données ProtegeGX ou ProtegeGXEvents et sélectionnez **Tasks > Back Up...**.
3. Si une sauvegarde a été créée précédemment, le fichier sera affiché dans le champ **Destination**. Si vous souhaitez utiliser ce fichier, cliquez sur l'onglet **Options multimédia** et indiquez si vous allez ajouter la sauvegarde actuelle au fichier existant ou remplacer le fichier existant.

   Pour sauvegarder dans un autre fichier, cliquez sur **Supprimer**. Cliquez ensuite sur **Ajouter...** pour saisir le nom et l'emplacement du nouveau fichier de sauvegarde. Cliquez sur **OK**.

   Le fichier de sauvegarde doit être au format .bak. Il est recommandé d'ajouter le numéro de version de la base de données au nom de fichier.
4. Cliquez sur **OK** pour effectuer la sauvegarde.

Restaurer des sauvegardes de la base de données

Il n'est pas possible de restaurer une sauvegarde de base de données dans Protege GX. Ces instructions montrent comment restaurer des sauvegardes à l'aide de SQL Server Management Studio (SSMS).

Avant de restaurer une base de données, sauvegardez votre base de données actuelle afin de pouvoir revenir à un point connu en cas de problème.

1. Si vous restaurez une base de données avec le cryptage transparent des données sur un Serveur différent, vous devez d'abord charger le certificat de cryptage sur le nouveau Serveur.

   Consultez Restauration des sauvegardes avec cryptage transparent des données pour obtenir les instructions
2. Vérifiez la version de la base de données que vous restaurez par rapport à la version actuelle du logiciel (**À propos | Version**).

   Si la version de la base de données est supérieure au troisième numéro de la version du logiciel, ne continuez pas (consultez la page 30).
3. Ouvrez le composant logiciel enfichable **Services** en suivant les étapes ci-après :
   - Appuyez sur les touches **Windows + R**
   - Tapez **services.msc** dans la barre de recherche et appuyez sur **Entrer**
4. Recherchez le Protege GX Update Service. Faites un clic droit sur le service et cliquez sur **Arrêter**. Cela arrête également les autres services Protege GX.
5. Ouvrez SSMS et connectez-vous à l'instance Protege GX.
6. Développez le nœud **Bases de données**. Faites un clic droit sur la base de données ProtegeGX ou ProtegeGXEvents et sélectionnez **Tâches > Restaurer > Base de données...**.
7. Réglez la **Source** sur **Appareil**, puis cliquez sur le bouton d'ellipse **[...]**.
8. Cliquez sur **Ajouter** pour naviguer vers le fichier de sauvegarde (.bak) que vous allez restaurer. Cliquez sur **OK**.
9. La section **Plan de restauration** affiche le(s) jeu(x) de sauvegarde disponible(s) pour la restauration. S'il y en a plus d'un, utilisez la date de sauvegarde pour déterminer celui qui doit être restauré, puis cochez la case **Restaurer** à côté du jeu de sauvegarde sélectionné.
10. Dans l'onglet **Options**, activez l'option **Écraser la base de données existante**.
11. Cliquez sur **OK** pour lancer le processus de restauration.
12. Si la version de la base de données que vous avez restaurée est antérieure à la version actuelle du logiciel, elle doit être mise à niveau avant que les services ne démarrent. Désinstallez et réinstallez Protege GX pour mettre à jour la base de données.
13. Dans le snap-in **Services**, faites un clic droit sur le Protege GX Data Service et cliquez sur **Commencer**. Si le service de données (data service) démarre, la restauration de la base de données a réussi.

Le démarrage du service de données démarre également le service d'événements et le service de mise à jour; toutefois, le service de téléchargement doit être démarré manuellement. Il est recommandé de vérifier la configuration avant de lancer le service de téléchargement, car celui-ci commencera à télécharger la programmation vers les contrôleurs.

Restauration des sauvegardes avec cryptage transparent des données

Lorsqu'une base de données a un Cryptage transparent des données (CTD) activé, toutes les sauvegardes de cette base de données sont également chiffrées. Si vous devez restaurer la base de données sur un autre serveur, vous devez d'abord créer une clé principale de base de données (DMK) et ajouter le certificat de sauvegarde au nouveau serveur.

Avant de commencer, vous aurez besoin du certificat, de la clé privée et du mot de passe utilisé pour chiffrer la clé privée. Si vous ne disposez pas de sauvegardes de ceux-ci, vous pouvez les exporter à partir du serveur d'origine.

1. Sur le serveur d'origine, cliquez sur **Nouvelle requête** et saisissez la requête suivante :

```
BACKUP CERTIFICATE TDECertificate TO FILE = 'c:\storedcerts\TDE
Certificate'
    WITH PRIVATE KEY ( FILE = 'c:\storedkeys\TDE Key' ,
    ENCRYPTION BY PASSWORD = '<UseAStrongPasswordHere>' );
GO
```

2. Cliquez sur **Exécuter**. SQL Server va exporter les fichiers de certificat et de clé privée aux emplacements spécifiés.

Vous devez sauvegarder le certificat, la clé privée et le mot de passe utilisé pour chiffrer la clé privée dans un emplacement sécurisé. Si vous les perdez, il ne sera pas possible de restaurer les sauvegardes de la base de données sur un autre serveur.

3. Transférez les fichiers vers le nouveau serveur.

Vous devrez ensuite créer une clé principale de base de données et un certificat sur le nouveau serveur.

1. Ouvrir SQL Server Management Studio (SSMS) et se connecter à l'instance Protege GX en tant qu'utilisateur administrateur.
2. Cliquez sur **Nouvelle requête**.
3. Saisissez la requête suivante :

```
USE master;
GO
CREATE MASTER KEY ENCRYPTION BY PASSWORD = '<UseStrongPasswordHere>';
GO
CREATE CERTIFICATE TDECertificate
    FROM FILE = 'c:\storedcerts\TDE Certificate.cer'
    WITH PRIVATE KEY (FILE = 'c:\storedkeys\TDE Key.pvk',
    DECRYPTION BY PASSWORD = '<EnterPrivateKeyPasswordHere>');
GO
```

4. Cliquez sur **Exécuter**. Le certificat sera téléchargé sur le serveur et chiffré à l'aide de la clé principale de base de données.
5. Restaurez les sauvegardes de la base de données comme en temps normal, en suivant les instructions dans Restaurer des sauvegardes de la base de données.

Visualisation du statut de santé du contrôleur

La fonction **Obtenir le statut** de santé fournit des détails sur le statut général du système et peut être utile pour identifier les zones problématiques qui doivent être traitées.

Voir le statut de santé

1. Allez vers **Sites | Contrôleurs**.
2. Cliquez avec le bouton droit de la souris sur le contrôleur et choisissez **Obtenir le statut de santé**.
3. La **fenêtre de statut du contrôleur** apparaît, indiquant toutes les partitions qui doivent être adressées.

   Si la demande de statut échoue, il se peut qu'il y ait un problème de connexion entre le contrôleur et le serveur. Voir plus loin.

Dépannage de la connectivité du contrôleur

La section suivante fournit des étapes de dépannage utiles pour les situations où le contrôleur et le serveur ne communiquent pas.

Pour une démonstration, voir la section Mise d'un contrôleur Protege GX en ligne sur la chaîne ICT YouTube.

Exigences en matière de communication

Pour que le serveur et le contrôleur puissent communiquer, les éléments suivants sont nécessaires :

1. Le contrôleur doit être physiquement mis en réseau avec le serveur, ou connecté via le Web.
2. Les Protege GX services doivent être en cours d'exécution.
3. Le serveur doit disposer de l'adresse IP correcte pour le contrôleur.
4. Le serveur doit disposer du numéro de série correct du contrôleur pour identifier correctement les messages entrants en provenance de celui-ci.
5. L'adresse IP et le port du serveur d'événements doivent être correctement définis sur le contrôleur (port 22 000 par défaut).
6. Le contrôleur doit être joignable sur les ports de téléchargement et de contrôle (ports 21 000 et 21 001 par défaut).
7. Protege GX doit avoir le nom de l'ordinateur correctement configuré pour les serveurs de téléchargement et d'événements.
8. Le logiciel Protege GX et les bases de données doivent avoir la même version de base de données.
9. Le chiffrement doit être soit désactivé aux deux extrémités, soit activé aux deux extrémités avec la bonne clé de chiffrement.

Vérifier que les services sont en cours d'exécution

La première et la plus simple chose à vérifier, est que les services Protege GX fonctionnent.

1. Ouvrez le composant logiciel enfichable **Services** en suivant les étapes ci-après :
   - Appuyez sur les touches **Windows + R**
   - Tapez **services.msc** dans la barre de recherche et appuyez sur **Entrer**
2. Faire défiler jusqu'aux services Protege GX. Assurez-vous que les services suivants sont en cours d'exécution :
   - Protege GX Service des données
   - Protege GX Service de téléchargement
   - Protege GX Service d'événement
   - Protege GX Service de mise à jour
3. Si un service n'est pas en cours d'exécution, faites un clic droit dessus et cliquez sur **Démarrer**.

Si certains services ne démarrent pas, il peut y avoir un autre problème avec votre installation. Par exemple, la version de la base de données peut être incompatible (consultez la page 40).

Confirmer l'adresse IP du contrôleur

Pour que le serveur puisse communiquer avec le contrôleur, il doit avoir programmé l'adresse IP correctement et être en mesure d'atteindre cette adresse IP.

1. Dans Protege GX, naviguer vers **Sites | Contrôleurs**.
2. Dans l'onglet **Général**, mettre en évidence et copier (CTRL + C) **l'adresse IP**.

3. Coller (CTRL +V) l'adresse IP dans la barre d'adresse d'un navigateur web sur le serveur, avec le préfixe https:// (par exemple https://192.168.1.2).

   Il est possible qu'un avertissement relatif à la sécurité du certificat vous soit présenté à la connexion.

4. Si vous ne pouvez pas vous connecter, supprimez le préfixe https:// et réessayez (par exemple 192.168.1.2), car votre contrôleur n'est peut-être pas configuré pour HTTPS.
5. Si le contrôleur est accessible à l'aide de cette adresse IP, un écran de connexion simple s'affiche.
6. Connectez-vous au contrôleur en utilisant les informations d'identification de l'administrateur.

Si vous ne parvenez pas à naviguer sur le site du contrôleur, il se peut que vous n'ayez pas la bonne adresse IP. Si l'adresse IP est inconnue, vous devrez la consulter/modifier à partir d'un clavier ou définir par défaut l'adresse IP du contrôleur (voir ci-dessous).

Si vous avez l'adresse IP correcte, il est probable que vous ayez un problème de réseau. Assurez-vous que le serveur et le contrôleur sont sur le même sous-réseau ou que la redirection de port est correctement configurée sur le routeur.

A partir de la version 2.08.911 du micrologiciel, la fonction "ping" est désactivée par défaut. Si le contrôleur reçoit des téléchargements, vous pouvez autoriser le ping en ajoutant la commande **`EnablePing = true`** dans les commandes du contrôleur.

Configuration de l'adresse IP à partir d'un clavier

Si l'adresse IP actuelle du contrôleur est inconnue, elle peut être visualisée et modifiée à l'aide d'un clavier Protege.

1. Connectez le clavier au réseau du module.
2. Connectez-vous au clavier à l'aide d'un code installateur valide. Le code d'installation par défaut est 000000.

   Si le code par défaut a été modifié et que vous ne connaissez pas les nouveaux codes, vous devrez réinitialiser le contrôleur (voir la section Réinitialisation du contrôleur dans ce document) pour réinitialiser le code.

   Notez que cette opération efface **toutes** les programmations existantes et établit le code installateur.

3. Une fois connecté, sélectionnez le **Menu 4** (Menu Installation) puis le **Menu 2** (Menu IP) et affichez ou modifiez l'adresse IP, le masque de réseau et la passerelle selon vos besoins.

Une fois les paramètres modifiés, vous devez les enregistrer en appuyant sur les touches **[Arm]**. Vous serez invité à confirmer les modifications en appuyant sur **[Enter]**. Vous devez ensuite redémarrer le contrôleur, soit par le menu **[4], [2], [2]** soit par une mise sous tension, pour que les réglages prennent effet.

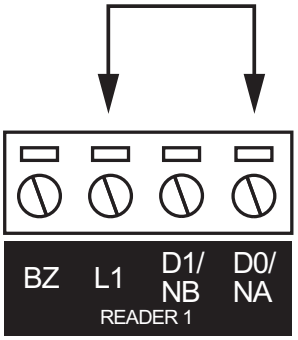
Définir l'adresse IP par défaut

Si l'adresse IP actuellement configurée est inconnue, elle peut être temporairement réglée sur 192.168.111.222 afin que vous puissiez vous connecter à l'interface Web pour la voir et/ou la changer. Cela désactivera également temporairement la sécurité HTTPS, ce qui pourrait résoudre certains problèmes de connexion.

Cette option définit par défaut l'adresse IP tant que l'alimentation est en cours, mais ne sauvegarde pas le changement en permanence. Une fois que le lien est enlevé et que l'alimentation est rétablie sur l'unité, l'adresse IP configurée est utilisée.

Définir l'adresse IP par défaut d'un contrôleur 2 portes

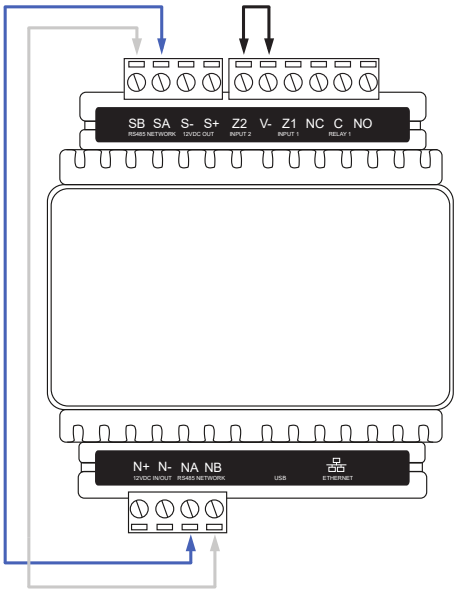
1. Enlevez l'alimentation du contrôleur en débranchant l'entrée 12 V CC.
2. Attendez jusqu'à ce que l'indicateur d'alimentation soit off.
3. Connectez un lien filaire entre le **Lecteur 1** entrée D0 et le **Lecteur 1** sortie L1.



4. Allumez l'alimentation du contrôleur. Attendez que l'indicateur d'état commence à clignoter de façon continue.

Définir l'adresse IP par défaut d'un contrôleur 1 porte

1. Enlevez l'alimentation du contrôleur en débranchant l'entrée 12 V CC.
2. Attendez jusqu'à ce que l'indicateur d'alimentation soit off.
3. Connectez un lien filaire entre **NA** du réseau de modules et **SA** du réseau de lecteurs, et entre **NB** du réseau de modules et **SB** du réseau de lecteurs.
4. Connectez **Entrée 2** à la terre.



5. Allumez l'alimentation du contrôleur. Attendez que l'indicateur d'état commence à clignoter de façon continue.

Accéder au contrôleur

6. Lorsque le contrôleur commence à fonctionner, il utilise les paramètres temporaires suivants :
   - **Adresse IP** : 192.168.111.222
   - **Masque de sous-réseau** : 255.255.255.0
   - **Passerelle** : 192.168.111.254
   - **DHCP** : Désactivé
   - **Utiliser HTTPS** : Désactivé
7. Connectez-vous au contrôleur en tapant http://192.168.111.222 dans la barre d'adresse de votre navigateur web, puis vue ou modifiez l'addresse IP et les autres paramètres réseau selon vos besoins.

N'oubliez pas de changer le sous-réseau de votre PC ou de votre ordinateur portable pour qu'il corresponde au sous-réseau du contrôleur.

8. Enlevez le(s) lien(s) filaire(s) et mettez encore le contrôleur sous tension.
   Le contrôleur va maintenant utiliser les paramètres réseau configurés.

Confirmer le numéro de série du contrôleur

Les messages entrants du contrôleur vers le serveur sont identifiés par le numéro de série du contrôleur.

1. Dans l'interface web du contrôleur, naviguez vers la page **Paramètres**.
2. Mettez en évidence et copier le **numéro de série**.
3. Dans Protege GX, naviguez vers **Sites | Contrôleurs | Général** .
4. Collez dans le champ du **numéro de série**.

Dupliquer une adresse IP ou un numéro de série

Bien que le logiciel vous avertisse, il est possible d'enregistrer deux contrôleurs avec la même IP ou le même numéro de série. Dans ce cas, le contrôleur créé en premier est prioritaire.

- Assurez-vous de ne pas avoir créé un contrôleur avec une adresse IP ou un numéro de série en double. Vérifiez tous vos sites.
- Si vous avez créé un site pour les modèles, ceux-ci ne doivent pas avoir d'adresse IP ni de numéro de série.

Si votre serveur comporte deux contrôleurs ayant la même adresse IP ou le même numéro de série, il y aura des problèmes de communication avec au moins l'un d'entre eux.

Confirmer le fonctionnement du serveur d'événement

Pour confirmer que le serveur d'événement fonctionne et émet sur le bon port pour les événements entrants, ouvrez la fenêtre de diagnostic du serveur d'événement.

1. Dans Protege GX, naviguez vers **Sites | Contrôleurs | Général** et agrandir la section **Fenêtres de diagnostic**.
2. Sélectionnez **Ouvrir la fenêtre de diagnostic du serveur d'événement**. Vous devriez voir un message indiquant "Écoute sur le port : 22000".

   Le port par défaut du serveur d'événement est **22000**, mais il peut être modifié dans **Global | Serveurs d'événement** .
3. Si la fenêtre de diagnostic du serveur d'événements affiche des messages concernant un numéro de série inconnu, les événements sont reçus d'un contrôleur dont le numéro de série figure dans le message. Cela signifie également que le serveur d'événements accepte les événements entrants.
4. Dans l'interface web du contrôleur, assurez-vous que le **Port d'événement** correspond au port défini dans Protege GX.
5. Si vous modifiez le port d'événement, vous devez **sauvegarder** et **redémarrer le contrôleur** à l'aide des icônes en haut à droite pour que vos modifications soient prises en compte.

Si la fenêtre de diagnostic du serveur d'événement ne contient aucun texte, il y a un problème avec la configuration du serveur d'événement. Cela signifie que le serveur d'événement **n'accepte pas** les événements entrants. Ce problème peut parfois être résolu en redémarrant le Service d'événement Protege GX :

1. Ouvrez le composant logiciel enfichable **Services** en suivant les étapes ci-après :
   - Appuyez sur les touches **Windows + R**
   - Tapez **services.msc** dans la barre de recherche et appuyez sur **Entrer**
2. Localisez le Protege GX Service d'événement. Cliquez droit sur le service et sélectionnez **Redémarrer**.

Confirmer l'adresse IP du serveur d'événements

Pour que les messages puissent passer du contrôleur au serveur, le contrôleur doit avoir l'adresse IP correcte du serveur d'événements.

1. Sur le serveur ordinateur, ouvrez une invite de commande. Entrez la commande **`ipconfig`** et cliquez **[Enter]** .
2. On vous indiquera le statut et les détails du serveur sur différents sous-réseaux. Localisez et copiez **l'adresse IPv4** du sous-réseau auquel le contrôleur est connecté.

   Pour les réseaux plus complexes, il peut être préférable d'ouvrir une invite de commande sur une machine à laquelle le contrôleur est directement connecté et d'utiliser la commande **`ping`** pour vérifier l'adresse IP externe du serveur.
3. Dans l'interface web du contrôleur, sur la page **Paramètres**, vérifiez que l'adresse IP du **serveur d'événement 1** est correcte. Collez l'adresse située ci-dessus si elle ne correspond pas.

   Il y a trois espaces pour saisir l'IP du serveur d'événement. Ceci est pour les situations où les contrôleurs ont plusieurs chemins vers le serveur. Dans la plupart des cas, les deuxième et troisième adresses IP du serveur d'événement doivent être laissées avec des zéros ou des 255.

Confirmer les ports

Ensuite, assurez-vous que les ports de téléchargement et de contrôle définis sur le serveur correspondent à ceux définis dans l'interface du contrôleur.

1. Dans Protege GX , naviguez vers **Sites | Contrôleurs | Général** et vérifiez ces valeurs :
   - **Port de téléchargement** (par défaut 21000)
   - **Port de demande de contrôle et d'état** (par défaut 21001)
2. Dans l'interface web du contrôleur, sur la page **Paramètres**, assurez-vous que le **port de téléchargement** et le **port de contrôle** correspondent à ceux définis dans le logiciel.
3. Si vous avez modifié des paramètres sur le contrôleur, enregistrez vos modifications et redémarrez le contrôleur pour que les changements prennent effet.

Vérifier le nom de l'ordinateur

Les serveurs de téléchargement et d'événement doivent avoir un nom d'ordinateur exact qui correspond à la machine du serveur. En général, cela ne change que lorsque vous avez restauré une base de données à partir d'un autre ordinateur.

IMPORTANT : Le nom de l'ordinateur ne doit pas dépasser **15 caractères**, sinon les téléchargements échoueront.

1. Sur l'ordinateur serveur, ouvrez le **Panneau de configuration > Tous les éléments du panneau de configuration > Système** pour afficher l'information de l'ordinateur.
2. Copiez le **nom de l'ordinateur**.
3. Dans Protege GX, naviguez jusqu'à **Global | Serveur de téléchargement** et vérifiez que le **Nom de l'ordinateur** correspond au nom de la machine serveur. Si les noms ne correspondent pas, collez le nom copié précédemment.
4. Naviguez vers **Global | Serveur d'événement** et vérifiez et corrigez à nouveau le **Nom de l'ordinateur**.
5. Si vous avez changé le nom de l'ordinateur pour l'un ou l'autre des serveurs, vous devez redémarrer le service correspondant.

Ouvrez le composant logiciel enfichable **Services** en suivant les étapes ci-après :

- Appuyez sur les touches **Windows + R**
- Tapez **services.msc** dans la barre de recherche et appuyez sur **Entrer**

6. Localisez les services Protege GX. Cliquez avec le bouton droit de la souris sur le service de téléchargement et/ou le service d'événement et cliquez sur **Redémarrer**.

Réparer la compatibilité de la base de données

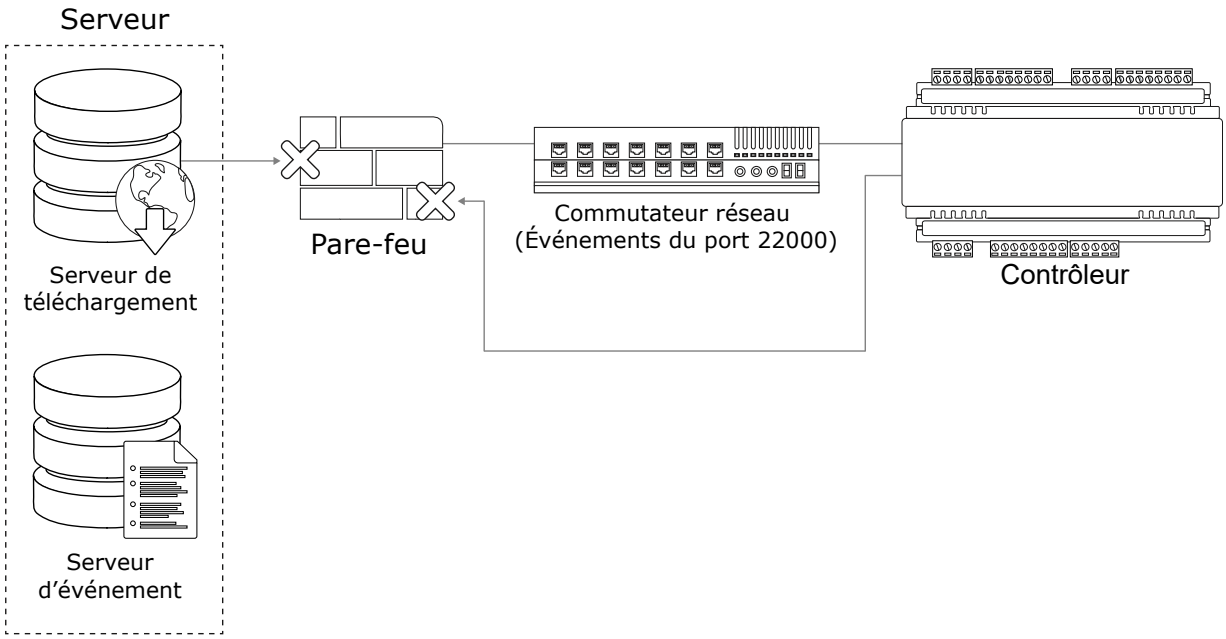
Si vous avez restauré une base de données à partir d'une ancienne version de Protege GX, il peut y avoir un décalage entre les versions du logiciel et de la base de données. Dans ce cas, le Service de données de Protege GX ne pourra pas démarrer, les fenêtres de diagnostic du serveur d'événements et de téléchargement resteront vides, et aucun téléchargement ne sera transmis au contrôleur.

Pour résoudre ce problème, vous devez **désinstaller et réinstaller** Protege GX. Cela déclenchera une mise à jour de la base de données.

Une sauvegarde effectuée à partir d'une version plus récente de Protege GX ne peut pas être restaurée vers une version plus ancienne.

Pare-feu Windows

Lorsque le contrôleur et le serveur se trouvent sur le même réseau local, le seul endroit où un pare-feu peut bloquer des messages est sur le serveur de la machine elle-même. C'est ce qu'on appelle le pare-feu Windows.



1. Ouvrez les paramètres du Pare-feu Windows dans **Panneau de contrôle > Tous les items du panneau de contrôle > Pare-feu Windows**. Si le pare-feu est activé, il est affiché en vert.
2. Pour éliminer le Pare-feu Windows comme cause des problèmes de communication, désactivez-le temporairement en cliquant **sur ON ou Off** sur le Défenseur Windows à gauche de l'écran. Désactivez le pare-feu pour chaque emplacement du réseau.

   Vérifiez si cela résout le problème. Si c'est le cas, vous pouvez réactiver le Pare-feu et autoriser les services Protege GX à travers le Pare-feu.
3. Cliquez sur le lien **Permettre une application ou une fonctionnalité via le pare-feu Windows Defender**, à gauche de l'écran.

Les logiciels antivirus ou pare-feu tiers peuvent empêcher la modification des règles du Pare-feu Windows. Si tel est le cas, consultez le fabricant tiers pour plus de détails sur l'autorisation des programmes à travers le pare-feu.

4. Sélectionnez **Permettre une autre application...** pour ajouter un programme en tant qu'exception.
5. Cliquez sur **Naviguer**, puis naviguez jusqu'au répertoire d'installation de Protege GX.

   Le répertoire d'installation par défaut est C:\Programmes (x86)\Integrated Control Technology\Protege GX.

6. Sélectionnez (double-cliquez ou sélectionner et **Ouvrir**) l'exécutable que vous voulez autoriser, puis cliquez sur **Ajouter** .

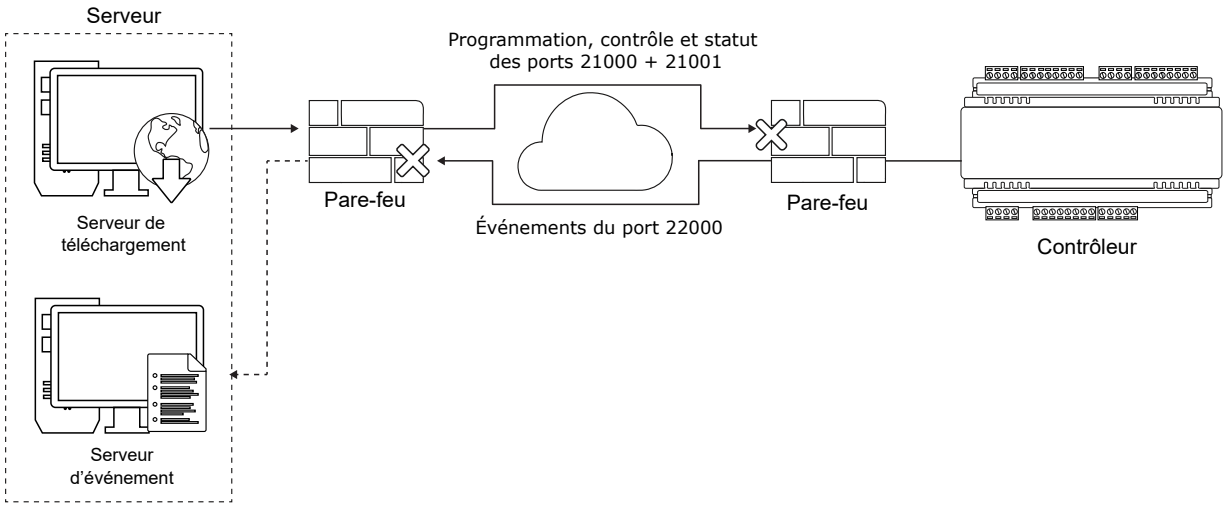
   Ajoutez les exécutables Protege GX suivants, un par un :
   - GXSV.exe
   - GXSV2.exe
   - GXSV3.exe
   - GXPI.exe
   - GXEvtSvr.exe
   - GXDVR1.exe
   - GXDVR2.exe

   Cela permet aux services nécessaires Protege GX d'accéder à travers le pare-feu Windows.

   Le processus ci-dessus n'autorisera l'accès qu'à travers votre connexion réseau principale. Si plusieurs réseaux sont connectés, vous devrez autoriser manuellement l'accès (en cochant la case dans la colonne réseau) pour chaque réseau supplémentaire auquel l'exécutable Protege GX doit accéder.

Plusieurs pare-feux

Il peut y avoir plusieurs pare-feux sur les réseaux d'entreprise.

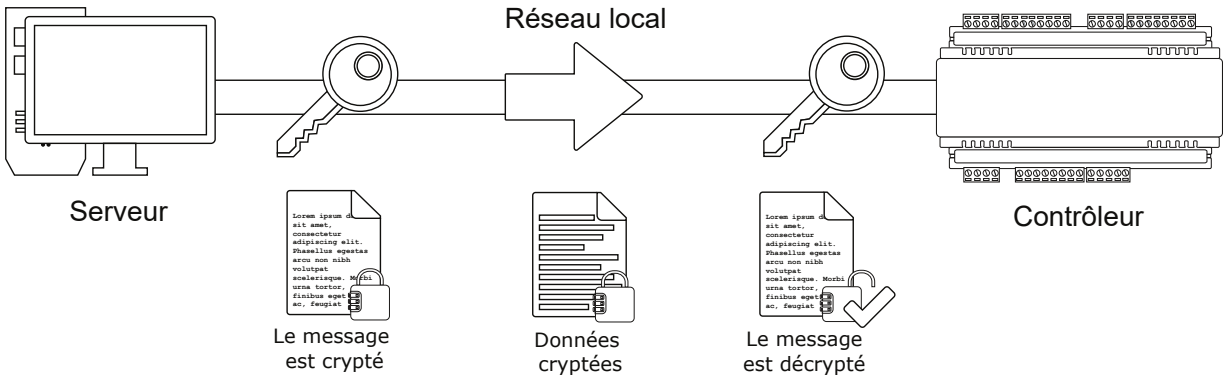


Pour s'assurer que ces derniers sont configurés correctement, fournissez le Guide de l'administrateur réseau Protege GX au membre du personnel informatique approprié. Ce document est inclus dans le paquet d'installation du logiciel.

Cryptage

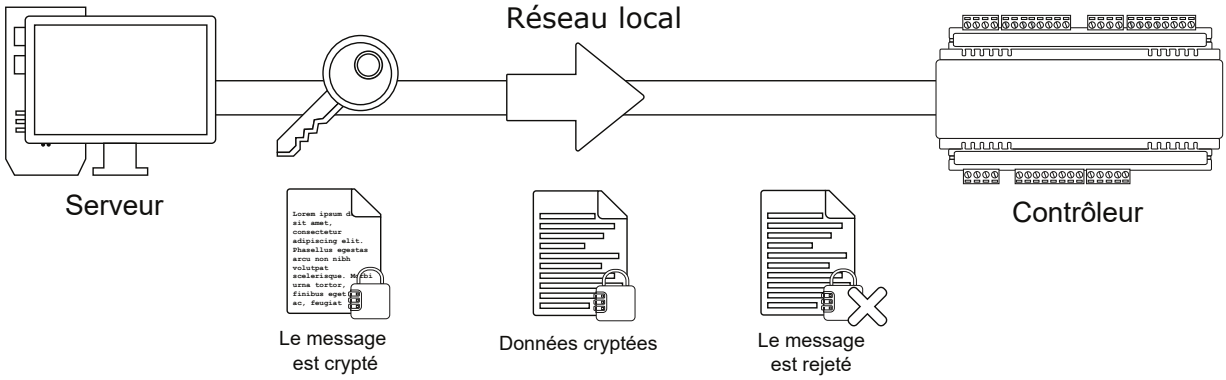
Cryptage du serveur et du contrôleur activé

Le cryptage repose sur une clé partagée que l'expéditeur et le destinataire d'un message connaissent tous deux. Le message est crypté à l'aide de la clé, puis décrypté par le destinataire à l'aide de cette même clé. Si le message est intercepté, il n'a aucun sens pour quiconque ne dispose pas de la clé de cryptage.



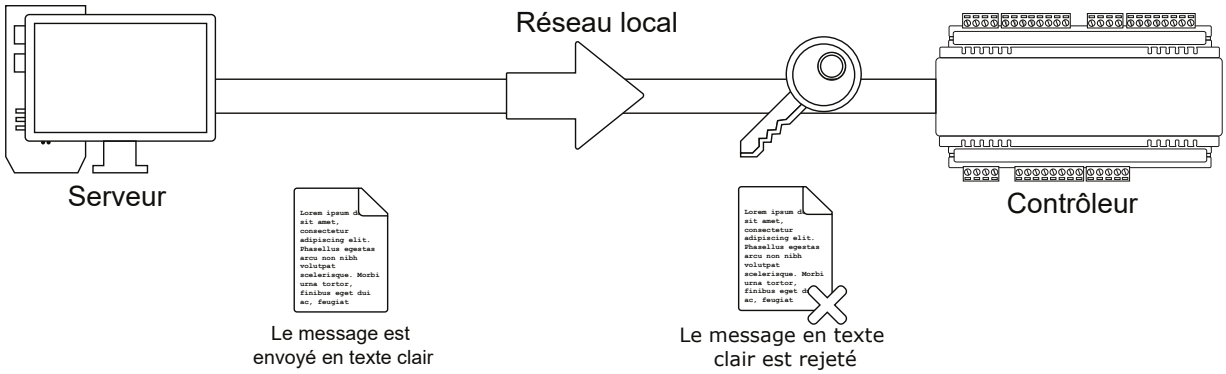
Serveur activé, contrôleur désactivé

Si le destinataire perd la clé, il ne peut pas décrypter les messages entrants. Dans ce cas, le message est rejeté.



Serveur désactivé, contrôleur activé

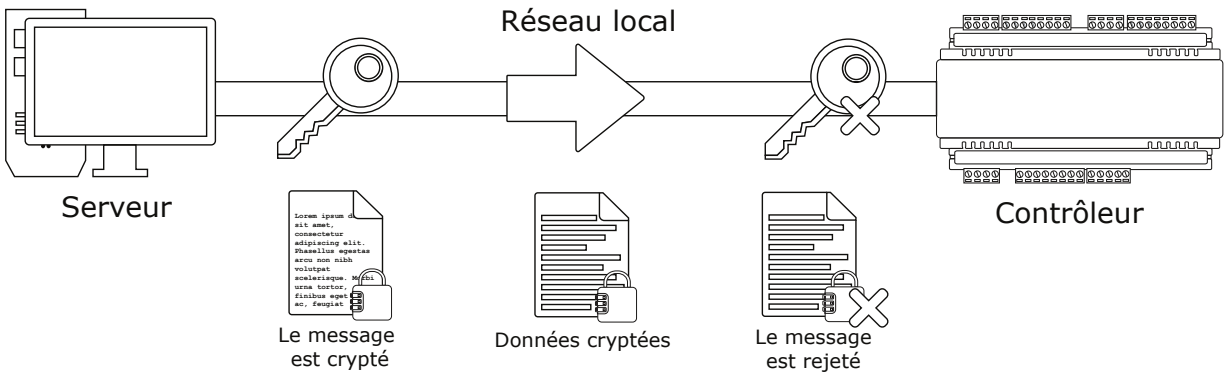
Si l'expéditeur perd la clé, le message est envoyé en texte clair. Le destinataire, qui s'attend à recevoir des événements chiffrés, rejette également le message car il peut être de nature malveillante.



Serveur et contrôleur avec des clés de cryptage différentes

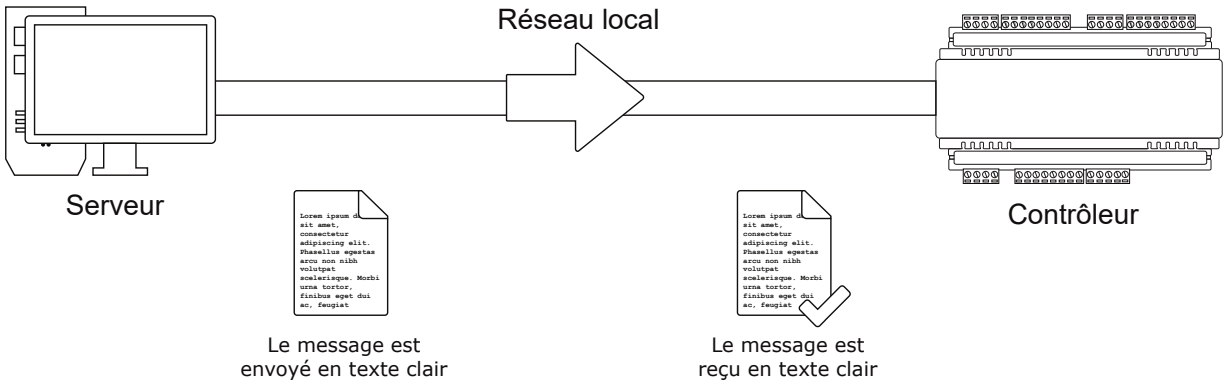
Si l'expéditeur et le destinataire ont des clés différentes, le message ne peut pas être décrypté par le destinataire. Cela entraîne également le rejet des messages entrants par le destinataire.

Une nouvelle clé de cryptage est générée chaque fois que le cryptage est activé sur le serveur. Chaque contrôleur possède une clé unique, indépendante de tous les autres contrôleurs. La clé est modifiée si le cryptage d'un contrôleur est désactivé, puis réactivé. Si le cryptage d'un contrôleur est désactivé sur le serveur, le contrôleur doit être défini par défaut. Il n'est pas possible de réactiver le cryptage sans d'abord définir le contrôleur par défaut.



Cryptage du serveur et du contrôleur désactivé

Si le cryptage est désactivé à la fois chez l'expéditeur et le destinataire, les messages reçus sont acceptés. L'inconvénient de ce scénario est que toute personne « écoutant » entre l'expéditeur et le destinataire peut également recevoir les messages.



Désactiver le cryptage

Définir le contrôleur par défaut est le seul moyen de supprimer la clé de cryptage. Il s'agit d'un dispositif de sécurité. Cela signifie que l'accès physique au contrôleur doit être obtenu avant de pouvoir désactiver le cryptage.

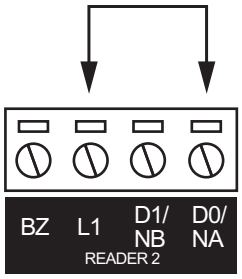
Si vous n'êtes pas sûr de l'état du cryptage du serveur ou du contrôleur, désactivez le cryptage sur le serveur, puis définissez le contrôleur par défaut. Cela permet de s'assurer que ni l'un ni l'autre n'est crypté et exclut cette possibilité comme cause des problèmes de communication. Le cryptage doit ensuite être réactivé une fois les communications établies.

Désactiver le cryptage sur le serveur

Si le contrôleur est défini par défaut, le cryptage doit être désactivé sur le serveur avant que les communications puissent être établies. Naviguez vers **Sites | Contrôleurs | Configuration** et cliquez sur **Désactiver cryptage du contrôleur**. Le logiciel vous avertit avant de désactiver le cryptage.

Définir un contrôleur 2 portes par défaut

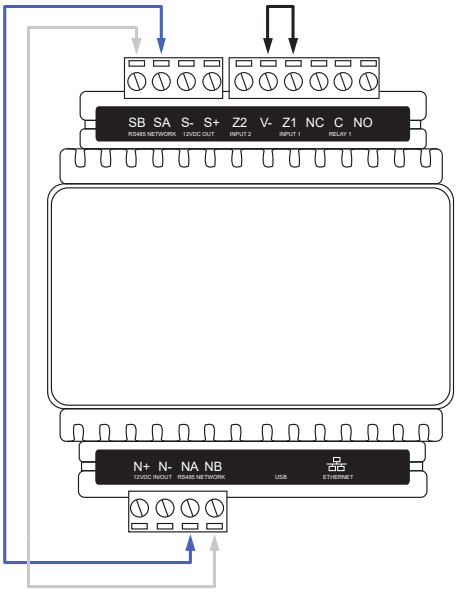
1. Enlevez l'alimentation du contrôleur en débranchant l'entrée 12 VCC.
2. Attendez jusqu'à ce que l'indicateur d'alimentation soit off.
3. Connectez un lien filaire entre le **lecteur 2** entrée D0 et le **lecteur 2** sortie L1.



4. Allumez l'alimentation du contrôleur. Attendez que l'indicateur d'état commence à clignoter de façon continue.
5. Retirez le lien filaire **avant d'effectuer tout changement dans la configuration du contrôleur**.

Définir un contrôleur 1 porte par défaut

1. Enlevez l'alimentation du contrôleur en débranchant l'entrée 12 VCC.
2. Attendez jusqu'à ce que l'indicateur d'alimentation soit off.
3. Connectez un lien filaire entre **NA** du réseau de modules et **SA** du réseau de lecteurs, et entre **NB** du réseau de modules et **SB** du réseau de lecteurs.
4. Connectez **l'entrée 1** à la terre.



5. Allumez l'alimentation du contrôleur. Attendez que l'indicateur d'état commence à clignoter de façon continue.
6. Retirez les liaisons filaires **avant d'apporter des modifications à la configuration du contrôleur**.

Le système sera désormais par défaut avec toute la programmation et les **paramètres système** ramenés à la configuration d'usine, y compris la réinitialisation de l'adresse IP et de toute la configuration du réseau, ainsi que la suppression de tous les registres des opérateurs.

- L'option par défaut du contrôleur réinitialise l'adresse IP sur l'adresse IP par défaut de 192.168.1.2.

  Les versions antérieures du micrologiciel du contrôleur ne réinitialisent pas l'adresse IP. Si le contrôleur n'est pas disponible sur 192.168.1.2, vous pourrez vous y connecter via son adresse IP précédente.
- Tous les paramètres configurés du système (par exemple, **la passerelle par défaut**, **le serveur d'événements**) sont réinitialisés à leurs valeurs par défaut.
- Tout certificat HTTPS personnalisé est enlevé et le certificat par défaut est réinstallé.

Les versions antérieures du contrôleur ne disposent pas d'un certificat HTTPS par défaut. Si le contrôleur n'est pas disponible via HTTPS, connectez-vous à lui via HTTP.

- Tous les registres des opérateurs sont enlevés et l'opérateur admin doit être recréé.
- Toute autre programmation est enlevée.

Après avoir défini un contrôleur par défaut

Avant d'apporter des modifications à la configuration du contrôleur ou de mettre à niveau le micrologiciel, **supprimez la liaison filaire utilisée pour configurer le contrôleur par défaut**.

Après l'option par défaut d'un contrôleur, un certain nombre d'étapes essentielles devront être effectuées pour reprendre un fonctionnement normal. Toutes les étapes suivantes ne seront pas forcément requises; tout dépend de la configuration de votre site :

1. Connectez-vous à l'interface Web du contrôleur en utilisant le protocole HTTPS, à moins qu'il ne s'agisse d'un contrôleur plus ancien ne disposant pas de certificat par défaut, auquel cas il se connectera en utilisant le protocole HTTP.
2. Recréez l'opérateur admin et connectez-vous à l'interface Web du contrôleur.

   Si vous n'êtes pas prompt à créer l'opérateur admin, le nom d'utilisateur par défaut est admin et le mot de passe est admin.

3. Réinitialisez l'adresse IP du contrôleur à sa valeur précédente.
4. Reconfigurez tous les paramètres supplémentaires du réseau.
5. Réinstallez les certificats HTTPS personnalisés installés précédemment.
6. Restaurez tous les autres paramètres système selon la configuration de votre site.

Telnet

Pour confirmer qu'il existe un chemin réseau entre le serveur et le contrôleur et que les ports corrects sont ouverts, vous pouvez vous connecter par telnet au contrôleur sur le port de téléchargement (par défaut, le port 21000).

1. Si la caractéristique Telnet n'est pas activée, ouvrez le **Panneau de configuration > Tous les éléments du panneau de configuration > Programmes et fonctionnalités**.
2. Cliquez sur **ON ou Off pour les caractéristiques de Windows** . Localisez **le client Telnet**, cochez la case suivante et cliquez sur **Ok**.
3. Ouvrez une commande prompte et essayez de vous connecter par telnet au contrôleur.

   Par exemple, saisissez la commande `telnet 192.168.1.2 21000`

   - Si le contrôleur peut accepter la connexion, un écran clair apparaît avec un curseur clignotant dans le coin supérieur gauche.
   - S'il n'y a pas de connexion, un message indique qu'il y a toujours un problème entre le serveur et le contrôleur. Si vous pouvez naviguer sur le réseau vers le contrôleur, il est probable qu'un pare-feu bloque la connexion quelque part.

Enfin, pour confirmer que le serveur d'événements est capable d'accepter des connexions, configurez un ordinateur portable avec les mêmes paramètres IP que le contrôleur.

1. Enlevez la fiche Ethernet du contrôleur et branchez-la sur votre ordinateur portable.
2. Essayez de vous connecter par telnet à l'adresse IP du serveur sur le port du serveur d'événements (22000 par défaut) :

   ```
   telnet 192.168.1.100 22000
   ```

- Si le serveur est en mesure d'accepter des connexions, l'écran clair et le curseur clignotant apparaissent.
- Si le serveur n'est pas joignable, un message indique qu'il y a encore un problème, indiquant qu'un pare-feu bloque le port 22000 vers le serveur.

Menu global

Les paramètres qui s'appliquent au fonctionnement de l'ensemble du système Protege GX sont regroupés dans le menu **Global** pour un accès facile.

Accueil

La page d'accueil s'affiche lorsque vous vous connectez pour la première fois et vous permet d'afficher les détails de l'opérateur, ainsi que de modifier votre mot de passe d'opérateur.

Détails de l'opérateur

- **Connecté en tant que** : Affiche le nom de l'opérateur actuellement connecté.
- **Connecté le** : Affiche la date et l'heure de votre connexion.

Options

- **Site actuel** : Affiche le site en cours de consultation. Les registres associés à ce site seront affichés par défaut sur les pages de programmation et dans le navigateur du système.
- **Thème de l'affichage** : Choisir entre deux thèmes d'affichage pour l'interface Protege GX : Clair (fond blanc, texte gris foncé) et Sombre (fond gris foncé, texte clair). Le thème d'affichage est sauvegardé pour chaque opérateur individuel sur chaque poste de travail.
- **Changer la couleur de l'affichage** : Choisir le thème de couleur qui sera affiché pour les menus, les en-têtes et les autres éléments de l'interface utilisateur. La couleur d'affichage est sauvegardée pour chaque opérateur individuel sur chaque poste de travail.
- **Se déconnecter** : Ferme la session Protege GX, vous déconnecte et vous ramène à l'écran de connexion.
- **Changer le mot de passe** : Ouvre une fenêtre vous permettant de modifier votre mot de passe opérateur.

Paramètres globaux

La page des paramètres globaux permet de configurer les paramètres qui s'appliquent à l'ensemble du système Protege GX.

Paramètres globaux | Général

Base de données principale

- **Version de base de données principale** : Numéro de version de la base de données actuelle (lecture seulement).
- **Sauvegarder changements de champs pour vérifier le journal** : Il s'agit d'une option héritée qui n'a aucun effet.
- **Formatage auto du nom d'affichage de l'utilisateur** : Détermine le nom d'affichage Protege GX par défaut pour les nouveaux registres d'utilisateurs. Lorsque vous saisissez le nom et le prénom d'un nouvel utilisateur, le champ **Nom** est rempli automatiquement en fonction du format sélectionné ici. Les options sont :
  - **Ne pas formater le nom d'affichage**
  - **Format court** (première initiale, nom de famille)
  - **Format court inversé** (nom de famille, première initiale)
  - **Format long** (premier nom, surnom)
  - **Format long inversé** (nom de famille, premier nom)

  Ce champ s'applique uniquement aux nouveaux utilisateurs créés par le biais de la programmation **Utilisateurs | Utilisateurs**. Cela n'affecte pas les noms d'affichage des utilisateurs existants.
- **Cryptage des NIP de l'utilisateur** : Activez cette option pour crypter de façon permanente les NIP de l'utilisateur dans la base de données Protege GX. Cela a les effets suivants :
  - Les opérateurs ne peuvent plus voir les NIP de l'utilisateur.
  - Les NIP de l'utilisateur peuvent uniquement être générés de manière aléatoire (pas de saisie manuelle).
  - Les NIP générés de façon aléatoire sont à usage unique. Lors de sa prochaine connexion à un clavier, l'utilisateur est invité à modifier son NIP.

  Avertissement : Le cryptage du NIP est permanent et ne peut être annulé que par la restauration d'une sauvegarde antérieure de la base de données.

  Pour plus de renseignements, consulter la Note d'application 306 : Cryptage du NIP de l'utilisateur et gestion avancée du NIP dans Protege GX.

Base de données d'événements

- **Purger les événements plus anciens que** : Sélectionnez la durée maximale de conservation des événements dans la base de données d'événements avant qu'ils ne soient supprimés (purgés). La valeur par défaut est de 1 an, mais les sites les plus fréquentés peuvent exiger que la base de données soit purgée plus fréquemment afin de s'assurer qu'il y a toujours de l'espace disponible pour les nouveaux événements.
- **Heure de début de purge** : Détermine l'heure à laquelle, chaque jour, les anciens événements sont supprimés (purgés) de la base de données.
- **Sauvegarder les événements de l'opérateur à la base de données des événements** : Lorsque cette option est activée, un événement est créé chaque fois qu'un registre est ajouté, modifié ou supprimé par un opérateur.

  Cette option est activée par défaut mais peut être désactivée pour réduire le nombre d'événements enregistrés dans la base de données d'événements.

- **Sauvegarder les événements de connexion échouée de l'opérateur à la base de données des événements** : Lorsque cette option est activée, un événement est créé chaque fois qu'une tentative de connexion au logiciel échoue. Cela vous permet de détecter et de signaler les problèmes de sécurité potentiels, tels que les attaques visant à deviner le mot de passe d'un opérateur.
- **Générer une sauvegarde des événements différentiels** : Lorsque cette option est activée, une sauvegarde différentielle de la base de données des événements est créée chaque fois que des événements sont purgés. Cette sauvegarde contient uniquement les événements qui ont été purgés, de sorte qu'ils peuvent être restaurés pour être consultés à une date ultérieure.

  Les sauvegardes seront créées sous forme de fichiers .bak dans le répertoire spécifié dans le **chemin de sauvegarde** (sous **Sauvegarde de la base de données principale** ci-dessous). Chaque nom de fichier est suivi du jour de la semaine où la sauvegarde a eu lieu. Si un fichier de sauvegarde portant ce nom existe déjà, les événements récemment purgés sont ajoutés au fichier existant.

  Pour plus de renseignements, consultez la Note d'application 279 : Sauvegardes différentielles dans Protege GX.

Sauvegarde base de données principale

- **Sauvegarder base de données principale tous les soirs** : Sélectionnez cette option pour sauvegarder automatiquement la base de données de programmation chaque jour à minuit. Les nouvelles sauvegardes écraseront les sauvegardes existantes portant le même nom.
- **Annexer le jour de la semaine au nom du fichier de sauvegarde** : Paramètre facultatif qui ajoute le jour de la semaine au nom du fichier de sauvegarde de la base de données principale. Cela permet au système de conserver une semaine de sauvegardes de la programmation.
- **Chemin de sauvegarde** : Le répertoire où les sauvegardes de la base de données principale sont créées. Si ce champ est laissé vide, les sauvegardes sont créées dans l'emplacement par défaut du serveur SQL.

  Lorsque vous définissez un chemin de sauvegarde, assurez-vous que le répertoire sélectionné existe déjà sur la machine serveur. Ne sélectionnez pas un répertoire qui refuse l'accès en écriture à SQL Server, tel que Program Files, Program Data, Users, Windows, etc.

- **Sauvegarde maintenant** : Cliquez pour effectuer une sauvegarde immédiate de la base de données de programmation. Le fichier .bak est généré dans le répertoire indiqué par le **Chemin de sauvegarde**, et inclut la version actuelle de la base de données Protege GX dans le nom du fichier.

Sauvegarde de la base de données des événements

- **Sélectionnez une option de sauvegarde** : Les sauvegardes de la base de données des événements peuvent être enregistrées sur le disque local, un lecteur réseau ou un emplacement FTP. Si vous sélectionnez FTP, vous devez saisir les informations suivantes :
  - Adresse IP
  - Numéro de port
  - Chemin du certificat (si l'authentification est requise)
  - Nom d'utilisateur
  - Mot de passe
- **Chemin de sauvegarde de la base de données des événements** : Le répertoire où les sauvegardes de la base de données d'événements sont sauvegardées. Cela inclut les sauvegardes différentielles (voir **Générer une sauvegarde des événements différentiels** ci-dessus).

  Lorsque vous définissez un chemin de sauvegarde, assurez-vous que le répertoire sélectionné existe déjà sur la machine serveur. Ne sélectionnez pas un répertoire qui refuse l'accès en écriture à SQL Server, tel que Program Files, Program Data, Users, Windows, etc.

- **Sauvegarde maintenant** : Cliquez pour effectuer une sauvegarde immédiate de la base de données des événements. Le fichier .bak est généré dans le répertoire indiqué par le **Chemin de sauvegarde de la base de données des événements**, et inclut la version actuelle de la base de données Protege GX dans le nom du fichier.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Paramètres globaux | Paramètres de messagerie

Paramètres SMTP courriel

- **Serveur de messagerie SMTP** : L'adresse du serveur de messagerie SMTP sortant. Les serveurs SMTP testés et pris en charge sont :
  - Microsoft Exchange Server 2016
  - Gmail lorsqu'il est configuré pour des applications moins sécurisées (voir ce lien)
  - Yahoo

  Le serveur SMTP peut nécessiter une certaine configuration pour lui permettre de recevoir et de relayer les courriels provenant de Protege GX.
- **Port SMTP** : Le port utilisé pour les connexions de courriel sortant.
- **Utiliser SSL** : Lorsque cette option est activée, Protege GX utilise TLS 1.2 pour transmettre les courriels au serveur SMTP. Le système d'exploitation hôte et le serveur SMTP doivent tous deux prendre en charge TLS 1.2, et le **port SMTP** ci-dessus doit être remplacé par un port compatible avec TLS (par exemple, 587, 2525).

  Lorsque cette option est désactivée, aucun cryptage n'est utilisé.
- **Connexion SMTP/mot de passe** : Le nom d'utilisateur et le mot de passe utilisés par Protege GX pour se connecter au serveur de messagerie SMTP.
- **Délai d'attente SMTP** : Définit le délai (en secondes) avant que la connexion au serveur de messagerie SMTP ne soit interrompue.
- **Adresse courriel de l'expéditeur** : L'adresse courriel utilisée lors de l'envoi de courrier sortant.
- **Nom d'affichage de l'expéditeur** : Le nom d'affichage utilisé lors de l'envoi de courriel sortant. Si aucun nom d'affichage n'est saisi, l'adresse courriel de l'expéditeur est utilisée.
- **Tester l'adresse courriel** : Saisissez une adresse courriel pour les notifications de test.
- **Tester les paramètres courriel** : Envoie un courriel de test à l'adresse indiquée ci-dessus.

  Le courriel de test est envoyé à partir de la machine cliente qui est actuellement utilisée. Pour valider les paramètres de messagerie du serveur Protege GX, assurez-vous que vous effectuez des tests en utilisant la machine serveur. Ceci est important pour les courriels de rapport programmés et autres courriels automatisés.

Paramètres globaux | Affichage

Couleurs symbole de statut

- **Carte couleur** : Définit la carte de couleurs utilisée pour représenter l'état des appareils (tels que les portes et les partitions) sur les plans d'étages et les pages des statuts. Celles-ci peuvent être configurées dans **Global | Cartes en couleur**.

Paramètres d'affichage des photos

- **Réinitialiser la taille d'affichage** : Réinitialise les paramètres d'affichage des photos de l'utilisateur à 300 pixels de large x 400 pixels de haut.
- **Pixels** : Définit la largeur et la hauteur par défaut des photos en pixels. Ce paramètre s'applique à toutes les photos des utilisateurs au niveau mondial, mais peut être remplacé pour des sites spécifiques dans **Global | Sites | Affichage**.

Afficher l'heure de l'horloge

- **Afficher la date et l'heure en mode plein écran** : Sélectionnez cette option pour afficher la date et l'heure dans le coin inférieur droit de la barre d'état lorsque l'interface Protege GX est en mode plein écran. Vous pouvez passer en mode plein écran en cliquant sur le bouton d'expansion en haut à droite.

Paramètres globaux | Son

Sons d'alarmes

- **Son d'alarme** : Définit le son de notification par défaut joué sur les stations de travail des opérateurs lorsqu'une alarme se déclenche.

  Choisissez entre le son Windows par défaut, un fichier d'ondes de votre choix ou Aucun son.
- **Chemin du fichier d'ondes** : Si vous utilisez un fichier d'ondes pour le **Son d'alarme**, cliquez sur le bouton d'ellipse**[...]** pour rechercher et sélectionner le fichier .wav.

  Ce fichier wave doit être situé dans un dossier réseau partagé auquel les clients ont accès. Si le fichier n'est pas accessible au même endroit sur tous les postes clients, aucun son ne sera joué lors du déclenchement d'une alarme.

Sons

Cette section vous permet d'ajouter des sons d'alarme personnalisés qui peuvent être attribués à des types d'alarmes spécifiques. Cela aide le personnel à distinguer rapidement les différents types d'alertes et à y répondre de manière appropriée.

1. Cliquez sur **Ajouter** pour ajouter un son personnalisé. Il doit s'agir d'un fichier wave d'une taille maximale de 3 Mo.
2. Définissez un **Nom** descriptif pour le son et cliquez sur **OK**.
3. Naviguez jusqu'à **Événements | Alarmes** et attribuez le son personnalisé comme **Son d'alarme** pour les enregistrements d'alarme correspondants.

   Toute alarme à laquelle aucun son personnalisé n'a été attribué utilisera le paramètre de notification par défaut **Son d'alarme** ci-dessus.

Les sons ajoutés à cette section et affectés à un enregistrement d'alarme seront automatiquement synchronisés sur chaque machine cliente lorsqu'un opérateur se connecte.

Sites

Les sites sont des divisions du système Protege GX qui peuvent être utilisées pour permettre à plusieurs systèmes de sécurité complets de résider sur le même serveur.

- Seuls les enregistrements globaux sont partagés entre les sites, c'est-à-dire la programmation dans le menu **Global**.
- La plupart des types d'enregistrements ne sont pas partagés entre les sites. Par exemple, les utilisateurs d'un site ne peuvent pas accéder aux portes et aux zones d'un autre site, et les sites ne peuvent pas partager les ressources matérielles telles que les entrées et les sorties.
- Les opérateurs Protege GX peuvent avoir accès aux enregistrements de plusieurs sites ou d'un seul site. Pour plus d'informations, consultez la section Rôles (la page 63).

Les sites sont généralement utilisés lorsqu'un seul serveur Protege GX est utilisé pour le fonctionnement des systèmes de sécurité de plusieurs clients différents. Cela permet de séparer complètement les clients les uns des autres tout en partageant les ressources du serveur et les paramètres globaux.

Il n'est pas recommandé de créer un nouvel enregistrement de site pour chaque emplacement ou compartiment du même système, car les enregistrements d'utilisateurs ne sont pas partagés entre les sites. Utiliser plutôt des groupes d'enregistrements pour organiser les enregistrements qui appartiennent à chaque site.

Utiliser le menu Sites pour créer et configurer votre ou vos sites. Cela inclut les paramètres d'affichage et les options liées à certaines intégrations. Lorsque vous ajoutez un nouveau site, l'assistant **ajouter un contrôleur** s'ouvre automatiquement, vous invitant à ajouter un contrôleur à votre nouveau site.

Le site du Système ne doit pas être modifié.

Sites | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Page de statut des alarmes**: Détermine la page de statut par défaut affichée lorsque vous cliquez sur l'icône **Voir les alarmes** dans la barre d'état.
- **Afficher le graphique à barres de stabilité du contrôleur**: Lorsque cette option est activée, la liste d'enregistrements **Sites | Contrôleurs** du site affiche une colonne Stabilité de connexion pour chaque contrôleur. Cette colonne utilise une barre pour afficher la stabilité de la connexion, où les blocs rouges représentent le temps hors ligne et les blocs verts le temps en ligne. Ceci est utile pour surveiller la connexion lorsque le contrôleur semble se déconnecter périodiquement.

Adresse

Coordonnées du site et/ou de l'organisation pour la référence de l'opérateur.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Sites | Affichage

Onglets des événements du plan d'étage

- **Fenêtre d'événements 1 à 6** : Sélectionner jusqu'à six rapports d'événements qui seront affichés sous forme d'onglets supplémentaires dans la fenêtre d'événements lors de la visualisation d'un plan d'étage.
- **Plan d'étage par défaut** : Le plan d'étage par défaut qui s'affiche en premier lors de l'ouverture de la vue du plan d'étage pour ce site.
- **Page de statut par défaut** : La page de statut par défaut qui s'affiche en premier lors de l'ouverture de la vue de la page d'état pour ce site.

Fenêtre utilisateur

- **Afficher les champs personnalisés prédéfinis dans les utilisateurs**: Sélectionner cette option pour afficher l'onglet **Utilisateurs | Utilisateurs | Élargis**, qui comprend une série de champs personnalisés prédéfinis.
- **Afficher les utilisateurs dans les groupes**: Sélectionnez cette option pour afficher les enregistrements d'utilisateurs dans une vue de groupe (ou arborescence) par défaut dans le menu **Utilisateurs | Utilisateurs**. Dans cette vue, les utilisateurs sont regroupés par **Groupe d'enregistrements**. Lorsque cette option est désactivée, les enregistrements d'utilisateur sont affichés par défaut en vue liste.
- **Afficher uniquement un emplacement de carte** : Sélectionnez cette option pour n'afficher qu'un seul champ **Numéro d'établissement/de carte** pour chaque utilisateur. Ceci empêche l'ajout de plus d'une carte à un utilisateur par le biais du logiciel Protege GX.

  Ce paramètre ne peut pas être activé si un ou plusieurs utilisateurs ont déjà plus d'une carte attribuée. Vous pouvez effectuer une recherche d'utilisateur (**Utilisateurs | Recherche d'utilisateur**) avec la colonne Numéro d'établissement/de carte pour voir quels utilisateurs ont des cartes excédentaires attribuées.

  Cette fonction ne peut pas être utilisée avec l'intégration Suprema, car les informations d'identification biométriques utilisent le deuxième emplacement de carte.

  Le service SOAP ignore la restriction du numéro de carte.
- **Afficher les colonnes du premier nom et du nom de famille dedans Types d'informations d'identification utilisateurs** : Sélectionner cette option pour afficher les colonnes pour **Premier nom** et **Dernier nom** dans la page **Utilisateurs | Utilisateurs**. Vous pouvez ensuite trier la liste des utilisateurs par premier nom ou surnom en cliquant sur l'en-tête de la colonne.

Date/heure d'expiration par défaut de l'utilisateur

Ces paramètres vous permettent de spécifier les paramètres de début et/ou d'expiration par défaut pour tous les nouveaux enregistrements d'utilisateur. Ils sont appliqués lorsque de nouveaux utilisateurs sont ajoutés, et n'affectent pas les enregistrements d'utilisateurs existants.

- **Début** : La date/heure de début par défaut pour tous les nouveaux enregistrements d'utilisateur. Les nouveaux utilisateurs ne pourront pas avoir accès avant cette heure et cette date.
- **Fin** : La date/heure d'expiration par défaut pour tous les nouveaux enregistrements d'utilisateur. Les enregistrements d'utilisateurs expireront après cette date et cette heure et les utilisateurs ne pourront plus accéder au système.

Ces paramètres peuvent être remplacés par les paramètres des utilisateurs individuels dans **Utilisateurs | Utilisateurs | Général**.

Paramètres d'affichage des photos

- **Réinitialiser la taille d'affichage**: Réinitialise les paramètres d'affichage des photos de l'utilisateur à 300 pixels de large x 400 pixels de haut.
- **Pixels** : Définit en pixels la largeur et la hauteur par défaut des photos. Ce paramètre s'applique à toutes les photos de l'utilisateur sur le site.

Affichage des actions sur le calendrier

- **Masquer les anciennes actions du calendrier**: Sélectionner cette option pour effacer automatiquement les actions du calendrier du système lorsqu'elles deviennent invalides (**Sites | Actions du calendrier**).

Sites | Répertoire Actif

Ces paramètres vous permettent de synchroniser utilisateurs Protege GX avec Windows Active Directory pour une gestion améliorée des utilisateurs. Pour la synchronisation des opérateurs Protege GX avec Répertoire Actif, voir les options dans **Global | Opérateurs | Général**.

L'intégration de Répertoire Actif est une fonctionnalité sous licence séparée. Pour plus d'informations, voir Note d'application 288 : Utilisation de Windows Active Directory dans Protege GX.

Paramètres d'importation des utilisateurs Répertoire Actif

- **Importer les utilisateurs à partir du Active Directory** : Sélectionnez cette option pour importer les détails de l'utilisateur depuis le répertoire actif vers la base de données Protege GX.
- **Domaine Active Directory** : Définit le domaine Active Directory de Windows utilisé.
- **Groupe Windows** : Le groupe Windows contenant les utilisateurs à importer.

  Un seul groupe de sécurité Windows sélectionné peut être synchronisé avec cette intégration.

- **Période de synchronisation (minutes)** : Définit la fréquence de synchronisation des utilisateurs avec Active Directory.
- **Désactiver les utilisateurs si les utilisateurs AD sont désactivés** : Désactive l'accès de l'utilisateur Protege GX si le compte du répertoire actif est désactivé.
- **Désactiver les utilisateurs si les utilisateurs AD sont supprimés** : Désactive l'accès de l'utilisateur Protege GX si le compte du répertoire actif est supprimé.

Sites | Valeurs par défaut des sites

Défauts d'inactivité de la carte utilisateur

- **Désactiver une carte d'utilisateur inactive**: Si cette option est activée, les nouveaux utilisateurs ajoutés au système se verront automatiquement appliquer une **période d'inactivité** par défaut à leurs informations d'identification. Si l'utilisateur n'utilise pas ses informations d'identification pendant cette période, celles-ci seront désactivées.

  Lorsque vous enregistrez une modification de ce paramètre, vous êtes invité à appliquer la modification à tous les utilisateurs. Sélectionnez **Oui** pour remplacer les paramètres programmés dans les enregistrements individuels des utilisateurs par la nouvelle valeur par défaut. Cette opération peut prendre un certain temps pour les sites comptant un grand nombre d'utilisateurs. Si vous sélectionnez **Non**, le paramètre par défaut ne sera appliqué qu'aux utilisateurs ajoutés après la modification.

- **Période d'inactivité par défaut de la carte** : Définir le nombre de jours, d'heures ou de minutes pendant lesquels le justificatif d'identité doit être inactif avant d'être désactivé.

Valeurs par défaut de l'inactivité des utilisateurs

- **Désactiver les utilisateurs inactifs**: Si cette option est activée, les nouveaux utilisateurs ajoutés au système auront automatiquement une **période d'inactivité** par défaut appliquée à leurs informations d'identification. Si l'utilisateur est complètement inactif pendant cette période, l'enregistrement sera désactivé.

Lorsque vous enregistrez une modification de ce paramètre, vous êtes invité à appliquer la modification à tous les utilisateurs. Sélectionnez **Oui** pour remplacer les paramètres programmés dans les enregistrements individuels des utilisateurs par la nouvelle valeur par défaut. Cette opération peut prendre un certain temps pour les sites comptant un grand nombre d'utilisateurs. Si vous sélectionnez **Non**, le paramètre par défaut ne sera appliqué qu'aux utilisateurs ajoutés après la modification.

- **Période d'inactivité par défaut de l'utilisateur**: Définir le nombre de jours, d'heures ou de minutes pendant lesquels l'utilisateur doit être inactif avant que l'enregistrement ne soit désactivé.
- **Suppression des utilisateurs inactifs**: Si cette option est activée, les nouveaux utilisateurs ajoutés au système se verront automatiquement appliquer une **période de suppression** par défaut à leurs informations d'identification. Si l'utilisateur est totalement inactif pendant cette période, l'enregistrement sera supprimé.

  Lorsque vous enregistrez une modification de ce paramètre, vous êtes invité à appliquer la modification à tous les utilisateurs. Sélectionnez **Oui** pour remplacer les paramètres programmés dans les enregistrements individuels des utilisateurs par la nouvelle valeur par défaut. Cette opération peut prendre un certain temps pour les sites comptant un grand nombre d'utilisateurs. Si vous sélectionnez **Non**, le paramètre par défaut ne sera appliqué qu'aux utilisateurs ajoutés après la modification.

- **Période de suppression par défaut de l'inactivité de l'utilisateur :** Précise le nombre de jours, d'heures ou de minutes pendant lesquels l'utilisateur doit être inactif avant que l'enregistrement ne soit supprimé.

Amélioration de la sécurité du site

Pour plus d'informations, voir Note d'application 275 : Configuration des améliorations de la sécurité du site dans Protege GX.

- **Exiger une double identification pour l'accès au clavier**: Si cette option est activée, les utilisateurs devront saisir à la fois un ID utilisateur et un code NIP pour avoir accès à un clavier. Chaque enregistrement d'utilisateur comprendra un type de justificatif d'identité d'utilisateur, qui doit être un identifiant numérique unique de 1 à 10 chiffres.

  En outre, aucun opérateur ne pourra visualiser les codes NIP des utilisateurs, que l'option **Afficher les numéros NIP pour les utilisateurs** soit activée ou non (**Global | Opérateurs**).
- **Remplissage automatique de la valeur du justificatif d'identification de l'utilisateur**: Cette fonction active le système pour générer automatiquement des numéros ID utilisateurs pour les utilisateurs. Lorsque l'option est activée pour la première fois, tous les utilisateurs qui n'ont pas d'ID utilisateur existant se voient attribuer automatiquement un ID unique (basé sur leur ID Base de données). Ensuite, tous les nouveaux utilisateurs créés se verront automatiquement attribuer un ID utilisateur unique à 8 chiffres. Les ID utilisateurs peuvent toujours être modifiés manuellement, même après avoir été autoproduits. Ceci est pratique sur les sites plus larges où il peut être difficile de s'assurer que chaque nouvel utilisateur se voit attribuer un ID unique.
- **Autoriser la duplication du NIP**: L'activation de cette fonction permet la création de NIP identiques dans les registres d'utilisateurs du site. Chaque utilisateur devra entrer un ID utilisateur unique pour s'identifier ainsi qu'un NIP, ce qui permettra au système d'identifier avec précision l'utilisateur qui se connecte au clavier et de maintenir l'intégrité de la sécurité du site.

  Les types de porte NIP Seulement et Carte ou NIP ne sont pas compatibles avec la duplication de NIP, car il n'existe aucun moyen d'identifier de manière unique l'utilisateur qui réclame l'accès.

- **Longueur du NIP par défaut** : La longueur par défaut des codes NIP lorsqu'ils sont générés automatiquement par le système, de 4 à 8 chiffres.

  Par exemple, si le réglage est fixé à 6, le système génère d'abord de nouveaux NIP à 6 chiffres. Une fois que ceux-ci sont épuisés, il génère des NIP avec un nombre plus élevé de chiffres, puis des NIP avec moins de chiffres.
- **Longueur minimale du code NIP**: Le nombre minimum de chiffres (options entre 1 et 8) autorisés pour les codes NIP. Plus la longueur du NIP est élevée, plus le niveau de sécurité est élevé, car la complexité du NIP augmente avec le nombre de chiffres.
- **Nombre maximum de chiffres séquentiels** : Le nombre maximum de chiffres séquentiels autorisés pour les codes PIN, entre 2 et 4 chiffres. Par exemple, en sélectionnant 4, vous autoriserez une séquence numérique de 1234 ou 4321, mais pas 12345.

- **Nombre maximal de chiffres répétés** : Le nombre maximum de chiffres répétés autorisés pour les codes PIN, entre 2 et 4 chiffres. Par exemple, en sélectionnant 4, vous autorisez un code PIN de 0000, mais pas de 00000.
- **Heure d'expiration du code NIP**: Les codes NIP des utilisateurs expireront après la durée définie dans ce champ. Lorsque l'utilisateur tentera de se connecter à un clavier après ce délai, il sera invité à saisir et à confirmer un nouveau code NIP. Ce paramètre s'applique à l'ensemble du site et peut être remplacé par les paramètres **Expiration du NIP** pour les utilisateurs individuels (**Utilisateurs | Utilisateurs | Général**).

  Lorsque l'expiration du code PIN est activée, tous les codes NIP créé par l'interface utilisateur expirera immédiatement lors de la première utilisation. L'utilisateur doit définir son propre code NIP permanent à l'aide d'un clavier. Cela garantit que seul l'utilisateur connaît son NIP.

  Lorsque vous enregistrez une modification de ce paramètre, vous êtes invité à appliquer la modification à tous les utilisateurs. Sélectionnez **Oui** pour remplacer les paramètres programmés dans les enregistrements individuels des utilisateurs par la nouvelle valeur par défaut. Cette opération peut prendre un certain temps pour les sites comptant un grand nombre d'utilisateurs. Si vous sélectionnez **Non**, le paramètre par défaut ne sera appliqué qu'aux utilisateurs ajoutés après la modification.
- **Nouveau NIP à générer par le système**: Lorsque cette option est activée, tout NIP permanent doit être généré par le système (autre qu'un NIP temporaire à usage unique créé par l'opérateur). Un utilisateur peut demander un nouveau code NIP lorsqu'il se connecte à un clavier. Si un NIP expiré est utilisé pour se connecter à un clavier, le système présente automatiquement un nouveau NIP à l'utilisateur.

  Cette option n'est disponible que lorsqu'un **Délai d'expiration du NIP** est défini.

Photo d'identification

- **Sauvegarde du numéro et de la date du badge après impression de la carte** : Lorsque cette option est activée, après l'impression d'une carte-photo d'identité, le **Numéro de badge** (à partir de 1) et **La date de production du badge** seront automatiquement sauvegardés dans l'enregistrement de l'utilisateur dans l'onglet **Prolongé**. Le **Type de badge** sera réglé sur Imprimé.

  Pour que cette option fonctionne, l'option **Afficher les champs personnalisés prédéfinis dans les utilisateurs** doit être activée dans l' onglet **Affichage**.

Sites | Exportation de photos d'utilisateurs

Les photos des utilisateurs stockées dans Protege GX peuvent être périodiquement exportées vers un répertoire de la machine serveur. Cette fonction peut être utilisée pour partager des images capturées dans Protege GX avec des systèmes tiers tels que des systèmes de RH ou d'impression de badges.

Général

- **Activé** : Active le processus d'exportation de photos.
- **Exporter le dossier**: L'emplacement sur le disque où les fichiers photo de l'utilisateur seront enregistrés.
- **Export le format photo**: Le format d'image sous lequel les fichiers photo sont enregistrés. Sélectionner parmi : .jpg, .png, .bmp, .gif, .tif ou .wdp.
- **Exporter le champ personnalisé du nom du fichier** : Les images exportées seront nommées numériquement (1, 2, 3, etc.). Le champ personnalisé sélectionné ici sera préfixé au nom du fichier, ce qui permettra de regrouper ou d'identifier spécifiquement les utilisateurs.

Type de calendrier

- **Débuter Manuellement** : L'exportation des photos de l'utilisateur se fait manuellement à l'aide du bouton **Exporter les photos de l'utilisateur maintenant**.
- **Une fois** : L'exportation des photos de l'utilisateur sera exécutée une fois. Après avoir sélectionné cette option, vous devrez spécifier la date et l'heure de début dans le champ **Heure de début**.
- **Récurrent** : L'exportation des photos de l'utilisateur sera exécutée de façon récurrente. Après avoir sélectionné cette option, vous devrez définir l'occurrence (quotidienne, hebdomadaire ou mensuelle) et la fréquence (jour

(s) et heure) de l'exportation. Vous pouvez également spécifier une **durée** (date de début et/ou de fin) pour le programme d'exportation.

- **Prochaine temps d'exécution** : Affiche l'heure de la prochaine exécution de l'exportation des photos d'utilisateur (en lecture seule).

Dernière exécution

- **Exporter les photos de l'utilisateur maintenant** : Cliquer sur ce bouton pour exporter manuellement les photos de l'utilisateur.
- **Dernière exécution**: Affiche la date et l'heure de la plus récente exportation de photos d'utilisateur (en lecture seule).
- **Statut de la dernière exécution**: Indique si l'exportation de photos d'utilisateur la plus récente a réussi ou échoué.

Sites | Biométrie

Les intégrations de biométrie Suprema et Princeton Identity sont des fonctionnalités sous licence séparée. Pour plus d'informations, voir Note d'application 264 : Intégration de la biométrie Suprema dans Protege GX et/ou Note d'application 297 : Intégration biométrique de l'identité Princeton avec Protege GX.

Suprema biometrics

- **Activer l'intégration Suprema** : Sélectionner cette option pour activer l'intégration de la biométrie Suprema pour ce site.
- **Numéro d'établissement par défaut** : Le numéro d'établissement par défaut utilisé pour les informations de connexion biométriques pour ce site. Lorsqu'un identifiant biométrique est enregistré, un numéro de carte est généré automatiquement et attribué à l'utilisateur en même temps que ce numéro d'établissement comme second identifiant.

  Assurez-vous que ce numéro n'est pas le même que le numéro d'établissement pour toutes les cartes utilisées sur le site. Le chiffre par défaut 100 est recommandé.

- **Lecteur d'inscription par défaut** : Définit quel lecteur biométrique sera utilisé comme appareil d'inscription par défaut pour les nouvelles informations de connexion biométriques. Les lecteurs biométriques peuvent être programmés dans **Sites | Lecteurs biométriques**. Cette option peut être remplacée pour des utilisateurs spécifiques (**Utilisateurs | Utilisateurs | Biométriques**).

Biométrie de Princeton

- **Activer l'intégration Princeton** : Sélectionner cette option pour activer l'intégration de la biométrie Princeton Identity pour ce site.
- **Numéro d'établissement par défaut** : Le numéro d'établissement par défaut utilisé pour les informations de connexion biométriques pour ce site. Lorsqu'un identifiant biométrique est enregistré, un numéro de carte est généré automatiquement et attribué à l'utilisateur en même temps que ce numéro d'établissement comme second identifiant.

  Assurez-vous que ce numéro n'est pas le même que le numéro d'établissement pour toutes les cartes utilisées sur le site. Le chiffre par défaut 100 est recommandé.

- **Lecteur d'inscription par défaut** : Définit quel lecteur biométrique sera utilisé comme appareil d'inscription par défaut pour les nouvelles informations de connexion biométriques. Les lecteurs biométriques peuvent être programmés dans **Sites | Lecteurs biométriques**. Cette option peut être remplacée pour des utilisateurs spécifiques (**Utilisateurs | Utilisateurs | Biométriques**).
- **Adresse IP** : L'adresse IP du serveur de Princeton Identity (IDS).
- **Port IP** : Le port IP du serveur de Princeton Identity. Le port par défaut est 8843.
- **Nom d'utilisateur** : Le nom d'utilisateur requis pour ouvrir une session sur le serveur de Princeton Identity.
- **Mot de passe** : Le mot de passe requis pour se connecter au serveur de Princeton Identity.

- **Type d'informations d'identification**: Lorsque l'intégration de Princeton est activée, un type d'informations d'identification par défaut PrincetonIris sera créé et attribué à la configuration du site ici. Ce type d'informations d'identification contient la programmation requise pour inscrire et utiliser les justificatifs de Princeton biometric. Il peut être consulté au niveau de **Sites | Types d'informations d'identification**.

Sites | Salto

Les paramètres saisis ici doivent correspondre aux paramètres de la programmation de l'interface Salto SHIP. Dans cette intégration, les cartes Salto des utilisateurs sont encodées directement dans Protege GX, à l'aide d'un encodeur de bureau. Pour obtenir le fichier encoder.ini requis, contactez ICT l'assistance technique.

L'intégration de Salto SHIP est une fonctionnalité sous licence séparée. Pour plus d'informations, consultez la Note d'application 188 : Salto SHIP RW Intégration de Pro Access avec Protege GX or Application Note 335: Salto SHIP ProAccess SPACE Intégration avec Protege GX.

Cet onglet n'est pas utilisé pour l'intégration de Salto SALLIS.

Options Salto

- **Activer l'intégration de Salto (SHIP)** : Sélectionnez cette option pour activer l'intégration de Salto SHIP pour ce site.
- **Activer l'enregistrement**: Active le journal des erreurs de Salto, qui enregistre toutes les données envoyées au système Salto. Le journal des erreurs est accessible dans Protege GX via **Salto | Journal des erreurs Salto**.

  Cette option peut être utile pour la configuration initiale et le dépannage, mais doit être désactivée pendant le fonctionnement normal afin d'économiser le stockage des événements.
- **Adresse IP** : L'adresse IP du serveur SHIP.
- **Port IP** : Le port utilisé pour communiquer avec le serveur SHIP.
- **Identifiant de l'encodeur Salto par défaut**: Si plusieurs encodeurs Salto sont connectés au PC utilisé pour encoder les informations d'identification Salto, par défaut, Protege GX utilisera le premier encodeur qui a été configuré. Si un autre encodeur doit être utilisé, spécifiez son identifiant ici.
- **Clé Mifare A** : La chaîne de Clé Mifare A de Salto pour l'encodage des cartes Salto. Ce champ peut être laissé vide - la valeur du fichier encoder.ini sera utilisée.
- **Clé Mifare B** : La chaîne de Clé Mifare B de Salto pour l'encodage des cartes Salto. Ce champ peut être laissé vide - la valeur du fichier encoder.ini sera utilisée.
- **Clé principale** : La chaîne de la clé maîtresse Salto pour l'encodage des cartes Salto. Ce champ peut être laissé vide - la valeur du fichier encoder.ini sera utilisée.

Sélection du secteur MIFARE 1K/4K

Pour encoder des cartes à partir de l'interface Protege GX, vous devez sélectionner les secteurs de carte qui sont alloués à Salto. Les secteurs alloués sont spécifiques au site et peuvent être consultés dans le fichier encoder.ini situé dans le dossier C:\Programmes (x86)\Integrated Control Technology\Protege GX.

Le secteur 14 doit être laissé pour être utilisé par le format ICT MIFARE.

Sites | Cencon

L'intégration Cencon vous permet de surveiller et de gérer les verrous Cencon à partir de Protege GX. Cela vous permet ainsi, de gérer les utilisateurs Cencon, créer des groupes de verrous logiques, afficher l'état d'un verrou Cencon et surveiller les événements Cencon.

L'intégration Cencon est une fonctionnalité sous licence séparée. Pour plus d'informations, consultez la Note d'application 160 : Configuration de l'intégration Cencon.

Options Cencon

- **Activer l'intégration de Cencon**: Sélectionnez cette option pour activer l'intégration Cencon pour ce site.
- **Chemin de la transaction d'entrée CenTran** : Le répertoire où Protege GX enverra les transactions Cencon sortantes.

  Pour que l'intégration fonctionne correctement, assurez-vous que ce répertoire est accessible à la fois par les services Protege GX et par CenTran.
- **Chemin de la transaction de sortie CenTran**: Le répertoire où Protege GX recevra les transactions Cencon entrantes.

  Pour que l'intégration fonctionne correctement, assurez-vous que ce répertoire est accessible à la fois par les services Protege GX et par CenTran.
- **Identification du répartiteur** : Le répartiteur identifie la source de la transaction dans la programmation CenTran. Si ce champ est vide, l'identifiant du répartiteur par défaut sera utilisé.
- **Nom de la branche**: Le nom de la branche Cencon que Protege GX gère.
- **Délai d'attente de la commande Cencon (secondes)**: Définit la durée (en secondes) pendant laquelle Protege GX attend une réponse de Cencon après avoir envoyé un fichier de transaction.

  Cette valeur ne doit pas être modifiée à moins d'être conseillé par ICT l'assistance technique.
- **Intervalle de synchronisation Cencon (minutes)**: Définit la fréquence (en minutes) d'une synchronisation entre Protege GX et Cencon.

  Cette valeur ne doit pas être modifiée à moins d'être conseillé par ICT l'assistance technique.
- **Enregistrer toutes les transactions Cencon**: Lorsque cette option est activée, Protege GX consigne toutes les transactions Cencon dans le journal des transactions Cencon (**Cencon | Journaux des transactions**). Lorsque cette option est désactivée, Protege GX ne consigne que les transactions d'erreur.

  Cette option peut être utile pour la configuration initiale et le dépannage, mais doit être désactivée pendant le fonctionnement normal afin d'économiser le stockage des événements.
- **Synchroniser**: Lorsque ce bouton est activé, Protege GX tentera de se synchroniser avec la base de données Cencon.

Sites | Armoires à clés

Les intégrations d'armoires à clés vous permettent de surveiller et de gérer l'accès aux boîtes à clés et aux clés à partir de Protege GX.

Les intégrations KeyWatcher et KeySecure sont des fonctionnalités sous licence séparée. Pour plus d'information, regardez Note d'application 220 : Intégration du tactile de KeyWatcher dans Protege GX ou Note d'application 331 : Intégration de KeySecure dans Protege GX.

Options d'intégration

- **Activer l'intégration** : Sélectionner cette option pour activer l'intégration de l'armoire à clés pour ce site.
- **Type d'intégration** : Sélectionner soit KeyWatcher – Morse Watchmans ou KeySecure – Technologie CIC .
- **Activer l'enregistrement**: Le fichier journal du service d'intégration est stocké dans le répertoire d'installation. Activer cette option pour enregistrer tous les messages disponibles. Désactiver cette option pour enregistrer uniquement les messages d'erreur.

  Cette option peut être utile pour la configuration initiale et le dépannage, mais doit être désactivée pendant le fonctionnement normal afin d'économiser le stockage des événements.

- **Longueur du chiffre de l'identifiant de l'utilisateur tiers**: Pour les intégrations KeyWatcher, il s'agit de la longueur de l'identifiant **KeyWatcher** qui sera automatiquement attribué à chaque utilisateur auquel est attribué un niveau d'accès valide comprenant des clés ou des groupes de clés KeyWatcher (**Utilisateurs | Utilisateurs | Général**). Tous les identifiants KeyWatcher doivent contenir ce nombre de chiffres.

  Ce paramètre doit correspondre au champ **longueur des chiffres de l'identifiant utilisateur** attribué dans le logiciel KeyWatcher True Touch client. Toute modification de ce champ doit correspondre au logiciel KeyWatcher.

Sites | Portail

La synchronisation du portail de location vous permet de synchroniser automatiquement les utilisateurs de Protege GX au portail de location Protege et de créer pour eux des comptes SIP et d'application mobile Protege. Cela permet aux visiteurs d'appeler directement les locataires à partir d'une station d'entrée.

Pour plus d'informations et d'instructions de configuration, consultez le Protege guide d'utilisation du portail de location.

Options générales

- **Activer la synchronisation du portail** : Activez ce paramètre pour permettre la synchronisation des utilisateurs avec le portail des locataires.

  Lorsque la synchronisation du portail de location est activée, les codes NIP des utilisateurs sont toujours renvoyés en texte clair lorsque le service SOAP obtient un enregistrement d'utilisateur. Ceci remplace les paramètres qui masquent normalement les codes NIP, tels que **Afficher les numéros NIP pour les utilisateurs** et **Chiffrer les codes NIP des utilisateurs**, et affecte **tous** les opérateurs utilisant le client Web et d'autres applications SOAP.

- **Activer la synchronisation sans contact de l'ascenseur** : Cette option est réservée pour un développement futur.

Informations d'identification

- **Nom d'utilisateur** : Le nom d'utilisateur de votre compte du portail des locataires.
- **Mot de passe** : Le mot de passe de votre compte de portail de location.

Opérateurs

Un opérateur est une personne qui utilise Protege GX et qui est responsable de la programmation et de la maintenance du système, ainsi que de la surveillance du site.

Certains champs dans le registre d'opérateur Admin par défaut ne peuvent pas être modifiés.

Opérateurs | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.

  Cela ne doit pas nécessairement être le même que le nom d'utilisateur de l'opérateur (ci-dessous).
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Configuration

- **Nom d'utilisateur** : Le nom d'utilisateur que l'opérateur utilise pour se connecter à Protege GX.
- **Mot de passe** : Le mot de passe de l'opérateur pour se connecter au logiciel. Ceci peut être réinitialisé en cliquant sur le bouton ellipse **[...]** et en saisissant un nouveau mot de passe. Les opérateurs peuvent également modifier leur propre mot de passe à partir de la page d'accueil.
- **Rôle** : Sélectionner le rôle approprié pour déterminer ce que l'opérateur peut voir et faire dans le logiciel. Les rôles peuvent être configurés dans **Global | Rôles**.

  Cliquer sur le bouton ellipse **[...]** pour ouvrir une fenêtre d'accès aux rôles, qui affiche les tableaux de base de données pour lesquelles l'opérateur dispose d'un accès en lecture, d'un accès en écriture et d'autorisations de commande manuelle. Vous pouvez imprimer le rapport en cliquant sur l'icône **Imprimer** de la barre d'outils, filtrer les résultats en saisissant des termes dans la deuxième ligne d'en-tête et regrouper les résultats en faisant glisser des colonnes dans la barre située au-dessus du tableau.
- **Fuseau horaire**: Le fuseau horaire où l'opérateur est basé. Cela détermine les temps d'enregistrement des événements indiqués sur les pages des statuts et les plans d'étages. Si l'opérateur utilise le même fuseau horaire que le serveur Protege GX, sélectionner utiliser le fuseau horaire du serveur.
- **Utiliser l'authentification Windows** : Sélectionnez cette option pour utiliser l'authentification Windows / Répertoire actif et permettre à l'opérateur de se connecter en utilisant ses informations d'identification Windows. Cela évite d'avoir à saisir un nom d'utilisateur et un mot de passe lors de la connexion à Protege GX, ce qui rend le processus de connexion plus sûr.

  Pour connecter cet opérateur à un utilisateur Répertoire actif, activer cette option puis cliquer sur le bouton d'ellipse **[...]** à côté du champ **Nom d'utilisateur**. Sélectionner un **domaine** et localiser l'utilisateur **Répertoire actif** qui correspond à cet opérateur.

  Cette fonction exige que l'option **Activer l'authentification Windows sur service de données / communications client** soit activée pendant l'installation. Pour plus d'informations, consulter la note d'application 288 : Utilisation de Répertoire actif dans Protege GX.
- **Afficher les NIP pour les utilisateurs** : Permettre à l'opérateur de visualiser les NIP des utilisateurs.
- **Montrer les clés Salto** : Permet à l'opérateur de visualiser les informations clés de Salto.

Courriel

- **Courriel** : L'adresse courriel de l'opérateur. Ceci peut être utilisé par Protege GX pour un courriel automatique sur l'événement et d'autres fonctions.

  Les fonctions de courrier électronique automatisées dans Protege GX exigent qu'un serveur de courrier SMTP soit configuré dans **Global | Paramètres globaux | Paramètres de courrier électronique**.

- **Langue par défaut du rapport** : La langue par défaut utilisée lorsqu'un rapport programmé est envoyé par courriel à l'opérateur. Sélectionner la première ou la deuxième langue (telle que déterminée par l'installation du logiciel).

Délai d'attente de l'opérateur

- **Activer le délai d'attente de l'opérateur** : Sélectionner cette option pour déconnecter automatiquement l'opérateur après une période d'inactivité.
- **Délai d'attente de l'opérateur en secondes** : Définit la période d'inactivité (en secondes). Si l'opérateur n'est pas actif pendant cette période, il y aura un avertissement de 30 secondes, après quoi le client se fermera.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Rôles

Les rôles définissent le niveau d'accès des opérateurs au système Protege GX. Chaque rôle est basé sur une présélection (administrateur, installateur, utilisateur final ou gardien) et peut être personnalisé davantage pour contrôler précisément les sections du système qu'un opérateur peut voir et modifier. Plusieurs niveaux de sécurité peuvent également être attribués à chaque rôle, ce qui permet de limiter l'accès des opérateurs à des sites ou à des groupes d'enregistrements spécifiques.

Le rôle par défaut de l'administrateur ne peut pas être modifié. Cela garantit que l'opérateur administrateur a un accès complet au système.

Les modifications apportées aux rôles ne prendront effet que lorsque les opérateurs concernés auront redémarré leurs sessions client.

Pour de plus amples informations et des exemples de programmation, voir la Note d'application 247 : Utilisation des groupes d'enregistrement dans Protege GX.

Rôles prédéfinis

Chaque rôle dans Protege GX doit être basé sur un préréglage spécifique qui a des paramètres d'accès prédéfinis. Les onglets **Tableaux** et **Niveaux de sécurité** vous permettent de personnaliser l'accès de chaque rôle, en utilisant le préréglage comme point de départ.

✓ Accès complet

✓ Lecture seule

✗ Refusé

Description	Admin	Installateur	Utilisateur final	Garde
Niveaux d'accès	✓	✓	✓	✗
Alarmes	✓	✓	✗	✗
Modules d'expansion analogiques	✓	✓	✗	✗
Appartements	✓	✓	✗	✗
Partitions	✓	✓	✗	✗
Groupes de zones	✓	✓	✗	✗
Présence	✓	✓	✗	✗
Automatisation	✓	✓	✗	✗
Valeurs des données binaires	✓	✓	✗	✗
Actions du calendrier	✓	✓	✗	✗
Caméras	✓	✓	✗	✗
Contrôleurs	✓	✓	✗	✗

Description	Admin	Installateur	Utilisateur final	Garde
Types de justificatifs	✓	✓	✓	✗
Champs personnalisés	✓	✓	✓	✗
Onglets des champs personnalisés	✓	✓	✓	✗
Valeurs des données	✓	✓	✗	✗
Heure d'été	✓	✓	✓	✗
États de l'appareil	✓	✓	✗	✗
Portes	✓	✓	✗	✗
Groupes de portes	✓	✓	✗	✗
Types de portes	✓	✓	✗	✗
Serveurs de téléchargement	✓	✓	✗	✗
DVR	✓	✓	✗	✗
Voitures d'ascenseur	✓	✓	✗	✗
Groupes d'ascenseurs	✓	✓	✗	✗
Filtres d'événements	✓	✓	✗	✗
Rapports d'événements	✓	✓	✓	✓
Serveurs d'événements	✓	✓	✗	✗
Étages	✓	✓	✗	✗
Groupes d'étages	✓	✓	✗	✗
Plans d'étage	✓	✓	✓	✓
Statut de santé	✓	✓	✓	✓
Jours fériés	✓	✓	✓	✗
Groupes fériés	✓	✓	✓	✗
Entrées	✓	✓	✗	✗
Modules d'expansion d'entrée	✓	✓	✗	✗
Types d'entrées	✓	✓	✗	✗
Interphones	✓	✓	✗	✗
Emplois	✓	✓	✗	✗

Description	Admin	Installateur	Utilisateur final	Garde
Groupes de serrures Kaba	✓	✓	✗	✗
Claviers	✓	✓	✗	✗
Groupes de claviers	✓	✓	✗	✗
Licence	✓	✓	✓	✓
Groupes de menus	✓	✓	✗	✗
Modems	✓	✓	✗	✗
Rapports de rassemblement	✓	✓	✗	✗
Opérateurs	✓	✓	✗	✗
Sorties	✓	✓	✗	✗
Modules d'expansion de sorties	✓	✓	✗	✗
Groupes de sortie	✓	✓	✗	✗
Numéros de téléphone	✓	✓	✗	✗
Modèles de photos d'identité	✓	✓	✓	✗
Fonctions programmables	✓	✓	✗	✗
Modules d'expansion	✓	✓	✗	✗
Groupes de registres	✓	✓	✓	✗
Historique des enregistrements	✓	✓	✓	✗
Rôles	✓	✓	✗	✗
Calendriers de Salto	✓	✓	✗	✗
Portes de Salto	✓	✓	✗	✗
Groupes de portes Salto	✓	✓	✗	✗
Salto Outputs	✓	✓	✗	✗
Périodes de temps de Salto	✓	✓	✗	✗
Horaires	✓	✓	✓	✗
Scripts	✓	✓	✗	✗
Niveaux de sécurité	✓	✓	✗	✗
Options de sécurité	✓	✓	✗	✗

Description	Admin	Installateur	Utilisateur final	Garde
Journal des événements du serveur	✓	✓	✓	✓
Services	✓	✓	✗	✗
Sites	✓	✓	✗	✗
Lecteurs intelligents	✓	✓	✗	✗
Définitions d'état	✓	✓	✗	✗
Listes des statuts	✓	✓	✓	✓
Pages des statuts	✓	✓	✓	✓
Système	✓	✓	✗	✗
Entrées troubles	✓	✓	✗	✗
Utilisateurs	✓	✓	✓	✗
Images de l'utilisateur	✓	✓	✓	✗
Importation par l'utilisateur	✓	✓	✗	✗
Rapports de l'utilisateur	✓	✓	✓	✗
Variables	✓	✓	✗	✗
Historique des variables	✓	✓	✓	✗
VMS	✓	✓	✓	✓
Cartes VMS	✓	✓	✓	✓
Images VMS	✓	✓	✓	✓
Pages VMS	✓	✓	✓	✓
Postes de travail VMS	✓	✓	✓	✓
Liens Web	✓	✓	✗	✗

Rôles | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

- **Prédéfini**: Sélectionner cette option pour choisir l'un des quatre rôles prédéfinis :

Rôle prédéfini	Fonction
Administrateur	Peut effectuer toutes les actions dans tous les sites sans aucune restriction
Installateur	Peut effectuer les actions requises pour installer et configurer le système
Utilisateurs finaux	Peut effectuer des rapports et une configuration limitée du système des utilisateurs
Garde	Peut surveiller le système et visualiser uniquement les événements

Les présélections de rôles constituent un moyen rapide de fournir un accès aux opérateurs. À moins que les permissions des rôles ne soient spécifiquement modifiées, toutes les permissions seront héritées du préréglage.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Rôles | Tableaux

L'onglet **Tableaux** détermine les autorisations dont dispose le rôle pour chaque tableau de la base de données.

Cela vous permet de personnaliser l'accès en fonction du rôle attribué à un opérateur. Par exemple, les opérateurs ayant un poste au sein des RH peuvent se voir accorder un accès en lecture seulement aux tableaux contenant des données sur le personnel et les employés, et se voir refuser l'accès à d'autres tableaux.

Pour chaque tableau, sélectionnez l'une des options suivantes :

- Reprendre du préréglage pour conserver les autorisations par défaut du préréglage de rôle sélectionné (consultez la page 63).
- Refuser pour empêcher l'accès aux données contenues dans le tableau. Cela permet de cacher à l'opérateur toutes les fonctions et options de menu pour ce tableau.
- Accorder un accès total pour accorder une autorisation complète de lecture/écriture.
- Accorder un accès en lecture seule pour accorder l'accès à la vue, mais pas à la mise à jour des données dans le tableau. L'opérateur pourra voir les paramètres pertinents, mais les options pour les mettre à jour sont désactivées.

Certaines autorisations pour les tableaux ne sont pas disponibles pour modification dans la programmation des rôles et ne sont accessibles que lorsque le préréglage **de rôle** est défini sur Administrateur. Par exemple, vous pouvez créer un opérateur qui a un accès complet au menu **Visiteur** uniquement, mais constater que le tableau Visiteur n'est pas disponible dans l'onglet **Tableaux**. Dans ce cas, vous pourriez créer un rôle avec le préréglage Administrateur (donnant à l'opérateur l'accès aux tableaux Visiteur) et supprimer l'accès aux tableaux qui ne sont pas nécessaires.

Rôles | Sites

L'onglet **Sites** détermine les sites auxquels le poste a accès. Les autorisations d'accès à des sites spécifiques peuvent être personnalisées davantage dans l'onglet **Niveaux de sécurité**.

- **A accès à tous les sites**: Cochez cette case pour accorder au poste, l'accès à tous les sites du système.
- **Sites**: Cochez la case **Active** en regard de chaque site pour accorder au poste l'accès à ce site (en fonction des autorisations accordées dans l' onglet **Tableaux**), ou désactivez-la pour refuser l'accès. Si l'accès à un site leur est refusé, les opérateurs seront en mesure de voir que l'autre site existe, mais pas de visualiser ni de modifier aucun de ses enregistrements.

Rôles | Niveaux de sécurité

L'onglet **Niveaux de sécurité** vous permet de définir les groupes d'enregistrements auxquels l'opérateur a accès, et de préciser les autorisations de l'opérateur au sein d'un site ou d'un groupe d'enregistrements à l'aide de niveaux de sécurité.

Les autorisations accordées dans un niveau de sécurité remplacent celles accordées dans l'onglet **Tableaux**.

Si aucun groupe d'enregistrements n'est sélectionné, l'opérateur pourra accéder à tous les groupes d'enregistrements. Si des groupes d'enregistrements sont ajoutés, l'opérateur ne pourra accéder qu'aux enregistrements des groupes spécifiés.

Plusieurs groupes d'enregistrements ayant le même niveau de sécurité peuvent être inclus, mais les groupes d'enregistrements ayant différents niveaux de sécurité ne sont pas pris en charge. Si cela est nécessaire, il est recommandé d'ajouter un enregistrement distinct pour l'opérateur.

Cliquez sur le bouton **Ajouter** pour attribuer un niveau de sécurité. Sélectionnez les options suivantes :

- **Site**: Le site pour lequel le niveau de sécurité souhaité est pertinent.
- **Niveau de sécurité**: Le niveau de sécurité qui accordera les permissions requises pour ce site.
- **Accéder à tous les groupes d'enregistrement**: Activer cette option pour accorder un accès basé sur les autorisations du niveau de sécurité à tous les groupes d'enregistrements (ou sélectionne des groupes d'enregistrements spécifiques dans le champ **Nom** ci-dessous).
- **Nom**: Sélectionner le ou les groupes d'enregistrements spécifiques auxquels ce niveau de sécurité s'appliquera. L'opérateur n'aura accès qu'à ces groupes d'enregistrements, en utilisant les autorisations du niveau de sécurité sélectionné.

Rôles | Affichage

Paramètres de notification d'alarme

- **S'ouvre en cas d'alarme**: Lorsque cette option est activée, l'opérateur reçoit une notification contextuelle lorsque des événements d'alarme spécifiques se produisent. Les alarmes peuvent être créées dans la programmation **Événements | Alarmes**.
- **Fréquence de la fenêtre contextuelle** : Le temps entre les rappels de notification contextuelle. Lorsqu'une fenêtre contextuelle d'alarme est affichée pour l'opérateur, l'ordinateur émet une notification sonore chaque fois que cette période s'écoule sans que l'alarme soit acquittée.

  En outre, un opérateur peut cliquer sur l'icône de sourdine en haut à droite de la fenêtre contextuelle et désactiver l'alarme pour la durée de la fréquence de la fenêtre contextuelle.
- **L'opérateur peut désactiver jusqu'à la prochaine connexion** : Lorsque cette option est activée, l'opérateur peut désactiver une fenêtre contextuelle d'alarme jusqu'à sa prochaine connexion en cliquant sur l'icône de sourdine en haut à droite de la fenêtre contextuelle.
- **L'opérateur peut mettre une fenêtre contextuelle d'alarme en veille pendant X minutes** : Lorsque cette option est activée, l'opérateur peut désactiver une fenêtre contextuelle d'alarme pendant un nombre défini de minutes en cliquant sur l'icône de sourdine en haut à droite.

Options de la caméra

- **Autoriser la caméra contextuelle**: Lorsque cette option est activée, l'opérateur peut recevoir des fenêtres contextuelles de la caméra affichant des séquences en direct lorsque des événements spécifiques se produisent. Ces fenêtres contextuelles peuvent être configurées en créant une action (**Événements | Actions**) dont le **type** est défini sur la fenêtre contextuelle de la caméra, ou via les paramètres **Fenêtre contextuelle de caméra automatique** dans **Programmation | Portes | Général**.

Serveur de téléchargement

Le serveur de téléchargement gère la communication entre l'interface utilisateur Protege GX et le contrôleur. En général, un seul serveur de téléchargement est nécessaire; cependant, pour les installations très importantes comportant de nombreux contrôleurs, des serveurs de téléchargement supplémentaires peuvent être utilisés pour réduire les temps de téléchargement de la programmation.

- Le serveur de téléchargement à registre unique (installé séparément) réduit les temps de téléchargement en envoyant aux contrôleurs uniquement le ou les registres qui ont été ajoutés, modifiés ou supprimés. Pour plus de renseignements, consulter la Note d'application 309 : Téléchargements des registres uniques dans Protege GX.
- Plusieurs serveurs de téléchargement standard peuvent être utilisés pour gérer des groupes distincts de contrôleurs. Pour plus de renseignements, consulter la Note d'application 290 : Configurer un serveur de téléchargement Protege GX secondaire.

Si les paramètres du serveur de téléchargement sont modifiés, vous devrez peut-être redémarrer le service de téléchargement Protege GX.

Serveur de téléchargement | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Configuration

- **Nom de l'ordinateur** : Le nom de l'ordinateur hébergeant le serveur de téléchargement.

  La longueur maximale du nom de l'ordinateur est de 15 caractères.
- **Nombre maximal de téléchargements concurrents** : Définit le nombre maximum de contrôleurs qui peuvent être téléchargés simultanément.
- **Version** : Affiche les détails de la version actuelle du serveur de téléchargement (lecture seulement).
- **Date de la version** : Affiche la date de la dernière mise à jour du serveur de téléchargement (lecture seulement).
- **Dernière fois de notification** : Affiche la date de la dernière notification générée par le serveur de téléchargement (lecture seulement).
- **Type de serveur de téléchargement** : Le type est automatiquement réglé sur Standard ou Registre unique.
- **Parent du serveur de téléchargement** : Si le **Type de serveur de téléchargement** est réglé sur Registre unique, il est possible de sélectionner un serveur de téléchargement standard comme parent. Cela limite le serveur de téléchargement à registre unique à télécharger uniquement vers les contrôleurs qui sont gérés par le serveur de téléchargement standard. Si aucun parent n'est sélectionné, le serveur de téléchargement à registre unique télécharge vers tous les contrôleurs.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Serveur d'événement

Le serveur d'événement gère la communication entre le contrôleur et l'interface utilisateur Protege GX.

Si les paramètres du serveur d'événement sont modifiés, vous devrez peut-être redémarrer le service d'événement Protege GX.

Serveur d'événement | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Configuration

- **Nom de l'ordinateur** : Le nom de l'ordinateur qui héberge le serveur d'événement.

  La longueur maximale du nom de l'ordinateur est de 15 caractères.
- **Port** : Le port IP par lequel les événements sont envoyés du contrôleur au logiciel. Par défaut, il s'agit du port 22000.
- **Nombre de fils de communication** : Le nombre de fils entre le serveur d'événement et les contrôleurs.
- **Nombre de fils de base de données** : Le nombre de fils entre le serveur d'événement et la base de données. Un paramètre plus élevé permet au serveur d'événement de sauvegarder plus rapidement les événements dans la base de données.

  Le nombre de fils est une fonction sous licence dans le serveur SQL.
- **Watch Dog** : Réinitialise automatiquement les communications si le serveur d'événement n'a pas reçu d'événements d'un contrôleur dans les 90 secondes.
- **Version** : Affiche les détails de la version actuelle du serveur d'événement (lecture seulement).
- **Date de la version** : Affiche la date de la dernière mise à jour du serveur d'événement (lecture seulement).
- **Dernière fois de notification** : Affiche la date de la dernière notification générée par le serveur d'événement, telle qu'une alarme opérateur (lecture seulement).

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Modem

Cette page de programmation fait référence à des fonctionnalités héritées et n'est plus utilisée dans Protege GX.

Carte couleur

Les cartes en couleur vous permettent de personnaliser les couleurs utilisées pour représenter l'état des objets (tels que les portes ou les sorties) sur un plan d'étage ou une page du statut. Par exemple, vous pouvez configurer une carte couleur pour que les portes déverrouillées soient affichées en bleu plutôt qu'en vert par défaut, afin d'aider les opérateurs atteints de daltonisme rouge-vert.

Vous pouvez sélectionner la carte couleur qui sera utilisée pour l'ensemble du système dans **Global | Paramètres globaux | Afficher**. Si aucune carte couleur n'est réglée, les couleurs par défaut seront utilisées.

Pour changer les paramètres de la carte couleur, il faut fermer et rouvrir Protege GX avant que les nouveaux paramètres ne soient appliqués aux objets affichés dans l'interface utilisateur.

Cartes couleur | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Onglets de l'appareil de cartes couleur

Une couleur personnalisée peut être appliquée aux icônes d'état suivantes. Les couleurs disponibles sont : gris, rouge, orange, jaune et vert.

Cartes couleur | Portes

- Porte hors ligne
- Porte verrouillée et sécurisée
- Porte déverrouillée
- Porte forcée ouverte
- Porte ouverte et déverrouillée
- Porte laissée ouverte, sens de la porte non scellé
- Porte laissée ouverte, sens des liens non scellé

Cartes couleur | Entrées

- Entrée hors ligne
- Entrée fermée
- Entrée ouverte
- Sabotage d'entrée
- Court-circuit d'entrée

Cartes couleur | Sorties

- Sortie hors ligne
- Sortie activée
- Sortie désactivée

Cartes couleur | Partitions

- Partition hors ligne
- Partition désarmée
- Partition armée
- Délai d'entrée de la partition
- Partition (autres états)

Cartes couleur | Ascenseurs

- Ascenseur hors ligne
- Ascenseur verrouillé
- Ascenseur déverrouillé

Symboles de plans d'étages

Les symboles de plan d'étage sont des symboles personnalisés qui représentent les différents objets (tels que les portes et les partitions) et leurs états lorsqu'ils sont affichés sur un plan d'étage.

Créer un symbole de plan d'étage

1. Dans **Global | Symboles d'aménagement**, cliquez sur **Ajouter**. Entrez un **Nom**.
2. Sélectionnez le **Type** de dispositif que vous voulez que ce symbole de plan d'étage représente. Vous ne pouvez sélectionner qu'un seul type de dispositif par enregistrement.
3. Pour chaque champ d'état, cliquez sur le bouton en forme d'ellipse **[...]** pour ajouter une image.
   - Si l'image est déjà stockée sur le réseau, sélectionnez l'ellipse **[...]** à côté de **Path** pour naviguer vers l'image. L'image doit être accessible depuis la machine serveur.
   - Si l'image n'existe pas encore, définissez le champ **Source de l'image** pour capturer une nouvelle image. Vous pouvez capturer une image à partir d'une webcam connectée ou d'un bloc de signature Topaz.
   - Lorsque vous avez terminé, cliquez sur **Suivant**.
4. Dans la fenêtre suivante, vous pouvez recadrer l'image si nécessaire :
   - Ajustez la taille et la position du rectangle pointillé pour inclure la section de l'image que vous souhaitez conserver. Cochez l'option **Aspect** pour fixer le rapport d'aspect du rectangle.
   - Pour recadrer l'image, cochez la case **Crop**.
   - Cliquez sur **Ok**.
5. Répétez les opérations ci-dessus pour tous les champs d'état, puis **Enregistrez** le symbole de plan d'étage.
6. Une fois qu'un symbole de plan d'étage est créé, vous pouvez sélectionner cet enregistrement comme **Style de dispositif** lorsque vous ajoutez un dispositif à un plan d'étage (**Surveillance | Configuration | Éditeur de plan d'étage**).

Symboles plans d'étages | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Type** : Sélectionnez le type de périphérique pour lequel vous souhaitez ajouter des symboles. Chaque enregistrement de symbole de plan d'étage ne peut contenir que des symboles pour un seul type de dispositif (toute autre image chargée ne sera pas disponible dans l'éditeur de plan d'étage).

États des portes

- Porte hors ligne
- Porte verrouillée et sécurisée
- Porte déverrouillée
- Porte forcée ouverte
- Porte ouverte et déverrouillée
- Porte laissée ouverte, sens de la porte non scellé
- Porte laissée ouverte, sens des liens non scellé

États des entrées

- Entrée hors ligne
- Entrée fermée
- Entrée ouverte
- Sabotage d'entrée
- Court-circuit d'entrée

États des sorties

- Sortie hors ligne
- Sortie activée
- Sortie désactivée

États des partitions

- Partition hors ligne
- Partition désarmée
- Partition armée
- Délai d'entrée de la partition
- Partition (autres états)

États des ascenseurs

- Ascenseur hors ligne
- Ascenseur verrouillé
- Ascenseur déverrouillé

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Types d'événements

La page des types d'événements fournit une liste complète des événements qui peuvent être générés par le système, ce qui vous permet de rechercher des événements spécifiques et d'identifier leurs ID base de données si nécessaire. Vous pouvez également définir la couleur d'affichage utilisée pour les événements dans la fenêtre d'événement, ce qui permet d'identifier rapidement des événements spécifiques.

Pour que les couleurs personnalisées des événements prennent effet, vous devez sauvegarder les modifications, fermer le client Protege GX et redémarrer les services Protege GX. Lorsque le client est rouvert, les couleurs personnalisées apparaissent sur les pages des statuts et les plans d'étages.

Types d'événements | Général

Général

- **Nom** : La description de l'événement en anglais, telle qu'elle apparaît dans les recherches et les rapports d'événements. Ce champ est en lecture seulement.
- **Nom (deuxième langue)** : La description de l'événement dans la deuxième langue installée avec le logiciel. Ce champ est en lecture seulement.

Couleurs d'affichage

- **Personnaliser les couleurs d'affichage** : Activez cette option pour personnaliser la couleur de fond et de texte du type d'événement.
- **Couleur de fond** : La couleur de fond de ce type d'événement dans le journalÉvénement. Saisissez un code RVB ou cliquez sur le bouton **[...]**d'ellipse pour ouvrir le sélecteur de couleur.
- **Couleur du texte** : La couleur du texte de ce type d'événement dans le journalÉvénement. Saisissez un code RVB ou cliquez sur le bouton **[...]**d'ellipse pour ouvrir le sélecteur de couleur.

Menu Sites

Le menu sites contient des enregistrements utilisés pour la configuration du site, tels que les contrôleurs, les horaires et les types d'information d'identification.

Les sites sont des divisions du système Protege GX qui peuvent être utilisées pour permettre à plusieurs systèmes de sécurité complets de résider sur le même serveur. Pour plus d'informations, consultez la section Sites (la page 52).

Horaires

Les horaires dans Protege GX sont essentiels pour automatiser le contrôle d'accès et la détection des intrusions. Les niveaux d'accès, les zones, les portes et autres enregistrements peuvent être configurés pour suivre un calendrier, ce qui leur permet de changer automatiquement d'état lorsqu'un calendrier devient valide ou invalide.

Chaque programme peut être programmé avec un maximum de 8 périodes comprenant différentes heures et jours de la semaine, programmées pour couvrir un large éventail de scénarios opérationnels. Un programme peut être programmé avec un groupe de jours fériés, ce qui lui permet d'être valable pendant des heures différentes les jours fériés. Un programme peut également suivre l'état d'une sortie, ce qui permet une automatisation plus complexe.

Pour une démonstration, voir Programmer un nouveau horaire dans Protege GX sur ICT la chaîne YouTube.

Horaires | Configuration

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Périodes et groupes de temps

- **Périodes**: Vous pouvez configurer jusqu'à 8 périodes de temps dans chaque horaire pour définir à quel moment l'horaire est valide et invalide. Définis une **Heure de début** et une **Heure de fin** pour chaque période à l'aide du sélecteur de temps. Vérifiez ensuite les jours de la semaine auxquels la période s'appliquera et définissez le mode **jours fériés** pour la période.

  Pour créer un programme 24 heures sur 24 et 7 jours sur 7, régler les **Heure de début** et **Heure de fin** sur 12 h 00 et vérifiez chaque jour de la semaine. Régler le mode **jours fériés** sur Ignorer les jours fériés.

- **Mode jours fériés**: Définit la manière dont le programme fonctionnera pendant un jour férié (tel que défini dans l'onglet **Groupes de jours**fériés). Pour chaque période individuelle, vous pouvez choisir entre

- **Désactivé pendant les jours fériés**: Lorsque cette option est sélectionnée, cette période ne fonctionnera pas lors d'un jour férié et l'horaire ne sera pas valide pendant cette période lors d'un jour férié. Par exemple, si une porte est programmée pour se déverrouiller pendant cette période, elle ne se déverrouillera pas lors d'un jour férié.
- **Activé pendant les jours fériés**: Lorsque cette option est sélectionnée, cette période fonctionnera uniquement pendant un jour férié et non pendant les jours ordinaires. Par exemple, une zone peut être programmée pour se désarmer pendant des périodes plus courtes, les jours fériés, mais plus longues les autres jours.
- **Ignorer les jours fériés**: Lorsque cette option est sélectionnée, la période fonctionnera sans tenir compte du fait que le jour est un jour férié ou non.

- **Salto**: Ces champs vous permettent de configurer des périodes spécifiques qui seront utilisées pour les jours fériés et les journées spéciales dans l'intégration de Salto SHIP. Si les H (Jours fériés), S1 (Spécial 1) ou S2 (Spécial 2) sont cochés, cette période sera utilisée ces jours-là, comme défini dans le calendrier Salto correspondant (voir **Salto | Calendriers**).

  Le calendrier Salto utilisé par l'agenda est défini dans la programmation utilisateur : **Utilisateurs | Utilisateurs | Salto**.

Vue graphique.

La vue graphique fournit une représentation visuelle des périodes du calendrier. Chaque jour de la semaine est représenté par une ligne de temps de 24 h indiquant les moments où le calendrier est valide (barre pleine) et invalide (vide). Noter que toutes les périodes sont combinées sur cette vue, indépendamment de leur mode jours fériés.

La vue graphique est en lecture seule. Les périodes de temps ne peuvent pas être ajustées à partir de cette zone de l'écran.

Horaires | Options

Qualifier la sortie

- **Valider le programme si vous qualifiez la sortie sur**: Lorsque cette option est activée, le programme ne peut devenir valide que lorsque la sortie **Qualifier** (ci-dessous) est sur.
- **Valider le programme si la sortie est désactivée**: Lorsque cette option est activée, le programme ne peut devenir valide que lorsque **Qualifier sortie** (ci-dessous) est désactivée.
- **Qualifier la sortie**: Ce champ vous permet d'attribuer une sortie qui permettra de qualifier le programme. Cela signifie que le programme ne sera valide que lorsque à la fois la période et la sortie qualifiée seront dans un état valide. L'état requis pour la sortie est défini par les options ci-dessus.

  Cette fonction a de nombreuses applications pour intégrer le contrôle d'accès, la détection des intrusions et l'automatisation. Par exemple, vous pouvez utiliser la sortie **Désarmée** d'un secteur comme sortie de qualification afin que la programmation ne soit valide que lorsque le secteur est désarmé. Le programme peut ensuite être utilisé pour contrôler d'autres zones, niveaux d'accès, types de portes et autres caractéristiques du système.

  Pour un exemple de programmation avancée utilisant un programme qualifié, voir Note d'application 307 : Programmation d'un interrupteur d'homme mort dans Protege GX.

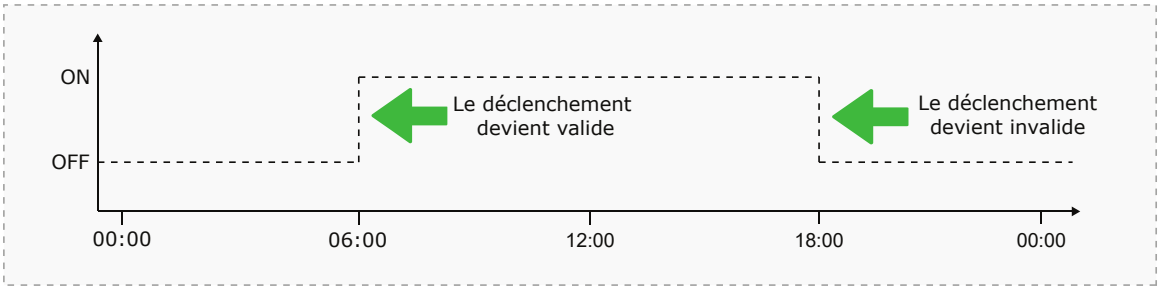
Horaires | Groupes de vacances

Les groupes de vacances permettent à un programme de fonctionner différemment les jours fériés et les jours ordinaires. Cet onglet vous permet de sélectionner les groupes de vacances qui s'appliqueront à un programme particulier en cliquant sur **Ajouter** et en sélectionnant des éléments dans la liste.

Les groupes de vacances peuvent être programmés dans **Sites | Groupes de vacances**.

Déclenchement par front d'impulsion

Les objets qui sont programmés pour changer lorsqu'un horaire change sont **déclenchés par front d'impulsion**. Cela signifie qu'ils sont vérifiés et modifiés par défaut uniquement lorsque l'horaire change d'état.



Par exemple, si une porte est programmée pour se déverrouiller à 6 h par un horaire, elle ne se déverrouille qu'au moment où l'horaire devient valide. Si vous avez assigné cet horaire comme horaire de déverrouillage de la porte à 10 h, cette porte ne se déverrouille pas avant 6 h le lendemain matin. En effet, le déclencheur qui déverrouille la porte ne se déclenche que lorsque l'horaire passe de non valide à valide.

En résumé :

- Les appareils qui sont contrôlés par un programme sont déclenchés par front d'impulsion par défaut.
- Le déclenchement par front d'impulsion permet un contrôle manuel complet des appareils entre les horaires.
- Le déclenchement par front d'impulsion n'est traité qu'au début et à la fin d'une période.
- Si vous programmez un appareil pour qu'il suive un horaire, le contrôle n'a pas lieu avant la prochaine heure de début.
- Si vous configurez l'appareil pour qu'il suive toujours l'horaire, l'état de l'appareil commence immédiatement à suivre l'horaire (par exemple, en utilisant l'option **Toujours vérifier horaire de déverrouillage** dans **Programmation | Portes | Options**).
- Lorsqu'un appareil est configuré pour toujours suivre l'horaire, le contrôle manuel de l'appareil n'est plus possible.

Configuration des horaires et des jours fériés

Les horaires sont des délais définis qui permettent à une fonction ou à un niveau d'accès de ne fonctionner que pendant certaines périodes déterminées. Ils peuvent être utilisés pour contrôler le moment où un utilisateur peut accéder, déverrouiller automatiquement les portes, armer ou désarmer des partition, activer et désactiver des appareils ou modifier leur comportement à certaines heures de la journée. Les horaires sont essentiels pour automatiser le contrôle d'accès et la détection des intrusions dans le système Protege.

Comme les horaires sont couramment utilisés pour contrôler l'accès ou sécuriser des partitions, il est habituel que l'horaire soit différent un jour férié. Pour ce faire, on ajoute les groupes de jours fériés, qui sont utilisés pour empêcher (ou permettre) que les périodes d'un horaire fonctionnent pendant la durée des jours fériés.

Une fois qu'un horaire est programmé, il est toujours soit valide, soit invalide. Lorsqu'il devient valide, les éléments qui sont programmés avec cet horaire sont activés. Par exemple :

- Un niveau d'accès n'accorde l'accès que lorsque son **horaire d'opération** est valable.
- Une porte se déverrouille lorsque son **horaire de déverrouillage** devient valide.
- Une sortie s'active lorsque son **calendrier d'activation** devient valide.

Cette section fournit quelques conseils utiles pour une programmation efficace des horaires.

Horaires et périodes multiples

Il peut arriver que les horaires doivent être activés et désactivés plus d'une fois, ou à des moments différents selon les jours. Chaque horaire comporte huit périodes pour tenir compte de ces scénarios.

Vous trouverez ci-dessous quelques exemples de situations dans lesquelles vous pourriez utiliser ce système.

Heures différentes pour la fin de semaine

Les locaux pourraient ouvrir pendant des heures plus courtes (ou plus longues) en fin de semaine.

Pour configurer ce système, il suffit d'ajouter une deuxième période d'heures réduites et de sélectionner le(s) jour (s) concerné(s).

Heures différentes un jour férié

Dans certaines installations, en particulier dans le commerce de détail, un horaire doit toujours être en place un jour férié, mais il peut être plus court ou plus long.

Pour ce faire, il suffit de définir une autre période avec les jours et les heures requis, et de régler le **mode congé** sur Activé pendant les congés.

Plusieurs périodes dans une même journée

Parfois, plusieurs périodes sont nécessaires dans une même journée. Prenons l'exemple d'un cinéma où il y a plusieurs séances et où les portes doivent être déverrouillées à certaines périodes.

Fixez autant de périodes indépendantes pour le(s) même(s) jour(s) que nécessaire.

Horaires de nuit

Lorsqu'un horaire doit être appliqué pendant la nuit, entrez une heure de début, mais fixez l'heure de fin à **00:00**. La période est donc valable à partir de l'heure de début jusqu'à minuit.

Programmez maintenant une deuxième période qui commencera à minuit et se poursuivra jusqu'à la fin du quart de travail. En prolongeant les jours de validité de la période, nous créons une équipe de nuit du lundi au vendredi.

La vue graphique est utile pour fournir une représentation visuelle de la période de validité de l'horaire.

Périodes de chevauchement

Lorsque les périodes se chevauchent, l'horaire prend la somme de toutes les périodes.

Règles relatives aux horaires et aux jours fériés

Si vous programmez des heures et des jours dans un horaire mais ne faites rien d'autre, alors l'horaire fonctionnera **toujours**.

Pour qu'un jour férié empêche l'horaire de devenir valable, il faut que les éléments suivants aient été programmés :

1. Le jour férié doit être programmé dans un groupe de jours fériés.
2. Ce groupe de congés doit être appliqué au calendrier dans l'onglet **Groupes de** congés.
3. Le **mode congés** pour la période de programmation doit être réglé sur Désactivé pendant les congés.

Actions du calendrier

Les actions de calendrier vous permettent de créer des actions de porte et de sortie qui remplacent les horaires pour une durée déterminée. Ces actions peuvent être définies comme ponctuelles ou programmées pour se répéter chaque jour, semaine, mois ou année.

Les actions de sortie peuvent être utilisées pour contrôler d'autres enregistrements tels que les partitions, les niveaux d'accès et les types de portes en utilisant la fonction **Qualifier sortie** (consultez la page 77) ou les fonctions programmables.

Pour plus d'informations sur l'application de cette fonction, reportez-vous à la note d'application 179 : Configuration des actions du calendrier dans Protege GX :

Visualisation des actions du calendrier

1. Naviguez vers **Sites | Actions du calendrier** . Cela affichera un calendrier montrant les actions passées et futures du calendrier.
2. Utilisez les boutons de navigation pour sélectionner la vue du calendrier la plus utile :

   - **Aujourd'hui** : Affiche les actions du calendrier se déroulant le jour en cours.
   - **Les 7 prochains jours** : Affiche les actions du calendrier se produisant au cours des 7 prochains jours.
   - **Semaine de travail** : Affiche les actions du calendrier qui ont lieu pendant une semaine de travail sélectionnée.
   - **Semaine** : Affiche les actions du calendrier qui ont lieu pendant une semaine de travail sélectionnée.
   - **Mois** : Affiche les actions du calendrier qui ont lieu pendant une semaine de travail sélectionnée.
   - **Vue Horaire** : Affiche les actions du calendrier dans une vue de planification.
   - **Liste** : Affiche les actions du calendrier dans une liste
3. Utilisez les Clés KeyWatcher fléchées ou la molette de défilement de votre souris pour naviguer dans le calendrier. Passez d'une semaine ou d'un mois à l'autre en utilisant les flèches en haut à gauche, ou naviguez avec la barre du calendrier sur le côté gauche.

Créer une action de calendrier

Pour créer une action de calendrier, rendez-vous sur **Sites | Actions de calendrier**.

1. Sélectionnez le jour (et l'heure si possible) où l'action du calendrier doit débuter.
2. Cliquez sur **Nouveau rendez-vous**.
3. Saisissez les informations requises (voir ci-dessous).
4. Cliquez sur **Enregistrer et fermer**.

Vous pouvez ouvrir une action de calendrier pour la modifier ou la supprimer à tout moment en double-cliquant dessus dans la vue calendrier.

Général

- **Description** : Le nom ou la description de l'action de calendrier.
- **Groupe de registres** : Le groupe de registres auquel appartient l'action de calendrier.
- **Heure de début/fin** : Définissez la période pendant laquelle l'action de calendrier doit être exécutée.

  Les heures de début et de fin peuvent être remplacées par les options de récurrence décrites ci-dessous.
- **Événement d'une journée** : Si cette option est activée, l'action de calendrier est exécutée pendant toute la journée, de minuit à minuit.

- **Liste des appareils** : Les actions de calendrier peuvent affecter à la fois les portes et les sorties, en annulant toute programmation ou tout autre facteur qui les contrôlerait normalement. Cliquez sur **Ajouter** pour ajouter des appareils à l'action. Sélectionnez le **TypeAppareil**, puis activez le(s) appareil(s) requis et cliquez sur **OK**.

  Les portes disposent des options d'action suivantes :

  - **Verrouiller** : La porte est verrouillée pour la durée de l'action.
  - **Porte déverrouillée maintenue** : La porte est déverrouillée (mais fermée) pendant toute la durée de l'action.
  - **Temps de verrouillage prolongé** : Pendant cette durée, chaque fois que la porte est déverrouillée par l'accès, la sortie de verrouillage est activée pendant le temps spécifié dans le champ **Temps prolongé** au lieu du **Temps d'activation du verrouillage** habituel (**Programmation | Portes | Sorties**).

  Les sorties peuvent être mises sur ON ou OFF par l'action de calendrier. Cette fonction peut être utilisée avec des fonctions programmables et des horaires pour contrôler d'autres parties du système, comme l'armement par partition.

Récurrence

Cliquez sur le bouton **Récurrence** pour ouvrir la fenêtre Récurrence de l'activité. Lorsque les options de récurrence sont configurées, un champ situé en bas de la fenêtre décrit le modèle de récurrence.

- **Horaire de l'activité** : Définissez l'heure de début, l'heure de fin et/ou la durée de l'action de calendrier. Ces paramètres ont priorité sur ceux de la programmation **générale**.
- **Modèle de récurrence** : Définissez la fréquence de répétition de l'action de calendrier, sur la base d'une récurrence quotidienne, hebdomadaire, mensuelle ou annuelle. Chaque fréquence comporte d'autres options permettant de déterminer plus précisément quand l'événement se reproduira.
- **Période de récurrence** : Définissez la date de début à laquelle l'action de calendrier est activée. Vous pouvez ne fixer aucune date de fin, une date de fin spécifique ou un nombre fixe d'occurrences.

Groupes fériés

Les groupes fériés permettent de désactiver (ou d'activer) les périodes d'horaire pendant des jours fériés. Les groupes fériés peuvent être assignés dans **Sites | Horaires | Groupes fériés**.

Pour plus d'informations, consultez la section Configuration des horaires et des jours fériés (la page 78).

Groupes fériés | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Groupes fériés | Jours fériés

Cliquez sur **Ajouter** pour ajouter des jours fériés au groupe.

- **Nom** : Le nom du jour férié.
- **Répéter** : Lorsque cette option est activée, le jour férié se répète sur une base annuelle.

  Gardez à l'esprit que certains jours fériés se répètent le même jour chaque année (par exemple, Noël), tandis que d'autres se produisent à des jours différents (par exemple, Pâques). Il est utile de programmer les jours fériés plusieurs années à l'avance.
- **Date de début** : Le premier jour du jour férié.
- **Date de fin** : Le dernier jour des congés.

  Pour créer un congé d'un jour, sélectionnez la même date de fin que la date de début. Par exemple, pour créer un congé de 24 heures pour le jour de l'an, vous devez régler à la fois la date de début et de fin sur le 1er janvier.

Contrôleurs

Le Protege GX contrôleur est l'unité centrale de traitement du Protege GX système. Le contrôleur communique avec tous les modules du système, conserve toutes les informations de configuration et de transaction, traite toutes les communications du système et signale les alarmes et les événements au Protege GX serveur.

Contrôleurs | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

  Certains types d'enregistrements, tels que les sorties, les entrées, les entrées trouble et les modules d'expansion, héritent du groupe d'enregistrements attribué au contrôleur.

Communications

- **Numéro de série** : le numéro de série du contrôleur. Il peut être obtenu à partir de la page de configuration de l'interface web intégrée, ou de l'étiquette sur le côté du contrôleur.
- **Adresse IP** : L'adresse IP du contrôleur. L'adresse IP par défaut est 192.168.1.2, qui peut être changée via l'interface Web intégrée.

  En général, l'adresse IP doit être la même ici et dans l'interface Web du contrôleur. Par ailleurs, si le contrôleur est externe au réseau du serveur, vous devrez peut-être entrer l'adresse IP externe du routeur qui redirige le trafic vers le contrôleur.

  La programmation de l'adresse IP, du masque de sous-réseau et de la passerelle par défaut nécessite une connaissance du réseau et du sous-réseau auxquels le système est connecté. Vous devez toujours consulter l'administrateur réseau ou système avant de programmer ces valeurs.
- **Mise à jour dynamique de l'adresse IP** : Lorsque cette option est activée, le logiciel détecte automatiquement l'adresse IP du contrôleur à partir des messages entrants et met automatiquement à jour le champ de l'**adresse IP**. Utilisez cette option dans les cas où l'adresse IP du contrôleur peut changer de façon inattendue, ou lorsque le contrôleur est configuré pour utiliser le protocole DHCP.
- **Nom d'utilisateur / Mot de passe** : Si le service de téléchargement d'enregistrement unique est utilisé, vous devez entrer un nom d'utilisateur et un mot de passe pour le contrôleur afin que le service puisse établir une connexion. Ceux-ci doivent correspondre à un opérateur dans l'interface web du contrôleur.

  Assurez-vous que le **Nom d'utilisateur** est saisi en lettres minuscules, sinon la connexion échouera.

  Ces champs ne sont pas nécessaires lorsque le service de téléchargement d'enregistrement unique n'est pas utilisé.
- **Port de téléchargement** : Le port TCP/IP qui est utilisé par le service de téléchargement pour envoyer les téléchargements de programmation au contrôleur. Par défaut c'est le port 21000.
- **Port de téléchargement d'enregistrement unique** : Le port TCP/IP qui sera utilisé par le service de téléchargement d'enregistrement unique (s'il est utilisé) pour envoyer les téléchargements de programmation au contrôleur. Il doit correspondre au **port HTTPS** du contrôleur. Par défaut, il s'agit du port 443.

- **Serveur de téléchargement** : Définit le serveur de téléchargement qui enverra les téléchargements au contrôleur. Si ce champ est <not set> le contrôleur ne recevra pas de téléchargements.
- **Port pour demande de contrôle et d'état** : Ce champ indique le port qui sera utilisé pour envoyer des commandes manuelles et des demandes d'état au contrôleur via TCP/IP. Par défaut il s'agit du port 21001.
- **Dernière adresse IP connue** : Indique la dernière adresse IP que le contrôleur a utilisée pour communiquer avec le serveur (lecture seule).
- **Dernier téléchargement** : Indique la date et l'heure du dernier téléchargement vers le contrôleur (lecture seule).

Affichage

- **Nom du panneau** : Le nom utilisé pour identifier le contrôleur aux services de rapports IP.

Fenêtres de diagnostic

- **Ouvrir la fenêtre de diagnostic du serveur de téléchargement** : Ouvre une fenêtre listant les transactions entre le contrôleur et le serveur de téléchargement. Cela peut être utile pour vérifier si les récents changements de programmation ont été téléchargés avec succès.
- **Ouvrir la fenêtre de diagnostic du serveur d'événements** : Ouvre une fenêtre montrant l'état actuel du serveur d'événements. Cela peut être utile pour diagnostiquer les problèmes de connexion du contrôleur.

Commandes

- Ce champ est utilisé pour envoyer des commandes de programmation à l'appareil. Il ne doit être utilisé que lorsqu'il est spécifiquement conseillé par la documentation ICT ou le support technique.

Télécharger le blob binaire

- **Définir le téléchargement d'un blob binaire à partir d'un fichier** : Cette fonction vous permet de sélectionner un fichier blob binaire et de le télécharger sur le contrôleur. Ceci est nécessaire pour certaines transitions et intégrations spécifiques.

  N'utilisez pas cette fonction à moins d'être spécifiquement conseillé par ICT.

- **Longueur des données de la base de données (octets)** : La taille du fichier qui a été sélectionné pour le téléchargement.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Contrôleurs | Configuration

Configuration

- **Heure du rapport de test (HH:MM)** : Le contrôleur teste périodiquement le service de rapport en ouvrant l'entrée de dérangement prédéfinie Test de rapport de service. Ce champ définit l'heure à laquelle l'entrée de dérangement sera ouverte.

  Lorsque l'option **L'heure du rapport de test est périodique** est activée dans l'onglet **Options**, l'heure programmée sera utilisée comme période entre les rapports en heures et minutes. Sinon, elle est traitée comme une heure de la journée.

- **Temps hors ligne automatique** : L'heure de la journée à laquelle le contrôleur mettra à jour les utilisateurs et d'autres paramètres hors ligne sur les modules d'expansions intelligents hérités. L'option **Activer le téléchargement automatique** hors ligne doit être activée. Cette option n'est pas utilisée pour les modules de rail DIN.

- **Délai de rétablissement du CA** : L'heure, en secondes, pendant laquelle l'entrée trouble de la panne du CA restera ouverte après une panne du CA avant de se rétablir. Ce réglage ne concerne que le matériel hérité alimenté par une source d'alimentation CA.
- **Heure de défaillance du CA** : L'heure, en secondes, à laquelle la tension secteur CA a failli avant que l'entrée trouble de panne CA ne soit ouverte. Ce réglage ne concerne que le matériel hérité alimenté par une source d'alimentation CA.
- **Port UDP du module** : Certains modules, tels que le module Protege Module Network Repeater, peuvent communiquer avec le contrôleur via une connexion Ethernet en utilisant le protocole UDP. Ce champ définit le port UDP qui sera utilisé pour ces communications. Le port par défaut est 9450. Si ce port est modifié sur le contrôleur, il doit également être mis à jour sur tous les modules concernés.

  After changing this port you must restart the controller for the setting to take effect.

  A partir de la version 2.08.886 du micrologiciel du contrôleur, les communications UDP/TCP du module sont désactivées par défaut. Vous pouvez réactiver les communications en entrant les commandes suivantes dans le champ **Commandes** (onglet **Général**) : `EnableModuleUDP = true` et `EnableModuleTCP = true`.
- **Pays du modem** : Cette option affecte le nombre de tentatives de numérotation effectuées par les services de rapport de ligne téléphonique, et peut remplacer le paramètre **Tentatives de numérotation** du service de rapport. Il est recommandé de tester le nombre de tentatives de numérotation pour s'assurer que vous êtes conforme aux exigences régionales.

  Ce paramètre n'est pris en charge que par les modèles de contrôleur dotés de composeurs modem embarqués.
- **Numéro de téléphone de secours du modem** : Si la communication Ethernet échoue, le modem intégré du contrôleur composera ce numéro pour signaler les événements. L'option **Sauvegarde du module en cas d'échec IP** doit être activée (onglet **Options**).

  Ce paramètre n'est pris en charge que par les modèles de contrôleur dotés de composeurs modem embarqués.
- **Langue par défaut** : La langue par défaut affichée sur le clavier pour les utilisateurs qui n'ont sélectionné aucune langue et pour tous les événements générés par un service d'imprimante de série (voir **Programmation | Services | Imprimante de série**).
- **Délai nouvelle tentative de téléchargement** : Ce champ vous permet de définir un délai minimum (en secondes) entre les téléchargements sur ce contrôleur. Une fois que le serveur de téléchargement aura terminé un téléchargement, il ne tentera pas de télécharger à nouveau vers ce contrôleur avant que le délai ne soit écoulé, sauf dans les circonstances suivantes où le serveur de téléchargement enverra le téléchargement dès que possible sans attendre la période de délai :
  - Lorsqu'une commande **Forcer le téléchargement** est envoyée
  - Lorsque des modifications sont apportées aux dispositifs matériels hébergés par le contrôleur (par ex. modules d'expansion, entrées, sorties)
  - Lorsque le service de téléchargement d'enregistrement unique déclenche un téléchargement complet

  Le délai minimum de réessai est de dix secondes.
- **Enregistrer comme lecteur expanseur** : L'adresse du module assignée au lecteur expanseur embarqué du contrôleur. Vous pouvez programmer le lecteur expanseur embarqué en créant un enregistrement avec la même adresse dans **Expanseurs | Lecteur expanseur**.

  Cette adresse ne doit pas être la même que celle d'un lecteur expanseur physique.
- **Sorties de verrouillage du lecteur embarqué** : Cette option détermine quelles sorties du contrôleur sont affectées aux sorties de verrouillage de l'extension du lecteur embarqué. Elle doit généralement être réglée sur Sorties relais 3/4 du contrôleur, qui associe les sorties 3 et 4 du contrôleur aux sorties 1 et 2 du lecteur extenseur. Si le contrôleur n'est pas utilisé pour le contrôle de porte, cette option peut être réglée sur None.
- **Port UDP de l'écran tactile** : Le port UDP sur lequel un écran tactile Protege communiquera. écran tactile communiquera.

A partir de la version 2.08.886 du micrologiciel du contrôleur, les communications avec l'écran tactile sont désactivées par défaut. Vous pouvez réactiver les communications en entrant la commande suivante dans le champ **Commandes** (onglet **Général**) : `EnableTLCDCommsUDP = true`.

- **Taille maximale des paquets** : La taille maximale des paquets qui peuvent être téléchargés sur le contrôleur.
- **Temps de grâce du contrôleur hors ligne** : Si un contrôleur tombe hors ligne, il y a un temps de grâce fixe d'une minute avant que Protege GX ne commence à indiquer que le contrôleur est hors ligne. Cette option vous permet de prolonger ce temps de grâce d'un certain nombre de minutes. Il convient de l'utiliser dans les situations où le contrôleur passe périodiquement hors ligne et se remet en ligne encore, ce qui vous permet d'éviter les alertes inutiles.

Cryptage

- **Initialiser cryptage du contrôleur** : Active le cryptage des messages envoyés entre le contrôleur et le serveur Protege GX. La sélection de cette option lance un processus unique qui génère de manière aléatoire une clé de cryptage AES de 256 bits. À l'aide d'un algorithme RSA, cette clé est échangée et stockée à la fois dans le contrôleur et dans la base de données Protege GX.
- **Désactiver cryptage du contrôleur** : Indique au logiciel de ne plus utiliser le cryptage. Pour éviter que le cryptage ne soit désactivé par accident ou par malveillance, cette option ne changera pas le réglage du cryptage dans le contrôleur lui-même. Vous devez configurer le contrôleur par défaut pour désactiver complètement le cryptage et permettre les communications.
- **Cryptage activé** : Champ en lecture seule qui indique si le cryptage est activé.

Clé publique HTTPS

- **Clé publique HTTPS** : Si le service de téléchargement de registres uniques est en cours d'utilisation, ce champ affiche la clé publique du certificat HTTPS du contrôleur. Ce champ est automatiquement rempli lorsque le service de téléchargement de registres uniques se connecte au contrôleur pour la première fois. Si le certificat est changé ou si le contrôleur est par défaut, vous devez effacer les informations dans ce champ pour permettre au service de téléchargement d'enregistrements uniques de se reconnecter.

Paramètres de la version 3

Cette section affiche les paramètres qui étaient utilisés dans la version 3 du logiciel et les versions antérieures. Ces paramètres ne nécessitent pas de configuration dans la version 4 ou ultérieure.

Contrôleurs | Configuration (Intégrations)

Les paramètres d'intégration suivants sont disponibles dans l'onglet **Configuration**.

Ascenseur HLI

Type ascenseur HLI : Définit le système d'ascenseur avec lequel le contrôleur s'intègre en utilisant une HLI (High Level Interface). Différentes options sont disponibles en fonction du système d'ascenseur choisi. Choisissez parmi :

- **KONE** : Pour plus de renseignements, consulter la Note d'application 170 : Protege GX intégration HLI KONE.
  - **Adaptateur réseau** : Seul le Câble est pris en charge pour cette intégration.
  - **Port primaire** : Le port TCP/IP pour la communication avec le contrôleur de groupe KONE primaire.
  - **Port secondaire** : Le port TCP/IP utilisé pour les communications avec le contrôleur de groupe KONE secondaire (de secours).
  - **Adresse IP primaire** : L'adresse IP du contrôleur de groupe KONE primaire.
  - **Adresse IP secondaire** : L'adresse IP du contrôleur de groupe secondaire (de secours). L'adresse IP du contrôleur de groupe KONE secondaire (de secours).
  - **Groupe d'étages Source DOP par défaut** : Ce groupe d'étages contient tous les étages qui ont un DOP KONÉ qui peut être utilisé pour appeler les ascenseurs. Ceci définit tous les étages à partir desquels un ascenseur peut partir (c'est-à-dire les étages sources). Cette option s'applique lorsque le système KONE est en ligne avec le contrôleur.

Cette option ne tient pas compte du réglage de l'**horaire** dans la programmation des groupes d'étages.

- **Groupe d'étages Destination DOP par défaut** : Ce groupe d'étages contient tous les étages auxquels on peut accéder librement à tout moment à partir d'un DOP KONE. Ceci définit les étages auxquels un ascenseur peut se rendre (c'est-à-dire les étages de destination). Cette option s'applique lorsque le système KONE est en ligne avec le contrôleur.

  Cette option ne tient pas compte du réglage de l'**horaire** dans la programmation des groupes d'étages. Les groupes d'étages avec horaires peuvent être appliqués à des registres DOP individuels dans **Programmation | Portes | Général**.

- **Groupe d'étages Destination COP par défaut :** Ce groupe d'étages contient tous les étages auxquels on peut accéder librement à tout moment à partir d'un COP KONE. Ceci définit les étages auxquels un ascenseur peut se rendre (c'est-à-dire les étages de destination). Cette option s'applique lorsque le système KONE est en ligne avec le contrôleur.

  Cette option ne tient pas compte du réglage de l'**horaire** dans la programmation des groupes d'étages. Les groupes d'étages avec horaires peuvent être appliqués à des registres COP individuels dans **Programmation | Portes | Général**.

- **Groupe d'étages Source de déconnexion DOP par défaut :** Ce groupe d'étages contient tous les étages avec un DOP KONE qui peut être utilisé pour appeler les ascenseurs pendant que le système KONE est déconnecté du contrôleur. Ceci définit tous les étages qu'un ascenseur peut quitter pendant une panne de communication (c'est-à-dire les étages sources).
- **Groupe d'étages Destination de déconnexion DOP par défaut :** Ce groupe d'étages contient tous les étages auxquels on peut accéder librement à partir d'un COP KONE alors que le système KONE est déconnecté du contrôleur. Ceci définit les étages auxquels un ascenseur peut se rendre pendant une panne de communication (c'est-à-dire les étages de destination).
- **Groupe d'étages Destination de déconnexion COP par défaut :** Ce groupe d'étages contient tous les étages auxquels on peut accéder librement à partir d'un COP KONE alors que le système KONE est déconnecté du contrôleur. Ceci définit les étages auxquels un ascenseur peut se rendre pendant une panne de communication (c'est-à-dire les étages de destination).
- **Activer fonctionnalité appel d'ascenseur** : Active la fonctionnalité de l'interface d'appel à distance KONE (RCGIF). Grâce à cette interface, un utilisateur peut badger sa carte pour appeler un ascenseur qui le conduira automatiquement à l'**étage de destination d'ascenseur** réglé dans son niveau d'accès (**Utilisateurs | Niveaux d'accès | Général**).
  - **Port primaire RCGIF** : Le port TCP/IP sur lequel le contrôleur principal RCGIF KONE est à l'écoute.
  - **Port secondaire RCGIF** : Le port TCP/IP sur lequel le contrôleur KONE RCGIF secondaire (sauvegarde) est à l'écoute.
  - **IP Primaire RCGIF** : L'adresse IP du contrôleur primaire RCGIF KONE.
  - **IP secondaire RCGIF** : L'adresse IP du contrôleur RCGIF KONE secondaire (sauvegarde).
- **Débogage HLI ascenseur :** Lorsque cette option est activée, tous les paquets HLI envoyés et reçus via ethernet sont visualisables à l'aide d'un terminal telnet. Cette fonction ne doit être utilisée que pour le dépannage, et désactivée pendant le fonctionnement normal.

  Pour voir les paquets HLI, configurez un service d'imprimante de série dans **Programmation | Services** et ouvrez une session telnet sur le port configuré. Lorsque des paquets sont échangés entre le contrôleur Protege GX et le contrôleur KONE, les données reçues sont répercutées dans la fenêtre telnet.

  Bien que certaines informations soient affichées en anglais simple, beaucoup de données nécessitent une compréhension de bas niveau du protocole KONE.

- **Thyssenkrupp** : Pour plus de renseignements, consulter la Note d'application 169 : Protege GX intégration HLI ThyssenKrupp.
  - **Adaptateur réseau** : Seul le Câble est pris en charge pour cette intégration.
- **OTIS** : Pour plus de renseignements, consulter la Note d'application 174 : Protege GX intégration HLI Otis Compass.

- **Adaptateur réseau** : Seul le Câble est pris en charge pour cette intégration.
- **Étage de sous-sol le plus bas** : L'étage souterrain physique le plus bas accessible par un ascenseur. Par exemple, s'il y a cinq étages souterrains, la valeur doit être 5. S'il n'y a pas d'étages souterrains, la valeur doit être 0.

  Ce qui est considéré comme un étage souterrain est déterminé par la configuration du système d'ascenseur.

- **Schindler** : Pour plus de renseignements, consulter la note d'application 196 : Protege GXintégration HLI Schindler.
  - **Adaptateur réseau** : Seul le Câble est pris en charge pour cette intégration.
  - **IP primaire du système de port** :} L'adresse IP primaire du serveur Schindler.
  - **Port système secondaire IP** : L'adresse IP secondaire du serveur Schindler (configuration rétrocompatible).
  - **Port Base de données en ligne** : Le port TCP de l'interface de base de données en ligne Schindler.
  - **Port d'interface d'appel** : Le port TCP de l'interface d'appel Schindler.
  - **Port d'interface de signalement de vie** : Le port TCP de l'interface de signalement de vie Schindler.
  - **Étage de sous-sol le plus bas** : L'étage souterrain physique le plus bas accessible par un ascenseur. Par exemple, s'il y a cinq étages souterrains, la valeur doit être 5. S'il n'y a pas d'étages souterrains, la valeur doit être 0.

    Ce qui est considéré comme un étage souterrain est déterminé par la configuration du système d'ascenseur.

  - **Groupe d'étages par défaut** : Le groupe d'étages contenant tous les étages accessibles et les horaires utilisés pour contrôler lorsque chaque étage est librement accessible.

    Ce groupe d'étages peut être créé dans **Groupes | Groupes d'étages**.

  - **Activer l'interface d'appel** : Active l'interface d'appel Schindler.
  - **Activez l'interface de signalement de la vie.** : Active l'interface de signalisation de la vie de Schindler.
  - **Activer le débogage HLI ascenseur :** Lorsque cette option est activée, les messages de débogage du système sont connectés au JournalÉvénement pour le dépannage.

    Cette option peut être utile pour la configuration initiale et le dépannage, mais doit être désactivée pendant le fonctionnement normal afin d'économiser le stockage des événements.

  - **Formats de code d'installation** : Définit les numéros d'installation et les formats des codes d'accès des utilisateurs qui seront envoyés au système Schindler. Les formats de code de site ne sont nécessaires que si des lecteurs et des informations d'identification Schindler sont utilisés pour cette intégration.
    - **Code du site** : Le code de site ou le numéro d'installation des informations d'identification de l'utilisateur qui seront formatées.
    - **Format** : Toutes les informations d'identification qui correspondent au **code du site** défini ci-dessus seront converties dans ce format et envoyées au système Schindler.
    - **Sous-format** : Défini à 0 par défaut. Uniquement pertinent lorsque le **Format** est réglé sur Wiegand inconnu.

    Pour une liste des formats Schindler pris en charge, voir la note d'application 196 : Protege GX Intégration Schindler HLI.

- **MCE** : Pour plus de renseignements, consulter la Note d'application 241 : Protege GXintégration HLI MCE.
  - **Adaptateur réseau** : Seul le Câble est pris en charge pour cette intégration.
  - **Sentinelle MCE IP** : L'adresse IP de l'interface MCE Sentry à laquelle le contrôleur est connecté.
  - **Port de MCE sentry** : Le port TCP que le contrôleur et l'interface MCE Sentry utiliseront pour communiquer.

- **Groupe d'étages par défaut** : Un groupe d'étages comprenant tous les étages accessibles par le système MCE, ainsi que leurs horaires de déverrouillage. Cette carte est utilisée comme carte de sécurité du bâtiment du système MCE.
- **Activer le débogage HLI ascenseur :** Lorsque cette option est activée, les messages de débogage du système sont connectés au JournalÉvénement pour le dépannage.

  Cette option peut être utile pour la configuration initiale et le dépannage, mais doit être désactivée pendant le fonctionnement normal afin d'économiser le stockage des événements.

Redémarrer HLI : Redémarre le service HLI de l'ascenseur.

Intégration entrée module d'expansion

Type d'intégration: Définit l'intégration du module d'expansion entrée pour lequel le contrôleur est utilisé. Choisissez parmi :

- **Redwall** : Pour plus de renseignements, consulter la Note d'application 181 : Protege GX Redwall Integration.
  - **Port** : Le port UDP que le contrôleur utilise pour recevoir les codes d'événement de Redwall.
  - **Port d'intégration du module**: Le port utilisé pour la communication entre le scanner Redwall et le Protege GX contrôleur lorsque le scanner agit comme un module d'expansion d'entrée Protege.
  - **Activer débogage Redwall** : Lorsque cette option est activée, les messages de débogage du système seront enregistrés dans le journal des événements pour le dépannage.

    Cette option peut être utile pour la configuration initiale et le dépannage, mais doit être désactivée pendant le fonctionnement normal afin d'économiser le stockage des événements.
- **Inovonics** : Pour plus de renseignements, consulter la Note d'application 183 : Protege GX Inovonics Integration.
  - **Port** : Définit le port TCP que le contrôleur utilise pour recevoir les codes d'événement Inovonics. Ceci doit être réglé sur le port 80.
  - **Port d'intégration du module:** Définit le port UDP que l'intégration utilise pour écouter les réponses aux demandes de Protege GX. Ceci doit être réglé sur le port 9452.
  - **Adresse IP Inovonics :** L'adresse IP de l'unité ACG Inovonics à laquelle le Protege GX contrôleur est connecté.
  - **Mot de passe Inovonics :** Le mot de passe utilisé par le contrôleur lorsqu'il tente d'accéder aux informations de l'ACG d'Inovonics. Le contrôleur doit se connecter en tant qu'administrateur, assurez-vous donc que le mot de passe saisi est le mot de passe administrateur utilisé pour l'ACG.

Intégration de VingCard Visionline

L'intégration de VingCard VisiOnline est une fonctionnalité sous licence séparée. Pour plus d'informations, voir la note d'application 215 : Protege GX Intégration de VingCard VisiOnline.

- **Activer l'intégration**: Sélectionner cette option pour activer l'intégration de VingCard VisiOnline pour ce contrôleur.
- **Adresse IP** : L'adresse IP du serveur VingCard.
- **Restaurer l'intégration** : Cliquez pour redémarrer l'intégration VingCard Visionline.
- **Port** : Le port TCP du serveur VingCard. Par défaut, il est défini sur 443.
- **Username** : Le nom d'utilisateur du compte à utiliser pour se connecter au serveur VingCard.
- **Mot de passe** : Le mot de passe du compte à utiliser pour se connecter au serveur VingCard.
- **Encodeur VingCard Visionline** : Le nom de l'encodeur à utiliser pour programmer les cartes dans le serveur VingCard.
- **Activer le débogage d'intégration** : Lorsque cette option est activée, les messages de débogage du système sont connectés au JournalÉvénement pour le dépannage.

  Cette option peut être utile pour la configuration initiale et le dépannage, mais doit être désactivée pendant le fonctionnement normal afin d'économiser le stockage des événements.

Contrôleurs | Options

Options

- **L'heure du rapport de test est périodique** : Quand cette option est activée, **l'heure du rapport de test** définie dans l'onglet **Configuration** sera traitée comme une fréquence plutôt que comme une heure de la journée. Par exemple, l'heure du rapport de test de 12h00 entraînera l'ouverture de l'entrée trouble du rapport de test du service toutes les 12 heures si cette option est activée, ou tous les jours à 12h00 si cette option est désactivée.
- **Rapport de test hebdomadaire** : Lorsque cette option est activée, le rapport de test est envoyé une fois par semaine en fonction du jour de la semaine sélectionné. Le Rapport de test du service de l'entrée trouble sera ouvert à l'heure spécifiée dans le champ **Heure du rapport de test** dans l'onglet **Configuration**. Lorsque cette option est désactivée, l'entrée trouble sera ouverte une fois par jour.
- **Jour de la semaine** : Définit le jour de la semaine où le rapport de test hebdomadaire est envoyé.
- **Les troubles nécessitent une reconnaissance** : Les troubles du système sont affichées dans le menu d'affichage des troubles du clavier (**[Menu] [5] [2]**). Normalement, si la condition de trouble se termine (c'est-à-dire si l'entrée trouble se ferme), le trouble n'est plus inclus dans cette liste ; cependant, si cette option est activée, la condition de trouble reste dans la liste jusqu'à ce qu'elle soit reconnue par un utilisateur autorisé.

  Les utilisateurs doivent avoir l'option **Reconnaître les troubles du système** activée dans **Utilisateurs | Utilisateurs | Options** et avoir accès au menu **Affichage (5)** de leur groupe de menu.

- **Générer la restauration de l'entrée sur l'entrée du rapport de test** : Quand cette option est activée, le contrôleur générera un événement de restauration pour la fermeture de l'entrée trouble du rapport de test du service après le rapport de test régulier. Cela se produit une minute après l'activation de l'entrée trouble du rapport de test du service.
- **Signaler une panne de communication de module de courte durée** : Lorsque cette option est activée, le contrôleur générera toujours des événements troubles pour toute panne de communication de module, sans accorder de délai de grâce pour que le module se remette en ligne.
- **Opération UL anticipée**: Lorsque cette option est activée, le Protege GX système fonctionne en mode de conformité UL.

  Ce réglage a les effets suivants :

  - Ajoute un temps de grâce de 10 secondes après l'échec d'un sondage avant qu'un module ne soit signalé comme hors ligne.

    Chaque module envoie un message de sondage au contrôleur toutes les 250 secondes. Le module sera considéré comme hors ligne si aucun sondage n'a été reçu pendant la durée de ce temps de sondage plus le temps de grâce de 10 secondes.

  - Supprime le rapport de toutes les alarmes et/ou événements à signaler à une station de surveillance dans les deux premières minutes de l'alimentation du contrôleur. Le système continuera à envoyer des messages de sondage comme d'habitude.
  - Signale les événements de « sabotage d'entrée » comme des événements d'« entrée ouverte » lorsque la partition à laquelle l'entrée est assignée est armée. Si la partition est désarmée, un message de « sabotage d'entrée » sera envoyé.
  - Limite les **Tentatives de composition** pour les signalisations du SERVICE à un maximum de 8.

  Ce paramètre doit être utilisé en conjonction avec les autres exigences de configuration du manuel d'installation du contrôleur.

- **Entrées duplex** : Lorsque cette option est activée, le contrôleur peut supporter deux fois le nombre d'entrées, câblées en configuration duplex. Pour plus d'informations, voir le manuel d'installation du contrôleur concerné.

Options misc

- **Activer le téléchargement automatique hors ligne** : Lorsque cette option est activée, le contrôleur met automatiquement à jour les utilisateurs et les autres paramètres hors ligne sur les modules d'expansion intelligents hérités au moment de la **mise hors ligne automatique** (onglet **Configuration**). Cette option n'est pas utilisée pour les modules de rail DIN.
- **Sauvegarde du modem en cas de défaillance de l'IP** : Lorsque cette option est activée, le contrôleur compose un numéro via le modem intégré s'il ne peut pas se connecter au logiciel via Ethernet pour signaler des événements. Le **numéro de téléphone du modem de sauvegarde** doit être défini dans l'onglet **Configuration**.

  Ce paramètre n'est pris en charge que par les modèles de contrôleur dotés de composeurs modem embarqués.
- **Sauvegarder uniquement les événements d'alarme** : Avec cette option activée, lorsque le contrôleur a perdu la connexion Ethernet, il ne signalera que les alarmes et autres événements à signaler sur la ligne téléphonique. Tous les événements stockés seront signalés lorsque la liaison Ethernet sera rétablie.

  Ce paramètre n'est pris en charge que par les modèles de contrôleur dotés de composeurs modem embarqués.
- **Inverser l'entrée d'autosurveillance du contrôleur** : Quand cette option est activée, le contrôleur inversera l'entrée d'autosurveillance du module, permettant ainsi l'utilisation d'un interrupteur d'autosurveillance normalement ouvert. Ce paramètre ne concerne que le matériel plus ancien qui comprend une entrée d'autosurveillance intégrée.
- **Enregistrer tous les événements du niveau d'accès** : Il s'agit d'une option héritée qui n'a aucun effet.
- **N'attendez pas la tonalité lorsque le modem compose un numéro** : Lorsque cette option est activée, la numérotation par modem se produit même si aucune tonalité n'est détectée.

  Ce paramètre n'est pris en charge que par les modèles de contrôleur dotés de composeurs modem embarqués.

Contrôleurs | Mise à jour du temps

Lorsque vous utilisez un serveur d'heure, l'heure fournie est toujours en UTC (Temps Universel Coordonné), qui n'a pas de fuseau horaire et n'est pas soumis à des règles d'heure d'été. Cela signifie que vous devez configurer correctement le serveur d'heure, le fuseau horaire dans lequel le contrôleur fonctionne et les réglages d'heure d'été pour que l'heure soit synchronisée correctement. Si l'un de ces paramètres n'est pas configuré, l'heure sera inexacte.
Les paramètres de changement d'heure peuvent être configurés dans **Programmation | Changement d'heure**.

- **Synchroniser automatiquement avec un serveur de temps Internet** : Sélectionnez cette option pour synchroniser automatiquement l'horloge interne du contrôleur avec un serveur de temps Internet.
- **Serveur de temps SNTP primaire** : L'adresse IP du serveur de temps SNTP primaire que le contrôleur utilisera pour mettre à jour son heure.
- **Serveur de temps SNTP secondaire** : L'adresse IP du serveur de temps SNTP secondaire (de secours) que le contrôleur utilisera pour mettre à jour son heure. Ce serveur de temps sera utilisé si le contrôleur ne peut pas se connecter au serveur primaire.
- **Fuseau horaire** : Le fuseau horaire actuel dans lequel le contrôleur est stationné. Chaque fuseau horaire est décrit par son décalage par rapport à GMT et les régions concernées.

Contrôleurs | Format de lecteur personnalisé

Cet onglet vous permet de définir un format de lecteur personnalisé (Wiegand ou Magnetic) qui peut être utilisé par les modules d'expansions du lecteur connectées au contrôleur. Pour utiliser ce format, réglez le **format du lecteur** (**Modules d'expansions | Modules d'expansions du lecteur | Lecteur 1/2**) sur Personnaliser le format .

Voir **Sites | Types d'identifiants** pour d'autres options de configuration d'identifiants personnalisés.

Personnaliser la configuration du lecteur

- **Type de lecteur personnalisé** : Définit le type de lecteur. La sortie des données peut se faire sous forme Wiegand (D0 et D1) ou Magnétique (Clock et Data).
- **Longueur de bits** : Le nombre total de bits qui sont envoyés par le lecteur de cartes pour chaque information d'identification.
- **Début du code du site** : Index où les données de code de site/facilité commencent dans les données d'accréditation transmises. Le compte commence à zéro.
- **Fin du code du site** : Index de la fin du code de site/facilité dans les données d'identification transmises. Le compte commence à zéro.
- **Début numéro de carte** : L'index où commencent les données du numéro de carte dans les informations d'identification transmises. Le compte commence à zéro.
- **Fin numéro de carte** : L'index où se terminent les données du numéro de carte dans les informations d'identification transmises. Le compte commence à zéro.
- **Format de données** : Ce champ décrit comment traiter le code de site/établissement et le numéro de carte reçus du lecteur. Si la taille du code du site/de l'établissement est inférieure à 16 bits et que la taille du numéro de carte est inférieure à 16 bits, réglez le format des données sur Données 16 bits. Sinon, utilisez Données 32 bits.

Options de parité 1 à 4

Il peut y avoir jusqu'à 4 blocs de parité calculés sur les données reçues.

Toutes les options de parité qui ne sont pas utilisées doivent être définies sur 255 .

- **Type de parité 1-4** :} La méthode de calcul de la parité pour le bloc. Il s'agit d'une parité paire ou impaire.
- **Parity location 1-4** : La position du bit de parité dans les données reçues. Le compte commence à zéro.
- **Début de parité 1-4** : L'indice où le bloc de parité commence dans les données reçues. Le compte commence à zéro.
- **Fin de parité 1-4** : L'index où le bloc de parité se termine dans les données reçues. Le compte commence à zéro.

Options binaires

Toutes les options binaires qui ne sont pas utilisées doivent être réglées sur 255 .

- **Définissez le bit 1-4** :} L'index d'un bit activé (un « 1 » logique) dans les données reçues. Le compte commence à zéro.
- **Effacer bit 1-4** : L'index d'un bit effacé (un « Faux » logique) dans les données reçues. Le compte commence à zéro.

Options données de cartes

- **Clé de cryptage AES données de cartes** : Les cartes Salto SALLIS et Aperio peuvent être encodées avec les informations du site/de la carte via le client encodeur ICT. Ce champ définit la clé de décryptage afin que Protege GX puisse décrypter les données de ces cartes.

  Pour plus de renseignements, consulter la note d'application correspondante à chaque intégration.

  Ce domaine définit la clé de cryptage AES des données de carte pour tous les ports de lecteur associés à ce contrôleur.

Commandes manuelles du contrôleur

Un clic droit sur un enregistrement de contrôleur (**Sites | Contrôleurs**) affiche un menu avec des commandes manuelles pour ce contrôleur.

Définir la date et l'heure du contrôleur

Si vous n'utilisez pas un serveur de mise à jour de l'heure pour synchroniser l'heure du contrôleur (voir **Sites | Contrôleurs | Mise à jour de l'heure**), vous pouvez mettre à jour l'heure et la date manuellement à l'aide de cette commande. Pour mettre à jour manuellement l'heure d'un contrôleur:

1. Cliquer à droite sur l'enregistrement du contrôleur dans **Sites | Contrôleurs**.
2. Le champ **Temps** affiche la date et l'heure actuelles du serveur. Si vous devez les modifier, entrer de nouvelles valeurs dans le champ ou cliquer sur l'icône de l'horloge pour utiliser le sélecteur d'heure et de date.
3. Cliquer sur **Définir la date et l'heure du contrôleur** pour envoyer l'heure saisie au contrôleur.

Mettre à jour les modules

Les changements de programmation qui modifient le fonctionnement du matériel nécessitent une mise à jour du module pour télécharger les paramètres spécifiques au matériel. Une commande de mise à jour du module entraîne le redémarrage du module.

Utilisez cette option pour effectuer une mise à jour du module sur le contrôleur et tous les modules connectés.

Avertissement : L'envoi de cette commande entraîne la mise hors ligne temporaire du contrôleur et de chaque module connecté pendant leur redémarrage. Cette option ne doit **pas** être utilisée dans un système actif.

Pour mettre à jour uniquement un module spécifique (tel qu'un module d'expansion du lecteur de clavier ou de lecteur), faites un clic droit sur l'enregistrement spécifique dans la programmation des **modules d'expansion** du lecteur et cliquez sur **Mettre à jour le module** .

Forcer le téléchargement

En fonctionnement normal, le service de téléchargement vérifie les modifications apportées à chaque contrôleur dans l'ordre de l'ID Base de donnée. Si des modifications sont détectées, les services téléchargent les modifications sur ce contrôleur, puis passent au contrôleur suivant.

Un opérateur peut utiliser la commande **Forcer le téléchargement** pour augmenter la priorité d'un contrôleur spécifique, afin qu'il soit le prochain dans la file d'attente après que le contrôleur précédent ait été complété. Le **Délai nouvelle tentative de téléchargement** sera ignoré afin que le téléchargement soit envoyé dès que possible.

Par ailleurs, le service de téléchargement télécharge vers le contrôleur même si aucune modification n'est détectée.

Obtenir le statut de santé

La fonction **Obtenir le statut de santé** envoie une commande au contrôleur pour récupérer son statut de santé actuel. La fenêtre de statut de santé s'ouvre, affichant tout avis ou problème relatif au contrôleur ou à son réseau de modules.

Le bouton **Effacer** peut être utilisé pour effacer certains avis qui ne nécessitent pas d'action (par ex. « Le Contrôleur a été redémarré »).

La fenêtre de statut de santé est statique. Le fait de résoudre ou d'effacer les avis n'entraîne pas la mise à jour du statut jusqu'à ce que la commande **Obtenir le statut de santé** soit envoyée à nouveau.

Adressage de modules

La commande **Adressage de modules** permet de visualiser le matériel connecté au réseau du système et de définir les adresses des modules. En sélectionnant cette option, une fenêtre s'ouvre affichant les détails de tous les modules qui sont actuellement connectés, ainsi que ceux qui ont été enregistrés précédemment mais qui sont actuellement hors ligne.

Par défaut, les modules Protege sont expédiés de l'usine avec une adresse de 254. Ceci est en dehors de la plage acceptée par le contrôleur, l'adresse doit donc être définie par l'installateur. Pour certains modules, comme les claviers, l'adresse réseau peut être définie dans le module lui-même (consulter le manuel d'installation correspondant). Pour la plupart des modules Protege, l'adresse est définie dans la fenêtre **Adressage de modules**.

L'adresse du module d'expansion du lecteur embarqué du contrôleur est définie par le réglage **Enregistrer comme module d'expansion de lecteur** dans **Sites | Contrôleurs | Configuration**.

Réglage des adresses réseau des modules

1. Assurez-vous que le contrôleur est correctement alimenté et qu'il communique avec le logiciel Protege GX.
2. Connectez le(s) module(s) nécessitant un adressage au réseau de modules. Assurez-vous que le voyant d'alimentation de chaque module est allumé et que l'indicateur d'état commence à clignoter rapidement.
3. Laissez un peu de temps au(x) module(s) pour tenter de s'enregistrer auprès du contrôleur.
   - Si le module a l'adresse par défaut de 254 ou a la même adresse qu'un autre module, l'indicateur de défaut commence à clignoter avec un code d'erreur.
   - Si le module a déjà été adressé et qu'il n'est pas un doublon, il réussit à s'enregistrer et l'indicateur état commence à clignoter à intervalles d'une seconde.
4. Une fois que tous les modules ont terminé le processus d'enregistrement (réussi ou non), ouvrez le logiciel Protege GX et naviguez vers **Sites | Contrôleurs**.
5. Cliquez du bouton droit de la souris sur l'enregistrement du contrôleur et sélectionnez **Adressage du module** pour ouvrir la fenêtre d'adressage du module. Cette fenêtre affiche tous les modules qui sont connectés au contrôleur avec les informations suivantes :
   - Le type de module (par exemple, contrôleur, clavier, etc.)
   - Le numéro de série
   - La version actuelle du micrologiciel et le numéro de compilation
   - L'adresse actuelle du module
   - Si l'adresse du module peut être modifiée (par exemple, l'adresse du contrôleur ne peut pas être modifiée)
   - Si le module a été enregistré avec succès auprès du contrôleur
   - Si le module est actuellement en ligne.

   Le module d'expansion intégré au contrôleur apparaîtra dans cette liste comme un module d'expansion du lecteur ayant le même numéro de série que le contrôleur. L'adresse de ce module d'expansion doit être définie dans le champ **Enregistrer comme module d'expansion de lecteur** (onglet **Configuration**).
6. Avant d'attribuer des adresses aux modules, vous devrez peut-être identifier des modules physiques spécifiques :
   - Pour les modules rail DIN, cliquez sur le bouton **Recherche** pour activer le mode d'identification pendant la durée spécifiée. En mode identification, les indicateurs d'état et de défaut clignotent en alternance, vous permettant d'identifier le module spécifique.
   - Pour tous les modules, comparez la colonne **En série** avec le numéro de série de chaque module (qui se trouve sur l'étiquette du module).
7. Pour chaque module, définissez l'adresse réseau dans la colonne **Adresse**. Les nouvelles adresses seront affichées en **caractères gras**, indiquant qu'elles n'ont pas encore été mises à jour dans les modules.
8. Transférez les adresses dans les modules en cliquant sur **Mise à jour** pour chaque module individuel ou en cliquant sur **Mettre tous à jour**. Laissez environ 5 secondes au module pour qu'il se réenregistre auprès du contrôleur à la nouvelle adresse.
9. Cliquez sur **Actualiser**. Les nouvelles adresses doivent passer du caractère gras à la police normale et les modules nouvellement adressés doivent être en ligne.
   - Si l'adresse n'a pas changé, vérifiez que le module a terminé sa tentative d'enregistrement auprès du contrôleur.
   - Si l'adresse a changé mais que le module n'est pas enregistré ou en ligne, vérifiez que l'adresse est dans la plage des adresses valides et qu'elle n'est pas un doublon de l'adresse d'un autre module.

Une fois que tous les modules sont en ligne et enregistrés avec les adresses souhaitées, le processus d'adressage est terminé.

Legacy Protege Les modules PCB ne peuvent pas être adressés par ce processus. Ils doivent être adressés à l'aide de commutateurs DIP comme décrit dans le manuel d'installation correspondant.

Nombre max. d'adresses de modules

Le contrôleur Protege a une limite fixe sur le nombre de modules de chaque type qu'il peut supporter. Cela s'applique aux modules physiques et virtuels. Le nombre maximum d'adresses disponibles pour chaque type de module est indiqué dans le tableau ci-dessous :

Type de module	Adresse maximale
Clavier	200
Module d'expansion de zone	248
Module d'expansion du lecteur	64
Module d'expansion de sortie	32
Module d'expansion analogique	32
Lecteur intelligent	248

Tout module dont l'adresse est supérieure à ces limites ne sera pas mis en ligne avec le contrôleur. Un message sera généré dans le statut de santé du contrôleur.

Mettre à jour le firmware

Utilisez l'option **Mettre à jour le micrologiciel** pour mettre à jour le micrologiciel d'un ou plusieurs contrôleurs.

Les contrôleurs ne prennent pas en charge la mise en défaut et la mise à niveau du micrologiciel en même temps. Avant de mettre à niveau le micrologiciel du contrôleur, assurez-vous que la liaison filaire utilisée pour la mise en défaut du contrôleur n'est **pas** connectée.

1. Cliquez sur le bouton ellipsis**[...]** et recherchez le fichier .bin du micrologiciel. Cliquez sur **Ouvrir** .
2. Cochez les cases du ou des contrôleurs que vous souhaitez mettre à jour.
3. Cliquez sur **Mise à jour** .

Ce processus prendra environ 10 minutes par contrôleur et il est recommandé d'effectuer les mises à jour du micrologiciel lorsque le site est fermé pour maintenance ou en période de faible activité. Le contrôleur ne sera pas en mesure d'exécuter sa fonction normale pendant la mise à jour du micrologiciel.

Un message contextuel peut apparaître dans l'interface utilisateur avec le message Mise à jour interrompue. Il s'agit d'un comportement attendu pour certaines versions du micrologiciel et cela n'indique pas que la mise à jour a échoué.

Ajout d'un contrôleur

Pour ajouter un contrôleur au Protege GX système, naviguez dans **Sites | Contrôleurs** et cliquez sur **Ajouter** . Plusieurs options sont disponibles, vous permettant de définir les enregistrements qui seront créés avec votre contrôleur.

- **Utilisez l'assistant du contrôleur** : L'assistant du contrôleur vous permet de spécifier les entrées, les sorties, les portes et les modules d'expansions requis par votre site. Certaines options supplémentaires peuvent également être configurées. Les enregistrements par défaut sélectionnés sont automatiquement ajoutés à la base de données avec le contrôleur.
- **Ajouter simplement un Contrôleur**: Seul l'enregistrement du contrôleur lui-même est ajouté à la base de données. Tous les autres enregistrements doivent être programmés séparément.

- **Ajoutez un nouveau contrôleur basé sur un contrôleur existant** : L'enregistrement du contrôleur et toute la programmation connectée sont dupliqués à partir d'un contrôleur existant. Cela comprend des dispositifs tels que les modules d'expansions, les entrées, les sorties et les portes.

  Il peut être pratique de créer un enregistrement de contrôleur "modèle" qui servira de base à l'ajout de nouveaux contrôleurs.

Une fois l'enregistrement du contrôleur créé, mettez-le en ligne en saisissant le **numéro de série**, **l'adresse IP**, **le port de téléchargement**, **le serveur de téléchargement** et **le port de demande de contrôle et d'état** dans l'onglet **Général**. Si le contrôleur ne se met pas en ligne, vous devrez dépanner la connexion (consultez la page 35).

Ajout d'un contrôleur avec des Enregistrements par défaut

Lorsque vous sélectionnez **Utiliser l'assistant du contrôleur**, la fenêtre **Ajouter une configuration de contrôleur** s'affiche. Cela vous permet d'ajouter automatiquement des enregistrements par défaut (entrées, sorties, modules d'expansion, portes) à côté du contrôleur. Les enregistrements ont des noms et des paramètres par défaut, et peuvent être renommés, modifiés ou supprimés selon les besoins.

Général

- **Nom** : Le nom du contrôleur dans le Protege GX logiciel.
- **Compter** : Le nombre de contrôleurs qui seront ajoutés avec les mêmes enregistrements par défaut. Si plus d'un contrôleur est ajouté, les contrôleurs suivants se verront attribuer des noms par défaut qui pourront être modifiés ultérieurement.
- **Prédire le nom du contrôleur aux enregistrements ajoutés** : Lorsque cette option est activée, tous les nouveaux enregistrements générés par l'assistant incluront le nom du contrôleur au début du nom de l'enregistrement. Par exemple, si le contrôleur est nommé Bureau, la première sortie du contrôleur aura le nom Bureau CP1 Sirène 1 .

Contrôleur

- **Type** : Le code du modèle du contrôleur qui est ajouté au système. Elle est affichée en haut à droite de la face du contrôleur.
- **Entrées** : Le nombre d'entrées intégrées qui seront créées pour le contrôleur. Ce paramètre est défini automatiquement en fonction du **Type** de contrôleur sélectionné.

  Toutes les entrées du contrôleur peuvent ne pas être nécessaires si le module d'expansion du lecteur intégré est utilisé, car les entrées peuvent être affectées à l'enregistrement du module d'expansion du lecteur.

- **Sorties** : Le nombre de sorties intégrées qui seront créées pour le contrôleur. Ce paramètre est défini automatiquement en fonction du **Type** de contrôleur sélectionné.

  Ce nombre ne comprend que la cloche et les sorties relais (sorties 1, 3 et 4). Les sorties des lecteurs sont affectées à l'enregistrement du module d'expansion du lecteur embarqué (même s'il n'est pas utilisé pour les lecteurs connectés).

  La sortie du contrôleur 2 n'existe que sur le matériel ancien. Cette adresse est ignorée lorsque l'assistant ajoute automatiquement les enregistrements par défaut.

- **Ajouter des entrées troubles** : Activer cette option pour ajouter automatiquement les entrées trouble associées au contrôleur.

Claviers, modules d'expansions d'entrée, modules d'expansions du lecteur, modules d'expansions de sortie et modules d'expansions analogiques.

Saisir le **type** et le numéro de chaque module d'expansion qui doit être ajouté à ce contrôleur. Le nombre d'entrées et de sorties nécessaires devrait être défini automatiquement. Activer l'option **Ajouter des entrées trouble** pour inclure les entrées trouble pour chaque module.

Si le module d'expansion du lecteur intégré au contrôleur est utilisé, il doit être inclus dans le nombre des modules d'expansions du lecteur afin que la programmation correspondante puisse être créée.

Options

- **Créer le groupe de menu " Installer "** : Crée un groupe de menu avec chaque menu activé pour être utilisé par les installateurs de sites.
- **Créer un plan d'étage** : Crée un plan d'étage comprenant toutes les entrées et sorties du contrôleur. Cette fonction est utile pour les petits sites ne comportant que quelques entrées et sorties. Pour les sites plus importants, il est généralement préférable de créer les plans d'étage manuellement.
- **Carte de rapport CID** : La carte de rapport Contact ID qui sera utilisée pour attribuer **l'ID de rapport** à chaque entrée. Les options sont :
  - **Standard** : Convient aux petites installations d'effraction et de contrôle d'accès.
  - **Large** : Convient aux installations de détection d'intrusion avec un grand nombre de modules d'expansions d'entrée.
  - **SIMS II**: Une variante du format Contact ID qui peut envoyer un nombre beaucoup plus important d'entrées. Pour que ce mappage fonctionne correctement, le service doit également être configuré pour SIMS II en définissant l'option de **Cartographie cid** pour un service Contact ID, ou l'option de **Paramètres carte CID** pour un service Report IP.

Pour plus d'informations, voir la note d'application 316 : Rapports au format Contact ID dans Protege GX et Protege WX.

Portes

- **Portes** : Création automatique du nombre défini d'enregistrements de porte. En général, cela devrait être 2 portes par module d'expansion du lecteur.
- **Attribuer aux modules d'expansions du lecteur** : Attribue automatiquement les portes aux ports des modules d'expansions du lecteur, dans l'ordre de leur création.
- **Ajouter des portes pour les entrées trouble** : Crée les entrées trouble pertinentes pour chaque enregistrement de porte.
- **Affecter la sortie de verrouillage du lecteur à la configuration de la porte** : Configure automatiquement la **sortie de verrouillage** de chaque porte à la sortie relais du module d'expansion du lecteur associé.
- **Assigner beeper du lecteur à la configuration de l'alarme de porte** : Configure automatiquement la **sortie de pré-alarme**, la **sortie d'alarme d'ouverture à gauche** et la **sortie de porte** forcée pour chaque porte à la sortie du beepeur du module d'expansion du lecteur associé.

Ajout d'un contrôleur basé sur un contrôleur existant

Lorsque vous sélectionnez **Copier un contrôleur existant**, la fenêtre **Copier la configuration du contrôleur** s'affiche. Cela vous permet de sélectionner le contrôleur à copier et de configurer certaines options.

Les enregistrements copiés comprennent les entrées, les sorties, les portes, les partitions et les groupes associés à ce contrôleur.

Le nouvel enregistrement du contrôleur aura un **Numéro de série**, une **adresse IP** et un **Serveur de téléchargement** vides.

- **Site (copie de)** : Définit le site à partir duquel la programmation sera copiée.
- **Contrôleur (copie de)** : Définit le contrôleur à partir duquel la programmation sera copiée.
- **Nouveau nom du contrôleur**: Le nom du nouveau contrôleur dans le Protege GX logiciel.
- **Nom (deuxième langue)** : Le nom du nouveau contrôleur dans la deuxième langue.
- **Faire précéder le nom du contrôleur de tous les noms d'enregistrements** : Lorsque cette option est activée, tous les nouveaux enregistrements générés par le processus de copie comporteront le nom du nouveau contrôleur au début du nom de l'enregistrement. Cela signifie que tous les nouveaux enregistrements auront le même nom que ceux du contrôleur d'origine, avec le nom du nouveau contrôleur ajouté.

  Si les enregistrements originaux comprenaient le nom du contrôleur, ce nom sera toujours inclus dans les nouveaux enregistrements (c'est-à-dire qu'il ne sera pas remplacé par le nouveau nom).

- **Copier les niveaux d'accès** : Lorsque cette option est activée, les niveaux d'accès du contrôleur d'origine sont copiés pour le nouveau contrôleur. Les nouveaux niveaux d'accès sont affectés aux portes, partitions et autres enregistrements équivalents du nouveau contrôleur, mais ne sont affectés à aucun utilisateur.
- **Copier des enregistrements globaux** : Lorsque cette option est activée, les enregistrements de l'ensemble du site, tels que les horaires et les codes de fonction, seront copiés pour être utilisés avec le nouveau contrôleur.

Lecteurs biométriques

Protege GX peuvent être intégrés aux systèmes d'identification biométrique, ce qui vous permet d'utiliser des identifiants biométriques tels que les empreintes digitales et la reconnaissance faciale pour autoriser l'accès aux portes.

L'intégration de lecteurs biométriques est une fonctionnalité sous licence séparée. Pour plus d'informations, voir Note d'application 264 : Intégration de Biometric Suprema avec Protege GX et Note d'application 297 : Intégration biométrique de l'identité Princeton avec Protege GX.

Lecteurs biométriques | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Configuration

- **Adresse IP** : L'adresse IP du lecteur biométrique.
- **Port IP** : Le port qui sera utilisé pour communiquer avec le lecteur biométrique.
- **Type** : La marque du lecteur biométrique.
- **Type secondaire** : Le type secondaire ou sous-type de lecteur biométrique, le cas échéant. Pour l'intégration Suprema, cela indique si le système Suprema utilise Biostar 1 (version 1) ou Biostar 2 (version 2).
- **Télécharger automatiquement les utilisateurs sur ce lecteur**. : Lorsqu'il est activé, le serveur de téléchargement télécharge automatiquement les utilisateurs vers le lecteur. Désactivez cette option si vous ne voulez pas que les utilisateurs soient téléchargés. Par exemple, si le lecteur est uniquement utilisé pour l'enrôlement (capture des empreintes digitales) et n'est pas fixé à une porte pour l'accès.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Niveaux de sécurité

Les niveaux de sécurité définissent l'accès d'un opérateur au sein du système Protege GX. Vous pouvez ajouter des niveaux de sécurité aux rôles dans **Global | Rôles | Niveaux de sécurité** pour contrôler plus précisément ce que les opérateurs individuels peuvent voir ou faire, ou limiter les opérateurs à des groupes d'enregistrements particuliers. Les autorisations accordées dans un niveau de sécurité remplacent celles accordées dans le rôle.

Pour plus d'informations, consultez la section Rôles | Niveaux de sécurité (la page 68). Pour un exemple de programmation, voir la Note d'application 247 : Utilisation des groupes d'enregistrement dans Protege GX.

Niveaux de sécurité | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Niveaux de sécurité | Tableaux

L'onglet Tableaux détermine les autorisations dont dispose chaque niveau de sécurité pour les différents tableaux de la base de données d'un site. Les autorisations accordées ou refusées ici peuvent être utilisées pour remplacer celles attribuées dans la programmation des rôles.

Pour chaque tableau, sélectionnez l'une des options suivantes :

- Reprendre à partir du rôle pour conserver les autorisations du rôle auquel ce niveau de sécurité est attribué.
- Refuser pour empêcher l'accès aux données contenues dans le tableau. Cela permet de cacher à l'opérateur toutes les fonctions et options de menu pour ce tableau.
- Autoriser l'accès complet pour accorder des droits complets de lecture/écriture vers les tableaux.
- Accorder un accès en lecture seule pour accorder l'accès, mais pas à la mise à jour des données dans le tableau. L'opérateur pourra voir les paramètres pertinents, mais les options pour les mettre à jour sont désactivées.

Niveaux de sécurité | Commandes manuelles

Les commandes manuelles permettent à un opérateur de contrôler manuellement un dispositif à partir du logiciel Protege GX : par exemple, un clic droit sur une porte et son déverrouillage à partir d'un plan d'étage. Les paramètres des commandes manuelles définissent les commandes manuelles spécifiques qui sont disponibles pour les opérateurs ayant ce niveau de sécurité.

Pour chaque commande, choisissez entre Reprendre (du rôle), Autoriser ou Refuser.

Commandes de contrôle des appareils

Définis les autorisations pour contrôler les zones, les portes, les ascenseurs, les claviers et les sorties. Ces commandes peuvent être activées par un clic droit sur l'enregistrement concerné dans une liste d'enregistrements, une page du statut ou un plan d'étage. Pour plus d'informations sur ces commandes, consultez la section Commandes manuelles pour chaque élément concerné dans ce manuel.

Vous pouvez également définir des groupes d'enregistrements pour limiter davantage le contrôle. Par exemple, un gardien peut n'être autorisé à contrôler le groupe de portes que dans la zone du bâtiment qui lui est attribuée.

Diverses commandes

- **Contrôle d'entrée**: Cliquer avec le bouton droit de la souris sur un enregistrement d'entrée pour le contourner, le contourner de façon permanente ou supprimer le contournement de l'entrée.
- **Redémarrer et arrêter les services**: Cliquer avec le bouton droit de la souris sur un enregistrement de service pour démarrer ou arrêter le service.
- **Réinitialiser les commandes de l'utilisateur**: Cliquer avec le bouton droit de la souris sur un enregistrement d'utilisateur pour réinitialiser le statut anti-passback de l'utilisateur.
- **Mettre à jour les commandes du module**: Cliquer avec le bouton droit de la souris sur l'enregistrement d'un module (par ex. le lecteur d'extension) pour effectuer une mise à jour du module.
- **Contrôle de la variable**: Cliquer avec le bouton droit de la souris sur une icône de variable sur un plan d'étage pour définir manuellement la valeur de la variable.
- **Contrôle des fonctions programmables**: Cliquer avec le bouton droit de la souris sur un enregistrement de fonction programmable pour lancer ou arrêter la fonction.
- **Mettre à jour l'heure du contrôleur**: Cliquer avec le bouton droit de la souris sur un enregistrement de contrôleur pour mettre à jour la date et l'heure du contrôleur.
- **Changer l'ouverture de vérification dans les clés**: Dans l'intégration de Salto SHIP, les événements de porte hors ligne sont stockés dans les clés utilisateur. Cette option détermine si un opérateur est autorisé à désactiver ou à activer la vérification dans les clés utilisateur dans **Salto | Portes Salto | Général** ou **Utilisateurs | Utilisateurs | Salto**.
- **Commandes Allegion** : Faites un clic droit sur une porte Allegion pour la verrouiller ou la déverrouiller.

Groupes de registres

Les groupes de registres permettent de diviser un site en groupes fonctionnels, qui peuvent être utilisés pour limiter l'accès des opérateurs en utilisant des rôles et des niveaux de sécurité. Ils facilitent également le tri, la recherche et le rapport pour un grand nombre de registres. C'est idéal pour les grands systèmes où il peut être pratique de regrouper les registres par bâtiment, succursale ou région.

La plupart des types de registres du système Protege GX vous permettent d'attribuer un groupe de registres à chaque registre individuel. D'autres types de registres, tels que les sorties, les entrées, les entrées troubles et les modules d'expansion ne peuvent se voir attribuer un groupe de registres, et ils héritent à la place du groupe de registres attribué au contrôleur.

Pour des exemples de programmation, consulter la note d'application 247 : Utilisation des groupes de registres dans Protege GX.

Groupes de registres | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Groupe de registres parent** : Attribuer un autre groupe de registres qui servira de « parent » à celui-ci. Tout ce qui est inclus dans un groupe de registres enfant sera inclus dans le groupe de registres parent, et plusieurs groupes enfants peuvent être attribués à un parent.

  Cela vous permet de créer une hiérarchie de groupes de registres. Par exemple, un responsable régional peut être en mesure de voir les registres de plusieurs succursales (chacune ayant son propre groupe de registres), tandis que le responsable global peut accéder aux registres de chaque région.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Groupe de registres | Données personnalisées

Données personnalisées

- **Données numériques** : Un nombre qui identifie le groupe de registres. Ces informations sont incluses dans le schéma XML des groupes de registres et peuvent être utilisées pour identifier le groupe de registres dans des intégrations tierces personnalisées.
- **Données texte** : Une chaîne de texte qui identifie le groupe de registres. Ces informations sont incluses dans le schéma XML des groupes de registres et peuvent être utilisées pour identifier le groupe de registres dans des intégrations tierces personnalisées.

Types d'informations d'identification

Les types d'informations d'identification permettent au système de Protege GX d'utiliser divers types de données personnalisées – telles que les plaques d'immatriculation, les codes barres, les codes QR, les informations d'identification biométriques ou Wiegand personnalisés – pour identifier les utilisateurs. Lorsque des données sont envoyées à Protege GX depuis un système tiers (via RS-485 ou Ethernet), un type d'informations d'identification peut être utilisé pour interpréter ces données comme informations d'identification d'un utilisateur spécifique.

Par exemple, un système tiers de reconnaissance de plaques d'immatriculation (RPI) peut envoyer des données ASCII à Protege GX, qui utilise la programmation du type d'informations d'identification pour « traduire » ces données en plaques d'immatriculation spécifiques.

Les types d'informations d'identification peuvent être appliqués à des types de portes personnalisés comme **mode de lecture d'entrée/de sortie** (**Programmation | Types de portes | Général**). Le **format du lecteur** doit également être défini sur Custom Credential dans le port du module d'expansion du lecteur ou le lecteur intelligent qui reçoit les données des informations d'identification. Des informations d'identification spécifiques peuvent être saisies dans les registres d'utilisateurs sous **Utilisateurs | Utilisateurs | Général**.

Pour plus de renseignements, consulter la Note d'application 276 : Configuration des types d'informations d'identification dans Protege GX.

Types de conformité

Les types de conformité sont une implémentation spécifique des types d'informations d'identification qui vous permettent de contrôler l'accès en fonction de toute exigence de conformité personnalisée qui peut être saisie pour un utilisateur. Par exemple, l'accès peut être contrôlé sur la base de l'initiation à la santé et à la sécurité, du permis de conduire ou du statut actuel de certification du secteur.

Les types de conformité peuvent fournir une panne d'accès permanente ou temporaire, ainsi que des messages d'avertissement ou d'expiration dont il faut accuser réception, ce qui vous permet d'établir un registre des problèmes de conformité sur le site.

Pour plus de renseignements et des exemples de programmation, consulter la Note d'application 286 : Programmation des types de conformité dans Protege GX. Les messages d'avertissement et d'expiration nécessitent un lecteur de carte à écran tactile ICT compatible.

ID utilisateur

Le type d'informations d'identification de l'ID utilisateur généré par le système est utilisé pour l'accès au clavier par doubles informations d'identification (lorsque l'option **Exiger une double identification pour l'accès au clavier** est activée dans **Global | Sites | Valeurs par défaut du site**). Pour plus de renseignements, consulter la Note d'application 275 : Configurer des améliorations de la sécurité du site dans Protege GX.

Veuillez **ne pas** modifier ou supprimer le type d'informations d'identification de l'ID utilisateur. Cela entraîne des problèmes d'accès critiques.

Types d'informations d'identification | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

Configuration

- **Format** : Les données qui sont envoyées au contrôleur Protege GX par l'appareil tiers. Les formats pris en charge incluent :
  - **Unicode** : Les données d'identification envoyées au contrôleur utilisent deux octets pour représenter chaque caractère conformément à la norme Unicode.
  - **UTF8** : Les données d'identification envoyées au contrôleur utilisent un nombre variable d'octets pour représenter chaque caractère conformément à la norme UTF-8.
  - **ASCII** : Les données d'identification envoyées au contrôleur utilisent un seul octet pour représenter chaque caractère conformément à la norme ASCII.
  - **Numérique** : Les données d'identification envoyées au contrôleur sont un nombre binaire composé de 8 octets au maximum. Les octets sont ordonnés selon la méthode « little endian ». Les paramètres des caractères précédents, suivants et préfixes sont ignorés.
  - **Hexadécimal** : Les données d'identification sont envoyées au contrôleur sous la forme d'un tableau de nombres binaires. Lorsque l'identifiant spécifique est entré dans la programmation utilisateur pour chaque utilisateur, le format utilisé est hexadécimal avec les chiffres 0-9 et les lettres A-F représentant chaque bit de l'identifiant.
  - **Wiegand** : Les informations d'identification envoyées au contrôleur ou au module d'expansion du lecteur sont composées d'un flux binaire Wiegand.

    Ce flux binaire peut être codé de nombreuses façons différentes et un descripteur de format doit être inclus dans le champ **Wiegand ou TLV format**. Pour le format Wiegand, il n'est pas tenu compte des caractères précédents, suivants et préfixes, ni de la casse.
  - **TLV** : Cette option est réservée pour un développement futur.
  - **Conformité** : Un type d'identification spécial qui vous permet d'utiliser des exigences personnalisées telles que des certificats de santé et de sécurité, des permis de conduire et des qualifications industrielles comme identifiants. Ce type d'informations d'identification peut être utilisé avec les contrôleurs et les modules d'expansion.

  Différentes options sont disponibles ci-dessous lorsque ce champ est réglé sur Conformité.
- **Parce que les caractères précédents** : Le nombre maximum de caractères qui peuvent être ignorés au début du paquet de données reçu par le contrôleur. Si l'identifiant est trouvé avant que ce nombre de caractères soit compté, il sera quand même accepté.

  Ce réglage est déterminé par l'appareil/application tiers.
- **Caractères de fin** : Le nombre maximum de caractères qui peuvent être ignorés à la fin du paquet de données reçu par le contrôleur. S'il y a moins que ce nombre de caractères de queue après que l'identifiant est trouvé, l'identifiant sera quand même accepté.

  Par exemple, ce champ peut être défini sur 1 pour garantir que les informations d'identification seront acceptées même si elles sont suivies d'un caractère de retour chariot.

  Ce réglage est déterminé par l'appareil/application tiers.
- **Préfixe** : Les caractères qui doivent figurer au début du paquet de données d'identification envoyé au contrôleur.

  Ce réglage est déterminé par l'appareil/application tiers.
- **Sensible à la casse** : Définit si les données sont sensibles ou non à la casse.

  Ce réglage est déterminé par l'appareil/application tiers.

- **Valeur unique** : Lorsque cette option est activée, les justificatifs d'identité dupliqués ne sont pas autorisés (c'est-à-dire que deux utilisateurs ne peuvent pas avoir le même justificatif d'identité). Lorsqu'elle est désactivée, les justificatifs d'identité en double sont autorisés.

  Si les valeurs d'identification non uniques sont autorisées, assurez-vous que tout type de porte utilisant ce type d'identification requiert également une identification unique (par exemple, une carte) pour l'authentification à deux facteurs afin que Protege GX puisse identifier avec précision l'utilisateur demandant l'accès.

- **Limite des informations d'identification par utilisateur** : Cette option vous permet de restreindre le nombre d'informations d'identification qui peuvent être ajoutées à chaque utilisateur par le biais du logiciel Protege GX. La limite des informations d'identification est définie sur Illimité par défaut, et peut être limitée à un nombre de 1 à 10.

  Les types de conformité sont toujours illimités.

  Il n'est pas possible de définir une limite d'informations d'identification si un ou plusieurs utilisateurs possèdent déjà plus que le nombre maximum d'informations d'identification. Vous pouvez effectuer une recherche d'utilisateur (**Utilisateurs | Recherche d'utilisateur**) avec la colonne Type d'informations d'identification pour voir quels utilisateurs ont des informations d'identification excédentaires.

  Le service SOAP ignore la restriction du nombre d'informations d'identification.

Définir l'inactivité de l'identifiant de l'utilisateur par défaut

Cette section n'est pas disponible pour les types de conformité.

- **Désactiver les informations d'identification des utilisateurs inactifs** : Lorsque cette option est activée, les nouveaux utilisateurs ajoutés au système auront automatiquement une **période d'inactivité** par défaut appliquée à ce type d'informations d'identification (**Utilisateurs | Utilisateurs | Général**). Si l'utilisateur n'utilise pas les informations d'identification pendant cette période, elles seront désactivées.

  Lorsque vous enregistrez une modification de ce paramètre, vous êtes invité à appliquer la modification à tous les utilisateurs. Sélectionnez **Oui** pour remplacer les paramètres programmés dans les enregistrements individuels des utilisateurs par la nouvelle valeur par défaut. Cette opération peut prendre un certain temps pour les sites comptant un grand nombre d'utilisateurs. Si vous sélectionnez **Non**, le paramètre par défaut ne sera appliqué qu'aux utilisateurs ajoutés après la modification.

- **Période d'inactivité des informations d'identification par défaut** : Réglez le nombre de jours, d'heures ou de minutes pendant lesquels les informations d'identification doivent être inactives avant d'être désactivées.

  La période d'inactivité maximale est de 365 jours. Si vous saisissez une période plus longue, le champ sera réinitialisé à la période par défaut de 30 jours.

Configuration de la conformité

Différentes options sont disponibles lorsque le **Format** ci-dessus est réglé sur Conformité.

- **Période d'avertissement** : Nombre de jours avant l'expiration de la conformité pendant lesquels le **texte d'avertissement** sera affiché à l'utilisateur.
- **Texte d'avertissement** : Le message qui sera affiché sur l'écran du lecteur de carte pour avertir les utilisateurs que leur conformité est sur le point d'expirer. Les utilisateurs doivent accuser réception de l'avertissement avant de se voir accorder l'accès.

  En raison de la taille de l'écran du lecteur, les messages de conformité sont limités à 32 caractères.

- **Texte d'expiration** : Le message qui sera affiché sur l'écran du lecteur de carte pour informer les utilisateurs que leur conformité a expiré. Si le type de conformité est configuré pour une défaillance souple, l'utilisateur doit accuser réception de l'avis d'expiration avant que l'accès ne lui soit accordé.

  En raison de la taille de l'écran du lecteur, les messages de conformité sont limités à 32 caractères.

- **Défaillance grave** : Lorsque cette option est activée, l'utilisateur se verra refuser l'accès lorsque sa conformité aura expiré.

  Lorsque cette option est désactivée (défaillance passagère), si la conformité d'un utilisateur a expiré, le message d'expiration s'affiche mais l'accès est toujours accordé. L'utilisateur doit accuser réception de l'avis d'expiration avant que l'accès ne lui soit accordé.

  Il est également possible de configurer une panne temporaire pour les utilisateurs qui ne disposent pas du tout de la conformité, en utilisant l'option **Permettre la panne temporaire en cas de conformité manquante** dans **Programmation | Types de portes | Général**.

- **N'expire jamais** : Lorsque cette option est activée, le type de conformité sera traité comme s'il n'expirait jamais pour tout utilisateur, qu'une date d'expiration ait été définie ou non. La **date de début** et la **date de fin** de la programmation utilisateur seront ignorées.

Commandes

- Ce champ est utilisé pour envoyer des commandes de programmation à l'appareil. Il ne doit être utilisé que lorsqu'il est spécifiquement conseillé par la documentation ICT ou le support technique.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Codes de fonction

Cette fonctionnalité vous permet de définir une fonction – telle que l'armement d'une partition ou l'activation d'une sortie – qui peut être activée par les utilisateurs à partir d'un lecteur de carte avec un clavier NIP. Au niveau du lecteur, l'utilisateur peut saisir un chiffre spécifique (0-9) et appuyer sur la touche Entrée, suivi de la séquence d'informations d'identification de la porte, pour activer cette fonction.

Si vous utilisez des lecteurs ICT avec des LED RVB et un câblage RS-485, vous pouvez également programmer des couleurs de LED d'accusé de réception uniques pour indiquer si la fonction a réussi ou échoué.

Une fois que vous avez créé un code de fonction, vous devez l'assigner à des portes spécifiques afin qu'il puisse être activé à partir des lecteurs associés (**Programmation | Portes | Codes de fonction**).

Pour plus de renseignements et des exemples de programmation, consulter la Note d'application 240 : Codes de fonction dans Protege GX.

Codes de fonction | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

Configuration

- **Chiffre** : Le chiffre (0-9) utilisé pour activer ce code de fonction. L'utilisateur peut appuyer sur ce numéro, sur la touche d'entrée, puis sur la séquence d'informations d'identification de la porte pour activer le code de fonction.
- **Couleur de la LED de début de fonction** : La couleur que la LED du lecteur affichera pour indiquer que le code de fonction a été lancé. Ceci peut être utilisé pour inviter l'utilisateur à entrer ses informations d'identification.

  Les couleurs des LED ne sont disponibles que pour les lecteurs équipés de LED RVB.
- **Fin du succès de la fonction Couleur LED** : La couleur que la LED du lecteur affichera pour indiquer que le code de fonction a été effectué avec succès.

  Les couleurs des LED ne sont disponibles que pour les lecteurs équipés de LED RVB.
- **Fin de l'échec de la fonction Couleur LED** : La couleur que la LED du lecteur affichera pour indiquer que le code de fonction n'a pas abouti. Par exemple, cette couleur sera affichée si l'utilisateur ne parvient pas à saisir une séquence d'informations d'identification correcte.

  Les couleurs des LED ne sont disponibles que pour les lecteurs équipés de LED RVB.

Actions

Cliquez sur **Ajouter** pour ajouter des actions au code de fonction, avec les options suivantes :

- **Type d'appareil** : Sélectionnez la porte, la partition ou la sortie.
- **Nom** : Sélectionnez l'appareil requis.

- **Action** : Les actions disponibles correspondent à celles disponibles en tant que commandes manuelles lors d'un clic droit sur un registre de périphérique. Pour plus de renseignements sur des options spécifiques, consultez la section correspondante des Commandes manuelles de ce manuel.
- **Autoriser non autorisé** : Lorsque cette option est activée, aucun identifiant n'est requis pour activer le code de fonction. Par défaut, les informations d'identification définies dans le type de porte sont nécessaires pour activer le code de fonction.

  Si cette option est activée, le journalÉvénement n'indique pas quel utilisateur a activé le code de fonction.
- **Horaire** : Le code de fonction ne peut être utilisé que si l'horaire sélectionné est valide. Si l'horaire n'est pas valide, le lecteur indique que le code de fonction a échoué (en utilisant la couleur de la LED **Fin de fonction** et un long bip). Pour permettre l'activation du code de fonction à tout moment, réglez le programme sur Toujours.
- **Timeout** : La durée (en secondes) pendant laquelle le lecteur attendra que l'utilisateur saisisse ses informations d'identification après avoir appuyé sur la touche **[ENTER]**. Si aucune identification n'est saisie pendant cette période, le lecteur indique que le code de fonction a échoué (en utilisant la couleur de la LED **Fin de fonction** et un long bip).

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Emplois

Les tâches sont une fonctionnalité héritée qui ne nécessite pas de configuration dans Protege GX.

Importation utilisateur étape de travail

Importation utilisateur étape de travail sont une fonctionnalité héritée. Les alternatives suivantes sont disponibles :

- La fonction d'importation d'utilisateurs sous **Sites | Importer des utilisateurs** permet d'importer une seule fois des utilisateurs à partir d'un fichier CSV(consultez ci-dessous).
- L'option ICT Data Sync Service vous permet de configurer des importations récurrentes d'utilisateurs, ce qui peut permettre une intégration de bas niveau avec des systèmes de réservation et de RH tiers.

  Pour plus d'informations, voir le ICT Data Sync Service Guide d'intégration.

Importer utilisateurs

Il n'est pas rare d'avoir des centaines d'utilisateurs qui doivent être chargés dans le système. La saisie manuelle des données peut être fastidieuse et prendre du temps, et la saisie des données est souvent sujette à des erreurs humaines. Protege GX vous permet d'utiliser un fichier CSV standard pour importer des informations sur les utilisateurs à partir de systèmes existants, tels que des systèmes de RH ou d'inscription des étudiants. Les colonnes de la feuille de calcul peuvent être mises en correspondance avec les champs des tableaux utilisateur Protege GX, ce qui offre une grande flexibilité.

La fonctionnalité d'importation d'utilisateurs est utile pour les importations initiales uniques de registres d'utilisateurs. Pour les importations récurrentes, utilisez le ICT Data Sync Service.

Pour une démonstration, voir Importer utilisateurs via CSV dans Protege GX sur la chaîne YouTube ICT.

Importation d'utilisateurs depuis un CSV

1. Naviguez vers **Sites | Importer utilisateurs** pour lancer l'assistant d'importation d'utilisateurs.
2. Recherchez et sélectionnez le fichier CSV à partir duquel vous souhaitez importer des utilisateurs, puis cliquez sur **Suivant**.
3. Sélectionnez la ligne à partir de laquelle vous souhaitez commencer à importer des données et le DélimiteurTexte à utiliser, puis cliquez sur **Suivant**.

   Si votre fichier contient une ligne d'en-tête, assurez-vous de commencer l'importation à la ligne 2 afin que la ligne d'en-tête ne soit pas importée.
4. Sélectionnez chaque colonne dans le panneau de gauche et mettez-la en correspondance avec le champ associé à importer sur la droite. Les données du volet supérieur sont mises à jour au fur et à mesure que vous effectuez vos sélections.
5. Définissez vos préférences de **Formatage auto du nom d'affichage de l'utilisateur**. Cela détermine la façon dont le champ **Nom** sera rempli. Cliquez sur **Suivant** pour continuer.

   Les options Format court inversé (Smith, J) et Format long inversé (Smith, John) ne sont pas disponibles. Si elles sont nécessaires, modifier le fichier CSV de sorte que la colonne **Nom** ait le format correct.
6. Attribuez le numéro d'établissement, le premier numéro de carte et le niveau d'accès si vous ne l'avez pas déjà fait. Vous pouvez également choisir de générer automatiquement des NIP. Cliquez sur **Suivant** pour continuer.
7. Cliquez sur **Finir** pour lancer le processus d'importation. Les registres d'utilisateurs sont importés et l'assistant se ferme.

Ajout d'utilisateurs par lot

En ajoutant des utilisateurs par lots, vous pouvez créer automatiquement un certain nombre d'enregistrements d'utilisateurs par défaut avec un numéro d'installation attribué et une série de numéros de cartes. Ces nouveaux enregistrements seront vides, prêts pour la configuration en tant qu'utilisateurs spécifiques.

Ajout d'utilisateurs par lots

1. Naviguer sur **Site | Ajouter les utilisateurs en lots**.
2. Entrer les détails suivants qui s'appliqueront à tous les enregistrements d'utilisateurs ajoutés dans ce lot :
   - **Nom et prénom** : Vous pouvez saisir un nom ou un prénom provisoire afin de faciliter l'identification et la recherche des nouveaux enregistrements d'utilisateurs.
   - **Format automatique du nom d'affichage de l'utilisateur :** : Ce paramètre détermine la façon dont le champ **Nom** de l'enregistrement de l'utilisateur sera rempli pour l'affichage dans Protege GX (sur la base du prénom et du nom de famille). Le nom d'affichage peut être modifié ultérieurement pour chaque enregistrement.
   - **Numéro d'établissement** : Le numéro de l'établissement/site qui sera attribué pour la première identification de tous les utilisateurs ajoutés.
   - **Début/fin du numéro de carte** : Chaque utilisateur ajouté se verra attribuer un numéro de carte, à partir de la valeur de départ et de l'incrémentation jusqu'à ce que la valeur finale soit atteinte. Ces valeurs déterminent également le nombre d'enregistrements d'utilisateurs qui seront créés.
   - **Niveau d'accès** : Le niveau d'accès qui sera attribué à tous les utilisateurs dans ce lot.
3. Cliquez sur **OK**. Les enregistrements des utilisateurs sont maintenant ajoutés et prêts à être configurés individuellement (**Utilisateurs | Utilisateurs**).
4. La fenêtre surgissante **Ajouter résultats de l'utilisateur** confirme le nombre d'enregistrements utilisateur créés.

Menu Utilisateurs

Le menu usager contient les fonctions permettant de travailler avec les utilisateurs, de les configurer et de définir l'accès dont ils disposent dans un site.

Pour les démonstrations, voir ICT Conseil rapide : Ajouter un utilisateur dans Protege GX et Créer et gérer des utilisateurs dans Protege GX sur la chaîne YouTube ICT.

Tri et filtrage des registres de l'utilisateur

Divers outils sont disponibles sur la page de l'utilisateur pour trier et filtrer la liste des utilisateurs afin de trouver les registres nécessaires :

- **Pagination** : La liste des utilisateurs est paginée et affiche 200 registres par page par défaut. Vous pouvez passer à d'autres pages et changer le **Nombre de registres à afficher par page** à l'aide des paramètres situés en bas de la liste.

  Le réglage du **Nombre de registres à afficher par page** sur Tous peut entraîner des retards lors du chargement d'un très large nombre d'utilisateurs. Les tailles de page plus petites se chargent plus rapidement.

- **Tri** : Vous pouvez trier la liste des utilisateurs en cliquant sur les en-têtes de colonne (par exemple, cliquez une fois sur l'en-tête **Nom** pour trier alphabétiquement, et une Seconde fois pour un tri inverse). Vous pouvez également activer les colonnes **Premier nom** et **Nom de famille** en utilisant l'option **Afficher les colonnes du premier nom et du nom de famille dans utilisateurs** dans **Global | Sites | Afficher**.
- **Filtrage** : Il existe deux méthodes de filtrage de la liste de l'utilisateur :
  - La barre de recherche en haut de la liste vous permet de filtrer rapidement les utilisateurs par le champ **Nom**.
  - L'outil **Trouver** dans la barre d'outils permet de filtrer les utilisateurs en fonction de n'importe quel réglage. Pour plus d'informations, consultez la section Utiliser l'outil de recherche (la page 20).

Utilisateurs

Un utilisateur est une personne programmée dans le système avec des identifiants de contrôle d'accès, d'alarme, biométriques ou photographiques. L'utilisateur peut se voir attribuer l'accès à des portes et des fonctions programmées du système.

Vous pouvez visualiser les enregistrements d'utilisateurs en **mode Énumérer la Vue** ou dans **une vue arborescente** (organisée par groupe d'enregistrements) en cliquant sur les icônes de la barre d'outils. Énumérer la Vue est la valeur par défaut, mais vous pouvez la remplacer par une vue en arbre en activant l'option **Afficher les utilisateurs dans les groupes** (**Global | Sites | Affichage**).

Utilisateurs | Général

Général

- **Prénom** : Le prénom de l'utilisateur.
- **Nom de famille** : Le nom de famille de l'utilisateur.
- **Nom** : Le nom d'affichage de l'utilisateur tel qu'il apparaît sur les claviers et dans le logiciel. Ce champ se remplit automatiquement en fonction des paramètres définis dans la section **formatage auto du nom d'affichage de l'utilisateur** (**Global | Paramètres globaux | General**).
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

Les groupes d'enregistrements déterminent également comment les utilisateurs seront regroupés dans la **vue arborescente**(activée à partir de la barre d'outils).

- **Langue par défaut** : Définit la langue qui sera utilisée lorsque l'utilisateur se connectera à un clavier. Il peut s'agir de n'importe quelle langue prise en charge et n'est pas limité par l'installation Protege GX.
- **Courriel** : L'adresse courriel de l'utilisateur.

  Ceci est utilisé par la fonction de synchronisation du portail de location (regardez **Général | Sites | Portail**). L'adresse courriel sera utilisée pour synchroniser l'utilisateur et créer un compte d'application mobile, permettant aux visiteurs d'appeler l'utilisateur par vidéo depuis la station d'entrée. Si l'utilisateur possède déjà un compte d'application mobile, entrez l'adresse courriel associée à ce compte.

  Pour plus d'informations, consultez le Protege guide de l'utilisateur du portail de location.

NIP

- **NIP** : Le NIP d'un utilisateur est utilisé pour se connecter aux claviers et accéder aux portes (via des lecteurs de cartes avec des claviers NIP). Cliquez sur les boutons**[4] [5] [6]** pour générer automatiquement un nouveau NIP aléatoire de la longueur sélectionnée.

  La longueur maximale du NIP acceptée par les claviers et les lecteurs est de 8 chiffres. Tout chiffre supplémentaire est ignoré.

  Les NIP des utilisateurs existants ne sont visibles que pour les **opérateurs dont l'option Afficher les NIP des utilisateurs** est activée (**Global | Opérateurs**).

- **Réinitialiser le NIP** : Cliquez sur ce bouton pour générer un nouveau NIP aléatoire avec le nombre de chiffres spécifié dans le **champ Longueur du NIP par défaut** (**Global | Sites | Valeurs par défaut du site**).
- **NIP de l'armoire à clés** : Ce champ est visible lorsque l'utilisateur a accès aux clés ou aux groupes de clés via son niveau d'accès. Le NIP de l'armoire à clés est basé sur le NIP habituel de l'utilisateur, mais tronqué en fonction des exigences du système tiers.

  Pour plus de renseignements, reportez-vous à la Note d'application 220 : Intégration Touch de KeyWatcher dans Protege GX ou Note d'application 331 : Intégration de KeySecure avec Protege GX.

- **Heure d'expiration du code NIP** : Définit la durée avant l'expiration du NIP actuel. La première fois que l'utilisateur se connecte à un clavier après l'expiration de son NIP, il lui est demandé de changer son NIP. L'utilisateur ne pourra pas utiliser un NIP expiré pour accéder à la porte.

  Ce qui précède décrit le fonctionnement par défaut. Voir la section **Amélioration de la sécurité du site** dans **Global | Sites | Défauts du site** pour d'autres options de configuration.

Numéros de cartes

- **Carte du programme** : Ce bouton permet de programmer des cartes d'utilisateurs à utiliser avec l'intégration du Salto SHIP, en utilisant un encodeur de bureau USB(PRX-ENC-DT). Assurez-vous que tous les paramètres utilisateur requis sont définis dans l'onglet **Salto** avant d'encoder la carte.
- **Numéro de l'établissement/de la carte** : Chaque utilisateur peut avoir jusqu'à 8 justificatifs d'identité standard (cartes, étiquettes, données biométriques) qui peuvent être utilisés à n'importe quelle porte avec des lecteurs compatibles. Chaque justificatif se compose d'un numéro d'établissement (premier champ, également appelé code de site) et d'un numéro de carte (deuxième champ), qui ont chacun une limite de 10 chiffres.

  De nouvelles informations d'identification peuvent être attribuées aux utilisateurs en saisissant ici les numéros d'établissement et de carte. Par ailleurs, lorsque vous badgez une carte non assignée sur un lecteur, vous pouvez cliquer avec le bouton droit de la souris sur l'événement Lire les données brutes et sélectionner **Ajouter un nouvel utilisateur** ou **Ajouter une carte à un utilisateur existant** pour saisir automatiquement les informations d'identification.

Les données biométriques doivent être saisies dans la deuxième ligne (intitulée **Numéro de l'établissement/carte ou données biométriques**). Si des données existent déjà dans cette rangée au moment de l'enregistrement d'une pièce d'identité biométrique, les données existantes seront déplacées vers le bas de la liste.

Note : La base de données Protege GX ne peut pas stocker les numéros d'installation ou de carte d'utilisateur de 2147483648 ou plus. Les événements faisant référence à ces cartes n'afficheront aucune donnée. Il s'agit d'une limitation connue.

- **Lire carte** : Cette fonction est utilisée avec un encodeur de bureau compatible (tel que PRX-ENC-DT). Placez une carte sur l'encodeur et cliquez sur ce bouton pour remplir automatiquement les champs relatifs au **numéro de l'établissement et de** la carte.

L'encodeur doit être capable de lire le type de carte utilisé. L'ICT encodeur USB de bureau ne prend en charge que les ICT cartes Mifare et DESFire sécurisées.

- **Carte désactivée** : Ce paramètre permet de désactiver un identifiant sans en supprimer les détails. L' identifiant peut être réactivé en décochant la case. Si un utilisateur possède plusieurs identifiants, le paramètre peut être activé ou désactivé, le cas échéant, pour chaque identifiant.
- **Dernière utilisation / modification de la carte** : Indique la date et l'heure auxquelles la carte a été autorisée pour la dernière fois à accéder à une porte ou modifiée par un opérateur dans le système (lecture seule).

L'heure de la dernière utilisation n'est mise à jour que lorsque la carte est utilisée pour accéder à une porte (c'est-à-dire lorsque **le mode du lecteur** 1/2 est réglé sur Accès). Il n'est pas mis à jour sur les lecteurs en mode ascenseur ou partition. Il s'agit d'une limitation connue.

- **Période d'inactivité** : Lorsque cette option est activée, vous pouvez définir une période d'inactivité en jours, heures ou minutes. Si la carte n'est pas utilisée pendant cette période, elle sera automatiquement désactivée.

Date/Heure d'expiration de l'utilisateur

- **Commencer** : Lorsque cette option est activée, l'utilisateur ne pourra pas obtenir l'accès avant l'heure et la date spécifiées. Par exemple, cela peut être utilisé pour activer automatiquement un employé qui doit commencer à travailler à une date spécifique.
- **Fin** : Lorsque cette option est activée, l'enregistrement de l'utilisateur expirera après l'heure et la date spécifiées et l'utilisateur ne pourra plus y accéder. Par exemple, cela pourrait être utilisé pour retirer automatiquement l'accès à un entrepreneur qui doit terminer le travail à une certaine date.

Désactivation / suppression de l'utilisateur

- **Dernier utilisateur actif** : Indique la date et l'heure de la dernière autorisation d'accès de l'utilisateur à une porte ou à un clavier du système (en lecture seule).

Ce champ n'est pas mis à jour lorsque l'utilisateur accède à un enregistrement de porte qui représente un COP ou un DOP dans une intégration d'ascenseur HLI.

- **Désactiver la période** : Lorsque cette option est activée, vous pouvez définir une période d'inactivité en jours, heures ou minutes. S'il n'y a aucune activité de l'utilisateur pendant cette période (c'est-à-dire qu'il n'accède à aucune porte ou clavier), l'enregistrement de l'utilisateur sera désactivé (à l'aide de l'option **Désactiver l'utilisateur** dans l'onglet **Options**).
- **Supprimer la période** : Lorsque cette option est activée, vous pouvez définir une période d'inactivité en jours, heures ou minutes. S'il n'y a aucune activité de l'utilisateur pendant cette période (c'est-à-dire s'il n'accède à aucune porte ou clavier), l'enregistrement de l'utilisateur sera supprimé de la base de données.

Partitions

- **Partition de l'utilisateur** : Ce champ vous permet de définir une partition à laquelle l'utilisateur est associé. Cette fonctionnalité a plusieurs applications :

- Si l'option **Désactiver la partition lors de la connexion si l'utilisateur a accès** est activée (**onglet** Options), chaque fois que l'utilisateur se connecte à un clavier, cette partition est automatiquement désarmée.
- L'option **Désactiver la partition des utilisateurs sur carte** valide (**Modules d'expansions| Modules d'expansion | Lecteur 1/2**) permet à l'utilisateur de désarmer automatiquement sa partition lorsqu'il badge sur le lecteur correspondant. L'option **Armer la partition des utilisateurs** (même emplacement) permet à l'utilisateur d'armer automatiquement sa partition lorsqu'il badge deux fois au lecteur.

La même fonctionnalité est disponible pour plusieurs partitions dans l'onglet **Groupes de partitions**. La partition de l'utilisateur doit être incluse dans les groupes **Utilisateurs | Niveaux d'accès | Désarmement de la partition**.

Configuration

- **Signaler ID** : Le code qui sera utilisé pour identifier cet utilisateur dans les rapports destinés aux stations de surveillance. Les services de déclaration Contact ID, SIA et Rapport IP utilisent ce code.

  Le système générera automatiquement un numéro unique pour chaque nouvel utilisateur. Il n'est pas nécessaire de modifier ces chiffres, sauf en cas d'exigences spécifiques en matière de rapports.

KeyWatcher

- **Identifiant KeyWatcher** : Lorsqu'un utilisateur se voit accorder l'accès à des clés ou à des groupes de clés, un ID utilisateur unique est attribué pour être utilisé avec le système d'armoire à clés. Il peut être modifié si nécessaire.

Pour plus de renseignements, reportez-vous à la Note d'application 220 : Intégration Touch de KeyWatcher dans Protege GX ou Note d'application 331 : Intégration de KeySecure avec Protege GX.

Clé Cencon

Ces options sont uniquement disponibles lorsque l'intégration de Cencon est activée dans **Global | Sites | Cencon**. Pour plus d'informations, voir la note d'application 160 : Configuration de l'intégration de Cencon dans Protege GX.

- **ID de clé Cencon** : Lorsqu'une clé Cencon a été initialisée, ce champ affiche automatiquement l'ID de la clé.
- **Touche d'initialisation** : Si l'intégration Cencon a été configurée, ce bouton est utilisé pour attribuer une clé Cencon à un utilisateur. Lorsque vous cliquez sur ce bouton, vous êtes invité à placer une clé dans la boîte à clé connectée. Si l'initialisation est réussie, l'utilisateur sera ajouté à la base de données Cencon et le **champ ID de la clé Cencon** ci-dessus sera rempli automatiquement.

  Après l'attribution d'une clé, le même bouton vous permettra de désactiver la clé de l'utilisateur.

Informations d'identification

Cette section vous permet d'attribuer des informations d'identification personnalisées aux utilisateurs. Lorsqu'un type d'informations d'identification a été créé dans **Sites | type d'informations d'identification**, il sera automatiquement ajouté ici ou vous pouvez également utiliser les boutons **Ajouter** et **Supprimer** pour gérer les accréditations disponibles de l'utilisateur.

- **Types d'informations d'identification** : Le type de justificatif personnalisé auquel le justificatif est associé (par exemple, plaque d'immatriculation, format de carte personnalisé, type de conformité, etc.)
- **Carte désactivée** : Cochez cette case pour désactiver l'identifiant sans le supprimer.
- **Types d'informations d'identification** : Les données d'identification spécifiques de l'utilisateur (par exemple, sa plaque d'immatriculation).
- **Commencer** : Uniquement applicable aux types de conformité. Lorsque cette option est activée, l'utilisateur ne pourra pas obtenir l'accès en utilisant cette conformité avant la date spécifiée.
- **Fin** : Uniquement applicable aux types de conformité. Lorsque cette option est activée, la conformité expirera après l'heure et la date spécifiées et l'utilisateur ne pourra pas l'utiliser pour obtenir un accès.

- **Période d'inactivité** : Lorsque cette option est activée, vous pouvez définir une période d'inactivité en jours, heures ou minutes. Si l'Identifiant n'est pas utilisée pendant cette période, elle sera automatiquement désactivée.

  La période d'inactivité maximale est de 365 jours. Si vous saisissez une période plus longue, le champ sera réinitialisé à la période par défaut de 30 jours.

Pour les sites dont la**R fonction Exiger une double identification pour l'accès** au clavier est activée dans **Global | Sites | Paramètres par défaut du site** , chaque utilisateur aura un type d'identification par défaut et devra indiquer un ID utilisateur valide dans le champ **Identification**.

VingCard VisiOnline

Il s'agit d'une fonction sous licence séparée Pour plus d'informations, voir la note d'application 215 : Protege GX Intégration de VingCard VisiOnline.

- **Carte du personnel du programme** : Appuyez sur ce bouton pour encoder une carte pour cet utilisateur en utilisant l'encodeur VingCard spécifié dans la programmation du contrôleur (**Sites | Contrôleurs | Configuration**).

Utilisateurs | Niveaux d'accès

Cet onglet contrôle les niveaux d'accès attribués à chaque utilisateur. Chaque fois que l'utilisateur effectue une action (comme demander l'accès à une porte ou se connecter à un clavier), le système vérifie le ou les niveaux d'accès qui lui ont été attribués pour déterminer s'il dispose des autorisations nécessaires.

Cliquez sur **Ajouter** pour sélectionner et attribuer un niveau d'accès, ou sur **Supprimer** pour supprimer un niveau d'accès. La **fenêtre de visualisation graphique** affiche des chronologies pour indiquer quand l'utilisateur a accès à chaque porte du système, en fonction des horaires définis dans la programmation de l'utilisateur, du niveau d'accès et du groupe de portes.

Le contrôleur vérifie tous les niveaux d'accès appliqués à un utilisateur. En général, si l'accès est accordé par un niveau d'accès et refusé par un autre, l'accès sera accordé.

- **Nom** : Nom du niveau d'accès attribué à l'utilisateur.
- **Niveau d'accès expire** : Lorsque cette option est activée, le niveau d'accès expire en fonction des dates de début et de fin définies. L'utilisateur ne pourra utiliser ce niveau d'accès qu'entre les dates de début et de fin d'expiration.

  Plusieurs copies du même niveau d'accès peuvent être attribuées à un seul utilisateur avec des heures d'expiration différentes, ce qui permet un accès périodique. Par exemple, un technicien peut ne pouvoir accéder au bâtiment que quelques jours par mois.
- **Début d'expiration**: Ce niveau d'accès ne sera pas valable pour l'utilisateur avant cette date et cette heure.
- **Fin d'expiration** : Ce niveau d'accès ne sera pas valable pour l'utilisateur après cette date et cette heure.
- **Horaire** : Ce calendrier détermine quand les permissions fournies par le niveau d'accès sont valides pour cet utilisateur. Il est combiné à tous les horaires définis dans le niveau d'accès lui-même, ainsi que dans les groupes de portes ou d'étages.

  L'utilisateur n'a accès que si tous les horaires pertinents sont valides.

Utilisateurs | Options

Options générales

- **Désactiver l'utilisateur** : Lorsque cette option est sélectionnée, l'enregistrement de l'utilisateur est désactivé, ce qui l'empêche d'utiliser toutes les autorisations d'accès. L'enregistrement n'est pas supprimé et peut être réactivé à tout moment.

Lorsqu'un utilisateur est désactivé, une commande est envoyée aux contrôleurs concernés pour mettre à jour leurs bases de données internes. Cela signifie que les enregistrements des utilisateurs sont désactivés immédiatement sans attendre le téléchargement d'un contrôleur.

- **Montrer un message d'accueil à l'utilisateur** : Lorsque cette option est activée, l'utilisateur reçoit un message d'accueil (par ex. Bonjour John Smith') sur le clavier lorsqu'il se connecte. La désactivation de cette option indique au clavier de passer directement au menu lorsque l'utilisateur se connecte.

Cette option est équivalente à l'option **Montrer le message d'accueil de l'utilisateur** dans **Groupes | Groupes de menus | Options**. Le message d'accueil sera affiché si l'option l'une ou l'autre est activée.

- **Aller directement au menu dès connexion (aucun contrôle de partition)** : Par défaut, lorsqu'un utilisateur se connecte à un clavier, il voit apparaître le menu de contrôle de partition, qui lui permet d'armer et de désarmer les zones disponibles. Lorsque cette option est activée, l'utilisateur accède directement au menu principal du clavier à la place. Les utilisateurs peuvent toujours accéder au contrôle de partition à partir du menu principal.

- **L'utilisateur peut reconnaître la mémoire d'alarme** : Lorsque cette option est activée, l'utilisateur peut reconnaître la mémoire d'alarme pour les zones disponibles sur le clavier. La mémoire d'alarme peut être visualisée en appuyant sur **[Menu] [5] [1]**, et elle enregistre les quatre dernières activations d'alarme dans chaque partition.

Cette option est équivalente à l'option **L'utilisateur peut reconnaître la mémoire d'alarme** dans **Groupes | Groupe de menus | Options**. Les alarmes peuvent être reconnues si l'une ou l'autre des options est activée.

- **Montrer la mémoire d'alarme à l'ouverture de session** : Avec cette option activée, s'il y a eu des alarmes dans la zone primaire du clavier, le clavier affiche la mémoire d'alarme à l'utilisateur dès qu'il se connecte. Si cette option est désactivée, l'utilisateur doit naviguer dans le menu Visualisation pour reconnaître les alarmes.

Cette option est équivalente à l'option **Montrer la mémoire d'alarme de l'utilisateur à la connexion** dans **Groupes | Groupes de menus | Options**. Les alarmes peuvent être reconnues si l'une ou l'autre des options est activée. La zone principale du clavier est définie dans la **Partition à laquelle appartient cet écran LCD** (**Modules d'expansions | Claviers | Configuration**).

- **Désactiver la zone primaire si l'utilisateur a accès à la connexion** : Avec cette option activée, chaque fois que l'utilisateur se connecte au clavier, la zone primaire du clavier est désarmée. Cela ne fonctionne que si l'utilisateur a accès au désarmement de ce secteur, c'est-à-dire si le secteur est inclus dans l'onglet **Désarmement des groupes de secteurs** du niveau d'accès.

La zone primaire du clavier est définie dans le **Partition à laquelle appartient cet écran LCD** (**Modules d'expansions | Claviers | Configuration**).

- **Éteindre la partition de l'utilisateur dès connexion si l'utilisateur a accès** : Si cette option est activée, chaque fois que l'utilisateur se connecte au clavier, la **Partition de l'utilisateur** (définie dans l'onglet **General**)) sera désarmée.
- **Reconnaître troubles de systèmes** : Lorsque cette option est activée, l'utilisateur peut reconnaître certains problèmes de système à l'aide du clavier. Les problèmes de système peuvent être vus en appuyant**[Menu] [5] [2]** sur le clavier, et reconnus en appuyant sur **[Enter]**.
- **Traiter le code PIN utilisateur plus 1 comme une contrainte** : Lorsque cette option est activée, le code PIN + 1 de l'utilisateur est traité comme un code sous contrainte. Lorsque ce code spécial est saisi sur un clavier ou un lecteur, l'accès est accordé (ou refusé) comme d'habitude, mais un Code PIN utilisateur sous contrainte (pour les claviers) ou Duress de porte. (pour les claviers NIP de lecteur) sera ouverte. L'entrée de défectuosité est fermée lorsque le code PIN normal de l'utilisateur est saisi.

  Pour calculer le code sous contrainte, 1 est ajouté au dernier chiffre du code PIN de l'utilisateur. Par exemple, si le code PIN normal est 1234, le code sous contrainte sera 1235. Si le dernier chiffre est 9, alors 0 comme dernier chiffre génère un code sous contrainte. Le code PIN de l'utilisateur doit être supérieur à 3 chiffres pour que cette fonction fonctionne correctement.

Si vous utilisez un contrôleur PCB avec la version 4.0 ou supérieure du logiciel, l'activation de cette option pour un utilisateur l'active globalement pour tous les utilisateurs.

Options avancées

- **L'utilisateur dispose de super droits et peut passer outre l'antipassback** : Lorsque cette option est activée, l'utilisateur est considéré comme un super utilisateur par le système. Ceci accorde les permissions suivantes :
  - Annulez les exigences du double code pour les portes et les partitions.
  - Ignorer les règles antipassback
  - Déverrouiller les portes qui ont été verrouillées
- **L'utilisateur fait fonctionner la fonction d'accès étendu aux portes** : Si cette option est activée, chaque fois que cet utilisateur se voit accorder l'accès à une **porte, la serrure s'ouvrira pendant le temps d'accès prolongé de la porte** (défini **dans Programmation | Portes | Options avancées**) au lieu du temps d'activation **standard de la serrure**.

  Cette mesure devrait être utilisée pour accorder aux personnes à mobilité réduite un délai supplémentaire pour accéder aux portes.
- **Décompte d'expiration de flânage d'Utilisateur activé** : Lorsque cette option est activée, l'utilisateur sera inclus dans le traitement des partitions. Cette fonction peut être utilisée pour empêcher les utilisateurs de rester trop longtemps dans les partitions de transition, comme les couloirs et les parkings. Lorsque cette option est désactivée, cet utilisateur n'est pas affecté par la programmation des partitions.

  La programmation des partitions de flânage doit être configurée correctement dans la ou les partitions concernées. Pour plus d'informations, voir **l'option partition activée en mode** de flânage **dans la page Programmation | Zones | Options (1)**.
- **Utilisateur peut modifier les paramètres utilisateur à partir du clavier :** Il s'agit d'une option héritée qui n'a aucun effet.
- **L'utilisateur est un utilisateur sous contrainte** : Si cette option est activée, lorsque le code PIN de cet utilisateur est saisi sur un clavier ou un lecteur, il sera traité comme un code sous contrainte. L'accès sera accordé (ou refusé) comme d'habitude, en fonction du niveau d'accès de l'utilisateur sous contrainte, mais un User Duress (pour les claviers) ou Durée de la porte (pour les portes) sera ouverte. L'entrée de défectuosité sera fermée lorsqu'un NIP d'utilisateur normal sera saisi.

  Cette option doit être utilisée lorsque le site exige des codes sous contrainte communs à plusieurs utilisateurs.

  Cette option ne doit pas être appliquée aux utilisateurs normaux. Utilisez l'option **Traiter le code PIN de l'utilisateur plus 1 comme un code sous contrainte** pour donner à chaque utilisateur un code sous contrainte unique.
- **Réarmer la partition en mode séjour** : L'activation de cette option permet à l'utilisateur de définir des zones à réarmer automatiquement en mode séjour. Lorsque l'utilisateur désarme une zone avec l'option **Réarmement par l'utilisateur en mode permanent** activée (**Programmation | Zones | Options 2**), la zone reste désarmée pendant une période déterminée (la **Durée de réarmement de la zone** dans **Programmation | Zones | Configuration**), puis s'arme automatiquement.

  Cette option est utile pour les personnes qui travaillent en dehors des heures normales, leur permettant de désarmer l'intérieur du bâtiment et de sécuriser le périmètre.

Options de garde double

- **Master de garde double** : Lorsque l'option de **double authentification** est activée pour un type de porte (**Programmation | Types de porte | Options**), deux utilisateurs doivent entrer des informations d'identification valides pour que la porte se déverrouille. Par défaut, un **master de garde double** doit d'abord entrer ses informations d'identification pour lancer la double authentification, suivi par un fournisseur de double garde ou un autre maître.
- **Fournisseur de garde double** : Lorsque l'option de **double authentification** est activée pour un type de porte (**Programmation | Types de porte | Options**), deux utilisateurs doivent entrer des informations d'identification valides pour que la porte se déverrouille. Par défaut, un **fournisseur de double garde** ne peut pas initier la double authentification, mais il peut compléter le processus une fois qu'un master de double garde l'a initié.

  Lorsque l'option **Le fournisseur de la double carte peut initier l'accès** est activée dans la programmation des types de porte, un master ou un fournisseur de la double garde peut initier la double authentification.

Options d'ascenseur OTIS HLI

Ces options ne sont disponibles uniquement lorsque l'intégration Otis HLI est activée. Pour plus de renseignements, voir la Note d'application 174 : intégration HLI Otis Compass Protege GX.

- **L'utilisateur est un VIP** : Les utilisateurs VIP bénéficient d'un service prioritaire ininterrompu vers leur étage de destination dans des cabines d'ascenseur dédiées. Ceci doit être configuré dans le système Otis.
- **Activer Vertigo** : Lorsque Vertigo est activé, le système Otis sélectionne des cabines d'ascenseur spécifiques pour cet utilisateur en fonction d'une caractéristique particulière (telle que configurée dans Otis). Par exemple, les passagers souffrant de vertiges ne seront pas affectés à des cabines d'ascenseur en verre.
- **Activer le fonctionnement du groupe divisé** : Active le contrat spécial 1, tel que configuré dans le système Otis.
- **Activer Vertigo 2** : Suite à l'option **Activer Vertigo** ci-dessus, cette option définit en outre le type d'ascenseur qui sera attribué à l'utilisateur, tel que configuré dans le système Otis. Par exemple, les ascenseurs peuvent être ralentis pour ce passager.
- **Activer le service de chariot** : Cette caractéristique minimise les cas où une cabine d'ascenseur arrive sans la capacité physique requise pour un passager et un chariot (par exemple, dans les ascenseurs de service des hôtels/hôpitaux).
- **Activer la fonction d'écrasement CIM** : Lorsque le fonctionnement de la CIM est activé dans le système Otis, le système empêche des groupes d'utilisateurs spécifiques de partager des cabines d'ascenseur ou de se rendre aux mêmes étages. Activez cette option pour les utilisateurs qui doivent accéder à toutes les cabines d'ascenseur et à tous les étages, comme les gestionnaires de bâtiments.

Options d'ascenseur KONE HLI

Ces options ne sont disponibles uniquement lorsque l'intégration KONE HLI est activée. Par défaut, tous les appels sont de type normal. Utilisez les options ci-dessous pour spécifier un autre type d'appel.

Pour plus d'informations, voir la note d'application 274 : Protege GX Intégration de KONE Destination 880 et la documentation opérateur fournie par KONE.

- **Activer l'appel normal**
- **Activer l'appel de handicap**
- **Activer l'appel prioritaire**
- **Activer l'appel de la voiture vide**
- **Activer l'appel d'allocation d'espace**

Utilisateurs | Photo

La photo d'identification est une fonction sous licence séparée. Pour plus d'informations, voir la note d'application 149 : Création d'un modèle de carte d'identité avec photo dedans Protege GX.

Il n'est pas possible d'afficher les photos des utilisateurs lors de la sélection multiple d'utilisateurs. Si plusieurs enregistrements d'utilisateurs sont sélectionnés, la vue des photos ne sera pas disponible, et cela persistera même après la suppression de la sélection multiple. Vous devrez naviguer hors du menu Utilisateurs | Utilisateurs pour actualiser la vue des photos.

Photo

- **Ajouter la photo...** Cliquez sur ce bouton pour ajouter une photo pour l'utilisateur.
  - Si l'image est déjà stockée sur le réseau, sélectionnez l'ellipse **[...]** à côté de **Path** pour naviguer vers l'image. L'image doit être accessible depuis la machine serveur.
  - Si l'image n'existe pas encore, définissez le champ **Source de l'image** pour capturer une nouvelle image. Vous pouvez capturer une image à partir d'une webcam connectée ou d'un bloc de signature Topaz.
  - Lorsque vous avez terminé, cliquez sur **Suivant**.
- **Supprimer la photo** : Supprimez la photo de l'utilisateur de la base de données.

- **Paramètres photo** : Par défaut, la taille de la photo correspond au paramètre défini dans **Global | Sites | Affichage**. Les paramètres ici vous permettent de remplacer ce paramètre pour les utilisateurs individuels.
- **Imprimer Carte** : Imprime la photo d'identification avec photo en fonction du **modèle de carte**sélectionné ci-dessous. Il existe plusieurs options pour l'impression de cartes. Passez la souris sur la flèche pour voir les options disponibles :
  - **Imprimer Carte** : Imprimer la carte sans lire ou écrire l'identifiant (numéro de carte à puce, bande magnétique ou ICT secteur). Vous serez invité à sélectionner l'imprimante à utiliser.
  - **Imprimer & Lire** : Imprimez la carte et lisez le numéro de la carte dans le champ des informations d'identification de l'utilisateur.
  - **Imprimer & Traiter le modèle** : Imprimer la carte et lire ou écrire la bandemag ou le secteur ICT. L'action entreprise dépend des paramètres définis dans **Utilisateurs | Éditeur de modèle de carte | Encodage de carte** .
  - **Traiter modèle seulement** : Lire ou écrire la bandemag ou ICT le secteur sans imprimer la carte. L'action entreprise dépend des paramètres définis dans **Utilisateurs | Éditeur de modèle de carte | Encodage de carte** .

  Il est possible d'imprimer des cartes par lots pour un certain nombre d'utilisateurs à la fois. Exécutez un rapport de l'utilisateur avec les utilisateurs souhaités, puis cliquez sur **Impression par lot** pour imprimer les cartes de tous les utilisateurs actuellement visibles dans le rapport.
- **Prévisualisation** : Affiche un aperçu de la carte d'utilisateur basé sur le **modèle de carte** sélectionné ci-dessous.

Photo d'identification

- **Modèle de carte :** Définit le modèle IDPhoto à utiliser. Créez un modèle IDPhoto dans **Utilisateurs | Éditeur de modèles de cartes**.
- **Étirer l'image pour la remplir** : Cela oblige l'image à s'étirer à la taille définie dans les **paramètres photo** ci-dessus. Lorsque cette option est activée, le rapport d'aspect de l'image n'est pas maintenu et une certaine déformation peut se produire.

Utilisateurs | Prolongé

Cet onglet n'est visible que lorsque l'option **Afficher les champs personnalisés prédéfinis dans les utilisateurs** est activée dans **Global | Sites | Affichage** , et vous permet de saisir des informations supplémentaires sur les utilisateurs. Un certain nombre de champs prédéfinis sont disponibles.

Pour les champs utilisateur personnalisés, utilisez **les onglets Champs personnalisés** et **Champs personnalisés** (**menu**Utilisateurs).

Les champs élargis disponibles sont les suivants :

- Numéro de badge
- Type de badge
- Nom du service
- Numéro du service
- Fonction d'employé
- Numéro de licence
- Union
- Site
- Date de production de badge
- Date d'expiration de badge
- Champs personnalisés 1-6
- Champ de note personnalisée 1 1-2
- Numéro de Carte

- Type de carte
- Numéro de salaire

Si l'option **Enregistrer le numéro et la date du badge après l'impression de la carte** est activée (**Global | Sites | Valeurs par défaut du site**), les champs **Numéro de badge**, **Type de badge** et **Date de production du badge** seront automatiquement remplis après l'impression d'une carte d'utilisateur. Les autres champs peuvent être mis à jour en fonction des paramètres définis dans **Utilisateurs | Éditeur de modèles de cartes | Actions d'impression de cartes** .

En outre, les champs de cet onglet peuvent être inclus sur une carte d'utilisateur sous forme de code-barres. Cela vous permet de vous interfacer avec des systèmes qui utilisent des scanners de codes-barres pour identifier les utilisateurs. Pour plus d'informations, consultez la section Menus de l'éditeur de modèle de carte (la page 136).

Utilisateurs | Présence

Cet onglet vous permet de visualiser facilement les derniers événements d'entrée et de sortie (présence) d'un utilisateur.

- **Chargement des événements** : Charge les événements d'entrée et de sortie de porte les plus récents pour l'utilisateur.
- **Ajouter événements dedans/dehors** : Permet d'ajouter un nouvel événement de temps et de présence pour l'utilisateur (entrée/sortie d'une porte spécifique).

  Lors de l'ajout d'événements de temps et de présence, toutes les heures seront arrondies à l'heure la plus proche.

- **Copier au presse-papier** : Copie le ou les événements sélectionnés dans le presse-papiers sous forme de données CSV.

Utilisateurs | Groupes de partitions

l'onglet Groupes de partitions a une fonctionnalité similaire à celle de la **partition Utilisateur** (onglet **Général**), vous permettant de spécifier un ou plusieurs groupes de partitions auxquels l'utilisateur est associé. Par exemple, cela peut être utilisé pour permettre à un utilisateur de désarmer rapidement une section spécifique du bâtiment. Cette fonctionnalité a plusieurs applications :

- Si **l'option Éteindre la partition de l'utilisateur dès connexion si l'utilisateur a accès** est activée (**onglet** Options), chaque fois que l'utilisateur se connecte à un clavier, chaque partition du groupe de partition est automatiquement désarmée.
- L'option **Désarmer la zone des utilisateurs sur carte** valide (**module d'expansion| module d'expansion du lecteur| Lecteur 1/2**) permet à l'utilisateur de désarmer automatiquement toutes les partitions du groupe de zones lorsqu'il badge sur le lecteur correspondant. L'option **Armer Partition des utilisateurs** (même emplacement) permet à l'utilisateur d'armer automatiquement toutes les partitions du groupe de partitions lorsqu'il badge deux fois au lecteur.

Les groupes de partitions attribuées ici doivent être incluses dans l'onglet **Utilisateurs | Niveaux d'accès |Désarmement groupes de partitions**.

Utilisateurs | Biométriques

Cet onglet n'est affiché que lorsque l'intégration biométrique de Suprema ou de Princeton Biometrics est activée dans **Global | Sites | Biométriques**. Pour plus de renseignements, reportez-vous à la note d'application 264 : Intégration Suprema Biometric dans Protege GX ou note d'application 297 : Intégration dans Princeton Identity Biometric avec Protege GX.

L'onglet biométrique vous permet de coder les données biométriques de l'utilisateur et de les enregistrer à partir du lecteur sélectionné. L'identifiant sera saisi dans la deuxième ligne des numéros de carte de l'utilisateur, en utilisant le **numéro d'établissement par défaut** défini dans **Global | Sites | Biométriques** . Les données du doigt et du visage peuvent être enregistrées dans un seul dossier d'utilisateur.

Configuration du lecteur biométrique

- **Appareil d'inscription** : Sélectionnez le lecteur biométrique connecté qui sera utilisé pour enregistrer les données biométriques de l'utilisateur. **Lecteur d'inscription par défaut** peut être défini dans **Global | Sites | Biométriques**.

Doigt un/deux

- **Activer** : Utilisez ce doigt pour l'information d'identification Deux doigts peuvent être scannés, ce qui vous permet de définir un doigt de secours au cas où le premier serait blessé, ou d'utiliser un doigt comme signal de contrainte.
- **Contrainte** : Si cette option est activée, le doigt sera traité comme une pièce d'identité sous contrainte. L'accès sera accordé normalement, mais une entrée de trouble de contrainte de porte sera ouverte.
- **Scan** : Lance le lecteur biométrique sélectionné pour scanner le doigt de l'utilisateur.

Visage

- **Scan** : Lance le lecteur biométrique sélectionné pour scanner le visage de l'utilisateur

Utilisateurs | Salto

Cet onglet permet de configurer les options relatives aux verrous Salto pour cet utilisateur.

Cet onglet n'est visible que lorsque l'option Activer **l'intégration de Salto (SHIP)** est cochée dans **Global | Sites | Salto**. Pour plus d'informations, voir la note d'application 188 : Salto SHIP RW Pro Access Intégration avec Protege GX ou note d'application 335 : Salto SHIP ProAccess SPACE Intégration avecProtege GX .

Options Salto

- **Calendrier** : Un calendrier Salto définit les jours où les autorisations d'accès de l'utilisateur ont des heures différentes (comme les jours fériés).

  Les calendriers peuvent être programmés dans **Salto | Calendriers**. Le ou les horaires attribués au niveau d'accès de l'utilisateur définissent les périodes qui sont activées à des jours différents (voir la colonne **Salto** de **Sites | Horaires | Configuration**).
- **Utiliser temps d'ouverture prolongé** : Si cette option est activée, chaque fois que cet utilisateur se voit accorder l'accès à une porte Salto, la serrure s'ouvrira pendant le **Augmenter le temps d'ouverture** au lieu du **Temps d'ouverture** programmé dans **Salto | Portes | Général**. Ceci devrait être utilisé pour accorder aux personnes ayant des problèmes de mobilité des temps prolongés pour accéder aux portes.
- **Bureau** : Lorsque cette option est activée, l'utilisateur peut mettre les portes Salto en "mode bureau" (déverrouillage du loquet). Le mode bureau est activé en présentant une clé Salto tout en maintenant la poignée intérieure enfoncée, et annulé en répétant la procédure.

  Le **mode ouvert** de la porte doit supporter le mode bureau (**Salto | Portes**).
- **Utiliser l'antipassback** : Avec cette option activée, l'utilisateur sera affecté par toute restriction antipassback définie sur les portes Salto.
- **Ouvertures de vérification dans la clé** : Si cette option est activée, le système Salto générera une piste d'audit sur les informations d'identification Salto elles-mêmes lorsque cet utilisateur ouvrira une porte Salto. L'option **Audit sur les clés** doit également être sélectionnée dans la programmation **Salto | Portes | Général**.
- **PIN** : Lorsque cette option est activée, l'utilisateur peut utiliser son code PIN (onglet **Général**) pour accéder aux serrures Salto à clavier.
- **L'utilisateur peut surpasser la confidentialité** : Lorsque cette option est activée, l'utilisateur peut accéder à une porte Salto même si elle a été réglée en mode privé (verrouillée de l'intérieur).
- **L'utilisateur peut surpasser le verrouillage** : Lorsque cette option est activée, l'utilisateur peut ouvrir une porte Salto même si elle a été fermée par un verrouillage (fermeture d'urgence).

- **L'utilisateur peut verrouiller la porte** : Lorsque cette option est activée, l'utilisateur peut déclencher un verrouillage sur les portes Salto compatibles (avec écussons AMOK). Le verrouillage est initié en présentant la carte au lecteur AMOK (poignée intérieure inférieure) et annulé de la même manière.

Expiration de l'utilisateur et la clé

Une clé Salto peut être encodée et attribuée à un utilisateur à l'aide de la **fonction** Carte du programme **dans l'onglet** Général.

- **Début** : Lorsque cette option est activée, la clé Salto de l'utilisateur ne sera pas active avant la date spécifiée. Il ne sera pas en mesure d'accéder aux portes Salto avant cette date.
- **Fin** : Lorsque cette option est activée, la clé Salto de l'utilisateur expire après la date spécifiée. Ils ne pourront plus avoir accès aux portes Salto après cette date.
- **Activer revalidation de l'expiration de clé** : Lorsque cette option est activée, la clé Salto expirera à la fin de la **période de mise à jour**. Chaque fois que la clé est présentée à une Ubox ou à une serrure en ligne, elle est revalidée et la période de mise à jour est renouvelée.
- **Période de mise à jour** : Définit la durée de validité de la clé Salto après sa mise à jour sur une Ubox ou une serrure en ligne. Par exemple, pour une résidence de courte durée, vous pouvez régler la clé pour qu'elle expire toutes les 48 heures si elle n'est pas revalidée.
- **Période** : Définit la **Période de mise à jour** en jours ou en heures.
- **Touche d'annulation** : Ce bouton désactive la clé Salto de l'utilisateur.

Statut de la clé

- **Clé assignée** : La date à laquelle la clé a été attribuée (en lecture seulement).
- **Valide jusqu'à** : La date d'expiration de la clé (en lecture seulement).

Utilisateurs | Portes Salto / groupes de portes

Ces onglets ne sont visibles que lorsque l'option **Activer l'intégration de Salto (SHIP)** est activée dans **Global | Sites | Salto**. Pour plus d'informations, voir la note d'application 188 : Salto SHIP RW Pro Access Intégration avec Protege GX ou note d'application 335 : Salto SHIP ProAccess SPACE Intégration avec Protege GX .

Ces onglets vous permettent d'attribuer une ou plusieurs portes Salto ou groupes de portes auxquels l'utilisateur est autorisé à accéder. Vous pouvez également définir des horaires sur ces portes pour contrôler le moment où l'utilisateur a accès.

Les portes Salto peuvent également être attribuées à plusieurs utilisateurs en utilisant des niveaux d'accès (**Utilisateurs | Niveaux d'accès | Portes Salto / Groupes de portes**).

Le nombre maximum de portes que Salto prend actuellement en charge est de 64 000 par base de données. Un maximum de 96 portes (portes individuelles ou portes dans un groupe) peut être attribué à un utilisateur. Cette règle s'applique à l'ajout de portes/groupes de portes à un utilisateur directement ou via un niveau d'accès.

Utilisateurs | Serrures Cencon

Cet onglet n'est affiché que lorsque **l'option Permettre l'intégration de Cencon** est activée dans **Global | Sites | Cencon**. Pour plus de renseignements, reportez-vous à la Note d'application 160 : Configuration de l'intégration de Cencon avec Protege GX.

Cet onglet vous permet d'attribuer un ou plusieurs serrures Cencon auxquelles l'utilisateur est autorisé à accéder. Les serrures et groupes de serrures Cencon peuvent également être attribués aux utilisateurs par le biais de niveaux d'accès (**Utilisateurs | Niveaux d'accès | Serrures / groupes de serrures Cencon**).

Utilisateurs | Hébergement

L'hébergement est une fonctionnalité héritée qui n'est plus disponible.

Utilisateurs | Visiteurs

Cet onglet n'est affiché que si le VMS (système de gestion des visiteurs) a fait l'objet d'une licence. Pour plus d'informations, consulter la note d'application 287 : Protege GX système de gestion des visiteurs.

Recevoir les paramètres des visiteurs

- **L'utilisateur supporte les visiteurs** : Lorsqu'un visiteur se connecte au VMS, il doit sélectionner l'utilisateur qu'il visite. En activant cette option, cet utilisateur peut être sélectionné par les visiteurs.
- **Niveau d'accès du visiteur** : Le niveau d'accès sélectionné ici sera automatiquement attribué à tout visiteur qui sélectionne cet utilisateur. Définissez-le sur Aucun si aucun niveau d'accès ne doit être attribué aux visiteurs.
- **Mode de notification de visiteurs** : Définissez cette option sur Courriel pour que l'utilisateur reçoive une notification par courriel lorsqu'un visiteur se connecte pour lui rendre visite. Définissez-le sur Aucun pour ne pas recevoir de notifications.

  Les fonctions de courrier électronique automatisées dans Protege GX exigent qu'un serveur de courrier SMTP soit configuré dans **Global | Paramètres globaux | Paramètres de courrier électronique**.
- **Adresse courriel de notification** : L'adresse courriel à laquelle les notifications de visiteurs pour cet utilisateur seront envoyées.

Visiteur

- **L'utilisateur est un visiteur** : Champ en lecture seulement qui indique si cet utilisateur est un visiteur.
- **Départ prévu** : Lorsqu'un visiteur s'inscrit dans le VMS, il doit indiquer combien de temps il compte rester dans les locaux. Ce champ affiche leur heure de départ estimée, qui peut être mise à jour par un opérateur si nécessaire.

  Vous pouvez rechercher tous les visiteurs en retard en exécutant un rapport ou une recherche par utilisateur.
- **Checked In** : L'heure à laquelle le visiteur s'est connecté au VMS (en lecture seulement).
- **Checked Out** : L'heure à laquelle le visiteur a quitté le VMS (en lecture seulement).
- **Carte du visiteur désactivée** : Champ en lecture seule qui indique si le visiteur a actuellement un Identifiant attribuée. Lorsqu'un enregistrement de visiteur est désactivé (soit en se déconnectant du VMS, soit en cliquant sur le bouton ci-dessous), son identifiant est supprimé et cette case est cochée.
- **Déconnecter le visiteur** : Cliquez sur ce bouton pour désactiver immédiatement la fiche du visiteur.

Utilisateurs | Portail

Cet onglet est utilisé pour la fonction de synchronisation du portail des locataires. Pour des informations et des instructions de programmation, consultez le [[(Variable1)]]] guide de l'utilisateur du portail des locataires.Protege

Options générales

- **Numéro de téléphone** : Le numéro de téléphone de l'utilisateur sera synchronisé avec sa location et son enregistrement dans le répertoire téléphonique.

  Si l'utilisateur n'a pas de **courriel**, le numéro de téléphone sera utilisé comme méthode alternative pour synchroniser les détails de la location de l'utilisateur avec le répertoire de la station d'entrée, permettant aux visiteurs d'appeler vocalement l'utilisateur depuis la station d'entrée.

  Le numéro de téléphone n'est utilisé dans l'annuaire que si l'utilisateur n'a pas saisi d'adresse courriel.

  Les numéros de téléphone en double sont autorisés afin que plusieurs utilisateurs d'une même location puissent utiliser le même numéro de contact dans l'annuaire.
- **Nom de la location** : Le nom de la location de l'utilisateur, correspondant généralement à un numéro d'appartement ou à une adresse similaire. Une location portant ce nom sera créée dans le portail des locations

avec l'utilisateur comme locataire.

Un nom de location doit être saisi pour que l'utilisateur soit synchronisé avec le portail des locations.

Commandes manuelles de l'utilisateur

Un clic droit sur un enregistrement d'utilisateur (**Utilisateurs | Utilisateurs**) affiche un menu avec des commandes manuelles pour cet utilisateur.

Réinitialiser Antipassback

Cette commande réinitialise l'état d'antipassback d'un utilisateur. Cela permettra à l'utilisateur d'entrer ou de quitter toute partition dont l'accès lui a été refusé en raison de règles antipassback.

La fonctionnalité antipassback doit être configurée à l'aide du mode passback **entrée/sortie** dans **Programmation | Types de porte | Général**.

Recherche d'utilisateur

La fonction de recherche d'utilisateurs vous permet de générer des rapports temporaires ponctuels sur les utilisateurs, qui peuvent être imprimés, exportés ou envoyés par courriel. Il est idéal pour créer des rapports ad hoc qui n'ont pas besoin d'être répétés fréquemment.

Les recherches des utilisateurs sont équivalentes aux rapports des utilisateurs, mais la configuration ne peut pas être sauvegardée. Pour plus d'informations, consultez la section Rapports | Configuration | Utilisateur (la page 165).

Exécution d'une recherche d'utilisateur

1. Naviguez vers **Utilisateurs | Recherche d'utilisateurs**.
2. Sélectionnez le **type de rapport** . Choisissez parmi :
   - **Tous les utilisateurs** : Tous les utilisateurs actuellement programmés dans ce site.
   - **Tous les utilisateurs qui ont accès aux portes sélectionnées** : Tous les utilisateurs ayant des niveaux d'accès qui donnent accès aux portes sélectionnées.
   - **Tous les utilisateurs inclus dans les niveaux d'accès suivants** : Tous les utilisateurs auxquels sont attribués les niveaux d'accès sélectionnés.
   - **Tous les utilisateurs par événements** : Tous les enregistrements d'utilisateurs inclus dans les événements du filtre d'événements sélectionné, pendant la période spécifiée.
   - **Tous les utilisateurs par groupe de registres** : Tous les utilisateurs du groupe de registres sélectionné.
   - **Utilisateurs par type/portes d'événements** : Tous les utilisateurs qui ont déclenché des événements aux portes sélectionnées pendant la période de temps spécifiée.
   - **Cartes à veille d'expirer** : Tous les enregistrements d'utilisateurs dont l'expiration est prévue dans la période sélectionnée.
   - **Derniers utilisateurs à travers le(s) porte(s)** : Les derniers utilisateurs (et l'heure d'accès) qui ont accédé à la (aux) porte(s) sélectionnée(s).
   - **Tous les utilisateurs ne participant pas aux événements** : Tous les utilisateurs non inclus dans les événements du filtre d'événements sélectionné, au cours de la période spécifiée.
   - **Tous les visiteurs actuels** : Tous les visiteurs actuellement connectés (nécessite un système de gestion de visiteurs).
   - **Tous les visiteurs en attente** : Tous les visiteurs encore connectés après l'heure de fermeture prévue (nécessite un système de gestion de visiteurs).
   - **Tous les visiteurs par date** : Tous les visiteurs qui se sont connectés au cours d'une période spécifique (nécessite un système de gestion de visiteurs).
   - **Enregistrer l'historique modifié**: Tous les enregistrements d'utilisateur qui ont été modifiés au cours de la période sélectionnée, regroupés par utilisateur. Il comprend les paramètres qui ont été modifiés, les anciennes et nouvelles valeurs et l'opérateur.
   - **Tous les utilisateurs par niveaux d'accès** : Les utilisateurs ayant les niveaux d'accès spécifiés, regroupés par niveau d'accès. Les délais d'expiration des niveaux d'accès sont affichés. Les utilisateurs qui ont été désactivés ou dont le niveau d'accès a expiré ne sont pas inclus.
   - **Tous les niveaux d'accès par utilisateurs** : Les utilisateurs ayant les niveaux d'accès spécifiés, regroupés par utilisateur. Les délais d'expiration des niveaux d'accès sont affichés. Les utilisateurs qui ont été désactivés ou dont le niveau d'accès a expiré ne sont pas inclus.
3. Définissez le **titre** du rapport, qui sera affiché en haut de la page lorsque le rapport sera imprimé.
4. Saisissez les critères de **tri** que vous souhaitez :
   - **Colonne de tri**: Détermine la colonne dans laquelle les résultats seront triés.
   - **Sens de tri** : Détermine si les données renvoyées sont triées par ordre croissant ou décroissant.
   - **Groupe par** : Regroupe les données retournées selon la colonne définie.

5. Définissez toutes les options supplémentaires requises en fonction du **type de rapport** sélectionné. Par exemple, vous pouvez avoir besoin de spécifier une période de temps, ou des enregistrements supplémentaires tels que des portes ou des niveaux d'accès.
6. Dans l'onglet **Colonnes**, cliquez **sur Ajouter** et **Supprimer** pour sélectionner les colonnes qui seront incluses dans le rapport. Ceux-ci correspondent aux champs de la programmation des utilisateurs. Par défaut, seuls le prénom et le nom de famille sont inclus.
7. Pour modifier l'ordre des colonnes, sélectionnez un élément et utilisez les boutons **Déplacer vers le haut** et **Déplacer vers le bas** jusqu'à ce que vous obteniez la séquence souhaitée.
8. Cliquez sur **Trouver** pour commencer la recherche.
9. Un rapport temporaire est généré et affiché dans une vue en grille. Vous pouvez redimensionner ou réorganiser les colonnes affichées :
   - **Redimensionnez les colonnes** en plaçant votre souris sur le bord de l'en-tête de colonne jusqu'à ce qu'il forme une double flèche, puis faites glisser la colonne à la taille requise. Vous pouvez également utiliser le menu du bouton droit de la souris pour redimensionner automatiquement vos colonnes afin de les adapter au mieux.
   - **Réorganisez les colonnes** en faisant glisser et en déposant un en-tête de colonne vers une nouvelle position dans la grille.
   - **Supprimez des colonnes** en les faisant glisser de la section d'en-tête de colonne vers la liste. Lorsqu'une icône de suppression rouge apparaît sur l'en-tête de colonne, relâchez la souris pour supprimer la colonne.

   Vous pouvez utiliser la vue en grille pour trier, regrouper et filtrer davantage les résultats. Pour plus d'informations, consultez la section Travailler avec la vue de grille (la page 172).
10. L'icône **Sauvegarder** vous permet de sauvegarder la mise en page actuelle du rapport afin qu'elle puisse être utilisée pour d'autres recherches ou rapports générés par cet opérateur.
11. Cliquez sur l'icône **Imprimer** pour ouvrir la fenêtre d'aperçu avant impression dans laquelle vous pouvez imprimer, exporter ou envoyer les résultats par courriel(consultez la page 175).

Niveaux d'accès

Les niveaux d'accès sont attribués aux utilisateurs afin de déterminer l'accès dont ils disposent au sein du Protege GX site. Les niveaux d'accès attribués à un utilisateur définissent les portes, les partitions, les étages, les cabines d'ascenseur et les menus des claviers auxquels il est autorisé à accéder, ainsi que le moment où cet accès est valable.

Pour une démonstration, voir Configuration d'un niveau d'accès de base dans Protege GX sur la ICT chaîne YouTube.

Niveaux d'accès | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

Configuration

- **Horaire d'opération** : Ce calendrier détermine quand le niveau d'accès est valide. Lorsque le calendrier est invalide, les utilisateurs ne pourront utiliser aucune des autorisations accordées par le niveau d'accès.

  La plupart des caractéristiques individuelles d'un niveau d'accès peuvent également être contrôlées selon un calendrier spécifique sans affecter aucune des autres autorisations.

- **Temps pour activer la sortie** : Si l'une des options **Activer la sortie** ci-dessous est activée, la sortie/le groupe de sortie sera activé pendant la période (en secondes) définie ici.

  Ce paramètre a priorité sur le **temps d'activation** dans **Programmation | Sorties | Général** .

- **Accès du lecteur active la sortie** : Lorsque cette option est activée, toutes les sorties attribuées dans l'onglet **Sorties** ou **Groupes de sorties** seront activé lorsqu'un utilisateur obtient l'accès à un lecteur de cartes en utilisant ce niveau d'accès.

  L'option **Activer la sortie de niveau d'accès** doit être activée pour tout port du module d'expansion du lecteur où cette fonction sera utilisée (**Modules d'expansions | Modules d'expansions du lecteur | Lecteur 1/2**).

- **Accès au clavier active la sortie** : Lorsque cette option est activée, toutes les sorties attribuées dans l'onglet **Sorties** ou **Groupes de sorties** seront activées lorsqu'un utilisateur se connectera à un clavier en utilisant ce niveau d'accès.

  L'option **Activer la sortie de niveau d'accès** doit être activée pour tout clavier sur lequel cette fonction sera utilisée (**Modules d'expansions | Claviers | Options 1**).

- **Activer la sortie jusqu'à l'expiration du niveau d'accès** : Lorsque cette option est activée, si une sortie est activée par le niveau d'accès, elle sera désactivée lorsque le niveau d'accès expire dans l'enregistrement de l'utilisateur. Cela nécessite que l'utilisateur utilise les **options d'accès au lecteur qui active la sortie** ou **l'accès au clavier qui active la sortie** ci-dessus.

Cette fonction est utile pour les niveaux d'accès à court terme qui ne sont détenus que par un seul utilisateur, comme dans les systèmes de réservation. Par exemple, un utilisateur peut se voir attribuer l'accès à une salle de réunion particulière pendant une heure. Lorsqu'ils accèdent à la chambre pour la première fois, toutes les lumières s'allument (à partir de **l'accès du lecteur active à la sortie** ci-dessus). Lorsque le niveau d'accès expire, les lumières s'éteignent.

- **Basculer la sortie du niveau d'accès** : Lorsque cette option est activée, l'état de la sortie sera basculé chaque fois qu'il est déclenché par le niveau d'accès. Cela nécessite également que **l'accès au lecteur active la sortie** ou que **l'accès au clavier active la sortie** pour être autorisé..

  Par exemple, si les deux **Basculer la sortie du niveau d'accès** et **Accès du lecteur active la sortie** sont activées, lorsqu'un utilisateur badge sa carte à un lecteur pour la première fois, la sortie s'activera. Lorsqu'ils badgeront une deuxième fois au lecteur, la sortie s'éteindra.
- **Activer l'armement multi-badges** : Lorsque cette option est activée, les utilisateurs disposant de ce niveau d'accès peuvent exécuter diverses fonctions (telles que l'armement d'une partition ou le basculement d'une sortie) en badgeant ou en saisissant leurs informations d'identification plusieurs fois sur un lecteur de cartes.

  Les fonctions multi-badges sont définies par le paramètre du **mode d'armement du lecteur** dans **Modules d'expansions| Modules d'expansions du lecteur | Lecteur 1/2**.
- **Utiliser le type de porte du niveau d'accès** : Avec cette option activée, lorsqu'un utilisateur utilise ce niveau d'accès pour accéder à une porte, il utilise des informations d'identification alternatives au lieu de celles définies dans le type de porte primaire. Ces informations d'identification alternatives sont définies comme le **type de porte du niveau d'accès** dans **Programmation | Types de porte | Général** .

  Par exemple, cette fonction peut être utilisée pour faciliter le déplacement du personnel de sécurité sur le site.

Important: Cette option s'applique à toutes les portes qui sont intégrées dans ce niveau d'accès. Vérifier que toutes ces portes ont un **type de porte du niveau d'accès** valide attribué, sinon les utilisateurs peuvent se voir refuser l'accès en raison d'un type de porte non valide.

Restriction d'utilisation

- **Activer la restriction d'utilisation** : Cette fonction vous permet de limiter le nombre de fois qu'un utilisateur peut accéder aux portes en utilisant ce niveau d'accès. Une fois que l'utilisateur a dépassé la **limite d'utilisation**, il doit attendre que la **période de réinitialisation** soit écoulée avant que la limite ne soit réinitialisée et qu'il puisse utiliser le niveau d'accès pour accéder à nouveau aux portes.
- **Limite d'utilisation** : Détermine le nombre de fois qu'un utilisateur est autorisé à accéder aux portes concernées avant de déclencher la **période de réinitialisation**.
- **Réinitialiser la période** : La durée (en minutes, heures ou jours) pendant laquelle un utilisateur se verra refuser l'accès après avoir atteint la **limite d'utilisation** avant que cette limite ne soit réinitialisée.

La **période de réinitialisation** commence lorsque l'utilisateur atteint la **limite d'utilisation** et recommence si l'utilisateur tente à nouveau d'obtenir un accès pendant cette période.

Commandes

- Ce champ est utilisé pour envoyer des commandes de programmation à l'appareil. Il ne doit être utilisé que lorsqu'il est spécifiquement conseillé par la documentation ICT ou le support technique.

Ascenseur HLI

- **Étage de destination de l'ascenseur** : Si le système KONE RCGIF a été activé, lorsqu'un utilisateur badge à un lecteur DOP, un ascenseur sera appelé pour le transporter à l'étage défini ici. Pour plus d'informations, voir la note d'application 170 : Protege GX Intégration KONE HLI .

  Cette option vous permet également de définir l'étage d'origine pour un niveau d'accès dans l'intégration Schindler HLI. Pour plus d'informations, voir la note d'application 196 : Protege GX Intégration de Schindler HLI .

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Niveau d'accès | Portes

Cet onglet définit les **portes** auxquelles l'utilisateur à accès, **l'horaire** utilisé et la **direction d'accès** (entrée, sortie ou les deux) dans lequel l'utilisateur peut franchir la porte.

- Par défaut, **l'horaire** est réglé sur Toujours, ce qui signifie que l'accès à la porte définie est autorisé à tout moment. Lorsqu'un horaire est attribué, la porte ne sera accessible que si l'horaire est valide. Par exemple, vous pouvez souhaiter limiter l'accès des employés de bureaux aux heures de bureau.
- Par défaut, la **direction d'accès** est défini sur Les deux (entrée et sortie). Certaines portes peuvent être configurées pour permettre un accès dans une seule direction.

Niveaux d'accès | Groupes de portes

Cet onglet définit les **groupes de portes** auxquels l'utilisateur à accès, **l'horaire** utilisé et la **direction d'accès** (entrée, sortie, ou les deux) dans lequel l'utilisateur peut franchir les portes.

- **Inclure toutes les portes** : Sélectionner cette option pour affecter toutes les portes du site à ce niveau d'accès.

  Cette option doit être utilisée avec prudence, car elle donne un accès illimité à toutes les portes existantes et nouvelles du système. Dans de nombreux cas, il est plus sûr de créer un groupe de portes contenant toutes les portes actuelles à cette fin.

- Par défaut, **l'horaire** est réglé sur Toujours, ce qui signifie que l'accès au groupe de portes défini est autorisé à tout moment. Lorsqu'un horaire est attribué, les portes ne seront accessibles que lorsque l'horaire est valide. Par exemple, vous pouvez souhaiter limiter l'accès des employés de bureaux aux heures de bureau.
- Par défaut, la **direction d'accès** est défini sur Les deux (entrée et sortie). La limitation de la direction peut être utilisée, par exemple, pour permettre aux employés de sortir d'un bâtiment mais de ne pas y entrer à nouveau après les heures de travail.

Niveaux d'accès | Étages

Cet onglet définit les étages auxquels l'utilisateur a accès et **l'horaire** qui est utilisé.

- Par défaut, **l'horaire** est réglé sur Toujours, ce qui signifie que l'accès aux étages définis est autorisé à tout moment. Lorsqu'un horaire est attribué, l'étage ne sera accessible que lorsque l'horaire est valide.

Niveaux d'accès | Groupes d'étage

Définit les groupes d'étage auxquels l'utilisateur a accès et l'horaire qu'il utilise.

- **Inclure tous les étages** : Sélectionner cette option pour affecter tous les étages du site à ce niveau d'accès.

  Cette option doit être utilisée avec prudence, car elle donne un accès illimité à tous les étages existants et nouveaux du système. Dans de nombreux cas, il est plus sûr de créer un groupe d'étages contenant tous les étages actuels à cette fin.

- Par défaut, **l'horaire** est réglé sur Toujours, ce qui signifie que l'accès au groupe d'étages défini est autorisé à tout moment. Lorsqu'un horaire est attribué, les étages ne sont accessibles que lorsque l'horaire est valide.

Niveaux d'accès | Groupes d'ascenseurs

Cet onglet définit les **groupes d'ascenseurs** auxquels l'utilisateur a accès et **l'horaire** utilisé.

- **Inclure tous les ascenseurs**: Sélectionner cette option pour affecter tous les ascenseurs du site à ce niveau d'accès.

Cette option doit être utilisée avec prudence, car elle donne un accès illimité à tous les ascenseurs existants et nouveaux du système. Dans de nombreux cas, il est plus sûr de créer un groupe d'ascenseur contenant tous les ascenseurs actuels à cette fin.

- Par défaut, **l'horaire** est réglé sur Toujours, ce qui signifie que l'accès au groupe d'ascenseurs défini est autorisé à tout moment. Lorsqu'un horaire est attribué, les ascenseurs ne sont accessibles que lorsque l'horaire est valide.

Niveaux d'accès | Groupes de Menu

Cet onglet définit le groupe de menu auquel l'utilisateur a accès. Les groupes de menu déterminent les menus auxquels l'utilisateur a accès sur un clavier, et peuvent être programmés dans **Groupes | Groupes de menu** .

Un seul groupe de menu peut être attribué à chaque niveau d'accès.

Niveaux d'accès | Groupes de partitions d'armement

Cet onglet définit les groupes de partitions que l'utilisateur est autorisé à armer.

Si un utilisateur est autorisé à désarmer une partition (onglet **Désarmement des groupes de partitions**), il sera automatiquement autorisé à armer cette partition également ; cependant, l'autorisation d'armer une partition (onglet **Armement des groupes de partition**) n'accorde pas l'autorisation de désarmer cette dernière.

- **Inclure toutes les partitions** : Sélectionner cette option pour permettre l'armement de toutes les partitions du site à ce niveau d'accès.
- Par défaut, **L'horaire** est réglée sur Toujours, ce qui signifie que l'armement du groupe de partitions défini est autorisé à tout moment. Lorsqu'un horaire est attribué, les partitions ne peuvent être activées que lorsque l'horaire est valide.

Niveaux d'accès | Désarmement groupes de partitions

Cet onglet définit les groupes de partitions que l'utilisateur est autorisé à désarmer .

Si un utilisateur est autorisé à désarmer une partition (onglet **Désarmement des groupes de partitions**), il sera automatiquement autorisé à armer cette partition également ; cependant, l'autorisation d'armer une partition (onglet **Armement des groupes de partition**) n'accorde pas l'autorisation de désarmer cette dernière.

- **Inclure toutes les partitions** : Sélectionner cette option pour permettre le désarmement et l'armement de toutes les partitions du site à ce niveau d'accès.
- Par défaut, **l'horaire** est réglé sur Toujours, ce qui signifie que le désarmement du groupe de Partitions défini est autorisé à tout moment. Lorsqu'un horaire est attribué, les partitions ne peuvent être désarmées que lorsque l'horaire est valide.

Niveaux d'accès | Sorties

Cet onglet définit les sorties qui sont associées à ce niveau d'accès. Ces sorties peuvent être automatiquement activées ou basculées lorsque les utilisateurs accèdent aux lecteurs ou se connectent aux claviers.

Les options suivantes doivent également être configurées :

- Pour activer les sorties lorsque l'utilisateur accède à une porte :
  - **L'accès du lecteur active la sortie** (Onglet **Général**)
  - **Activer Sortie Niveau d'accès**. (**Modules d'expansion | Modules d'expansion du lecteur | Lecteur 1/2**)
- Pour activer les sorties lorsque l'utilisateur se connecte à un clavier :
  - **L'accès au clavier active la sortie** (Onglet **Général**)
  - **Activer la sortie de niveau d'accès** (**Modules d'expansions | Claviers | Options 1**)
- Options générales :

- **Temps d'activation de la sortie** (Onglet **Général**)
- **Activer la sortie jusqu'à l'expiration du niveau d'accès** (Onglet **General**)
- **Basculer la sortie du niveau d'accès** (Onglet **Général**)

Pour des exemples de programmation, voir Note d'application 204 : Sorties de niveau d'accès dans Protege GX.

Niveaux d'accès | Groupes de sortie

Cet onglet vous permet d'affecter un groupe de sortie à ce niveau d'accès. Les sorties de ce groupe peuvent être automatiquement activées ou basculées lorsque les utilisateurs accèdent aux lecteurs ou se connectent aux claviers.

Les options suivantes doivent également être configurées :

- Pour activer les sorties lorsque l'utilisateur accède à une porte :
  - **L'accès du lecteur active la sortie** (Onglet **Général**)
  - **Activer Sortie Niveau d'accès**. (**Modules d'expansion | Modules d'expansion du lecteur | Lecteur 1/2**)
- Pour activer les sorties lorsque l'utilisateur se connecte à un clavier :
  - **L'accès au clavier active la sortie** (Onglet **Général**)
  - **Activer la sortie de niveau d'accès** (**Modules d'expansions | Claviers | Options 1**)
- Options générales :
  - **Temps d'activation de la sortie** (Onglet **Général**)
  - **Activer la sortie jusqu'à l'expiration du niveau d'accès** (Onglet **General**)
  - **Basculer la sortie du niveau d'accès** (Onglet **Général**)

Pour des exemples de programmation, voir Note d'application 204 : Sorties de niveau d'accès dans Protege GX.

Niveaux d'accès | Portes Salto / groupes de porte

Ces onglets ne sont visibles que lorsque l'option **Activer l'intégration de Salto (SHIP)** est activée dans **Global | Sites | Salto** . Pour plus d'informations, voir la note d'application 188 : Salto SHIP RW Pro Access Intégration avec Protege GX ou Note d'application 335 : Salto SHIP ProAccess SPACE Intégration avec Protege GX .

Ces onglets vous permettent d'attribuer une ou plusieurs portes Salto individuelles ou groupes de portes auxquelles les utilisateurs sont autorisés à accéder. Les portes Salto peuvent également être attribuées à des utilisateurs individuels (**Utilisateurs | Utilisateurs | Portes Salto / Groupe de porte**).

- Par défaut, **l'horaire** est réglé sur Toujours, ce qui signifie que l'accès aux portes Salto définies est autorisé à tout moment. Lorsqu'un horaire est attribué, les portes ne seront accessibles que lorsque l'horaire est valide.

Le nombre maximum de portes que Salto prend actuellement en charge est de 64 000 par base de données. Un maximum de 96 portes (portes individuelles ou portes dans un groupe) peut être attribué à un utilisateur. Cette règle s'applique à l'ajout de portes/groupes de portes à un utilisateur directement ou via un niveau d'accès.

Niveaux d'accès | Serrures Cencon / groupes de serrures

Ces onglets ne sont affichés que lorsque l'option **Activer l'intégration Cencon** est activée dans **Global | Sites | Cencon** . Pour plus de renseignements, voir la Note d'application 160 : Configuration de l'intégration Cencon avec Protege GX.

Ces onglets vous permettent d'attribuer un ou plusieurs serrures Cencon individuels ou groupes de serrure auxquels les utilisateurs sont autorisés à accéder. Les serrures et groupes de serrures Cencon peuvent également être attribués aux utilisateurs par le biais de niveaux d'accès (**Utilisateurs | Niveaux d'accès | Serrures / groupes de serrures Cencon**).

Niveaux d'accès | Clés / Groupes de clés

Ces onglets ne sont disponibles que lorsque l'intégration des cabinets de clés est activée dans **Global | Sites | Cabinets de clés** , et que certaines clés ou groupes de clés ont été synchronisés avec Protege GX. Pour plus de renseignements, reportez-vous à la Note d'application 220 : Intégration Touch de KeyWatcher dans Protege GX ou Note d'application 331 : Intégration de KeySecure avec Protege GX.

Ces onglets vous permettent d'attribuer une ou plusieurs clés individuelles ou groupes de clés auxquels les utilisateurs sont autorisés à accéder.

- Par défaut, **l'horaire** est réglé sur Toujours, ce qui signifie que l'accès aux clés définies est autorisé à tout moment. Lorsqu'un horaire est attribué, les clés ne seront accessibles que lorsque l'horaire est valide.

Champs personnalisés

Les champs personnalisés sont des champs définis par l'opérateur qui peuvent être affichés dans un registre d'utilisateur. Ceux-ci peuvent enregistrer de nombreuses données différentes, telles que du texte, des chiffres, des dates et des sélections déroulantes.

Afin d'afficher et d'utiliser les champs personnalisés, vous devez créer des onglets de champs personnalisés dans **Utilisateurs | Onglets de champs personnalisés**.

Champs personnalisés | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

Configuration

- **Onglet** : Définit l'onglet du champ personnalisé dans lequel le champ personnalisé apparaît dans chaque registre d'utilisateur. Ceux-ci peuvent être créés dans les onglets **Utilisateurs | Onglets de champ personnalisé**.
- **Type de champ** : Définit le type d'informations qui seront enregistrées dans ce champ personnalisé. Choisissez parmi :
  - Texte
  - Numérique
  - Heure
  - Date
  - Heure et date
  - Option (une seule case à cocher)
  - Lien (dans l'onglet utilisateur, vous pouvez cliquer sur le bouton **Lien** pour ouvrir automatiquement le lien)
  - Case déroulante (les options sont définies dans l'onglet **Articles déroulants**)
  - Image
- **Valeur par défaut** : Définissez éventuellement une valeur par défaut pour le champ. La valeur requise varie en fonction du **Type de champ** (par exemple, texte, nombre, opérateur booléen).
- **Pixels** : Définit la largeur et la hauteur en pixels lorsque le **Type de champ** est réglé sur Image.

Si un champ personnalisé est modifié en un type de champ Option après sa création initiale, l'option sera automatiquement activée pour tous les utilisateurs (y compris les utilisateurs d'appartement). Si vous créez un champ personnalisé et que vous oubliez de définir le type de champ sur Option avant de l'enregistrer, vous devez supprimer le champ personnalisé et le réinscrire correctement plutôt que de modifier le type.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Champs personnalisés | Articles déroulants

Cet onglet vous permet de définir les options qui apparaîtront dans la liste déroulante lorsque le **Type de champ** est réglé sur Case déroulante. Cliquez sur **Ajouter** pour créer un nouvel article de liste déroulante.

- **Texte d'affichage** : La description de l'article de la liste.
- **Valeur** : L'index ID de l'article. Cela détermine l'ordre des articles dans la liste déroulante.

Onglets de champ personnalisé

Les onglets de champ personnalisé sont des onglets supplémentaires personnalisables qui apparaissent sous les registres des utilisateurs pour afficher les champs personnalisés. Vous pouvez assigner des champs personnalisés à un onglet de champ personnalisé en utilisant l'option **Onglet** dans **Utilisateurs | Champs personnalisés | Général**.

Onglets de champ personnalisé | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Éditeur de modèle de carte

Utilisez l'éditeur de modèles de cartes pour créer des modèles personnalisés de photos ID et définir la mise en page et les informations incluses sur la carte ou l'étiquette d'un utilisateur.

La photo ID est une fonction sous licence séparée. Pour les instructions de programmation, voir la note d'application 149 : Création d'un modèle de Photo ID dans Protege GX.

Menus de l'éditeur de modèle de carte

Propriétés du modèle de carte

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.
- **Imprimer les deux côtés** : Lorsque cette option est activée, les deux côtés du modèle de carte sont imprimés. Si cette option n'est pas activée, seul le recto de la carte sera imprimé.

Pinceaux

La section des pinceaux est utilisée pour définir la couleur, la visibilité et l'opacité des lignes, du texte et des boutons sur le modèle de carte.

1. Développez la section **Pinceaux** et sélectionnez un élément dans l'éditeur.
2. Choisissez si vous modifiez la couleur de **fond**, la **Bordure** ou le **Premier plan** de l'élément. Cela dépend de l'élément en cours de configuration.
3. Définissez les couleurs de l'élément :
   - Pour définir une couleur solide, cliquez sur l'onglet **Solid** et sélectionnez la couleur à l'aide du sélecteur de couleur ou en saisissant des valeurs RVB.
   - Pour créer un dégradé, cliquez sur l'onglet **Gradient** pour afficher une barre de glissement sous les sélecteurs de couleur. Cliquez sur chaque curseur pour définir la couleur de chaque côté individuellement, puis ajustez les curseurs pour obtenir l'effet souhaité.
   - Pour ne définir aucune couleur (transparent), cliquez sur l'onglet **Null**.
4. Indiquez si l'élément est **Visible** ou **Caché**.
5. Définissez la **Opacité** de l'élément.

Champs d'utilisateurs

Cette section vous permet d'ajouter des champs utilisateur au modèle de carte dans différents formats. Par exemple, vous pouvez afficher le nom et la date d'expiration de la carte de chaque utilisateur (texte), les détails des informations d'identification, la photo et les données personnalisées telles que le numéro de badge sous la forme d'un code à barres.

1. Développez la section **Champs d'utilisateur** et cliquez sur **Ajouter** pour ajouter un nouveau champ d'utilisateur.
2. Définir le **type de champ** Les options sont :

- **Champs d'utilisateur** : Champs standard disponibles pour tout utilisateur, par exemple le nom, le numéro d'établissement/de carte, la date d'expiration, etc.
- **Porte-photo** : La photo de l'utilisateur telle que renseignée dans l'onglet **Utilisateurs | Utilisateurs | Photo**.
- **Champs élargis** : Les champs affichés dans l'onglet **Étendu** de l'utilisateur. **L'affichage des champs personnalisés prédéfinis dans utilisateurs** doit être activé dans **Global | Sites | Affichage**.

  Consultez les **Actions d'impression de la carte** ci-dessous pour remplir automatiquement certains champs lors de l'impression de la carte.
- **Champs personnalisés** : Tous les champs personnalisés des utilisateurs définis dans **Utilisateurs | Utilisateurs | Champs personnalisés**.
- **Masquer** Une bande noire utilisée pour isoler les sections de la carte où l'impression doit être évitée. Le masque est automatiquement placé dans la position par défaut correspondant au type de masque requis (par exemple, un masque de bande magnétique est placé horizontalement sur la largeur de la carte), mais il peut être déplacé et redimensionné si nécessaire.
- **Code barre** : Un code barre contenant les données d'un champ pertinent de l'onglet utilisateur **Étendu**. Sélectionnez le champ personnalisé requis, puis choisissez le format de code barre requis pour votre système.

3. Faites glisser et déposez le ou les éléments requis sur le modèle de carte. Puis **Fermez** la fenêtre surgissante.
4. Déplacer le champ utilisateur en cliquant et en le faisant glisser, le redimensionner en utilisant les carrés dans les coins, et le faire pivoter en utilisant les cercles dans les coins.
5. Pour les champs de texte, définissez les détails de mise en forme tels que **Police**, **Taille de la police** et le style du texte.

Le champ **Données** est en lecture seule et n'a pas besoin d'être configuré.

Lignes

Cette section vous permet de dessiner des lignes et des formes de base sur le modèle de carte.

1. Développez la section **Lignes** et cliquez sur **Ajouter**.
2. Votre curseur se transformera en une forme **+**. Cliquez quelque part dans le champ de dessin pour créer le premier nœud de la ligne.
3. Pour créer un nœud ou un coin supplémentaire, cliquez une fois. La ligne peut avoir autant de coins que nécessaire, ce qui vous permet de créer des formes complexes.
4. Pour compléter la ligne, double-cliquez.
5. Donnez à la ligne un **Nom** descriptif.
6. Une fois la ligne terminée, vous pouvez
   - Définir la **Largeur de la ligne** dans la section **Lignes**.
   - Définir la couleur avec l'attribut **Bordure** dans le menu **Pinceaux**.
   - Déplacez la ligne en cliquant et en la faisant glisser à l'intérieur de la boîte en pointillés.
   - Redimensionnez la ligne en cliquant et en faisant glisser les carrés aux coins.
   - Faites pivoter la ligne en cliquant et en faisant glisser les cercles dans les coins.
   - Déplacez la ligne devant ou derrière d'autres éléments à l'aide des boutons **Front** et **Back** de la barre d'outils.

Texte

Cette section vous permet d'ajouter des étiquettes de texte à votre modèle de carte (par exemple, descriptions des champs, notes).

1. Développez la section **Texte** et cliquez sur **Ajouter**.
2. Votre curseur se transformera en une forme **+**. Cliquez et faites glisser quelque part sur le champ de dessin pour créer une zone de texte.
3. Donnez au texte un **Nom** descriptif.
4. Dans le champ **Texte**, entrez le texte requis.
5. Une fois le texte terminé, vous pouvez :
   - Définir la **Police**, la **Taille de la police** et le style du texte dans la section **Texte**.
   - Définir la couleur avec l'attribut **Premier plan** dans le menu **Pinceaux**.
   - Déplacez la zone de texte en cliquant et en la faisant glisser à l'intérieur de la boîte en pointillés.
   - Redimensionnez la zone de texte en cliquant et en faisant glisser les carrés dans les coins.
   - Faites pivoter la zone de texte en cliquant sur les cercles situés dans les coins et en les faisant glisser.
   - Déplacez la zone de texte devant ou derrière d'autres éléments à l'aide des boutons **Front** et **Back** de la barre d'outils.

Images

Vous pouvez ajouter des images telles que des logos d'entreprise et des images d'arrière-plan au modèle de carte.

1. Cliquez sur **Ajouter**, puis saisissez un chemin de fichier ou cliquez sur l'ellipse **[...]** pour naviguer vers une image. L'image peut être au format .bmp ou .jpg.

   Assurez-vous que toutes les images sont situées dans un dossier réseau partagé auquel les clients ont accès. Si le lien vers une image est rompu ou si l'ordinateur client ne peut pas y accéder, l'image n'apparaîtra pas dans le client Protege GX.

2. Votre curseur se transformera en une forme **+**. Cliquez et glissez quelque part dans le champ de conception pour ajouter l'image.
3. Donnez à l'image un **Nom** descriptif.
4. Une fois l'image terminée, vous pouvez :
   - Déplacer l'image en cliquant et en faisant glisser à l'intérieur de la boîte en pointillés.
   - Redimensionner l'image en cliquant et en faisant glisser les carrés situés dans les coins.
   - Faire pivoter l'image en cliquant et en faisant glisser les cercles aux coins.
   - Déplacez l'image devant ou derrière d'autres éléments en utilisant les boutons **Front** et **Back** de la barre d'outils.

     Vous pouvez utiliser le bouton **Arrière** pour créer une image de fond.

Codage des cartes

Cette section vous permet d'encoder ICT des cartes MIFARE sécurisées (MIFARE diversifié) ou d'imprimer des bandes magnétiques, si l'imprimante de cartes est capable de coder des cartes. Ces processus ont lieu si l'opérateur sélectionne **Imprimer & modèle de processus** ou **Modèle de processus uniquement** lors de l'impression d'une carte d'utilisateur à partir de **Utilisateurs | Utilisateurs | Photo**.

- **ICT secteur** : Activez cette option pour demander à l'imprimante à cartes de lire ou d'écrire des cartes avec un encodage MIFARE sécurisé ICT (MIFARE diversifié).

  Contactez ICT pour plus d'informations sur l'encodage des cartes.

- **Processus** : Le processus qui se déroulera lors de l'impression de la carte :
  - **Lecture** : Lorsque la carte est imprimée, l'encodeur lit le justificatif existant et le saisit dans le champ **Numéro d'établissement/de carte** de l'utilisateur.
  - **Écrire** : Lorsque la carte est imprimée, l'encodeur écrit sur la carte le justificatif d'identité du champ **Numéro d'établissement/de carte** de l'utilisateur. Les numéros d'établissement et de carte doivent correspondre à ceux inclus dans le fichier encoder.ini.

- **Bande magnétique** : Avec cette option activée, lorsque la carte est imprimée, l'imprimante peut également écrire une bande magnétique sur la base des données utilisateur. Assurez-vous que vous avez inclus le masque approprié dans la section **Champs utilisateur** ci-dessus.
- **Piste1-3** : Définissez les données qui seront écrites sur chaque piste de la bande magnétique. Les champs disponibles sont ceux de l'onglet **Users | Users | Extended**.

Actions d'impression de cartes

Cette section permet au modèle de modifier la fiche de l'utilisateur lorsque la carte est imprimée. Ceci peut être utilisé avec les champs de l'onglet **Utilisateurs | Utilisateurs | Étendus**. Par exemple, vous pouvez configurer le modèle de carte pour qu'il mette à jour le champ **Type de badge** avec le type de carte qui est imprimé.

L'onglet **Étendu** n'est visible que lorsque l'option **Afficher les champs personnalisés prédéfinis dans les utilisateurs** est activée dans **Global | Sites | Affichage**. Voir également l'option **Enregistrer le numéro de badge et la date après l'impression de la carte** dans **Global | Défauts du site**.

Les actions disponibles sont :

- **Mise à jour du champ utilisateur avec la date d'impression** : La date d'impression sera écrite dans le champ utilisateur spécifié.
- **Mettre à jour champ d'utilisateur avec valeur** : Une chaîne ou une valeur spécifique sera écrite dans le champ utilisateur spécifié. Le type de **Valeur** dépend du type de champ utilisateur sélectionné (par exemple, le champ **Date d'expiration du badge** nécessite la saisie d'une date).
- **Copier la valeur entre les champs utilisateur** : Les données dans un champ utilisateur seront écrasées par les informations d'un autre champ utilisateur. Les deux champs doivent avoir le même type (par exemple, les deux textes ou les deux dates). Les champs personnalisés des utilisateurs définis dans **Utilisateurs | Champs personnalisés** peuvent également être saisis ici.

Barre d'outils de l'éditeur de modèles de cartes

La barre d'outils offre une fonctionnalité permettant de contrôler la disposition et le positionnement des éléments ajoutés à un modèle de carte.

Bouton	Fonction
Refaire	Vous permet de rétablir (refaire) la dernière action qui a été défaite.
Défaire	Vous permet de défaire la dernière action.
Copier	Copie le ou les objets sélectionnés dans le presse-papiers.
Coller	Colle le contenu du presse-papier dans le champ de conception.
Effacer	Enlève l'objet sélectionné du champ de conception.
Aligner	Si cette option est activée, lorsque vous dessinez, redimensionnez ou déplacez un objet, il s'alignera ou s'enclenchera sur les objets les plus proches dans le champ de conception, même si la règle n'est pas visible. Si votre objet ne se déplace pas là où vous le souhaitez, désactivez cette option.
Angle	Aligne le ou les objets sélectionnés sur l'angle de grille polaire le plus proche.
Règle	Sélectionnez cette option pour faire basculer la règle sur on ou sur off.
Avant	Déplace l'objet sélectionné devant d'autres objets
Arrière	Déplace l'objet sélectionné derrière d'autres objets
Aligner en haut	Aligne tous les objets sélectionnés sur le bord supérieur du dernier objet sélectionné.
Alig bas	Aligne tous les objets sélectionnés sur le bord inférieur du dernier objet sélectionné
Alig Gch	Aligne tous les objets sélectionnés sur le bord gauche du dernier objet sélectionné.

Bouton	Fonction
Alig Drt	Aligne tous les objets sélectionnés sur le bord droit du dernier objet sélectionné.
Paysage	Fait basculer la mise en page de la carte entre l'orientation paysage et portrait.

Menu Événements

Le menu événements contient les fonctions utilisées pour créer des filtres d'événements, configurer des alarmes opérateur et créer des actions automatiques qui se produisent lors d'événements spécifiques.

Recherche d'événement

La fonction de recherche d'événement vous permet de générer des rapports temporaires ponctuels sur les utilisateurs, qui peuvent être imprimés, exportés ou envoyés par courriel. Cela permet de visualiser simplement ce qui se passe dans le système.

Les recherches d'événements sont semblables aux rapports d'événements (consultez la page 155), mais la configuration ne peut pas être sauvegardée et moins d'options de personnalisation sont disponibles.

Recherche d'événement en cours d'exécution

1. Naviguez vers **Événements | Recherche d'événement**.
2. Sélectionnez la période de temps pour les événements. Choisissez une période dans la liste disponible ou saisissez une date et une heure de début spécifiques.
3. Vous pouvez choisir **d'inclure tous les types d'événements** ou désactiver cette option et sélectionner des types d'événements spécifiques.
4. Si l'option **Inclure tous les types d'événements** a été désactivée, sélectionnez le(s) type(s) d'événements à inclure.
   - Cliquez sur **Ajouter** pour ouvrir la fenêtre **Sélectionner les types d'événements**.
   - Les types d'événements sont classés par catégories (par exemple, Tous les événements des partitions). Sélectionnez des types d'événements et des catégories en les mettant en évidence et en cliquant sur **OK**, ou en les faisant glisser et en les déposant dans la fenêtre principale.
   - Lorsque tous les types d'événements requis ont été ajoutés, cliquez sur **OK**.

   Il n'est actuellement pas possible de sélectionner plusieurs événements.
5. Dans l'onglet **Registres**, vous pouvez spécifier jusqu'à deux filtres de registre pour affiner la recherche. Par exemple, vous pouvez sélectionner un groupe d'utilisateurs et une porte pour rechercher les événements liés à cette porte.
   - Cliquez sur **Ajouter** pour ouvrir la fenêtre **Sélectionner les appareils**.
   - Sélectionnez le **TypeAppareil** (et le **Contrôleur**, le cas échéant), puis sélectionnez les **Appareils** parmi ceux disponibles.
   - Créez un second filtre de registre si nécessaire.
6. Cliquez sur **Trouver** pour commencer la recherche.
7. Un rapport temporaire est généré et affiché dans une vue de grille. Vous pouvez redimensionner ou réorganiser les colonnes affichées :
   - **Redimensionnez les colonnes** en plaçant votre souris sur le bord de l'en-tête de colonne jusqu'à ce qu'il forme une double flèche, puis faites glisser la colonne à la taille requise. Vous pouvez également utiliser le menu du bouton droit de la souris pour redimensionner automatiquement vos colonnes afin de les adapter au mieux.
   - **Réorganisez les colonnes** en faisant glisser et en déposant un en-tête de colonne vers une nouvelle position dans la grille.
   - **Supprimez des colonnes** en les faisant glisser de la section d'en-tête de colonne vers la liste. Lorsqu'une icône de suppression rouge apparaît sur l'en-tête de colonne, relâchez la souris pour supprimer la colonne.

   Vous pouvez utiliser la vue de grille pour trier, regrouper et filtrer davantage les résultats. Pour plus d'informations, consultez la section Travailler avec la vue de grille (la page 172).

8. L'icône **Sauvegarder** vous permet de sauvegarder la mise en page actuelle du rapport afin qu'elle puisse être utilisée pour d'autres recherches ou rapports générés par cet opérateur.
9. Si plus de 200 événements sont retournés, utilisez les boutons **Précédent** et **Suivant** pour naviguer entre les résultats qui couvrent plusieurs pages.
10. Cliquez sur l'icône **Imprimer** pour ouvrir la fenêtre d'aperçu avant impression dans laquelle vous pouvez imprimer, exporter ou envoyer les résultats par courriel (consultez la page 175).

Filtres d'événements

Les filtres d'événements sont utilisés pour trier et catégoriser les données d'événements et d'alarmes. Ils peuvent servir à déterminer les événements qui déclenchent des alarmes et d'autres actions, ainsi que les événements qui sont inclus dans les rapports et les listes des statuts en direct.

Pour plus de renseignements et d'instructions de programmation, consulter la Note d'application 332 : Configurer les notifications d'événements dans Protege GX.

Filtres d'événements | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Filtres d'événements | Types d'événements

- **Inclure tous les types d'événements** : Activez cette option pour inclure tous les types d'événements dans le filtre. Cela signifie que tout type d'événement sera inclus (par exemple, dans un rapport d'événement), à condition qu'il réponde aux conditions de l'onglet **Registres**.

Types d'événements

Cliquez sur **Ajouter** pour sélectionner les types d'événements qui seront inclus par le filtre. Les types d'événements sont classés par catégories (par exemple, Tous les événements des partitions). Vous pouvez sélectionner des types d'événements et des catégories en les mettant en évidence et en cliquant sur **OK**, ou en les faisant glisser et en les déposant dans la fenêtre principale.

Filtres d'événements | Registres

Vous pouvez configurer jusqu'à deux filtres de registre pour restreindre davantage les éléments que le filtre d'événements inclura.

- Si un quelconque registre est saisi dans ces champs, le filtre d'événements n'inclut que les événements impliquant ces registres.
- Si aucun registre n'est saisi dans ces champs, le filtre d'événements inclut les événements de tous les registres.

Cliquez sur **Ajouter** pour saisir les registres pour chaque champ. Sélectionnez un **TypeAppareil** (par exemple, sortie, partition) et un **Contrôleur** si nécessaire, puis cochez les cases des registres pertinents et cliquez sur **OK**.

Alarmes

Les alarmes sont des événements spécifiques qui génèrent des notifications pour les Protege GX opérateurs. Les notifications d'alarme doivent être reconnues par un opérateur, soit à partir de la notification surgissante, soit sur la page d'état prédéfinie Toutes les alarmes.

Ce type d'alarme est une alarme opérateur, c'est-à-dire un événement qui génère une notification pour inciter un opérateur à agir. Ceci est différent des alarmes de partition qui sont générées sur place et signalées à la station centrale de surveillance. Les événements qui provoquent des alarmes de partition ne génèrent pas automatiquement des alarmes opérateur - ils doivent être configurés spécifiquement.

Lorsqu'un opérateur reçoit une notification d'alarme, il peut faire un clic droit sur l'événement et reconnaître l'alarme. En option, il est possible de laisser un commentaire sur l'alarme. Au besoin, ils peuvent également désactiver temporairement l'alarme en cliquant sur l'icône en haut à droite de la fenêtre surgissante. Les paramètres d'affichage de l'opérateur pour les alarmes peuvent être modifiés sous **Global | Rôles | Affichage**.

Pour plus de renseignements et d'instructions de programmation, consulter la Note d'application 332 : Configuration des notifications d'événements dans Protege GX.

Problème connu : Si une deuxième fenêtre surgissante (telle que l'outil de recherche ou la boîte de dialogue d'armement de partition) est ouverte alors que la fenêtre d'alarmes est déjà ouverte, celle-ci peut apparaître derrière la fenêtre d'alarmes et rendre la fenêtre d'alarmes inactive. Si cela se produit, vous pouvez fermer la deuxième fenêtre en appuyant sur **Echap** , ou utiliser **Windows + Gauche/Droite/Haut** pour déplacer la deuxième fenêtre vers une autre partie de l'écran. Pour éviter ce problème, déplacer la fenêtre des alarmes avant d'ouvrir toute autre fenêtre surgissante.

Alarmes | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Configuration

- **Instructions** : Le texte saisi ici sera inclus dans la fenêtre contextuelle d'alarme dans la colonne Instructions. Ceci est utile pour saisir de brèves instructions à l'intention de l'opérateur lorsqu'il visualise l'alarme. Des instructions peuvent également être envoyées au personnel à l'aide de l'action email sur événement (regardez **Événements | Actions**).

  Ce champ ne prend en charge que 256 caractères. Tout caractère dépassant cette limite ne sera pas enregistré.

- **Instructions 2** : Ce champ peut être utilisé pour saisir des instructions dans une deuxième langue. Ceux-ci seront affichés dans l'événement d'alarme dans l'autre langue qui a été installée avec le logiciel.

  Ce champ ne prend en charge que 256 caractères. Tout caractère dépassant cette limite ne sera pas enregistré.

- **Filtre d'événement**: Ce filtre d'événement est utilisé pour déterminer les événements qui déclencheront la notification d'alarme.
- **Plan d'étage** : Le plan d'étage associé à l'alarme peut être affiché en faisant un clic droit sur l'événement dans une page du statut.

- **Priorité d'alarme**: La priorité affectée à l'alarme détermine l'ordre dans lequel les alarmes sont affichées dans la notification surgissante et la page de statut. Les numéros les plus élevés apparaîtront plus haut dans la liste. Les priorités d'alarme peuvent être créées dans **Événements | Priorités d'alarme**.
- **Liste de routage d'alarme**: L'enregistrement d'acheminement de l'alarme associé à l'alarme détermine le "chemin" que suivra l'alarme, c'est-à-dire les postes de travail des opérateurs qui recevront l'alarme en premier, et ceux qui seront notifiés si les premiers ne la reconnaissent pas. Le routage d'alarme peut être configuré dans **Événements | Routage d'alarme**.
- **Commentaires de reconnaissance d'alarme** : Définir si les commentaires sont obligatoires, facultatifs ou non autorisés lorsque les opérateurs reconnaissent les alarmes. Si Jamais est sélectionné, la fenêtre de commentaire d'alarme ne sera pas affichée.

  Lorsque plusieurs alarmes sont reconnues en même temps ou que le même événement est inclus dans plusieurs enregistrements d'alarme, les alarmes qui nécessitent ou permettent des commentaires sont prioritaires par rapport à celles qui n'en nécessitent pas. Par exemple, si l'alarme A est réglée sur Doit et l'alarme B sur Jamais, lorsque les deux alarmes sont reconnues ensemble, l'opérateur doit entrer un commentaire.

- **Son de l'alarme** : Définissez le son personnalisé qui sera joué lorsque cette alarme se produit. Vous pouvez ajouter des sons d'alarme personnalisés dans **Global | Paramètres globaux | Son**.

  Si cette option n'est pas définie, le paramètre **Son de l'alarme** dans **Global | Paramètres globaux | Son** sera utilisé.

Options de la caméra

- **Permettre le pop up de la caméra** : Activez cette option pour afficher une fenêtre contextuelle de la caméra à côté de la fenêtre contextuelle de l'événement d'alarme. Cela affichera la caméra associée à l'événement (c'est-à-dire la **Caméra** assignée à la porte, à la partition, à l'entrée ou à la sortie programmable spécifique).

  La fenêtre contextuelle de la caméra respecte les règles de routage d'alarme, ce qui lui permet d'être envoyée vers des stations de travail spécifiques. Vous pouvez également restreindre la fenêtre contextuelle de la caméra pour des opérateurs spécifiques en utilisant le paramètre **Permettre le pop up de la caméra** dans **Global | Rôles | Afficher**.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Actions

Les actions permettent de déclencher un processus qui s'exécute automatiquement lorsque des événements spécifiques se produisent. Par exemple, vous pouvez envoyer des événements par courriel pour avertir les personnes concernées, déclencher une caméra ou un DVR pour se concentrer sur la source de l'événement, ou envoyer des événements à des systèmes tiers intégrés.

L'action préconfigurée par défaut est Enregistrer les événements, qui enregistre automatiquement tous les événements entrants dans la base de données Protege GX. Ceci ne peut pas être modifié.

Actions | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Configuration

- **Type** : Sélectionner le type d'action qui se produira lorsqu'un événement pertinent est enregistré. Différents paramètres de configuration sont disponibles/pertinents selon le type sélectionné. Choisissez parmi :
  - **Enregistrer vers la base de données**: Sauvegarde un enregistrement de l'événement dans la base de données ProtegeGXEvents . Cette option est uniquement utilisée pour l'action préconfigurée Enregistrer les événements.
  - **Envoyer commande PTZ** : Envoie une commande PTZ à un DVR connecté. Cela permet à la caméra de se déplacer vers une position spécifique prédéfinie. Par exemple, lorsqu'une porte est forcée, vous pouvez souhaiter qu'une caméra proche se concentre sur cette porte.
  - **Fenêtre surgissante de la caméra** : Une fenêtre surgissante affiche les flux en direct et archivés d'une caméra aux opérateurs.
  - **Exécuter le scr**iptCette option est réservée pour un développement futur.:
  - **Envoyer courriel**: Envoie un courriel au sujet de l'événement à une ou plusieurs adresses électroniques spécifiées.
  - **Envoyer l'événement**: Envoie l'événement à une adresse IP définie au format XML. Cela peut être utilisé pour créer des intégrations personnalisées avec des systèmes tiers.
  - **Action DVR personnalisée**: Envoie une chaîne de commande personnalisée à un DVR connecté. Cela peut être utilisé pour créer des intégrations personnalisées avec les systèmes DVR.
  - **Supprimer la carte du visiteur**: Déconnecte automatiquement le visiteur qui a déclenché l'événement. L'enregistrement du visiteur sera soit désactivé, soit supprimé en fonction du paramètre du **Mode de paiement** (**Visiteur | Modèles | Général**). Cela peut être utilisé pour faire sortir automatiquement les visiteurs lorsqu'ils quittent le bâtiment.

    Pour que cette action fonctionne, le filtre d'événement doit inclure les événements de l'utilisateur.
  - **Envoyer l'événement au MSMQ**: Transmet l'événement à une file d'attente à l'aide de Microsoft Message Queuing (MSMQ) qui peut ensuite être lue par des systèmes tiers.
  - **Envoyer un rapport récapitulatif par courriel**: Envoie un rapport récapitulatif à une adresse électronique spécifique. Cela peut être utilisé en cas d'incendie ou de verrouillage pour déterminer immédiatement quels utilisateurs sont sur le site au moment de l'urgence.
- **Filtre d'événement**: Ce filtre d'événement détermine les événements qui déclencheront l'action.

- **Commande PTZ** : Si le type est défini sur Envoyer commande PTZ, ce champ détermine la commande qui sera envoyée au DVR connecté.

  Les commandes PTZ peuvent être programmées dans **Surveillance | Configuration | Commandes PTZ** .
- **Fenêtre surgissante de la caméra** : Si le type est défini sur Fenêtre de la caméra surgissante, ce champ définit le flux de caméra utilisé par la fenêtre surgissante. Choisissez parmi :
  - Caméra par défaut associée avec l'événement
  - Caméra d'entrée de la porte
  - Caméra de sortie de la porte
  - Sélectionner la caméra à partir de la liste
- **Caméra** : Si l'option Sélectionner la caméra dans la liste est sélectionnée ci-dessus, définir la caméra spécifique qui sera affichée dans la fenêtre surgissante. Les caméras peuvent être programmées dans**Surveillance | Configuration | Caméras**.
- **Script**: Cette option est réservée pour un développement futur.

Paramètres de courriel

Ces paramètres sont disponibles lorsque le type est défini sur Envoyer courriel . Diverses variables de champ sont disponibles pour être utilisées avec l'action d'envoi de courriel, ce qui vous permet d'inclure des informations sur l'événement spécifique qui s'est produit (consultez page suivante).

Pour plus de renseignements et d'instructions de programmation, consulter la Note d'application 332 : Configuration des notifications d'événements dans Protege GX.

Les fonctions de courrier électronique automatisées dans Protege GX exigent qu'un serveur de courrier SMTP soit configuré dans **Global | Paramètres globaux | Paramètres de courrier électronique**.

- **Adresse courriel** : L'adresse ou les adresses auxquelles le courriel sera envoyé.

  Vous pouvez ajouter plusieurs adresses courriel dans ce champ, en les séparant par des points-virgules; toutefois, ce champ est limité à 128 caractères. Si plusieurs adresses sont nécessaires, créez une action en double.
- **Sujet**: Définit le sujet du courriel.
- **Message** : Définit le contenu du message du courriel.

Paramètres IP

Ces paramètres sont disponibles lorsque le type est défini sur Envoyer l'événement . Les événements seront envoyés au format XML.

- **Adresse IP** : L'adresse IP où les événements XML seront envoyés.
- **Port IP** : Le port vers lequel les événements XML seront envoyés.

Personnaliser Commande DVR

Ces paramètres sont disponibles lorsque le type est défini sur Personnaliser Action DVR .

- **DVR**: Le DVR auquel la commande sera envoyée. Les DVRs peuvent être programmés dans**Surveillance | Configuration | DVRs**.
- **Chaîne de commandes**: La chaîne qui sera envoyée au DVR. Cela sera déterminé par les exigences du système tiers.

MSMQ

Ces paramètres sont disponibles lorsque le type est défini sur Envoyer l'événement au MSMQ .

Pour plus de renseignements, voir la Note d'application 144 : Configuration de l'intégration MSMQ .

- **File des messages**: Le nom de la file des messages à laquelle les données de l'événement seront envoyées. Il est conseillé de donner à la file d'attente un nom en rapport avec son utilisation, par exemple "ALARMES".

Paramètres de messagerie (Rapport récapitulatif)

Ces paramètres sont disponibles lorsque le type est défini sur Envoyer rapport récapitulatif par courriel .

Les fonctions de courrier électronique automatisées dans Protege GX exigent qu'un serveur de courrier SMTP soit configuré dans **Global | Paramètres globaux | Paramètres de courrier électronique**.

- **Adresse courriel** : L'adresse ou les adresses auxquelles le courriel sera envoyé.

  Vous pouvez ajouter plusieurs adresses courriel dans ce champ, en les séparant par des points-virgules; toutefois, ce champ est limité à 128 caractères. Si plusieurs adresses sont nécessaires, créez une action en double.

- **Rapport récapitulatif** : Le rapport récapitulatif qui sera envoyé lorsque l'action est déclenchée. Les rapports récapitulatif peuvent être créés dans **Rapports | Configuration | Récapitulatif** .

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Variables de champ de courrier

Le type d'action d'envoi courriel prend en charge un certain nombre de variables de champ qui peuvent être saisies dans les champs **Objet** ou **Message**. Lors de l'envoi de courriel, chaque espace réservé sera remplacé par des informations spécifiques sur l'événement déclencheur.

Les variables de champ sont case sensible.

Variable de champ	Information
`<EVENTID>` ou `<EVENT_ID>`	L'ID de la base de données de l'événement enregistré.
`<FIELDTIME>` ou `<FIELD_TIME>`	L'heure du champ, ou l'heure à laquelle l'événement a été généré par le contrôleur.
`<LOGGEDTIME>` ou `<LOGGED_TIME>`	L'heure d'enregistrement, ou l'heure à laquelle l'événement a été enregistré par le serveur.
`<DESCRIPTION>`	La description ou le texte complet de l'événement tel qu'il apparaît dans le journal des événements.
`<DESCRIPTION2>`	La description de l'événement dans la deuxième langue.
`<DOORNAME>` ou `<DOOR_NAME>`	Le nom de la porte impliquée dans l'événement.
`<USERNAME>` ou `<USER_NAME>`	Le nom de l'utilisateur impliqué dans l'événement.
`<USERID>` ou `<USER_ID>`	L'ID de la base de données de l'utilisateur impliqué dans l'événement.
`<FACILITYNUMBER>` ou `<FACILITY_NUMBER>`	Le numéro d'installation de la carte d'identité de l'utilisateur concerné par l'événement.

Variable de champ	Information
<CARDNUMBER> ou <CARD_NUMBER>	Le numéro de carte de l'identifiant de l'utilisateur concerné par l'événement.
<ALARM>	Une valeur binaire qui indique si l'événement est classé comme une alarme. • **0** = L'événement n'est pas une alarme. • **1** = L'événement est une alarme.
<INSTRUCTIONS>	Le texte du champ **Instructions** pour les alarmes.
<INSTRUCTIONS2>	Texte du champ **Instructions 2** pour les alarmes (instructions dans la deuxième langue).
<ACKNOWLEDGED>	Une valeur binaire qui indique si l'événement a été reconnu. Ceci ne s'applique qu'aux alarmes. • **0** = L'alarme n'a pas été reconnue. • **1** = L'alarme a été reconnue.
<COMMENTS>	Le texte de tout commentaire fait par l'opérateur qui a reconnu l'alarme.

Priorités d'alarme

Les priorités d'alarme vous permettent de déterminer l'ordre dans lequel les alarmes sont affichées dans les fenêtres surgissantes d'alarme et d'événement. Les alarmes ayant une priorité plus élevée apparaîtront plus haut dans la liste.

Les priorités d'alarme peuvent également être utilisées dans le routage des alarmes afin de s'assurer que les alarmes de haute priorité sont redirigées vers d'autres postes de travail si elles ne sont pas reconnues.

Priorités d'alarme | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Priorité** Plus la priorité est élevée, plus l'alarme apparaîtra en haut de toute liste d'alarmes multiples.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Routage d'alarme

Les enregistrements de routage des alarmes définissent les groupes de poste de travail qui reçoivent les alarmes et dans quel ordre. Cela vous permet d'acheminer une alarme vers des postes de travail spécifiques plutôt que vers tous les postes de travail à la fois, et de transférer l'alarme à un autre poste de travail si elle n'est pas reconnue dans un délai défini.

Pour créer un enregistrement de routage d'alarme, vous devez d'abord configurer les postes de travail et les groupes de postes de travail. Les paramètres SIP n'ont pas besoin d'être programmés pour le poste de travail. Les enregistrements d'acheminement des alarmes peuvent être affectés à la **liste d'acheminement des alarmes** dans la programmation **Événements | Alarmes**.

Routage d'alarme | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Routage d'alarme | Groupes de poste de travail

Cet onglet répertorie les groupes de poste de travail qui sont disponibles pour le routage des alarmes.

- **Nom** : Le nom de chaque groupe de poste de travail. Ceux-ci peuvent être programmés dans **Événements | Groupes de poste de travail**.
- **Transférer après**: Définit la période (en secondes) pendant laquelle les alarmes attendront dans ce groupe de poste de travail avant d'être acheminées vers le groupe suivant dans la liste.
- **Priorité de transfert**: Sélectionner une priorité d'alarme qui sera utilisée pour ce groupe de poste de travail. Lorsqu'elle est définie, seules les alarmes ayant cette priorité seront acheminées vers le groupe. Les alarmes ayant toute autre priorité seront transférées au groupe de poste de travail suivant dans la liste. Si ce champ n'est pas défini, toutes les alarmes seront acheminées vers ce groupe de poste de travail.
- **Ordre du routage**: Définit la séquence dans laquelle les alarmes seront acheminées. Le groupe de poste de travail qui reçoit les alarmes en premier doit être réglé sur 1, le deuxième groupe sur 2, etc.
- **Actif** : Activer cette option pour inclure le groupe de poste de travail dans la liste de routage.

Stations de travail

Les stations de travail identifient des Protege GX ordinateurs clients spécifiques sur le réseau. Il n'est pas nécessaire de programmer un enregistrement de poste de travail pour exécuter le clientProtege GX, mais ils sont utilisés pour certaines applications spécifiques :

- Les enregistrements des stations de travail sont utilisés dans les groupes de stations de travail et le routage des alarmes pour envoyer des alarmes aux stations de travail définies (voir **Événements | Routage des alarmes**).
- Les stations de travail sont également utilisées pour configurer Protege GX en tant que client SIP, ce qui permet aux opérateurs de tenir des appels avec un interphone directement dans l'interface Protege GX en utilisant la VoIP.

  La fonction VoIP fait l'objet d'une licence distincte. Une licence est nécessaire pour chaque interphone connecté et les enregistrements d'interphones doivent être programmés dans **Surveillance | Configuration | Interphones** . Pour plus d'informations, voir la note d'application 339 : Intégration des interphones SIP avec les Protege GX stations de travail .
- L'intégration de Cencon exige que chaque boîte à clés soit affectée à une station de travail.

  Pour plus d'informations, voirla note d'application 160 : Configuration de l'intégration de Cencon avec Protege GX.

Stations de travail | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Nom de l'ordinateur** : Le nom de l'ordinateur client Protege GX sur le réseau. Il doit être unique.

Client SIP

Certains paramètres ne peuvent être configurés que sur la station de travail que vous utilisez actuellement. Chaque station de travail doit également être enregistrée avec une extension dans le serveur SIP.

- **Adresse du serveur** : Le nom de domaine ou l'adresse IP du serveur SIP.
- **Nom du compte** : Le nom de l'extension SIP qui a été attribuée sur le système PBX SIP pour cette station de travail.
- **Mot de passe du compte** : Le mot de passe de l'extension SIP qui a été attribuée sur le système PBX SIP pour cette station de travail.
- **Domaine** : Le domaine de sécurité sous lequel ce compte est valide. Par exemple, pour un serveur PBX basé sur Asterisk, vous devez saisir Asterisk , tandis que pour un serveur 3CX, vous devez saisir 3CXPhoneSystem.
- **Port SIP** : Le port UDP qui sera utilisé pour les communications avec le serveur SIP PBX.
- **Interface réseau** : La carte d'interface réseau utilisée pour les communications.
- **Microphone** : Le microphone qui est connecté à la station de travail. Un microphone doit être connecté pour que la station de travail s'enregistre en tant que client SIP.
- **Réglage par défaut du microphone** : Définit le niveau du microphone qui sera utilisé lorsque la fenêtre d'appel est lancée.
- **Haut-parleurs** : Les haut-parleurs qui sont connectés à la station de travail.

- **Paramètres haut-parleur par défaut** : Définit le niveau du haut-parleur qui sera utilisé lorsque la fenêtre d'appel est lancée.

Boîte de clés Cencon

Pour plus d'informations sur l'intégration de Cencon, voir la note d'application 160 : Configuration de l'intégration de Cencon avec Protege GX.

- **ID de la boîte à clés** : Chaque boîte à clés Cencon doit être affectée à un Protege GX poste de travail client.

  Avant d'essayer d'affecter une boîte à clés à un poste de travail, assurez-vous que la boîte à clés est connectée au poste de travail par USB et qu'elle est visible dans la liste du client Centran Configuration Manager.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Groupes de stations de travail

Les groupes de stations de travail sont utilisés pour définir les stations de travail qui recevront les alarmes et dans quel ordre. Pour plus d'informations, consultez la section Routage d'alarme (la page 151).

Groupes de stations de travail | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Groupes de stations de travail | Stations de travail

Cet onglet affiche une liste des stations de travail programmées. Activez la case à cocher **Actif** pour inclure les stations de travail nécessaires dans le groupe de stations de travail.

Menu Rapports

Utilisez le menu des rapports pour créer et visualiser une série de rapports. Grâce aux options de rapport flexibles de Protege GX, vous pouvez facilement obtenir des informations détaillées et pertinentes selon vos besoins. Tous les rapports peuvent être filtrés, regroupés et triés, puis imprimés, envoyés par courriel ou exportés vers divers formats de fichiers.

Les rapports suivants sont disponibles dans Protege GX :

- Registres d'événements
- Rapports Muster (licence requise)
- Rapports de présence (licence requise)
- Rapports de l'utilisateur
- Rapports de la station centrale (génère une carte de rapport à l'usage des stations de surveillance)
- Rapports d'autorisation des opérateurs

Paramétrage des rapports

Vous pouvez créer et enregistrer des rapports d'événements, de rassemblement, de présence et d'utilisateurs dans le menu **Rapports | Configuration**. Chaque type de rapport dispose d'une variété d'options qui vous permettent de trouver les informations dont vous avez besoin. En outre, il est possible de configurer des exportations régulières de fichiers ou des courriels de configurations de rapports sauvegardés.

Rapports | Configuration | Événement

Les rapports d'événements vous permettent de visualiser facilement ce qui s'est passé ou se passe actuellement dans le système. Utiliser des filtres d'événements (**Événement | Filtres d'événements**) et des groupes d'enregistrements pour vous assurer que seuls les événements pertinents sont inclus dans chaque rapport.

Par défaut, il existe trois rapports d'événements préconfigurés :

- Tous les événements
- Toutes les alarmes
- Toutes les alarmes reconnues

D'autres peuvent être créés si nécessaire. Une fois qu'un enregistrement de rapport d'événement a été créé, il peut être exécuté comme un rapport, permettant aux résultats d'être examinés, regroupés et exportés selon les besoins. Vous pouvez également inclure un rapport d'événement sur une page d'état ou un plan d'étage, ce qui permet de visualiser en direct les événements survenus dans le système.

Registres d'événements | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.
- **Titre** : Le titre du rapport sera affiché en tant qu'en-tête sur les fichiers imprimés et exportés.

Configuration

- **Afficher**: Champ en lecture seulement qui indique la description qui est affichée dans la fenêtre du rapport d'événement.
- **Alarmes**: Définit les types d'événements à inclure dans le rapport d'événements. Choisissez si vous voulez inclure tous les événements, toutes les alarmes ou seulement les alarmes reconnues.

  Les rapports d'événements avec alarmes peuvent être intégrés à une page de statut et utilisés pour accuser réception des alarmes actives.
- **Nombre d'événements**: Définit le nombre maximum d'événements à inclure, ce qui vous permet de limiter le nombre d'événements qui seront inclus dans les résultats.

Filtres d'événements

Cliquez sur **Ajouter** pour sélectionner un ou plusieurs filtres d'événements. Les options suivantes sont disponibles dans la fenêtre contextuelle :

- **Filtre d'événement**: Le filtre d'événement qui sera utilisé pour filtrer les résultats du rapport d'événement. Les filtres d'événements peuvent être programmés dans **Événements | Filtres d'événements**.
- **Accéder à tous les groupes d'enregistrement**: Le filtre d'événements inclura les dossiers de tous les groupes d'enregistrements. Autrement, sélectionner un ou plusieurs groupes d'enregistrements à appliquer au filtre.

Filtre par défaut des rapports d'événements

Si une mise en page de rapport par défaut a été créée pour ce rapport, vous pouvez voir les filtres enregistrés ici. Pour plus d'informations, consultez la section Sauvegarder les mises en page des rapports (la page 174).

- **Modifier dans la vue du rapport** : En cliquant sur ce bouton, le rapport d'événement est ouvert dans une fenêtre de dépannage, ce qui vous permet d'exécuter le rapport, de configurer des filtres et de sauvegarder la mise en page par défaut du rapport.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Registres d'événements | Colonnes

Cet onglet vous permet de définir les colonnes qui apparaîtront dans le rapport. Presque tous les champs du système peuvent être inclus dans un rapport d'événement, ce qui permet aux opérateurs de créer des rapports hautement personnalisés avec des options infinies de regroupement et de filtrage.

Pour ajouter une colonne à un rapport d'événement, cliquez sur **Ajouter**. Sélectionnez le **Tableau** (par. exemple., niveaux d'accès, portes) et **Onglet** (par exemple, Général, Options) pour afficher les champs disponibles pour cet onglet particulier.

Colonnes

- **Type d'enregistrement** : Le type d'enregistrement d'où provient la colonne/le champ.
- **Nom** : Le nom anglais du champ dans le logiciel.
- **Nom de la deuxième langue** : Le nom de la deuxième langue du champ dans le logiciel.
- **Nom personnalisé** : L'opérateur peut définir un autre Nom anglais pour le champ. Celle-ci apparaîtra dans l'en-tête de colonne du rapport.
- **Nom de langue seconde personnalisé** : L'opérateur peut définir un autre seconde langue pour le champ. Cela apparaîtra dans l'en-tête de colonne du rapport lorsqu'il sera exécuté dans la seconde langue installée avec le logiciel.

  Les noms personnalisés ne sont pas traduits automatiquement. Les traductions doivent être ajoutées manuellement.

Rapports | Configuration | Rassemblement

Les rapports de rassemblement vous permettent de savoir quels utilisateurs se trouvent actuellement dans une salle, un bâtiment ou sur un site. En contrôlant les portes extérieures (d'entrée et de sortie) d'une zone spécifique, le rapport de rassemblement peut générer une liste de tous les utilisateurs qui ont été actifs pendant une période donnée et indiquer s'ils se trouvent actuellement à l'intérieur ou à l'extérieur de cette zone.

Outre l'exécution manuelle du rapport de rassemblement, vous pouvez également l'inclure dans une page du statut, fournissant ainsi des informations régulièrement mises à jour sur le statut des utilisateurs dans le système.

Les rapports de rassemblement sont particulièrement utiles dans les situations d'urgence où il est vital de savoir exactement quel personnel se trouve sur place. Vous pouvez configurer une action pour envoyer automatiquement par courriel des rapports de rassemblement à la suite d'événements spécifiques, comme l'activation d'une alarme incendie (consultez la page 146).

Les rapports de rassemblement sont une fonction sous licence séparée.

RassemblerRapports | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

Configuration

- **Période**: La période de temps qui sera incluse dans le rapport de rassemblement. Par exemple, en fixant la période à 8 h, on obtient des données sur le dernier accès à la porte de chaque utilisateur au cours des 8 h précédentes.
- **Type de rapport**: Les types de rapport de rassemblement suivants sont disponibles :
  - **Normal**: Les utilisateurs qui n'ont pas été actifs pendant la **période** sélectionnée seront exclus du rapport.
  - **Détail / liste**: Les utilisateurs qui n'ont pas été actifs au cours de la **période** sélectionnée seront inclus dans le rapport avec un statut « Inconnu ». Il n'y a pas de différence entre les options de détail et de liste.
- **Taux d'actualisation**: La fréquence à laquelle les données du rapport seront mises à jour lorsque le rapport de rassemblement est affiché sur une page d'état. Contrairement aux rapports d'événements, les rapports de rassemblement ne fournissent pas une liste « en direct » des événements, mais sont mis à jour toutes les 5 ou 30 min.

  Le lancement actif d'un rapport fournira toujours les informations les plus récentes.
- **Fuseau horaire**: Détermine le fuseau horaire que le rapport utilisera pour calculer la période d'activité. Cette heure doit correspondre à l'heure du contrôleur (champ) pour que les données correctes soient incluses dans le rapport. L'option Utiliser le fuseau horaire du serveur utilise le fuseau horaire actuel du serveur Protege GX.

  Par exemple, le contrôleur peut être situé à l'heure normale de l'Est (HNE) tandis que le serveur est à l'heure normale du Pacifique (HNP). L'opérateur lance un rapport à 15 h 15 HNP, ce qui équivaut à 18 h 15 HNE. Si le **fuseau horaire** du rapport est défini sur HNP et que la **période** est définie sur 30 min, les données du rapport commenceront à 17 h 45 (heure du champ) au lieu de 14 h 45 (heure du serveur).

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

RassemblerRapports | Portes

Dans cet onglet, vous pouvez définir les portes d'entrée et de sortie (ou points de passage obligés) sur lesquelles le rapport de rassemblement portera. Par exemple, pour générer un rapport sur tous les utilisateurs qui se trouvent actuellement à l'intérieur d'un bâtiment spécifique, vous devez suivre l'accès à toutes les portes extérieures.

Portes

Cliquez sur **Ajouter** pour ouvrir la fenêtre de sélection et choisir les portes à inclure.

- **Nom**: Le nom de la porte pour laquelle le rapport d'appel est destiné
- **Trajectoire**: Détermine les types d'accès qui seront utilisés pour suivre l'emplacement de l'utilisateur.
  - **Les deux**: L'accès d'entrée et de sortie sera suivi pour ce porte. Il doit être utilisé pour les portes du périmètre extérieur qui servent à la fois de points d'entrée et de sortie. Lorsqu'un utilisateur franchit une porte, il est identifié comme étant sur place (son **statut** est réglé sur dedans). Lorsqu'ils sortent par une porte, ils sont identifiés comme étant hors site (leur **statut** est réglé sur dehors).
  - **Entrée**: Seule l'entrée sera suivie pour ce porte. Elle doit être utilisée pour les portes intérieures. Lorsqu'un utilisateur sort par un porte interne, il se trouve toujours sur le site, dans une autre zone, et son **statut** reste réglé sur dedans.
  - **Sortir**: Seule la sortie sera suivie pour ce porte. Cette option doit être utilisée pour les points d'accès externes qui ne sont utilisés que comme sorties. Lorsqu'un utilisateur sort de l'une de ces portes, son **Statut** est défini comme dehors.

RassemblerRapports | Colonnes

Cet onglet vous permet de définir les colonnes qui apparaîtront dans le rapport. Mise à part les colonnes par défaut du rapport d'appel, les rapports d'appel peuvent également comprendre une série de champs utilisateur et tout autre champ personnalisé, permettant aux opérateurs de créer des rapports personnalisés avec des options supplémentaires de regroupement et de filtrage.

Pour ajouter une colonne à un rapport de rassemblement, cliquez sur **Ajouter**. Sélectionnez le **tableau** (par exemple, utilisateurs) et **Onglet** (par exemple, Général, Options) pour afficher les champs disponibles pour cet onglet particulier.

Les rapports de rassemblement affichés sur les pages du statut ne comprendront que les colonnes par défaut.

Colonnes

- **Type d'enregistrement** : Le type d'enregistrement d'où provient la colonne/le champ.
- **Nom** : Le nom anglais du champ dans le logiciel.
- **Nom de la deuxième langue** : Le nom de la deuxième langue du champ dans le logiciel.
- **Nom personnalisé** : L'opérateur peut définir un autre Nom anglais pour le champ. Celle-ci apparaîtra dans l'en-tête de colonne du rapport.
- **Nom de langue seconde personnalisé** : L'opérateur peut définir un autre seconde langue pour le champ. Cela apparaîtra dans l'en-tête de colonne du rapport lorsqu'il sera exécuté dans la seconde langue installée avec le logiciel.

  Les noms personnalisés ne sont pas traduits automatiquement. Les traductions doivent être ajoutées manuellement.

Rapports | Configuration | Présence

Les fiches de présence permettent de suivre facilement les mouvements des utilisateurs, ce qui facilite la gestion des salaires et des ressources humaines. En utilisant les informations d'entrée et de sortie qui sont déjà enregistrées dans le cadre du fonctionnement normal de l'opération Protege GX les rapports de présence peuvent suivre l'absentéisme des employés, contrôler les heures de début, de fin et de pause, et comptabiliser les heures supplémentaires.

Les rapports de présence sont une fonctionnalité sous licence séparée. Pour plus d'informations, voir la Note d'application 3080: Temps et présence en Protege GX. Pour un exemple de programmation, voir la Note d'application 163 : Configuration des rapports d'équipe dans Protege GX.

Rapports de présences | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.
- **Source de l'utilisateur**: Détermine de quelle manière le rapport sélectionne les utilisateurs à inclure. Choisissez parmi :
  - **Liste d'utilisateurs** : Le rapport inclut tous les utilisateurs sélectionnés individuellement dans l'onglet **Utilisateurs**.
  - **Niveau d'accès** : Le rapport inclura les utilisateurs ayant un ou plusieurs niveaux d'accès sélectionnés dans l'onglet **Niveaux d'accès**.
  - **Groupe de registres** : Le rapport comprendra tous les utilisateurs inclus dans la sélection **Groupe de registres de l'utilisateur**.
- **Groupe d'enregistrement de l'utilisateur**: Si la **Source de l'utilisateur** est définie sur Groupe d'enregistrements, le rapport comprendra tous les utilisateurs de ce groupe d'enregistrements.
- **Type de rapport**: Définit le type de données de présence que le rapport produira. Choisissez parmi :
  - **Premier entré, dernier sorti** quotidien : Le rapport utilise le premier événement d'entrée et le dernier événement de sortie de chaque jour pour déterminer la présence de l'utilisateur et les heures travaillées. Tout événement entre ces deux moments est ignoré, ce qui signifie que tout temps passé hors du site pendant la journée n'est pas déduit.
  - **Equipe première entrée dernière sortie** : Le rapport utilise le premier événement d'entrée et le dernier événement de sortie chaque jour, ainsi que tout événement d'entrée/sortie supplémentaire pendant la journée. Protege GX il compare ensuite les différents événements d'entrée/sortie aux heures de travail et de pause définies pour calculer les heures travaillées.
  - **Premier et dernier événement quotidiens de l'utilisateur** : Le rapport utilise le premier et le dernier événement utilisateur de chaque jour pour déterminer la présence et les heures travaillées. Tout événement entre ces deux moments est ignoré, de sorte que tout temps passé hors site pendant la journée n'est pas déduit.
  - **Premier et dernier événement de l'utilisateur du quart de travail** : Le rapport utilisera le premier et le dernier événement utilisateur chaque jour, ainsi que tout événement supplémentaire au cours de la journée. Protege GX il compare ensuite les différents événements d'entrée/sortie aux heures de travail et de pause définies pour calculer les heures travaillées.

- **Premier scan d'entrée** : Le rapport indique la première entrée de chaque utilisateur pour chaque jour.
- **Dernier scan de sortie** : Le rapport indiquera le dernier événement de sortie pour chaque utilisateur chaque jour.
- **Premier scan d'entrée et dernier scan de sortie** : Le rapport indique l'événement d'entrée le plus précoce et l'événement de sortie le plus tardif pour chaque utilisateur, chaque jour.
- **Entrée en retard** : Le rapport indique l'heure de la première entrée de chaque utilisateur pour les jours où l'utilisateur est arrivé en retard.

  Ce nom est calculé après que la **Période de grâce** ait été appliquée.
- **Les 10 premiers entrés en retard** : Le rapport montrera les 10 utilisateurs avec le plus grand nombre d'entrées tardives dans la période sélectionnée.
- **Sortie en retard** : Le rapport indique l'heure de la dernière sortie de chaque utilisateur pour les jours où l'utilisateur est sorti en retard.

  Ce nom est calculé après que la **Période de grâce** ait été appliquée.
- **Entrée précoce** : Le rapport indique l'heure de la première entrée de chaque utilisateur pour les jours où l'utilisateur est entré tôt.

  Ce nom est calculé après que la **Période de grâce** ait été appliquée.
- **Sortie précoce** : Le rapport indiquera l'heure de la dernière sortie de chaque utilisateur pour les jours où l'utilisateur est sorti tôt.

  Ce nom est calculé après que la **Période de grâce** ait été appliquée.
- **Absent** : Le rapport montrera les utilisateurs sans données d'entrée de temps pour tous les jours couverts par le rapport.
- **Les 10 premiers absents** : Le rapport affichera les 10 utilisateurs ayant le plus grand nombre de jours d'absence pendant la période sélectionnée.

- **Fuseau horaire**: Détermine le fuseau horaire que le rapport utilisera pour calculer la période pertinente. Cette heure doit correspondre à l'heure du contrôleur (champ) pour que les données correctes soient incluses dans le rapport. L'option Utiliser le fuseau horaire du serveur utilise le fuseau horaire actuel du serveur Protege GX.

  Par exemple, le contrôleur peut être situé aux États-Unis, tandis que le serveur est situé en Australie. Le matin du 29 avril en Australie, c'est le soir du 28 Avril aux États-Unis. Si le fuseau horaire du rapport est correctement réglé, lorsque l'opérateur exécute un rapport pour le jour précédent, il génère des données pour le 27 avril (heure du champ) au lieu du 28 avril (heure du serveur).
- **Jours de travail non programmés (à l'exception des jours fériés)** : Lorsque cette option est activée le rapport n'affiche que les entrées pour les jours où les utilisateurs ont travaillé en dehors des horaires configurés (voir l'onglet **Horaires de**travail). Les heures de travail des jours fériés sont exclues. Cela vous permet de calculer les heures supplémentaires effectuées les fins de semaine ou autres jours de congés.

  Cette option ne fonctionne correctement que lorsque le **Type d'équipe** (onglet **Horaires d'équipe**) est défini sur Horaire hebdomadaire (c'est-à-dire fixe). (c'est-à-dire fixe). Des résultats inattendus peuvent être générés lorsque le **Type d'équipe** est défini sur Rotation.
- **Jours de travail fériés**: Lorsque cette option est activée, le rapport n'affiche que les entrées pour les jours où les utilisateurs ont travaillé pendant les jours fériés (voir l'onglet **Jours** fériés). Cela vous permet de calculer les éventuelles heures supplémentaires effectuées les jours fériés.

  Cette option ne fonctionne correctement que lorsque le **Type d'équipe** (onglet **Horaires d'équipe**) est défini sur Horaire hebdomadaire (c'est-à-dire fixe). (c'est-à-dire fixe). Des résultats inattendus peuvent être générés lorsque le **Type d'équipe** est défini sur Rotation.
- **Modèle d'impression de rapport**: Ce champ définit le niveau de détail qui sera intégré au rapport, ainsi que les types de détails qui sont requis. Choisissez parmi :

- **Résumé** : Le rapport affiche un résumé des présences quotidiennes pour chaque utilisateur.
- **Détail** : Le rapport affiche une répartition détaillée des présences pour chaque utilisateur chaque jour, y compris les heures de début, de pause et de fin, ainsi que les calculs d'entrée et de sortie correspondants pour chaque événement. Ce modèle permet également l'ajout de champs personnalisés étendus dans l'onglet **Champs de l'utilisateur**.
- **Sommaire ICT** : Le rapport est généré dans un format CSV qui fournit un résumé de la présence de chaque utilisateur et inclut leur code d'employé et leur code de paie, pour faciliter la génération de la paie. Ce modèle permet également l'ajout de champs d'utilisateur personnalisés étendus dans l'onglet **Champs d'utilisateur**.
- **Sommaire MYOB** : Ce rapport est généré dans un format CSV qui peut être lu directement dans le programme MYOB. Il fournit un résumé de la présence de chaque utilisateur et comprend des champs pour le code de l'employé et le code de paie pour faciliter la génération de la paie, ainsi que des champs pour le département et le centre de coût pour le suivi des coûts salariaux.
  - Le **Code employé** est défini dans l'onglet **Champs utilisateur**.
  - Le **Code de rémunération** est défini dans le champ **Code de rémunération normale** de l'onglet **Général**.
  - Les colonnes **Département** et **Centre de coût** fournissent des champs dans le fichier CSV qui peuvent être remplis manuellement avec les détails de MYOB.
- **Action HRM** : Le rapport est généré dans un format CSV qui peut être lu directement dans le programme ActionHRM. Il fournit un résumé de la présence de chaque utilisateur, y compris les heures d'entrée et de sortie et le nombre total d'heures travaillées.

Pour certaines options de **Type de rapport**, seul le modèle d'impression Sommaire est disponible.

- **Période de grâce**: Ce champ définit le temps (en heures et minutes) pendant lequel un utilisateur peut être en retard ou en avance avant de subir une retenue de temps. Cela permet d'éviter que les employés ne soient inutilement pénalisés pour ne pas avoir pointé à l'heure exacte.

  Par exemple, si le délai de grâce est fixé à 5 min et qu'un utilisateur fait usage de son badge avec 3 min de retard, le temps ne sera pas déduit du total des heures de travail. Cependant, si l'utilisateur a 10 min de retard, la totalité des 10 min lui sera déduite.
- **Code de rémunération normale**: Ce champ spécifie la colonne **Code de rémunération** utilisée dans les modèles d'impression des rapports Sommaire ICT et Sommaire MYOB

Période

- **Période**: La période de temps couverte par le rapport. Choisir parmi le jour, la semaine, deux semaines ou quatre semaines précédentes, ou sélectionnez Période personnalisée pour définir une date de début et de fin spécifique.
- **Démarrage**: Détermine le jour de la semaine à partir duquel le rapport commencera. Par exemple, un rapport avec une **période** de semaine précédente commençant le lundi affichera les données de 00:00 le lundi à 23:59 le dimanche.
- **Date de début**: Si le champ **période** est défini sur période personnalisée, ce champ détermine la date de début du rapport de présence.
- **Date d'expiration**: Si la **période** est définie sur période personnalisée, ce champ détermine la date à laquelle le rapport de présence se termine.
- **Demande la date**: Au lieu d'utiliser la période définie dans les champs ci-dessus Protege GX invitera l'opérateur à saisir une période chaque fois que le rapport est exécuté.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Rapports de présences | Changer Temps

Type de quart de travail

- **Type de quart de travail**: Il existe deux options pour définir les équipes dans un rapport de présence : Hebdomadaire ou par rotation. L'option hebdomadaire est utilisée pour les quarts réguliers et répétitifs qui ne se déroulent pas pendant la nuit. L'option de rotation vous permet de configurer des équipes rotatives, des équipes multiples par jour et des équipes de nuit.
- **Durée de la rotation**: Le nombre de jours de rotation des équipes. Par exemple, un hôpital peut affecter des équipes sur un cycle de 10 jours.
- **Date de début de rotation**: La date à laquelle la rotation commencera.

Détails du quart de travail

Si le **type de quart de travail** est défini sur Semaine, cette section vous permet de définir les jours de la semaine qui seront inclus dans le quart de travail, ainsi que les **heures de début** et **heures de fin** pour chaque jour.

Si le **type de quart de travail** est défini sur rotation, cette section vous permet de configurer et de vérifier les équipes qui se produiront sur tels jours de la rotation. Pour créer une rotation :

1. Créer tous les types de quart de travail requis dans **Rapports | Configuration | Type de quart de travail**.
2. Définir la **durée de la rotation** et **la date de début de la rotation** comme ci-dessus. Le mini calendrier au bas de la page de programmation affichera un seul cycle de la rotation à partir de la date du début.
3. **Ajouter** les types de quart de travail requis à la liste. Les quarts de travail peuvent être inclus un nombre illimité de fois dans une rotation.

   Si nécessaire, vous pouvez créer d'autres types de quart de travail en cliquant sur **Ajouter**, puis **Créer un type de quart de travail**.
4. Utiliser la liste défilante pour sélectionner le premier type de quart de travail.
5. Dans le mini calendrier, cliquer sur chaque date qui comprend ce type de quart de travail spécifique. Les jours où le quart de travail ont lieu, seront marqués de la couleur du type de quart de travail.

   Si vous devez supprimer un type de quart de travail d'un jour, réglez la liste déroulante sur **Aucun quart de travail** et cliquer sur ce jour.
6. **Sauvegarder** l'enregistrement, puis cliquer sur **Visualisation du calendrier** pour voir quand le changement aura lieu sur un calendrier annuel.
7. Répéter ce qui précède pour les autres types de quart de travail.

Rapports de présences | Temps pause

Lorsque le **Type d'équipe** (**l'onglet** Horaires d'équipe) est défini sur Semaine cet onglet vous permet de définir les pauses programmées qui auront lieu chaque jour. Ils seront utilisés avec certains paramètres de **Type de rapport**.

Vous pouvez saisir jusqu'à 6 pauses pour chaque jour. Cocher la case à côté de chaque pause pour activer cette pause pour chaque jour du programme hebdomadaire.

- **Nom** : Un nom pour la pause, par ex. Thé du matin'.
- **Début/Fin** : Les heures de début et de fin de la pause. Elles définissent la plage de temps pendant laquelle l'employé est autorisé à prendre sa pause. Par exemple, les employés peuvent avoir droit à 30 minutes pour le déjeuner, qui peut être pris à tout moment entre 12h00 et 14h00.
- **Durée** : La durée de la pause en minutes. Ceci sera utilisé pour calculer les heures de travail de l'employé et les déductions d'heures.

  La durée de la pause doit être plus courte que l'espace entre les heures de début et de fin. Par exemple, pour une pause de 10 minutes commençant à 10h30, l'heure de fin devrait être au moins 10h41 pour permettre la durée totale de la pause.

- **Calcul** : Détermine comment l'heure de pause sera utilisée dans les calculs de présence. Exclure déduit la durée de la pause des heures de travail, la pause n'est donc pas rémunérée. Inclure ne permet pas de déduire la pause.

Rapports de présences | Utilisateurs / Niveaux d'accès

Si la **Source de l'utilisateur** (dans **l'onglet** Général) est définie sur Liste d'utilisateurs, vous pouvez ajouter à l'onglet **Utilisateurs** les utilisateurs spécifiques qui seront inclus dans ce rapport.

Si la **Source de l'utilisateur** est définie sur Niveau d'accès, vous pouvez ajouter dans l'onglet **Niveaux d'accès** les niveaux d'accès qui seront inclus dans ce rapport.

Rapports de présences | Portes permises

Cet onglet vous permet de définir les portes qui seront utilisées pour générer les données de présence. Lorsqu'un utilisateur passe une porte, il sera compté comme étant sur place ou pointé. Lorsqu'un utilisateur sort d'une porte, il sera compté comme hors site ou ayant pointé son départ. Il convient donc d'utiliser généralement les portes extérieures d'un site, d'un bloc ou d'un espace de travail.

- **Portes**: Cliquer sur **Ajouter** pour sélectionner les portes qui seront utilisées pour déterminer quand les employés travaillent. Ces portes peuvent être utilisées pour pointer à l'entrée et à la sortie d'une équipe ou d'une pause. Par exemple, si vous créez un rapport de présence pour le personnel des entrepôts, vous devez vous assurer que vous suivez les portes d'entrée et de sortie de l'entrepôt.
- **Trajectoire**: Définissez la trajectoire qui sera suivie pour chaque porte :
  - **Les deux**: À utiliser pour les portes qui servent à la fois de point d'entrée et de point de sortie.
  - **Entrée**: À utiliser pour les points d'accès qui ne sont utilisés que pour le pointage. Ce système peut être utilisé pour les portes intérieures, afin de permettre aux utilisateurs de pointer lorsqu'ils sont déjà à l'intérieur du bâtiment.
  - **Sortir**: À utiliser pour les points d'accès qui ne sont utilisés que pour le pointage.

Rapports de présences | Champs d'utilisateurs

Les champs personnalisés de l'utilisateur et les champs élargis peuvent être inclus dans les rapports détaillés afin de fournir les données requises par les opérateurs ou les systèmes de RH/feuilles de paye.

Cet onglet n'est disponible que pour certains **types de rapport** (**onglet**Général). Pour faire apparaître l'onglet **élargi** dans la programmation utilisateur, activez l'option **Afficher les champs personnalisés prédéfinis dans les utilisateurs** dans **Global | Sites | Affichage**.

Champs d'utilisateur transférés par défaut

- **Code d'employé**: Les modèles d'impression des sommaires MYOB et sommaire ICT (**Onglet**Général) identifient les utilisateurs par un code d'employé unique. Ce champ vous permet de définir le code de l'employé pour n'importe quel champ d'utilisateur élargi (par exemple, le numéro de licence, le champ personnalisé 1).

Champs d'utilisateur supplémentaires exportés

Pour ajouter des champs étendus ou personnalisés supplémentaires au rapport de présence, cliquer sur **Ajouter** et sélectionner les champs appropriés.

Rapports de présences | Jours fériés

Cet onglet vous permet d'ajouter des jours fériés au rapport de présence. Les jours fériés ne seront pas pris en compte dans le calcul de la présence, de sorte que les employés ne seront pas sanctionnés s'ils ne se présentent pas au travail un jour férié.

Vous pouvez également utiliser l'option **Jours de travail fériés** (onglet **Général**) pour générer un rapport qui inclut uniquement les quarts de travail effectués les jours fériés, ce qui vous permet de calculer la rémunération des jours fériés.

Jours fériés

- **Nom** : Le nom du jour férié.
- **Répéter** : Lorsque cette option est activée, le jour férié se répète sur une base annuelle.

  Gardez à l'esprit que certains jours fériés se répètent le même jour chaque année (par exemple, Noël), tandis que d'autres se produisent à des jours différents (par exemple, Pâques). Il est utile de programmer les jours fériés plusieurs années à l'avance.

- **Date de début** : Le premier jour du jour férié.
- **Date de fin** : Le dernier jour des congés.

  Pour créer un congé d'un jour, sélectionnez la même date de fin que la date de début. Par exemple, pour créer un congé de 24 heures pour le jour de l'an, vous devez régler à la fois la date de début et de fin sur le 1er janvier.

Rapports | Configuration | Utilisateur

Les rapports sur les utilisateurs contiennent des informations détaillées sur les utilisateurs de votre système. Vous pouvez rapidement générer des données pertinentes telles que, les utilisateurs qui ont accès à certaines portes, qui ont déclenché des événements définis ou dont les cartes arrivent à expiration.

Rapports de l'utilisateur | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

Type de rapport

- **Type de rapport**: Les types de rapports suivants sont disponibles pour les rapports de l'utilisateur. Des colonnes supplémentaires peuvent être ajoutées à tout type de rapport dans l'onglet **Colonnes**.
  - **Tous les utilisateurs** : Tous les utilisateurs actuellement programmés dans ce site.
  - **Tous les utilisateurs qui ont accès aux portes sélectionnées** : Tous les utilisateurs ayant des niveaux d'accès qui donnent accès aux portes sélectionnées.
  - **Tous les utilisateurs inclus dans les niveaux d'accès suivants** : Tous les utilisateurs auxquels sont attribués les niveaux d'accès sélectionnés.
  - **Tous les utilisateurs par événements** : Tous les enregistrements d'utilisateurs inclus dans les événements du filtre d'événements sélectionné, pendant la période spécifiée.
  - **Tous les utilisateurs par groupe de registres** : Tous les utilisateurs du groupe de registres sélectionné.
  - **Utilisateurs par type/portes d'événements** : Tous les utilisateurs qui ont déclenché des événements aux portes sélectionnées pendant la période de temps spécifiée.
  - **Cartes à veille d'expirer** : Tous les enregistrements d'utilisateurs dont l'expiration est prévue dans la période sélectionnée.
  - **Derniers utilisateurs à travers le(s) porte(s)** : Les derniers utilisateurs (et l'heure d'accès) qui ont accédé à la (aux) porte(s) sélectionnée(s).
  - **Tous les utilisateurs ne participant pas aux événements** : Tous les utilisateurs non inclus dans les événements du filtre d'événements sélectionné, au cours de la période spécifiée.
  - **Tous les visiteurs actuels** : Tous les visiteurs actuellement connectés (nécessite un système de gestion de visiteurs).
  - **Tous les visiteurs en attente** : Tous les visiteurs encore connectés après l'heure de fermeture prévue (nécessite un système de gestion de visiteurs).
  - **Tous les visiteurs par date** : Tous les visiteurs qui se sont connectés au cours d'une période spécifique (nécessite un système de gestion de visiteurs).
  - **Enregistrer l'historique modifié**: Tous les enregistrements d'utilisateur qui ont été modifiés au cours de la période sélectionnée, regroupés par utilisateur. Il comprend les paramètres qui ont été modifiés, les anciennes et nouvelles valeurs et l'opérateur.
  - **Tous les utilisateurs par niveaux d'accès** : Les utilisateurs ayant les niveaux d'accès spécifiés, regroupés par niveau d'accès. Les délais d'expiration des niveaux d'accès sont affichés. Les utilisateurs qui ont été désactivés ou dont le niveau d'accès a expiré ne sont pas inclus.

- **Tous les niveaux d'accès par utilisateurs** : Les utilisateurs ayant les niveaux d'accès spécifiés, regroupés par utilisateur. Les délais d'expiration des niveaux d'accès sont affichés. Les utilisateurs qui ont été désactivés ou dont le niveau d'accès a expiré ne sont pas inclus.

- **Titre** : Le titre du rapport sera affiché en tant qu'en-tête sur les fichiers imprimés et exportés.

Tri

Les critères de tri définis ici seront mis en œuvre automatiquement dans un rapport transféré, mais peuvent être remplacés lorsque le rapport est exécuté manuellement.

- **Colonne de tri**: Détermine la colonne dans laquelle les résultats seront triés.
- **Sens du tri**: Détermine si les données renvoyées sont triées par ordre croissant ou décroissant.
- **Regroupement par**: Regroupe les données renvoyées par la colonne définie.

Filtres de rapports spécifiques

Des options supplémentaires sont affichées en fonction du **type de rapport** sélectionné. Vous pouvez peut-être préciser un ou plusieurs des éléments suivants :

- Portes
- Niveaux d'accès
- Groupes de registres
- Période de temps
- Filtres d'événements
- Types d'événements
- Période d'expiration des enregistrements des utilisateurs

Filtre de rapport utilisateur par défaut

Si une mise en page de rapport par défaut a été créée pour ce rapport, vous pouvez afficher les filtres enregistrés ici. Pour plus d'informations, consultez la section Sauvegarder les mises en page des rapports (la page 174).

- **Modifier dans la vue du rapport** : En cliquant sur ce bouton, le rapport d'événement est ouvert dans une fenêtre de dépannage, ce qui vous permet d'exécuter le rapport, de configurer des filtres et de sauvegarder la mise en page par défaut du rapport.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Rapports de l'utilisateur | Colonnes

Cet onglet vous permet de définir les colonnes qui apparaîtront dans le rapport. Tout champ d'utilisateur peut être ajouté au rapport, y compris les champs élargis (voir **Utilisateurs | Utilisateurs | Élargis**) et les champs personnalisés. Cela permet aux opérateurs de créer des rapports hautement personnalisés avec de nombreuses options de regroupement et de filtrage.

Clique sur **Ajouter** pour sélectionner les colonnes, c'est-à-dire les champs d'utilisateur, qui seront inclus dans le rapport. Utilise les boutons **Déplacer vers le haut** / **Déplacer vers le bas** pour réorganiser les colonnes selon vos besoins.

Rapports | Configuration | Type de quart de travail.

Les secteurs tels que l'application de la loi, la sécurité, les soins de santé et l'industrie manufacturière exigent souvent que les opérations soient exécutées 24 heures sur 24, 7 jours sur 7. Dans cette pratique, la journée est généralement divisée en quart de travail qui fonctionnent souvent par rotation.

Chaque type d'équipe définit les heures de début, de fin et de pause pour une seule équipe. Il est possible d'ajouter plusieurs équipes à un rapport de présence et d'établir une rotation, de sorte que les données relatives aux heures et aux présences puissent être calculées pour chaque équipe. Pour plus d'informations, consultez la section Rapports de présences | Changer Temps (la page 162).

Pour plus d'informations et un exemple de programmation, voir la Note d'application 163 : Configuration des rapports d'équipe dans Protege GX.

TypesdeQuartsdeTravail | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Couleur**: La couleur utilisée pour identifier le type de quart de travail dans un rapport de présence. Définir la couleur à l'aide du sélecteur de couleur ou saisissez manuellement les valeurs RVB requises.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

TypesdeQuartsdeTravail | Heure

Types quart de travail

- **Heure de début /fin**: Les heures de début et de fin de ce type de quart de travail à chaque fois qu'il se produit.
- **Inclure les minutes avant le début du service**: Définit une période de grâce pendant laquelle les utilisateurs peuvent faire usage de leur badge avant le début du quart de travail. Les événements survenus pendant cette période seront inclus dans le rapport de présence de l'équipe.
- **Intègre les minutes après la fin du quart de travail** : Définit une période de grâce pendant laquelle les utilisateurs peuvent faire usage de leur badge après la fin du quart de travail. Les événements survenus pendant cette période seront inclus dans le rapport de présence de l'équipe.

Heures de pause

Vous pouvez faire jusqu'à 6 pauses pour chaque quart de travail. Cocher la case à côté de chaque pause pour activer la pause pour ce quart de travail.

- **Nom** : Un nom pour la pause, par ex. Thé du matin'.
- **Début/Fin** : Les heures de début et de fin de la pause. Elles définissent la plage de temps pendant laquelle l'employé est autorisé à prendre sa pause. Par exemple, les employés peuvent avoir droit à 30 minutes pour le déjeuner, qui peut être pris à tout moment entre 12h00 et 14h00.
- **Durée** : La durée de la pause en minutes. Ceci sera utilisé pour calculer les heures de travail de l'employé et les déductions d'heures.

  La durée de la pause doit être plus courte que l'espace entre les heures de début et de fin. Par exemple, pour une pause de 10 minutes commençant à 10h30, l'heure de fin devrait être au moins 10h41 pour permettre la durée totale de la pause.

- **Calcul** : Détermine comment l'heure de pause sera utilisée dans les calculs de présence. Exclure déduit la durée de la pause des heures de travail, la pause n'est donc pas rémunérée. Inclure ne permet pas de déduire la pause.

Mise en place de rapport réguliers de courriel

Chaque page de programmation de la configuration des rapports comporte un onglet **Courriel** qui peut être utilisé pour configurer des courriels automatisés réguliers pour les rapports.

Les fonctions de courrier électronique automatisées dans Protege GX exigent qu'un serveur de courrier SMTP soit configuré dans **Global | Paramètres globaux | Paramètres de courrier électronique**.

Opérateurs

Ajoutez un ou plusieurs opérateurs Protege GX qui recevront le rapport. Chaque opérateur doit avoir une **adresse de courriel** définie dans **Global | Opérateurs | Général**.

Rapport par courriel

- **Rapport par courriel**: Cocher cette case pour activer les courriels de rapport réguliers.
- **Format de rapport**: Préciser le format du fichier dans lequel le rapport sera envoyé. Choisir parmi les formats PDF, CSV, Texte ou XLS.
- **Temps**: Précise l'heure à laquelle le rapport sera envoyé, selon le fuseau horaire du serveur Protege GX.
- **Heure actuelle du serveur**: Affichage de l'heure locale actuelle du serveur Protege GX pour référence.
- **Exclure l'en-tête et le pied de page du rapport** : Par défaut, la plupart des rapports incluent un en-tête et un pied de page avec des détails supplémentaires sur le rapport (par exemple, le nom du rapport, la date d'exportation). Cependant, cela peut entraîner l'apparition de colonnes vides dans les rapports exportés ou envoyés par courriel dans certains formats, ce qui peut interférer avec les processus automatisés. Activez cette option pour supprimer l'en-tête et le pied de page des rapports d'événements, évitant ainsi ce problème.

  Cette option n'est pas disponible pour les rapports de présence car ils n'ont pas d'en-tête ou de pied de page.
- **Nombre d'événements**: Pour les rapports d'événements, vous pouvez spécifier le nombre d'événements qui seront exportés et envoyés par courriel. Les rapports très lourds seront divisés en plusieurs fichiers et envoyés sous forme de plusieurs courriels.
- **Samedi-Dimanche**: Définit le(s) jour(s) de la semaine où le rapport sera envoyé.

Période de temps

- **Période**: Seulement valable pour les rapports d'événements. La période de temps que couvrira le rapport par courriel. Les options sont :
  - Depuis la dernière fois que le rapport a été envoyé par courriel: Comprend tous les événements depuis le dernier courriel de rapport jusqu'à maintenant.
  - Depuis minuit: Comprend tous les événements depuis minuit jusqu'à maintenant.
  - Les dernières 24 h: Comprend tous les événements depuis la même heure hier jusqu'à présent.
  - Les dernières 48 h: Comprend tous les événements depuis la même heure il y a deux jours jusqu'à présent.
  - Une semaine précédente: Comprend tous les événements de la semaine précédente, du lundi au dimanche (inclus).
  - Les deux dernières semaines: Comprend tous les événements de la quinzaine précédente, du lundi au dimanche (inclus).
  - Mois civil précédent: Comprend tous les événements du mois précédent, du 1er au 30/31 (inclus).
- **Dernière date d'exécution**: Indique quand le dernier courriel de rapport automatique a été envoyé (seulement pour lecture).

Configuration des exportations régulières de fichiers de rapport

Chaque page de programmation de la configuration du rapport comporte un onglet **Exportation de fichier** qui peut être utilisé pour configurer des exportations de fichiers automatisées, programmées ou périodiques, du rapport.

Rapport de fichier

- **Activer l'exportation de fichiers**: Cocher cette case pour activer l'exportation de rapports périodiques.
- **Format de rapport**: Définit le format de fichier vers lequel le rapport sera transféré. Choisir parmi les formats PDF, CSV, Texte ou XLS.
- **Temps**: Par défaut, ce champ définit l'heure de la journée à laquelle le rapport sera transféré. Lorsque **l'heure d'exportation périodique** est activée, les chiffres des minutes seront traités comme une période.
- **Heure actuelle du serveur**: Indique l'heure actuelle du serveur (seulement le champ de lecture).
- **Répertoire d'exportation**: Définit l'emplacement réseau vers lequel le rapport sera transféré. S'assurer que ce chemin de fichier soit accessible sur le serveur Protege GX.
- **Exécuter le rapport en tant qu'opérateur**: Pour les rapports de l'utilisateur, vous pouvez spécifier l'opérateur qui sera utilisé pour exécuter le rapport. Ceci est important car différents opérateurs peuvent avoir accès à différents enregistrements d'utilisateurs.
- **Nombre d'événements**: Pour les rapports d'événements, vous pouvez spécifier le nombre d'événements qui seront transférés.
- **Ajouter l'identifiant unique au nom du fichier**: Lorsque cette option est activée, un identifiant unique sera ajouté au nom de fichier de chaque fichier transféré. Cela vous permet d'exécuter des transferts programmés sans craindre que les fichiers soient endommagés.
- **Le temps de transfert est périodique (minutes)**: Lorsqu'il est activé, le **Temps** programmé ci-dessus sera utilisé comme période entre les rapports. La période est définie par les chiffres des minutes. Par exemple, si la valeur **Temps** est fixée à 12:02, le rapport sera transféré toutes les deux minutes.
- **Exclure l'en-tête et le pied de page du rapport** : Par défaut, la plupart des rapports incluent un en-tête et un pied de page avec des détails supplémentaires sur le rapport (par exemple, le nom du rapport, la date d'exportation). Cependant, cela peut entraîner l'apparition de colonnes vides dans les rapports exportés ou envoyés par courriel dans certains formats, ce qui peut interférer avec les processus automatisés. Activez cette option pour supprimer l'en-tête et le pied de page des rapports d'événements, évitant ainsi ce problème.

  Cette option n'est pas disponible pour les rapports de présence car ils n'ont pas d'en-tête ou de pied de page.
- **Jours du transfert**: Sélectionne les jours de la semaine où le rapport sera transféré. Ces options sont automatiquement désactivées si **l'heure du transfert périodique** est activée.

Période de temps

Cette section s'applique uniquement aux rapports d'événements.

- **Période**: Seulement valable pour les rapports d'événements. La période de temps que couvrira le rapport transféré. Les options sont :
  - Depuis le dernier transfert du rapport: Inclut tous les événements depuis le dernier transfert de rapport jusqu'à maintenant.
  - Depuis minuit: Comprend tous les événements depuis minuit jusqu'à maintenant.
  - Les dernières 24 h: Comprend tous les événements depuis la même heure hier jusqu'à présent.
  - Les dernières 48 h: Comprend tous les événements depuis la même heure il y a deux jours jusqu'à présent.
  - Une semaine précédente: Comprend tous les événements de la semaine précédente, du lundi au dimanche (inclus).
  - Les deux dernières semaines: Comprend tous les événements de la quinzaine précédente, du lundi au dimanche (inclus).
  - Mois civil précédent: Comprend tous les événements du mois précédent, du 1er au 30/31 (inclus).
- **Dernière date d'exécution**: Indique la date à laquelle le dernier transfert automatique de rapport a été effectué (seulement pour lecture).

Visualisation des rapports

Protege GX Les rapports sont faciles à exécuter et à consulter, et disposent d'un certain nombre de fonctionnalités puissantes qui vous permettent de tirer le meilleur parti de vos événements archivés et de vos données utilisateur. Créez un rapport personnalisé, groupez et filtrez par différentes colonnes à la volée, puis imprimez ou exportez selon vos besoins.

Le processus d'exécution et de configuration des rapports est le même quel que soit le type de rapport (à l'exception des rapports de la station centrale, qui produisent un fichier CSV).

Pour une démonstration, voirICT Conseil rapide : Visualisation des rapports d'événements dans Protege GX sur ICT la chaîne YouTube.

Exécution d'un rapport

1. Naviguer vers le programme de configuration du rapport que vous souhaitez exécuter (par exemple, **Rapports | Configuration | Événement**) puis créer et sauvegarder un nouvel enregistrement de rapport avec les paramètres dont vous avez besoin. Pour plus d'informations, consultez la section Paramétrage des rapports (la page 155).

   Ce qui précède n'est pas nécessaire pour les rapports d'autorisation des opérateurs.

2. Dans le menu **Rapports**, sélectionnez le type de rapport à exécuter (par. exemple., **Rapports | Événement**).
3. Dans la barre d'outils, sélectionnez le rapport enregistré que vous souhaitez exécuter, puis cliquez sur **Exécuter**.
4. Pour les rapports d'événements, il vous sera demandé de spécifier une **période**. Vous pouvez définir manuellement une **date de début** et une **date de fin**, ou sélectionnez une **période** prédéfinie parmi les options suivantes :
   - Aujourd'hui (depuis minuit), hier, avant-hier: Les événements qui se sont produits le jour sélectionné, de minuit à minuit.
   - Dernière heure, 12 dernières heures, 1 à 21 derniers jours: Les événements qui se sont produits entre maintenant et la date/heure de début sélectionnée. Par exemple, le rapport 1 dernier jour commence 24 h avant l'heure actuelle.
   - Le mois dernier, 2 à 6 derniers mois, l'année dernière, les 2 dernières années: Les événements qui se sont produits entre aujourd'hui et la date de début sélectionnée. Par exemple, le dernier mois commence à minuit le même jour du mois précédent et va jusqu'au jour présent (par exemple du 14 juin au 14 juillet).
   - Janvier à décembre dernier: Les événements qui se sont produits au cours du mois sélectionné. Par exemple, le rapport juin dernier comprend tous les événements survenus du 1er au 30 juin (inclus). Si le mois en cours est sélectionné, le rapport couvre ce mois de l'année précédente.
5. Pour les rapports d'événements, vous pouvez affiner votre recherche en sélectionnant un **contrôleur**.
6. Pour les rapports d'événements, vous pouvez entrer une **recherche par nom d'enregistrement** pour n'inclure que les enregistrements portant le nom spécifié.
7. Le rapport sera exécuté et affichera les enregistrements résultants.

   Pour les rapports d'événements, vous pouvez utiliser les icônes de la barre d'outils pour basculer l'affichage entre **la vue en liste** (simple liste de résultats) et **la grille**. (grille/tableau de résultats permettant des opérations plus complexes d'ordonnancement et de regroupement).
8. Si plus de 200 résultats sont renvoyés, utilisez les boutons **Précédent** et **Suivant** de la barre d'outils pour naviguer entre les résultats qui couvrent plusieurs pages.
9. Trier, regrouper et filtrer les résultats selon vos besoins à l'aide de la vue en grille (consultez page suivante).
10. Utiliser le bouton **Imprimer** pour ouvrir la fenêtre d'aperçu avant impression, dans laquelle vous pouvez imprimer, exporter ou envoyer par courriel les résultats actuellement visibles (consultez la page 175).

En outre, le bouton **Imprimer par lot** dans les rapports d'utilisateurs vous permet d'imprimer des cartes d'identité avec photo pour tous les utilisateurs actuellement visibles dans le rapport. Cela nécessite une imprimante de cartes XPS connectée.

Travailler avec la vue de grille

La vue de grille vous permet de formater, trier, grouper et filtrer facilement les résultats des rapports.

Réglage de l'affichage des colonnes

Les colonnes de la grille peuvent être réorganisées si nécessaire :

- **Redimensionnez les colonnes** en plaçant votre souris sur le bord de l'en-tête de colonne jusqu'à ce qu'il forme une double flèche ↔. Puis faites glisser la colonne à la taille requise.

  L'option **Meilleur ajustement** vous permet de redimensionner automatiquement les colonnes en vue de grille afin qu'elles aient la largeur optimale pour afficher les données qu'elles contiennent.
  - Pour redimensionner automatiquement une seule colonne, passez votre souris sur le bord de l'en-tête de la colonne jusqu'à ce qu'elle forme une double flèche ↔, puis double-cliquez.
  - Pour redimensionner automatiquement toutes vos colonnes, cliquez avec le bouton droit de la souris sur n'importe quel en-tête de colonne et sélectionnez **Meilleur ajustement (toutes les colonnes)** .
- **Réorganisez les colonnes** en faisant glisser et en déposant un en-tête de colonne vers une nouvelle position dans la grille.
- **Enlevez les colonnes** en faisant glisser l'en-tête de la colonne vers le bas. Lorsqu'une icône de suppression rouge **x** apparaît sur l'en-tête de colonne, relâchez la souris pour supprimer la colonne.

  Pour retrouver les colonnes que vous avez enlevées, faites un clic droit sur n'importe quel en-tête et sélectionnez **Afficher le sélecteur de colonnes** pour afficher une liste des colonnes disponibles.

Tri des données par colonne

Une exigence courante consiste à trier un grand nombre de résultats de rapports dans un ordre logique. Par exemple, vous pourriez vouloir trier un rapport d'utilisateur alphabétiquement par **Nom de famille** ou numériquement par **ID de base de données**.

Vous pouvez trier les résultats en utilisant les données d'une colonne particulière en cliquant simplement sur l'en-tête de la colonneque ce soit en vue liste ou en vue grille. Une flèche s'affiche dans la colonne active pour indiquer que la liste est triée selon cette colonne. Le sens de la flèche (haut ou bas) indique si les données sont triées par ordre croissant ou décroissant. Cliquez à nouveau sur l'en-tête de la colonne pour modifier l'ordre de tri.

Un clic droit sur un en-tête de colonne offre une autre méthode de sélection des options de tri pour la colonne sélectionnée :

- Pour trier une colonne, cliquez avec le bouton droit de la souris sur l'en-tête de la colonne et sélectionnez **Trier par ordre croissant** ou **Trier par ordre décroissant** .
- Pour effacer tout tri appliqué à la colonne, cliquez avec le bouton droit de la souris sur l'en-tête de la colonne et sélectionnez **Effacer le tri** .

Groupe par colonne

Le regroupement par colonnes vous permet de classer un grand nombre d'événements ou de registres de façon plus lisible. Par exemple, vous pouvez regrouper un rapport de l'utilisateur en fonction de son niveau d'accès, ou séparer les événements en fonction des portes concernées.

Regroupez les données en faisant glisser un en-tête de colonne au-dessus des autres dans la zone de regroupement. Cela permet de regrouper les entrées du rapport sous des titres basés sur les données de cette colonne. Vous pouvez agrandir chaque titre en cliquant dessus.

Vous pouvez faire glisser autant de colonnes que vous le souhaitez dans la zone de regroupement, ou supprimer le regroupement en faisant glisser une colonne jusqu'au niveau normal. L'ordre des colonnes dans la zone de regroupement crée une hiérarchie qui divise les résultats en une structure arborescente.

Un clic droit sur un en-tête de colonne offre une autre méthode de sélection des options de regroupement. Cliquez simplement avec le bouton droit de la souris sur l'en-tête de la colonne requise et sélectionnez **Regrouper sous cette colonne**. Pour dégrouper, faites un clic droit sur l'en-tête de la colonne groupée et sélectionnez **Dégrouper**.

Filtrer les résultats de rapport

Plusieurs méthodes permettent de filtrer les données dans les résultats du rapport retourné :

- En utilisant les en-têtes de colonne.
- En utilisant la rangée de filtre.
- En utilisant l'éditeur de filtre.

Vous pouvez également modifier les filtres que vous avez ajoutés ou supprimer les filtres dont vous n'avez plus besoin.

Filtrer en utilisant les en-têtes de colonne

Filtrez les données en passant votre souris sur un en-tête de colonne jusqu'à ce qu'une petite icône de filtre apparaisse. Cliquez sur l'icône pour sélectionner vos critères de filtre :

- **Vides :** Affiche uniquement les résultats dont la colonne sélectionnée comporte une entrée vide (aucune donnée saisie).
- **Non vides** : Afficher uniquement les événements qui n'ont pas d'entrée vide dans la colonne sélectionnée.
- **Résultats** : Une liste des résultats qui apparaissent dans cette colonne s'affiche. Sélectionnez-en un ou plusieurs pour filtrer le rapport en fonction de résultats spécifiques.

  Par exemple, sélectionnez Personnel de bureau dans la colonne du niveau d'accès pour afficher uniquement les registres correspondant à ce niveau d'accès.

Filtrer en utilisant la rangée de filtre

Dans tout rapport, la rangée située directement sous l'en-tête est la rangée de filtre. Vous pouvez filtrer n'importe quelle colonne en saisissant un mot, une phrase ou des caractères sous l'en-tête de la colonne concernée.

Par exemple, le personnel de l'entrepôt peut utiliser plusieurs niveaux d'accès : Quart d'entrepôt 1, Quart d'entrepôt 2 et Superviseur d'entrepôt. Vous pouvez filtrer un rapport de l'utilisateur pour ces trois niveaux d'accès en saisissant le terme commun « Entrepôt » dans la rangée de filtre.

L'éditeur de filtres

L'éditeur de filtres vous permet de créer des filtres complexes pour contrôler les résultats affichés. Pour ouvrir la fenêtre de l'éditeur de filtres, cliquez avec le bouton droit de la souris sur un en-tête de colonne et sélectionnez **Éditeur de filtres** .

Vous pouvez ajouter des conditions (lignes) à l'éditeur de filtres en cliquant sur l'icône verte **[+]** (ou en utilisant la **touche Insertion**), et supprimer des lignes avec la rouge**[x]** (ou en utilisant la touche **Effacer**). Chaque terme de chaque condition peut être édité en cliquant sur le terme et en sélectionnant une option dans la liste déroulante, ou en tapant un mot ou une phrase pertinente.

Utilisation de l'éditeur de filtres

- **Type de condition** : Pour sélectionner le type de condition pour le filtre, cliquez sur le terme rouge en haut de la fenêtre de l'éditeur. Ce type s'appliquera à toutes les conditions du filtre (ou du groupe) : par exemple, si vous sélectionnez Ou , le filtre aura la structure A ou B ou C . Les conditions disponibles sont les suivantes :
  - **Et** : Toutes les conditions du filtre doivent être remplies pour qu'un résultat soit inclus.
  - **Ou** : Une ou plusieurs des conditions du filtre doivent être remplies pour qu'un résultat soit inclus.
  - **NotAnd**: Une seule des conditions doit être remplie pour qu'un résultat soit inclus. Si plus d'un critère est rempli, il est exclu.
  - **NotOr** : Aucune des conditions ne doit être remplie pour qu'un résultat soit inclus. Si l'une des conditions s'applique à un événement, celui-ci est exclu.
  - **Ajouter une condition** : Ajoute une nouvelle ligne/condition au filtre.

- **Ajouter un groupe** : Ajoute un nouveau groupe de conditions au filtre. Ce groupe peut avoir son propre type de condition, ce qui vous permet de créer des conditions plus complexes telles que A et B et (C ou D) .
- **Effacer tout** : Supprime toutes les conditions et tous les groupes du filtre.

- **Colonne** : La première entrée de chaque condition. Cela détermine la colonne à laquelle la condition s'appliquera.
- **Opérateur** : L'entrée centrale (bleue) dans chaque condition. Ceci définit un opérateur logique qui sera utilisé pour cette condition. Les options disponibles dépendent de la colonne sélectionnée pour le filtre.
- **Valeur** : Le terme à droite de la condition, se référant aux entrées de la colonne évaluée.
  - Si l'opérateur sélectionné nécessite une valeur, cliquez sur le lien gris pour la saisir ou la sélectionner. Par exemple, si l'opérateur sélectionné est **Égal**, vous devez saisir ou sélectionner la valeur qui doit figurer dans cette colonne pour que la condition de filtrage soit remplie.
  - Certains opérateurs exigent ou vous donnent la possibilité d'entrer plus d'une valeur. Par exemple, si l'opérateur sélectionné est **Se situe entre** , vous devez saisir les deux valeurs entre lesquelles la condition sera remplie.
  - Si l'opérateur sélectionné est **Est l'un de**, vous pouvez cliquer sur le bouton plus pour ajouter d'autres valeurs.

Lorsque le filtre est terminé, cliquez sur **OK** pour l'appliquer au rapport et fermer l'éditeur de filtres, ou sur **Appliquer** pour appliquer le filtre sans fermer l'éditeur.

Modifier ou effacer des filtres

Vous pouvez facilement supprimer ou modifier les filtres qui ont été appliqués. Tous les filtres qui sont actuellement appliqués sont affichés dans une barre d'état au bas de la fenêtre de la grille.

La barre d'état du filtre

Nom	Description
Désactiver le filtre	Décochez la case pour désactiver le(s) filtre(s) actuel(s). Sélectionnez à nouveau pour réactiver le filtre actuel.
Modifier le filtre	Cliquez sur le bouton d'édition pour afficher l'éditeur de filtres qui vous permet de modifier le(s) filtre(s) actuellement appliqué(s).
Effacer le filtre	Cliquez sur le bouton d'effacement pour supprimer définitivement le filtre.

Caractéristiques supplémentaires de la vue de grille

Un certain nombre de caractéristiques supplémentaires sont disponibles dans le menu contextuel (clic droit) des colonnes. Pour afficher ces caractéristiques, faites un clic droit sur la colonne et sélectionnez :

- **Masquer/afficher le panneau du groupe** : Le panneau de groupe est affiché au-dessus des en-têtes de colonne, et est utilisé lors du regroupement des colonnes. Si vous n'utilisez pas le regroupement, vous pouvez masquer le panneau de regroupement afin de libérer de l'espace pour l'affichage des résultats.
- **Afficher/masquer le sélecteur de colonne** : Le sélecteur de colonne affiche les titres de toutes les colonnes que vous avez supprimées du rapport principal, ce qui vous permet de les réintégrer au rapport si nécessaire.
- **Masquer/afficher la barre de recherche** : Le panneau de recherche est un outil de recherche de base, qui vous permet de rechercher des rapports pour des résultats spécifiques.

Sauvegarder les mises en page des rapports

Une fois que vous avez configuré les critères de tri, d'assemblage et de filtrage souhaités dans la grille en vue, vous pouvez enregistrer votre mise en page pour une utilisation ultérieure avec le même rapport.

Les mises en page de rapport sauvegardées ne sont appliquées que dans le logiciel client Protege GX. Il est impossible de conserver les mises en page des rapports dans le client Web.

Sauvegarde de la mise en page du rapport de l'opérateur

Les opérateurs individuels peuvent enregistrer une mise en page de rapport pour chaque rapport spécifique, qui sera appliquée automatiquement chaque fois que cet opérateur exécutera le rapport. Cette fonction est accessible à tous types de rapports, de même pour les recherches d'utilisateurs et d'événements.

Pour sauvegarder une mise en page de rapport, configurez la grille en vue comme vous le souhaitez, puis cliquez sur le bouton **Sauvegarder la mise en page du rapport** dans la barre d'outils. La prochaine fois que l'opérateur exécutera le rapport, la mise en page enregistrée sera appliquée automatiquement.

Sauvegarder les mises en page des rapports par défaut

Pour les rapports d'événements et d'utilisateurs, il est aussi possible de sauvegarder une mise en page de rapport par défaut. Cette mise en page sera appliquée automatiquement lorsqu'un opérateur exécutera ce rapport.

Pour enregistrer une mise en page de rapport par défaut, configurez la grille en vue comme vous le souhaitez et cliquez sur le bouton **Enregistrer la mise en page de rapport par défaut** dans la barre d'outils. Lorsqu'un opérateur exécute le rapport, il peut très vite appliquer cette mise en page sauvegardée en cliquant sur le bouton **Charger la mise en page par défaut du rapport**.

Le filtre défini pour cette mise en page de rapport par défaut peut être consulté sur la page de configuration du rapport. À ce niveau là, cliquez sur **Modifier dans le rapport en vue** pour exécuter le rapport et enregistrer une nouvelle mise en page.

Si des mises en page individuelles pour les opérateurs et une mise en page de rapport par défaut pour l'ensemble du site sont utilisées, la dernière mise en page consultée par l'opérateur sera utilisée lors de la prochaine génération du rapport par défaut.

Fenêtre Imprimer l'aperçu

Une fois que vous avez généré un rapport, utilisez le bouton **Imprimer** de la barre d'outils pour ouvrir la fenêtre Imprimer l'aperçu. Cette fenêtre n'affichera que les résultats qui sont actuellement visibles dans le rapport, afin que vous puissiez filtrer, regrouper et ordonner selon vos besoins, puis exporter facilement les résultats.

L'aperçu avant impression n'affiche que la « page » actuelle du rapport (c.à.d. 200 résultats). Plusieurs exportations peuvent être nécessaires pour des rapports volumineux.

Utiliser les options de la barre d'outils pour prévisualiser, imprimer, exporter ou envoyer les résultats par courriel.

Bouton	Fonction
Recherche	Ouvre un outil de recherche de base, vous permettant de rechercher des termes spécifiques dans le fichier de prévisualisation.
Ouvrir	Vous permet d'ouvrir un fichier de prévisualisation de rapport précédemment enregistré (format .prnx).
Sauvegarder	Enregistre le fichier de prévisualisation du rapport en cours au format .prnx pour stocker temporairement les rapports afin de les ouvrir à nouveau dans Protege GX. Pour exporter un rapport dans un format plus répandu, utiliser l'option **Exporter**.
Imprimer	Ouvre une boîte de dialogue d'impression qui vous permet de sélectionner une imprimante, des préférences d'impression, une plage de pages et le nombre de copies avant l'impression. Il n'est pas possible d'imprimer des rapports en orientation paysage directement sur une imprimante. Pour l'orientation paysage, il est nécessaire d'exporter le rapport au format PDF, qui peut ensuite être envoyé à l'imprimante.
Impression rapide	Imprime le rapport sur votre imprimante par défaut avec les paramètres par défaut.
Configuration de page	Affiche la boîte de dialogue de configuration de page, dans laquelle vous pouvez indiquer les paramètres d'impression tels que le format du papier, l'orientation de la page et les marges.

Bouton	Fonction
Échelle	Met à l'échelle le contenu du rapport sur la page. Cela vous permet d'adapter la largeur du rapport à un certain nombre de pages. Par exemple, une échelle de 100 % signifie que la largeur du rapport s'étend sur une seule page. Avec une échelle de 200 %, le rapport sera mis à l'échelle et fera deux pages de large.
Zoom arrière	Effectue un zoom arrière d'un pas.
Zoom	Change le niveau de zoom à l'une des tailles prédéfinies.
Zoom avant	Effectue un zoom avant d'un pas.
Première page	Passe à la première page du rapport.
Page précédente	Permet de revenir en arrière d'une page dans le rapport.
Page suivante	Permet d'avancer d'une page dans le rapport.
Dernière page	Passe à la dernière page du rapport.
Exporter	Exporte le rapport dans l'un des nombreux formats disponibles : PDF, HTML, MHT, RTF, XLS, XLSX, CSV, Text, Image ou XPS. Le bouton principal exporte automatiquement au format PDF; vous pouvez cliquer sur la flèche à droite du bouton pour sélectionner un autre format. Chaque format nécessite que vous configuriez des options spécifiques à ce format. En cochant la case **Ouvrir après l'exportation** en haut de la fenêtre, le fichier exporté s'ouvrira une fois l'exportation terminée. Vous pouvez également configurer une exportation régulière par fichier de rapports spécifiques dans la programmation **Rapports | Configuration**. Les fichiers CSV exportés peuvent contenir des colonnes vides. Il s'agit d'un problème connu.
Envoyer par courriel	Enregistre le rapport dans un format spécifié, puis ouvre un nouveau message avec le rapport en pièce jointe en utilisant le programme de courriel par défaut de votre ordinateur. Vous pouvez également configurer une exportation régulière par courriel de rapports spécifiques dans la programmation **Rapports | Configuration**.

Rapport de la station centrale

Vous devrez généralement fournir à votre station de surveillance hors site une carte de rapport qui spécifie les codes de rapport pour les partitions, les entrées et les utilisateurs. Ces cartes peuvent être facilement exportées à partir de Protege GX pour être utilisées avec les services Contact ID et Rapport IP.

Cette fonction n'est pas liée aux autres options de rapport.

Générateur de cartes de rapport

Ouvrez le générateur de carte de rapport en naviguant vers **Rapports | Rapport de la station centrale**.

- **Services de rapports** : Le service pour lequel la carte de rapport sera générée.
- **Répertoire de sortie**: Le répertoire sur le réseau local où la carte de rapport sera générée. La carte de rapport sera exportée aux formats HTML et CSV.
- **Réinitialisation des ID de partition, d'entrée et d'entrée trouble** : Par défaut, la carte de rapport utilisera **l'ID de rapport** qui a été programmé dans chaque partition individuelle, entrée et enregistrement d'entrée trouble. Activez cette option si vous voulez réinitialiser les ID de rapport pour suivre un schéma de mappage Contact ID spécifique.
- **Type de carte de rapport :** : Si l'option **Réinitialiser les ID de partition, d'entrée et d'entrée trouble** est activée, sélectionnez le schéma de mappage Contact ID à utiliser :

- **Standard** : Convient aux petites installations d'effraction et de contrôle d'accès.
- **Large** : Convient aux installations de détection d'intrusion avec un grand nombre de modules d'expansions d'entrée.
- **SIMS II**: Une variante du format Contact ID qui peut envoyer un nombre beaucoup plus important d'entrées. Pour que ce mappage fonctionne correctement, le service doit également être configuré pour SIMS II en définissant l'option de **Cartographie cid** pour un service Contact ID, ou l'option de **Paramètres carte CID** pour un service Report IP.
- **Aucun** : Un mappage séquentiel : la première entrée sera mappée en tant que 001, la seconde en tant que 002 et ainsi de suite. Les entrées seront rapportées avant les entrées trouble. Toutes les ID supérieures à la valeur maximale déclarable (999) seront déclarées comme 999.

Pour plus d'informations, voir la note d'application 316 : Rapports au format Contact ID dans Protege GX et Protege WX.

- **Générer** : Cliquez sur ce bouton pour créer le rapport. Lorsque le rapport est terminé, cliquez sur **Ouvrir** pour ouvrir le dossier d'exportation.

Rapport d'autorisation de l'opérateur

Le rapport sur les autorisations des opérateurs vous permet de visualiser tous les opérateurs dans le système, ainsi que les rôles qui leur sont attribués, afin de voir facilement toutes les autorisations des opérateurs d'un seul coup d'œil, et de les exporter, les envoyer par courriel ou les imprimer selon les besoins.

Pour exécuter un rapport d'autorisation de l'opérateur, naviguer vers **Rapports | Autorisation de l'opérateur** et cliquer sur **Exécuter**. Il n'y a pas de programmation de configuration pour ce type de rapport.

Vous pouvez ordonner, regrouper et filtrer les résultats pour afficher les informations requises. Pour plus d'informations, consultez la section Travailler avec la vue de grille (la page 172).

Menu Surveillance

Les fonctions de surveillance de votre site se trouvent ici. À partir de ce menu, vous pouvez créer et afficher des plans d'étages et des pages des statuts, créer des listes des statuts et des liens Web, et configurer des caméras autonomes ainsi que des intégrations DVR.

Vue page du statut

Les pages de statut fournissent un aperçu intuitif et efficace de votre système. Chaque page de statut est entièrement personnalisable, avec jusqu'à 16 tuiles qui peuvent être remplies avec des journaux d'événements, des informations sur le statut des appareils, des plans d'étage, des flux de caméras ou d'autres éléments qui nécessitent une surveillance.

Pour ouvrir une page de statut, naviguez vers **Surveillance | Vue page du statut** . Sélectionnez la page de statut que vous souhaitez afficher dans la liste déroulante de la barre d'outils. Il est pratique d'utiliser le bouton **Ouverture** pour ouvrir la page de statut dans une nouvelle fenêtre, afin de pouvoir la visualiser sur un second moniteur tout en continuant à programmer le système.

Les pages de statut peuvent être créées dans **Surveillance | Configuration | Éditeur de page de statut** (consultez la page 188). La page de statut qui s'affiche en premier lorsque vous ouvrez la vue de la page de statut est définie comme la page de statut par **défaut** dans **Global | Sites | Affichage**.

Interactions sur la page de statut

Vous pouvez cliquer sur l'ellipse verticale ⋮en haut à droite de chaque tuile pour les interactions suivantes :

- **Actif** : Lorsque cette case est cochée, la tuile affiche une vue en direct ou active qui se met à jour en permanence. Décochez cette case pour figer le statut actuel de la tuile.
- **Copier** : Cliquez sur ce bouton pour copier la ou les lignes actuellement sélectionnées. Les informations seront copiées dans le presse-papiers au format CSV, qui pourra ensuite être collé dans un fichier texte ou une feuille de calcul.
- **Mise à jour** : Cliquez sur ce bouton pour mettre immédiatement à jour l'état de la tuile en fonction des informations fournies par le contrôleur. Cela ne fonctionnera pas si l'option **Active** n'est pas cochée.
- **Effacer** : Cliquez sur ce bouton pour effacer la fenêtre des événements et n'afficher que les nouveaux événements.

Vous pouvez faire un clic droit sur les appareils et certains événements pour afficher un menu contextuel permettant d'effectuer des commandes manuelles. Par exemple :

- Faites un clic droit sur les appareils pour ouvrir les commandes manuelles de cet appareil. Par exemple, vous pouvez verrouiller/déverrouiller des portes, armer/désarmer des partitions, contourner des entrées et activer/désactiver des sorties.
- Vous pouvez badger un nouvel identifiant sur un lecteur et cliquer avec le bouton droit de la souris sur l'événement "Lire les données brutes" pour l'attribuer à un utilisateur nouveau ou existant.
- Lorsqu'un événement se produit concernant un enregistrement auquel est associée une caméra, vous pouvez cliquer avec le bouton droit de la souris sur l'événement pour ouvrir une fenêtre de caméra avec les séquences archivées au moment de l'événement.
- Lorsqu'un utilisateur se voit refuser l'accès par l'anti-passback, vous pouvez faire un clic droit sur l'événement pour réinitialiser le statut anti-passback de l'utilisateur.

Page de statut des alarmes

La page de statut des alarmes préconfigurée fournit une vue en direct des alarmes opérateur actives et reconnues dans le système. Pour reconnaître une alarme, faites un clic droit sur l'événement dans la section Toutes les alarmes et cliquez sur **Reconnaître** . L'événement sera déplacé vers la section Toutes les alarmes reconnues.

Pour plus d'informations, consultez la section Alarmes (la page 144).

Il est recommandé de ne pas modifier ni supprimer cette page de statut des alarmes par défaut, afin qu'elle soit toujours disponible pour reconnaître les alarmes.

Vue plan d'étage

Les plans d'étages permettent de visualiser et de contrôler en temps réel les portes, les sorties, les entrées, les caméras, les partitions, les entrées trouble, les ascenseurs et les variables à partir d'un plan d'étage. Les appareils d'un plan d'étage sont mis à jour de façon dynamique à la fois sur l'affichage graphique et dans le volet d'état situé à droite du plan d'étage.

Pour ouvrir un plan d'étage, naviguez vers **Surveillance | Vue plan d'étage**. Sélectionnez le plan d'étage que vous souhaitez afficher dans la liste déroulante de la barre d'outils. Il est pratique d'utiliser le bouton **Incrustation** pour ouvrir le plan d'étage dans une nouvelle fenêtre, afin de pouvoir la visualiser sur un second moniteur tout en continuant à programmer le système.

Les plans d'étages peuvent être créés dans **Surveillance | Configuration | Éditeur de plan d'étages** (consultez page suivante). Le plan d'étage qui apparaît en premier lorsque vous ouvrez la vue plan d'étage est défini comme le **Plan d'étage par défaut** dans **Global | Sites | Affichage**.

Pour plus de renseignements sur la visualisation et la programmation des plans d'étages, consulter la Note d'application 340 : Programmation des plans d'étages dans Protege GX.

Sections du plan d'étage

Le plan d'étage se compose des sections suivantes :

- Une représentation graphique du construction ou du site, y compris des icônes interactives pour les appareils. Vous pouvez faire un clic droit sur n'importe quelle icône d'appareil sur l'image pour ouvrir un menu contextuel pour les commandes manuelles (par exemple, verrouiller/déverrouiller des portes, armer/désarmer des partitions).

  Le plan d'étage peut également inclure des boutons qui sont utilisés pour afficher une vue de caméra ou ouvrir un autre plan d'étage.
- Une liste d'état qui se met dynamiquement à jour pour afficher l'état en temps réel des appareils sur le plan d'étage. Vous pouvez faire un clic droit sur n'importe quel appareil pour ouvrir un menu contextuel pour les commandes manuelles.
- Une fenêtre d'événements affichant en temps réel une liste d'Événements du plan d'étage : événements liés aux appareils du plan d'étage. Vous pouvez faire un clic droit sur n'importe quel événement pour exécuter les événements du plan d'étage comme un rapport standard, qui peut être exporté, envoyé par courriel ou imprimé comme d'habitude.

  Jusqu'à six registres d'événements supplémentaires peuvent être affichés sous des onglets distincts dans ce volet. Ce réglage peut être effectué comme **Fenêtre d'événement 1-6** dans **Global | Sites | Affichage** .

Surveillance | Configuration

Le sous-menu de configuration comprend des pages de configuration pour les pages des statuts et les plans d'étages, ainsi que la programmation des intégrations de caméras et d'interphones.

Éditeur de plan d'étages

Utilisez l'**Éditeur de plans d'étages** pour créer et adapter les plans d'étages aux besoins spécifiques de votre système. Chaque plan d'étage peut représenter une section du système, comme un seul étage de bureau ou un appareil spécifique, ou le système dans son ensemble.

Pour plus de renseignements sur la visualisation et la programmation des plans d'étages, consulter la Note d'application 340 : Programmation des plans d'étages dans Protege GX.

Menus de l'éditeur de plan d'étages

Propriétés du plan d'étage

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.
- **Fond** : Cliquez sur le bouton ellipse **[...]** pour définir une image de fond pour le plan d'étage. Celle-ci doit se trouver dans un emplacement de fichier accessible sur la machine serveur, tel qu'un dossier réseau partagé. L'image peut être dans les formats de fichier .bmp, .jpg ou .png.

  Assurez-vous que toutes les images sont situées dans un dossier réseau partagé auquel les clients ont accès. Si le lien vers une image est rompu ou si l'ordinateur client ne peut pas y accéder, l'image n'apparaîtra pas dans le client Protege GX.

- **Largeur** : Définit la largeur du plan d'étage (en pixels).
- **Hauteur** : Définit la hauteur du plan d'étage (en pixels).
- **Color picker** : Définit la couleur de fond du plan d'étage.
  - Pour définir une couleur solide, cliquez sur l'onglet **Solid** et sélectionnez la couleur à l'aide du sélecteur de couleur ou en saisissant des valeurs RVB.
  - Pour créer un dégradé, cliquez sur l'onglet **Gradient** pour afficher une barre de glissement sous les sélecteurs de couleur. Cliquez sur chaque curseur pour définir la couleur de chaque côté individuellement, puis ajustez les curseurs pour obtenir l'effet souhaité.
  - Pour ne définir aucune couleur (transparent), cliquez sur l'onglet **Null**.
- Utilisez les onglets situés au-dessus du sélecteur de couleur pour indiquer si la couleur sera **Solid**, **Gradient** ou **Null** (sans couleur). (pas de couleur), puis définissez la couleur de fond en utilisant le sélecteur de couleur ou en saisissant des valeurs RVB.

Pinceaux

La section des pinceaux est utilisée pour définir la couleur, la visibilité et l'opacité des lignes, du texte et des boutons sur le plan d'étage.

1. Développez la section **Pinceaux** et sélectionnez un élément dans l'éditeur.
2. Choisissez si vous modifiez la couleur de **fond**, la **Bordure** ou le **Premier plan** de l'élément. Cela dépend de l'élément en cours de configuration.
3. Définissez les couleurs de l'élément :
   - Pour définir une couleur solide, cliquez sur l'onglet **Solid** et sélectionnez la couleur à l'aide du sélecteur de couleur ou en saisissant des valeurs RVB.
   - Pour créer un dégradé, cliquez sur l'onglet **Gradient** pour afficher une barre de glissement sous les sélecteurs de couleur. Cliquez sur chaque curseur pour définir la couleur de chaque côté individuellement, puis ajustez les curseurs pour obtenir l'effet souhaité.
   - Pour ne définir aucune couleur (transparent), cliquez sur l'onglet **Null**.
4. Indiquez si l'élément est **Visible** ou **Caché**.
5. Définissez la **Opacité** de l'élément.

Appareils

Cette section permet d'ajouter au plan d'étage des représentations d'appareils physiques tels que des portes, des partitions, des entrées et des variables. Lorsque vous visualisez le plan d'étage, chaque icône d'appareil affiche son état actuel et vous pouvez faire un clic droit pour le modifier.

1. Développez la section **Périphériques** et cliquez sur **Ajouter** pour ajouter un nouveau périphérique.
2. Définissez le **Type de périphérique** comme il convient.
3. Définissez le **Style de dispositif** que vous souhaitez utiliser. Cela détermine le type d'icône qui sera utilisé pour ce périphérique sur le plan d'étage.

   Si vous avez créé un enregistrement de symbole de plan d'étage (**Global | Symboles de plan d'étage**) pour un type de dispositif spécifique, lorsque vous ajoutez un dispositif, vous pouvez définir le **Style de dispositif** pour utiliser vos symboles personnalisés.
4. Faites glisser et déposez le(s) dispositif(s) requis sur le plan d'étage. Puis **Fermez** la fenêtre contextuelle.
5. Déplacez le dispositif en cliquant et en le faisant glisser, redimensionnez-le en utilisant les carrés dans les coins et faites-le pivoter en utilisant les cercles dans les coins.

Il n'est pas nécessaire de configurer le champ **Données**.

Lignes

Les lignes vous permettent de dessiner des formes de base sur le plan d'étage, qui peuvent être utilisées pour les murs et autres caractéristiques du site.

1. Développez la section **Lignes** et cliquez sur **Ajouter**.
2. Votre curseur se transformera en une forme **+**. Cliquez quelque part dans le champ de dessin pour créer le premier nœud de la ligne.
3. Pour créer un nœud ou un coin supplémentaire, cliquez une fois. La ligne peut avoir autant de coins que nécessaire, ce qui vous permet de créer des formes complexes.
4. Pour compléter la ligne, double-cliquez.
5. Donnez à la ligne un **Nom** descriptif.
6. Une fois la ligne terminée, vous pouvez
   - Définir la **Largeur de la ligne** dans la section **Lignes**.
   - Définir la couleur avec l'attribut **Bordure** dans le menu **Pinceaux**.
   - Déplacez la ligne en cliquant et en la faisant glisser à l'intérieur de la boîte en pointillés.
   - Redimensionnez la ligne en cliquant et en faisant glisser les carrés aux coins.
   - Faites pivoter la ligne en cliquant et en faisant glisser les cercles dans les coins.

- Déplacez la ligne devant ou derrière d'autres éléments à l'aide des boutons **Front** et **Back** de la barre d'outils.

Texte

Le texte vous permet d'ajouter des étiquettes de texte à votre plan d'étage (par exemple, des noms de partition, des directions).

1. Développez la section **Texte** et cliquez sur **Ajouter**.
2. Votre curseur se transformera en une forme **+**. Cliquez et faites glisser quelque part sur le champ de dessin pour créer une zone de texte.
3. Donnez au texte un **Nom** descriptif.
4. Dans le champ **Texte**, entrez le texte requis.
5. Une fois le texte terminé, vous pouvez :
   - Définir la **Police**, la **Taille de la police** et le style du texte dans la section **Texte**.
   - Définir la couleur avec l'attribut **Premier plan** dans le menu **Pinceaux**.
   - Déplacez la zone de texte en cliquant et en la faisant glisser à l'intérieur de la boîte en pointillés.
   - Redimensionnez la zone de texte en cliquant et en faisant glisser les carrés dans les coins.
   - Faites pivoter la zone de texte en cliquant sur les cercles situés dans les coins et en les faisant glisser.
   - Déplacez la zone de texte devant ou derrière d'autres éléments à l'aide des boutons **Front** et **Back** de la barre d'outils.

Images

Dans cette section, vous pouvez ajouter des images à votre plan d'étage à partir de fichiers.

1. Cliquez sur **Ajouter**, puis saisissez un chemin de fichier ou cliquez sur l'ellipse **[...]** pour naviguer vers une image. L'image peut être au format .bmp ou .jpg.

   Assurez-vous que toutes les images sont situées dans un dossier réseau partagé auquel les clients ont accès. Si le lien vers une image est rompu ou si l'ordinateur client ne peut pas y accéder, l'image n'apparaîtra pas dans le client Protege GX.

2. Votre curseur se transformera en une forme **+**. Cliquez et glissez quelque part dans le champ de conception pour ajouter l'image.
3. Donnez à l'image un **Nom** descriptif.
4. Une fois l'image terminée, vous pouvez :
   - Déplacer l'image en cliquant et en faisant glisser à l'intérieur de la boîte en pointillés.
   - Redimensionner l'image en cliquant et en faisant glisser les carrés situés dans les coins.
   - Faire pivoter l'image en cliquant et en faisant glisser les cercles aux coins.
   - Déplacez l'image devant ou derrière d'autres éléments en utilisant les boutons **Front** et **Back** de la barre d'outils.

     Vous pouvez utiliser le bouton **Arrière** pour créer une image de fond.

Boutons

Dans cette section, vous pouvez ajouter des boutons cliquables qui effectuent des actions spécifiques. Un type de bouton ouvre une fenêtre de caméra en direct, ce qui vous permet de vérifier facilement les sites clés. L'autre type ouvre un plan différent, vous permettant de naviguer rapidement dans le système.

1. Développez la section **Boutons** et cliquez sur **Ajouter**.
2. Votre curseur se transformera en une forme **+**. Cliquez et faites glisser quelque part sur le plan pour créer un bouton.
3. Dans le champ **Texte**, entrez un libellé pour le bouton.

4. Définissez les détails de mise en forme tels que **Police**, **Taille de la police** et le style du texte.
5. Développez la section **Actions**. Sélectionnez soit une **Caméra** ou un **Plan d'étage** qui sera ouvert par ce bouton.
6. Une fois le bouton complété, vous pouvez :
   - Définir les couleurs avec les attributs **Fond**, **Bordure** et **Premier plan** dans le menu **Pinceaux**.
   - Déplacez le bouton en cliquant et en le faisant glisser dans la boîte en pointillés.
   - Redimensionnez le bouton en cliquant et en faisant glisser les carrés situés dans les coins.
   - Faites pivoter le bouton en cliquant sur les cercles situés dans les coins et en les faisant glisser.
   - Déplacez le bouton devant ou derrière d'autres éléments à l'aide des boutons **Front** et **Back** de la barre d'outils.

Si la couleur d'arrière-plan d'un bouton est définie sur **Null**, vous devez cliquer sur l'étiquette de texte plutôt que sur l'arrière-plan pour activer le bouton.

Actions

Des actions sont requises pour l'utilisation des boutons. Pour appliquer une action à un bouton, sélectionnez le bouton et définissez soit la **Caméra**, soit le **Plan d'étage**.

Barre d'outils de l'éditeur de plan d'étages

La barre d'outils offre une fonctionnalité permettant de contrôler la disposition et le positionnement des éléments ajoutés à un plan d'étage.

Bouton	Fonction
Refaire	Vous permet de rétablir (refaire) la dernière action qui a été défaite.
Défaire	Vous permet de défaire la dernière action.
Copier	Copie le ou les objets sélectionnés dans le presse-papiers.
Coller	Colle le contenu du presse-papier dans le champ de conception.
Effacer	Enlève l'objet sélectionné du champ de conception.
Aligner	Lorsque cette option est activée, lorsque vous dessinez, redimensionnez ou déplacez un objet, celui-ci s'aligne ou s'accroche aux objets les plus proches dans le champ de conception, même si la règle n'est pas visible. Si votre objet ne se déplace pas là où vous le souhaitez, désactivez cette option.
Angle	Aligne le ou les objets sélectionnés sur l'angle de grille polaire le plus proche.
Règle	Sélectionnez cette option pour faire basculer la règle sur on ou sur off.
Avant	Déplace l'objet sélectionné devant d'autres objets.
Arrière	Déplace l'objet sélectionné derrière d'autres objets.
Aligner en haut	Aligne tous les objets sélectionnés sur le bord supérieur du dernier objet sélectionné.
Alig bas	Aligne tous les objets sélectionnés sur le bord inférieur du dernier objet sélectionné.
Alig Gch	Aligne tous les objets sélectionnés sur le bord gauche du dernier objet sélectionné.
Alig Drt	Aligne tous les objets sélectionnés sur le bord droit du dernier objet sélectionné.

Éditeur de plan d'étage (lot)

L'éditeur de plan d'étage par lot vous permet de modifier des caractéristiques spécifiques des plans d'étages dans une fenêtre de programmation normale, ce qui est pratique pour les modifications par lot ou pour rechercher les détails de la création d'un registre.

Éditeur de plan d'étage (lot) | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.
- **Mode d'étirement** :
  - **Remplir** : Lorsqu'il est activé, le rapport d'aspect s'ajuste à l'écran de sorte que le plan d'étage est redimensionné en fonction de la taille de la fenêtre.
  - **Uniforme** : Lorsqu'il est activé, le ratio d'aspect du plan d'étage est conservé lorsque la fenêtre est redimensionnée.
- **Largeur** : Définit la largeur du plan d'étage (en pixels).
- **Hauteur** : Définit la hauteur du plan d'étage (en pixels).

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Ajouter des plans de masse

La fonction **Ajouter des Plans d'étage en vrac** vous permet de créer rapidement un plan d'étage pour chaque contrôleur sur un site, y compris tous les appareils (portes, entrées, sorties et/ou partitions) contrôlés par ce contrôleur.

Cela vous permet de définir une image de fond cohérente qui sera utilisée par tous les plans d'étage, garantissant ainsi que tous les plans d'étage respectent les directives de marque ou de style d'entreprise. Le processus crée également une image de remplacement pour chaque plan d'étage, qui est stockée en dehors de la base de données Protege GX. Cela permet, à vous ou à un graphiste, de remplacer et de mettre à jour les plans d'étage sans ouvrir Protege GX.

Ajout de plusieurs plans d'étage

1. Naviguez jusqu'à **Surveillance | Configuration | Ajouter des plans de masse**. La fenêtre **Ajouter plusieurs plans d'étage** s'ouvre.
2. Entrez les propriétés requises comme décrit ci-dessous.
3. Cliquez sur **Ajouter maintenant** pour créer les plans d'étage.
4. Dans l'emplacement défini comme répertoire **Image**, vous trouverez des images PNG vierges pour chaque contrôleur. Vous pouvez modifier ou remplacer ces images par des représentations de la disposition de chaque plan d'étage.
5. Dans l'éditeur de plan d'étage (**Surveillance | Configuration | Editeur de plan d'étage**), ouvrez chaque plan d'étage et finalisez le positionnement et la conception des dispositifs et autres éléments.

Modèle de base

- **Image de fond** : Définit le chemin et le nom de fichier d'une image qui sera utilisée comme fond pour tous les plans d'étage qui sont créés. Assurez-vous de saisir le nom de fichier complet d'une image existante à utiliser comme fond.

  Pour de meilleurs résultats, les dimensions de l'image doivent déjà correspondre à la taille et au ratio d'aspect souhaités des plans d'étage finaux afin de maintenir le ratio d'aspect et d'éviter tout problème de distorsion.

  Assurez-vous que toutes les images sont situées dans un dossier réseau partagé auquel les clients ont accès. Si le lien vers une image est rompu ou si l'ordinateur client ne peut pas y accéder, l'image n'apparaîtra pas dans le client Protege GX.
- **Largeur** : Définit la largeur du fond (en pixels).
- **Hauteur** : Définit la hauteur du fond (en pixels).

Image du plan d'étage

- **Répertoire d'images** : Définit la location où les images de placement seront créées. Ce processus créera une nouvelle image PNG vierge pour chaque contrôleur. Notez que cela remplacera toutes les images existantes portant le même nom à cet emplacement.

  Assurez-vous que toutes les images sont situées dans un dossier réseau partagé auquel les clients ont accès. Si le lien vers une image est rompu ou si l'ordinateur client ne peut pas y accéder, l'image n'apparaîtra pas dans le client Protege GX.
- **Décalage horizontal** : Règle la distance (en pixels) à laquelle l'image sera décalée horizontalement par rapport à la gauche.
- **Décalage vertical** : Règle la distance (en pixels) à laquelle l'image sera décalée verticalement par rapport au haut.
- **Largeur de l'image** : Définit la largeur des images (en pixels).
- **Hauteur de l'image** : Définit la hauteur des images (en pixels).

Boutons

Le processus d'ajout en masse crée également deux boutons qui renvoient à d'autres plans d'étage - plus précisément, un plan d'étage « accueil » et « répertoire ». Cela permet de naviguer facilement entre les plans d'étage lors de la surveillance du système.

Les plans d'étage de l'accueil et du répertoire doivent déjà avoir été créés.

- **Texte du bouton d'accueil** : Définit le texte (étiquette) du premier bouton.
- **Plan d'étage** : Définit le plan d'étage de l'accueil auquel le bouton sera lié.
- **Texte du bouton répertoire** : Définit le texte (étiquette) du second bouton.
- **Plan d'étage** : Définit le plan d'étage du « répertoire » auquel le bouton sera lié.

Appareils

- **Portes** : Lorsque cette option est activée, elle inclut chacune des portes disponibles sur le plan d'étage pour chaque contrôleur.
- **Entrées** : Lorsque cette option est activée, elle inclut chacune des entrées disponibles sur le plan d'étage pour chaque contrôleur.
- **Sorties** : Lorsque cette option est activée, elle inclut chacune des sorties disponibles sur le plan d'étage pour chaque contrôleur.
- **Partitions** : Lorsque cette option est activée, elle inclut chacune des partitions disponibles sur le plan d'étage pour chaque contrôleur.

Éditeur Page de statut

Les pages de statut sont un moyen rapide et efficace d'obtenir un aperçu de votre Protege système en un seul endroit. Chaque page de statut peut comprendre jusqu'à 16 tuiles, chacune d'entre elles pouvant afficher un seul élément ou une seule liste.

Création d'une page de statut

1. Naviguez vers **Surveillance | Configuration | Éditeur Page de statut** et cliquez **sur Ajouter** . La fenêtre **Ajouter une page** de statut s'ouvre.
2. Saisissez **un nom** pour votre page de statut, sélectionnez une mise en page par défaut, puis cliquez sur **OK**. La fenêtre de programmation affiche un nombre de cases correspondant à la disposition sélectionnée.
3. Si vous avez besoin d'une mise en page personnalisée qui n'est pas disponible dans les options par défaut, vous pouvez le faire :
   - Ajustez le nombre de **rangées** et **de colonnes** de cases qui sont incluses dans la page de statut en haut de la fenêtre de l'éditeur.
   - Ajustez le nombre de **rangées** et de **colonnes** que chaque case individuelle couvre.
4. Pour chaque case de la page de statut, définissez le **type** sur l'un des types disponibles :
   - **Des listes de statuts** qui se mettent à jour dynamiquement pour afficher l'état en temps réel des appareils sélectionnés. Ceux-ci peuvent être programmés dans **Surveillance | Configuration | Liste des statuts** .
   - **Des plans d'étage**qui fournissent une représentation visuelle du site et de l'état en temps réel des appareils et des objets de votre système. Ceux-ci peuvent être programmés dans **Surveillance | Configuration | Éditeur de plan d'étage** .
   - **Caméras** d'un système DVR/NVR intégré affichant un flux vidéo en direct. Ils peuvent être programmés dans **Surveillance | Caméras** .
   - **Fenêtres d'événements**qui affichent une vue en direct des événements dans un rapport d'événements particulier. Ceux-ci peuvent être programmés **dans Rapports | Configuration | Événement** .
   - **Variables** qui renvoient des informations sur des données variables telles que la température de la chambre ou le taux d'humidité. Ceux-ci peuvent être programmés dans **Automatisation | Variables** .
   - **Pages Web** affichant le contenu d'un site Web spécifique ou d'une page HTML stockée localement. Ils peuvent être programmés dans **les pages Surveillance | Configuration | Pages Web** .
   - **Des rapports Muster** qui montrent une liste des emplacements les plus récents des utilisateurs dans le système. Ceux-ci peuvent être programmés dans **Rapports | Configuration | Muster** .

   Si une case s'étend sur plusieurs lignes ou colonnes, assurez-vous que les cases adjacentes sont laissées comme<not set> afin d'éviter que le contenu ne se chevauche sur la page de statut.
5. Définissez **l'enregistrement** approprié pour chaque case (par exemple, une liste des statuts ou un rapport d'événement).
6. Une fois que vous avez la configuration et la mise en page que vous souhaitez, cliquez sur **Sauvegarder** .

Éditeur Page de statut (lot)

L'éditeur de pages de statut par lots vous permet d'apporter des modifications aux noms et aux mises en page des pages de statut dans une fenêtre de programmation standard.

Éditeur Page de statut (lot) | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Nom d'affichage du clavier** : Le nom qui sera téléchargé vers le contrôleur. Ce dernier sera affiché sur le clavier et dans les rapports des services de surveillance IP. Le clavier ne peut afficher que les 16 premiers caractères du nom. Il doit donc décrire de manière concise l'emplacement physique et la fonction de l'appareil.
- **Rangées** : Définit le nombre de lignes affichées sur la page de statut.
- **Colonnes** : Définit le nombre de colonnes affichées sur la page de statut.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Listes des statuts

Les listes de statuts peuvent être utilisées dans une page d'état pour fournir un affichage en temps réel de l'état des appareils sélectionnés tels que les portes et les partitions. Vous pouvez cliquer avec le bouton droit de la souris sur un appareil dans une liste des statuts pour ouvrir le menu des commandes manuelles, ce qui vous permet de verrouiller/déverrouiller des portes, d'armer/désarmer des partitions ou d'ouvrir des vues de caméras en direct.

Listes des statuts | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Appareils

Cliquez **sur Ajouter** pour ouvrir la fenêtre de sélection des appareils. Sélectionnez le **type d'appareil** (et **le contrôleur**, le cas échéant) et cochez les cases en regard des enregistrements souhaités, puis cliquez sur **OK** pour ajouter les appareils sélectionnés à la liste des statuts.

Vous pouvez ajouter les types d'appareils suivants :

- Portes
- Sorties
- Entrées
- Partitions
- Zones troubles (c.-à-d. entrées troubles)
- Ascenseurs
- Variables

D'autres enregistrements peuvent être disponibles en fonction des intégrations activées pour le site.

Listes des statuts | Filtres

Les filtres de statut vous permettent d'afficher dans la liste de statut uniquement les dispositifs qui ont un statut particulier (tel que déverrouillé ou désarmé).

Filtres des statuts

- **Filtre statut de la partition** : Les zones ne seront affichées dans la liste des statuts que si elles ont le statut sélectionné. Par exemple, vous pouvez créer une liste des statuts qui n'affiche que les partitions actuellement désarmées.
- **Filtre statut de porte** : Les portes ne seront affichées dans la liste des statuts que si elles ont le statut sélectionné. Par exemple, vous pouvez créer une liste des statuts qui n'affiche que les portes qui sont actuellement déverrouillées.

Liens web

Les liens Web peuvent être utilisés dans les pages d'état et les alarmes pour afficher le contenu d'un site Web ou d'une page HTML spécifique.

Outre l'affichage de sites web en ligne, cette fonction peut renvoyer à des contenus tels qu'un répertoire du personnel ou des informations sur les politiques et procédures de l'intranet de l'entreprise. Il suffit de créer une page HTML avec les informations que vous souhaitez afficher, d'enregistrer le fichier à un emplacement sur le Protege GX serveur ou dans un dossier réseau partagé, puis de créer un lien web qui renvoie à ce fichier.

Liens web | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Configuration

- **URL** : L'adresse de la page web ou l'emplacement du répertoire de la page HTML. Veillez à inclure le préfixe https:// pour les pages sur Internet.

  Si vous utilisez une page HTML personnalisée, le fichier HTML et tous les fichiers de soutien tels que les images ou les fichiers CSS doivent se trouver dans un dossier auquel l'opérateur Windows a le droit d'accéder. Ces fichiers doivent être situés sur le serveur Protege GX ou dans un dossier réseau partagé.
- **URL2** : Une autre adresse web ou de répertoire qui sera utilisée lorsque Protege GX est exploité dans la deuxième langue. La case à cocher ci-dessous doit être activée.
- **Utiliser le champ URL2 comme deuxième langue** : Sélectionnez cette option pour permettre l'utilisation de **l'URL2** dans la deuxième langue.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

DVR

Protege GX s'intègre à un certain nombre de systèmes de gestion vidéo (VMS) tiers pour fournir une surveillance vidéo intégrée. Les caméras peuvent être liées à des appareils particuliers dans le système, fournissant une vue en direct de la caméra et des documents archivés en fonction d'événements et de déclencheurs disponibles dans Protege GX. La plupart des intégrations fournissent également une interface de haut niveau (HLI), permettant à Protege GX d'enregistrer des événements HLI tels que « Mouvement détecté ».

Cette page de programmation vous permet de configurer une connexion à un DVR ou NVR qui se trouve sur le même réseau que le serveur Protege GX.

L'intégration avec des systèmes de gestion vidéo tiers requiert une licence adéquate et généralement l'installation d'un service d'intégration dédié. Pour plus de renseignements, consulter la note d'application correspondante à chaque intégration.

Pour voir une démonstration, reportez-vous à Configuration des systèmes de gestion vidéo dans Protege GX sur la chaîne YouTube ICT.

DVR | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Configuration

- **Adresse IP** : L'adresse IP du DVR.
- **Port DVR** : Le port utilisé par Protege GX pour communiquer avec le DVR. Ce paramètre est généralement défini dans le service d'intégration VMS concerné.
- **Type de DVR** : Le type de DVR ou d'intégration en cours de configuration. Si un service d'intégration VMS est utilisé, ce champ doit être réglé sur Personnalisé, quelle que soit la marque du DVR intégré.

HLI

- **Surveiller les événements à partir de ce DVR/NVR** : Lorsque cette option est activée, les événements HLI de ce DVR peuvent être enregistrés dans Protege GX. Chaque intégration dispose de différents événements HLI, tels que « DVR/NVR hors ligne » et « Espace disque faible ».

  Note : Pour recevoir les événements HLI de la caméra tels que « Mouvement détecté », l'option **Surveiller les événements** doit également être activée dans **Surveillance | Configuration | Caméras | Général**.

- **Se connecter à ce DVR/NVR au démarrage** : Lorsque cette option est activée, Protege GX envoie une demande de connexion au DVR lorsque le client démarre. Sinon, Protege GX ne se connecte pas au DVR jusqu'à ce qu'il ait besoin de demander une liste ou des images de caméra.

  Cette option est uniquement disponible lorsque le **Type de DVR** est réglé sur Personnalisé.

Connexion

- **Connexion requise** : Sélectionnez cette option si le DVR exige des détails d'informations d'identification pour se connecter.
- **Nom d'utilisateur/mot de passe** : Les informations d'identification que Protege GX utilise pour se connecter au DVR. Assurez-vous que cette connexion dispose des autorisations nécessaires pour visualiser les images et les événements de la caméra dans Protege GX.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Caméras

Cette page de programmation vous permet de configurer les caméras pour qu'elles affichent des séquences vidéo en direct et archivées dans Protege GX. Vous pouvez configurer des caméras IP autonomes ou des caméras associées à un DVR ou NVR intégré (voir **Surveillance | Configuration | DVRs**).

Une fois que les caméras ont été configurées, elles peuvent être surveillées sur les pages d'état et associées à des dispositifs particuliers, ce qui vous permet de visualiser les séquences de caméra en direct et archivées des événements.

Caméras | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Configuration

- **Type** : Il y a trois types de caméras disponibles :
  - **DVR**: Les caméras qui sont connectées à un DVR ou NVR intégré.
  - **Caméra directe** : Caméras IP autonomes connectées en réseau à Protege GX qui fournissent un accès URL direct à un flux d'images JPEG statique ou un flux MJPEG en streaming. Cette option est utilisée pour les caméras de protocole RTSP.
  - **Caméra H.264 & motion JPEG stream** : Caméras IP autonomes qui fournissent un accès URL direct à un flux H.264.
- **DVR**: L'enregistrement DVR auquel la caméra est associée (le cas échéant). Ceux-ci peuvent être programmés dans**Surveillance | Configuration | DVRs**.
- **Nom de caméra DVR** : Cliquez sur l'ellipse **[...]** pour ouvrir une liste des caméras connectées au DVR sélectionné. Cette liste doit être extraite du VMS intégré. Si aucune caméra n'apparaît dans la liste, vérifiez que l'intégration est correctement configurée.
- **URL** : Si la caméra n'est pas connectée à un DVR, saisissez ici son adresse URL ou IP. Il s'agit du lien que vous utiliserez pour vous connecter à l'interface Web de la caméra.
- **Nom d'utilisateur/mot de passe** : Les informations d'identification utilisées pour se connecter à l'interface Web de la caméra.

  Ce champ n'est disponible que lorsque le **Type** est défini sur Caméra directe. Pour les caméras H.264 et Motion JPEG Stream, inclure le nom d'utilisateur et le mot de passe d'ouverture de session dans l'URL. par exemple, http://nom d'utilisateur:mot de passe@192.168.1.2/video

Affichage

- **Afficher les commandes de la barre latérale dans la page d'état** : Lorsque cette option est activée, les commandes PTZ sont affichées par défaut lorsque le flux de la caméra est visualisé sur une page d'état. Lorsque cette option est désactivée, la barre latérale de contrôle peut être ouverte mais ne sera pas affichée par défaut.
- **Étirer l'image** : Lorsque cette option est activée, l'image de la caméra est étirée pour remplir la tuile où elle est affichée. Cela peut ne pas préserver le rapport hauteur/largeur.
- **Plan d'étage** : Le plan d'étage auquel appartient la caméra. Cela vous permet de faire un clic droit sur un événement de caméra dans le journal événement et d'ouvrir le plan d'étage associé à la caméra.

HLI

- **Surveiller les événements** : Lorsque la caméra est utilisée dans le cadre d'une intégration VMS, vous pouvez activer cette option pour enregistrer des événements HLI tels que "Mouvement détecté" à partir de cette caméra. L'opérateur peut cliquer avec le bouton droit de la souris sur l'événement pour ouvrir une caméra avec des séquences archivées depuis le moment de l'événement.

  Cette option nécessite que l'option **Surveiller les événements du DVR** soit activé dans **Surveillance | Configuration | DVRs**.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Commandes PTZ

Les commandes PTZ sont des signaux de commande qui peuvent être envoyés à des caméras PTZ intégrées. Des commandes PTZ peuvent être envoyées en réponse à certains événements, afin de demander aux caméras d'effectuer un panoramique, une inclinaison et un zoom pour se concentrer sur les partitions concernées.

Par exemple, vous pourriez commander une caméra pour qu'elle se focalise sur une porte voisine chaque fois qu'un événement de porte forcée se produit, afin d'obtenir des images directes de l'événement en cours.

Une fois qu'une commande PTZ a été programmée, vous devez créer une action qui contrôlera quand cette commande doit être envoyée. Pour plus d'informations, consultez la section Actions (la page 146).

Commandes PTZ | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Configuration

- **Caméra :** La caméra que la commande PTZ va contrôler. Celles-ci peuvent être programmées dans**Surveillance | Configuration | Caméras**.
- **Chaîne de commandes** : Le texte qui doit être envoyé au DVR pour activer le mouvement PTZ. Il s'agit généralement du nom d'une commande sauvegardée dans le VMS intégré. Reportez-vous à la note d'application correspondante ou à la documentation de votre DVR pour obtenir des informations sur le format de commande requis.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Interphones

Les registres d'interphone permettent d'intégrer Protege GX aux systèmes d'interphone compatibles avec la VoIP. Si une station de travail a été configurée comme un client SIP dans **Événements | Postes de travail**, les opérateurs peuvent recevoir des appels depuis l'interphone, ainsi qu'un plan d'étage ou un flux de caméra pertinent.

En outre, les interphones peuvent être liés à des registres de porte, ce qui permet aux opérateurs d'appeler l'interphone en faisant un clic droit sur le registre de porte dans le logiciel. Par exemple, cela permet aux gardes de communiquer avec un visiteur avant de lui accorder l'accès à distance.

Les interphones VoIP sont une fonctionnalité sous licence séparée. Pour plus d'informations et d'instructions de programmation, consulter la note d'application 339 : Intégration des interphones SIP avec les stations de travail Protege GX. Il s'agit d'une fonctionnalité différente du service d'interphone qui peut être programmée dans **Programmation | Services**.

Interphones | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **URI :** Définit l'URI (Uniform Resource Identifier) de l'interphone.

Graphiques

- **Caméra** : Définit la caméra attribuée à l'interphone. Un flux de cette caméra est affiché lorsqu'un appel est passé ou reçu.
- **Plan d'étage** : Le plan d'étage qui sera lancé lorsqu'un appel provenant de l'interphone est accepté.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Menu Salto

Ce menu vous permet de programmer les portes, les groupes de portes et les calendriers de Salto, et de visualiser les erreurs dans le journal des erreurs de Salto.

L'intégration de Salto SHIP est une fonctionnalité sous licence séparée. Pour plus d'informations, voir la Note d'application 188 : Salto SHIP RW Intégration de Pro Access avec Protege GX or Application Note 335: Salto SHIP ProAccess SPACE Intégration avec Protege GX. Ce menu de programmation n'est pas utilisé avec l'intégration de Salto SALLIS.

Salto | Portes

Les portes Salto représentent les serrures sans fil Salto SHIP. Une fois que vous avez programmé les enregistrements de porte Salto, ils peuvent être affectés à des groupes de porte Salto et à des niveaux d'accès pour accorder l'accès aux utilisateurs.

Lorsque les portes Salto hors ligne ont été programmées dans Protege GX et synchronisées avec le serveur Salto SHIP, le matériel doit être mis à jour manuellement à l'aide d'un dispositif de programmation à distance. Il est recommandé de terminer la programmation de toutes les portes avant d'effectuer cette mise à jour.

Le nombre maximum de portes que Salto prend actuellement en charge est de 64 000 par base de données. Un maximum de 96 portes (portes individuelles ou portes dans un groupe) peut être attribué à un utilisateur. Cette règle s'applique à l'ajout de portes/groupes de portes à un utilisateur directement ou via un niveau d'accès.

Salto | Portes | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Nom d'affichage de Salto** : Le nom de l'enregistrement tel qu'il sera affiché dans le logiciel Salto. Il s'agit d'un champ en lecture seule, basé sur le **Nom** défini ci-dessus. Il est recommandé de nommer les enregistrements Salto de manière à ce qu'ils soient reconnaissables à la fois dans Protege GX et dans Salto.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

Paramètres

- **Heure d'ouverture**: La durée (en secondes) pendant laquelle la porte Salto restera déverrouillée après que l'accès ait été accordé. Par défaut, cette valeur est fixée à 6 secondes.
- **Augmenter le temps d'ouverture**: Un temps d'ouverture alternatif utilisé pour les utilisateurs qui ont besoin d'une durée d'accès prolongée, comme les personnes ayant des problèmes de mobilité. Cette durée sera utilisée pour les utilisateurs dont l'option **Utiliser le temps d'ouverture prolongé** est activée dans **Utilisateurs | Utilisateurs | Salto**. Par défaut, cette valeur est fixée à 20 secondes.

Anti-passback

- **Activer l'anti-passback**: Lorsque cette option est activée, l'anti-passback sera activé pour cette porte Salto. Si un utilisateur tente de franchir cette porte Salto dans la même direction sans sortir par la porte, l'accès lui sera refusé. Cela empêche les utilisateurs de transmettre leurs informations d'identification à une autre personne pour lui donner accès à des zones restreintes.

  L'anti-passback ne doit être utilisé qu'avec les paramètres **Mode ouvert** qui nécessitent des informations d'identification à tout moment.

- **Trajectoire**: Si l'anti-passback est activé ci-dessus, ce champ définit la direction du contrôle de l'anti-passback. Les options sont : De l'extérieur vers l'intérieur (entrée) et De l'intérieur vers l'extérieur (sortie).

Options de vérification

- **Vérification des clés**: Lorsque cette option est activée, les portes Salto hors ligne génèrent une piste d'audit des événements d'accès sur la carte de chaque utilisateur. Ces événements sont téléchargés sur le serveur chaque fois qu'un utilisateur fait usage de son badge sur une serrure en ligne.

  Les ouvertures **de vérification dans la clé** doivent être activées pour les utilisateurs dans **Utilisateurs| Utilisateurs | Salto**. Vous pouvez empêcher les opérateurs de désactiver cette vérification au niveau de **Sites | Niveaux de sécurité | Commandes manuelles**.

Mode et périodes d'ouverture

- **Mode ouvert** : Ce champ détermine le mode de fonctionnement de cette serrure électronique, c'est-à-dire la manière dont on peut y accéder pendant les différentes périodes prévues.
  - **Standard** : Les utilisateurs doivent badger une clé Salto autorisée pour avoir accès.
  - **Bureau** : Les utilisateurs peuvent mettre la porte en mode bureau. Le mode bureau est activé en présentant une clé Salto tout en maintenant la poignée intérieure enfoncée, et annulé en répétant la procédure. En mode bureau, la porte est déverrouillée et tout utilisateur sans justificatif peut y accéder.

    Seuls les utilisateurs ayant activé l'option **Bureau** peuvent mettre une porte en mode bureau (**Utilisateurs | Utilisateurs | Salto**).

  - **Basculer** : Lorsque cette option est sélectionnée, les utilisateurs peuvent activer et annuler le mode bureau en badgeant leur carte, sans maintenir la poignée intérieure.

    Seuls les utilisateurs ayant activé l'option **Bureau** peuvent mettre une porte en mode bureau (**Utilisateurs | Utilisateurs | Salto**).

  - **Modifications automatiques** : Cette option permet à la porte de fonctionner sous différents modes à différents moments. Le fonctionnement de ce paramètre peut être configuré dans le logiciel Salto.
  - **Ouverture automatique** : Dans ce mode, la porte se déverrouille automatiquement lorsque le programme des **périodes ouvertes** devient valide. Lorsque l'horaire n'est pas valide, la porte se verrouille automatiquement et fonctionne en mode standard.
  - **Ouverture automatique + bureau** : Dans ce mode, la porte se verrouille et se déverrouille automatiquement lorsque l'horaire devient valide. La porte se verrouille lorsque l'horaire devient invalide, mais les utilisateurs peuvent toujours activer le mode bureau en badgeant une carte avec la poignée intérieure maintenue enfoncée.
  - **Ouverture automatique + basculer** : Dans ce mode, la porte se verrouille et se déverrouille automatiquement lorsque l'horaire devient valide. La porte se verrouille lorsque l'horaire devient invalide, mais les utilisateurs peuvent toujours activer le mode bureau en badgeant une carte.
  - **Clé + code PIN** : La porte nécessite à la fois une clé/carte Salto valide et un code PIN valide à saisir sur le clavier. Ce code est valide à tout moment.

    L'option **PIN** doit être activée dans l'onglet **Utilisateurs | Utilisateurs | Salto**.

- **Clavier uniquement** : La porte peut être ouverte en entrant un code valide au clavier. Ce code est valide à tout moment.
- **Touche programmée + code PIN** : Ce mode est identique au mode Touche + NIP, sauf qu'un NIP n'est requis que lorsque l'horaire des **périodes ouvertes** est valide. En dehors de cette période, seule une carte est requise pour l'accès.
- **Clavier chronométré** : Ce mode est identique au Clavier, sauf que le code ne peut être utilisé que lorsque l'horaire des **périodes ouvertes** est valide. En dehors de cette période, une carte peut être utilisée pour l'accès.
- **Bureau à horaires fixes** : Cette option est similaire à Bureau, sauf que le mode bureau ne peut être activé que lorsque l'horaire des **périodes ouvertes** est valide. La porte se verrouille automatiquement et fonctionne en mode standard à la fin de l'horaire programmé.
- **Basculement chronométré** : Cette option est identique à Basculer, sauf que le mode bureau ne peut être activé que lorsque l'horaire des **périodes ouvertes** est valide. La porte se verrouille automatiquement et fonctionne en mode standard à la fin de l'horaire programmé.
- **Sortie laisse ouverte** : Lorsque cette option est sélectionnée, la porte fonctionne en mode standard. Cependant, lorsque la poignée intérieure est maintenue enfoncée, la porte se verrouille et se déverrouille.

  L'option `EXIT_LEAVES_OPEN` doit également être activée dans le logiciel Salto (**Options avancées**).
- **Basculer + sortie laisse ouverte :** Il s'agit d'une combinaison des deux modes. Lorsqu'une carte valide est présentée, la porte commence à fonctionner en mode Basculer. L'utilisation de la poignée intérieure active le mode Sortie laisse ouverte.

  L'option `EXIT_LEAVES_OPEN` doit également être activée dans le logiciel Salto (**Options avancées**).

- **Périodes ouvertes** : L'horaire qui est associé à la porte Salto. Ceci est équivalent à un enregistrement de périodes dans le logiciel Salto. Le fonctionnement de cet horaire dépend du **mode ouvert** sélectionné ci-dessus.

Caméras

- **Caméra**: Lorsqu'une caméra est affectée à une porte Salto, vous pouvez maintenant cliquer sur le bouton droit de la souris sur tout événement impliquant cette porte dans le journal des événements afin de visualiser les séquences archivées de la caméra pour cet événement.

Salto | Groupes de portes

Les groupes de portes Salto vous permettent de regrouper les portes Salto afin de les attribuer plus efficacement aux utilisateurs et aux niveaux d'accès. Dans le logiciel Salto, les groupes de portes sont appelés des zones.

Salto | Groupes de portes | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Nom d'affichage de Salto** : Le nom de l'enregistrement tel qu'il sera affiché dans le logiciel Salto. Il s'agit d'un champ en lecture seule, basé sur le **Nom** défini ci-dessus. Il est recommandé de nommer les enregistrements Salto de manière à ce qu'ils soient reconnaissables à la fois dans Protege GX et dans Salto.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Salto | Groupes de portes | Portes

Portes Salto

Pour ajouter des portes Salto au groupe, cliquez sur **Ajouter**. Vous pouvez faire glisser et déposer des registres individuels dans le champ, ou sélectionner plusieurs registres à l'aide des touches Maj + Clic. Ensuite, cliquez sur **OK**.

Salto| Calendriers

Les calendriers Salto sont utilisés pour définir des jours spécifiques comme des jours fériés ou des jours spéciaux pour le fonctionnement du système Salto.

Dans la programmation horaire, vous pouvez définir des périodes spécifiques pour fonctionner sur H (jours fériés), S1 (Spécial 1) ou S2 (Spécial 2) tels que définis dans le calendrier (colonne **Sites | Horaires | Configuration**, **Salto**). Ensuite, le calendrier peut être appliqué à un enregistrement d'utilisateur (**Utilisateurs | Utilisateurs | Salto**), de sorte que leurs autorisations d'accès seront modifiées à ces jours spécifiques. Les calendriers peuvent également être utilisés pour modifier les horaires des portes Salto à des jours spécifiques.

Salto| Calendriers | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Nom d'affichage de Salto** : Le nom de l'enregistrement tel qu'il sera affiché dans le logiciel Salto. Il s'agit d'un champ en lecture seule, basé sur le **Nom** défini ci-dessus. Il est recommandé de nommer les enregistrements Salto de manière à ce qu'ils soient reconnaissables à la fois dans Protege GX et dans Salto.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Salto | Calendriers | Dates

Cliquez sur **Ajouter** pour ajouter des dates au calendrier.

- **Nom**: Décrit la date (par exemple. Noël).
- **Date**: La date du jour férié ou de la journée spéciale.
- **Type**: Le type de journée. Choisir entre jours fériés, Spécial 1 ou Spécial 2.

Journal de Salto

Lorsque l'option **Activer la journalisation de Salto** est activée dans le menu **Global | Sites | Salto**, le journal des erreurs de Salto montre les événements de toutes les données envoyées au système Salto. Ces informations sont utilisées pour le débogage.

Les messages stockés dans le journal d'erreurs sont généralement enregistrés par paires, un message indiquant les informations envoyées au système Salto et l'autre indiquant la réponse du système Salto.

Les événements courants sont les suivants

- **GetInfo** : Ce message est enregistré une fois à chaque fois que le serveur de téléchargement démarre, et affiche la version SHIP actuelle que le système Salto exécute.
- **InsertOrUpdate** : Ce message indique que Protege GX est en train de mettre à jour les enregistrements dans le système Salto.

Manuel Salto Commandes des portes/groupes de portes

Un clic droit sur un enregistrement de porte Salto ou de groupe de portes Salto affiche un menu avec des commandes manuelles pour cet enregistrement.

Les commandes disponibles sont les suivantes :

- Ouvrir
- Ouverture de secours
- Fermeture de secours
- Annuler l'urgence

Ces commandes ne concernent que les serrures en ligne. L'utilisation de ces commandes avec des serrures hors ligne entraîne le renvoi d'une erreur par Protege GX.

Menu Cencon

Le menu Cencon vous permet de programmer les groupes de verrouillage Cencon et de visualiser le journal des transactions Cencon. Les verrous Cencon affectés à la branche seront automatiquement ajoutés à Protege GX lors de la synchronisation.

Ce menu n'est disponible que lorsque l'option **Activer l'intégration Cencon** est sélectionnée dans **Global | Sites | Cencon**.

L'intégration de Cencon est une fonctionnalité sous licence séparée. Pour plus d'informations, consultez la Note d'application 160 : Configuration de l'intégration de Cencon dans Protege GX.

Groupes de serrure Cencon

Les groupes de serrures Cencon vous permettent de regrouper les serrures Cencon connectées afin de les attribuer plus efficacement aux niveaux d'accès.

Groupes de serrure Cencon | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Inclure toutes les serrures

- **Inclure toutes les serrures** : Sélectionnez cette option pour inclure toutes les serrures connectées dans le groupe.

Serrures Cencon

Les serrures qui appartiennent à ce groupe de serrures. Cliquez sur **Ajouter** pour ouvrir une liste de serrures qui ont été programmées dans le système Cencon. Vous pouvez faire glisser et déposer des registres individuels dans le champ, ou sélectionner plusieurs registres à l'aide des touches Maj + Clic. Ensuite, cliquez sur **OK**.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Journaux de transactions de Cencon

Lorsque **l'option Enregistrer toutes les transactions** Cencon est activée dans **Global | Sites | Cencon** , les communications entre la base de données Cencon et Protege GX seront enregistrées ici. Cela vous permet de visualiser les transactions XML afin de résoudre les problèmes éventuels.

Menu Programmation

Les fonctions de programmation des registres tels que les portes, les partitions, les entrées, les sorties, les cabines d'ascenseur, les étages et les services se trouvent dans le menu Programmation.

Portes

Dans Protege GX, les portes sont utilisées pour contrôler l'accès des utilisateurs, ainsi que pour surveiller et contrôler le flux de personnes dans une partition.

Un certain nombre d'options pour les portes, telles que les informations d'identification requises pour l'accès et les paramètres d'anti-passback, sont définies dans le type de porte (**Programmation | Types de portes**).

Portes | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Nom d'affichage du clavier** : Le nom qui sera téléchargé vers le contrôleur. Ce dernier sera affiché sur le clavier et dans les rapports des services de surveillance IP. Le clavier ne peut afficher que les 16 premiers caractères du nom. Il doit donc décrire de manière concise l'emplacement physique et la fonction de l'appareil.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

Configuration

- **Type de porte** : Le type de porte assigné à une porte contrôle les informations d'identification requises pour l'accès dans diverses conditions, ainsi que le fonctionnement de l'anti-passback et de l'authentification double. Pour plus de renseignements, voir **Programmation | Types de portes**.
- **Porte esclave** : Vous pouvez assigner une autre porte comme porte esclave. Lorsqu'un utilisateur déverrouille la porte principale, la porte esclave sera également déverrouillée si l'utilisateur y a accès. Cela peut servir à contrôler deux portes adjacentes avec un seul port du lecteur.

  Par défaut, les portes esclaves ne suivent la porte principale que lorsqu'elle est déverrouillée par un accès avec des informations d'identification valides. Pour activer le fonctionnement de la porte esclave pour les commandes REX, REN et manuelles, ajoutez `SlaveREX = true` dans le champ **Commandes** de la porte principale.
- **Porte à l'intérieur/extérieur de la partition** : Ces champs vous permettent de définir les partitions qui sont à l'intérieur et à l'extérieur des portes, ce qui permet d'intégrer les fonctions de contrôle d'accès de la porte avec le contrôle de partition et la détection d'intrusion. La configuration de ces partitions vous permet d'utiliser une série de caractéristiques telles que :
  - Déverrouiller et verrouiller automatiquement les portes en fonction du statut de la partition (voir l'onglet **Options**)
  - Empêcher les utilisateurs d'entrer dans les partitions armées (voir l'onglet **Options avancées** et **Modules d'expansion | Modules d'expansion du lecteur | Lecteur 1/2**)

- Permettre aux utilisateurs d'armer ou de désarmer des partitions à partir du lecteur d'entrée/sortie (voir **Modules d'expansion | Modules d'expansion du lecteur | Lecteur 1/2**)
- Anti-passback (voir **Mode de passback d'entrée/sortie** dans **Programmation | Types de portes | Général**)
- Partitions de flânage (voir **Partition activée en mode de flânage** dans **Programmation | Partitions | Options (1)**)
- Comptage des partitions (voir **Activer comptage d'utilisateur** dans **Programmation | Partitions | Options (1)**)

S'il n'y a pas de partition surveillée à l'extérieur de la porte (c'est-à-dire si la porte est extérieure), vous pouvez laisser la partition extérieure réglée sur <non définie>.

- **Déverrouiller l'horaire** : L'horaire de déverrouillage peut être utilisé pour déverrouiller le loquet de la porte, permettant un accès libre sans informations d'identification lorsque l'horaire est valide. Par défaut, la fonction de déverrouillage est déclenchée par front d'impulsion : le loquet de la porte est déverrouillé lorsque l'horaire devient valide et se verrouille lorsque l'horaire n'est plus valide, mais elle peut être annulée par des commandes de l'utilisateur ou de l'opérateur. Ce comportement peut être modifié à l'aide des paramètres de l'onglet **Options**.

  Par exemple, un magasin peut définir un horaire de déverrouillage afin que la porte soit déverrouillée pour les clients pendant ses heures d'ouverture. En dehors de ces heures, la porte est verrouillée mais les employés peuvent y accéder en utilisant leurs informations d'identification.
- **Temps de délai de pré-alarme de la porte** : Lorsqu'une porte est laissée ouverte, elle génère une pré-alarme après cette période (en secondes). Cette pré-alarme génère un événement et active le **Groupe de sorties programmables / sortie pré-alarme** (défini dans l'onglet **Sorties**), avertissant les utilisateurs que l'alarme de porte laissée ouverte sera bientôt activée.

  Cette fonction peut être désactivée dans des circonstances spécifiques dans l'onglet **Options d'alarme**.
- **Temps d'alarme de la porte laissée ouverte** : Lorsque la porte est laissée ouverte, l'alarme de porte laissée ouverte se déclenche après cette période (en secondes). Cette alarme ouvre l'entrée trouble Porte laissée ouverte et active la **Sortie / groupe de sorties programmables d'alarme de porte laissée ouverte** (onglet **Sorties**).

  La minuterie de l'alarme de porte laissée ouverte commence lorsque la porte est ouverte pour la première fois, et non après l'activation de la pré-alarme. Par exemple, avec les paramètres par défaut, la pré-alarme est activée 30 s après l'ouverture de la porte, et l'alarme de porte laissée ouverte est activée 15 s plus tard (45 s au total).

  Cette fonction peut être désactivée dans des circonstances spécifiques dans l'onglet **Options d'alarme**.
- **Supporter commandes manuelles** : Lorsque cette option est activée, les opérateurs disposant des autorisations adéquates peuvent utiliser des commandes manuelles pour contrôler la porte. Par exemple, un gardien peut faire un clic droit sur l'icône d'une porte sur un plan d'étage pour la déverrouiller.

  Pour plus d'informations, consultez la section Commandes manuelles des portes (la page 219).
- **Interverrouiller Groupe de portes** : Lorsqu'un groupe de portes est assigné à ce champ, cette porte ne peut être déverrouillée que si toutes les portes assignées à Interverrouiller Groupe de portes sont fermées et verrouillées. Cela permet de s'assurer qu'une seule porte du groupe peut être ouverte à tout moment.

  Cette fonction permet d'empêcher l'ouverture d'un chemin libre entre les partitions sûres et les partitions dangereuses. Par exemple, elle peut être appliquée à un point d'entrée dans une salle blanche ou un site sécurisé.

  Pour plus de renseignements, consulter la Note d'application 206 : Interverrouillage des portes dans Protege GX. Pour voir une démonstration, reportez-vous à Configuration du verrouillage des portes dans Protege GX sur la chaîne YouTube ICT.

Commandes

- Ce champ est utilisé pour envoyer des commandes de programmation à l'appareil. Il ne doit être utilisé que lorsqu'il est spécifiquement conseillé par la documentation ICT ou le support technique.

Graphiques

Les caméras peuvent être programmées dans**Surveillance | Configuration | Caméras**.

- **Caméra (entrée/sortie)** : La caméra qui surveille respectivement le côté entrée ou sortie de la porte. Vous pouvez visualiser les séquences archivées des événements de la porte en faisant un clic droit sur l'événement sur une page du statut ou un plan d'étage.
- **Interphone (entrée/sortie)** : L'interphone qui est installé respectivement du côté de l'entrée ou de la sortie de la porte. Vous pouvez passer un appel vers cet interphone en faisant un clic droit sur le registre de la porte et en cliquant sur **Appeler l'interphone**.

  Les registres d'interphone sont programmés dans **Surveillance | Configuration | Interphones**. La station de travail doit également être configurée comme un client SIP dans **Événements | Stations de travail**.
- **Plan d'étage** : Le plan d'étage auquel la porte appartient. Cela vous permet de faire un clic droit sur un événement de porte dans le journal événement et d'ouvrir le plan d'étage associé à la porte.

Popup de caméra automatique

- **Popup de caméra automatique sur tout événement de porte** : Lorsque cette option est activée, une fenêtre contextuelle affiche les images en direct et archivées de la caméra chaque fois que n'importe quel événement de porte est généré.
- **Popup de caméra automatique sur événement de porte forcée** : Lorsque cette option est activée, une fenêtre contextuelle affiche les images en direct et archivées de la caméra chaque fois qu'un événement « Porte forcée » est généré.
- **Caméra** : La caméra utilisée par le popup de caméra automatique. Ces paramètres ne doivent pas nécessairement être identiques à ceux de la **Caméra (entrée)** ou de la **Caméra (sortie)** définis ci-dessus.

Ascenseur HLI

Différentes options sont disponibles en fonction du type d'ascenseur HLI configuré. Pour plus de renseignements, consulter la note d'application d'ascenseur HLI correspondante.

- **Porte utilisée pour ascenseur HLI** : Lorsque cette option est activée, cette porte est traitée comme faisant partie de l'intégration d'ascenseur HLI. En général, le registre de porte est utilisé pour représenter soit un panneau de commande de destination (DOP) situé à un étage, soit un panneau de commande de cabine (COP) situé dans une cabine d'ascenseur.
- **Contrôleur** : Le contrôleur auquel le registre de porte est associé. Seuls les contrôleurs dont la fonction d'ascenseur HLI est activée dans **Sites | Contrôleurs | Configuration** seront disponibles pour la sélection.
- **Type ascenseur HLI** : Le type d'ascenseur HLI pour lequel la porte est utilisée (lecture seulement). Cela dépend du **Type ascenseur HLI** défini dans **Sites | Contrôleurs | Configuration**.
- **KONE** : Pour plus de renseignements, consulter la Note d'application 170 : Protege GX intégration HLI KONE.
  - **Type de panneau opérateur** : Définit si cette porte sera configurée comme un DOP (panneau de commande de destination) ou un COP (panneau de commande de voiture).
  - **ID DOP/COP** : L'ID unique du DOP/COP qui a été configuré dans le système KONE.
  - **Groupe d'étages** : Le groupe d'étages accessible depuis le DOP/COP. Cette fonction permet de déverrouiller des étages spécifiques selon l'horaire pour ce DOP/COP.
  - **Étage** : Pour DOP seulement. Définit l'étage où se situe le DOP.

    La combinaison de l'identifiant DOP et de l'étage doit être unique.
  - **Groupe d'ascenseurs** : Pour COP seulement. Règle le numéro du groupe d'ascenseurs interne qui a été configuré dans le système KONE.

- **DOP envoie un appel d'ascenseur** : Cette option active l'interface d'appel à distance pour ce DOP. Si cette option est sélectionnée, lorsqu'un utilisateur accède à ce DOP, un appel sera automatiquement envoyé pour transporter l'utilisateur à l'**étage de destination de d'ascenseur** défini dans son niveau d'accès (**Utilisateurs | Niveaux d'accès | Général**).

  L'interface d'appel à distance KONE doit être activée en utilisant **Activer fonctionnalité appel d'ascenseur** dans **Sites | Contrôleurs | Configuration**.

- **Thyssenkrupp** : Pour plus de renseignements, consulter la Note d'application 169 : Protege GX intégration HLI ThyssenKrupp.
  - **Type de panneau de l'opérateur** : Seule l'option DOP est prise en charge par cette intégration. Cela correspond aux kiosques par étage.
  - **ID DOP** : L'ID unique du kiosque qui a été configuré dans le système Thyssenkrupp.
  - **Groupe d'étages** : Le groupe d'étages accessible depuis le kiosque. Cela permet de déverrouiller des étages spécifiques en fonction de l'horaire pour ce kiosque.
  - **Étage** : Définit l'étage sur lequel se situe le kiosque.
  - **Numéro de groupe** : Le numéro de groupe pour ce DOP qui a été configuré dans le système Thyssenkrupp.

    La combinaison de l'identifiant DOP, de l'étage et du numéro de groupe doit être unique.

- **OTIS** : Pour plus de renseignements, consulter la Note d'application 174 : Protege GX intégration HLI Otis Compass.
  - **Type de panneau de l'opérateur** : Seule l'option DOP est prise en charge par cette intégration. Cela correspond aux DEC (ordinateurs d'entrée de destination) par étage.
  - **ID DOP** : Cette information est fournie par le système d'ascenseur Otis Compass et spécifie l'ID unique du DEC Otis Compass. Cela doit correspondre au quatrième octet de l'adresse IP du DEC.
  - **Groupe d'étages** : Ce groupe d'étages définit tous les étages auxquels le DEC peut accéder. Lorsque les horaires attribués aux étages de ce groupe sont valides, les étages seront déverrouillés pour un accès libre.
  - **Numéro de groupe** : Cette information est fournie par le système d'ascenseur Otis Compass et doit correspondre au troisième octet de l'adresse IP du DEC.
  - **Mode d'opération DEC** : Cette fonction définit le mode d'opération DEC (celui-ci doit correspondre au mode fourni par le système d'ascenseur Otis Compass). Les modes suivants sont pris en charge :
    - **(1) Étage par défaut** : L'utilisateur présente ses informations d'identification au lecteur de carte ou saisit un code NIP sur un appareil DEC. Si les informations d'identification de l'utilisateur sont valides, le système de sécurité envoie l'étage par défaut de l'utilisateur au DEC. Si l'accès à l'étage est refusé, le DEC fournit un retour textuel ou sonore à l'utilisateur l'informant que la demande d'appel a été refusée.

      L'étage par défaut est défini comme **l'étage de destination de l'ascenseur** dans **Utilisateurs | Niveaux d'accès | Général**.

    - **(3) Entrée utilisateur de l'étage de destination** : Sans avoir besoin d'informations d'identification, l'utilisateur sélectionne son étage de destination. Si l'étage de destination est en accès libre, le DEC transmet la demande d'appel au DES. Si l'étage sélectionné n'est pas en accès libre, l'utilisateur est promptement invité à présenter ses informations d'identification.
    - **(4) Étage par défaut ou entrée utilisateur de l'étage de destination** : L'utilisateur présente ses informations d'identification et, si elles sont valides, son étage par défaut est envoyé au DEC. Dans un délai défini, l'utilisateur peut annuler la sélection de l'étage par défaut et choisir un autre étage de destination.

      L'étage par défaut est défini comme **l'étage de destination de l'ascenseur** dans **Utilisateurs | Niveaux d'accès | Général**.

- **MCE** : Pour plus de renseignements, consulter la Note d'application 241 : Protege GXintégration HLI MCE.

- **Type de panneau opérateur** : Définit si cette porte sera configurée comme un DOP (panneau de commande de destination) ou un COP (panneau de commande de voiture).
- **ID DOP/COP** : L'ID unique du DOP/COP qui a été configuré dans le système MCE.
- **Groupe d'étages** : Le groupe d'étages accessible depuis le DOP/COP. Cette fonction permet de déverrouiller des étages spécifiques selon l'horaire pour ce DOP/COP.
- **Étage** : Pour DOP seulement. Définit l'étage sur lequel se situe le kiosque.
- **Cabine d'ascenseur** : Pour COP seulement. Configure la cabine d'ascenseur du système MCE dans laquelle se trouve le lecteur de cabine.
- **DOP envoie un appel d'ascenseur** : Cette option permet aux tourniquets MCE d'envoyer un appel à l'interface MCE. Cette option doit être activée pour que les registres de portes fassent office de tourniquet. Elle doit être désactivée pour les kiosques normaux par palier.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Portes | Sorties

Sortie de verrouillage

- **Sortie / groupe de sorties programmables de verrouillage** : La sortie ou le groupe de sorties programmables qui contrôle le verrouillage physique de la porte. Il s'agit généralement des sorties relais du module d'expansion du lecteur, mais il peut s'agir de n'importe quelle sortie ou groupe de sorties programmables du système.
- **Temps d'activation du verrouillage** : Le temps de déverrouillage en secondes, c'est-à-dire le temps pendant lequel la sortie de verrouillage est activée lorsque la porte est déverrouillée. Si des sorties de verrouillage supplémentaires sont utilisées, cela contrôle le temps d'activation de la première sortie de verrouillage.

  En réglant le temps d'activation sur 0, l'état de la porte bascule entre verrouillée et porte déverrouillée maintenue lorsqu'elle est déverrouillée par un utilisateur ou un opérateur. Cependant, les fonctions REX et REN sont désactivées.

  Le temps d'activation du verrouillage maximal est de 255 secondes.
- **Activer les sorties de verrouillage supplémentaires** : Lorsque cette option est activée, les sorties de verrouillage supplémentaires 2-6 sont disponibles. Elles sont généralement utilisées lorsque plus d'une sortie de verrouillage commande le verrou de la porte ou lorsque des fonctions supplémentaires telles qu'une pompe de porte automatique sont nécessaires.

Sortie de verrouillage 2-6

Lorsque l'option **Activer les sorties de verrouillage supplémentaires** est activée, jusqu'à 5 sorties de verrouillage supplémentaires peuvent être programmées ci-dessous. La sortie de verrouillage standard s'active toujours en premier, et les sorties de verrouillage supplémentaires peuvent s'activer en même temps ou après un délai.

Il est recommandé de tester les minutages des sorties de verrouillage supplémentaires avec toutes les autres caractéristiques de verrouillage/déverrouillage utilisées sur le site (telles que les temps de déverrouillage prolongés ou les fonctions de reverrouillage) avant de les appliquer. En règle générale, les sorties de verrouillage sont toujours activées et désactivées dans le même ordre.

- **Sortie / groupe de sorties programmables de verrouillage 2-6** : La sortie ou le groupe de sorties programmables qui commande le verrou supplémentaire de la porte.
- **Temps d'activation du verrouillage 2-6** : La durée (en secondes) pendant laquelle la sortie de verrouillage supplémentaire reste activée lorsque la porte est déverrouillée.

Lorsqu'il est utilisé avec un temps de déverrouillage prolongé tel que le **Temps d'activation du REX** (onglet **Entrées**), l'option **Porte a prolongé temps d'accès** (onglet **Options avancées**) ou une action de calendrier de déverrouillage prolongé, les temps d'activation de tous les verrous sont prolongés (pas seulement le premier verrou).

Le temps d'activation du verrouillage maximal est de 255 secondes.

- **Délai avant l'activation du verrou 2-6** : Le délai (en secondes) entre l'activation de la première sortie de verrouillage et l'activation de cette sortie de verrouillage supplémentaire. Par exemple, si le délai pour la sortie de verrouillage 3 est réglé sur 5 secondes, lorsque l'accès est accordé, la première sortie de verrouillage s'active immédiatement et la sortie de verrouillage 3 s'active 5 secondes plus tard.

  Important : Tous les temps de **Délai avant activation** doivent être écoulés avant que toute autre sortie de serrure ne soit désactivée. Cela signifie que toutes les sorties doivent être activées avant que toutes les sorties ne soient désactivées.

Sortie pré-alarme

- **Sortie / groupe de sorties programmables de pré-alarme** : La porte génère une pré-alarme lorsqu'une porte est laissée ouverte, afin de prévenir les utilisateurs que l'alarme de porte laissée ouverte sera bientôt activée. La sortie ou le groupe de sorties programmables de pré-alarme est activé(e) lorsque le **Temps de délai de pré-alarme de la porte** (onglet **Général**) est atteint.

  Cette fonction peut être désactivée dans des circonstances spécifiques dans l'onglet **Options d'alarme**.

- **Temps d'impulsion on/off de pré-alarme** : Ces champs sont utilisés pour faire en sorte que la sortie ou le groupe de sorties programmables de pré-alarme passe en impulsion on/off à l'activation.

  La sortie ou le groupe de sorties s'activera pendant le temps de pulsion on, s'éteindra pendant le temps de pulsion off, puis se répétera. Ces durées sont définies par incréments de 100ms. Par exemple, si le temps d'activation de l'impulsion est réglé sur 2 et que le temps de désactivation de l'impulsion est réglé sur 8, la sortie s'activera pendant 200 ms, s'éteindra pendant 800 ms, puis se répétera, pour un cycle total de 1 seconde.

  Si l'une ou l'autre des durées d'activation et de désactivation de l'impulsion est définie sur 0, la sortie s'activera en continu. Chacun de ces champs prend en charge une valeur maximale de 255 (25,5 secondes).

Sortie porte laissée ouverte

- **Sortie / groupe de sorties programmables d'alarme laissée ouverte** : Lorsqu'une porte est laissée ouverte trop longtemps, une alarme de porte laissée ouverte est générée pour demander aux utilisateurs de fermer la porte immédiatement. La sortie ou le groupe de sorties programmables d'alarme laissée ouverte est activé(e) lorsque le **Temps d'alarme de la porte laissée ouverte** (onglet **Général**) est atteint.

  Par ailleurs, lorsque l'alarme est générée, l'entrée trouble Porte laissée ouverte est ouverte.

  Cette fonction peut être désactivée dans des circonstances spécifiques dans l'onglet **Options d'alarme**.

- **Temps d'impulsion on/off d'alarme laissée ouverte** : Ces champs sont utilisés pour faire en sorte que la sortie ou le groupe de sorties programmables d'alarme laissée ouverte passe en impulsion on/off à l'activation.

  La sortie ou le groupe de sorties s'activera pendant le temps de pulsion on, s'éteindra pendant le temps de pulsion off, puis se répétera. Ces durées sont définies par incréments de 100ms. Par exemple, si le temps d'activation de l'impulsion est réglé sur 2 et que le temps de désactivation de l'impulsion est réglé sur 8, la sortie s'activera pendant 200 ms, s'éteindra pendant 800 ms, puis se répétera, pour un cycle total de 1 seconde.

  Si l'une ou l'autre des durées d'activation et de désactivation de l'impulsion est définie sur 0, la sortie s'activera en continu. Chacun de ces champs prend en charge une valeur maximale de 255 (25,5 secondes).

Sortie porte forcée ouverte

- **Sortie / groupe de sorties programmables forcée ouverte** : Lorsqu'une porte est ouverte de force sans aucun accès, une alarme de porte forcée est générée. La sortie ou le groupe de sorties programmables forcée ouverte est immédiatement activé(e).

  Par ailleurs, lorsque l'alarme est générée, l'entrée trouble Porte laissée ouverte, forcée... est ouverte.

  Cette fonction peut être désactivée dans des circonstances spécifiques dans l'onglet **Options d'alarme**.

- **Temps d'impulsion on/off de porte ouverte de force** : Ces champs sont utilisés pour faire en sorte que la sortie ou le groupe de sorties programmables forcée ouverte passe en impulsion on/off à l'activation.

  La sortie ou le groupe de sorties s'activera pendant le temps de pulsion on, s'éteindra pendant le temps de pulsion off, puis se répétera. Ces durées sont définies par incréments de 100ms. Par exemple, si le temps d'activation de l'impulsion est réglé sur 2 et que le temps de désactivation de l'impulsion est réglé sur 8, la sortie s'activera pendant 200 ms, s'éteindra pendant 800 ms, puis se répétera, pour un cycle total de 1 seconde.

  Si l'une ou l'autre des durées d'activation et de désactivation de l'impulsion est définie sur 0, la sortie s'activera en continu. Chacun de ces champs prend en charge une valeur maximale de 255 (25,5 secondes).

Portes | Sorties de fonction

Pour plus de renseignements et d'instructions de programmation, consulter la Note d'application 336 : Programmer des sorties de fonction dans Protege GX et Protege WX.

Sortie de fonction 1-3

- **Sortie / groupe de sorties programmables de fonction 1-3** : Cette sortie ou ce groupe de sorties programmables est activé lorsque la porte est déverrouillée. Jusqu'à trois sorties de fonction peuvent être programmées pour chaque porte, fonctionnant indépendamment. Celles-ci peuvent être utilisées pour activer des mécanismes ou une logique supplémentaires lorsque la porte est déverrouillée, comme des shunts de contournement ou des pompes de porte automatiques.

  Par défaut, les sorties de fonction sont activées pendant le temps d'activation défini lorsque la porte est déverrouillée par une méthode quelconque. Les options ci-dessous peuvent modifier ce comportement.

- **Temps d'activation de fonction 1-3** : La durée (en secondes) pendant laquelle la sortie de fonction est activée lorsque la porte est déverrouillée. Lorsque le temps d'activation est réglé sur 0, la sortie de fonction est activée indéfiniment.

  Lorsque le loquet de la porte est déverrouillé, la sortie de fonction est activée jusqu'à ce que la porte soit à nouveau verrouillée. Après le verrouillage de la porte, la sortie de fonction reste activée pendant le temps d'activation programmé, puis est désactivée.

  Le temps d'activation maximum des sorties de fonction est de 86400 secondes (24 heures).

  Ce réglage a priorité sur le **Temps d'activation** défini dans la programmation de la sortie.

- **Activer lors de l'accès** : Lorsque cette option est activée, la sortie de fonction n'est activée que lorsque la porte est déverrouillée par l'accès. Elle n'est pas activée lorsque la porte est déverrouillée par d'autres méthodes telles que l'horaire, la partition ou la fonction programmable.

  Cette option peut être associée à l'option **Activer sur REX/REN** ci-dessous.

- **Activer sur REX/REN** : Lorsque cette option est activée, la sortie de fonction n'est activée que lorsque la porte est déverrouillée par REX ou REN. Elle n'est pas activée lorsque la porte est déverrouillée par d'autres méthodes telles que l'horaire, la partition ou la fonction programmable.

  Cette option peut être associée à l'option **Activer sur lors de l'accès** ci-dessus.

- **Désactiver à l'ouverture de la porte** : Lorsque cette option est activée, la sortie de fonction est désactivée immédiatement lorsque la porte est ouverte. Si la porte n'est pas ouverte, la sortie se désactive quand même après le temps d'activation normal.

  Cette fonction ne fonctionne pas lorsque le loquet de la porte est déverrouillé.

- **Désactiver à la fermeture de la porte** : Lorsque cette option est activée, la sortie de fonction est désactivée immédiatement lorsque la porte est fermée. Si la porte n'est pas fermée, la sortie se désactive quand même après le temps d'activation normal.

  Cette fonction ne fonctionne pas lorsque le loquet de la porte est déverrouillé.

- **Réenclencher le temps lors de l'accès** : Lorsque cette option est activée, le fait de déverrouiller à nouveau la porte par l'accès lorsque la sortie de fonction est toujours activée réinitialise le temps d'activation de la sortie de fonction. Cela permet aux utilisateurs de prolonger la durée d'activation de la sortie de fonction.

  L'option **Activer lors de l'accès** doit être activée pour utiliser cette fonction. Vous devez également saisir la commande `RecycleDoorTimeOnAccess = true` dans l'onglet **Général**.

- **Réenclencher le temps sur REX/REN** : Lorsque cette option est activée, le fait de déverrouiller à nouveau la porte sur REX lorsque la sortie de fonction est toujours activée réinitialise le temps d'activation de la sortie de fonction. Cela permet aux utilisateurs de prolonger la durée d'activation de la sortie de fonction.

  L'option **Activer sur REX/REN** doit être activée pour utiliser cette fonction. Les options **Toujours permettre REX** et **Recycle temps REX** doivent également être activées dans l'onglet **Entrées**.

Portes | Entrées

Options d'entrée de porte

- **Entrée du Contact de porte** : Cette entrée est utilisée pour détecter la position de la porte. Lorsque cette entrée est ouverte, l'état de la porte passe à « ouvert »; lorsque l'entrée est fermée, l'état de la porte passe à « fermé ».

  On parle également d'entrée reed, car un interrupteur reed est généralement utilisé pour cette fonction.

- **Inverser l'entrée de la porte** : Lorsque cette option est activée, le fonctionnement de l'entrée du Contact de porte est inversé. Lorsque l'entrée est fermée, la porte est considérée comme ouverte. Lorsque l'entrée est ouverte, la porte est considérée comme fermée.

  Note : Si le paramètre **Type de contact** (**Programmation | Entrées | Options**) est réglé sur Normalement ouvert, il n'est pas nécessaire d'inverser également l'entrée ici.

Options entrée REX

- **Entrée du détecteur REX** : Cette entrée est utilisée pour la fonction REX (demande de sortie). Lorsqu'un utilisateur active cette entrée, celle-ci génère une demande de sortie et de déverrouillage de la porte. Lorsque la porte est déverrouillée par REX, elle utilise le **Temps d'activation du verrouillage** standard, à moins que l'option **Temps de REX différent du temps de verrou** ait été activée ci-dessous.

  Le REX est généralement utilisé dans les situations où une porte dispose de lecteurs d'entrée mais pas de lecteurs de sortie. Les entrées du détecteur REX sont généralement des boutons, et ont donc généralement un **Type de contact** normalement ouvert (**Programmation | Entrées | Options**).

  L'option **Déverrouiller la porte sur requête de sortie** doit être activée dans l'onglet **Options**.

- **Inverser l'entrée REX** : Lorsque cette option est activée, le fonctionnement de l'entrée REX est inversé. Lorsque l'entrée est fermée (désactivée), une demande de sortie est générée.

  Note : Si le paramètre **Type de contact** (**Programmation | Entrées | Options**) est réglé sur Normalement ouvert, il n'est pas nécessaire d'inverser également l'entrée ici.

Options d'entrée de liaison

- **Entrée du détecteur de liaison** : Cette entrée est utilisée pour détecter la position du verrou de la porte. Lorsque cette entrée est ouverte, l'état de la porte devient « non verrouillé »; lorsque l'entrée est fermée, l'état de la porte devient « verrouillé » (en supposant que l'entrée du Contact de porte est également fermée).

  Les alarmes de porte laissée ouverte et de porte forcée peuvent être générées en fonction de la position de l'entrée du détecteur de liaison.

  Cette fonction peut être utilisée avec n'importe quel verrou qui dispose d'une surveillance de liaison ou de détection de verrou. Par exemple, un détecteur de liaison magnétique est un contact qui indique si la liaison magnétique entre l'électroaimant et la pince est complète.
- **Inverser l'entrée de la liaison** : Lorsque cette option est activée, le fonctionnement de l'entrée du détecteur de liaison est inversé. Lorsque l'entrée est fermée, la porte est considérée comme non verrouillée et inversement.

  Note : Si le paramètre **Type de contact** (**Programmation | Entrées | Options**) est réglé sur Normalement ouvert, il n'est pas nécessaire d'inverser également l'entrée ici.

Options entrée REN

- **Entrée du détecteur REN** : Cette entrée est utilisée pour la fonction REN (demande d'entrée). Lorsque l'utilisateur active l'entrée, celle-ci génère une demande d'entrée et de déverrouillage de la porte. Le **Temps d'activation du verrouillage** standard est utilisé.

  Le REN est généralement utilisé pour les portes qui permettent une entrée libre. Il est également possible de placer un bouton REN dans un poste de garde pour permettre aux gardes de déverrouiller une porte à distance. Les entrées du détecteur REN sont généralement des boutons, et ont donc généralement un **Type de contact** normalement ouvert (**Programmation | Entrées | Options**).

  L'option **Déverrouiller la porte sur requête d'entrée** doit être activée dans l'onglet **Options**.
- **Inverser l'entrée REN** : Lorsque cette option est activée, le fonctionnement de l'entrée du détecteur REN est inversé. Lorsque l'entrée est fermée (désactivée), une demande d'entrée est générée.

  Note : Si le paramètre **Type de contact** (**Programmation | Entrées | Options**) est réglé sur Normalement ouvert, il n'est pas nécessaire d'inverser également l'entrée ici.

Options d'entrée de faisceau

- **Entrée du détecteur de faisceau** : Cette entrée permet de s'assurer que les portes automatiques restent déverrouillées et ouvertes en cas d'obstruction du passage de la porte. Lorsque l'entrée du détecteur de faisceau est ouverte (alors que la porte est déjà ouverte), la porte est déverrouillée et le verrou est maintenu ouvert. Lorsque l'entrée est fermée, la ou les sorties de verrouillage restent activées pendant le **Temps d'activation du verrouillage** programmé (onglet **Sorties**) avant de s'éteindre à nouveau.

  Cette fonction est généralement utilisée avec les portes et portails automatiques qui utilisent une pompe de porte comme sortie de verrouillage. Cela permet à la porte de recommencer à s'ouvrir lorsqu'elle est sur le point d'entrer en collision avec un obstacle.

  L'entrée du détecteur de faisceau ne redémarre pas les minuteries de pré-alarme et d'alarme de porte laissée ouverte.
- **Inverser l'entrée de faisceau** : Lorsque cette option est activée, le fonctionnement de l'entrée du détecteur de faisceau est inversé. Lorsque l'entrée est fermée, la fonction faisceau est déclenchée.

  Note : Si le paramètre **Type de contact** (**Programmation | Entrées | Options**) est réglé sur Normalement ouvert, il n'est pas nécessaire d'inverser également l'entrée ici.

Options générales

- **Toujours permettre REX** : Lorsque cette option est activée, la porte traite une demande de sortie même si la porte est déjà ouverte. Cela active le verrou mais ne réinitialise pas les alarmes de porte forcée ou de porte ouverte trop longtemps. Lorsque cette option est désactivée, la fonction REX ne fonctionne que lorsque la porte est fermée.

  Cette option est utile lorsque la sortie de verrouillage commande un ouvre-porte automatique. Cela permet à la porte de s'ouvrir à nouveau si l'on appuie sur le REX alors qu'elle est en train de se fermer; cependant, certains verrous, comme les verrous magnétiques, doivent rester verrouillés lorsque la porte est ouverte pour éviter que la porte ne « rebondisse » à la fermeture.
- **Recycler temps d'ouverture de porte sur REX** : Lorsque cette option est activée, les utilisateurs peuvent appuyer sur l'entrée du détecteur REX lorsque la porte est ouverte pour réinitialiser la durée pendant laquelle elle peut être laissée ouverte. Si la pré-alarme s'est déclenchée, le fait d'appuyer sur le bouton REX l'arrête; cependant, si l'alarme de porte laissée ouverte a déjà été activée, le fait d'appuyer sur le bouton REX ne réinitialise pas la minuterie.

  Par exemple, si le **Temps d'alarme de la porte laissée ouverte** est réglé sur 45 secondes, le fait d'appuyer sur le bouton REX pendant cette période réinitialise la minuterie, permettant à la porte d'être ouverte pendant 45 secondes supplémentaires.

  L'option **Toujours permettre REX** doit aussi être activé.
- **Porte forcée envoie porte ouverte** : Lorsque cette option est activée, lorsque la porte est ouverte de force (c'est-à-dire ouverte sans être déverrouillée), elle est traitée comme un état « porte ouverte ». Lorsque cette option est désactivée, l'état de porte forcée est traité normalement.

  Cela peut être utilisé dans les situations où la porte peut être ouverte sans être contrôlée par le contrôleur. Par exemple, certaines portes sont équipées d'une clé physique permettant de déverrouiller manuellement la porte, ce qui provoquerait normalement une alarme de porte forcée.
- **Recycle temps REX** : Lorsque cette option est activée, le fait d'appuyer sur le bouton REX alors que la porte est déverrouillée par REX réinitialise le temps d'activation du verrouillage afin que la porte reste déverrouillée plus longtemps.

  Par exemple, si le **Temps d'activation du verrouillage** est réglé sur 5 secondes, le fait d'appuyer sur le bouton REX pendant cette période réinitialise la minuterie, permettant au verrou de rester ouvert pendant 5 secondes supplémentaires.

  Cette fonction ne s'applique que lorsque la porte a été déverrouillée par REX. L'option **Toujours permettre REX** doit aussi être activé.
- **Maintenir le REX** : Lorsque cette option est activée, la porte reste déverrouillée tant que le bouton REX est maintenu enfoncé. Lorsque le bouton REX est relâché, la porte se verrouille à nouveau après le temps d'activation du REX. Le fait de maintenir le bouton REX enfoncé empêche également la minuterie de porte laissée ouverte de démarrer, de sorte que la porte peut être maintenue ouverte indéfiniment sans activer d'alarme.
- **Pulser le bip du lecteur sur REX** : Lorsque cette option est activée, les lecteurs associés à la porte émettent deux bips lorsqu'on appuie sur le bouton REX. Lorsque cette option est désactivée, il n'y a pas de réponse audible de la fonction de demande de sortie.
- **Temps de REX différent du temps de verrou** : Par défaut, le temps d'activation du REX est le même que le **Temps d'activation du verrouillage** (onglet **Sorties**). Avec cette option activée, le **Temps d'activation du REX** peut être configuré séparément et a priorité sur le temps d'activation du verrouillage lorsque le bouton REX est pressé.

  Par exemple, si le temps d'activation du verrouillage est de 5 secondes et le temps d'activation du REX de 10 secondes, lorsqu'un utilisateur badge pour entrer dans une pièce, la porte se déverrouille pendant 5 secondes; lorsqu'il appuie sur le bouton REX pour sortir, la porte se déverrouille pendant 10 secondes.
- **Temps d'activation du REX** : Si l'option **Temps de REX différent du temps de verrou** est activée ci-dessus, ce champ définit la durée pendant laquelle le verrou de la porte est activée lorsque le bouton REX est pressé.

  Le temps d'activation du REX ne peut pas être réglé sur 0.

Portes | Options

Options de portes

- **Toujours vérifier horaire de déverrouillage** : Activez cette option pour que le loquet de la porte se déverrouille lorsque **l'horaire de déverrouillage** est valide, et se verrouille lorsque le programme n'est pas valide. Pendant que l'horaire est valide, la porte se déverrouille immédiatement si elle est verrouillée par une autre fonction. Cela évite que la porte soit verrouillée manuellement alors qu'elle devrait être déverrouillée.

  Vous pouvez utiliser cette option avec **Horaire a priorité sur le loquet** pour empêcher également de déverrouiller le loquet de la porte lorsque l'horaire n'est pas valide.

  L'utilisation des options **Empêcher déverrouillage sur horaire si partition intérieure / partition extérieure zone armée** en conjonction avec ce paramètre empêchera la porte de se déverrouiller tant que l'horaire est valide, mais ne reverrouille pas la porte lorsque la zone est armée. Pour cela, utilisez plutôt **Partition désarmée ET horaire valide déverrouillage porte**.
- **Activer événements ouvert/fermé sur l'horaire** : Par défaut, lorsque la porte est déverrouillée ou verrouillée par l'horaire de déverrouillage, un événement est enregistré. Vous pouvez désactiver cette option pour éviter que ces événements réguliers ne soient enregistrés, ce qui permet d'économiser de l'espace dans la base de données d'événements.
- **Reverrouiller sur fermeture de porte** : Si cette option est activée, le verrou se reverrouille dès que la porte se ferme. Si la porte n'est pas fermée, le verrou se désactive quand même après le temps d'activation du verrouillage normal.
- **Verrouillage sur porte ouverte** : Lorsque cette option est activée, le verrou se reverrouille dès que la porte s'ouvre. Si la porte n'est pas ouverte, le verrou se désactive quand même après le temps d'activation du verrouillage normal.
- **Déverrouiller la porte sur requête de sortie** : Lorsque cette option est activée, l'ouverture de **l'entrée du détecteur REX** (définie dans l'onglet **Entrées**) déverrouille la porte.

  Lorsque cette option est désactivée, la porte ne se déverrouille pas automatiquement lorsque l'entrée du détecteur REX est actionnée, mais entre temporairement dans un état de « sortie libre », supprimant les alarmes de porte forcée pendant le temps d'activation normal du REX. Cela permet d'utiliser des verrous à mortaise avec une poignée de sortie libre qui déverrouille mécaniquement la porte.
- **Déverrouiller la porte sur requête d'entrée** : Lorsque cette option est activée, **l'entrée du détecteur REN** (définie dans l'onglet **Entrées**) peut être utilisée pour déverrouiller la porte en utilisant la fonction de demande d'entrée. Désactivez cette option pour désactiver le processus REN pour cette porte.
- **Horaire fonctionne en retard pour ouvrir** : Lorsque cette option est activée, le loquet de la porte ne se déverrouille pas lorsque l'horaire est valide jusqu'à ce qu'un utilisateur ou un opérateur déverrouille la porte. Cela peut être utilisé pour éviter le déverrouillage automatique de la porte les jours où personne ne se rend sur le site.

  Cette option a priorité sur l'option **Toujours vérifier horaire de déverrouillage** ci-dessus. Pour que la porte se verrouille lorsque l'horaire n'est pas valide, activez également l'option **Horaire a priorité sur le loquet** ci-dessous.

Options de portes 2

- **Le verrouillage de la porte suit la partition intérieure/extérieure** : Activez l'une de ces options pour choisir si la **Partition à l'intérieur de la porte** ou la **Partition à l'extérieur de la porte** (onglet **Général**) doit être utilisée avec les options de contrôle de partition ci-dessous.
- **Empêcher déverrouillage esclave sur partition intérieure** : Si une **Porte esclave** est définie dans l'onglet **Général**, par défaut, la porte esclave suit toujours l'état de la porte principale lorsqu'elle se déverrouille à l'accès. Cette option empêche la porte esclave de suivre la porte principale lorsque la partition intérieure de la porte esclave est armée, ce qui évite les fausses alarmes. Cette option doit être activée dans la programmation de la porte esclave.

Cette fonction ne fonctionne pas avec la commande `SlaveREX = true`. Lorsque la porte principale est déverrouillée par des commandes REX, REN ou manuelles, la porte esclave est déverrouillée quel que soit l'état de la partition.

- **Empêcher le déverrouillage sur horaire si la partition intérieure/extérieure est armée** : Lorsqu'une de ces options est activée, si l'horaire de déverrouillage devient valide mais que la partition intérieure ou extérieure de la porte est toujours armée, la porte ne se déverrouille pas. Cela peut être utilisé pour empêcher le déverrouillage d'une porte les jours où personne ne vient désarmer la partition.
- **Partition désarmée ET horaire valide déverrouillage porte** : Lorsque cette option est activée, le loquet de la porte se déverrouille automatiquement lorsqu'à la fois l'horaire de déverrouillage est valide et la partition concernée est désarmée. Lorsque l'horaire n'est pas valide ou que la partition est armée, la porte se verrouille automatiquement.

  Si le loquet de la porte est déverrouillé ou verrouillé par une autre fonction, il est immédiatement remis dans l'état correct.

  La zone concernée est déterminée par les options **Le verrouillage de porte suit la zone intérieure** ou **Le verrouillage de porte suit la zone extérieure** ci-dessus.
- **Partition désarmée OU horaire valide déverrouillage porte** : Lorsque cette option est activée, le loquet de la porte se déverrouille automatiquement soit lorsque l'horaire de déverrouillage est valide, soit lorsque la partition concernée est désarmée. Lorsque l'horaire n'est pas valide et que la partition est armée, la porte se verrouille automatiquement.

  Si le loquet de la porte est déverrouillé ou verrouillé par une autre fonction, il est immédiatement remis dans l'état correct.

  La zone concernée est déterminée par les options **Le verrouillage de porte suit la zone intérieure** ou **Le verrouillage de porte suit la zone extérieure** ci-dessus.
- **Activer accès pris sur événements de requête de sortie/requête d'entrée** : Si cette option est activée, lorsqu'un REX ou un REN est enregistré à la porte, le système enregistre si l'accès demandé a été pris ou non. Par exemple, si le bouton REX est pressé et que la porte est ensuite ouverte, un événement « Demande de sortie prise » est enregistré. Si la porte n'est pas ouverte, un événement « Demande de sortie non prise » est enregistré.
- **Horaire a priorité sur le loquet** : Avec cette option activée, la porte se verrouille automatiquement lorsque l'horaire de déverrouillage n'est pas valide. Par ailleurs, si l'option **Toujours vérifier horaire de déverrouillage** est également activée, si le loquet de la porte est déverrouillé par une autre fonction, il est immédiatement reverrouillé par l'horaire. Cela évite que le loquet de la porte soit verrouillé manuellement alors qu'il devrait être déverrouillé.

Portes | Options avancées

Options avancées

- **Mettre à jour partition de l'utilisateur lorsque passback désactivé** : Par défaut, sauf si l'anti-passback est activé, le système ne suit pas la partition dans laquelle se trouve un utilisateur lorsqu'il franchit la porte. Lorsque cette option est activée, le contrôleur met à jour la partition dans laquelle se trouve l'utilisateur même si l'anti-passback est désactivé sur cette porte. Cette fonction est utile sur les sites où certaines portes ont l'anti-passback activé mais d'autres non.

  Il n'y a pas de connexion à l'option **Partition de l'utilisateur** configurée dans **Utilisateurs | Utilisateurs | Général**.
- **Déverrouiller requête de sortie lorsque partition intérieure armée** : Lorsque cette option est activée, la porte refuse toute demande de sortie faite lorsque la partition intérieure a été armée. Cela peut permettre d'empêcher les personnes de sortir d'une partition armée. Les utilisateurs peuvent toujours sortir avec des informations d'identification valides.
- **Refuser l'entrée si partition intérieure est armée** : Lorsque cette option est activée, la porte refuse l'entrée à tous les utilisateurs lorsque la partition intérieure de la porte est armée.

Cette option a priorité sur l'option **Désactiver la partition pour la porte sur accès** dans la programmation **Modules d'expansion | Modules d'expansion du lecteur | Lecteur 1/2**, de sorte que les utilisateurs seront verrouillés même s'ils ont accès au désarmement de la partition.

- **Refuser la sortie si partition extérieure est armée** : Lorsque cette option est activée, la porte refuse l'entrée à tous les utilisateurs lorsque la partition extérieure de la porte est armée.

  Cette option a priorité sur l'option **Désactiver la partition pour la porte sur accès** dans la programmation **Modules d'expansion | Modules d'expansion du lecteur | Lecteur 1/2**, de sorte que les utilisateurs seront verrouillés même s'ils ont accès au désarmement de la partition.

- **interroger l'utilisateur pour code de raison d'accès** : Lorsque cette option est activée, les utilisateurs qui demandent l'accès à la porte doivent saisir un code de motif d'accès sur un clavier associé avant que la porte ne soit déverrouillée.

  Lorsque l'utilisateur badge sa carte, le clavier lui demande de saisir une Partition comprise entre 001 et 009, puis d'appuyer sur **[Enter]**. Lorsqu'ils le font, l'accès est accordé et un événement est enregistré dans le format : « Utilisateur a déverrouillé la porte par Type[XX] ». Le code Type de l'événement correspond au code motif de la Partition moins 1, de sorte que les codes Partition 001-009 correspondent au Type 00-08.

  L'utilisation de cette fonction nécessite les paramètres suivants dans la programmation **Modules d'expansion | Modules d'expansion du lecteur | Lecteur 1/2** :

  - **Type de clavier du lecteur 1/2** : Clavier ACL
  - **Clavier à utiliser pour NIP du lecteur 1/2** : Sélectionnez un clavier à proximité de la porte

  Cette fonction n'est pas prise en charge avec l'opération carte et NIP.

- **Activer l'accès pris sur les événement de déverrouillage de portes** : Si cette option est activée, lorsqu'un utilisateur se voit accorder l'accès à la porte, le système enregistre si l'accès demandé a été pris ou non. Par exemple, si une carte est badgée et que la porte est ensuite ouverte, un événement « Accès pris » est enregistré. Si la porte n'est pas ouverte, un événement « Accès non pris » est enregistré.

  Lorsque cette option n'est pas activée, le système n'indique pas si l'accès a été pris ou non.

Options de temps d'accès prolongé

Les options d'anti-passback ci-dessous s'appliquent lorsque le type de porte associé à la porte a des paramètres d'anti-passback configurés (**Programmation | Types de portes | Général**).

- **Porte a prolongé temps d'accès** : La durée (en secondes) pendant laquelle la porte reste déverrouillée pour les utilisateurs qui ont besoin de temps d'accès prolongés. Ceci a priorité sur le **Temps d'activation du verrouillage** pour tous les utilisateurs dont l'option **Utilisateur opère la fonction d'accès de porte prolongé** est activée (**Utilisateurs | Utilisateurs | Options**).
- **Temps de réinitialisation de l'utilisateur de l'entrée/sortie de l'anti-passback** : Si l'option **Permettre réinitialisation de l'anti-passback chronométré de l'utilisateur** est activée ci-dessous, ces champs définissent la période (en minutes) de réinitialisation de l'état de l'anti-passback de tous les utilisateurs qui sont entrés ou sortis par la porte.
- **Réinitialiser statut anti-passback sur l'horaire** : Si cette option est activée, l'état de l'anti-passback de tous les utilisateurs qui ont accédé à cette porte est réinitialisé chaque fois que **l'Horaire de réinitialisation anti-passback** ci-dessous change d'état (c'est-à-dire qu'il devient valide ou non valide).
- **Permettre réinitialisation de l'anti-passback chronométré de l'utilisateur** : Avec cette option activée, l'état d'anti-passback de tous les utilisateurs qui ont accédé à cette porte est réinitialisé régulièrement. La période est définie dans les champs **Temps de réinitialisation de l'utilisateur d'entrée/sortie de l'anti-passback** ci-dessus.

  Par exemple, si le temps de réinitialisation de l'entrée est réglé sur 120 minutes, le système réinitialise le statut anti-passback de tous les utilisateurs qui ont franchi la porte pendant cette période toutes les deux heures.
- **Horaire de réinitialisation anti-passback** : Si l'option **Réinitialiser statut anti-passback sur l'horaire** est activée, ce champ définit l'horaire utilisé pour réinitialiser l'état de l'anti-passback.

Portes | Options d'alarmes

Pour configurer les sorties utilisées par les alarmes ci-dessous, voir l'onglet **Sorties**.

Options de pré-alarme

- **Activer les événements pré-alarme** : La pré-alarme de porte est activée lorsque la porte est laissée ouverte pendant le **Temps de délai de pré-alarme de la porte**, activant une sortie pour avertir les utilisateurs que l'alarme de porte laissée ouverte est sur le point d'être activée. Désactivez cette option pour désactiver la fonction de pré-alarme pour cette porte.
- **Désactiver pendant le calendrier de déverrouillage** : Activez cette option pour désactiver la pré-alarme de porte lorsque le loquet de la porte a été déverrouillé par un horaire de déverrouillage.
- **Désactiver pendant les commandes manuelles** : Activez cette option pour désactiver la pré-alarme de porte lorsque la porte a été déverrouillée par loquet par un opérateur à l'aide d'une commande manuelle. La pré-alarme s'active toujours lorsque la porte a été déverrouillée (c'est-à-dire temporairement déverrouillée) par une commande manuelle.
- **Désactiver pendant les actions de calendrier** : Activez cette option pour désactiver la pré-alarme de porte lorsque le loquet de la porte a été déverrouillé par une action de calendrier.
- **Désactiver lorsque déverrouillé par partition** : Activez cette option pour désactiver la pré-alarme de porte lorsque le loquet de la porte a été déverrouillé par une partition (par exemple, à l'aide de l'option **Partition désarmée OU horaire valide déverrouillage porte** dans l'onglet **Options**).
- **Désactiver lorsque déverrouillé par fonction programmable** : Activez cette option pour désactiver la pré-alarme de porte lorsque le loquet de la porte a été déverrouillé par une fonction programmable.
- **Désactiver lorsque déverrouillé par déverrouillage incendie** : Activez cette option pour désactiver la pré-alarme de porte lorsque le loquet de la porte a été déverrouillé par une fonction programmable dans le **Mode de contrôle de porte** 2 - Déverrouiller porte de contrôle d'incendie.
- **Calendrier de fonctionnement de l'alarme** : La pré-alarme de la porte est activée lorsque cet horaire est valide et désactivée lorsque cet horaire n'est pas valide.

Options de porte laissée ouverte

- **Activer événements laissés ouverts** : L'alarme de porte laissée ouverte est activée lorsque la porte est laissée ouverte pour le **Temps d'alarme de la porte laissée ouverte**, activant une sortie et ouvrant l'entrée trouble de Porte laissée ouverte pour signaler l'alarme à la station de surveillance. Désactivez cette option pour désactiver toutes les fonctions d'alarme de porte laissée ouverte.

  Désactiver l'alarme de porte laissée ouverte ne désactive pas automatiquement la pré-alarme.

- **Désactiver pendant le calendrier de déverrouillage** : Activez cette option pour désactiver l'alarme de porte laissée ouverte lorsque la porte a été déverrouillée par un horaire de déverrouillage.
- **Désactiver pendant les commandes manuelles** : Activez cette option pour désactiver l'alarme ouverte gauche lorsque la porte a été déverrouillée par loquet par un opérateur à l'aide d'une commande manuelle. La pré-alarme s'active toujours lorsque la porte a été déverrouillée (c'est-à-dire temporairement déverrouillée) par une commande manuelle.
- **Désactiver pendant les actions de calendrier** : Activez cette option pour désactiver l'alarme de porte laissée ouverte lorsque le loquet de la porte a été déverrouillé par une action de calendrier.
- **Désactiver lorsque déverrouillé par partition** : Activez cette option pour désactiver l'alarme de porte laissée ouverte lorsque le loquet de la porte a été déverrouillé par une partition (par exemple, à l'aide de l'option **Partition désarmée OU horaire valide déverrouillage porte** dans l'onglet **Options**).
- **Désactiver lorsque déverrouillé par fonction programmable** : Activez cette option pour désactiver l'alarme de porte laissée ouverte lorsque le loquet de la porte a été déverrouillé par une fonction programmable.
- **Désactiver lorsque déverrouillé par déverrouillage incendie** : Activez cette option pour désactiver l'alarme de porte laissée ouverte lorsque le loquet de la porte a été déverrouillé par une fonction programmable dans le **Mode de contrôle de porte** 2 - Déverrouiller porte de contrôle d'incendie.

- **Calendrier de fonctionnement de l'alarme** : L'alarme de porte laissée ouverte est activée lorsque cet horaire est valide et désactivée lorsque cet horaire n'est pas valide.

Options ouvert de force

L'opération de porte forcée peut également être retardée par des commandes. Pour plus de renseignements, consulter la Note d'application 304 : Commandes de retardement de porte forcée.

- **Activer les alarmes d'ouverture forcée** : L'alarme de porte forcée est activée lorsque la porte est forcée, activant une sortie et ouvrant l'entrée trouble de Porte laissée ouverte, forcée... pour signaler l'alarme à la station de surveillance. Désactivez cette option pour désactiver toutes les fonctions d'alarme de porte forcée pour cette porte (bien que la porte ait toujours le statut « Porte forcée » sur un plan d'étage ou une page du statut).

  Vous pouvez également consulter l'option **Porte forcée envoie porte ouverte** (onglet **Entrées**).

- **Calendrier de fonctionnement de l'alarme** : L'alarme de porte forcée est activée lorsque cet horaire est valide et désactivée lorsque cet horaire n'est pas valide.

Portes | Codes de fonction

Les codes de fonction peuvent être créés dans **Sites | Codes de fonction**. Pour plus de renseignements, consulter la Note d'application 240 : Codes de fonction dans Protege GX.

Options des codes de fonction

Ajoutez un code de fonction à la porte en cliquant sur **Ajouter**. Vous pouvez configurer la **Direction** du code de fonction pour spécifier le(s) lecteur(s) pouvant être utilisé(s) pour l'activer : Entrée, Sortie ou Entrée/Sortie.

La porte doit être affectée au module d'expansion du lecteur auquel le lecteur est connecté. Les codes de fonction ne fonctionneront pas correctement si la **porte lecteur 1/2** <non réglé>. Pour les lecteurs tiers et OSDP qui nécessitent une fiche de lecteur intelligent pour la configuration, en plus de l'onglet **Lecteur** de la fiche de lecteur intelligent, la porte doit également être affectée dans l'onglet **Lecteur 1/2** du port de lecteur auquel le lecteur est physiquement connecté.

Commandes manuelles des portes

Un clic droit sur un registre de porte dans **Programmation | Portes** ou sur une icône de porte sur un plan d'étage ou une page du statut ouvre un menu avec des commandes manuelles pour cette porte.

Contrôle de portes

Ces commandes vous permettent de contrôler les fonctionnalités de base de la porte. Les commandes disponibles sont les suivantes :

- **Verrouiller**
- **Déverrouiller** (activer temporairement le verrou)
- **Porte déverrouillée maintenue** (activer le verrou et laisser la porte déverrouillée)

Verrouillage de porte

Ces commandes vous permettent de verrouiller des portes individuelles. Toute commande de verrouillage verrouille la porte indépendamment de toute autre fonction entraînant son déverrouillage. Certains modes de verrouillage permettent l'entrée ou la sortie avec des informations d'identification valides ou REX/REN, tandis que d'autres refusent l'accès. Les commandes disponibles sont les suivantes :

- **Permettre l'entrée**
- **Permettre la sortie**
- **Permettre l'entrée et la sortie**

- **Refuser l'entrée et la sortie**
- **Effacer** (retirer le verrouillage de la porte)

Pour établir des procédures de verrouillage automatique sur plusieurs portes, utilisez les fonctions programmables de **Contrôle de portes** (**Automatisation | Fonctions programmables**).

Afficher les événements récents

Cette commande lance automatiquement une recherche d'événement dans une fenêtre en incrustation, montrant tous les événements récents pour cette porte.

Pour trier, grouper, filtrer et exporter ce rapport, voir Affichage des rapports (consultez la page 171).

Entrées

Les détecteurs de mouvement, les contacts de porte et autres appareils de détection numériques sont connectés au système en tant qu'entrées. Les entrées peuvent être programmées dans des partitions et surveillées pour protéger la partition contre les entrées non autorisées.

Cependant, les entrées ne se limitent pas à la détection d'intrusion et au contrôle de portes : elles peuvent également être utilisées pour le contrôle de sorties et l'automatisation. Comme chaque entrée peut être programmée dans un maximum de quatre partitions différentes, avec des types d'entrée différents dans chacune d'elles, une seule unité peut servir à plusieurs fins dans le système.

Par exemple, l'utilisation traditionnelle d'un PIR (détecteur de mouvement infrarouge) consiste à détecter les intrus lorsqu'une partition est armée; cependant, le PIR est tout aussi efficace pour détecter les mouvements des utilisateurs pendant les heures de travail. En programmant l'entrée dans une partition de contrôle (qui est toujours armée), la même entrée peut également être utilisée pour allumer des lumières lorsqu'un mouvement est détecté, ou pour armer automatiquement la partition lorsqu'il n'y a pas eu de mouvement pendant une période donnée.

Entrées | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Nom d'affichage du clavier** : Le nom qui sera téléchargé vers le contrôleur. Ce dernier sera affiché sur le clavier et dans les rapports des services de surveillance IP. Le clavier ne peut afficher que les 16 premiers caractères du nom. Il doit donc décrire de manière concise l'emplacement physique et la fonction de l'appareil.

Adresse

- **Type de module** : Le type de module auquel l'entrée est physiquement connectée (p. ex., contrôleur, module d'expansion d'entrée).
- **Adresse du module** : L'**adresse physique** du module auquel l'entrée est connectée.
- **Module entrée** : L'index de l'entrée sur le module connecté. Consulter le manuel d'installation correspondant pour les instructions de câblage.

Configuration

- **Sortie de contrôle / Groupe de sorties programmables** : Vous pouvez définir une sortie ou un groupe de sorties qui est contrôlé par cette entrée (contrôle « sortie suit entrée »), ce qui a une grande variété d'applications. Par exemple, vous pouvez configurer un interrupteur à clé qui déverrouille une porte spécifique (contrôle un à un) ou configurer un groupe de lumières pour qu'elles s'allument en appuyant sur le bouton REX (contrôle un à plusieurs).

  La relation entre l'état de l'entrée et l'état de la sortie doit être configurée dans la programmation du type d'entrée (**Programmation | Types d'entrée | Options (3) | Options de contrôle**).

  Vous pouvez également définir une **sortie de contrôle / un groupe de sorties** dans la programmation du type d'entrée, ce qui permet un contrôle de plusieurs à un et de plusieurs à plusieurs (**Programmation | Types d'entrée | Général**).

  > Pour cette méthode de contrôle des sorties, la partition programmée pour l'entrée doit être **armée**. Il est recommandé de créer une partition dédiée à l'utilisation des fonctions de contrôle de sorties.

- **Automatisation de contrôle** : Il s'agit d'une option héritée qui n'a aucun effet.

Le contrôle d'automatisation peut être programmé dans la configuration du type d'entrée.

- **Supporter commandes manuelles** : Lorsque cette option est activée, un opérateur disposant des autorisations adéquates peut envoyer des commandes manuelles à l'entrée. Par exemple, un garde pourrait cliquer avec le bouton droit de la souris sur une entrée d'un plan d'étage et la contourner.

  Pour plus d'informations, consultez la section Commandes des entrées manuelles (la page 225).

- **Signaler ID** : L'ID de signalement de l'entrée est le numéro de partition qui représentera cette entrée auprès de la station de surveillance. Chaque entrée nouvellement créée se verra automatiquement attribuer l'ID le plus bas disponible. Sinon, vous pouvez attribuer manuellement un ID à chaque entrée, ce qui permet une grande flexibilité dans le rapport des entrées. Par exemple, si deux entrées ont le même ID de signalement, elles seront toutes deux déclarées comme la même entrée.

  Si une entrée a été attribuée à un numéro supérieur au maximum qui peut être signalé à un service particulier, le numéro le plus élevé possible sera signalé. Les entrées et les entrées troubles partagent la même gamme de numéros de partition.

  Vous pouvez visualiser, réinitialiser et exporter les ID de signalement à l'aide du **générateur de cartes de signalisation** (**Signalements | Rapport de la station centrale**). Pour plus d'informations, voir la note d'application 316 : Rapports au format Contact ID dans Protege GX et Protege WX.

- **Vitesse d'entrée d'alarme** : Ce paramètre détermine la durée pendant laquelle une entrée doit être ouverte avant que le système n'enregistre qu'elle a été ouverte (mise sous alarme). Par exemple, si ceci est réglé sur 30 secondes, l'entrée doit être ouverte pendant 30 secondes avant qu'un événement « Entrée ouverte » ne soit généré.

  La vitesse d'entrée d'alarme peut être réglée entre 0 seconde et 1 heure. Des temps plus courts sont utiles pour les entrées qui nécessitent une réponse rapide, comme les boutons REX. Des délais plus longs peuvent être utilisés pour éviter que les alarmes ne soient déclenchées par de petits mouvements.

  Si la vitesse de l'entrée d'alarme est réglée sur 0 seconde, la vitesse de l'entrée de restauration ne peut pas être réglée en dessous de 100 ms.

  Une mise à jour du module sera nécessaire chaque fois que ce paramètre sera modifié. Si le contrôleur est enregistré en tant que module d'expansion du lecteur, cette option doit être définie dans la programmation de l'entrée du contrôleur, et non de l'entrée du module d'expansion du lecteur.

- **Restaurer la vitesse d'entrée** : Ce paramètre détermine la durée pendant laquelle une entrée doit être fermée avant que le système n'enregistre qu'elle a été fermée (restaurée). Par exemple, si ce temps est réglé sur 30 secondes, l'entrée doit être fermée pendant 30 secondes avant qu'un événement « Entrée fermée » ne soit généré.

  La vitesse d'entrée de restauration peut être réglée entre 0 seconde et 1 heure.

  Si la vitesse de l'entrée d'alarme est réglée sur 0 seconde, la vitesse de l'entrée de restauration ne peut pas être réglée en dessous de 100 ms.

  Une mise à jour du module sera nécessaire chaque fois que ce paramètre sera modifié. Si le contrôleur est enregistré en tant que module d'expansion du lecteur, cette option doit être définie dans la programmation de l'entrée du contrôleur, et non de l'entrée du module d'expansion du lecteur.

- **Activer lock-out de partition** : Lorsque cette option est activée, chaque fois que cette entrée déclenche une alarme, un compteur est incrémenté. Une fois que le compteur atteint le **Compte de lock-out de partition**, l'entrée est verrouillée et les activations ultérieures ne provoquent pas d'alarmes. Le verrouillage est réinitialisé lorsque la partition est désarmée et armée à nouveau. Cette fonctionnalité est utile pour les entrées qui déclenchent occasionnellement de fausses alarmes.
- **Compte de lock-out de partition** : Si cette entrée utilise la fonction **Activer lock-out de partition** ci-dessus, ce paramètre définit le nombre de fois que l'entrée peut activer l'alarme avant d'être verrouillée.

Commandes

- Ce champ est utilisé pour envoyer des commandes de programmation à l'appareil. Il ne doit être utilisé que lorsqu'il est spécifiquement conseillé par la documentation ICT ou le support technique.

Graphiques

- **Caméra** : L'association d'une caméra à une entrée vous permet de faire un clic droit sur n'importe quel événement de entrée dans une fenêtre d'événement pour ouvrir un flux de caméra archivé à l'heure de l'événement.
- **Plan d'étage** : L'association d'un plan d'étage à une entrée vous permet de faire un clic droit sur n'importe quelle entrée dans une fenêtre d'événement pour ouvrir le plan d'étage.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Entrées | Types de partitions et d'entrées

Une grande partie de la fonctionnalité d'une entrée est contrôlée par les partitions et les types d'entrée qui lui sont associés. Le type d'entrée décrit le fonctionnement de l'entrée dans chaque partition : par exemple, une entrée de contact de porte peut activer le délai d'entrée dans une partition et générer instantanément une alarme dans une autre. Les entrées peuvent être programmées dans quatre partitions différentes, ce qui permet d'utiliser la même entrée pour diverses fonctions de détection des intrusions, de contrôle et d'automatisation du système.

Les changements apportés aux paramètres de cet onglet peuvent nécessiter de désarmer et de réarmer les partitions concernées avant qu'ils ne soient pris en compte. Vous devez armer à nouveau à la fois la partie principale et la partie 24 heures de la partition. Le contrôleur génère un message d'état de santé si un réarmement est nécessaire.

Partitions attribuées

- **Partition 1-4** : La partition qui surveille cette entrée. Chaque entrée peut être programmée dans quatre partitions différentes au maximum et exécuter des fonctions différentes dans chacune d'elles.
- **Type d'entrée 1-4** : Le type d'entrée définit le mode de fonctionnement de l'entrée dans une partition particulière. Une grande variété d'options et de types d'entrées préconfigurées sont disponibles pour des fonctions telles que la détection d'intrusion, la détection de sabotage, la détection de fumée/feu et l'automatisation / le contrôle.

  Par exemple, le type d'entrée préconfiguré Instantané entraîne l'activation immédiate de l'alarme de partition lorsque l'entrée est ouverte, tandis que le type d'entrée Délai entraîne le démarrage du délai d'entrée de la partition. Pour en savoir plus, consulter **Programmation | Types d'entrée**.
- **DEL de l'entrée KLES 1 à 4** : Si un clavier Eclipse est utilisé dans cette partition, chaque entrée peut être programmée avec un index dans ce champ. Lorsqu'un utilisateur tente d'armer la partition, si l'entrée est ouverte, le numéro de DEL correspondant à cet index clignote pour indiquer quelle entrée empêche l'armement de la partition.

  Un index de 1 à 19 peut être attribué à l'entrée dans chaque partition. Le clavier indique les entrées supérieures à 9 en faisant clignoter la DEL 0 pour représenter le chiffre des dizaines.

Entrées | Options

Options 1

- **Enregistrer à la mémoire tampon de l'événement** : Lorsque cette option est activée (par défaut), l'entrée génère un événement lorsqu'elle est ouverte, fermée, altérée ou court-circuitée. Désactiver cette option pour empêcher de générer des événements de entrée. Le contrôleur continuera à signaler les alarmes, les restaurations et les altérations à la station de surveillance (comme configuré dans le type d'entrée).

  Il peut être utile de désactiver l'enregistrement des événements pour les entrées qui sont principalement utilisées pour l'automatisation ou le contrôle, afin de réduire leur incidence sur le stockage des événements.
- **Test pour condition de trouble** : Il s'agit d'une option héritée qui n'a aucun effet. Les conditions d'entrée trouble (altération et court-circuit) sont générées et signalées en fonction des paramètres du type d'entrée (voir **Générer des alarmes de 24 heures** et **Signaler sabotages** dans **Programmation | Types d'entrées | Options (1)**).
- **Contournement non permis** : Lorsque cette option est activée, l'entrée ne peut pas être contournée (de façon temporaire ou permanente) pour armer une partition. Cette option doit être utilisée pour les entrées de haute sécurité qui ne doivent pas être laissées ouvertes et non surveillées lorsqu'une partition est armée.

  Cette option n'empêche pas l'armement forcé de la zone lorsque l'entrée est ouverte. Pour éviter cela, assurez-vous que l'option **Entrée forcée** est désactivée dans le type d'entrée attribué (**Programmation | Types d'entrée | Options (1)**).
- **Contournement de verrouillage non permis**: Lorsque cette option est activée, l'entrée ne peut pas être contournée par verrouillage (c'est-à-dire contournée de façon permanente); cependant, elle peut être contournée temporairement jusqu'au prochain désarmement de la partition.

  Cette option n'empêche pas l'armement forcé de la zone lorsque l'entrée est ouverte. Pour éviter cela, assurez-vous que l'option **Entrée forcée** est désactivée dans le type d'entrée attribué (**Programmation | Types d'entrée | Options (1)**).
- **Sabotage suit l'état de contournement** : Avec cette option activée (par défaut), vous pouvez contourner une entrée altérée pour permettre l'armement de la partition. Avec cette option désactivée, la condition d'altération ne peut pas être contournée, vous ne pourrez donc pas armer une partition dont l'entrée a été altérée.
- **Aucun contournement si n'importe quelle partition est armée** : Lorsque cette option est activée, cette entrée ne peut pas être contournée si l'une des quatre prtitions attribuées dans l'onglet**Types de partitions et d'entrées** est armée.
- **Enregistrer l'événement d'entrée lorsque contournée** : Par défaut, si l'entrée est contournée, le système n'enregistre pas les événements lorsqu'elle change d'état (par exemple, s'ouvre ou se ferme). Avec cette option activée, les événements seront consignés même si l'entrée est contournée.
- **Falsifier l'entrée si module hors ligne** : Lorsque cette option est activée, si le module d'expansion passe hors ligne, le contrôleur signale que l'entrée présente une condition d'altération. Cela ne se produit que si le module a été préalablement enregistré et mis en ligne avec le contrôleur.

Options 2

- **Entrée Fin de ligne (EOL)** : La configuration de la résistance EOL utilisée dans le câblage physique de cette entrée doit être saisie ici. Cela détermine si le système peut surveiller les conditions de sabotage et de court-circuit, ainsi que les conditions d'ouverture et de fermeture. Consulter le manuel d'installation pertinent pour connaître les configurations de résistance EOL compatibles.

  Une mise à jour du module sera nécessaire chaque fois que ce paramètre sera modifié. Si le contrôleur est enregistré en tant que module d'expansion du lecteur, cette option doit être définie dans la programmation de l'entrée du contrôleur, et non de l'entrée du module d'expansion du lecteur.
- **Type de contact** : Le type de contact utilisé dans le câblage physique de cette entrée doit être saisi ici. Les entrées peuvent être câblées normalement fermées (par défaut) ou normalement ouvertes. Ce paramètre détermine comment l'entrée sera traitée par le système.

Par exemple, les entrées REX (boutons) sont généralement câblées avec un contact normalement ouvert. Avec ce champ réglé sur Normalement ouvert, lorsque le bouton n'est pas pressé, l'entrée sera marquée comme Fermée/Désactivée et lorsque le bouton est pressé, elle sera marquée comme Ouverte/Activée.

Une mise à jour du module sera nécessaire chaque fois que ce paramètre sera modifié. Si le contrôleur est enregistré en tant que module d'expansion du lecteur, cette option doit être définie dans la programmation de l'entrée du contrôleur, et non de l'entrée du module d'expansion du lecteur.

Commandes des entrées manuelles

Un clic droit sur un registre d'entrée dans **Programmation | Entrées** ou sur une icône d'entrée sur un plan d'étage ou une page d'état ouvre un menu avec des commandes manuelles pour cette entrée.

Contourner

Ces commandes vous permettent de contourner une entrée. Cela signifie que la partition peut être armée même si cette entrée est ouverte ou altérée, mais l'entrée ne sera pas surveillée et ne fera pas passer la partition en mode alarme. Les commandes disponibles sont les suivantes :

- **Enlever** (enlever tout contournement de l'entrée)
- **En permanence** (contourner l'entrée en permanence, afin qu'elle soit toujours ignorée par l'armement de la partition)
- **Jusqu'au prochain désarmement** (contourne l'entrée jusqu'à ce qu'une partition attribuée à l'entrée soit désarmée)

Types de portes

Les types de portes définissent le mode de fonctionnement de chaque porte, ce qui vous permet de définir des paramètres qui peuvent être appliqués à plusieurs portes. Les informations d'identification requises pour l'accès (par exemple, carte, NIP, biométrie) et les paramètres d'anti-passback sont définis dans le type de porte.

Il existe un certain nombre de types de portes préconfigurées qui offrent une fonctionnalité de base. Il est recommandé de ne pas modifier ces registres, afin de disposer d'une base de référence connue à utiliser pour les tests et le dépannage. Les registres par défaut suivants sont disponibles :

- Carte
- Carte et NIP
- Carte ou NIP
- NIP seulement

Types de portes | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

Configuration générale

- **Horaire d'opération** : L'horaire d'opération détermine quand ce type de porte spécifique est actif. Lorsque cet horaire est valide, les paramètres de ce type de porte seront utilisés pour ces portes. Lorsque le programme n'est pas valide, les paramètres du **Type de porte secondaire** définis ci-dessous seront utilisés.

  Par exemple, vous pouvez configurer un type de porte pour que l'accès par carte seulement soit autorisé pendant les heures de travail. En dehors des heures de travail, la porte utilise le type de porte secondaire avec un accès par carte et NIP pour améliorer la sécurité.
- **Type de porte secondaire** : Le type de porte utilisé lorsque **l'horaire d'opération** défini ci-dessus n'est pas valide. Tous les paramètres de ce type de porte sont utilisés (y compris, par exemple, les paramètres d'anti-passback).
- **Type de porte de secours** : Ce type de porte fournit un ensemble d'informations d'identification de secours qui peuvent être utilisées pour accéder à une porte à tout moment.

  Par exemple, si un portail de parc de stationnement est configuré pour accorder l'accès en fonction de la reconnaissance des plaques d'immatriculation, il est utile de disposer d'un lecteur de carte traditionnel au cas où les utilisateurs auraient besoin d'ouvrir le portail sans voiture.

  Seules les informations d'identification d'entrée/sortie du type de porte de secours sont utilisées, et non les autres paramètres tels que l'anti-passback.
- **Type de porte de niveau d'accès** : Ce type de porte alternatif est utilisé par les utilisateurs dont l'option **Utiliser le type de porte de niveau d'accès** est sélectionnée dans **Utilisateurs | Niveaux d'accès | Général**. Les paramètres du type de porte de niveau d'accès seront utilisés à la place du type de porte principal.

  Par exemple, cette fonction peut être utilisée pour faciliter les déplacements des responsables ou du personnel de sécurité sur un site.

- **Permettre la panne temporaire en cas de conformité manquante** : Si le(s) champ(s) ci-dessous relatif(s) aux **Types d'informations d'identification d'entrée/sortie** comporte(nt) un type de conformité, l'utilisateur doit normalement disposer de cette conformité comme informations d'identification pour pouvoir accéder à la porte. Si cette option est activée, l'utilisateur ne se voit pas refuser l'accès lorsqu'il lui manque une conformité. Le **message** ci-dessous s'affiche sur l'écran d'un lecteur compatible, et l'utilisateur doit l'accepter avant que l'accès ne lui soit accordé.

  Pour plus de renseignements, consulter la Note d'application 286 : Programmation des types de conformité dans Protege GX.

- **Message** : Si l'option **Permettre la panne temporaire en cas de conformité manquante** ci-dessous est activée, ce message s'affiche sur l'écran du lecteur de carte pour avertir les utilisateurs qu'ils ne respectent pas la conformité.

  En raison de la taille de l'écran du lecteur, les messages de conformité sont limités à 32 caractères.

Entrée/sortie

Les options de ces sections font référence aux paramètres d'entrée et de sortie de porte respectivement, et peuvent être configurées indépendamment pour les directions d'entrée et de sortie.

- **Passback d'entrée/sortie est qualifié avec ouverture de porte** : Par défaut, la partition actuelle de l'utilisateur est mise à jour dès que l'accès à une porte lui est accordé. Lorsque cette option est activée, la partition actuelle et l'état de l'anti-passback ne sont pas mis à jour, sauf si l'utilisateur ouvre la porte après avoir obtenu l'accès.
- **Mode de passback d'entrée/de sortie** : Ce champ vous permet d'activer l'anti-passback pour ce type de porte (dans le sens de l'entrée et de la sortie respectivement). Activer l'anti-passback pour une porte lui permet de surveiller les partitions dans lesquelles les utilisateurs se trouvent actuellement, en fonction de la **partition intérieure/extérieure de la porte** (qui doit être définie dans **Programmation | Portes | Général**).

  Si un utilisateur tente de franchir une porte depuis la mauvaise partition, il enfreint les règles anti-passback. L'option sélectionnée ici détermine ce qui se passe dans cette situation :

  - **Passback sévère** : L'utilisateur se voit refuser l'accès jusqu'à ce qu'il entre dans la bonne partition ou que son état d'anti-passback soit réinitialisé.
  - **Passback souple** : L'utilisateur se voit refuser l'accès mais un événement « Violation de passback souple » est enregistré.

  L'état d'anti-passback de l'utilisateur peut être réinitialisé manuellement en faisant un clic droit sur un registre d'utilisateur ou automatiquement sur une minuterie ou un horaire à l'aide des options dans **Programmation | Portes | Options avancées**.

  L'anti-passback a un certain nombre d'applications. Il sert principalement à empêcher les utilisateurs de transmettre leur carte ou NIP d'accès à des personnes non autorisées, ou à empêcher les personnes de suivre les utilisateurs légitimes. L'anti-passback peut également améliorer la précision du comptage des partitions, des rapports Muster et des rapports de présence, et vous permettre de gérer les partitions de flânage.

  L'anti-passback est global sur l'ensemble du site. Lorsqu'un utilisateur franchit une porte contrôlée par un système anti-passback, le contrôleur informe les autres contrôleurs de la partition actuelle de l'utilisateur par le biais d'opérations inter-contrôleurs. Il peut également être utile d'activer l'option **Mettre à jour partition de l'utilisateur lorsque passback désactivé** dans **Programmation | Portes | Options avancées** pour les portes qui n'utilisent pas l'anti-passback.

  Pour plus de renseignements et des exemples de programmation, consulter la Note d'application 337 : Configurer un anti-passback dans Protege GX. L'antipassback est également pris en charge pour les tourniquets et les portes de sécurité dans les intégrations d'ascenseurs de haut niveau (regardez la note d'application correspondante).

- **Mode de lecture d'entrée/de sortie** : Le mode de lecture détermine les informations d'identification ou la séquence d'informations d'identification que la porte accepte pour entrer ou sortir respectivement. Même si les utilisateurs ont des autorisations valides, l'accès leur est refusé s'ils ne possèdent pas le(s) type(s) d'informations d'identification requis par le type de porte.

Les informations d'identification par défaut disponibles sont : Carte seulement, NIP seulement, Carte et NIP, Carte ou NIP, Carte et biométrique et Carte ou biométrique. La sélection de Personnalisé ouvre la section **Types d'informations d'identification d'entrée/sortie**, ce qui vous permet de saisir une séquence personnalisée d'informations d'identification.

- **L'entrée/sortie de la porte nécessite une vérification** : Si cette option est activée, les utilisateurs doivent obtenir la vérification d'un opérateur avant de pouvoir déverrouiller la porte. Lorsqu'un utilisateur saisit ses informations d'identification pour demander l'accès, les opérateurs reçoivent une fenêtre contextuelle avec un flux de caméra en direct. Cela permet à un opérateur de confirmer visuellement l'identité de l'utilisateur et de cliquer sur un bouton **Déverrouiller** pour déverrouiller la porte.

  Cette option nécessite la programmation d'une **Caméra (entrée)** et/ou d'une **Caméra (sortie)** pour chaque porte dans **Programmation | Portes | Général**.

- **Avertir opérateur mais permettre l'entrée/la sortie** : Si cette option est activée, les opérateurs reçoivent une fenêtre contextuelle de caméra comme ci-dessus, mais la porte se déverrouille sans l'intervention de l'opérateur.

Types d'informations d'identification d'entrée/sortie

Ces sections sont disponibles lorsque le **Mode de lecture d'entrée/sortie** (respectivement) est réglé sur Personnalisé. Cliquez sur **Ajouter** pour créer une liste personnalisée des informations d'identification qui seront acceptées par ce type de porte. Il peut s'agir d'informations d'identification standard (carte, NIP, biométrie), de types d'informations d'identification et de types de conformité (tous deux programmés dans **Sites | Types d'informations d'identification**).

Toutes les informations d'identification saisies dans ce champ doivent être saisies pour obtenir l'accès à la porte.

- **Séquence** : Lorsque cette option est activée, les informations d'identification doivent être saisies à la porte dans l'ordre où elles figurent dans le champ ci-dessous. Lorsque cette option n'est pas activée, les informations d'identification peuvent être saisies dans n'importe quel ordre.

  Les types de conformité ne sont pas affectés par cette option et sont toujours vérifiés en dernier dans la séquence.

Pour plus de renseignements et des exemples de programmation, consulter la Note d'application 276 : Configuration des types d'informations d'identification dans Protege GX. Pour l'utilisation des types de conformité, consulter la Note d'application 286 : Programmation des types de conformité dans Protege GX

Commandes

- Ce champ est utilisé pour envoyer des commandes de programmation à l'appareil. Il ne doit être utilisé que lorsqu'il est spécifiquement conseillé par la documentation ICT ou le support technique.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Types de portes | Options

- **Requête de sortie de porte non permise** : Si cette option est activée, l'opération REX (demande de sortie) est désactivée pour toutes les portes utilisant ce type de porte. Ceci a priorité sur les paramètres de la programmation de la porte.
- **Requête d'entrée de porte non permise** : Si cette option est activée, l'opération REN (demande d'entrée) est désactivée pour toutes les portes utilisant ce type de porte. Ceci a priorité sur les paramètres de la programmation de la porte.
- **Requiert une authentification double** : Lorsque cette option est activée, toutes les portes utilisant ce type de porte devront faire l'objet d'une authentification double (c'est-à-dire deux informations d'identification d'utilisateur distincts) pour y accéder. Pour obtenir l'accès, il faut suivre les étapes suivantes :

- Un utilisateur dont l'option **Master de garde double** est activée (**Utilisateurs | Utilisateurs | Options**) saisit des informations d'identification valides.
- La porte active la **Sortie d'attente d'authentification double du Lecteur 1/2** et attend le second utilisateur. Si le **Temps d'attente de l'authentification double du Lecteur 1/2** est dépassé, la demande d'accès expire.

  Les deux options peuvent être configurées dans **Modules d'expansion | Modules d'expansion du lecteur | Lecteur 1/2**.
- Un deuxième utilisateur dont l'option **Master de garde double** ou **Fournisseur de garde double** est activée (**Utilisateurs | Utilisateurs | Options**) saisit des informations d'identification valides.
- L'accès est accordé et la porte se déverrouille.

Cette fonction est utilisée pour les partitions de haute sécurité telles que les coffres-forts des banques ou les salles de serveurs qui nécessitent un niveau de surveillance élevé. Elle peut également être utilisée pour s'assurer qu'il y a toujours deux personnes présentes dans les partitions dangereuses telles que les laboratoires.

- **Fournisseur de carte double peut initier l'accès** : Lorsque cette option est activée, un **Fournisseur de garde double** peut initier la séquence d'authentification double sans avoir besoin d'un **Master de garde double**. Toute combinaison de fournisseur et de maître peut initier et compléter la séquence d'informations d'identification.

Types d’entrées

Les types d’entrée définissent le mode de fonctionnement d’une entrée ou d’une entrée trouble dans une partition particulière. Ceci couvre une grande variété d’applications : de la génération d’alarme au signalement, à la surveillance des troubles et au contrôle des sorties, des partitions et de l’automatisation. Comme chaque entrée peut être programmée dans un maximum de quatre partitions avec un type d’entrée différent dans chacune, les types d’entrées constituent une méthode souple et efficace pour appliquer la programmation à une ou plusieurs entrées.

Il existe un certain nombre de types d’entrées préconfigurées qui offrent une fonctionnalité de base. Il est recommandé de ne pas modifier ces registres, afin de disposer d’une base de référence connue à utiliser pour les tests et le dépannage. Vous pouvez également copier ces valeurs par défaut, afin de disposer d’un modèle pour votre propre programmation. Les registres disponibles sont :

- Instantané : Lorsque l’entrée est ouverte dans une partition armée, la partition passe immédiatement en alarme.
- Force instantanée : Identique à Instantané, mais l’entrée peut être armée de forcée.
- Délai : Lorsque l’entrée est ouverte dans une partition armée, la partition commencer le délai d’entrée.
- Suivre délai : Si l’entrée est ouverte pendant le délai d’entrée, l’alarme n’est pas activée. Si l’entrée est ouverte alors que la partition est armée et qu’elle n’est pas en délai d’entrée, la partition passe immédiatement en alarme.
- Force suivre délai : Identique à Suivre délai, mais l’entrée peut être armée de forcée.
- Trouble Silence : Utilisé pour les entrées troubles. Si cette entrée est ouverte alors que la partie 24 heures de la partition est armée, une alarme 24 heures (altération) est générée. La sortie de la cloche de la partition n’est pas activée.
- Trouble Sirène : Utilisé pour les entrées troubles. Identique à Trouble Silence, mais la sortie de la cloche de la partitionsera activée.
- Incendie : Utilisé pour les détecteurs de fumée et autres entrées de détection d’incendie. Lorsque cette entrée est ouverte dans une partition armée, la partition se met en alarme et un code « incendie » est envoyé à la station de surveillance.

  Il est recommandé de programmer les entrées de détection d'incendie dans une zone d'incendie dédiée qui est toujours armée.

- Force de retard : Identique à Délai, mais l’entrée peut être armée de forcée.
- Alarme 24 heures : Utilisé pour les entrées de panique. Lorsque cette entrée est ouverte, elle génère une alarme même si la partition est désarmée. Un code « panique » est envoyé à la station de surveillance.

Types d’entrées | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

- **Horaire d'opération** : Ce programme détermine quand ce type d'entrée particulier est actif. Lorsque cet horaire est valide, les paramètres pour ce type d'entrée seront utilisés. Lorsque l'horaire n'est pas valide, les paramètres du **Type d'entrée secondaire** ci-dessous sont utilisés à la place.
- **Type d'entrée secondaire** : Lorsque l'**horaire d'opération** défini ci-dessus est invalide, les entrées utilisent ce type d'entrée secondaire.
- **Groupe d'affichage de l'alarme du clavier** : Lorsqu'une entrée utilisant ce type d'entrée génère une alarme, seuls les claviers de ce groupe de claviers affichent les informations relatives à l'alarme. Par exemple, vous pouvez souhaiter que les alarmes d'entrée trouble n'apparaissent que sur des claviers spécifiques accessibles aux installateurs et au personnel de maintenance, plutôt qu'aux utilisateurs habituels.

  Si ce champ n'est pas défini, tous les claviers afficheront les alarmes provenant de ces entrées.
- **Automatisation de contrôle** : L'automatisation qui sera contrôlée par les entrées avec ce type d'entrée. Les automatisations peuvent être utilisées pour contrôler des sorties, ou peuvent être connectés à des groupes C-Bus pour une automatisation intégrée au bâtiment.

  La relation entre l'état de l'entrée et l'état de l'automatisation doit être configurée dans la section **Automatisation** de l'onglet **Options (3)**.

  Cette méthode de contrôle de l'automatisation ne fonctionne que lorsque la partition attribuée à l'entrée est armée. Il est recommandé de créer une partition de contrôle qui est toujours armée à cette fin.

  Pour plus d'informations et d'instructions de programmation, consulter la note d'application 289 : Intégration C-Bus avec Protege GX et Protege WX.
- **Code personnalisé de signalisation** : Lorsque cette entrée déclenche une alarme, le Code personnalisé de signalisation détermine le code d'événement signalé à la station centrale de surveillance. Il est également inclus en tant que « code spécial » dans le journal des événements Protege GX.

  Cela vous permet de fournir plus d'informations sur le type d'alarme déclenchée (p. ex., une alarme médicale, un détecteur de fumée, etc.). Si ce champ est défini sur Aucun, le code de cambriolage standard sera utilisé.

  Les codes personnalisés de signalisation disponibles ici sont tirés des codes d'événement standard Contact ID. Pour plus d'informations, voir la note d'application 316 : Rapports au format Contact ID dans Protege GX et Protege WX.
- **Temps de sortie de contrôle** : Les entrées avec ce type d'entrée activeront la **sortie de contrôle / le groupe de sorties** (défini ci-dessous) pendant cette période (en secondes). Si ce temps est réglé sur 0, la sortie s'activera indéfiniment.

  Par défaut, ce champ s'applique uniquement à la sortie de contrôle définie dans le type d'entrée, toutefois, si l'option **Utiliser temps de sortie de type d'entrée** est activée (onglet **Options (3))**, ce temps s'applique également à la sortie de contrôle définie dans la programmation de l'entrée.

  Ce réglage a priorité sur le **temps d'activation** défini dans **Programmation | Sorties | Général** et sur le **temps de sortie** défini dans **Groupes | Groupes de sortie | Général**.
- **Sortie de contrôle / Groupe de sorties programmables** : Cette sortie ou ce groupe de sorties est contrôlé(e) par des entrées avec ce type d'entrée. La relation entre l'état de l'entrée et l'état de la sortie doit être configurée à l'aide des **Options d'activation de sortie** (onglet **Options (2)**).

  Cela permet un contrôle « sortie suit entrée » dans une configuration plusieurs à un ou plusieurs à plusieurs. Par exemple, vous pouvez configurer un groupe de lumières pour qu'elles s'allument lorsqu'un mouvement est détecté sur l'un des nombreux PIR de la pièce. Vous pouvez également définir une **sortie de contrôle / un groupe de sorties** dans la programmation de l'entrée, permettant un contrôle un à un ou un à plusieurs.

  Pour cette méthode de contrôle des sorties, la partition programmée pour l'entrée doit avoir sa **partie 24 heures armée**. Il est recommandé de créer une partition dédiée à l'utilisation des fonctions de contrôle de sorties.

- **Partition de contrôle** : Cette partition peut être armée et/ou désarmée par des entrées avec ce type d'entrée. La relation entre l'état de l'entrée et l'état de la partition doit être configurée à l'aide des **options diverses** de l'onglet **Options (2)**.

  Par exemple, cela peut être utilisé pour créer des interrupteurs à clé qui arment et désarment une partition spécifique.

  La partition de contrôle doit avoir l'option **Activer armement par force** cochée dans **Programmation | Partitions | Options (2)**.

Commandes

- Ce champ est utilisé pour envoyer des commandes de programmation à l'appareil. Il ne doit être utilisé que lorsqu'il est spécifiquement conseillé par la documentation ICT ou le support technique.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Types d'entrées | Options (1)

Options d'alarmes

- **Générer des alarmes :** Lorsque cette option est activée, les entrées utilisant ce type d'entrée génèrent des alarmes. Les alarmes sont générées lorsqu'une entrée est ouverte dans une partition armée, entraînant le passage de la partition en état d'alarme. La sortie de la cloche peut être activée et l'alarme peut être sauvegardée dans la mémoire de la partition (selon les paramètres de l'onglet **Options (2)**).

  La désactivation de cette option empêchera les entrées avec ce type d'entrée de générer des alarmes. Les entrées continueront à générer des événements d'ouverture/fermeture. Par exemple, les types d'entrées qui sont utilisés uniquement pour l'automatisation ne doivent pas générer d'alarmes.

  Cette fonctionnalité n'est pas liée aux alarmes opérateur qui peuvent être programmées dans **Événements | Alarmes**.

- **Générer des alarmes de 24 heures** : Lorsque cette option est activée, les entrées utilisant ce type d'entrée génèrent des alarmes de 24 heures (altération). Les alarmesde 24 heures (parfois appelées alarmes de sabotage) sont générées lorsqu'une entrée est altérée ou court-circuitée dans une partition dont la partie 24 heures est armée. Les alarmes de 24 heures ne mettent pas la partition en état d'alarme et n'activent pas (normalement) la sortie de la cloche (mais consulter les paramètres dans **Options (3)**).

  Les entrées troubles génèrent également des alarmes de 24 heures lorsqu'elles sont ouvertes, toutefois, les alarmes d'entrée troubles mettent la partition en alarme et peuvent activer la sortie de la cloche comme d'habitude. Cette option doit être activée pour tout type d'entrée utilisé par les entrées trouble.
- **Entrée de délai d'entrée** : Avec cette option activée, les entrées utilisant ce type d'entrée activeront le délai d'entrée lorsqu'elles sont ouvertes dans une partition armée. Si cette option n'est pas activée, la partition se met en alarme instantanément sans délai d'entrée.

  Par exemple, cette option pourrait être activée pour les entrées sur les portes extérieures qui sont utilisées pour entrer dans le bâtiment.
- **Suivre entrée de délai d'entrée** : Lorsque cette option est activée, les entrées utilisant ce type d'entrée ne généreront pas d'alarmes pendant la période de délai d'entrée, mais généreront des alarmes si le délai d'entrée n'a pas commencé. Si cette option n'est pas activée, les entrées généreront des alarmes, même pendant le délai d'entrée.

  Cette option doit être utilisée pour les entrées qui couvrent le trajet entre l'entrée et le point de désarmement. Par exemple, un PIR situé dans la voie d'entrée ne doit pas générer d'alarme lorsque quelqu'un entre par la porte (ce qui fait commencer le délai d'entrée), mais doit générer une alarme si quelqu'un est détecté dans la pièce sans ouvrir la porte.

- **Entrée de délai de sortie** : Lorsque cette option est activée, les entrées avec ce type d'entrée ne génèrent pas d'alarmes pendant la période de délai de sortie. Lorsque cette option est désactivée, l'entrée générera des alarmes, même pendant le délai de sortie.

  Cette option doit être activée pour toutes les entrées que les utilisateurs peuvent déclencher lorsqu'ils quittent le bâtiment pendant l'armement. Ceci peut être désactivé pour d'autres entrées, afin d'empêcher les personnes de pénétrer à nouveau dans certaines parties du bâtiment pendant le processus d'armement.
- **Sortie courte sur restauration** : Avec cette option activée, une entrée avec ce type d'entrée peut être utilisée pour raccourcir la minuterie du délai de sortie d'une partition. Lorsque l'entrée est restaurée (fermée) pendant le délai de sortie, le délai de sortie est réduit à 5 secondes.

  Par exemple, vous pouvez activer cette option pour un contact de porte afin que la partition s'arme 5 secondes après la fermeture de la porte.
- **Entrée de panique de vingt quatre heures** : Lorsque cette option est activée, les entrées avec ce type d'entrée génèrent des alarmes, même lorsque la partition assignée n'est pas armée. Un code d'action de « panique » sera inclus dans le rapport de la station centrale. Cela permet aux entrées d'agir comme des « boutons de panique » et de générer des alarmes lorsqu'elles sont ouvertes, quel que soit l'état de la partition.

  Cette fonction utilise la surveillance de l'altération de 24 heures pour générer des alarmes lorsque la partition principale n'est pas armée. Par conséquent, les éléments suivants sont également requis :
  - L'option **Générer des alarmes de 24 heures** ci-dessus doit être activée (toutefois, **Générer des alarmes** peut être désactivé).
  - La partie 24 heures de la partition attribuée doit être armée.

  Pour fournir plus d'informations sur l'alarme, réglez également le **Code de rapport personnalisé** dans l'onglet **Général** sur un code approprié.
- **Entrée d'incendie** : Avec cette option activée, les entrées utilisant ce type d'entrée génèrent des alarmes incendie lorsqu'elles sont ouvertes dans une partition armée. Un code d'action de « incendie » sera inclus dans le rapport de la station centrale. Il est recommandé de programmer toutes les entrées d'incendie dans une partition d'incendie dédiée qui est toujours armée.

  Pour fournir plus d'informations sur l'alarme, réglez également le **Code de rapport personnalisé** dans l'onglet **Général** sur un code approprié.

  La plupart des détecteurs de fumée utilisent un contact normalement ouvert. Assurez-vous que ces entrées ont les paramètres corrects de **type de contact** et de **fin de ligne d'entrée** (onglet **Programmation | Entrées | Options**).

Options de signalisation

- **Rapport des alarmes** : Lorsque cette option est activée, le contrôleur signalera à la station centrale de surveillance toutes les alarmes générées par ces entrées. En outre, un événement de signalement sera enregistré dans le journal des événements.

  L'option **Générer des alarmes** doit être activée pour que cette option fonctionne. Cette fonctionnalité n'est pas liée aux alarmes opérateur qui peuvent être programmées dans **Événements | Alarmes**.
- **Signalement des effractions** : Lorsque cette option est activée, le contrôleur signalera à la station centrale de surveillance toutes les alarmes de 24 heures (alarmes de sabotage) générées par ces entrées. Cette option doit également être activée pour permettre le signalement des alarmes d'entrée trouble. En outre, un événement de signalement sera enregistré dans le journal des événements.

  L'option **Générer des alarmes de 24 heures** doit être activée pour que cette option fonctionne.
- **Signaler contournement** : Avec cette option activée, le contrôleur signale à la station centrale de surveillance tous les cas où ces entrées sont contournées pour armer un secteur. Elle signalera également le moment où le contournement a été retiré. Les événements de signalement seront enregistrés dans le journal des événements.

  L'option **Signaler contournement d'utilisateur** doit également être activée dans **Programmation | Partitions | Options (1)**.

- **Signaler restaurations** : Avec cette option activée, le contrôleur signalera tous les événements de restauration d'entrée à la station centrale de surveillance. Cela se produit lorsqu'une entrée est fermée à nouveau après avoir généré une alarme ou une alarme de 24 heures. Les événements de signalement seront enregistrés dans le journal des événements.
- **Entrée de séjour** : Lorsque cette option est activée, les entrées avec ce type d'entrée sont surveillées lorsque la partition attribuée est armer de séjour. Les entrées avec cette option désactivée ne seront pas surveillées lorsque la partition reste armée.

  Par exemple, vous pouvez souhaiter rester armé dans une partition pour surveiller le périmètre alors que des gens sont encore à l'intérieur. Dans ce cas, l'option **Entrée de séjour** doit être activée pour les entrées de périmètre telles que les contacts de porte, et désactivée pour les PIR internes et les autres entrées.
- **Entrée de force** : Lorsque cette option est activée, les entrées utilisant ce type d'entrée peuvent être forcées. Cela signifie que la partition assignée peut être armée par force lorsque ces entrées attribuée ouvertes sans les contourner. Les entrées sont toujours surveillées et peuvent encore générer des alarmes si elle sont fermées et ouvertes à nouveau.

  Si cette option est désactivée, ces entrées ne peuvent pas être forcées, toutefois, cela peut être annulé par l'option **Utiliser armement par force brute sans surveillance** dans **Programmation | Partitions | Options (1)**.

  Il se peut que vous deviez contourner des entrées lorsqu'elles sont armées par force pour générer des rapports de contournement. Entrez l'une des commandes suivantes dans l'onglet **Général** :
  - `EnableForceBypass = true` (contourne l'entrée jusqu'à ce que la zone soit désarmée)
  - `ForceSendsBypass = true` (contourne l'entrée jusqu'à ce qu'elle soit fermée)
- **Entrée de sortie de l'allée ne pas la tester** : Les entrées dont cette option est activée ne seront pas testées lorsque la partition attribuée est en cours d'armement. Cela signifie que la partition peut être armée même si ces entrées sont ouvertes et non contournées.

  Ceci doit être utilisé pour les entrées telles que les PIR qui passent outre les claviers et autres points d'armement, qui devraient autrement être contournés chaque fois que la partition est armée. Elle doit être utilisée parallèlement à l'option **Entrée de délai de sortie**.
- **Recycler alarme de l'entrée sur fin de délai de sortie** Par défaut, les entrées dotées de la fonctionnalité **Entrée de délai de sortie** ne génèrent pas d'alarmes si elles restent ouvertes après la fin du délai de sortie. Une alarme ne sera générée que si l'entrée se ferme et s'ouvre à nouveau après l'armement. Lorsque cette option est activée, toute entrée encore ouverte à la fin du délai de sortie sera recyclée (fermée et ouverte à nouveau), générant une alarme.

  Utiliser cette fonctionnalité pour les entrées qui peuvent être violées pendant le délai de sortie, comme les contacts de fenêtre ou de porte.

Types d'entrées | Options (2)

Options diverses

- **Activer sortie de sonnerie** : Avec cette option activée, lorsqu'une entrée ou une entrée trouble avec ce type d'entrée génère une alarme, la sortie de la cloche pour la partition attribuée est activée. Ceci peut être désactivé dans les cas où une alarme silencieuse est requise (p. ex., entrées sous contrainte).

  Pour les entrées régulières, cette option ne s'applique normalement pas aux alarmes de 24 heures/sabotages, mais les paramètres **24 heures génère une sonnerie si armée** ou **24 heures génère toujours une sonnerie (Options (3)**) peuvent être activés selon les besoins.
- **Redéclencher temps de sonnerie** : Lorsque cette option est activée, ces entrées peuvent déclencher à nouveau la minuterie d'alarme/de sonnerie de la partition. Si l'alarme a déjà été activée lorsque l'entrée est ouverte, la minuterie de l'alarme sera réinitialisée pour prolonger la durée d'activation de la sortie de la cloche.
- **Enregistrer dans la mémoire de la partition** : Avec cette option activée, les alarmes générées par ces entrées sont enregistrées dans la mémoire d'alarme de la partition. La mémoire d'alarme peut être visualisée et reconnue dans le menu Vue d'un clavier (**[Menu][5][1]**). Les alarmes en mémoire sont effacées lors du prochain armement de la partition.

  Désactiver cette option pour empêcher l'enregistrement des alarmes dans la mémoire d'alarme.

- **Désarmer partition de contrôle sur restauration de l'entrée** : Lorsque cette option est activée, la **partition de contrôle** définie dans l'onglet **Général** sera désarmée lorsque toute entrée avec ce type d'entrée est fermée (restaurée).
- **Armer la partition de contrôle sur alarme d'entrée** : Lorsque cette option est activée, la **partition de contrôle** définie dans l'onglet **Général** sera armée lorsque toute entrée avec le type d'entrée est ouverte (mise sous alarme).

  Il n'est pas nécessaire d'activer l'alarme de zone pour exécuter la fonction de contrôle.

- **Activer/désactiver la partition de contrôle sur alarme d'entrée** : Lorsque cette option est activée, chaque fois qu'une entrée avec ce type d'entrée est ouverte, l'état de la **Partition de contrôle** définie dans l'onglet **Général** est activé/désactivé. Cela signifie que chaque fois que l'entrée est ouverte, la partition passe de désarmée à armée, ou vice versa.

  Il n'est pas nécessaire d'activer l'alarme de zone pour exécuter la fonction de contrôle.

- **Permettre armement de force de l'entrée falsifiée** : Par défaut, les partitions ne peuvent pas être armées de force si elles contiennent une entrée qui est dans un état d'altération. Avec cette option activée, les partitions peuvent être armées par force même si les entrées avec ce type d'entrée sont altérées.

  L'option **Entrée de force** doit être activée dans l'onglet **Options (1)**.

- **Activer la sortie d'entrée sur temps de sonnerie** : Il s'agit d'une option héritée qui n'a aucun effet.
- **Test pendant l'essai de marche de cambriolage** : Un test de marche de cambriolage est un test de marche spécial qui peut être activé pour une partition dans **Programmation | Partitions | Options (1)**. Toutes les entrées pour lesquelles cette option est activée doivent être testées pendant le test de marche de cambriolage. Cette option est utile lorsqu'il existe un petit nombre d'entrées critiques qui doivent être testées régulièrement, comme les boutons de panique ou de contrainte.

  Pour plus d'informations, consulter la note d'application 197 : Configuration du maintien d'un test de marche de cambriolage dans Protege GX .

Options d'activation de sorties

- **Activer la sortie de contournement** : Avec cette option activée, ces entrées peuvent activer la **sortie / le groupe de sorties des entrées contournées de la partition**. C'est activé lorsque la partition est armée avec des entrées contournées, et désactivé lorsque la partition est désarmée.
- **Activer sortie de sabotage 24 heures** : Avec cette option activée, ces entrées peuvent activer la **sortie / le groupe de sorties de l'alarme de sabotage**. Ceci est activé lorsqu'une entrée génère une alarme de 24 heures (altération) et désactivé lorsque la partie 24 heures de la partition est désarmée.
- **Activer la sortie mémoire** : Avec cette option activée, ces entrées peuvent activer la **sortie / le groupe de sorties de mémoire d'alarme**. Cette sortie est activée lorsqu'une alarme se déclenche dans une partition et reste active jusqu'à ce que la partition soit désarmée.

  Cette fonction peut être utilisée pour indiquer aux utilisateurs qu'il y a eu une alarme, les empêchant ainsi de pénétrer dans une partition potentiellement non sécurisée.
- **Activer la sortie de contrôle sur alarme** : Avec cette option activée, la **sortie de contrôle / le groupe de sorties** sera désactivé(e) chaque fois qu'une entrée avec ce type d'entrée sera ouverte (mise sous alarme).

  Cette option fait référence à la sortie de contrôle définie dans la programmation du type d'entrée (onglet **Général**). Il n'est pas nécessaire d'activer l'alarme de zone pour exécuter la fonction de contrôle.

- **Activer la sortie de contrôle sur restauration** : Avec cette option activée, la **sortie de contrôle / le groupe de sorties** défini(e) dans la programmation des entrées sera activé(e) chaque fois qu'une entrée avec ce type d'entrée sera fermée (restaurée).

  Cette option fait référence à la sortie de contrôle définie dans la programmation du type d'entrée (onglet **Général**).

- **Désactiver la sortie de contrôle sur alarme** : Avec cette option activée, la **sortie de contrôle / le groupe de sorties** sera désactivé(e) chaque fois qu'une entrée avec ce type d'entrée sera ouverte (mise sous alarme).

Cette option fait référence à la sortie de contrôle définie dans la programmation du type d'entrée (onglet **Général**). Il n'est pas nécessaire d'activer l'alarme de zone pour exécuter la fonction de contrôle.

- **Désactiver la sortie de contrôle sur restauration** : Avec cette option activée, la **sortie de contrôle / le groupe de sorties** sera désactivé(e) chaque fois qu'une entrée avec ce type d'entrée sera fermé (restaurée).

  Cette option fait référence à la sortie de contrôle définie dans la programmation du type d'entrée (onglet **Général**).

- **Basculer l'état de la sortie de contrôle sur alarme** : Avec cette option activée, la **sortie de contrôle / le groupe de sorties** sera activé(e)/désactivé(e) chaque fois qu'une entrée avec ce type d'entrée sera ouverte (mise sous alarme). Cela signifie que chaque fois que l'entrée est ouverte, la sortie passe de désactivée à activée, ou vice versa.

  Cette option fait référence à la sortie de contrôle définie dans la programmation du type d'entrée (onglet **Général**). Il n'est pas nécessaire d'activer l'alarme de zone pour exécuter la fonction de contrôle.

- **Entrée redéclenche temps de sortie** : Lorsque cette option est activée, ces entrées peuvent être ouvertes/fermées une seconde fois pour redémarrer le **temps de sortie de contrôle** (onglet **Général**), afin que la sortie de contrôle reste active plus longtemps.

  Par exemple, cela peut permettre aux lumières contrôlées par le mouvement de rester allumées plus longtemps lorsqu'une deuxième personne déclenche le détecteur de mouvement.

  Cette fonctionnalité fonctionne également avec la **sortie de contrôle / le groupe de sorties** défini dans la programmation des entrées. L'option **Utiliser temps de sortie de type d'entrée** doit être activée dans l'onglet **Options (3)**.

  Cette option ne fonctionne correctement que lorsque la partition attribuée à l'entrée est armée.

Types de portes | Options (3)

Options d'automatisation

- **Activer l'automatisation sur alarme** : Avec cette option activée, l'**automatisation de contrôle** sera activée chaque fois qu'une entrée avec ce type d'entrée sera ouverte (mise sous alarme).

  Cette option fait référence à l'automatisation du contrôle définie dans la programmation du type d'entrée (onglet **Général**). Il n'est pas nécessaire d'activer l'alarme de zone pour exécuter la fonction de contrôle.

- **Activer l'automatisation sur restauration** : Avec cette option activée, l'**automatisation de contrôle** sera activée chaque fois qu'une entrée avec ce type d'entrée sera fermée (restaurée).

  Cette option fait référence à l'automatisation du contrôle définie dans la programmation du type d'entrée (onglet **Général**).

- **Désactiver l'automatisation sur alarme** : Avec cette option activée, l'**automatisation de contrôle** sera désactivée chaque fois qu'une entrée avec ce type d'entrée sera ouverte(mise sous alarme).

  Cette option fait référence à l'automatisation du contrôle définie dans la programmation du type d'entrée (onglet **Général**). Il n'est pas nécessaire d'activer l'alarme de zone pour exécuter la fonction de contrôle.

- **Désactiver l'automatisation sur restauration** : Avec cette option activée, l'**automatisation de contrôle** sera désactivée chaque fois qu'une entrée avec ce type d'entrée sera fermée (restaurée).

  Cette option fait référence à l'automatisation du contrôle définie dans la programmation du type d'entrée (onglet **Général**).

- **Basculer l'état d'automatisation** : Avec cette option activée, l'**automatisation de contrôle** sera activée/désactivée chaque fois qu'une entrée avec ce type d'entrée sera ouverte (mise sous alarme). Cela signifie que chaque fois que l'entrée est ouverte, l'automatisation passe de désactivée à activée, ou vice versa.

  Cette option fait référence à l'automatisation du contrôle définie dans la programmation du type d'entrée (onglet **Général**). Il n'est pas nécessaire d'activer l'alarme de zone pour exécuter la fonction de contrôle.

- **24 heures génère une sonnerie si armée** : Lorsque cette option est activée, les entrées avec ce type d'entrée peuvent activer la sortie de la cloche de la partition en cas d'alarme de 24 heures / de sabotage, mais uniquement lorsque la partition est armée. L'option **Activer sortie de sonnerie** doit être activée dans l'onglet **Options (2)**.

  Cette option n'est pas nécessaire pour les entrées de dérangement.

- **24 heures génère toujours une sonnerie** : Lorsque cette option est activée, les entrées avec ce type d'entrée activeront toujours la sortie de la cloche de la partition en cas d'alarme de 24 heures / de sabotage. La sonnerie sera activée même si la partition n'est pas armée. L'option **Activer sortie de sonnerie** doit être activée dans l'onglet **Options (2)**.

  Cette option n'est pas nécessaire pour les entrées de dérangement.

Options de contrôle

- **Utiliser temps de sortie de type d'entrée** : Cette option permet à **la sortie de contrôle ou au groupe de sorties** défini(e) dans la programmation de l'entrée d'utiliser le **temps de sortie de contrôle** défini dans la programmation du type d'entrée. Lorsque la sortie de contrôle est activée, elle est désactivé après la période définie dans le type d'entrée.
- **Activer sortie de contrôle d'entrée sur alarme** : Avec cette option activée, la **sortie de contrôle / le groupe de sorties** défini(e) dans la programmation des entrées sera désactivé(e) chaque fois qu'une entrée avec ce type d'entrée sera ouvert(e) (mise sous alarme).

  Cette option fait référence à la sortie de contrôle définie dans la programmation de chaque entrée individuelle (**Programmation | Entrées | Général**). Il n'est pas nécessaire d'activer l'alarme de zone pour exécuter la fonction de contrôle.

- **Activer sortie de contrôle d'entrée sur restauration** : Avec cette option activée, la **sortie de contrôle / le groupe de sorties** défini(e) dans la programmation des entrées sera activé(e) chaque fois qu'une entrée avec ce type d'entrée sera fermé(e) (restaurée).

  Cette option fait référence à la sortie de contrôle définie dans la programmation de chaque entrée individuelle (**Programmation | Entrées | Général**).

- **Désactiver sortie de contrôle d'entrée sur alarme** : Avec cette option activée, la **sortie de contrôle / le groupe de sorties** défini(e) dans la programmation des entrées sera désactivé(e) chaque fois qu'une entrée avec ce type d'entrée sera ouvert(e) (mise sous alarme).

  Cette option fait référence à la sortie de contrôle définie dans la programmation de chaque entrée individuelle (**Programmation | Entrées | Général**). Il n'est pas nécessaire d'activer l'alarme de zone pour exécuter la fonction de contrôle.

- **Désactiver sortie de contrôle d'entrée sur restauration** : Avec cette option activée, la **sortie de contrôle / le groupe de sorties** défini(e) dans la programmation des entrées sera désactivé(e) chaque fois qu'une entrée avec ce type d'entrée sera fermé(e) (restaurée).

  Cette option fait référence à la sortie de contrôle définie dans la programmation de chaque entrée individuelle (**Programmation | Entrées | Général**).

- **Basculer l'état de sortie et d'entrée** : Avec cette option activée, la **sortie de contrôle / le groupe de sorties** défini(e) dans la programmation des entrées sera activé(e)/désactivé(e) chaque fois qu'une entrée avec ce type d'entrée sera ouvert(e) (mise sous alarme). Cela signifie que chaque fois que l'entrée est ouverte, la sortie passe de désactivée à activée, ou vice versa.

  Cette option fait référence à la sortie de contrôle définie dans la programmation de chaque entrée individuelle (**Programmation | Entrées | Général**). Il n'est pas nécessaire d'activer l'alarme de zone pour exécuter la fonction de contrôle.

Types de portes | Options (4)

Options générales

- **Toujours enregistrer événement d'entrée** : Lorsque cette option est activée, les entrées avec ce type d'entrée généreront toujours des événements, que l'option **Enregistrer à la mémoire tampon de l'événement** soit désactivée ou non dans la programmation de l'entrée (**Programmation | Entrées | Options**).
- **Utiliser une autre heure d'entrée** : Lorsque cette option est activée, chaque fois qu'une entrée de ce type d'entrée déclenche un délai d'entrée, elle utilise l'**heure d'entrée alternative** définie dans **Programmation | Partitions | Configuration**. Par exemple, vous pouvez utiliser cette option pour le contact de porte d'une entrée arrière ou d'une porte de garage, afin de laisser à l'utilisateur plus de temps pour atteindre le clavier.

Partitions

Les partitions représentent généralement des espaces physiques dans le Protege GX site , et sont utilisées pour surveiller les entrées et générer des alarmes lorsque des intrus sont détectés. Elles sont parfois appelées partitions d'alarme ou partitions.

Lorsqu'une partition est armée, elle commence à surveiller les entrées qui lui sont attribuées. Si une entrée est ouverte, la partition réagira en fonction du type d'entrée qui lui est attribué - par exemple, en passant en alarme ou en commençant le délai de saisie. Désarmer la partition mettra fin à la surveillance et mettra fin aux alarmes.

Les partitions ont également une partie 24 heures, qui doit être armé (activé) en tout temps. Cette partie de la partition est utilisée pour surveiller les conditions de sabotage ou de courte durée et peut également déclencher une alarme (généralement sans activer la sonnerie). Les partitions peuvent également être intégrées au contrôle d'accès en étant affectées à la **Partition de la porte intérieure/extérieure** (**Programmation | Portes | Général**).

Pour certains usages, il est utile de créer des partitions qui ne correspondent pas à des espaces physiques et qui peuvent ne pas avoir de sorties d'alarme physiques, mais qui sont toujours armées afin de pouvoir être utilisées pour la surveillance et le contrôle. Par exemple, une "partition système" vous permet de surveiller les entrées de trouble et de signaler à tout moment les troubles du système. Une "partition de contrôle" ou "partition d'automatisation" est généralement utilisée pour le contrôle de sortie et d'autres fonctions d'automatisation, et ne génère pas d'alarmes. Chaque entrée peut être assignée à un maximum de quatre partitions, afin qu'elles puissent exécuter une fonction différente dans chacune indépendamment de l'état des autres partitions. Pour plus d'informations, consultez la section Entrées | Types de partitions et d'entrées (la page 223).

Partitions | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Nom d'affichage du clavier** : Le nom qui sera téléchargé vers le contrôleur. Ce dernier sera affiché sur le clavier et dans les rapports des services de surveillance IP. Le clavier ne peut afficher que les 16 premiers caractères du nom. Il doit donc décrire de manière concise l'emplacement physique et la fonction de l'appareil.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

Graphiques

- **Caméra** : L'association d'une caméra à une partition vous permet de faire un clic droit sur n'importe quel événement de partition dans une fenêtre d'événement pour ouvrir un flux de caméra archivé à l'heure de l'événement.
- **Plan d'étage** : L'association d'un plan d'étage à une partition vous permet de faire un clic droit sur n'importe quelle partition dans une fenêtre d'événement pour ouvrir le plan d'étage.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Partitions | Configuration

Minutages

- **Heure d'entrée** : La durée du délai d'entrée de la partition, en secondes. Si une entrée de délai d'entrée est déclenchée alors que la partition est armée, la zone passe en délai d'entrée. Si la partition n'est pas désarmée avant la fin de cette période, l'alarme sera activée.

  Si cette heure est réglée sur Faux, la partition se mettra immédiatement en alarme, quelle que soit l'entrée activée.

  Pour qu'une entrée commence le délai de saisie, **L'entrée du délai de saisie** doit être activée dans le type d'entrée (**Programmation | Types d'entrée | Options (1)**).

  La fonction de délai de notification à distance vous permet de retarder la transmission hors site des alarmes qui se produisent pendant le délai d'entrée. Pour plus d'information, consultez Image de fond de l'application 312 : Minimiser la transmission hors site des faux alarmes dans Protege GX et Protege WX.

- **Heure d'entrée alternative** : Une durée alternative pour le délai de saisie de la partition, en secondes. Ceci sera utilisé si le délai de saisie est déclenché par une entrée avec l'option **Utiliser une autre heure de saisie** activée dans le type d'entrée (**Programmation | Types d'entrée | Options (4)**).

  Ceci peut être utilisé pour accorder aux utilisateurs un délai plus long pour désarmer le système lorsqu'ils entrent par une autre entrée, comme un garage ou une porte arrière.

- **Heure de sortie** : La durée du délai de sortie de la partition, en secondes. Chaque fois que la partition est armée, le délai de sortie commence, donnant aux utilisateurs le temps de quitter la partition avant qu'elle ne soit armée. Lorsque le délai de sortie est écoulé, la partition est armée. Si cette heure est réglée sur Faux, la partition sera immédiatement armée.

  Pendant le délai de sortie, les entrées avec l'option **Délai de sortie** activée (**Programmation | Types d'entrée | Options (1)**) ne généreront pas d'alarmes. Cela devrait être utilisé pour toutes les entrées que les utilisateurs peuvent déclencher lorsqu'ils sortent de la partition (par exemple, les IRP, les contacts de porte).

- **Heure de l'alarme 1** : La durée (en minutes) pendant laquelle la sortie de la cloche restera active lorsque l'alarme de la partition est activée. L'heure minimale de l'alarme est de 1 minute.

  Certaines partitions peuvent avoir des limites quant à la durée d'activation d'une sonnerie ou d'une sirène. Assurez-vous de vérifier les réglementations locales avant de définir ce champ.

- **Minuterie d'entrée Intelligente** : La fonction d'entrée intelligente empêche les fausses alarmes dans les partitions en comptant plusieurs activations d'entrée uniques avant d'activer l'alarme. Lorsqu'une entrée est ouverte, l'alarme ne se déclenchera pas à moins qu'une ou plusieurs autres entrées s'ouvrent dans la période définie ici (en secondes).

  Pour utiliser cette fonction, cochez l'option **Activer les entrées intelligentes** dans l'onglet **Options (2)**. Le nombre d'entrées est défini par le **Nombre d'Entrées Intelligentes** ci-dessous.

- **Temps de réarmement de la partition** : Si l'option **Réarmement activé** est cochée dans l'onglet **Options (1)**, chaque fois que cette partition est désarmée, elle sera automatiquement réarmée après le temps défini ici (en minutes). Si ce temps est réglé sur 0, la partition sera réarmée après 1 minute.
- **Délai de désarmement de la chambre forte** : Si l'option **Contrôle de partition de la chambre forte** est activée dans l'onglet **Options (2)** , chaque fois qu'un utilisateur tente de désarmer la partition à partir d'un clavier, il y aura un délai supplémentaire avant que la partition ne soit désarmée. Ce champ définit le temps de retard (en minutes). Si ce temps est réglé sur 0, la partition sera immédiatement désarmée.
- **Délai du double code de la chambre forte** : Si l'option de **Contrôle de la chambre forte à double code** est activée dans l'onglet **Options (2)**, la partition nécessitera deux codes d'utilisateur pour se désarmer. Ce champ définit la limite de temps (en secondes) dans laquelle un deuxième utilisateur doit se connecter au clavier et désarmer la partition, une fois le délai de désarmement de la chambre forte écoulé. Si le deuxième utilisateur n'entre pas de NIP dans ce délai, le processus de désarmement expirera.

- **Heure de fermeture récente** : Ce temps (en secondes) définit le délai après lequel une partition est considérée comme "récemment fermée" après l'armement. Si une alarme est générée dans la partition pendant cette période (en secondes), un message de Fermeture récente sera envoyé à la station de surveillance avec le message d'alarme. Cette option ne fonctionnera que lorsque l'option **Rapport d'alarmes** est activée pour l'entrée concernée dans **Programmation | Types d'entrée | Options (1)**.

  L'alarme sera activée, que la partition ait été récemment armée ou non.

Horaire

- **Horaire armer/désarmer** : Cet horaire peut être utilisé pour armer et désarmer une partition automatiquement. La fonction dépend des options sélectionnées ci-dessous. Voir aussi **Toujours vérifier l'horaire de partition** dans l'onglet **Options (2)**.
- **Désarmer la partition lorsque l'horaire débute** : Lorsque cette option est activée, la partition se désarme automatiquement lorsque **L'horaire Armer/Désarmer** ci-dessus devient valide.

  Utiliser cette option avec précaution, car la partition sera désarmée, qu'il y ait ou non des utilisateurs autorisés présents.

- **Désarmer la partition lorsque l'horaire débute** : Lorsque cette option est activée, la partition s'arme automatiquement lorsque **L'horaire Armer/Désarmer** ci-dessus devient invalide. Cela peut être utilisé pour garantir que la partition est sécurisée chaque jour, même si les utilisateurs oublient de l'armer.

  Cette fonction permet d'armer de force la partition, l'option **Activer l'armement par force** doit donc être activée (onglet **Options 2**).

Configuration

- **Partition enfant** : Une partition enfant peut être armée et désarmée automatiquement en fonction de l'état d'une ou plusieurs partitions parents. La relation entre l'état de la partition enfant et parent est basée sur les options sélectionnées dans l'onglet **Options (1)**.

  Étant donné que plusieurs partitions parentales peuvent être appliquées à une seule partition enfant, cette fonctionnalité peut être utilisée pour créer une "partition commune" qui dépend d'un certain nombre d'autres partitions.
- **Nombre maximal d'entrées de contournement** : Le nombre maximum d'entrées qui peuvent être contournées dans la partition programmée. Si plus de ce nombre d'entrées ont été contournées, la partition ne peut pas être armée. Lorsque ce champ est réglé sur 0, il n'y a pas de limite au nombre d'entrées contournées.
- **Nombre maximum d'utilisateurs** : Si l'option **Activer comptage d'utilisateur** est sélectionnée (onglet **Options (1)**), ce champ vous permet de définir le nombre maximum d'utilisateurs qui peuvent se trouver dans la partition en même temps. Par exemple, si la limite d'utilisateurs est fixée à 10, le 11e utilisateur qui tente d'entrer dans la partition se verra refuser l'accès.

  Cette fonctionnalité est utile lorsqu'il y a un code d'incendie, de sécurité ou de santé et de sûreté limitant le nombre de personnes autorisées dans une certaine partition, ou pour limiter le nombre d'utilisateurs entrant dans un parking. Vous pouvez définir une **Sortie Nombre d'utilisateurs atteint** (onglet **Sorties**) qui sera activée lorsque la partition est à son nombre d'utilisateurs maximum.

  Ce champ doit être défini sur une valeur supérieure à zéro pour permettre le comptage des partitions. S'il n'y a pas de limite sur le nombre d'utilisateurs autorisés dans la partition, vous pouvez définir ce champ à la valeur maximale (65535).

- **Code Client** : Ce code représente la partition dans les rapports adressés à la station de surveillance centrale. Il s'agit généralement d'un nombre hexadécimal, mais le format peut dépendre de la compatibilité du récepteur. Si le code client de la partition est laissé à la valeur par défaut (FFFF), la partition utilisera le **Code client** réglé dans signalisation du SERVICE (**Programmation | Services | Général**).

  Il peut être utile de définir des codes client différents pour chaque partition dans les situations où un seul Protege GX système contient plusieurs locations différentes, comme des bureaux ou des appartements.

- **Interverrouiller groupe de partitions** : Lorsqu'une partition est dotée d'un groupe de partition d'interverrouillage, elle ne peut être désarmée que si toutes les autres partitions du groupe sont armées. Cela peut garantir qu'une partition de haute sécurité ne sera pas désarmée tant que les partitions qui l'entourent ne seront pas sécurisées.
- **Nombre d'entrée Intelligente** : La fonction d'entrée intelligente empêche les fausses alarmes dans les partitions en comptant plusieurs activations d'entrée uniques avant d'activer l'alarme. L'alarme ne sera pas activée jusqu'à ce que ce nombre d'entrées uniques soient ouvertes dans un certain temps.

  Pour utiliser cette fonction, cochez l'option **Activer les entrées intelligentes** dans l'onglet **Options (2)**. La période de temps est définie dans le champ de la **Minuterie Entrée Intelligente** ci-dessus.

- **Signaler ID** : L'ID de rapport de la partition est le numéro de groupe qui représentera cette partition spécifique à la station de surveillance. Le prochain ID disponible sera automatiquement attribué lors de la création de chaque partition, ou vous pouvez attribuer manuellement les ID requis. Si une partition a été attribuée à un numéro supérieur au maximum qui peut être signalé à un service particulier, le service le plus élevé possible sera signalé.

  Vous pouvez visualiser et exporter les ID de rapport de partition à l'aide du générateur de cartes de rapport (**Rapports | Rapport de station centrale**). Pour plus d'informations, voir la note d'application 316 : Rapports au format Contact ID dans Protege GX et Protege WX.

- **Groupe de porte verrouillées à l'armement** : Lorsque cette partition est armée, les portes de ce groupe de portes seront automatiquement verrouillées. Ceci peut être utilisé pour s'assurer que toutes les portes d'entrée d'une partition sont verrouillées lorsque la partition est armée, empêchant ainsi les utilisateurs de pénétrer accidentellement dans une partition armée.

Services de rapports

Ce champ vous permet d'assigner les services de rapports qui enverront des rapports pour cette zone et toutes les entrées ou entrées de dérangement qui y sont programmées.

Les services peuvent être programmés dans **Programmation | Services**.

Mise en attente

- **Minuterie de mise en attente** : Lorsque l'option **Partition activée en mode mise en attente** est sélectionnée pour la partition (**onglet Options (1)**), ce champ détermine combien de temps (en minutes) un utilisateur peut rester dans cette partition avant d'être déplacé dans la **partition de réinitialisation du mode mise en attente**.

  Lorsque ce champ est défini sur 0, les utilisateurs ne seront jamais déplacés dans la partition de réinitialisation de mise en attente.
- **Partition de réinitialisation de mise en attente** : Lorsque l'option **partition activée en mode mise en attente** est sélectionnée pour la partition (onglet **Options (1)**), l'utilisateur sera "déplacé" vers la partition définie ici lorsque la **minuterie de mise en attente** est écoulée. Une fois que l'utilisateur a été déplacé dans la partition de réinitialisation de mise en attente de l'antiretour, les règles peuvent l'empêcher de quitter la partition physique dans laquelle il se trouve jusqu'à ce que son statut d'antiretour soit réinitialisé.

Retarder l'avertissement

- **Retarder l'avertissement du groupe de clavier** : Lorsque la partition a l'option **Retarder l'armement automatique** activée (onglet **Options (2)**), les claviers de ce groupe émettront un bip et afficheront un message d'avertissement lorsque la partition est sur le point de s'armer automatiquement. Pendant que le message est affiché, les utilisateurs peuvent se connecter au clavier et utiliser la **[DISARM]** touche pour empêcher l'armement automatique de la partition.

  L'option **Afficher les messages retardés d'avertissement de la partition** doit également être activée pour chaque clavier dans **Modules d'expansion | Claviers | Options 1**. Les messages de priorité supérieure (par exemple, les alarmes) peuvent remplacer l'avertissement de retard d'armement.

- **Retarder l'heure d'avertissement** : Lorsque l'option **Retarder l'armement automatique** est activée pour la partition (onglet **Options (2)**), l'armement automatique sera retardé du temps défini ici (en minutes). Utiliser ce paramètre pour donner aux utilisateurs suffisamment de temps pour quitter la partition ou se connecter au clavier et annuler l'armement.

Commandes

- Ce champ est utilisé pour envoyer des commandes de programmation à l'appareil. Il ne doit être utilisé que lorsqu'il est spécifiquement conseillé par la documentation ICT ou le support technique.

Partitions | Sorties

Sorties

- **Sortie de la cloche / Groupe de sorties programmables** : Cette sortie programmable ou groupe de sorties programmables est activé lorsqu'une alarme est générée dans la partition. La sortie de la cloche reste activée pendant l'**heure de l'alarme 1** (onglet **Configuration**) ou jusqu'à ce que la partition soit désarmée.

  L'activation de la sortie de la cloche dépend du type d'entrée qui a généré l'alarme. L'option **Activer sortie de sonnerie** dans **Programmation | Types d'entrées | Options 2** doit être activée.
- **Heure d'impulsion on/off de la sirène** : Ces champs sont utilisés pour faire en sorte que la sortie sirène ou le groupe de sorties programmables émettent des impulsions on et off lorsqu'ils sont activés.

  La sortie ou le groupe de sorties s'activera pendant le temps de pulsion on, s'éteindra pendant le temps de pulsion off, puis se répétera. Ces durées sont définies par incréments de 100ms. Par exemple, si le temps d'activation de l'impulsion est réglé sur 2 et que le temps de désactivation de l'impulsion est réglé sur 8, la sortie s'activera pendant 200 ms, s'éteindra pendant 800 ms, puis se répétera, pour un cycle total de 1 seconde.

  Si l'une ou l'autre des durées d'activation et de désactivation de l'impulsion est définie sur 0, la sortie s'activera en continu. Chacun de ces champs prend en charge une valeur maximale de 255 (25,5 secondes).
- **Sortie délai de sortie / Groupe de sorties programmables** : Cette sortie ou ce groupe de sorties programmables est activé pendant le délai de sortie de la partition. la fonction est désactivée lorsque le délai de sortie est terminé ou si la partition est encore désarmée.

  Utilisez cette sortie, généralement un signal sonore de clavier ou de lecteur, pour avertir les utilisateurs de quitter la partition avant qu'elle ne soit armée.
- **Délai de sortie Heure d'impulsion on/off** : Ces champs sont utilisés pour faire en sorte que la sortie du délai de sortie ou le groupe de sorties programmables s'active et s'éteigne lorsqu'ils sont activés.

  La sortie ou le groupe de sorties s'activera pendant le temps de pulsion on, s'éteindra pendant le temps de pulsion off, puis se répétera. Ces durées sont définies par incréments de 100ms. Par exemple, si le temps d'activation de l'impulsion est réglé sur 2 et que le temps de désactivation de l'impulsion est réglé sur 8, la sortie s'activera pendant 200 ms, s'éteindra pendant 800 ms, puis se répétera, pour un cycle total de 1 seconde.

  Si l'une ou l'autre des durées d'activation et de désactivation de l'impulsion est définie sur 0, la sortie s'activera en continu. Chacun de ces champs prend en charge une valeur maximale de 255 (25,5 secondes).
- **Sortie délai d'entrée / Groupe de sorties programmables** : Cette sortie ou ce groupe de sorties programmables est activé pendant le délai d'entrée de la zone. La fonction est désactivée lorsque le délai d'entrée expire (ce qui active l'alarme) ou lorsque la partition est désarmée.

  Utilisez cette sortie, généralement un signal sonore de clavier ou de lecteur, pour avertir les utilisateurs de désarmer la partition avant que l'alarme ne soit activée.
- **Délai d'entrée Heure d'impulsion on/off** : Ces champs sont utilisés pour faire en sorte que la sortie du délai d'entrée ou le groupe de sorties programmables s'active et se désactive lorsqu'il est activé.

La sortie ou le groupe de sorties s'activera pendant le temps de pulsion on, s'éteindra pendant le temps de pulsion off, puis se répétera. Ces durées sont définies par incréments de 100ms. Par exemple, si le temps d'activation de l'impulsion est réglé sur 2 et que le temps de désactivation de l'impulsion est réglé sur 8, la sortie s'activera pendant 200 ms, s'éteindra pendant 800 ms, puis se répétera, pour un cycle total de 1 seconde.

Si l'une ou l'autre des durées d'activation et de désactivation de l'impulsion est définie sur 0, la sortie s'activera en continu. Chacun de ces champs prend en charge une valeur maximale de 255 (25,5 secondes).

- **Sortie de la sirène / Groupe de sorties programmables** : Cette sortie programmable ou ce groupe de sorties programmables est activé lorsque la partition est désarmée. Cette fonction est désactivée lorsque la partition commence à s'armer.

  Cette fonction peut être utilisée pour donner aux utilisateurs une indication visuelle lorsque la partition est désarmée (par exemple, la LED verte sur un clavier). Ceci pourrait également être utilisé pour activer tout relais de verrouillage qui n'est pas contrôlé par des lecteurs, de sorte que les portes internes se déverrouillent lorsque la partition est désarmée. Les sorties désarmées peuvent également entraîner d'autres processus qui sont activés lorsqu'une partition est désarmée.
- **Heure d'impulsion on/off désarmée** : Ces champs sont utilisés pour faire en sorte que la sortie désarmée ou le groupe de sorties programmables émettent des impulsions on et off lorsqu'ils sont activés.

  La sortie ou le groupe de sorties s'activera pendant le temps de pulsion on, s'éteindra pendant le temps de pulsion off, puis se répétera. Ces durées sont définies par incréments de 100ms. Par exemple, si le temps d'activation de l'impulsion est réglé sur 2 et que le temps de désactivation de l'impulsion est réglé sur 8, la sortie s'activera pendant 200 ms, s'éteindra pendant 800 ms, puis se répétera, pour un cycle total de 1 seconde.

  Si l'une ou l'autre des durées d'activation et de désactivation de l'impulsion est définie sur 0, la sortie s'activera en continu. Chacun de ces champs prend en charge une valeur maximale de 255 (25,5 secondes).
- **Sortie armée / Groupe de sorties programmables** : Cette sortie programmable ou ce groupe de sorties programmables est activé lorsque la partition est armée avec succès. Cette fonction est désactivée lorsque la partition est désarmée.

  Cette fonction peut être utilisée pour donner aux utilisateurs une indication visuelle lorsque la partition est armée (par exemple, la LED rouge sur un clavier), empêchant ainsi les utilisateurs de tenter de pénétrer dans des partitions armées. Les sorties armées sont également utiles pour piloter d'autres processus qui sont activés lorsqu'une partition est armée.
- **Heure d'impulsion on/off armée** : Ces champs sont utilisés pour faire en sorte que la sortie armée ou le groupe de sorties programmables émettent des impulsions on et off lorsqu'ils sont activés.

  La sortie ou le groupe de sorties s'activera pendant le temps de pulsion on, s'éteindra pendant le temps de pulsion off, puis se répétera. Ces durées sont définies par incréments de 100ms. Par exemple, si le temps d'activation de l'impulsion est réglé sur 2 et que le temps de désactivation de l'impulsion est réglé sur 8, la sortie s'activera pendant 200 ms, s'éteindra pendant 800 ms, puis se répétera, pour un cycle total de 1 seconde.

  Si l'une ou l'autre des durées d'activation et de désactivation de l'impulsion est définie sur 0, la sortie s'activera en continu. Chacun de ces champs prend en charge une valeur maximale de 255 (25,5 secondes).
- **Sortie programmable des zones contournées / Groupe de sorties programmables** : Cette sortie ou ce groupe de sorties programmables est activé lorsque la partition est armée avec une ou plusieurs entrées contournées. Cette fonction est désactivée lorsque la partition est désarmée.

  Cette sortie ne sera activée que par les entrées dont l'option **Activer la sortie de contournement** est activée dans le type d'entrée (**Programmation | Types d'entrée | Options 2**).
- **Heure d'impulsion on/off des entrées contournées** : Ces champs sont utilisés pour faire en sorte que la sortie des entrées contournées ou le groupe de sorties programmables émettent des impulsions on et off lorsqu'ils sont activés.

La sortie ou le groupe de sorties s'activera pendant le temps de pulsion on, s'éteindra pendant le temps de pulsion off, puis se répétera. Ces durées sont définies par incréments de 100ms. Par exemple, si le temps d'activation de l'impulsion est réglé sur 2 et que le temps de désactivation de l'impulsion est réglé sur 8, la sortie s'activera pendant 200 ms, s'éteindra pendant 800 ms, puis se répétera, pour un cycle total de 1 seconde.

Si l'une ou l'autre des durées d'activation et de désactivation de l'impulsion est définie sur 0, la sortie s'activera en continu. Chacun de ces champs prend en charge une valeur maximale de 255 (25,5 secondes).

- **Sortie d'alarme anti-effraction / groupe de sorties** : Cette sortie ou ce groupe de sorties est activé(e) lorsqu'une alarme 24 heures / autoprotection est générée dans la zone. Elle est désactivée lorsque la partie 24 heures du secteur est désarmée (désactivée). Cette fonction peut être utilisée pour alerter le personnel qu'une entrée a été altérée, sans activer la sortie de sonnerie du secteur.

  Cette sortie ne sera activée que par les entrées dont le type d'entrée (**Programmation | Types d'entrée | Options 2**) contient l'option **Activer sortie sabotage 24 heures**.

- **Temps d'activation et de désactivation de l'impulsion de l'alarme d'autoprotection** : Ces champs sont utilisés pour activer et désactiver l'impulsion de la sortie ou du groupe de sorties d'alarme anti-sabotage lorsqu'il est activé.

  La sortie ou le groupe de sorties s'activera pendant le temps de pulsion on, s'éteindra pendant le temps de pulsion off, puis se répétera. Ces durées sont définies par incréments de 100ms. Par exemple, si le temps d'activation de l'impulsion est réglé sur 2 et que le temps de désactivation de l'impulsion est réglé sur 8, la sortie s'activera pendant 200 ms, s'éteindra pendant 800 ms, puis se répétera, pour un cycle total de 1 seconde.

  Si l'une ou l'autre des durées d'activation et de désactivation de l'impulsion est définie sur 0, la sortie s'activera en continu. Chacun de ces champs prend en charge une valeur maximale de 255 (25,5 secondes).

- **Sortie de mémoire d'alarme / Groupe de sorties programmables** : Cette sortie ou ce groupe de sorties programmables est activé dès qu'une alarme est générée dans la partition. Cette fonction est désactivée lorsque la partition est désarmée. Cette fonction peut être utilisée pour avertir les utilisateurs lorsqu'il y a eu une alarme, les empêchant ainsi de pénétrer dans une partition potentiellement non sécurisée.

  Cette sortie ne sera activée que par les entrées dont l'option **Activer la sortie mémoire** est activée dans le type d'entrée (**Programmation | Types d'entrée | Options 2**).

- **Mémoire d'alarme Heure d'impulsion on/off** : Ces champs sont utilisés pour faire en sorte que la sortie de mémoire d'alarme ou le groupe de sorties programmables émettent des impulsions on et off lorsqu'ils sont activés.

  La sortie ou le groupe de sorties s'activera pendant le temps de pulsion on, s'éteindra pendant le temps de pulsion off, puis se répétera. Ces durées sont définies par incréments de 100ms. Par exemple, si le temps d'activation de l'impulsion est réglé sur 2 et que le temps de désactivation de l'impulsion est réglé sur 8, la sortie s'activera pendant 200 ms, s'éteindra pendant 800 ms, puis se répétera, pour un cycle total de 1 seconde.

  Si l'une ou l'autre des durées d'activation et de désactivation de l'impulsion est définie sur 0, la sortie s'activera en continu. Chacun de ces champs prend en charge une valeur maximale de 255 (25,5 secondes).

- **Sortie / groupe de sorties atteint par le compte utilisateur** : Cette sortie ou ce groupe de sorties est activé(e) lorsque le nombre d'utilisateurs dans une zone atteint le **nombre maximal d'utilisateurs** défini dans l'onglet **Configuration**. Il est désactivé lorsque la zone ne contient plus le nombre maximum d'utilisateurs. Par exemple, cela peut être utilisé dans un parking pour activer un panneau "Parking complet" lorsqu'il n'y a plus de places disponibles.

  L'option **Activer le comptage d'utilisateurs** doit être sélectionnée dans l'onglet **Options 1**.

- **Durée d'activation/désactivation de l'impulsion de comptage de l'utilisateur** : Ces champs permettent d'activer et de désactiver l'impulsion de la sortie ou du groupe de sorties atteint par le comptage utilisateur lorsqu'il est activé.

La sortie ou le groupe de sorties s'activera pendant le temps de pulsion on, s'éteindra pendant le temps de pulsion off, puis se répétera. Ces durées sont définies par incréments de 100ms. Par exemple, si le temps d'activation de l'impulsion est réglé sur 2 et que le temps de désactivation de l'impulsion est réglé sur 8, la sortie s'activera pendant 200 ms, s'éteindra pendant 800 ms, puis se répétera, pour un cycle total de 1 seconde.

Si l'une ou l'autre des durées d'activation et de désactivation de l'impulsion est définie sur 0, la sortie s'activera en continu. Chacun de ces champs prend en charge une valeur maximale de 255 (25,5 secondes).

- **Sortie armement différé de partition débutée / Groupe de sorties programmables** : Cette sortie ou ce groupe de sorties programmables est activé lorsque la partition reporte l'armement automatique. Cette fonction est désactivée lorsque **Heure de différer l'avertissement** (**onglet Configuration**) expire et que la partition s'arme ou lorsque l'armement est annulé par un clavier. Utilisez cette fonction pour notifier les utilisateurs se trouvant dans la partition qu'elle est sur le point de commencer à s'armer.

  Le **report de l'armement automatique** doit être activé dans l'onglet **Options 2**.

- **Différer l'armement a déclenché l'heure d'impulsion on/off** : Ces champs sont utilisés pour faire en sorte que la sortie armement différé ou le groupe de sorties programmables émettent des impulsions on et off lorsqu'ils sont activés.

  La sortie ou le groupe de sorties s'activera pendant le temps de pulsion on, s'éteindra pendant le temps de pulsion off, puis se répétera. Ces durées sont définies par incréments de 100ms. Par exemple, si le temps d'activation de l'impulsion est réglé sur 2 et que le temps de désactivation de l'impulsion est réglé sur 8, la sortie s'activera pendant 200 ms, s'éteindra pendant 800 ms, puis se répétera, pour un cycle total de 1 seconde.

  Si l'une ou l'autre des durées d'activation et de désactivation de l'impulsion est définie sur 0, la sortie s'activera en continu. Chacun de ces champs prend en charge une valeur maximale de 255 (25,5 secondes).

- **Sortie d'Échec d'armement / Groupe de sorties programmables** : Cette sortie ou ce groupe de sorties programmables est activé pendant 5 secondes chaque fois que la partition ne parvient pas à s'armer (par exemple, lorsque certaines entrées n'ont pas été contournées).
- **Sortie prête / Groupe de sortie** : Cette sortie ou ce groupe de sorties est activé(e) lorsque toutes les entrées et entrées de dérangement programmées dans le secteur sont fermées, signalant ainsi que le secteur est prêt à être armé. Elle est désactivée lorsque le secteur est armé ou lorsqu'une entrée ou une entrée de dérangement est ouverte et que le secteur n'est plus prêt à être armé.

Partitions | Options(1)

Options générales

- **Restauration de l'entrée sur la coupure de la sonnerie** : Avec cette option activée, lorsque cette partition passe en alarme, toutes les entrées qui sont ouvertes entrent dans un état de "verrouillage de la sirène". Cela signifie que si les entrées sont rétablies (fermées) ou rouvertes, la station de surveillance n'en sera pas informée jusqu'à ce que la sonnerie s'arrête ou soit réduite au silence.

  Cette option empêche le fonctionnement de la fonction **Relancer l'heure de la sonnerie** dans **Programmation | Types d'entrée | Options (2)**.

- **Réarmement activé** : Avec cette option activée, chaque fois que la partition est désarmée, elle sera automatiquement réarmée après un certain temps. Le délai avant le réarmement est défini par **Heure de réarmer la partition** (onglet **Configuration**). Cette fonction arme par force la partition, il faut donc sélectionner **Activer l'armement par force** (onglet **Options (2)**).

  Cette fonction doit être utilisée pour les partitions qui sont utilisées pour la surveillance et le contrôle du système, qui ne doivent jamais être désarmées. Il peut également être utilisé pour s'assurer que les chambres fortes des banques, les guichets automatiques et autres ne sont pas désarmés plus longtemps que le temps programmé.

  Lorsque vous activez le réarmement, vous devez armer et désarmer la partition pour que le réglage prenne effet.

- **Armer partition enfant** : Lorsque cette option est activée, chaque fois que cette partition termine son armement, la **partition Enfant** (onglet **Configuration**) sera armée.

  Cette option doit être activée dans le(s) secteur(s) parent(s).

- **Armer l'enfant si toutes les autres partitions sont armées** : Lorsque cette option est activée, la **partition Enfant** (onglet **Configuration**) sera armée chaque fois que cette partition est armée, à condition que toutes les autres partitions parent soient déjà armées. L'option **Armer la partition enfant** ci-dessus doit également être activée.

  Par exemple, il peut y avoir trois partitions; A, B et C, où C est partition enfant de A et B. Par défaut, C sera armé lorsque A OU B est armé. Avec cette option activée, la partition C sera armée lorsque A ET B sont tous deux armés.

  Cette option doit être activée dans le(s) secteur(s) parent(s).

- **Désarmer partition enfant** : Lorsque cette option est activée, chaque fois que cette partition termine son désarmement, la **partition Enfant** (onglet **Configuration**) sera désarmée.

  Cette option doit être activée dans le(s) secteur(s) parent(s).

- **Désarmer l'enfant si toutes les autres partitions sont désarmées** : Lorsque cette option est activée, la **partition Enfant** (onglet **Configuration**) sera désarmée chaque fois que cette partition est désarmée, à condition que tous les autres partitions parent soient déjà désarmées.

  Par exemple, il peut y avoir trois partitions; A, B et C, où C est partition enfant de A et B. Par défaut, C sera désarmé lorsque A OU B est désarmé. Avec cette option activée, la partition C sera désarmée lorsque A ET B sont tous deux désarmés.

  Cette option doit être activée dans le(s) secteur(s) parent(s).

- **Utiliser l'armement par force brute sans surveillance** : En général, une partition ne peut pas être armé de force s'il y a des entrées ouvertes avec l'option **Forcer Entrée** désactivée (**Programmation | Types d'entrée | Options (1)**). L'activation de cette option vous permet "d'armer la partition par force brute" en utilisant des méthodes non surveillées ou à distance, même si ces entrées sont ouvertes.

  Utiliser cette option pour s'assurer que la partition peut toujours être armée par force par le système (par exemple, sur programmation ou réarmement automatique), un opérateur ou un utilisateur à un lecteur de carte. Cela ne permettra pas aux utilisateurs d'un clavier d'armer la partition par force brute.

  Par défaut, lorsqu'une zone est armée par force brute, le statut est défini sur Armé. Pour utiliser Armé par force pour le statut, entrez la commande `UnattendedForceArm = true`.

- **Partition activée en mode de mise en attente** : Le mode mise en attente vous permet de limiter le temps que les utilisateurs passent dans une partition. Ce système est couramment utilisé dans les parkings, où les utilisateurs doivent traverser la partition de stationnement publique pour atteindre leur place de stationnement désignée.

  Lorsqu'un utilisateur entre dans la partition, la **minuterie de mise en attente** démarre. S'il reste dans la partition plus longtemps que le temps imparti, le système déplace automatiquement l'utilisateur dans la **partition de réinitialisation de mise en attente** (une "partition d'attente" virtuelle). Lorsque l'utilisateur tente de quitter la partition physique, le système détecte qu'il se trouve dans la mauvaise partition et lui refuse la sortie en raison de la violation de l'antiretour. L'utilisateur ne peut pas sortir tant que son statut antiretour n'a pas été réinitialisé (par exemple, par un opérateur ou en badgeant à un lecteur désigné qui permet de sortir de la partition de mise en attente).

  Les éléments suivants doivent être configurés pour achever la programmation des partitions de mise en attente :

  - **Minuterie de mise en attente** (onglet **Configuration**)
  - **Partition de réinitialisation de mise en attente** (onglet **Configuration**)
  - **Le mode de passback d'entrée/sortie** est réglé sur passback dur (**Programmation | Types de portes | Général**)

- **Partition intérieure/extérieure de la porte** (**Programmation | Portes | Général**)
- **Compte d'expiration de mise en attente de l'utilisateur activé** (**Users | Users | Options**)

Pour de plus amples informations et des exemples de programmation, voir la Note d'application 341 : Fonctionnalité de la partition de programmation de mise en attente dans Protege GX .

Options de signalisation

- **Rapport d'armement** : Avec cette option activée, chaque fois que cette partition est armée, un rapport sera envoyé à la station de surveillance et enregistré dans le journal des événements. Ce rapport inclut l'utilisateur qui a initié l'armement. Désactiver cette option lorsque ces rapports ne sont pas nécessaires (par exemple, pour les partitions de contrôle virtuelles).
- **Rapport de désarmement** : Avec cette option activée, chaque fois que cette partition est désarmée, un rapport sera envoyé à la station de surveillance et enregistré dans le journal des événements. Ce rapport inclut l'utilisateur qui a initié le désarmement. Désactiver cette option lorsque ces rapports ne sont pas nécessaires (par exemple, pour les partitions de contrôle virtuelles).
- **Rapport sur le désarmement de la partition 24 heures** : Lorsque cette option est activée, chaque fois que la partie 24 heures de cette partition est désarmée (désactivée), un rapport sera envoyé à la station de surveillance et enregistré dans le journal des événements. Ce rapport inclut l'utilisateur qui a initié le désarmement. Il n'y a pas de rapport équivalent disponible pour l'armement / l'activation de la partie 24 heures de la partition.
- **Rapport sur le contournement des utilisateurs** : Lorsque cette option est activée, chaque fois que cette partition est armée, elle rapportera toutes les entrées contournées de la partition. Les rapports seront envoyés à la station de surveillance et enregistrés dans le journal des événements. L'option **Rapport de contournement** doit également être activée pour la ou les entrées concernées dans **Programmation | Types d'entrée | Options (1)**.
- **Activer le comptage d'utilisateur** : Avec cette option activée, le système comptera le nombre d'utilisateurs dans la partition. Lorsqu'un utilisateur entre dans la partition, le compte est augmenté de un, et lorsqu'il en sort, le compte est diminué de un.

  Cette fonction ne doit être utilisée que dans les partitions desservies par des portes équipées de lecteurs d'entrée et de sortie, car REX et REN ne modifieront pas le nombre d'utilisateurs. La **porte intérieure/extérieure de la partition** doit être réglée correctement dans **Programmation | Portes | Général**. Il est recommandé d'utiliser le comptage de l'utilisateur en même temps que l'antiretour (voir **Programmation | Types de portes | Généralités**) afin de garantir la précision du comptage de l'utilisateur.

  Un certain nombre de fonctionnalités sont disponibles avec le comptage des utilisateurs :

  - **Nombre maximal d'utilisateurs** (onglet **Configuration**)

    Cette option doit être définie sur une valeur non nulle pour que le comptage des utilisateurs fonctionne.

  - **Nombre d'utilisateurs ayant atteint une sortie / groupe de sorties** (onglet **Sorties**)
  - **Armer sur le nombre d'utilisateurs à 0** (onglet **Options (1)**)
  - **Effacer le compte utilisateur lorsqu'il est armé** (onglet **Options (1)**)
  - **Empêcher l'armement sur un compte non nul** (onglet **Options (2)**)

  Pour plus d'informations, consulter la note d'application 205 : Comptage de partition dans Protege GX . Pour les applications avancées, voir la note d'application 278 : Comptage de partition par niveau d'accès dans Protege GX.

- **Armer le nombre d'utilisateurs à 0** : Lorsque l'option **Activer le comptage d'utilisateur** est sélectionnée ci-dessus, cette fonction entraîne l'armement automatique de la partition lorsque le comptage d'utilisateur atteint zéro. Cette fonction garantit que la partition sera sécurisée lorsque le dernier utilisateur quittera les lieux, qu'il ait ou non armé la partition. Cette fonction est particulièrement utile dans les grands bureaux où il n'est pas pratique pour les utilisateurs de vérifier s'il y a quelqu'un d'autre dans la partition.

  Il est recommandé d'utiliser cette fonction en même temps que les paramètres d'antiretour pour s'assurer que le nombre d'utilisateurs est exact. Sinon, la partition peut s'armer alors qu'il y a encore des personnes à l'intérieur.

- **Signaler immédiatement l'alarme d'entrée** : Lorsque cette option est activée, si une saisie d'entrée s'ouvre dans une partition armée, un rapport est immédiatement envoyé à la station de surveillance et au journal des événements, même si la partition est en retard de saisie. Un deuxième rapport sera généré si la partition passe en alarme. Lorsque cette option est désactivée, l'ouverture d'une entrée qui déclenche le délai de saisie ne sera pas signalée.

  Cette option s'applique aux entrées dont les options de **Saisie du délai d'entrée** et de **rapports d'alarmes** sont activées dans le type d'entrée (**Programmation | Types d'entrée | Options (1)**).

- **Effacer le compte utilisateur lorsqu'il est armé** : Lorsque cette option est activée (par défaut), le comptage des utilisateurs pour la partition (voir **Activer le comptage des utilisateurs** ci-dessus) sera effacé / remis à zéro lorsque la partition est armée. Lorsque cette option est désactivée, le compte des utilisateurs ne sera pas effacé.

Maintenir la partition de test de marche

- **Activer le maintien du test de marche lors du désarmement** : Un maintien du test de marche est un type particulier de test de marche qui permet de tester des entrées spécifiques à chaque fois que la partition est désarmée. Les entrées qui doivent être testées ont le **Tester pendant le maintien du test de marche** activé dans le type d'entrée (**Programmation | Types d'entrée | Options (2)**). Cette fonction est utilisée pour tester régulièrement un petit nombre d'entrées critiques, comme les boutons de panique.

  Lorsqu'un utilisateur tente de désarmer la partition à partir d'un clavier, le maintien du test de marche commence automatiquement. Toutes les entrées requises doivent être testées (ouvertes) avant que le **temps de test maximum** ne soit écoulé. Si le test se termine avant que toutes les entrées aient été testées, la zone ne sera pas désarmée.

  Pendant le test, le clavier émet des bips réguliers et affiche des messages, notamment le nom de chaque entrée testée. Après l'ouverture de la première entrée, la **sortie / le groupe de sorties à activer pendant le test** (défini ci-dessous) sera activé. Ils sont désactivés lorsque le test est terminé ou qu'il arrive à échéance.

  Pour les instructions de programmation, voir la note d'application 197 : Configuration du maintien d'un test de marche dans Protege GX .

- **Durée maximale de test (secondes)** : La durée maximale (en secondes) que le maintien du test de marche fonctionnera. Après ce délai, le test est terminé et la partition ne sera pas désarmée. Vérifier que le temps est suffisant pour tester toutes les entrées requises.
- **Code d'identification du groupe de contacts pour le démarrage du test** : Ce code d'événement Contact ID est envoyé à la station de surveillance lorsque le maintien de test de marche commence.
- **Code d'identification du groupe de contacts pour l'activation de l'entrée** : Ce code d'événement Contact ID est envoyé à la station de surveillance lorsque chaque entée est activée pendant le maintien de test de marche.
- **Code d'identification du groupe de contacts pour le test réussi** : Ce code d'événement Contact ID est envoyé à la station de surveillance lorsque le maintien de test de marche est réussi commence (c'est-à-dire que toutes les entrées ont été activées avec succès).
- **Code d'identification du groupe de contacts pour le test annulé** : Ce code d'événement Contact ID est envoyé à la station de surveillance lorsque le maintien de test de marche est annulé manuellement ou le temps est écoulé.
- **Sortie / Groupe de sortie à activer pendant le test** : Cette sortie ou ce groupe de sortie est activé pendant le maintien du test de marche dès que la première entrée a été activée. C'est désactivé quand le test est terminé ou quand le temps est écoulé. Utiliser cette option pour informer les utilisateurs que le test est actif et les inviter à activer leurs entrées.

Partitions | Options(2)

Options avancées

- **Activer armement de séjour** : Lorsqu'une partition est armée de séjour, seules les entrées dont l'option **Entrée de séjour** est activée (**Programmation | Types d'entrée | Options (1)**) seront surveillées. Par exemple, cela vous permet d'armer le périmètre d'une partition sans armer les capteurs internes, afin que les utilisateurs puissent rester en sécurité à l'intérieur. Avec cette option désactivée, la partition ne peut pas être armée de séjour.
- **Activer armement par force** : Lorsqu'une partition est armée par force, elle est armée sans tester les entrées. La partition sera armée même si des entrées sont ouvertes, à condition que l'option **Entrée par force** soit activée pour ces entrées (**Programmation | Types d'entrée | Options (1)**). Quand cette option est désactivée, la partition ne peut pas être armée par force.

  Voir aussi **Utiliser l'armement par force brute sans surveillance** ci dessous.

- **Activer l'armement instantané** : Lorsqu'une partition est armée instantané, elle s'arme immédiatement avec un délai de sortie d'une seconde. De même, toutes les entrées qui devraient normalement initier le délai de saisie déclenchent l'alarme immédiatement (c'est-à-dire que toutes les entrées sont traitées comme des entrées "instantanées"). Quand cette option est désactivée, la partition ne peut pas être armée instantané.

  Les partitions peuvent être armées instantanées ou armés par force instantanées à partir du logiciel, et armées séjour instantanées ou armées par force instantanées à partir d'un clavier.

- **Ne pas armer si condition trouble** : Lorsque cette option est activée, l'armement de la partition sera empêché s'il y a une entrée trouble ouverte dans le système. Cela permet de s'assurer que toutes les conditions trouble sont résolus avant que la partition ne soit armée.

  Ceci est utile pour les partitions de haute sécurité qui ne doivent pas être libérées avant que tous les problèmes soient résolus.
- **Partition de contrôle de chambre forte :**: Lorsque cette option est activée, la partition ne sera pas désarmée avant que la période de retard définie ne soit écoulée. Le **Délai de désarmement de la chambre forte** est défini dans l'onglet **Configuration**. Cela permet d'éviter que des partitions de très haute sécurité, comme les coffres-forts des banques, ne puissent être désarmées rapidement en cas de cambriolage.

  Pour plus d'informations et d'instructions de programmation, consulter la note d'application 338 : Programmation Protege Claviers.

- **Contrôle de la chambre forte à double code** : Lorsque cette option est activée, deux utilisateurs distincts doivent se connecter à un clavier et appuyer sur le bouton de désarmement afin de désarmer la partition. Une fois que le premier utilisateur a appuyé sur la touche de désarmement, le délai de désarmement de la chambre forte doit expirer avant que le deuxième utilisateur puisse saisir son code. Le temps alloué au deuxième utilisateur pour désarmer la partition est le **Délai de double code de la chambre forte** défini dans l'onglet **Configuration**.

  Le paramètre de **la partition de contrôle de la chambre forte** ci-dessus doit également être activé.

- **Empêcher l'armement sur un compte non nul** : Lorsque le comptage des utilisateurs est activé (onglet **Options (1)**), cette option empêche l'armement de la partition lorsque le comptage des utilisateurs n'est pas nul. Cela garantit que la partition ne peut pas être armée (manuellement ou automatiquement) lorsqu'il y a encore des utilisateurs dans la partition.

  Il est recommandé d'utiliser cette fonction en même temps que les paramètres d'antiretour pour s'assurer que le nombre d'utilisateurs est exact. S'il y a une erreur dans le comptage des utilisateurs, il peut devenir impossible d'armer la partition même après le départ de tous les utilisateurs.

- **Toujours vérifier horaire de partition** : Par défaut, la partition ne vérifie **l'horaire d'armement/désarmement** (onglet **Configuration**) que sur les bords, c'est-à-dire lorsque l'horaire devient valide ou invalide. Cela signifie que la partition peut être désarmée ou armée manuellement, quel que soit le statut de l'horaire.

  Lorsque cette option est activée, la partition vérifie l'horaire toutes les minutes. Si la partition n'est pas dans l'état armé/désarmé requis par l'horaire, elle passera dans l'état correct.

- **Activer l'entrée intelligente :** Par défaut, une partition se met en alarme sur la base de l'activation d'une seule entrée. En mode entrée intelligente, plusieurs entrées uniques doivent être activées avant que la partition n'active l'alarme. Ceci est utile pour éviter les fausses alarmes.

  Lorsqu'une entrée est ouverte dans la partition armée, une minuterie démarre en fonction de la **minuterie entrée intelligente** (onglet **Configuration**). La partition comptera les activations d'entrée uniques (la réactivation de la même entrée n'augmentera pas le compteur). Si le nombre d'activations atteint le **nombre d'entrée intelligente** (onglet **Configuration**), l'alarme sera activée. Le même nombre d'activations est nécessaire pour déclencher le délai de saisie.

  La réponse de la partition dépend du type d'entrée de l'entrée finale qui est déclenchée. Par exemple, si la première entrée déclenchait le délai de saisie mais que la dernière provoque une alarme instantanée, la partition se mettra en alarme instantané.

  Les entrées intelligentes peuvent être utilisées conjointement avec la fonction de délai de notification à distance pour envoyer des rapports d'alarme confirmés à la station de surveillance. Pour plus d'informations, consultez Note d'application 312 : Minimiser la transmission hors site des faux alarmes dans Protege GX et Protege WX.

- **Partition peut être réinitialisée** : Lorsque cette option est activée, la partition peut être réarmée à partir d'un clavier sans être désarmée au préalable. Cela signifie qu'une partition qui se met en alarme peut être réinitialisée (en faisant taire la sortie de la sonnerie) sans être désarmée. Utiliser cette option pour les partitions qui ne devraient pas être désarmées après une alarme.

Options d'armement

- **Retarder armement automatique** : Lorsque cette option est activée, chaque fois que la partition commence à s'armer automatiquement selon un horaire, l'armement peut être différé (retardé) pour une période de temps définie. Les utilisateurs sont avertis que la partition est sur le point de s'armer, ce qui leur permet de quitter la partition ou de se connecter au clavier et d'appuyer sur la touche de désarmement pour retarder l'armement automatique.

  L'option **Toujours vérifier l'horaire de la partition** (voir ci-dessus) **doit être désactivée** car elle annule tout armement retardé.

  Les options suivantes sont disponibles :
  - L'option **Retarder l'heure de l'avertissement** (onglet **Configuration**) détermine la durée pendant laquelle la partition affichera l'avertissement avant de commencer à s'armer.
  - Vous pouvez donner aux utilisateurs une indication visuelle et/ou sonore que la partition est sur le point d'être armée en utilisant **Retarder l'avertissement du groupe de clavier** (onglet **Configuration**) et **Retarder l'armement de sortie ou d'un groupe de sorties d'une partition** (onglet **Sorties**).
  - Lorsqu'un utilisateur retarde l'armement à partir du clavier, l'option **L'heure de réarmement de la partition** (onglet **Configuration**) définit la durée d'attente de la partition avant de tenter de s'armer à nouveau.
  - Par ailleurs, la commande `DemandeHeureRetard = vrai` permet aux utilisateurs de spécifier le nombre d'heures pendant lesquelles l'armement sera retardé lorsqu'ils annulent l'armement au clavier.
  - La commande `ReArmAsDeferArea = true` permet à la partition de retardé le réarmement automatique, de sorte que l'armement retardé peut être utilisé parallèlement à la fonction de **Réarmement activé** (onglet **Options (1)**).

  Pour plus d'informations et d'instructions de programmation, consulter la note d'application 338 : Programmation Protege Claviers.

- **Toujours armer par force utilisant le lecteur de carte** : Lorsque cette option est activée, chaque fois qu'un utilisateur arme une partition à l'aide d'un lecteur de carte, la partition sera armée par force. Si cette option est désactivée, les entrées ouvertes peuvent empêcher l'armement de la partition.

  Les options d'armement à l'aide d'un lecteur de carte se trouvent sous **Mode d'armement du lecteur** dans **Modules d'expansion | Modules d'expansion de lecteur | Lecteur 1/2** .

- **Désactiver sortie de la sortie sur armement de séjour** : Lorsque cette option est activée, la **Délai de sortie de la sortie/ groupe de sortie** (onglet **Sorties**) ne sera pas activé lorsque la partition est armée de séjour. Ceci est utile lorsqu'il n'est pas nécessaire d'inviter les utilisateurs à quitter la partition armée.
- **Effacer mémoire d'alarme après l'armement** : Lorsque cette option est activée (par défaut), la mémoire d'alarme de la partition est effacée chaque fois que la partition est armée. Lorsqu'elle est désactivée, les alarmes restent dans la mémoire d'alarme jusqu'à ce qu'un utilisateur les reconnaisse sur un clavier (**[MENU] [5] [1]**).
- **Activer rapport armement en retard** : Lorsque cette option est activée, le système générera un rapport pour la station de surveillance et le journal des événements lorsque la partition est armée plus tard que prévu. Le rapport est généré si la partition est toujours désarmée lorsque **l'horaire d'armement normal** défini ci-dessous devient invalide. Cela permet de s'assurer que les opérateurs et les stations de surveillance sont alertés de toutes anomalies.
- **Activer le rapport de désarmement anticipé** : Lorsque cette option est activée, le système générera un rapport pour la station de surveillance et le journal des événements lorsque la partition est désarmée plus tôt que prévu. Le rapport est généré si la partition est désarmée avant que l'horaire d'armement normal défini ci-dessous devienne **valide**. Cela permet de s'assurer que les opérateurs et les stations de surveillance sont alertés de toutes anomalies.
- **Désactiver le réarmement sur horaire** : Lorsque cette option est activée, le réarmement automatique sera désactivé lorsque la partition a été désarmée par **l'horaire d'armement/désarmement** (onglet **Configuration**). Utiliser cette option pour s'assurer que la partition ne se réarme pas automatiquement lorsqu'elle est censée être désarmée.

  La commande `ReArmLevelTrigger = true` empêche la partition de se réarmer automatiquement pendant que l'horaire est valide, quelle que soit la façon dont la partition a été désarmée.
- **L'utilisateur Réarme la partition en mode séjour** : Avec cette option activée, lorsque certains utilisateurs désarment la partition, celle-ci se réarmera automatiquement en mode séjour après un certain temps. Les utilisateurs doivent avoir l'option **Réarmer la partition en mode séjour** activée dans **Utilisateurs | Utilisateurs | Options**. La partition restera désarmée pendant la durée spécifiée dans le paramètre **Temps de réarmement** (onglet **Configuration**).

  Cette option est utile pour permettre aux utilisateurs d'entrer dans le bâtiment pour désarmer temporairement la partition et rester à l'intérieur pendant que le périmètre est à nouveau sécurisé.

  L'armement de séjour doit être activé (ci-dessus).

Options d'alerte

L'opération Squawk n'est pas prise en charge sur les sorties des modules d'expansion du lecteur embarqué du contrôleur.

- **Alerte de la sonnerie au début de l'armement** : Lorsque cette option est activée, la **sortie de la sonnerie** de la partition (onglet **Sorties**) émettra une alerte (un son bref) lorsque la partition commence à s'armer.
- **Alerte de la sonnerie à l'armement fini** : Lorsque cette option est activée, la **sortie de la sonnerie** de la partition (onglet **Sorties**) émettra une alerte (un son bref) lorsque la partition a bien terminé de s'armer.
- **Cri de sonnette seulement lorsque aucune surveillance** : Lorsque cette option est activée, la sortie de cloche n'émet un signal sonore que lorsque la zone est armée ou désarmée par une méthode non surveillée telle qu'une programmation, un réarmement automatique ou une fonction programmable. Elle n'émet pas de signal sonore lorsqu'elle est armée ou désarmée par le clavier ou le lecteur de cartes.

  Une ou plusieurs des autres **options d'alerte** doivent également être activées.
- **Alerte de la sonnerie au désarmement** : Lorsque cette option est activée, **la sortie de la sonnerie** de la partition (onglet **Sorties**) émettra deux fois une alerte lorsque la partition est désarmé.
- **Alerte de sonnerie sur rapport de succès** : Lorsque cette option est activée, **la sortie de sonnerie** de la partition (onglet **Sorties**) émettra une alerte lorsqu'un rapport "partition armée" a été envoyé avec succès et que le service de notification en a accusé réception.

Horaire

- **Horaire de désarmement normal** : Cet horaire définit quand la partition doit être désarmée un jour donné. Avec l'option **Activer le rapport de désarmement anticipé** ci-dessus, cela vous permet de générer des rapports si la partition est désarmée plus tôt que prévu.

  Par exemple, vous pouvez définir l'horaire normal de désarmement entre 8h30 et 9h30 tous les jours de la semaine. Cela représente le moment où vous attendez que la partition soit désarmée pour la première fois. Si la partition est désarmée à 7h00 du matin (avant que cet horaire ne devienne valide), un événement indiquera que la partition est "en avance sur le désarmement".
- **Horaire d'armement normal** : Cet horaire définit quand la partition doit être armée un jour donné. Avec l'option **Activer le rapport d'armement tardif** ci-dessus, cela vous permet de générer des rapports si la partition est armée plus tard que prévu.

  Par exemple, vous pouvez définir l'horaire normal de d'armement entre 8h30 et 9h30 tous les jours de la semaine. Cela représente le moment où vous attendez que la partition soit armée pour la dernière fois. Si la partition est toujours désarmée à 17h30 (lorsque l'horaire devient invalide), un événement indique que la partition est "en retard d'armement".

Commandes manuelles de partition

Un clic droit sur un enregistrement de partition dans **Programmation | Partitions** ou sur une icône de partition sur un plan d'étage ou une page d'état ouvre un menu avec des commandes manuelles pour cette partition.

Désarmer

- **Désarmer** : Désarme la partie principale de la partition. Cela désactive la supervision des entrées dans la partition.
- **Désarmer 24 heures** : Désarme la partie 24 heures de la partition. Cela désactive la surveillance des entrées trouble et de sabotage dans la partition.

Armer

- **Armer** : Arme à la fois la partie principale et la partie 24 heures de la partition. Dans un premier temps, le système teste toutes les entrées de la partition. Si l'un d'eux est ouvert ou altéré, il doit être contourné avant que la partition ne commence à s'armer. Ensuite, le délai de sortie de la partition commence. Lorsque le délai de sortie est terminé, la partition signale un armement réussi à la station de surveillance et dans le journal d'événements.

  Les entrées contournées ne sont pas surveillées par la partition armée.
- **Armement par force** : Arme par force la partie principale de la partition. Une partition peut être armée par force sans contourner aucunes entrées ouvertes. Ces entrées seront toujours surveillées par la partition armée par force.

  L'armement par force doit être activé dans l'onglet **Options (2)**. Les entrées ne peuvent pas être armées par force si l'option **Forcer Entrée** est désactivée dans le type d'entrée (**Programmation | Types d'entrée | Options (1)**).
- **Armer de séjour** : Arme de séjour la partie principale de la partition. Une partition armée de séjour surveillera certaines entrées ("entrées de séjour") mais en ignorera d'autres.

  L'armement de séjour doit être activé dans l'onglet **Options (2)**. Seules les entrées avec l'option **Entrée de séjour** activée dans le type d'entrée (**Programmation | Types d'entrée | Options (1)**) seront surveillées lorsque la partition est armée de séjour.
- **Armement instantané** : Arme instantané la partie principale de la partition. Lorsqu'une partition est armée instantané, le délai de sortie est réduit à 1 seconde. De même, toutes les entrées qui devraient normalement initier le délai d'entrée déclenchent l'alarme immédiatement (c'est-à-dire que toutes les entrées sont traitées comme des entrées "instantanées").

L'armement instantané doit être activé dans l'onglet **Options (2)**.

- **Armement par force instantané** : Arme par force la partie principale de la partition avec un délai de sortie d'une seconde. Toutes les entrées qui devraient normalement initier le délai d'entrée déclenchent l'alarme immédiatement (c'est-à-dire que toutes les entrées sont traitées comme des entrées "instantanées").

L'armement par force et l'armement instantané doivent être activés dans l'onglet **Options (2)**.

- **Armer 24 heures** : Arme la partie 24 heures de la partition pour permettre la surveillance et l'établissement de rapports sur les conditions de sabotage et les entrées trouble. Il n'y a pas de test ni de délai de sortie.
- **Activer le test de marche** : Arme la partition en mode test de marche, qui est utilisé pour tester la fonction d'entrée. Au cours d'un test de marche, les entrées de la partition ne génèrent pas d'alarmes et la surveillance de la station centrale est suspendue pour la partition. Un événement sera enregistré pour chaque activation d'entrée (même si l'entrée est activée plusieurs fois). Lorsque le test de marche se termine, un événement sera enregistré pour chaque entrée qui n'a pas été activée.

L'armement de la partition en mode test de marche n'est pas signalé à la station de surveillance.

- **Désactiver test de marche** : Désarme la partition pour terminer le test de marche. Cela n'est pas rapporté à la station de surveillance.
- **Faire taire l'alarme** : Si l'alarme a été activée, ceci fait taire l'alarme et désarme la partition.

Sorties

Les sorties représentent généralement des appareils physiques connectés au système Protege GX, tels que des sirènes, des bips, des indicateurs DEL et des relais de verrouillage de porte. Tout appareil ayant un état binaire On-Off peut être connecté à Protege GX en tant que sortie. Cela signifie que Protege GX peut être utilisé pour contrôler un large éventail d'appareils, de l'éclairage au CVC.

Cependant, les sorties n'ont pas besoin d'être physiques : Protege GX peut utiliser des sorties virtuelles pour suivre des états binaires sans avoir besoin d'un appareil physique. Cela permet une programmation avancée à l'aide d'horaires, de types d'entrée, d'automatisations et de fonctions programmables.

Sorties | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Nom d'affichage du clavier** : Le nom qui sera téléchargé vers le contrôleur. Ce dernier sera affiché sur le clavier et dans les rapports des services de surveillance IP. Le clavier ne peut afficher que les 16 premiers caractères du nom. Il doit donc décrire de manière concise l'emplacement physique et la fonction de l'appareil.

Adresse

- **Type de module** : Le type de module auquel la sortie est connectée (p. ex., un clavier, un module d'expansion de sortie).
- **Adresse du module** : L'**adresse physique** du module auquel la sortie est connectée.
- **Sortie du module** : L'index de la sortie sur le module connecté. Consulter le manuel d'installation correspondant pour les instructions de câblage.

Configuration

- **Calendrier d'activation** : Cet horaire est utilisé pour activer et désactiver automatiquement la sortie. Lorsque l'horaire devient valide, la sortie est activée. Lorsque l'horaire devient non valide, la sortie est désactivée.

  Par défaut, l'horaire d'activation contrôle la sortie uniquement lorsque l'horaire change d'état (devient valide ou non valide). Dans l'intervalle, la sortie peut encore être contrôlée par d'autres méthodes. Pour s'assurer que la sortie reste dans l'état programmé, activez **Toujours vérifier l'horaire** ci-dessous.
- **Toujours vérifier l'horaire** : Avec cette option activée, la sortie vérifie l'horaire toutes les minutes. Si la sortie n'est pas dans l'état correct, elle sera activée ou désactivée pour correspondre à l'état de l'horaire.
- **Temps d'activation** : La durée (en secondes) pendant laquelle la sortie restera active lorsqu'elle est activée. Cela s'applique à la plupart des méthodes d'activation (p. ex., activation manuelle, calendrier d'activation, fonction programmable, automatisation). L'état de la sortie sera affiché comme « ON chronométré » sur une page du statut.

  Si le temps d'activation est réglé sur 0, la sortie reste activée en permanence jusqu'à ce qu'elle soit désactivée par une méthode quelconque.

  Certaines méthodes d'activation des sorties (p. ex., groupe de sorties, type d'entrée, niveau d'accès) ont des temps spécifiques qui peuvent remplacer le temps d'activation.
- **Redéclencheur d'activation** : Avec cette option activée, si une sortie est activée une deuxième fois alors qu'elle est déjà « ON chronométré », le temps d'activation redémarre. Cela permet aux sorties telles que les lumières de rester allumées plus longtemps lorsqu'elles sont déclenchées à nouveau.

- **Supporter commandes manuelles** : Lorsque cette option est activée, un opérateur disposant des autorisations adéquates peut envoyer des commandes manuelles à la sortie. Par exemple, un opérateur peut faire un clic droit sur une sortie d'éclairage sur un plan d'étage pour allumer les lumières.

Pour plus d'informations, consultez la section Commandes des sortie manuelles (page suivante).

Ascenseur HLI

Cette section ne concerne que l'intégration HLI de Schindler. Pour plus de renseignements, consulter la note d'application 196 : intégration HLI Schindler dans Protege GX.

- **Sortie utilisée pour ascenseur HLI** : Avec cette option activée, la sortie peut être configurée pour être utilisée avec un ascenseur HLI. Ceci devrait typiquement être utilisé avec des sorties virtuelles.
- **Contrôleur** : Le contrôleur utilisé pour l'intégration Schindler.
- **Type ascenseur HLI** : Indique le type d'ascenseur HLI réglé sur le contrôleur (lecture seulement).
- **Mode d'activation SOM** : Ce paramètre permet Protege GX aux sorties (généralement des sorties virtuelles) d'activer les modes de fonctionnement spéciaux (Special Operating, SOM) de Schindler. Ils peuvent être utilisés pour des fonctions telles que l'envoi d'un ascenseur express ou la libération de passagers bloqués.

  Ce champ détermine quand le SOM sera contrôlé : soit lorsque la sortie est activée, soit lorsqu'elle est désactivée, soit chaque fois qu'elle change d'état. Si vous utilisez une seule sortie pour activer et désactiver un SOM, sélectionnez l'option ON change.

  Le nom du SOM à activer doit être défini comme le **nom d'affichage du clavier** pour la sortie.
- **Ajouter l'état de sortie au message SOM** : Lorsque cette option est sélectionnée, l'état de la sortie est ajouté à la fin du message SOM. Activer cette option si le **mode d'activation SOM** ci-dessus est réglé sur ON change.
- **ID du terminal primaire SOM** : L'ID du terminal Schindler auquel les messages seront envoyés lorsque le contrôleur communique via l'adresse IP primaire du serveur Schindler.
- **ID du terminal secondaire SOM** : L'ID du terminal Schindler auquel les messages seront envoyés lorsque le contrôleur communique via l'adresse IP secondaire du serveur Schindler.

Commandes

- Ce champ est utilisé pour envoyer des commandes de programmation à l'appareil. Il ne doit être utilisé que lorsqu'il est spécifiquement conseillé par la documentation ICT ou le support technique.

Graphiques

- **Plan d'étage** : L'association d'un plan d'étage à une sortie vous permet de faire un clic droit sur n'importe quel événement de sortie dans une fenêtre d'événement pour ouvrir le plan d'étage.
- **Caméra** : L'association d'une caméra à une sortie vous permet de faire un clic droit sur n'importe quel événement de sortie dans une fenêtre d'événement pour ouvrir un flux de caméra archivé à l'heure de l'événement.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Sorties | Options

Général

- **Enregistrer événements de sortie** : Lorsque cette option est activée, la sortie génère un événement lorsqu'elle est activée ou désactivée. Désactiver cette option pour empêcher de générer des événements de sortie.

  Vous pouvez désactiver la journalisation des événements pour les sorties qui sont principalement utilisées pour l'automatisation ou le contrôle (comme les sorties virtuelles), afin de réduire leur incidence sur le stockage des événements.

- **Inverser sortie** : Lorsque cette option est activée, l'activation de la sortie sera inversée. Par exemple, si une sortie d'éclairage est inversée, la désactivation de la sortie activera l'éclairage et l'activation de la sortie désactivera l'éclairage.

  Une mise à jour du module sera nécessaire chaque fois que ce paramètre sera modifié.

  Si la sortie se trouve sur le contrôleur, l'option doit être activée à la fois sur la sortie du contrôleur et sur la sortie correspondante du module d'expansion du lecteur intégré. Il faut alors l'activer et le désactiver manuellement pour que ce changement prenne effet.

État de préréglage

- **Prérégler mise sous tension du contrôleur** : Lorsque cette option est activée, la sortie est réglée sur un état spécifique lorsque le contrôleur est redémarré ou mis sous tension pour la première fois. Sinon, la sortie sera réinitialisée à son dernier état connu.
- **Sortie s'allume lorsque le contrôleur est mis sous tension** : Cette option définit l'état initial de la sortie lorsque le contrôleur est mis sous tension. Lorsque cette option est activée, la sortie est activée. Lorsque cette option est désactivée, la sortie est désactivée.
- **Prérégler mise sous tension du module** : Lorsque cette option est activée, la sortie est réglée sur un état spécifique lorsque le module auquel elle est connectée est mis sous tension. Cela annule le dernier état connu de l'entrée et le paramètre **Prérégler mise sous tension du contrôleur** ci-dessus.

  Une mise à jour du module sera nécessaire chaque fois que ce paramètre sera modifié.

- **Sortie s'allume lorsque le module est mis sous tension** : Cette option définit l'état initial de la sortie lorsque le module connecté est mis sous tension. Lorsque cette option est activée, la sortie est activée. Lorsque cette option est désactivée, la sortie est désactivée.
- **Module prédéfini hors ligne** : Lorsque cette option est activée, la sortie est réglée sur un état spécifique lorsque le module connecté passe hors ligne. Par exemple, cela pourrait être utilisé pour activer un voyant ou un signal sonore lorsqu'un module est hors ligne, ou pour s'assurer que l'éclairage de secours s'allume si une connexion est endommagée.

  Une mise à jour du module sera nécessaire chaque fois que ce paramètre sera modifié.

- **La sortie s'active lorsque le module est hors ligne** : Cette option définit l'état de la sortie lorsque le module connecté passe hors ligne. Lorsque cette option est activée, la sortie est activée. Lorsque cette option est désactivée, la sortie est désactivée.

Commandes des sortie manuelles

Un clic droit sur un registre de sortie dans **Programmation | Sorties** ou sur une icône de sortie sur un plan d'étage ou une page de statut ouvre un menu avec des commandes manuelles pour cette partition.

Contrôle

- **Activer**
- **Désactiver**
- **Activer chronométré** (activer la sortie pour la durée saisie dans le champ ci-dessous)

Entrées trouble

Les entrées trouble sont utilisées pour surveiller l'état et la condition du système. Comme les entrées physiques, les entrées de trouble ont un état binaire on-off; toutefois, elles représentent des troubles du système tels que des pannes de courant, des défauts de communication, des altérations et autres problèmes.

Les entrées trouble peuvent être programmées dans des partitions avec des types d'entrée spécifiques afin qu'elles soient surveillées par le système et signalées à la station de surveillance. Contrairement aux entrées normales, les entrées de trouble génèrent des alarmes 24 heures / altération lorsqu'elles sont ouvertes, au lieu des alarmes normales. En général, ils sont programmés dans une partition système dédiée dont la partie 24 heures est toujours activée, en utilisant les types d'entrée préconfigurés Trouble Silence et Trouble Sirène (consultez la page 230).

Chaque type de module possède ses propres entrées de trouble, qui sont ajoutées automatiquement lorsque l'enregistrement du module est ajouté au système. L'entrée **Module de chaque entrée** de trouble correspond à un trouble particulier du système pour ce module, tel qu'une panne d'alimentation ou un sabotage de module. Les portes disposent également d'entrées de trouble dédiées pour les conditions de porte laissée ouverte, de contrainte de porte et de porte forcée.

Consultez la section Entrées de trouble du manuel d'installation correspondant pour obtenir la liste complète de chaque module.

Entrées trouble | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Nom d'affichage du clavier** : Le nom qui sera téléchargé vers le contrôleur. Ce dernier sera affiché sur le clavier et dans les rapports des services de surveillance IP. Le clavier ne peut afficher que les 16 premiers caractères du nom. Il doit donc décrire de manière concise l'emplacement physique et la fonction de l'appareil.

Adresse

- **Type de module** : Le type d'appareil auquel l'entrée de trouble est associée (par exemple, contrôleur, module d'expansion du lecteur, porte).
- **Adresse du module** : L'**adresse physique** du module ou le nom de la porte à laquelle l'entrée de trouble est associée.
- **Entrée du module** : L'index de l'entrée de trouble sur le module associé. Cette fonction permet de déterminer la panne du système que l'entrée de trouble surveille et le code d'événement qui est envoyé à la station de surveillance lorsque cette entrée de trouble génère une alarme. Par exemple, l'entrée de trouble 3 sur un module d'expansion analogique s'ouvre lorsqu'il y a une condition de 'Batterie faible / manquante', et envoie un code d'événement de 302.

  Consultez la section Entrées de trouble du manuel d'installation correspondant pour obtenir la liste complète de chaque module.

Configuration

- **Groupe trouble** : Les groupes de troubles et les options de groupe de **troubles associées ci-dessous** déterminent la manière dont les conditions de trouble seront affichées sur le clavier. Le paramétrage de ces champs permet d'afficher cette entrée de trouble sur le clavier dans le menu Vue de l'installateurce qui est utile pour les techniciens qui vérifient les problèmes du système. En outre, un message personnalisé basé sur l'option de groupe de troubles sélectionnée s'affiche dans le menu Affichage des troubles et, s'il est activé sur le clavier, également dans le menu Affichage des troubles hors ligne.

  En général, il n'est pas nécessaire de modifier les groupes de troubles, car ils sont automatiquement définis pour chaque entrée de trouble.

  Les groupes de troubles disponibles sont les suivants :

  - **0 - Aucun** : Cette entrée de trouble n'entre dans aucune des catégories ci-dessous et ne sera pas affichée sur le clavier. Cette option est utilisée pour les entrées de trouble dont les techniciens sur site n'ont pas besoin d'avoir connaissance (par exemple) 'Installateur connecté').
  - **1 - Général** : Ce groupe de troubles comprend les troubles qui concernent le fonctionnement général du système. Cela inclut des conditions telles qu'une panne de courant, des problèmes de rapport et des défauts d'entrée.
  - **2 - Système** : Ce groupe de troubles est utilisé pour les troubles liés au module (par exemple, le sabotage du module).
  - **3 - Accès** : Ce groupe de troubles est utilisé pour les troubles liés au contrôle d'accès et au fonctionnement de la porte (par exemple, porte forcée, trop de tentatives d'accès).

  Les utilisateurs peuvent accéder au menu Trouble View en se connectant à un clavier et en appuyant**[MENU] [5] [2]** sur, et au menu Installer View en appuyant **[MENU] [4] [1] [2]**. Ils peuvent y voir les troubles actuels du système.

  Si cette option est activée sur le clavier (**module d'expansion | Claviers | Options 2**), vous pouvez accéder au menu Offline Trouble View en appuyant sur**[MENU] [2]** , sans vous connecter au clavier.

  Ces champs n'affectent pas les codes d'événement utilisés pour les rapports.

- **Options du groupe trouble** : L'option de groupe de troubles détermine le message qui sera affiché sur les claviers lorsque cette entrée de trouble est ouverte. Chaque option qui peut être sélectionnée comporte une ou plusieurs variantes, en fonction du **groupe de troubles** sélectionné ci-dessus. Si le groupe de troubles est réglé sur 1, la première entrée de chaque option sera utilisée, et ainsi de suite.

  Il n'est généralement pas nécessaire de modifier les options du groupe de problèmes, car elles sont automatiquement définies pour chaque entrée de problème.

- **Signaler ID** : L'ID de rapport de l'entrée de trouble est l'index **d'ID de zone**qui représentera cette entrée de trouble à la station de surveillance. Vous pouvez attribuer manuellement un ID à chaque entrée, ce qui permet une grande flexibilité dans le rapport des entrées. Par exemple, si deux entrées ont le même ID de signalement, elles seront toutes deux déclarées comme la même entrée.

  Un ID de rapport doit être attribué à chaque entrée de trouble. Ainsi, chaque entrée de trouble nouvellement créée se verra automatiquement attribuer l'ID disponible le plus bas. Si une entrée de trouble a reçu un numéro supérieur au maximum qui peut être signalé à un service particulier, le service le plus élevé possible sera signalé.

  Vous pouvez visualiser et exporter les ID de rapport à l'aide du **générateur de cartes de rapport** (**Rapports | Rapport de station centrale**). Les entrées et les entrées de trouble partagent la même gamme d'identifiants de zone, mais les entrées de trouble utilisent généralement des indices plus élevés.

Graphiques

- **Plan d'étage** : L'association d'un plan d'étage à une entrée de trouble vous permet de cliquer avec le bouton droit de la souris sur n'importe quel événement d'entrée de trouble dans une fenêtre d'événement pour ouvrir le plan d'étage.

Commandes

- Ce champ est utilisé pour envoyer des commandes de programmation à l'appareil. Il ne doit être utilisé que lorsqu'il est spécifiquement conseillé par la documentation ICT ou le support technique.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Entrées de trouble | Types de partitions et d'entrées

Comme les entrées, les entrées de trouble peuvent être affectées à quatre partitions au maximum, un type d'entrée distinct étant programmé dans chacune d'elles. Le type d'entrée définit le mode de fonctionnement de l'entrée de trouble dans cette partition. En général, les entrées de trouble doivent être utilisées dans les partitions du système pour générer des alarmes 24 heures sur 24 (en utilisant les types d'entrée préconfigurés Trouble Silent et Trouble Bell), mais elles peuvent également être utilisées pour le contrôle des sorties et l'automatisation.

Partitions attribuées

- **Partition 1-4** : Chaque entrée de trouble peut être programmée dans un maximum de quatre partitions différentes. En général, les entrées de trouble sont affectées à une "partition du système" qui est utilisée pour surveiller les troubles du système.
- **Type d'entrée 1-4** : Le type d'entrée définit le mode de fonctionnement de l'entrée de trouble dans cette partition particulière. Par exemple, le type d'entrée Trouble Silence permet à l'entrée de trouble de générer des alarmes de sabotage de 24 heures sans activer la sortie de cloche de la partition, tandis que le type d'entrée Trouble Bellentraîne l'activation de la sortie de cloche.

Entrées trouble | Options

Options générales

- **Enregistrer à la mémoire tampon de l'événement** : Lorsque cette option est activée (par défaut), l'entrée de trouble génère un événement lorsqu'elle est ouverte ou fermée. Désactivez cette option pour empêcher la génération d'événements d'entrée de trouble, ce qui réduit leur impact sur le stockage des événements. Les rapports seront toujours envoyés à la station de surveillance.
- **Contournement non permis**: Il est possible de contourner les entrées trouble à partir du clavier, mais le contournement ne peut être enlevé qu'en mettant le contrôleur sous tension. Par conséquent, il est recommandé de désactiver le contournement pour les entrées trouble.
- **Contournement de verrouillage non permis**: Il est possible de contourner les entrées trouble à partir du clavier, mais le contournement ne peut être enlevé qu'en mettant le contrôleur sous tension. Par conséquent, il est recommandé de désactiver le contournement pour les entrées trouble.

Options avancées

- **Aucun contournement si n'importe quelle partition est armée**: Il est possible de contourner les entrées trouble à partir du clavier, mais le contournement ne peut être enlevé qu'en mettant le contrôleur sous tension. Par conséquent, il est recommandé de désactiver le contournement pour les entrées trouble.

Cabines d'ascenseurs

Les registres de cabine d'ascenseur sont utilisés pour le contrôle d'ascenseurs de bas niveau, ce qui permet au système de contrôler et de surveiller l'accès des utilisateurs aux étages d'un bâtiment à plusieurs étages. Lorsqu'un utilisateur badge sa carte au lecteur associé, la cabine d'ascenseur déverrouille brièvement les étages auxquels il a accès. Les cabines d'ascenseurs peuvent également être câblées pour permettre le rapport de destination, ce qui permet à Protege GX de contrôler exactement l'étage sélectionné par l'utilisateur.

Les cabines d'ascenseurs peuvent être ajoutées aux pages des statuts et aux plans d'étages, où elles affichent le statut des étages disponibles et permettent un contrôle manuel de base.

Pour plus de renseignements et d'instructions de programmation concernant le contrôle d'ascenseurs de bas niveau et le rapport de destination, consulter la Note d'application 248 : Contrôle de base de l'ascenseur. Les registres de cabine d'ascenseur sont également utilisés dans certaines intégrations d'ascenseur HLI. Consultez la note d'application correspondante.

Cabines d'ascenseurs | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

Configuration

- **Module d'expansion du lecteur** : Les cabines d'ascenseurs doivent être associées au module d'expansion du lecteur qui est utilisé pour contrôler l'accès des utilisateurs à cette cabine.

  Le **Mode du lecteur 1/2** et **l'Ascenseur du lecteur 1/2** doivent également être réglés correctement pour ce module d'expansion du lecteur (**Modules d'expansions | Modules d'expansion du lecteur | Lecteur 1/2**).

- **Port du lecteur** : Le port du module d'expansion du lecteur qui contrôle l'accès à cette cabine d'ascenseur.
- **Déverrouiller temps d'accès** : La durée (en secondes) pendant laquelle les sorties d'étage sont activées lorsque l'accès est accordé à un utilisateur. Lorsque le rapport de destination n'est pas activé, l'utilisateur dispose de ce délai pour sélectionner un étage. Lorsque le rapport de destination est activé, l'étage sélectionné est activé pendant cette durée.
- **Déverrouiller temps de l'intercom** : La durée de l'heure (en secondes) pendant laquelle un étage reste déverrouillé lorsqu'il est déclenché par un service d'interphone. Une fois l'accès accordé par l'interphone, l'utilisateur dispose de ce délai pour entrer dans la cabine d'ascenseur et sélectionner un étage.

  Pour plus de renseignements sur la programmation de l'interphone et l'intégration des ascenseurs, voir le Manuel d'installation Protege Vandal Resistant Touchscreen Entry Station.

- **Temps de sélection de l'étage** : Lorsque le rapport de destination est activé, l'utilisateur dispose de ce délai (en secondes) pour appuyer sur un bouton d'étage après avoir obtenu l'accès. Cette option n'est pas nécessaire lorsque le rapport de destination n'est pas activé.

- **Activer signalisation de destination** : Le rapport de destination permet au système de savoir quel étage un utilisateur a sélectionné. Lorsqu'un utilisateur se voit accorder l'accès, le système attend l'activation d'une entrée au lieu de déverrouiller immédiatement tous les étages. L'utilisateur peut sélectionner un seul étage auquel il a accès, et seul cet étage est déverrouillé. De plus, un événement est enregistré pour consigner l'étage spécifique que l'utilisateur a sélectionné.

  Cette fonction est utile dans les situations de haute sécurité où il peut être important de savoir précisément à quels étages les utilisateurs se rendent. Cela empêche également les utilisateurs d'appuyer sur plusieurs boutons d'étage après avoir obtenu l'accès.

  Les rapports de destination ont des exigences de câblage spécifiques qui sont différentes de celles du contrôle d'ascenseurs de base.

- **Mode d'authentification** : Le type d'informations d'identification requis pour accéder à cette cabine d'ascenseur (carte, carte et NIP, carte ou NIP, NIP seulement). Si cette option est réglée sur <non définie>, la cabine d'ascenseur utilise l'opération de carte.

  Les cabines d'ascenseur peuvent utiliser des types d'informations d'identification personnalisés lorsque le **mode d'authentification** est défini sur <non réglé>. Le **format du lecteur 1/2** dans **Modules d'expansion | Modules d'expansion du lecteur | Lecteur 1/2** doit être défini sur Custom Credential. Dans ce mode d'authentification, le port du lecteur comparera les données de la carte à ce premier type d'informations d'identification programmé avec une longueur de bit compatible.

Commandes

- Ce champ est utilisé pour envoyer des commandes de programmation à l'appareil. Il ne doit être utilisé que lorsqu'il est spécifiquement conseillé par la documentation ICT ou le support technique.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Cabines d'ascenseurs | Horaires et Partitions

Cet onglet vous permet d'ajouter les étages qui sont accessibles à partir de cette cabine d'ascenseur, et de configurer le fonctionnement de cet étage. Les étages peuvent être programmés dans **Programmation | Étages**.

Étages

Cliquez sur **Ajouter** pour ajouter un nouvel étage à la cabine d'ascenseur, et définissez les paramètres suivants :

- **Horaire** : Ce champ configure un horaire de déverrouillage pour l'étage. Lorsque cet horaire est valide, l'étage est en accès libre depuis cette cabine d'ascenseur sans informations d'identification. Lorsque l'horaire n'est pas valide, des informations d'identification sont requises pour accéder à l'étage.

  Par défaut, l'horaire de déverrouillage contrôle l'étage uniquement lorsque l'horaire change d'état (devient valide ou non valide). Dans l'intervalle, l'étage peut encore être contrôlé par d'autres méthodes. Pour s'assurer que l'étage reste dans l'état programmé, activez **Vérifier horaire**.
- **Partition** : Ce champ définit la partition intérieure de cet étage (c'est-à-dire la partition dans laquelle les utilisateurs entrent lorsqu'ils descendent de la cabine d'ascenseur). La partition intérieure doit être paramétrée pour permettre l'intégration du contrôle de partition avec l'accès à l'ascenseur à l'aide des options **Suivre statut de la partition** et **Activer le contrôle de zone**.
- **Ouverture en retard** : Si cette option est activée, lorsque **l'horaire** devient valide, l'étage ne se déverrouille pas tant qu'un utilisateur n'a pas obtenu l'accès. Cela empêche les étages de se déverrouiller à l'horaire prévu les jours où personne ne se rend sur le site.

  Cette fonction requiert un rapport de destination.

- **Vérifier horaire** : Si cette option est activée, l'état de l'étage est vérifié toutes les minutes et mis à jour en fonction de l'horaire. Si l'horaire est valide, l'étage est déverrouillé. Si l'horaire n'est pas valide, l'étage est verrouillé.
- **Suivre statut de la partition** : Lorsque cette option est activée, l'étage suit le statut de la **Partition** assignée. Si la partition est armée, l'étage se verrouille. Si la partition est désarmée, l'étage se déverrouille.
- **Entrée** : L'entrée définie ici correspond au bouton de sélection d'étage dans la cabine d'ascenseur. Il s'agit d'un paramètre obligatoire pour les rapports de destination. Ce champ n'est pas nécessaire si le rapport de destination n'est pas utilisé.
- **Sortie** : La sortie relais définie ici correspond au bouton de sélection d'étage dans la cabine d'ascenseur. Une sortie est requise par étage contrôlé dans chaque cabine d'ascenseur, mais pas pour les étages non contrôlés (toujours déverrouillés). Cette configuration est nécessaire pour le contrôle de base et les rapports de destination.
- **Activer le contrôle de zone** : Lorsque cette option est activée, la **Partition** de cet étage est automatiquement désarmée lorsque l'accès est accordé à un utilisateur disposant de permissions suffisantes. Par ailleurs, l'accès est refusé si la partition est armée et que l'utilisateur ne dispose pas des autorisations suffisantes pour la désarmer.

  Cette fonction requiert un rapport de destination.

Commandes manuelles (d'étage) de la cabine d'ascenseur

Lorsqu'une cabine d'ascenseur a été ajoutée à une page du statut ou à un plan d'étage, les étages accessibles depuis cette cabine d'ascenseur sont affichés. Un clic droit sur l'icône d'un étage ouvre un menu avec des commandes manuelles pour cet étage.

Contrôle

- **Activer** (déverrouiller les loquets de l'étage jusqu'à ce qu'il soit à nouveau verrouillé)
- **Désactiver** (verrouiller l'étage)
- **Activer chronométré** (déverrouiller l'étage pour la durée configurée dans le champ ci-dessous)

Les commandes manuelles n'affectent que l'accès à l'étage par cette cabine d'ascenseur spécifique. Par exemple, si vous déverrouillez l'étage avec une commande, il peut être en libre accès depuis une cabine d'ascenseur, mais pas depuis les autres.

Étages

Les registres d'étage représentent un étage physique sur le site. Dans l'intégration des ascenseurs de bas niveau, ils sont appliqués aux cabines d'ascenseurs qui peuvent y accéder (consultez la page 262). Les étages sont également utilisés dans les intégrations d'ascenseur HLI.

Pour plus d'informations, consultez Note d'application 248 : Contrôle d'ascenseurs à bas niveau dans Protege GX et Protege WX ou la note d'application ascenseur HLI pertinente.

Étages | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Relai d'étage** : Le relais d'étage représente le niveau de l'étage tel que programmé dans le système. Les relais d'étage doivent être uniques, programmés par ordre numérique (en commençant par 1) et commencer à l'étage accessible le plus bas, y compris les sous-sols. Les portes des ascenseurs arrière doivent être programmées avec des relais d'étage à partir de 65.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

Options d'ascenseur HLI

Pour plus de renseignements, consulter la Note d'application 196 : intégration HLI Schindler dans Protege GX.

- **Schéma d'heure valide pour l'horaire de Schindler** : Définit le message qui est envoyé à l'interface d'appel de Schindler lorsque l'horaire attribué à l'étage devient valide.
- **Schéma d'heure non valide pour l'horaire de Schindler** : Définit le message qui est envoyé à l'interface d'appel Schindler lorsque l'horaire attribué à l'étage devient invalide.
- **ID du terminal primaire de Schindler** : Définit l'ID du terminal de Schindler auquel le message d'horaire valide/invalide est envoyé lorsque le contrôleur communique via l'adresse IP primaire.
- **ID du terminal secondaire de Schindler** : Définit l'ID du terminal Schindler auquel le message de validité/invalidité de l'horaire est envoyé lorsque le contrôleur communique via l'adresse IP secondaire.

Commandes

- Ce champ est utilisé pour envoyer des commandes de programmation à l'appareil. Il ne doit être utilisé que lorsqu'il est spécifiquement conseillé par la documentation ICT ou le support technique.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Heure d'été

Les registres d'heure d'été sont associés à un contrôleur et lui ordonnent de modifier son **Heure champ** lorsque l'heure d'été locale commence ou se termine. Ceci est nécessaire pour s'assurer que l'heure du contrôleur est mise à jour correctement pour son fuseau horaire.

Lorsque vous programmez et enregistrez un registre d'heure d'été, l'heure du contrôleur s'ajuste automatiquement s'il est actuellement en heure d'été. Vous devez vérifier que l'heure du contrôleur est correctement réglée.

- Si l'heure du contrôleur est réglée manuellement, vous pouvez vérifier l'heure actuelle en faisant un clic droit sur le registre dans **Sites | Contrôleurs**. Pour mettre à jour l'heure, cliquez sur **Régler date heure du contrôleur**.
- Lorsque vous utilisez un serveur d'heure, l'heure fournie est toujours en UTC (Temps Universel Coordonné), qui n'a pas de fuseau horaire et n'est pas soumis à des règles d'heure d'été. Cela signifie que vous devez configurer correctement le serveur d'heure, le fuseau horaire dans lequel le contrôleur fonctionne et les réglages d'heure d'été pour que l'heure soit synchronisée correctement. Si l'un de ces paramètres n'est pas configuré, l'heure sera inexacte. Vérifiez les paramètres du serveur de temps dans l'onglet **Sites | Contrôleurs | Mise à jour de l'heure**.

Une fois cette opération effectuée, l'heure du contrôleur est automatiquement ajustée pour l'heure d'été.

Pour voir une démonstration, regardez Configurer l'heure d'été dans Protege GX sur la chaîne YouTube ICT.

Heure d'été | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Configuration

- **Débuter le jour** : Le jour où l'heure d'été commence, c'est-à-dire que l'horloge avance d'une heure. Cela se base sur un jour de la semaine (par ex. : le premier dimanche).
- **Débuter le mois** : Le mois où l'heure d'été commence.
- **Terminer le jour** : Le jour où l'heure d'été se termine, c'est-à-dire que l'horloge recule d'une heure. Cela se base sur un jour de la semaine (par ex. : le premier dimanche).
- **Terminer le mois** : Le mois où l'heure d'été se termine.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Heure d'été | Options

Options

- **Appliquer à tous les contrôleurs** : Par défaut, chaque registre d'heure d'été ne s'applique qu'à un seul contrôleur (sélectionné dans la barre d'outils). Si cette option est activée, le registre s'applique à tous les contrôleurs de ce site.

Numéros de téléphone

Des registres de numéros de téléphone peuvent être attribués aux services de signalement qui communiquent à l'aide d'une connexion téléphonique. La programmation de ces registres séparés facilite la mise à jour en cas de changement de numéro de téléphone et vous permet de créer un numéro de téléphone secondaire qui peut être utilisé pour les appels en dehors des heures de bureau.

Les numéros de téléphone ne sont utilisés que par les modèles de contrôleur dotés de composeurs modem intégrés.

Numéros de téléphone | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

Configuration

- **Horaire d'opération** : Cet horaire détermine quand ce numéro de téléphone peut être appelé. Lorsque l'horaire est valide, le numéro de téléphone défini dans ce registre sera appelé. Lorsque l'horaire n'est pas valide, le numéro de téléphone secondaire est appelé. Cela vous permet de définir un autre numéro de téléphone à appeler en dehors des heures de travail.
- **Numéro de téléphone secondaire** : Ce registre de numéro de téléphone sera utilisé lorsque l'**horaire d'opération** n'est pas valide. L'horaire d'opération du numéro de téléphone secondaire doit être valide.
- **Numéro de téléphone** : Le numéro de téléphone qui sera utilisé par ce registre.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Services

Les services servent de médiateur entre Protege GX et les systèmes externes tels que les stations de rapport, les contrôleurs d'automatisation et les interphones. Ils permettent aux contrôleurs Protege GX de communiquer directement avec d'autres systèmes via Ethernet, USB Ethernet ou le composeur modem intégré.

Une fois que vous avez programmé un service, vous pouvez le démarrer ou l'arrêter en faisant un clic droit sur l'enregistrement. Si vous modifier et sauvegarder l'enregistrement du service, celui-ci s'arrêtera et redémarrera automatiquement pour mettre en œuvre les modifications.

Les services peuvent nécessiter l'utilisation de dispositifs matériels embarqués ou de dispositifs d'extension. Tous les modèles de contrôleur ne prennent pas en charge tous les canaux de connexion, consultez donc la documentation de votre modèle de contrôleur avant de programmer les services.

Configuration des services de rapport

Certains types de services sont des services de rapport qui envoient des rapports à des stations de surveillance hors site, soit sur une ligne téléphonique, soit via le réseau IP. Les trois types de services de rapport sont :

- Identification du contact (Contact ID) (consultez la page 269)
- SIA (consultez la page 274)
- Rapport IP (consultez la page 281)

Lorsqu'un service de rapport est ajouté à un secteur, il peut envoyer des rapports relatifs à l'armement/désarmement du secteur et aux événements pour les entrées et les entrées de dérangement programmées dans ce secteur. Les étapes suivantes décrivent brièvement comment créer un service de rapport et commencer à faire des rapports sur une zone.

Pour une démonstration, voir Configuration de la surveillance hors site dans Protege GX sur la chaîne ICT YouTube.

1. Dans **Programmation | Services**, sélectionner le **Contrôleur** qui utilisera ce service de rapport.
2. Ajouter un nouveau service de rapport avec un **Service type** de ContactID, SIA ou Rapport IP.
3. Configurer les paramètres de communication requis pour envoyer des rapports à la station de surveillance, tels que le **Code client** et tout numéro de téléphone ou canal IP.
4. Sélectionner les types d'événements que ce service signalera (ouverture, fermeture, alarme, sabotage, restauration et/ou contournement) dans **l'onglet**Options.
5. Pour les services de rapport IP, ajoutez et configurez un **service de sauvegarde** si nécessaire. Ceci permet au contrôleur de faire un rapport sur une autre connexion IP ou une ligne téléphonique si la connexion échoue.
6. **Enregistrez** le service.
7. Naviguer vers **Programmation | Zones** et sélectionnez la ou les zones qui seront surveillées par ce service.
8. Dans l'onglet **Configuration**, faites défiler l'écran jusqu'à la section **Services de rapport** et cliquez sur **Ajouter**.
9. Sélectionner le nouveau service de rapport et cliquez sur **OK**. **Enregistrer** la ou les zones.
10. Il se peut que vous deviez fournir un rapport de station centrale à votre station de surveillance afin qu'elle puisse identifier les zones, les entrées et les utilisateurs dans les rapports. Pour plus d'informations, consultez la section Rapport de la station centrale (la page 176).
11. Retourner à **Programmation | Services**. Cliquer du bouton droit de la souris sur le nouveau service et cliquer sur **Démarrer**.

À présent, le service de rapport peut transmettre à la station de surveillance les types d'événements sélectionnés pour ces zones spécifiques.

Services | Type de service

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Type

- **Type de service**: Le type de service détermine le type d'opération ou de communication que ce service effectuera. Différents onglets de programmation seront disponibles en fonction du type de service sélectionné. Les options suivantes sont disponibles :
  - **ContactID** (service de rapport de ligne téléphonique)
  - **Imprimante série** (service d'envoi d'événements)
  - **SIA** (service de rapport par ligne téléphonique)
  - **Automatisation et contrôle** (service d'intégration)
  - **Modbus** (service d'intégration)
  - **C-Bus** (service d'intégration)
  - **Rapport IP** (service de rapport IP)
  - **Interphone** (service d'intégration)
  - **Link me** (service de communication entre contrôleurs)
  - **VizIP** (service d'intégration)
- **Mode de service**: Détermine le mode de démarrage du service. Le paramètre 0 - Mode manuel garantit que le service ne démarrera que sur commande manuelle d'un opérateur (clic droit sur l'enregistrement). Le paramètre 1 - Démarrage avec le système d'exploitation du contrôleur configure le service pour qu'il démarre automatiquement au démarrage du contrôleur.

Commandes

- Ce champ est utilisé pour envoyer des commandes de programmation à l'appareil. Il ne doit être utilisé que lorsqu'il est spécifiquement conseillé par la documentation ICT ou le support technique.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Contact ID

Ce service de rapport envoie des alarmes, des tests et d'autres événements à une station de surveillance via une ligne téléphonique, en utilisant le composeur modem intégré du contrôleur. Les rapports sont envoyés dans le format standard Ademco Contact ID.

Le signalement de la ligne téléphonique n'est disponible que pour les modèles de contrôleur dotés de composeurs modem intégrés.

Pour plus d'informations sur le format Contact ID, voir la note d'application 316 : Rapport Contact ID dans Protege GX et Protege WX.

Contact ID | Général

Les numéros de téléphone peuvent être programmés dans **Programmation | Numéros de téléphone**.

- **Code client**: Ce code représente le contrôleur ou le site dans les rapports destinés à la station centrale de surveillance. Il s'agit généralement d'un nombre hexadécimal à 4 chiffres, mais le format peut dépendre de la compatibilité du récepteur. Il sera émis par la station de surveillance.

  Les codes clients peuvent également être définis pour des partitions individuelles dans **Programmation | Partitions | Configuration**.
- **Numéro de PABX** : Si le contrôleur est connecté à un réseau téléphonique interne, il composera d'abord ce numéro pour obtenir une ligne téléphonique externe. Si le numéro PABX est désactivé par un **horaire d'opération** (**Programmation | Numéros de téléphone | Général**), le numéro externe sera composé immédiatement.
- **Numéro de téléphone 1** : Le numéro de téléphone principal de la station de surveillance. Le contrôleur compose ce numéro en premier pour signaler les événements.
- **Numéro de téléphone 2** : Ce numéro de téléphone est utilisé lorsque le contrôleur ne peut pas établir de connexion avec le **Numéro de téléphone 1** ou le **Numéro de téléphone de secours**.
- **Numéro de téléphone de secours** : Ce numéro de téléphone est utilisé lorsque le contrôleur ne peut pas établir de connexion avec le **Numéro de téléphone 1**. La séquence des tentatives de numérotation dépend de l'activation de l'option **Utiliser une autre méthode de numérotation** dans l'onglet **Options**.

Contact ID | Options

- **Utiliser méthode de composition alternative**: Cette option détermine l'ordre dans lequel le service essaiera les différents numéros de téléphone programmés dans l'onglet **Général** si le **numéro de téléphone 1** échoue.

  Les options sont :
  - **Séquentielle** (cette option est désactivée) : Lorsque le **numéro de téléphone 1** échoue, le service continue à essayer ce numéro de téléphone jusqu'à ce qu'il atteigne le nombre maximum de **tentatives de composition** (onglet **Général**). Si toutes les tentatives échouent, le service répète ce processus avec la **sauvegarde du téléphone**, puis avec le **numéro de téléphone 2**.
  - **Alternatif** (cette option activée) : Lorsque le **numéro de téléphone 1** ne fonctionne pas, le service essaie la **sauvegarde du téléphone** une fois, puis essaie encore le **numéro de téléphone 1**, puis répète en alternance. Lorsque les deux numéros ont atteint le nombre maximal de **tentatives de composition**, le service essaie le **numéro de téléphone 2** jusqu'à ce qu'il atteigne également le nombre maximal de tentatives.

  Lorsque tous les numéros ont atteint le nombre maximal de tentatives de composition, l'entrée trouble Signaler un échec est ouverte.
- **Pause après PABX**: Quand cette option est activée, le composeur insérera une pause de 2.5 secondes après avoir composé le numéro PABX.
- **Rapport ouvert** : Lorsque cette option est activée, le service signalera le désarmement (ouverture) de toutes les zones utilisant ce service.

- **Report close** : Lorsque cette option est activée, le service signalera l'armement (fermeture) de tous les secteurs utilisant ce service.
- **Rapport des alarmes** : Lorsque cette option est activée, le service signalera les alarmes d'entrée.
- **Signalement des effractions** : Lorsque cette option est activée, le service signalera les sabotages d'entrée et les alarmes d'entrées trouble.
- **Rapport de restauration** : Lorsque cette option est activée, le service signalera les restaurations d'entrée.
- **Report bypass** : Lorsque cette option est activée, le service signalera les contournements d'entrée.
- **Le service fonctionne comme une sauvegarde** : Lorsque cette option est activée, le service ne commencera pas à rapporter sauf s'il est initié par un autre service qui n'a pas réussi à rapporter. Ce service transmet tous les messages du service primaire qui n'ont pas réussi à les envoyer, puis le fonctionnement revient au service primaire. Le service de secours démarre et s'arrête en même temps que le service primaire.

  Seuls les services IP de rapport ont la possibilité de définir un **Service de secours**. (onglet **Général**).

- **Enregistrer les événements du modem dans le tampon d'événements** : Lorsque cette option est activée, des événements détaillés décrivant la progression de l'appel seront enregistrés dans le journal des événements pour chaque rapport. Cette option peut être utilisée pour le dépannage des problèmes mais doit être désactivée pendant le fonctionnement normal car un grand nombre d'événements seront générés.

Contact ID | Paramètres

Paramètres

- **Mappages Cid** :Cette option n'est pas nécessaire pour la plupart des formats de rapport d'identification du contact. Les codes de signalement sont réglés dans la programmation pour les utilisateurs, les entrées, les entrées trouble et les zones individuelles, et peuvent être réinitialisés à un schéma de mappage spécifique si nécessaire lorsqu'un opérateur génère la carte de rapport centrale (**Rapports | Rapport de la station centrale**). Toutefois, lorsque la cartographie SIMS II est en cours d'utilisation, cette option doit être réglée sur SIMS II.

  Pour plus d'informations, voir la note d'application 316 : Rapports au format Contact ID dans Protege GX et Protege WX.

- **Tentatives de composition** : Détermine combien de fois le contrôleur tentera de composer chaque numéro avant de passer au numéro de sauvegarde suivant. Cette limite s'applique même lorsque le rapport a été signalé avec succès.

  Ce réglage peut être annulé par le **pays du modem**. Pour les installations UL/ULC (avec la **fonction Advance UL** activée dans **Sites | Contrôleurs | Options**), le contrôleur ne permettra pas de valeurs supérieures à 8.

- **Tentatives de ports** : Détermine combien de fois le service tentera d'accéder au modem embarqué avant de signaler un échec de communication. Cela peut se produire lorsqu'un autre service utilise le même port pour les communications.
- **Nombre de rapports** : Détermine le nombre de rapports que le service peut envoyer dans chaque appel à la station de surveillance. Entre 8 et 16 est recommandé. Si la limite est atteinte, le contrôleur appelle à nouveau pour envoyer les messages restants.
- **Durée de la poignée de main** : Le temps (en secondes) que le contrôleur attendra pour recevoir une réponse au message de poignée de main de l'unité de réception à distance. Cette valeur peut être ajustée si une heure de fin d'appel plus longue que la normale est nécessaire.
- **Temps de composition** :Le temps (en secondes) que le contrôleur attendra après une tentative de signalement échouée avant de recomposer ou de composer un numéro de sauvegarde. La valeur minimale est de 10 secondes.
- **Sortie décrochée / groupe de sortie** : Cette sortie ou ce groupe de sorties est activé lorsque le service commence à utiliser le modem et est désactivé lorsque la communication est terminée. Elle peut être utilisée avec des systèmes d'échange à distance qui nécessitent des connexions de communication à démarrage au sol.

- **Rapport OK sortie / groupe de sortie** : Cette sortie ou ce groupe de sorties est activé(e) lorsque le service effectue un rapport avec succès. Elle n'est pas désactivée automatiquement et doit être programmée avec un **Temps d'activation**. (**Programmation | Sorties**) pour s'assurer qu'elle est désactivée entre les rapports.

Surveillance en arrière-plan

- **Activer la surveillance en arrière-plan** : Lorsque la surveillance en arrière-plan est activée, le service envoie régulièrement des messages de sondage pour confirmer que les lignes téléphoniques sont opérationnelles. Cela garantit que les problèmes de l'une ou l'autre des lignes téléphoniques (qu'elles soient primaires ou de sauvegarde) sont détectés.
  - **Temps de sondage en arrière-plan lorsque OK**: Détermine la fréquence (en secondes) à laquelle le contrôleur vérifie l'état du service lorsqu'il n'y a pas de problème connu.
  - **Temps de sondage en arrière-plan quand l'échec est connu**: Détermine la fréquence (en secondes) à laquelle le contrôleur vérifie l'état du service lorsqu'il n'y a un problème connu.
  - **Rapport test Code CID / groupe / zone** : Le code d'événement Contact ID, le numéro de groupe et le numéro de zone que le contrôleur enverra pour le rapport de test.
  - **Le téléphone 1 a échoué Code CID / groupe / zone**: Le code d'événement Contact ID, le numéro de groupe et le numéro de zone que le contrôleur utilisera pour signaler l'échec de la communication avec le **numéro de téléphone 1**.
  - **Le téléphone 2 a échoué Code CID / groupe / zone**: Le code d'événement Contact ID, le numéro de groupe et le numéro de zone que le contrôleur utilisera pour signaler l'échec de la communication avec le **numéro de téléphone 2**.
  - **Le téléphone de secours a échoué Code CID / groupe / zone :**: Le code d'événement Contact ID, le numéro de groupe et le numéro de zone que le contrôleur utilisera pour signaler l'échec de la communication avec le **téléphone de secours**.

Paramètres de la version 3

Cette section affiche les paramètres qui étaient utilisés dans la version 3 du logiciel et les versions antérieures. Ces paramètres ne nécessitent pas de configuration dans la version 4 ou ultérieure.

Imprimante série

Ce service permet au contrôleur d'envoyer des événements sous forme de texte ACSII via une connexion Ethernet. Ceci peut être utilisé pour des applications de surveillance intégrées, permettant aux événements d'être visualisés à partir d'une autre application sans utiliser le logiciel client Protege GX. Le service peut être programmé pour inclure des groupes d'événements et des détails spécifiques.

Le service d'imprimante série utilise le **Nom d'affichage du clavier** pour les périphériques au lieu du nom du logiciel. Les enregistrements qui n'ont pas de nom d'affichage du clavier peuvent ne pas être affichés correctement.

Imprimante série | Général

Configuration

- **Numéro de port** : Le numéro de port doit être défini sur TCP/IP pour les contrôleurs de rail DIN.
  Les options Port de communication externe 1-4 sont uniquement utilisées pour les contrôleurs PCB existants utilisant l'interface de communication série PRT-COMM .
- Vitesse du port : Le débit en bauds pour les communications série, qui peut être ajusté pour correspondre à la configuration de l'hôte. Ceci n'a aucun effet lorsque le **Numéro de port** est défini sur TCP/IP.
- **Parité** : La parité pour les communications série, qui peut être ajustée pour correspondre à la configuration de l'hôte. Ceci n'a aucun effet lorsque le **Numéro de port** est défini sur TCP/IP.
- **STX**: Cet octet est ajouté au début de chaque message transmis si l'option **Inclut le caractère de début de trame (STX)** est activé (**onglet**Options). L'indice décimal représente un seul caractère ASCII.
- **ETX**: Cet octet est ajouté à la fin de chaque message transmis si l'option **Inclut le caractère de la fin de trame (ETX)** est activée (**onglet**Options). L'indice décimal représente un seul caractère ASCII.
- **AR**: Cet octet doit être envoyé au contrôleur pour confirmer que chaque message envoyé a été reçu correctement. Le contrôleur attendra cet accusé de réception si **L'événement nécessite un accusé de réception** est activé (**Onglet**options). L'indice décimal représente un seul caractère ASCII.
- **Numéro de port IP**: Le port TCP/IP que le service utilisera pour communiquer. Ceci n'est pas nécessaire si un module PRT-COMM est dedans.

Paramètres de la version 3

Cette section affiche les paramètres qui étaient utilisés dans la version 3 du logiciel et les versions antérieures. Ces paramètres ne nécessitent pas de configuration dans la version 4 ou ultérieure.

Imprimante série | Options

Options

- Les options suivantes vous permettent de sélectionner les événements qui seront transmis par le service d'imprimante série:
  - **Événements du système**
  - **Événements de service**
  - **Événements liés au modem**
  - **Événements organisés par les utilisateurs**
  - **Événements d'entrée**
  - **Événements d'entrée en cas de problème**
  - **Événements de sortie**
  - **Événements de l'horaire**
  - **Événements de zone**
  - **Événements du module**
  - **Événements relatifs aux portes**

- **Événements liés aux ascenseurs**
- **Événements liés aux lecteurs**
- **Événements liés aux rapports**
- **Événements spéciaux**
- **Tous les événements du contrôleur**

Les événements qui sont inclus dans chaque catégorie peuvent être visualisés dans la programmation du filtre d'événements. Naviguer vers **Événements | Filtres d'événements | Types d'événements** et cliquer sur **Ajouter** pour visualiser les types d'événements.

- **Afficher en format texte**: Lorsque cette option est activée, les événements seront affichés en format texte. Lorsqu'elle est désactivée, seuls les caractères de contrôle ASCII seront reçus.
- **Affichage de l'heure**: Lorsque cette option est activée, l'heure (heures, minutes et secondes) sera préfixée à chaque événement transmis.
- **Afficher le jour de la semaine**: Lorsque cette option est activée, le jour de la semaine (au format de trois lettres) sera préfixé à chaque événement transmis.
- **Affichage du mois** : Lorsque cette option est activée, la date (dans le format jj/mm/aaaa) sera préfixée à chaque événement transmis.
- **Affichage des millisecondes** : Lorsque cette option est activée, les millisecondes seront préfixées à chaque événement transmis. L'option **Durée d'affichage** doit également être activée.
- **Affichage du mode brut**: Il s'agit d'une option héritée qui n'a aucun effet.
- **Affichage du mode brut ASCII (désactivé=binaire)**: Il s'agit d'une option héritée qui n'a aucun effet.
- **Non utilisé**: Il s'agit d'une option héritée qui n'a aucun effet.
- **L'événement nécessite un accusé de réception**: Lorsque cette option est activée, le contrôleur attendra un paquet d'accusé de réception de la part du dispositif récepteur après la réception de chaque message. Le contrôleur renverra régulièrement le message jusqu'à ce qu'un accusé de réception soit reçu.

  L'**AR** attendu est défini dans **l'onglet**General.
- **Inclure le numéro de séquence**: Il s'agit d'une option héritée qui n'a aucun effet.
- **Imprimer les entrées défectueuses**: Il s'agit d'une option héritée qui n'a aucun effet.
- **Inclure le nombre d'octets**: Il s'agit d'une option héritée qui n'a aucun effet.
- **Inclure le caractère de début de trame (STX)**: Lorsque cette option est activée, un caractère de début de trame (STX) sera préfixé au texte de l'événement. Le **STX** est défini dans **l'onglet** Général.
- **Inclure le caractère de fin de trame (ETX)**: Lorsque cette option est activée, un caractère de fin d'image (ETX) sera ajouté au texte de l'événement. L' **ETX** est défini dans **l'onglet**Général.

SIA

Ce service de rapport envoie des alarmes, des tests et d'autres événements à une station de surveillance via une ligne téléphonique, en utilisant le composeur modem intégré du contrôleur. Les rapports sont envoyés dans le format standard SIA niveau 2.

Le service de rapport de ligne téléphonique n'est disponible que pour les modèles de contrôleur dotés de composeurs modem intégrés.

Pour plus d'informations sur le format SIA niveau 2, consultez la note d'application 317 : rapport SIA L2 dans Protege GX et Protege WX.

SIA | Général

- **Code client**: Ce code représente le contrôleur ou le site dans les rapports destinés à la station centrale de surveillance. Il s'agit généralement d'un nombre hexadécimal de 4 ou 6 chiffres, selon la compatibilité du récepteur. Il sera émis par la station de surveillance.

  Voir les paramètres supplémentaires du code client dans l'**onglet**Options.

- **Numéro de PABX** : Si le contrôleur est connecté à un réseau téléphonique interne, il composera d'abord ce numéro pour obtenir une ligne téléphonique externe. Si le numéro PABX est désactivé par un **horaire d'opération** (**Programmation | Numéros de téléphone | Général**), le numéro externe sera composé immédiatement.
- **Numéro de téléphone 1** : Le numéro de téléphone principal de la station de surveillance. Le contrôleur compose ce numéro en premier pour signaler les événements.
- **Numéro de téléphone 2** : Ce numéro de téléphone est utilisé lorsque le contrôleur ne peut pas établir de connexion avec le **Numéro de téléphone 1** ou le **Numéro de téléphone de secours**.
- **Numéro de téléphone de secours** : Ce numéro de téléphone est utilisé lorsque le contrôleur ne peut pas établir de connexion avec le **Numéro de téléphone 1**. La séquence des tentatives de numérotation dépend de l'activation de l'option **Utiliser une autre méthode de numérotation** dans l'onglet **Options**.
- **Nombre de tentatives de numérotation**: Détermine combien de fois le contrôleur tentera de composer chaque numéro avant de passer au numéro de sauvegarde suivant. Cette limite s'applique même lorsque le rapport a été signalé avec succès.

  Ce réglage peut être annulé par le **pays du modem**. Pour les installations UL/ULC (avec la **fonction Advance UL** activée dans **Sites | Contrôleurs | Options**), le contrôleur ne permettra pas de valeurs supérieures à 8.

- **Nombre de tentatives d'ouverture de port**: Détermine combien de fois le service tentera d'accéder au modem embarqué avant de signaler un échec de communication. Cela peut se produire lorsqu'un autre service utilise le même port pour les communications.
- **Temps de connexion à distance**: Le temps (en secondes) que le contrôleur attendra pour recevoir une réponse au message de poignée de main de l'unité de réception à distance. Cette valeur peut être ajustée si une heure de fin d'appel plus longue que la normale est nécessaire.

  Par exemple, il peut être nécessaire d'augmenter ce temps lorsque les établissements de liaison pour les formats à faible vitesse doivent se produire avant l'établissement de liaison SIA.
- **Temps entre les recompositions en cas d'échec du message**: Le temps (en secondes) que le contrôleur attendra après une tentative de signalement échouée avant de recomposer ou de composer un numéro de sauvegarde. La valeur minimale est de 10 secondes.
- **Sortie / Le groupe de sortie s'active/désactive lorsque le composeur est raccroché/ décroché**: Cette sortie ou ce groupe de sorties est activé lorsque le service commence à utiliser le modem et est désactivé lorsque la communication est terminée. Elle peut être utilisée avec des systèmes d'échange à distance qui nécessitent des connexions de communication à démarrage au sol.
- **Sortie / Le groupe de sortie s'active quand un bon message est envoyé**: Cette sortie ou ce groupe de sorties est activé(e) lorsque le service effectue un rapport avec succès. Elle n'est pas désactivée

automatiquement et doit être programmée avec un **Temps d'activation**. (**Programmation | Sorties**) pour s'assurer qu'elle est désactivée entre les rapports.

Paramètres de la version 3

Cette section affiche les paramètres qui étaient utilisés dans la version 3 du logiciel et les versions antérieures. Ces paramètres ne nécessitent pas de configuration dans la version 4 ou ultérieure.

SIA | Options

- **Composition alternative**: Cette option détermine l'ordre dans lequel le service essaiera les différents numéros de téléphone programmés dans l'onglet **Général** si le **numéro de téléphone 1** échoue.

  Les options sont :

  - **Séquentielle** (cette option est désactivée) : Lorsque le **numéro de téléphone 1** échoue, le service continue à essayer ce numéro de téléphone jusqu'à ce qu'il atteigne le nombre maximum de **tentatives de composition** (onglet **Général**). Si toutes les tentatives échouent, le service répète ce processus avec la **sauvegarde du téléphone**, puis avec le **numéro de téléphone 2**.
  - **Alternatif** (cette option activée) : Lorsque le **numéro de téléphone 1** ne fonctionne pas, le service essaie la **sauvegarde du téléphone** une fois, puis essaie encore le **numéro de téléphone 1**, puis répète en alternance. Lorsque les deux numéros ont atteint le nombre maximal de **tentatives de composition**, le service essaie le **numéro de téléphone 2** jusqu'à ce qu'il atteigne également le nombre maximal de tentatives.

  Lorsque tous les numéros ont atteint le nombre maximal de tentatives de composition, l'entrée trouble Signaler un échec est ouverte.
- **Composer la tonalité DTMF**: Lorsque cette option est activée, le modem utilise la numérotation DTMF (tonalité) lorsqu'il compose le **Numéro de téléphone 1**. (Onglet**Général**). Lorsque l'option est désactivée, le modem utilise la numérotation par impulsions.
- **Composer la tonalité DTMF 2**: Lorsque cette option est activée, le modem utilise la numérotation DTMF (tonalité) lorsqu'il compose le **Numéro de téléphone 2**. (onglet **Général**). Lorsque l'option est désactivée, le modem utilise la numérotation par impulsions.
- **Rapport ouvert** : Lorsque cette option est activée, le service signalera le désarmement (ouverture) de toutes les zones utilisant ce service.
- **Report close** : Lorsque cette option est activée, le service signalera l'armement (fermeture) de tous les secteurs utilisant ce service.
- **Rapport des alarmes** : Lorsque cette option est activée, le service signalera les alarmes d'entrée.
- **Signalement des effractions** : Lorsque cette option est activée, le service signalera les sabotages d'entrée et les alarmes d'entrées trouble.
- **Rapport de restauration** : Lorsque cette option est activée, le service signalera les restaurations d'entrée.
- **Report bypass** : Lorsque cette option est activée, le service signalera les contournements d'entrée.
- **Enregistrer les événements du modem dans le tampon d'événements** : Lorsque cette option est activée, des événements détaillés décrivant la progression de l'appel seront enregistrés dans le journal des événements pour chaque rapport. Cette option peut être utilisée pour le dépannage des problèmes mais doit être désactivée pendant le fonctionnement normal car un grand nombre d'événements seront générés.
- **Envoyer un code client à 4 chiffres**: Lorsque cette option est activée, le service SIA envoie un code client à 4 chiffres au lieu des 6 chiffres standard. Ceci peut être utilisé avec des récepteurs qui ne sont pas conformes à la spécification SIA complète ou avec des logiciels qui ne peuvent pas accepter des numéros à gros chiffres.

  Vérifiez la configuration du récepteur avec la société de surveillance avant de régler cette option.
- **Le code client de la zone sera de 6 chiffres**: Le niveau 2 de SIA peut accepter des codes clients de 4 ou 6 chiffres. Lorsque cette option est activée, si le **Code Client** défini pour une zone (**Programmation | Zones | Configuration**) est composé de 4 chiffres, il sera étendu à 6 chiffres en ajoutant 00. Cette option peut être remplacée par **Envoyer un code client à 4 chiffres** ci-dessus.

  Vérifiez la configuration du récepteur avec la société de surveillance avant de régler cette option.

- **Envoyer les numéros d'entrée à 5 chiffres**: Lorsque cette option est activée, le service SIA envoie les identifiants d'entrée sous forme de 5 chiffres au lieu des 4 standard. Cela permet de spécifier des numéros d'entrée plus importants.

  Le format SIA niveau 2 prend en compte les codes d'entrée à 5 chiffres, mais cela peut ne pas être pris en compte par tous les récepteurs.

  Vérifiez la configuration du récepteur avec la société de surveillance avant de régler cette option.

- **Reporter les numéros d'utilisateur en hexadécimal**: Lorsque cette option est activée, le service SIA enverra l'identifiant de l'utilisateur sous la forme d'un nombre hexadécimal à 4 chiffres. Cette option peut remplacer l'option **Numéro d'utilisateur du rapport en 5 chiffres** ci-dessous.

  Vérifiez la configuration du récepteur avec la société de surveillance avant de régler cette option.

- **Numéro d'utilisateur du rapport en 5 chiffres**: Lorsque cette option est activée, le service SIA envoie les identifiants d'utilisateur sous forme de 5 chiffres au lieu des 4 standard. Cela permet de spécifier des numéros d'utilisateur plus importants.

  Le format SIA niveau 2 prend en charge les codes d'utilisateur à 5 chiffres, mais cela peut ne pas être pris en charge par tous les récepteurs.

  Vérifiez la configuration du récepteur avec la société de surveillance avant de régler cette option.

Automatisation et contrôle

Ce service d'intégration fournit une interface générique pour la communication avec des systèmes d'automatisation tiers (par exemple, Control 4, Crestron, AMX, C-Gate, Command Fusion) et d'autres programmes. Cela permet Protege au système d'être surveillé et contrôlé de l'extérieur par des applications personnalisées.

Les applications externes peuvent se connecter Protege au contrôleur à l'aide du NIP d'un utilisateur valide. Les messages sont envoyés et reçus via le ICT Protocole d'automatisation et de contrôle. Pour plus d'informations, contacter ICT.

Automatisation et contrôle | Général

Configuration

- **Numéro de port** : Le numéro de port doit être défini sur TCP/IP pour les contrôleurs de rail DIN.
  Les options Port de communication externe 1-4 sont uniquement utilisées pour les contrôleurs PCB existants utilisant l'interface de communication série PRT-COMM .
- Vitesse du port : Le débit en bauds pour les communications série, qui peut être ajusté pour correspondre à la configuration de l'hôte. Ceci n'a aucun effet lorsque le **Numéro de port** est défini sur TCP/IP.
- **Parité** : La parité pour les communications série, qui peut être ajustée pour correspondre à la configuration de l'hôte. Ceci n'a aucun effet lorsque le **Numéro de port** est défini sur TCP/IP.
- **Port IP** :Le port TCP/IP que le service utilisera pour communiquer. Ceci n'est pas nécessaire si un module PRT-COMM est dedans.
- **Niveau de cryptage** : Règle le type de cryptage utilisé pour crypter les messages du service. Les paramètres de cryptage doivent ici correspondre à ceux de l'appareil récepteur afin que les messages puissent être décryptés.
- **Clé de cryptage** : Si le **niveau de cryptage** est réglé, ce champ définit la clé de cryptage associée. La clé est une séquence quelconque de lettres et de chiffres partagée avec l'appareil récepteur. Pour un cryptage de 128 bits, la clé doit comporter 16 caractères; pour 192 bits, elle doit comporter 24 caractères; et pour 256 bits, elle doit comporter 32 caractères.
- **Type de somme de contrôle** : Définit le type de somme de contrôle qui sera ajouté à la fin de chaque paquet de contrôle. La somme de 8 bits est une simple addition de tous les octets précédents dans le paquet. Le CRC 16 bits est un CRC (Cyclic Redundancy Check) standard basé sur le polynôme CRC-16-CCITT.

Options

- **Les nombres sont de gros boutien**: La méthode par défaut pour envoyer des nombres multi-octets est Little Endian (l'octet le moins significatif en premier). Si cette option est sélectionnée, les nombres multi-octets seront envoyés en Big Endian (l'octet le plus significatif en premier).
- **Autoriser les demandes de statut lorsque l'utilisateur n'est pas connecté** : Lorsque cette option est activée, le programme externe connecté au service peut demander et recevoir des mises à jour d'état (par exemple, l'état de la partition) sans se connecter. Le programme ne peut pas envoyer de commandes de contrôle (par exemple., désarmer la partition) sans ouvrir une session avec un NIP d'utilisateur valide.
- **Utiliser la minuterie de verrouillage de connexion si un NIP incorrect est fourni** : Lorsque cette option est activée, si un NIP incorrect est fourni trois fois de suite, le service bloque toute nouvelle tentative pendant 60 secondes.
- **Commandes ACCUSÉ DE RÉCEPTION** : Avec cette option activée, le service enverra un paquet d'accusé de réception (AR) au programme externe après avoir reçu avec succès une commande de contrôle.
- **Attendre AR pour la surveillance de l'état** : Avec cette option activée, le service s'attend à ce qu'un paquet d'accusé de réception (AR) soit retourné après avoir envoyé une mise à jour de l'état. Si aucun accusé de réception n'est renvoyé dans les 3 secondes, la mise à jour du statut sera renvoyée.
- **Renvoyer le contrôle d'état si pas d'accusé de réception après 5 tentatives** : Si l'option **Attendre AR pour la surveillance de l'état** est activée ci-dessus, cette option contrôle le critère de coupure pour les mises à jour d'état non reconnues.

Lorsque cette option est activée, le service renverra chaque message d'état jusqu'à ce qu'il reçoive un AR du programme externe. Lorsque cette option est désactivée, le service cessera d'envoyer une mise à jour d'état si elle n'a pas été reconnue après 5 tentatives.

- **Attendre AR pour les événements** : Avec cette option activée, le service s'attendra à ce qu'un paquet d'accusé de réception (AR) soit retourné après avoir envoyé un événement. Si aucun accusé de réception n'est renvoyé dans les 3 secondes, l'événement sera renvoyé.
- **Renvoyer les événements si pas AR après 5 tentatives** : Si l'option **Attendre AR pour les événements** est activée ci-dessus, cette option contrôle le critère de coupure pour les événements non reconnus.

  Lorsque cette option est activée, le service renverra chaque événement jusqu'à ce qu'il reçoive un AR du programme externe. Lorsque cette option est désactivée, le service cessera d'envoyer un événement si elle n'a pas été reconnu après 5 tentatives.

Modbus

Ce service d'intégration configure le contrôleur Protege GX pour qu'il agisse comme un esclave MODBUS, ce qui lui permet de recevoir des messages de surveillance et de contrôle en provenance des systèmes clientes via le protocole MODBUS. Cela inclut les systèmes d'automatisation industrielle standard tels que Citect, Wonderware, The FIX et DAQ Factory.

Pour plus d'informations et d'instructions de programmation, consultez Note d'application 023 : Intégration du Serveur Modbus Protege GX. Il existe une intégration distincte qui permet au contrôleur d'agir en tant que client Modbus - consultez Note d'application 353 : Intégration du client Modbus Protege GX.

Modbus | Général

Configuration

- **Numéro de port** : Le numéro de port doit être défini sur TCP/IP pour les contrôleurs de rail DIN.
  Les options Port de communication externe 1-4 sont uniquement utilisées pour les contrôleurs PCB existants utilisant l'interface de communication série PRT-COMM .
- Vitesse du port : Le débit en bauds pour les communications série, qui peut être ajusté pour correspondre à la configuration de l'hôte. Ceci n'a aucun effet lorsque le **Numéro de port** est défini sur TCP/IP.

  La vitesse par défaut pour les applications Modbus est 9600.
- **Parité** : La parité pour les communications série, qui peut être ajustée pour correspondre à la configuration de l'hôte. Ceci n'a aucun effet lorsque le **Numéro de port** est défini sur TCP/IP.

  La parité par défaut pour les applications Modbus est Pair.
- **Adresse client** : L'adresse de l'appareil pour le module dans le réseau de communication Modbus. Il doit s'agir d'un nombre hexadécimal unique qui n'est pas 0x00 ou 0xFF. L'adresse client est généralement fournie par l'entreprise d'automatisation ou le système SCADA auquel le contrôleur sera connecté.
- **Temps de sondage** : Ce champ définit la durée maximale (en secondes) prévue entre les sondages du maître MODBUS. Par exemple, si le temps de sondage est fixé à 60, le contrôleur s'attendra à un sondage toutes les 60 secondes. S'il n'y a pas de sondage, une erreur sera consignée dans le journal des événements et **Sortie/groupe de sorties s'active lorsque sondage échoue** sera activé.
- **La sortie / le groupe de sorties s'active lorsqu'un sondage échoue** : Cette sortie ou ce groupe de sorties est activé(e) lorsque le **Temps de sondage** défini ci-dessus expire sans qu'aucun message de sondage ne soit reçu. Elle est désactivée lorsque le service Modbus complète une communication valide. Utiliser cette option pour avertir les utilisateurs qu'il y a un problème dans le système Modbus.

Options

- **Enregistrer les événements de communication** : Lorsque cette option est activée, les événements seront enregistrés pour toutes les communications MODBUS. Cette option peut être utile pour la configuration initiale et le dépannage, mais doit être désactivée pendant le fonctionnement normal afin d'économiser le stockage des événements.
- **Enregistrer les erreurs de communication** : Lorsque cette option est activée, les événements seront enregistrés pour toutes les erreurs de communication MODBUS.
- **Nombres entiers en tant que BIG ENDIAN** : La méthode par défaut pour envoyer des nombres multi-octets est Little Endian (l'octet le moins significatif en premier). Si cette option est sélectionnée, les nombres multi-octets seront envoyés en Big Endian (l'octet le plus significatif en premier).
- **Utiliser variables de registres à** distance Il s'agit d'une option héritée qui n'a aucun effet.:
- **Activer traduction d'entrée de bobine** : Il s'agit d'une option héritée qui n'a aucun effet.

C-Bus

Ce service d'intégration communique avec une interface réseau C-Bus (CNI) pour le contrôle de l'automatisation.

Pour plus d'informations et d'instructions de programmation, consulter la note d'application 289 : Intégration C-Bus avec Protege GX et Protege WX.

C-Bus | Général

Configuration

- **Numéro de port** : Le numéro de port doit être défini sur TCP/IP pour les contrôleurs de rail DIN.
  Les options Port de communication externe 1-4 sont uniquement utilisées pour les contrôleurs PCB existants utilisant l'interface de communication série PRT-COMM .
- Vitesse du port : Le débit en bauds pour les communications série, qui peut être ajusté pour correspondre à la configuration de l'hôte. Ceci n'a aucun effet lorsque le **Numéro de port** est défini sur TCP/IP.
- **Parité** : La parité pour les communications série, qui peut être ajustée pour correspondre à la configuration de l'hôte. Ceci n'a aucun effet lorsque le **Numéro de port** est défini sur TCP/IP.
- **Adresse IP CNI** : L'adresse IP de l'interface réseau C-Bus avec laquelle le contrôleur communique.
- **Port CNI** : Le port IP utilisé pour communiquer avec l'interface réseau du C-Bus. Ce port doit être le même port que celui utilisé pour les communications entre le CNI et le logiciel C-Bus Toolkit.
- **Echec de communication sortie / groupe de sortie** : Cette sortie ou ce groupe de sortie est activé en cas d'échec de la communication avec le CNI.

Options

- **Activer la sortie de texte** : Activez cette option pour convertir les communications du contrôleur en un format lisible par un humain. Cela permet le débogage si un appareil de surveillance est utilisé à la place du CNI ; cependant, l'intégration ne fonctionnera pas si cette option est activée.
- **Ajouter CR à la sortie de texte** : Lorsque **Activer la sortie texte** est utilisé, activer cette option ajoute un caractère de retour de transport à la fin de chaque message.
- **Ajouter LF à la sortie de texte** : Lorsque **Activer la sortie texte** est utilisé, activer cette option ajoute un caractère de saut de ligne à la fin de chaque message.
- **Enregistrer message d'échec du C-Bus PCI** : Avec cette option activée, les événements d'erreur seront enregistrés lorsque le CNI ne parvient pas à s'initialiser. Cette option peut être utile pour la configuration initiale et le dépannage, mais doit être désactivée pendant le fonctionnement normal afin d'économiser le stockage des événements.
- **Enregistrer le message d'accusé réception du C-Bus** : Lorsque cette option est activée, les événements seront enregistrés pour chaque paquet d'accusé de réception (AR) reçu du CNI. Cette option peut être utile pour la configuration initiale et le dépannage, mais doit être désactivée pendant le fonctionnement normal afin d'économiser le stockage des événements.
- **Enregistrer activité de données C-Bus** : Lorsque cette option est activée, les événements seront enregistrés pour tous les paquets envoyés à et reçus de la CNI. Cette option peut être utile pour la configuration initiale et le dépannage, mais doit être désactivée pendant le fonctionnement normal afin d'économiser le stockage des événements.

Rapport IP

Ce service de rapport envoie des alarmes, des tests et d'autres événements à une station de surveillance via une connexion IP. Le service de rapport IP prend en charge un certain nombre de formats sur des connexions UDP et TCP, cryptées ou non, ce qui lui permet d'envoyer des rapports plus informatifs à moindre coût et en toute sécurité que les rapports traditionnels par ligne téléphonique.

En plus de la connexion Ethernet embarquée, certains modèles de contrôleurs Protege GX incluent une interface USB-ethernet qui vous permet de connecter un Protege. Rail DIN Modem Cellulaire pour envoyer des messages de rapport sur un réseau cellulaire 4G. Pour plus d'informations et d'instructions de configuration, consultez le Protege Rail DIN Modem Cellulaire guide de configuration.

En outre, le service de rapport IP peut être configuré pour envoyer des notifications poussées à Protege l'application mobile. Pour plus d'informations, consulter la note d'application 201 : Protege GX Configuration de la notification poussée.

Rapport IP | Général

Configuration

- **Code client**: Ce code représente le contrôleur ou le site dans les rapports destinés à la station de surveillance centrale. Un code de compte pour rapport IP peut comporter jusqu'à 8 chiffres. Les zéros non significatifs seront tronqués de manière à ce que le nombre minimal de chiffres soit envoyé (par exemple, 004 311 sera raccourci à 4 311). Si le code client est plus long que ne le permet le format de rapport, il sera tronqué.
- **Protocole de signalement**: Le service de rapport IP prend en charge un certain nombre de formats de rapport. Il s'agit notamment de versions de formats traditionnels qui peuvent être envoyées via une connexion IP, offrant ainsi une flexibilité maximale.
  - **Armor IP**: ArmorIP est un protocole propriétaire de signalement IP par ICT. Les rapports sont envoyés à un serveur ArmorIP installé qui fournit une sortie Ademco 685 standard et permet le routage et la redirection des messages vers d'autres récepteurs. Ce format fournit une transmission textuelle complète qui comprend les noms des enregistrements (utilisateur, zone, entrée) qui ont généré le rapport et des informations supplémentaires telles que l'heure du champ et le nom du contrôleur. Il comprend également des codes ContactID standard pour l'automatisation.

    Le rapport ArmorIP est disponible en mode UDP et TCP, et en mode crypté ou non crypté.

    Pour plus d'informations, consulter le manuel d'utilisation de l'application de surveillance Internet ArmorIP Version 3:
  - **SIA sur IP (DC09)**: Communique au format SIA niveau 2 en utilisant la spécification SIA DC09 pour la communication numérique.
  - **CID sur IP**: Communique au format Contact ID en utilisant la spécification SIA DC09 pour la communication numérique.
  - **CSV IP**: CSV IP est un protocole de signalement IP utilisé par Alarm New Zealand. Il s'agit d'un protocole ASCII générique qui se présente sous forme de : nom d'utilisateur, mot de passe, code client, message. Ce service envoie des messages d'erreur au format Contact ID.
  - **Patriot LS30**: Patriot LS30 est un protocole propriétaire de signalement IP de Patriot Systems. Ce service envoie des messages d'erreur dans une variante du format Contact ID.
- **Nom d'utilisateur/mot de passe CSV IP**: Le nom d'utilisateur et le mot de passe requis pour le protocole CSV IP.
- **Niveau de cryptage** : Règle le type de cryptage utilisé pour crypter les messages du service. Les paramètres de cryptage doivent ici correspondre à ceux de l'appareil récepteur afin que les messages puissent être décryptés.
- **Clé de cryptage** : Si le **niveau de cryptage** est réglé, ce champ définit la clé de cryptage associée. La clé est une séquence quelconque de lettres et de chiffres partagée avec l'appareil récepteur. Pour un cryptage de 128 bits, la clé doit comporter 16 caractères; pour 192 bits, elle doit comporter 24 caractères; et pour 256 bits, elle doit comporter 32 caractères.

- **Temps de sondage**: Le temps (en secondes) entre les messages d'interrogation envoyés par le contrôleur au serveur de réception. Le format du message d'interrogation dépend du **protocole de signalement** défini ci-dessus.

  Assurez-vous que le même temps de sondage est réglé sur le contrôleur et sur le récepteur.

- **Service de sauvegarde**: Le service de secours sera utilisé lorsque le service rapport IP subira une perte de communication. Il est utile de choisir un service qui se connecte sur la ligne téléphonique pour s'assurer que les rapports peuvent être envoyés sur une connexion alternative en cas de panne de câble ou d'interruption de l'Internet.

  Le service sélectionné ici doit avoir **le service fonctionne comme sauvegarde** activée dans **l'onglet** Options.

- **Paramètres de la carte CID**: Cette option n'est pas nécessaire pour la plupart des formats de rapport d'identification du contact. Les codes de signalement sont réglés dans la programmation pour les utilisateurs, les entrées, les entrées trouble et les zones individuelles, et peuvent être réinitialisés à un schéma de mappage spécifique si nécessaire lorsqu'un opérateur génère la carte de rapport centrale (**Rapports | Rapport de la station centrale**). Toutefois, lorsque la cartographie SIMS II est en cours d'utilisation, cette option doit être réglée sur SIMS II.

  Pour plus d'informations, voir la note d'application 316 : Rapports au format Contact ID dans Protege GX et Protege WX.

- **Temps avant la sauvegarde**: Si un **service de sauvegarde** est configuré ci-dessus, ce champ définit la durée (en secondes) pendant laquelle la connexion IP doit être perdue avant que le service n'active la sauvegarde.

Paramètres du canal primaire/secondaire

Le canal secondaire fournit un chemin de sauvegarde pour la communication avec le poste de surveillance en cas de défaillance du canal primaire. Si le canal primaire ne peut être utilisé, le service essaiera le canal secondaire avant de lancer le service de sauvegarde.

Les deux canaux doivent au minimum avoir des adresses IP et/ou des numéros de port différents. Pour une plus grande fiabilité, utilisez deux supports différents pour l'accès à l'internet, par exemple des connexions câblées et sans fil.

- **Adresse IP / Nom d'hôte**: L'adresse du destinataire auquel les messages sont envoyés.
- **Numéro du port IP**: Le port utilisé pour la communication avec le récepteur. Cela dépend de la configuration du logiciel ou du matériel du récepteur.
- **Adaptateur**: La carte réseau du contrôleur que le service rapport IP utilise pour la communication. Cette variable doit être définie sur Câble pour utiliser l'interface ethernet embarquée, ou USB ethernet pour utiliser un modem cellulaire.

  Les rapports 3G ne sont disponibles qu'avec le contrôleur (PRT-CTRL-DIN-3G).

- **Tentatives d'ouverture du port**: Le nombre de fois que le service doit tenter d'ouvrir le port de communication avant d'enregistrer une panne de communication et de passer à l'autre canal ou à un service de sauvegarde. Pour contourner ce paramètre, utilisez l' **option Changer immédiatement d'adresse IP** secondaire (**onglet** Options).
- **Temps d'attente de l'accusé de réception**: La durée (en secondes) pendant laquelle le service attendra un paquet d'accusé de réception (AR) du récepteur avant de renvoyer le rapport.
- **Signaler sortie d'échec / Groupe de sorties**: Cette sortie ou ce groupe de sorties s'active lorsque le service subit une panne de communication. Il se désactive lorsque la communication est rétablie.
- **Activer l'interrogation hors ligne**: L'interrogation hors ligne se produit lorsque le service n'est pas normalement utilisé, c'est-à-dire qu'il fonctionne comme une sauvegarde. Si le service de sauvegarde perd la connexion, le rapport d'erreur s'ouvrira et un rapport sera envoyé à la station de surveillance. Cela permet de détecter tout problème avant que le service de sauvegarde ne soit nécessaire.
  - **Échec de la chaîne Code CID / groupe / zone**: Le code d'événement Contact ID, le numéro de groupe et le numéro de zone envoyés lorsque l'interrogation hors ligne échoue.

- **Nombre de sondages hors ligne**: Le nombre de sondages hors ligne qui doivent échouer avant que l'échec de la connexion ne soit signalé.
- **Heure du rapport de test hors ligne**: Le temps entre les sondages hors ligne, en minutes.

Paramètres de la version 3

Cette section affiche les paramètres qui étaient utilisés dans la version 3 du logiciel et les versions antérieures. Ces paramètres ne nécessitent pas de configuration dans la version 4 ou ultérieure.

Rapport IP | Options

- **Commutation immédiate de l'IP secondaire**: Si cette option est activée, lorsque le canal primaire ne parvient pas à se connecter, le service tentera immédiatement d'utiliser le canal secondaire au lieu de faire plusieurs tentatives de connexion sur le canal primaire (c'est-à-dire que le **paramètre de tentatives d'ouverture de port** est ignoré).
- **Rapport ouvert** : Lorsque cette option est activée, le service signalera le désarmement (ouverture) de toutes les zones utilisant ce service.
- **Report close** : Lorsque cette option est activée, le service signalera l'armement (fermeture) de tous les secteurs utilisant ce service.
- **Rapport des alarmes** : Lorsque cette option est activée, le service signalera les alarmes d'entrée.
- **Signalement des effractions** : Lorsque cette option est activée, le service signalera les sabotages d'entrée et les alarmes d'entrées trouble.
- **Rapport de restauration** : Lorsque cette option est activée, le service signalera les restaurations d'entrée.
- **Report bypass** : Lorsque cette option est activée, le service signalera les contournements d'entrée.
- **Enregistrer réponse de reconnaissance**: Lorsque cette option est activée, un événement sera enregistré chaque fois qu'un paquet d'accusé de réception (AR) sera reçu du récepteur de surveillance. Cette option peut être utile pour la configuration initiale et le dépannage, mais doit être désactivée pendant le fonctionnement normal afin d'économiser le stockage des événements.
- **Enregistrer le message de sondage**: Lorsque cette option est activée, un événement est enregistré chaque fois qu'un message de sondage est envoyé au récepteur de surveillance. Cette option peut être utile pour la configuration initiale et le dépannage, mais doit être désactivée pendant le fonctionnement normal afin d'économiser le stockage des événements.
- **Enregistrer les tentatives de message**: Lorsque cette option est activée, un événement sera enregistré chaque fois que le service renvoie un message qui a échoué.
- **Enregistrer les rapports de panne**: Quand cette option est activée, un événement sera enregistré lorsque les communications ont complètement échoué et que le service attend de faire une nouvelle tentative.
- **Le service fonctionne comme une sauvegarde** : Lorsque cette option est activée, le service ne commencera pas à rapporter sauf s'il est initié par un autre service qui n'a pas réussi à rapporter. Ce service transmet tous les messages du service primaire qui n'ont pas réussi à les envoyer, puis le fonctionnement revient au service primaire. Le service de secours démarre et s'arrête en même temps que le service primaire.

  Seuls les services IP de rapport ont la possibilité de définir un **Service de secours**. (onglet **Général**).

Interphone

Ce service d'intégration communique avec des interphones spécifiques de première et de seconde main, permettant aux utilisateurs de déverrouiller les étages et les portes des ascenseurs à partir de l'interphone.

Pour plus d'informations, consulter la la note d'application 143 : Intégration d'interphone dans Protege GX. Pour l'intégration avec une station d'entrée Protege, consulter le manuel d'installation Protege Vandal Resistant Touchscreen Entry Station .

Interphone | Général

Configuration

- **Numéro de port** : Le numéro de port doit être défini sur TCP/IP ou UDP/IP pour les contrôleurs de rail DIN.
  Les options Commande externe Port 1-4 sont uniquement utilisées pour les contrôleurs PCB hérités utilisant l'interface de communications en série PRT-COMM .
- Vitesse du port : Le débit en bauds pour les communications série, qui peut être ajusté pour correspondre à la configuration de l'hôte. Ceci n'a aucun effet lorsque le **Numéro de port** est défini sur TCP/IP.
- **Parité** : La parité pour les communications série, qui peut être ajustée pour correspondre à la configuration de l'hôte. Ceci n'a aucun effet lorsque le **Numéro de port** est défini sur TCP/IP.
- **Port TCP/IP** :Le port TCP/IP que le service utilisera pour communiquer. Ceci n'est pas nécessaire si un module PRT-COMM est dedans.
- **Type d'interphone** : Le type ou la marque de l'interphone avec lequel ce service communiquera. Les interphones dotés d'interfaces en série doivent être intégrés à l'aide d'un convertisseur en série-ethernet adapté, tel que le Moxa DE-211 ou le Moxa DE-311, afin de permettre au contrôleur Protege GX de communiquer avec l'interphone via TCP/IP.

  Les contrôleurs PCB hérités peuvent communiquer via l'interface en série à l'aide d'un module PRT-COMM .

  - **Siedle**
  - **Sentex Infinity multi points**
  - **Sentex Infinity unique**
  - **Enterphone** (l'unité Enterphone ne prend pas en charge les unités multiples et il n'est donc pas nécessaire que l'adresse de l'interphone soit définie).
  - **Interphone SES** (interphones TEC2 et TEC4)
  - **Mesh** (utilisé pour l'intégration des interphones MESH de Viscount et Protege des stations d'entrée)
- **Enregistrer les événements de débogage d'ascenseur** : Lorsque cette option est activée, des événements sont générés pour chaque paquet reçu de l'interphone. Ceci peut être utilisé pour diagnostiquer des problèmes, mais doit être désactivé pendant le fonctionnement normal afin d'économiser le stockage des événements.
- **Activer adresse interphone 1** : Par défaut, le **groupe d'ascenseurs** défini ci-dessous est utilisé pour déterminer les cabines d'ascenseurs auxquelles un utilisateur peut accéder à partir de l'interphone. Avec cette option activée, le groupe d'ascenseurs défini dans le niveau d'accès de l'utilisateur sera utilisé à la place.
- **Délai d'attente de communication** : Le temps d'inactivité maximum entre les octets avant que la communication ne soit considérée comme à l'arrêt. Cela garantit que le contrôleur attend un temps approprié pour qu'un paquet de données fragmentées provenant de l'interphone soit complété. Cette option n'a aucun effet lorsque le **Numéro de port** est défini sur TCP/IP ci-dessus.
- **Adresse interphone 1 à 4** : Le service d'interphone peut se connecter à un maximum de quatre interphones, chacun contrôlant une seule porte (**Porte 1 à 4** ci-dessous). Si un contrôle de portes est nécessaire, définir l'adresse de l'interphone qui contrôlera chaque porte correspondante.
- **Identifier type d'utilisateur** : Lorsqu'un utilisateur demande l'accès pour déverrouiller une porte ou un étage depuis l'interphone, il doit saisir un numéro d'identification. Cela permet au contrôleur de valider la demande d'accès par rapport au niveau d'accès de l'utilisateur et d'enregistrer un événement précis. Le type de numéro ID utilisé peut être l'un des suivants :

- **Numéro indice de l'utilisateur** : L'ID base de données de l'utilisateur dans le système Protege GX.
- **NIP de l'utilisateur** : Le NIP de l'utilisateur, défini dans **Utilisateurs | Utilisateurs | Général**.
- **Numéro de carte de l'utilisateur** : Le numéro de carte de l'utilisateur, défini dans **Utilisateurs | Utilisateurs | Général**. Le numéro d'installation doit être réglé sur 0 ou sur le numéro d'installation indiqué dans la documentation de l'interphone.
- **Numéro de décalage indice de l'utilisateur** : L'ID base de données de l'utilisateur ajouté à la **valeur de décalage indice de l'utilisateur** définie ci-dessous. Par exemple, si le décalage est égal à 1, l'utilisateur doit saisir son ID base de données + 1 à l'interphone.

- **Groupe d'ascenseurs** : Les cabines d'ascenseurs auxquelles on peut accéder depuis cet interphone. Lorsqu'un utilisateur accède à un groupe d'étages depuis l'interphone, les étages sont déverrouillés dans tous les ascenseurs du groupe.
- **Groupe d'étages** : Les étages auxquels on peut accéder depuis cet interphone. Lorsqu'un utilisateur saisit son numéro ID à l'interphone, tous les étages qui sont à la fois dans ce groupe et dans le niveau d'accès de l'utilisateur sont déverrouillés.

  Par exemple, si le groupe d'étages défini ici contient tous les étages du bâtiment, mais que l'utilisateur n'a accès qu'à son étage d'accueil, il peut saisir son ID à l'interphone pour déverrouiller uniquement son étage d'accueil.
- **Sortie demande d'interphone valide / groupe de sorties** : Cette sortie ou ce groupe de sorties est activé(e) lorsqu'une demande provenant de l'interphone est reçue et décodée avec succès. Elle n'est pas désactivée automatiquement et doit être programmée avec un **Temps d'activation** (**Programmation | Sorties | Général**) pour s'assurer qu'elle est désactivée entre les demandes.
- **Sortie accès accordé / groupe de sorties programmables** : Cette sortie ou ce groupe de sorties est activé lorsque l'accès est accordé avec succès à un utilisateur via l'interphone. Elle n'est pas désactivée automatiquement et doit être programmée avec un **Temps d'activation** (**Programmation | Sorties | Général**) pour s'assurer qu'elle est désactivée entre les demandes d'accès.
- **Valeur de décalage indice de l'utilisateur** : Lorsque le champ **Identifier type d'utilisateur** ci-dessus est défini sur Numéro de décalage indice de l'utilisateur, ce champ définit le numéro de décalage. Ce chiffre est soustrait du nombre saisi par l'utilisateur pour obtenir l'ID base de données.

Portes

- **Porte 1 à 4** : Le service d'interphone peut se connecter à un maximum de quatre interphones, chacun contrôlant une porte. Lorsqu'un utilisateur saisit son ID à l'un des interphones, la porte correspondante est déverrouillée (à condition que l'utilisateur dispose des autorisations correctes dans son niveau d'accès).

Me lier

Ce service de contrôle vous permet de cartographier les sorties entre deux contrôleurs Protege GX, de sorte que les sorties du contrôleur secondaire suivent l'état de celles du contrôleur primaire. Un service Me lier doit être programmé à la fois dans le contrôleur principal et dans le contrôleur suivant, afin que les signaux puissent être envoyés et reçus.

Il s'agit d'une fonctionnalité héritée. Une option plus simple et plus souple pour relier deux contrôleurs est fournie par des opérations entre contrôleurs (consultez la page 24).

Me lier | Général

Configuration

- **Fonction** : Le service Me lier peut soit envoyer soit recevoir des données. S'il envoie des données, ce contrôleur sera le primaire qui contrôle l'état de la sortie. S'il reçoit des données, ce contrôleur sera le secondaire qui suit l'état de la sortie primaire.
- **Adresse IP / Nom d'hôte** : L'adresse de l'autre contrôleur avec lequel ce service communique.
- **Numéro de port IP** : Le port TCP/IP que le service utilisera pour communiquer. Le même port doit être défini dans le Service Me lier correspondant programmé dans l'autre contrôleur.
- **Temps de sondage** : La durée (en secondes) entre les messages de sondage envoyés entre les deux contrôleurs. Régler un temps plus court garantit que les états de la sortie resteront synchronisés.
- **Début de sortie liée** : La première sortie est mise en correspondance entre les deux contrôleurs.
- **Nombre sorties liées** : Le nombre total de sorties qui seront mappées entre les deux contrôleurs, y compris le **début de sortie liée**. Le compte commence au début et compte par ID base de données jusqu'à ce qu'il comprenne le nombre de sorties défini ici.

  Chaque fois qu'une sortie de cette gamme change d'état, le changement est envoyé à l'autre contrôleur et la sortie correspondante est mise à jour. La valeur de comptage doit être la même dans les deux contrôleurs reliés par ce service afin que chaque sortie ait un équivalent sur l'autre contrôleur.
- **Sortie sondage OK / groupe de sorties** : Cette sortie ou ce groupe de sorties est activé lorsque la communication est établie avec succès entre les deux contrôleurs. Il se désactive lorsque la communication est perdue.
- **Sortie sondage échoué / groupe de sorties** : Cette sortie ou ce groupe de sorties est activé lorsque la communication entre les deux contrôleurs échoue. Il est désactivé lorsque la communication est rétablie.

Me lier | Options

- **Enregistrer reconnaissance d'événement** : Lorsque cette option est activée, des événements seront générés à chaque fois qu'un paquet de communication d'accusé de réception (ACK) est reçu. Cette fonction est utile pour la configuration initiale mais doit être désactivée pendant le fonctionnement normal, afin d'économiser le stockage des événements.
- **Enregistrer acceptation de sondage** : Lorsque cette option est activée, des événements sont générés chaque fois qu'un sondage a été accepté par l'autre contrôleur. Cette fonction est utile pour la configuration initiale mais doit être désactivée pendant le fonctionnement normal, afin d'économiser le stockage des événements.
- **Enregistrer nouvelle tentative de communication** : Lorsque cette option est activée, des événements sont générés chaque fois que le service tente à nouveau d'établir une communication après une panne de réseau ou une perte de service.
- **Enregistrer échec de communication** : Quand cette option est activée, des événements sont générés lorsque la communication a complètement échoué et que le service attend de faire une nouvelle tentative.

VizIP

Ce service d'intégration communique avec les DVRs par une connexion IP en utilisant le protocole VizIP. Cela vous permet de mapper Protege GX les sorties programmables aux sorties d'alarme sur le DVR, supprimant ainsi le besoin de connexions de câblage physique entre le DVR et le Protege GX contrôleur du système.

VizIP | VizIP

- **Adresse IP VizIP / Nom d'hôte**: L'adresse du DVR auquel le service VizIP se connectera.
- **Port IP VizIP** : Le port TCP/IP que le service utilisera pour communiquer avec le DVR.
- **Temps de sondage VizIP** : L'intervalle (en secondes) entre les messages de sondage envoyés par le contrôleur au DVR. La définition d'un temps plus court garantit que les statuts de sortie resteront synchronisés.
- **Début de sorties dehors** : La première sortie fait le lien entre le réseau du contrôleur et les sorties d'alarme du DVR.
- **Nombre de sorties dehors** : Le nombre total de sorties qui seront mappées entre le réseau du contrôleur et les sorties d'alarme du DVR. Le mappage commence au **début de sorties dehors** et incrémente l'adresse de la sortie programmable jusqu'à ce qu'elle comprenne le nombre de sorties défini ici. Chaque fois qu'une sortie de cette gamme change d'état, le changement est envoyé au DVR et la sortie d'alarme correspondante est mise à jour.

  Ce nombre doit correspondre au nombre de sorties d'alarme du DVR qui seront contrôlées.

- **Sortie communications échouent /Groupe de sorties programmables** : Cette sortie ou ce groupe de sorties programmables est activé lorsque la communication entre le contrôleur et le DVR échoue. Il est désactivé lorsque la communication est rétablie.
- **Enregistrer reconnaissance**: Lorsque cette option est activée, un événement est généré à chaque fois qu'un paquet de communication d'accusé de réception (ACK) est reçu. Cette fonction est utile pour la configuration initiale mais doit être désactivée pendant le fonctionnement normal afin de sauvegarder le stockage des événements.
- **Journal de sondage OK** : Lorsque cette option est activée, un événement sera généré chaque fois qu'un message de sondage est envoyé au DVR. Cette fonction est utile pour la configuration initiale mais doit être désactivée pendant le fonctionnement normal afin de sauvegarder le stockage des événements.

Appartements

Appartements dans Protege GX vous permet de gérer le contrôle d'accès et la détection d'intrusion pour les appartements individuels dans des immeubles et des complexes en copropriété. Cette fonctionnalité logicielle est utilisée en complément de la EliteSuite gamme de claviers, conçue pour la gestion de complexes d'appartements.

Vous pouvez ajouter un maximum de 248 maîtres EliteSuite claviers par contrôleur. Chaque clavier maître peut avoir un réseau d'esclaves comprenant jusqu'à 3 claviers esclaves et jusqu'à 4 lecteurs Nano Prox ou Vario Prox (avec l'utilisation d'unités PRX-SAM).

Le menu de programmation des appartements offre un endroit centralisé pour programmer les paramètres de chaque EliteSuite clavier et des appareils qui y sont connectés. L'ajout ou la modification d'un enregistrement d'appartement crée et met automatiquement à jour les claviers, entrées, entrées trouble, sorties, partitions et utilisateurs associés. C'est plus pratique que de programmer dans le EliteSuite clavier lui-même.

Les enregistrements associés aux appartements peuvent être consultés dans les menus de programmation correspondants, mais ne peuvent être modifiés que dans la programmation des appartements. Pour mettre à jour la programmation du EliteSuite clavier, naviguer vers **Sites | Contrôleurs** et exécuter une commande **Forcer le téléchargement** sur le contrôleur. Naviguer ensuite dans **Modules d'expansions | Claviers** et effectuer une **mise à jour du module** sur l'enregistrement du clavier.

Les appartements sont sous licence. Pour plus de renseignements, voir la Note d'application 184 : Configuration des appartements dans Protege GX. Voir également les manuels d'installation et d'utilisation correspondants de la EliteSuite gamme de claviers.

Il s'agit d'une fonctionnalité héritée. Le matériel décrit ci-dessus peut ne pas être disponible à l'achat.

Appartements | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Description** : Une description de l'appartement pour la commodité d'un gestionnaire d'immeuble ou d'un autre opérateur.
- **Adresse** : L'adresse de l'appartement.
- **Téléphone** : Le numéro de téléphone d'un contact pour l'appartement.
- **Courriel** : L'adresse courriel d'un contact pour l'appartement.
- **Question défi** : Une question défi peut être utilisée par le gestionnaire de l'immeuble dans les situations où il doit identifier l'utilisateur principal de l'appartement.
- **Réponse défi** : La réponse à la **Question défi**. L'utilisateur principal est censé connaître cette réponse.
- **Code du compte** : Ce code représente l'appartement dans les rapports adressés à la station de surveillance centrale. Il s'agit généralement d'un nombre hexadécimal, mais le format peut dépendre de la compatibilité du récepteur et du service de signalisation utilisé.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Appartements | Options

Options de temps

- **Heure d'entrée** : La durée du délai d'entrée de la partition, en secondes. Si une entrée de délai d'entrée est déclenchée alors que la partition est armée, la zone passe en délai d'entrée. Si la partition n'est pas désarmée avant la fin de cette période, l'alarme sera activée.

  Si cette heure est réglée sur Faux, la partition se mettra immédiatement en alarme, quelle que soit l'entrée activée.
- **Heure de sortie** : La durée du délai de sortie de la partition, en secondes. Chaque fois que la partition est armée, le délai de sortie commence, donnant aux utilisateurs le temps de quitter la partition avant qu'elle ne soit armée. Lorsque le délai de sortie est écoulé, la partition est armée. Si cette heure est réglée sur Faux, la partition sera immédiatement armée.
- **Heure de la sirène** : La durée (en minutes) pendant laquelle la sortie de la cloche restera active lorsque l'alarme de la partition est activée. L'heure minimale de l'alarme est de 1 minute.
- **Entrées EOL 1K + 1K** : Lorsque cette option est activée, les entrées connectées à ce clavier sont configurées avec une résistance EOL de type alarme 1K, sabotage 1K. Lorsque cette option est désactivée, la configuration EOL est configurée sur Pas de résistances.
- **Mode d'entrée duplex** : Lorsque cette option est activée, le clavier peut prendre en charge jusqu'à 4 entrées câblées en configuration duplex. Les entrées supplémentaires doivent être adressées comme entrées 3-4 sur le clavier.
- **Bip sur trouble** : Lorsque cette option est activée, si la partition présente un problème, le signal sonore du clavier émet un signal sonore toutes les 2 minutes jusqu'à ce que le problème soit vu. Les problèmes peuvent être vus en appuyant sur **[MENU] [4]**.
- **Mise sous tension désarmée** : Si cette option est activée, lorsque le clavier EliteSuite est mis sous tension, le secteur est désarmé, quel que soit l'état du secteur au moment de la coupure de courant.

  Si cette option est désactivée, le comportement dépend de l'état du secteur au moment de la coupure de courant. Si le secteur était en délai de sortie ou armé, le secteur commence le délai de sortie et s'arme à nouveau. Si le secteur était en délai d'entrée ou en alarme, le secteur passe en alarme. Si le secteur était désarmé, il reste désarmé.
- **PGM de réinitialisation de fumée** : Lorsque cette option est activée, la sortie de réserve du clavier EliteSuite (adresse 1) peut être utilisée pour réinitialiser le détecteur de fumée. Lorsque les touches **[CLEAR]** et **[ENTER]** sont maintenues enfoncées simultanément pendant 2 secondes, la sortie est activée pour désactiver le détecteur de fumée.

  L'activation de cette option définit automatiquement le **PGM de réinitialisation de fumée** sous l'onglet **Clavier | Configuration**.
- **PGM suit le statut d'alarme** : Lorsque cette option est activée, la sortie de réserve (adresse 1) du clavier EliteSuite est activée lorsque la zone est en alarme et désactivée lorsque l'alarme est arrêtée.
- **PGM suit le statut de région** : Lorsque cette option est activée, la sortie de réserve du clavier EliteSuite (adresse 1) est activée lorsque le secteur est armé et désactivée lorsque le secteur est désarmé.
- **Sortie de secours inversée** : Lorsque cette option est activée, les options **Sortie suit l'état d'alarme** et **Sortie suit l'état du secteur** fonctionnent de manière inversée. Par exemple, en utilisant **La sortie suit l'état du secteur**, la sortie sera désactivée lorsque le secteur est armé et activée lorsque le secteur est désarmé.
- **Message Affichage non prêt** : Lorsque cette option est activée, le clavier EliteSuite des messages lorsqu'il y a des entrées ouvertes. Les messages « Zone ouverte » s'affichent sur l'écran d'accueil et lorsque l'utilisateur tente d'armer la partition.
- **Format de temps 24hres** : Lorsque cette option est activée, le clavier affiche l'heure au format 24 heures. Lorsque cette option est désactivée, le clavier affiche l'heure au format 12 heures.
- **Armement rapide permis** : Lorsque cette option est activée, un utilisateur peut armer la partition en maintenant la touche **[ARM]** enfoncée pendant 2 secondes. Cela permet d'armer la partition sans entrer le NIP de l'utilisateur.

- **Armement de séjour rapide permis** : Lorsque cette option est activée, un utilisateur peut rester armé dans la partition en maintenant la touche **[STAY]** enfoncée pendant 2 secondes. Cela permet à la partition de rester armée sans avoir à entrer un NIP d'utilisateur.

  Lorsqu'une zone d'appartement est armée en permanence, les entrées dont l'option **L'entrée est une entrée permanente** est activée ne seront pas surveillées. Il s'agit du comportement opposé à l'option **Entrée permanente** dans **Programmation | Types d'entrée | Options (1)**.

- **Armement instantané rapide permis** : Lorsque cette option est activée, la partition peut être instantanément armée. Cela signifie que la partition reste armée mais que toutes les entrées qui devraient normalement déclencher le délai d'entrée déclenchent l'alarme immédiatement (c'est-à-dire que toutes les entrées sont traitées comme des entrées « instantanées »).

  Un utilisateur peut armer instantanément la partition en commençant le processus d'armement de séjour puis en maintenant la touche **[STAY]** enfoncée pendant 2 secondes alors que la partition est en délai de sortie. Le délai de sortie sera annulé et la partition sera immédiatement armée.

  Lorsqu'une zone d'appartement est armée en permanence, les entrées dont l'option **L'entrée est une entrée permanente** est activée ne seront pas surveillées. Il s'agit du comportement opposé à l'option **Entrée permanente** dans **Programmation | Types d'entrée | Options (1)**.

- **Armement de force rapide permis** : Lorsque cette option est activée, un utilisateur peut armer par force la partition en maintenant la touche **[FORCE]** enfoncée pendant 2 secondes. Cela permet d'armer la partition par force sans entrer le NIP de l'utilisateur.

  Seules les entrées dont l'option **Armement par force sur entrée autorisée** est activée dans l'onglet **Entrées** peuvent être armées par force.armé.

- **Rapport d'armement/désarmement** : Lorsque cette option est activée, le clavier EliteSuite informe le contrôleur lorsqu'il est armé ou désarmé. Les événements d'armement et de désarmement sont enregistrés dans le journal des événements et signalés à la station de surveillance. Cette option vous permet de visualiser l'état du secteur sur une page d'état ou un plan d'étage et d'envoyer des commandes manuelles d'armement/désarmement.
- **Rapport d'activation d'alarme** : Lorsque cette option est activée, le clavier EliteSuite informe le contrôleur lorsque l'alarme est activée, désactivée ou temporisée. Les événements d'alarme seront enregistrés dans le journal des événements et signalés à la station de surveillance. Cette option vous permet également de visualiser l'état d'alarme du secteur sur une page d'état ou un plan d'étage.
- **Contournement de l'entrée de rapport** : Lorsque cette option est activée, le clavier EliteSuite informe le contrôleur lorsque le secteur est armé avec une entrée contournée. Les événements de contournement sont enregistrés dans le journal des événements et signalés à la station de surveillance.

  L'état des entrées d'appartement ne peut pas être visualisé sur une page d'état ou un plan d'étage.

- **Signaler un sabotage d'entrée** : Lorsque cette option est activée, le clavier EliteSuite avertit le contrôleur lorsqu'une entrée connectée présente une condition de sabotage ou de court-circuit. Les événements de sabotage sont enregistrés dans le journal des événements et signalés à la station de surveillance.

  L'état des entrées d'appartement ne peut pas être visualisé sur une page d'état ou un plan d'étage.

- **Report de l'accès au menu maître** : Lorsque cette option est activée, le clavier EliteSuite notifie le contrôleur lorsque un utilisateur se connecte au clavier. Cet événement sera enregistré dans le journal des événements.
- Accès au menu de l'installateur **Rapport** : Lorsque cette option est activée, le clavier EliteSuite informe le contrôleur lorsque l'installateur (utilisateur 3) se connecte au menu local de l'installateur. Cet événement sera enregistré dans le journal des événements.
- **Rapport d'informations avancées** : Lorsque cette option est activée, le clavier EliteSuite notifie au contrôleur des informations étendues, telles que les conditions de sabotage de dispositif et de panne d'entrée d'incendie. Ces événements seront enregistrés dans le journal des événements et signalés à la station de surveillance.
- **Les clés 1+3 génèrent une alarme de panique** : Lorsque cette option est activée, le clavier EliteSuite génère une alarme de panique lorsque les touches **[1]** et **[3]** sont maintenues ensemble pendant 2 secondes. Cela active l'alarme de la partition et envoie un événement au JournalÉvénement et à la station de surveillance.

- **Les touches 4+6 génèrent une alarme médicale** : Lorsque cette option est activée, le clavier EliteSuite génère une alarme de panique médicale lorsque les touches **[4]** et **[6]** sont maintenues ensemble pendant 2 secondes. Cela active l'alarme de la partition et envoie un événement au JournalÉvénement et à la station de surveillance.
- **Les clés 7+9 génèrent une alarme incendie.** : Lorsque cette option est activée, le clavier EliteSuite génère une alarme incendie lorsque les touches **[7]** et **[9]** sont maintenues ensemble pendant 2 secondes. Cela active l'alarme et le signal sonore du clavier. Le clavier envoie un événement au JournalÉvénement et à la station de surveillance.
- **Le huitième utilisateur est un utilisateur sous contrainte** : Lorsque cette option est activée, le huitième utilisateur associé à l'appartement (voir l'onglet **Utilisateurs**) est un utilisateur sous contrainte. Lorsque le code PIN de cet utilisateur est saisi sur un clavier ou un lecteur, il peut désarmer les zones et accéder aux menus normalement sans activer l'alarme, mais un événement de contrainte sera envoyé au journal des événements et à la station de surveillance.

Appartements | Claviers

Les claviers ajoutés ici peuvent être visualisés, mais pas modifiés, sous **Modules d'expansions | Claviers**.

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Adresse du clavier** : L'index (adresse réseau) du clavier sur le réseau du contrôleur. Ce paramètre doit être réglé sur une valeur unique pour que l'enregistrement de l'appartement puisse être sauvegardé.

  Les adresses valides sont de 1 à 248. Cette fonction permet d'ajouter un maximum de 248 claviers EliteSuite à un seul contrôleur.

Commandes

- Ce champ est utilisé pour envoyer des commandes de programmation à l'appareil. Il ne doit être utilisé que lorsqu'il est spécifiquement conseillé par la documentation ICT ou le support technique.

Configuration

- **Partition à laquelle cet ACL appartient** : Ce champ indique la partition associée au clavier EliteSuite (lecture seule). La partition peut être configurée dans l'onglet **Partitions**.
- **PGM de réinitialisation de fumée** : Si le **PGM de réinitialisation de fumée** est activée (onglet **Options**), ce champ indique que la sortie 1 du clavier EliteSuite sera activée lorsqu'un utilisateur réinitialise le détecteur de fumée à partir du clavier.

Appartements | Entrées

Les seize entrées qui peuvent être associées à un EliteSuite clavier sont automatiquement créées ici. Seules les entrées 1 à 4 sont configurables dans Protege GX : Les entrées restantes appartiennent à n'importe quel clavier esclave connecté. Si les quatre entrées sont physiquement utilisées, assurez-vous que l'option **Mode d'entrée duplex** est activée dans l'onglet **Options**.

Pour plus d'informations sur la configuration des claviers esclaves, consultez le manuel relatif à EliteSuite l'installation du clavier.

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Nom d'affichage du clavier** : Le nom qui sera téléchargé vers le contrôleur. Ce dernier sera affiché sur le clavier et dans les rapports des services de surveillance IP. Le clavier ne peut afficher que les 16 premiers caractères du nom. Il doit donc décrire de manière concise l'emplacement physique et la fonction de l'appareil.

Adresse

- **Type de module** : Indique que l'entrée est connectée à un clavier (lecture seule).
- **Entrée d'adresse du module** : Indique l'adresse **du clavier** du clavier auquel cette entrée est connectée (lecture seule).
- **Module entrée** : Indique l'index de l'entrée sur le clavier (lecture seule).

Configuration

- **Sortie de contrôle / Groupe de sorties programmables** : Cette option n'est pas prise en charge pour les appartements.
- **Automatisation de contrôle** : Cette option n'est pas prise en charge pour les appartements.
- **Support des commandes manuelles** : Cette option n'est pas prise en charge pour les appartements.
- **Signaler ID** : L'ID de rapport de l'entrée est le numéro de zone qui représentera cette entrée auprès de la station de surveillance. Ce champ est en lecture seule pour les entrées d'appartement.
- **Vitesse d'entrée d'alarme** : Cette option n'est pas prise en charge pour les appartements.
- **Restauration de la vitesse de l'entrée** : Cette option n'est pas prise en charge pour les appartements.
- **Activer lock-out de zone** : Cette option n'est pas prise en charge pour les appartements.
- **Compte de lock-out de zone** : Cette option n'est pas prise en charge pour les appartements.

Commandes

- Ce champ est utilisé pour envoyer des commandes de programmation à l'appareil. Il ne doit être utilisé que lorsqu'il est spécifiquement conseillé par la documentation ICT ou le support technique.

Graphiques

- **Caméra** : L'association d'une caméra à une entrée vous permet de faire un clic droit sur n'importe quel événement de entrée dans une fenêtre d'événement pour ouvrir un flux de caméra archivé à l'heure de l'événement.
- **Plan d'étage** : L'association d'un plan d'étage à une entrée vous permet de faire un clic droit sur n'importe quelle entrée dans une fenêtre d'événement pour ouvrir le plan d'étage.

Types de partitions et d'entrées

Première partition attribuée

- **Partition** : La partition qui surveille cette entrée, c'est-à-dire la partition associée à l'appartement (lecture seule).
- **Type d'entrée** : Le type d'entrée définit comment l'entrée fonctionnera dans cette partition particulière. Les types d'entrées disponibles pour les entrées appartement sont les suivants : Délai, Suivre délai, Instantané, Alarme 24 heures, Incendie et Délai d'incendie.

Options générales

- **Contournement d'entrée activé** : Lorsque cette option est activée, l'entrée peut être contournée à partir du clavier EliteSuite pour armer la partition de l'appartement. Cela signifie que la partition peut être armée même si cette entrée est ouverte ou altérée, mais l'entrée ne sera pas surveillée et ne fera pas passer la partition en mode alarme.
- **L'entrée est une entrée permanente** : Si cette option est activée, cette entrée ne sera pas surveillée lorsque la partition reste armée. Avec cette option désactivée, cette entrée sera surveillée lorsque la partition reste armée.

  Pour surveiller le périmètre de l'appartement lorsqu'il y a des personnes à l'intérieur, vous pouvez activer cette option pour toutes les entrées internes telles que les IRP, et la désactiver pour les entrées externes telles que les contacts de porte et de fenêtre.

  Cette option a le comportement opposé à l'option **Entrée de séjour** dans **Programmation | Types d'entrée | Options(1)**.
- **Armement par force sur l'entrée permis** : Lorsque cette option est activée, la partition peut être armée par force quand cette entrée est ouverte sans contournement. L'entrée est surveillée et peut encore générer des alarmes si elle est fermée et ouverte à nouveau.

Appartements | Partitions

Chaque appartement a une partition associée, qui peut être armée et désarmée à partir du EliteSuite clavier ou du Protege GX.

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Nom d'affichage du clavier** : Le nom qui sera téléchargé vers le contrôleur. Ce dernier sera affiché sur le clavier et dans les rapports des services de surveillance IP. Le clavier ne peut afficher que les 16 premiers caractères du nom. Il doit donc décrire de manière concise l'emplacement physique et la fonction de l'appareil.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

Graphiques

- **Caméra** : L'association d'une caméra à une partition vous permet de faire un clic droit sur n'importe quel événement de partition dans une fenêtre d'événement pour ouvrir un flux de caméra archivé à l'heure de l'événement.
- **Plan d'étage** : L'association d'un plan d'étage à une partition vous permet de faire un clic droit sur n'importe quelle partition dans une fenêtre d'événement pour ouvrir le plan d'étage.

Configuration

Configuration

- **Partition enfant** : Cette option n'est pas prise en charge pour les appartements.
- **Nombre maximal d'entrées de contournement** :} Cette option n'est pas prise en charge pour les appartements.
- **Nombre maximum d'utilisateurs** :} Cette option n'est pas prise en charge pour les appartements.

- **Code Client** : Ce code représente la partition dans les rapports adressés à la station de surveillance centrale. Il s'agit généralement d'un nombre hexadécimal, mais le format peut dépendre de la compatibilité du récepteur. Si le code client de la partition est laissé à la valeur par défaut (FFFF), la partition utilisera le **Code client** réglé dans signalisation du SERVICE (**Programmation | Services | Général**).

  En général, les appartements doivent avoir des codes de rapport uniques car les locataires peuvent contracter des services de sécurité individuellement.
- **Interverrouiller groupe de partitions** : Cette option n'est pas prise en charge pour les appartements.
- **Compte des entrées intelligentes** : Cette option n'est pas prise en charge pour les appartements.
- **Signaler ID** : L'ID de rapport de la partition est le numéro de groupe qui représentera cette partition spécifique à la station de surveillance. Dans ce cas, il n'y a qu'une seule zone par appartement, donc l'ID de rapport est fixé à 1 (lecture seule).
- **Groupe de portes verrouillées à l'armement** :} Cette option n'est pas prise en charge pour les appartements.

Services de rapports

Ce champ vous permet d'assigner les services de rapports qui enverront des rapports pour cette zone et toutes les entrées ou entrées de dérangement qui y sont programmées.

Les services peuvent être programmés dans **Programmation | Services**.

Appartements | Utilisateurs

Chaque appartement peut gérer 8 utilisateurs. Ceux-ci sont automatiquement remplis lorsque l'appartement est créé. Par défaut, l'utilisateur 1 est considéré comme l'"utilisateur maître" et l'utilisateur 3 comme l'"utilisateur installateur".

Les utilisateurs des appartements peuvent armer et désarmer la partition de l'appartement et accéder aux lecteurs de cartes connectés, et peuvent également avoir accès à d'autres parties du Protege GX système (par exemple, les portes qui desservent l'ensemble du complexe).

Les utilisateurs d'appartement ne sont pas visibles dans la page standard **Utilisateurs | Utilisateurs** de Protege GX. Cependant, ils sont inclus dans la page des utilisateurs du client Web. Ces enregistrements ne doivent **pas** être modifiés dans le client Web, car les options pour les utilisateurs d'appartement ne sont pas les mêmes que celles des utilisateurs ordinaires.

Général

- **Prénom** : Le prénom de l'utilisateur.
- **Nom de famille** : Le nom de famille de l'utilisateur.
- **Nom** : Le nom d'affichage de l'utilisateur tel qu'il apparaît sur les claviers et dans le logiciel. Ce nom n'apparaîtra pas sur le clavier EliteSuite.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.
- **Langue par défaut** : Définit la langue qui sera utilisée lorsque l'utilisateur se connectera à un clavier. Il peut s'agir de n'importe quelle langue prise en charge et n'est pas limité par l'installation Protege GX.

  Seul l'anglais est pris en charge sur les claviers EliteSuite. Cette option s'applique aux autres claviers du système Protege GX.

Numéros de cartes

- **NIP** : Le NIP d'un utilisateur est utilisé pour se connecter aux claviers et accéder aux portes (via des lecteurs de cartes avec des claviers NIP). Ce code PIN peut être utilisé à la fois dans le réseau EliteSuite et dans le reste du système Protege GX.

Le nombre maximum de chiffres pour ce PIN est de 4. Cliquez sur le bouton **[4]** pour générer automatiquement un nouveau code PIN de cette longueur. Les améliorations de la sécurité du site (par exemple, les règles de complexité du PIN dans **Global | Sites | Valeurs par défaut du site**) ne s'appliquent pas aux utilisateurs d'appartement.

- **Numéro d'établissement/de carte** : Chaque utilisateur d'un appartement peut se voir attribuer une information d'identification, composée d'un numéro d'établissement (ou numéro de site) et d'un numéro de carte individuel. Cela peut être utilisé à la fois dans le réseau EliteSuite et dans le reste du système Protege GX.

  Une seule information d'identification peut être attribuée à chaque utilisateur d'appartement.

  Note : La base de données Protege GX ne peut pas stocker les numéros d'installation ou de carte d'utilisateur de 2147483648 ou plus. Les événements faisant référence à ces cartes n'afficheront aucune donnée. Il s'agit d'une limitation connue.

Configuration

- **Signaler ID** : Le code qui sera utilisé pour identifier cet utilisateur dans les rapports destinés aux stations de surveillance. L'ID de contact, le SIA et l'IP de rapport utilisent ce code. Ce champ est en lecture seule pour les utilisateurs d'appartements.

Options générales

- **Le code peut armer le système uniquement** : Lorsque cette option est activée, cet utilisateur peut armer la partition de l'appartement mais ne peut pas la désarmer. Cela peut être utilisé pour les entrepreneurs ou les nettoyeurs afin qu'ils ne puissent pas entrer sans la présence d'un résident mais qu'ils puissent sécuriser l'appartement lorsqu'ils partent.
- **L'utilisateur peut modifier d'autres utilisateurs** : Lorsque cette option est activée, cet utilisateur peut accéder au menu **Configuration utilisateur** sur le clavier EliteSuite (en appuyant sur **[MENU] [5]**). Ceci lui permet de modifier les codes PIN des utilisateurs, les numéros de carte et d'autres options.

  Lorsqu'un opérateur effectue une mise à jour du module sur le clavier EliteSuite, tous les enregistrements modifiés localement sont écrasés. Cela permet de réinitialiser les enregistrements si les locataires de l'appartement changent.

  Cette option est activée par défaut pour l'utilisateur principal (utilisateur 1).
- **Désarmement sur badge unique activé** : Lorsque cette option est activée, l'utilisateur peut désarmer la partition de l'appartement en badgeant sa carte une fois au lecteur d'entrée.

  Cette option s'applique uniquement aux lecteurs connectés au réseau esclave du clavier EliteSuite.
- **Armement sur 3 Badges activé** : Avec cette option activée, l'utilisateur peut armer la partition de l'appartement en badgeant sa carte trois fois de suite à un lecteur.

  Cette option s'applique uniquement aux lecteurs connectés au réseau esclave du clavier EliteSuite.
- **3 badges verrouillage - porte à bascule** : Avec cette option activée, l'utilisateur peut faire basculer une porte entre verrouillée et déverrouillée en badgeant sa carte trois fois de suite dans le lecteur.

  Cette option s'applique uniquement aux lecteurs connectés au réseau esclave du clavier EliteSuite.
- **3 badges verrouillent la porte 2 heures** : Avec cette option activée, l'utilisateur peut déverrouiller une porte pendant deux heures en badgeant sa carte trois fois de suite dans le lecteur. Pendant que la porte est déverrouillée, ils peuvent badger leur carte trois fois pour verrouiller la porte.

  Cette option s'applique uniquement aux lecteurs connectés au réseau esclave du clavier EliteSuite.
- **3 badges verrouillent la porte 4 heures** : Avec cette option activée, l'utilisateur peut déverrouiller une porte pendant quatre heures en badgeant sa carte trois fois de suite dans le lecteur. Pendant que la porte est déverrouillée, ils peuvent badger leur carte trois fois pour verrouiller la porte.

  Cette option s'applique uniquement aux lecteurs connectés au réseau esclave du clavier EliteSuite.

- **3 badges verrouillent la porte 8 heures** : Avec cette option activée, l'utilisateur peut déverrouiller une porte pendant huit heures en badgeant sa carte trois fois de suite dans le lecteur. Pendant que la porte est déverrouillée, ils peuvent badger leur carte trois fois pour verrouiller la porte.

  Cette option s'applique uniquement aux lecteurs connectés au réseau esclave du clavier EliteSuite.

Niveaux d'accès

Tous les utilisateurs associés à un appartement peuvent armer et désarmer la partition de l'appartement et accéder à toutes les portes connectées à tout moment ; cependant, vous pouvez également attribuer des niveaux d'accès ici pour accorder à l'utilisateur l'accès à d'autres parties du Protege GX système. Par exemple, en plus de leur propre appartement, les utilisateurs peuvent avoir besoin d'accéder à des espaces partagés tels que des entrées, des parkings et des salles de sport.

Cliquer **Ajouter** pour ajouter un nouveau niveau d'accès.

- **Nom** : Le nom du niveau d'accès attribué à l'utilisateur.
- **Niveau d'accès expire** : Lorsque cette option est activée, le niveau d'accès expire en fonction des dates de début et de fin définies. L'utilisateur ne pourra utiliser ce niveau d'accès qu'entre les dates de début et de fin d'expiration.

  Plusieurs copies du même niveau d'accès peuvent être attribuées à un seul utilisateur avec des heures d'expiration différentes, ce qui permet un accès périodique. Par exemple, un technicien peut ne pouvoir accéder au bâtiment que quelques jours par mois.
- **Début d'expiration**: Ce niveau d'accès ne sera pas valable pour l'utilisateur avant cette date et cette heure.
- **Fin d'expiration** : Ce niveau d'accès ne sera pas valable pour l'utilisateur après cette date et cette heure.
- **Horaire** : Ce calendrier détermine quand les permissions fournies par le niveau d'accès sont valides pour cet utilisateur. Il est combiné à tous les horaires définis dans le niveau d'accès lui-même, ainsi que dans les groupes de portes ou d'étages.

  L'utilisateur n'a accès que si tous les horaires pertinents sont valides.

Commandes manuelles d'appartement

Un clic droit sur un enregistrement d'appartement dans **Programmation | Appartements** ouvre un menu vous permettant d'envoyer un message au clavier. Cela permet aux gestionnaires d'immeubles d'envoyer des messages aux locataires de chaque appartement.

Les utilisateurs peuvent lire les messages en appuyant sur **[MENU]** la touche, en se connectant avec leur NIP et en appuyant sur **[2]** . Ils peuvent supprimer chaque message en appuyant sur la **[FORCE]** touche .

Ajouter des appartements par lots

La fonction d'ajout d'appartements par lot vous permet de créer un certain nombre d'appartements qui seront affectés à un contrôleur.

Ajouter des appartements en tant que lot

1. Naviguez vers **Programmation | Ajout d'appartements par lot**.
2. Définissez le nombre d'appartements (entre 5 et 248).
3. Entrez un préfixe **Nom** qui sera utilisé par tous les nouveaux appartements. Des numéros séquentiels seront ajoutés après le préfixe (par exemple, Appartement 1, Appartement 2, etc.).
4. Entrez l'adresse **Début du clavier**, qui définit l'adresse **Du clavier** du premier appartement. Les adresses suivantes seront attribuées de manière séquentielle.

   Lorsque des appartements sont ajoutés par lots, la première **adresse clavier** est supérieure d'une unité à la **adresse clavier** sélectionnée. Il s'agit d'un problème connu.
5. Sélectionnez le **Contrôleur** auquel les appartements seront affectés.
6. Cliquez sur **OK**.
7. Modifiez les détails de chaque appartement si nécessaire.

Menu Groupes

Le regroupement de dispositifs tels que des portes, des partitions et des sorties constitue un moyen pratique d'affecter plusieurs éléments à des niveaux d'accès et de contrôler plusieurs dispositifs avec une seule fonction. Par exemple, vous pouvez créer un groupe de sortie contenant plusieurs bips et LEDs qui peuvent être utilisés pour avertir les utilisateurs lorsqu'une partition est sur le point d'être armée.

En outre, les groupes de menus vous permettent de déterminer les menus auxquels chaque utilisateur peut accéder sur chaque clavier.

Groupes de portes

Lorsqu'ils sont assignés à un niveau d'accès, les groupes de portes sont utilisés pour définir les portes auxquelles un utilisateur peut accéder et/ou contrôler. Ils peuvent également être utilisés avec les fonctions **Interverrouiller Groupe de portes** (**Programmation | Portes | Général**) et **Verrouiller groupe de portes sur armement** (**Programmation | Partitions | Configuration**), ainsi que dans les fonctions programmables de la contrôle de portes.

Groupes de portes | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

Date/heure d'expiration du groupe de portes

L'expiration du groupe de portes vous permet d'activer/désactiver le groupe de portes pour tous les niveaux d'accès des utilisateurs à une date et une heure particulières. Par exemple, vous pouvez utiliser cette fonction pour préprogrammer une section du bâtiment en construction et la rendre accessible à tout le personnel le jour de son ouverture.

- **Commencer** : Avec cette option activée, le groupe de portes ne sera pas accessible avant la date et l'heure spécifiées.
- **Fin** : Si cette option est activée, le groupe de portes ne sera pas accessible après la date et l'heure spécifiées.

Portes

Cliquez sur **Ajouter** pour assigner des portes au groupe. Vous pouvez faire glisser et déposer des registres individuels dans le champ, ou sélectionner plusieurs registres à l'aide des touches Maj + Clic. Ensuite, cliquez sur **OK**.

- **Horaire** : Le programme détermine quand la porte est un membre valide de ce groupe de portes. Lorsque l'horaire est valide, la porte est incluse dans le groupe. Lorsque l'horaire n'est pas valide, la porte n'est pas incluse dans le groupe.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Groupes de partitions

Les groupes de partition peuvent être affectés à des niveaux d'accès pour définir les partitions qu'un utilisateur est autorisé à armer et à désarmer. Ils peuvent être affectés soit à des groupes de partition d'armement (armement uniquement autorisé), soit à des groupes de partition de désarmement (armement et désarmement autorisés). Les groupes de partition sont également attribués à des claviers (**Modules d'expansion | Claviers | Configuration**), utilisés avec la fonction de **groupe de partition de verrouillage** (**Programmation | Partitions | Configuration**) et utilisés dans les fonctions programmables de contrôle de partition.

Groupes de partition | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

Partitions

Cliquer sur **Ajouter** pour assigner des partitions au groupe. Vous pouvez faire glisser et déposer des registres individuels dans le champ, ou sélectionner plusieurs registres à l'aide des touches Maj + Clic. Ensuite, cliquez sur **OK**.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Groupes de claviers

Les groupes de claviers peuvent être attribués à des groupes de menus afin de déterminer les claviers auxquels les utilisateurs ont accès. Ils peuvent également être utilisés avec la fonctionnalité **Groupe de claviers différer avertissement** dans **Programmation | Partitions | Configuration**.

Groupes de claviers | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

Claviers

Cliquer sur **Ajouter** pour attribuer des claviers au groupe. Vous pouvez faire glisser et déposer des registres individuels dans le champ, ou sélectionner plusieurs registres à l'aide des touches Maj + Clic. Ensuite, cliquez sur **OK**.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Groupes de menus

Lorsqu'ils sont attribués à un niveau d'accès, les groupes de menus définissent les menus de claviers et les autres fonctions auxquels un utilisateur a accès. Des groupes de menus peuvent également être attribués à des claviers spécifiques (**Modules d'expansion | Claviers | Configuration**) pour limiter davantage les menus accessibles. Si l'accès à un menu est refusé soit par le niveau d'accès, soit par la programmation du clavier, l'utilisateur ne pourra pas accéder à ce menu à partir de ce clavier.

Groupes de menus | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Horaire d'opération** : L'horaire d'opération détermine quand ce groupe de menus particulier est actif dans un niveau d'accès. Lorsque le programme est valide, les paramètres de ce groupe de menus seront utilisés. Lorsque le programme n'est pas valide, les paramètres du **Groupe de menus secondaire** ci-dessous sont utilisés.
- **Groupe de menus secondaire** : Lorsque le **Horaire d'opération** ci-dessus est invalide, le groupe de menus secondaire sera utilisé par les niveaux d'accès.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

Paramètres

- **Partition (1)** : Lorsque cette option est activée, les utilisateurs peuvent accéder au menu de la partition en appuyant **[MENU] [1]** sur le clavier. Ce menu permet aux utilisateurs d'armer et de désarmer des partitions.
- **Utilisateur (2)** : Lorsque cette option est activée, les utilisateurs peuvent accéder au menu utilisateur en appuyant sur **[MENU] [2]** sur le clavier. Ce menu permet aux utilisateurs de modifier leur propre code PIN.
- **Événements (3)** : Lorsque cette option est activée, les utilisateurs peuvent accéder au menu des événements en appuyant **[MENU] [3]** sur le clavier. Ce menu permet aux utilisateurs de voir les événements sauvegardés sur le contrôleur.
- **Installateur (4)** : Lorsque cette option est activée, les utilisateurs peuvent accéder au menu installateur en appuyant **[MENU] [4]** sur le clavier. Ce menu permet aux utilisateurs de voir et de contrôler l'état des appareils dans le système et de changer l'adresse IP du contrôleur.
- **Voir (5)** : Lorsque cette option est activée, les utilisateurs peuvent accéder au menu de visualisation en appuyant sur **[MENU] [5]** sur le clavier. Ce menu permet aux utilisateurs de visualiser et de contrôler la mémoire d'alarme, les problèmes du système et certains états des dispositifs.
- **Heure (6)** : Il s'agit d'une option héritée qui n'a aucun effet.
- **Contourner (7)** : Lorsque cette option est activée, les utilisateurs peuvent accéder au menu de contournement en appuyant **[MENU] [7]** sur le clavier. Ce menu permet aux utilisateurs de contourner les entrées.
- **Système (8)** : Il s'agit d'une option héritée qui n'a aucun effet.
- **Installateur avancé (4, 8)** : Il s'agit d'une option héritée qui n'a aucun effet.
- **Menus de temps prolongé (6, 2-4)** : Il s'agit d'une option héritée qui n'a aucun effet.

- **Contourner entrée trouble (7, 2)** : Lorsque cette option est activée, les utilisateurs peuvent accéder au menu de contournement de la zone trouble en appuyant **[MENU] [7][2]**sur le clavier. Ce menu permet aux utilisateurs de contourner les entrées trouble.

  Il est possible de contourner les entrées trouble à partir du clavier, mais le contournement ne peut être enlevé qu'en mettant le contrôleur sous tension. Par conséquent, il est recommandé de désactiver le contournement pour les entrées trouble.

- **Contrôle groupe de partitions permis** : Lorsque cette option est activée, les utilisateurs peuvent appuyer sur la touche fléchée **[RIGHT]** du menu de partition pour armer/désarmer le groupe de partitions du clavier.

  Le clavier doit avoir un **Groupe de partitions pour ce clavier** configuré (**Modules d'expansions | Claviers | Configuration**) et l'option **Permettre l'accès du groupe de partitions** activée (**Modules d'expansions | Claviers | Options 1**).

- **Contrôle de zone de fraude autorisé** : Lorsque cette option est activée, les utilisateurs peuvent appuyer sur la touche fléchée **[LEFT]** dans le menu des zones pour armer/désarmer la partie 24 heures de chaque zone.

  Le clavier doit également avoir **Permettre accès 24 heures de la partition** activé (**Modules d'expansions | Claviers | Options 1**).

- **Armement prolongé** : Lorsque cette option est activée, les utilisateurs peuvent armer des zones en appuyant sur la touche **[STAY]**. L'armement permanent du ou des secteurs doit être activé dans **Programmation | Secteurs | Options 2**.
- **Armement de force** : Lorsque cette option est activée, les utilisateurs peuvent armer des partitions par force en appuyant sur la touche **[FORCE]**. L'armement par force de la ou des partitions doit être activé dans **Programmation | Partitions | Options 2**.
- **Armement instantané** : Lorsque cette option est activée, les utilisateurs peuvent armer instantanément des partitions en maintenant la clé **[STAY]** (armement de séjour instantané) ou la clé **[FORCE]** (armement de force instantané) pendant deux secondes. L'armement instantané de la ou des partitions doit être activé dans **Programmation | Partitions | Options 2**.

Groupes de claviers

Vous pouvez affecter des groupes de claviers à un groupe de menus pour restreindre les autorisations du menu à ces seuls claviers. Cela vous permet d'accorder aux utilisateurs des autorisations spécifiques sur différents claviers en affectant plusieurs groupes de menus à un seul niveau d'accès.

Si aucun groupe de claviers n'est attribué ici, le groupe de menu s'applique à tous les claviers de ce site.

Il est important qu'il n'y ait qu'un seul groupe de menus appliqué à chaque clavier auquel un utilisateur peut accéder. Si plusieurs groupes de menus sont disponibles pour un clavier, le contrôleur ne saura pas quelles autorisations devront être présentées à l'utilisateur. Cela peut entraîner un fonctionnement indéfini du système.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Groupes de menus | Options

- **Menu avancé de l'utilisateur** : Il s'agit d'une option héritée qui n'a aucun effet.
- **Groupe de menu installateur** : Cette option peut être activée pour les groupes de menus utilisés par les installateurs et les techniciens du site. Lorsqu'un utilisateur de ce groupe de menus se connecte au clavier, l'entrée trouble Installateur connecté est ouverte.

  En outre, les utilisateurs auxquels ce groupe de menus a été attribué peuvent rester connectés au clavier indéfiniment, indépendamment du réglage de **L'heure à laquelle l'utilisateur est connecté** dans **Modules d'expansions | Claviers | Configuration**. C'est pratique pour les installateurs qui assureront la mise en service et la maintenance du site.

- **Montrer le message d'accueil de l'utilisateur** : Activez cette option pour que le clavier affiche un message d'accueil personnel à l'utilisateur lorsqu'il se connecte. Par exemple, lorsque l'utilisateur John Smith se connecte au clavier à 9 heures du matin, celui-ci affiche le message 'Good Morning John Smith'. Cette option peut être désactivée pour réduire le temps de connexion à un clavier.

  Cette option est équivalente à l'option **Afficher un message d'accueil à l'utilisateur** dans **Utilisateurs | Utilisateurs | Options**. Le message d'accueil s'affiche si l'une ou l'autre des options est activée pour l'utilisateur.

- **L'utilisateur peut reconnaître la mémoire d'alarme** : Lorsque cette option est activée, les utilisateurs auxquels ce groupe de menus est attribué peuvent reconnaître les alarmes dans la mémoire d'alarme. Les utilisateurs peuvent accéder à la mémoire d'alarme en appuyant sur **[MENU] [5] [1]**. L'utilisateur doit également avoir accès au menu **Vue** (onglet **Général**).

  Lorsque cette option est désactivée, les utilisateurs peuvent visualiser les alarmes mais ne peuvent pas les acquitter.

  Cette option est équivalente à l'option **L'utilisateur peut reconnaître la mémoire d'alarme** dans **Utilisateurs | Utilisateurs | Options**. Les alarmes peuvent être acquittées si l'option l'une ou l'autre est activée pour l'utilisateur.

- **Montrer la mémoire d'alarme de l'utilisateur à l'ouverture de session** : Lorsque cette option est activée, le clavier affiche automatiquement la mémoire d'alarme de la zone principale du clavier à l'utilisateur lorsqu'il se connecte au clavier. L'utilisateur doit également avoir accès au menu **Vue** (onglet **Général**).

  Cette option est équivalente à l'option **Montrer la mémoire d'alarme à la connexion** dans **Utilisateurs | Utilisateurs | Options**. La mémoire d'alarme sera affichée si l'option l'une ou l'autre est activée pour l'utilisateur. La zone primaire du clavier peut être définie comme la **Partition à laquelle appartient cet écran LCD** (**Modules d'expansions | Claviers | Configuration**).

Groupes de sorties

Les groupes de sorties sont utilisés pour permettre à un certain nombre de sorties d'être contrôlées par une seule fonction. La plupart des caractéristiques qui contrôlent les sorties - telles que les fonctions de sortie de porte et de partition, le contrôle d'entrée et de type d'entrée, les sorties de niveau d'accès et les fonctions programmables - peuvent contrôler des groupes de sorties à la place.

Il existe une variété d'applications où il est avantageux d'utiliser un groupe de sorties au lieu d'une seule. Par exemple, les groupes de sorties peuvent améliorer l'accessibilité en incluant des signaux visuels et sonores dans les notifications et les alarmes; au lieu d'utiliser un seul bip de clavier pour les délais d'entrée et de sortie, vous pouvez créer un groupe de sortie contenant un certain nombre de bips et de DEL pour vous assurer que le signal peut être entendu et vu dans toute la pièce. Il existe également des applications d'automatisation, permettant à l'activation d'une seule entrée ou sortie de déclencher toute une série d'autres effets (programmation un à plusieurs).

Groupes de sorties | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.
- **Temps de sortie** : La durée (en secondes) pendant laquelle le groupe de sorties sera activé. Lorsque ce délai est écoulé, toutes les sorties du groupe sont désactivées. Si ce paramètre est réglé sur 0, les sorties resteront activées en permanence jusqu'à ce qu'elles soient désactivées.

  Le temps de sortie défini ici a priorité sur le **temps d'activation** défini dans les sorties individuelles.

Sorties

Cliquer sur **Ajouter** pour attribuer des sorties au groupe. Vous pouvez faire glisser et déposer des registres individuels dans le champ, ou sélectionner plusieurs registres à l'aide des touches Maj + Clic. Ensuite, cliquez sur **OK**.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Groupes d'ascenseurs

Lorsqu'ils sont assignés à un niveau d'accès, les groupes d'ascenseurs permettent de définir les cabines d'ascenseurs auxquelles un utilisateur a accès.

Assigner un groupe d'ascenseurs à un niveau d'accès n'accorde pas à l'utilisateur l'accès aux étages affectés à ces ascenseurs. Les groupes d'étages doivent être assignés au niveau d'accès séparément.

L'utilisation peut varier en fonction de l'intégration en cours de configuration. Pour plus de renseignements, consulter la note d'application spécifique à votre intégration d'ascenseur.

Groupes d'ascenseurs | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

Ascenseurs

Cliquez sur **Ajouter** pour assigner des cabines d'ascenseurs au groupe. Vous pouvez faire glisser et déposer des registres individuels dans le champ, ou sélectionner plusieurs registres à l'aide des touches Maj + Clic. Ensuite, cliquez sur **OK**.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Groupes d’étages

Lorsqu'ils sont assignés à un niveau d'accès, les groupes d'étages définissent les étages auxquels un utilisateur a accès.

Assigner un groupe d'étages à un niveau d'accès n’accorde pas à l'utilisateur l'accès aux cabines d'ascenseur qui desservent ces étages. Les groupes d'ascenseurs doivent être assignés au niveau d'accès séparément.

L'utilisation peut varier en fonction de l'intégration en cours de configuration. Pour plus de renseignements, consulter la note d’application d’ascenseur spécifique à votre intégration.

Groupes d’étages | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Groupe de registres** : Le groupe d'enregistrements auquel appartient cet élément. Cela permet d'organiser les enregistrements par catégories telles que le bâtiment, la branche ou la société. En utilisant des rôles et des niveaux de sécurité, vous pouvez restreindre l'accès des opérateurs afin qu'ils ne puissent voir ou contrôler que les enregistrements de groupes de registres spécifiques.

Étages

Cliquez sur **Ajouter** pour assigner des étages au groupe. Vous pouvez faire glisser et déposer des registres individuels dans le champ, ou sélectionner plusieurs registres à l'aide des touches Maj + Clic. Ensuite, cliquez sur **OK**.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Menu Modules d'expansions

Les modules d'expansions représentent les modules physiques connectés au Protegeréseau de modules. Cela comprend Protege les claviers et les modules d'expansions ainsi que les lecteurs intelligents (lecteurs tiers externes connectés au système).

Mises à jour du module

Lorsque vous mettez à jour la configuration d'un module d'expansion dans le logiciel, la nouvelle programmation n'est généralement pas appliquée immédiatement dans le module. Vous devez effectuer une mise à jour du module pour mettre à jour la configuration dans le module d'expansion lui-même. Cela s'applique à la plupart des modifications effectuées dans les menus de programmation des **Modules d'expansions** (à l'exception des lecteurs intelligents).

Si une mise à jour du module est nécessaire, le contrôleur génère un message d'état de santé indiquant le module qui doit être mis à jour. Pour mettre à jour un module d'expansion :

1. Modifiez la configuration comme exigé et cliquez sur **Sauvegarder**.
2. Attendez que la programmation soit téléchargée dans le contrôleur. Pour la télécharger immédiatement, naviguez vers **Sites | Contrôleurs**, faites un clic droit sur le contrôleur et cliquez sur **Forcer le téléchargement**.
3. Sur la page de programmation des **Modules d'expansions**, faites un clic droit sur le registre du module d'expansion et cliquez sur **MettreàjourModule**.
4. Le module va redémarrer, passant temporairement hors ligne. Lorsqu'il se connecte à nouveau, il utilise la nouvelle configuration. Le logiciel affiche la progression de la mise à jour du module.

Il est recommandé d'utiliser cette méthode pour mettre à jour les modules un par un, au lieu d'utiliser la commande **Mettre à jour les modules** sur le contrôleur, qui redémarre chaque module connecté au contrôleur (que la programmation ait été modifiée ou non).

Module Virtuel

Les modules virtuels sont des modules qui sont programmés et adressés dans le système, mais qui ne correspondent pas à des modules physiques. Ils agissent comme des emplacements logiques, ce qui vous permet de programmer des entrées et des sorties virtuelles à utiliser avec des fonctions programmables, la programmation de sortie suit l'entrée et d'autres fonctions avancées. Cela vous permet d'automatiser votre système sans utiliser de matériel supplémentaire.

Les modules virtuels présentent les caractéristiques suivantes :

- Les entrées et les sorties peuvent être assignées au module virtuel comme d'habitude. Ils agissent comme des supports de mémoire dans le contrôleur avec un état binaire. Les modules d'expansion analogiques virtuels peuvent également être utilisés pour télécharger des valeurs de données vers le contrôleur.
- Le processus de zone trouble est désactivé et le module n'affecte pas le statut de santé du contrôleur.
- Le module ne nécessite pas de mises à jour.
- Le module n'apparaît pas dans la fenêtre d'adressage du module du contrôleur.
- Les modules physiques et virtuels ne peuvent pas être programmés avec la même **adresse physique**. Si un module virtuel existe déjà, un module physique connecté au système ne pourra pas être mis en ligne et affichera un code d'erreur.

  Pour s'assurer que les modules physiques et virtuels ne se chevauchent pas, il est recommandé d'adresser les modules virtuels avec des numéros plus élevés que les modules d'expansions physiques.

pour programmer un module virtuel, ajoutez un nouveau module d'expansions avec les entrées et sorties requises, réglez **l'adresse physique** sur une valeur élevée (par exemple 32) et activez **l'option Module** virtuel.

Claviers

Les claviers sont la principale interface sur site du système Protege GX. Ils peuvent être utilisés pour armer et désarmer le système, visualiser la mémoire d'alarme, déverrouiller les portes, examiner l'état des appareils, les troubles et les événements du système, et configurer l'adresse IP du contrôleur.

Pour plus d'informations sur la programmation et le fonctionnement des claviers, consulter :

- Le manuel d'installation du clavier correspondant
- Note d'application 222 : Référence de menu du clavier Protege
- Note d'application 338 : Programmation claviers Protege

Claviers | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Adresse physique** : L'adresse réseau du module sur le réseau du contrôleur. Les modules d'extension connectés peuvent être adressés avec la fonction **Adressage de module** du contrôleur (clic droit sur l'enregistrement du contrôleur).

  Il est également possible d'adresser les claviers à l'aide du menu de configuration intégré (consulter le manuel d'installation correspondant).

  Le nombre maximum d'adresses physiques disponibles pour les modules de claviers est de 200.

Affichage

- **Défaut afficher ligne un/deux** : Le texte par défaut qui s'affiche sur le clavier lorsqu'aucun utilisateur n'est connecté. Ce texte personnalisé s'affiche lorsque l'option **Afficher un message personnalisé** est activée (onglet **Options 1**). Chaque ligne du clavier peut afficher jusqu'à 16 caractères, qui peuvent être des lettres, des chiffres ou des signes de ponctuation.

  Ces champs prennent également en charge les codes de format qui peuvent être utilisés pour afficher l'heure et la date sur le clavier dans différents formats. Consulter le tableau ci-dessous pour les codes de format disponibles :

  Si l'une des autres **options d'affichage** disponibles dans l'onglet **Options 1** est activée, elle remplacera ce texte.

Code de format	Texte affiché
&T	Heure au format 12 heures avec AM/PM en majuscules (par ex. 9:15AM).
&t	Heure au format 12 heures avec am/pm en minuscules (par ex. 9:15am).
&M	Heure au format 24 heures (militaire) avec un espace pour les heures à un chiffre (par ex. 9:15, 21:15).
&m	Heure au format 24 heures (militaire) avec un zéro devant pour les heures à un chiffre (par ex.09:15, 21:15).
&G	Heure au format 12 heures sans symbole am/pm (par ex. 9:15).

Code de format	Texte affiché
&A	Symbole AM/PM en majuscules (par ex. AM).
&a	Symbole AM/PM en minuscules (par ex. am).
&D	Jour du mois avec un espace pour les jours à un chiffre (par ex. 3, 27).
&R	Jour de la semaine en format abrégé de trois caractères (par ex. lun, ven).
&V	Nom du mois en format abrégé de trois caractères (par ex. Mar, Nov).
&v	Numéro du mois avec un espace pour les mois à un seul chiffre (par ex. 3, 11).
&s	Numéro du mois avec un zéro en tête pour les mois à un seul chiffre (par ex. 03, 11).
&Y	Année au format à deux chiffres, c'est-à-dire les deux derniers chiffres de l'année (par ex. 21).
&C	Siècle, c'est-à-dire les deux premiers chiffres de l'année (par ex. 20).

Souvent, le texte affiché d'un code de format utilise plus de caractères que le code lui-même. S'assurer qu'il y a suffisamment d'espace autour de chaque code de format pour qu'il s'affiche en entier sans être recouvert par d'autres textes.

Commandes

- Ce champ est utilisé pour envoyer des commandes de programmation à l'appareil. Il ne doit être utilisé que lorsqu'il est spécifiquement conseillé par la documentation ICT ou le support technique.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Claviers | Configuration

Configuration

- **Partition à laquelle cet ACL appartient** : La partition primaire de ce clavier est généralement la partition dans laquelle le clavier est physiquement situé. Le clavier affichera par défaut la partition primaire dans les menus de partition et de mémoire d'alarme.

  S'assurer que la partition primaire est incluse dans le **Groupe de partitions pour ce clavier** (ci-dessous).

- **Temps libre double** : Il s'agit d'une option héritée qui n'a aucun effet.
- **Maximum d'entrées NIP non valides** : Lorsque l'option **Verrouiller clavier sur tentatives excédentaires** est activée (onglet **Options 1**), ce champ définit le numéro maximum de tentatives de saisie de code NIP non valide que le clavier acceptera. Par exemple, si c'est réglé sur 3, après trois saisies incorrectes du NIP, le clavier empêche toute nouvelle tentative.
- **Temps de verrouillage du clavier** : Lorsque l'option **Verrouiller clavier sur tentatives excédentaires** est activée (onglet **Options 1**), ce champ définit la durée (en secondes) pendant laquelle le clavier se verrouillera après plusieurs tentatives de saisie de code NIP non valide. Pendant cette période, le clavier affiche le message « Clavier verrouillé » et ignore toute entrée utilisateur.
- **Porte connectée au clavier** : Placer une porte dans ce champ permet aux utilisateurs de la déverrouiller à partir du clavier à l'aide de la touche **[FUNCTION]** (en maintenant la touche **[MENU]** pendant 2 secondes sur le PRT-KLCS). Vous devez également activer **Touche de fonction déverrouille la porte lorsque connecté (REX)** ou **Touche de fonction déverrouille la porte lorsque déconnecté (REX)** dans l'onglet **Options 1**.
- **Groupe de menus pour ce clavier** : Définit les menus qui sont accessibles à partir de ce clavier. Pour qu'un utilisateur puisse accéder à un menu, celui-ci doit être autorisé à la fois par le clavier et par le niveau d'accès de l'utilisateur.

Si ce champ n'est <pas défini>, tous les menus seront accessibles à partir de ce clavier.

- **Groupe de partitions pour ce clavier** : Définit les partitions qui peuvent être visualisées et contrôlées à partir de ce clavier. Pour qu'un utilisateur puisse visualiser et contrôler une partition, celle-ci doit être autorisée à la fois par le clavier et par le niveau d'accès de l'utilisateur.

  En outre, le groupe de partitions défini ici peut être armé/désarmé ensemble à partir de ce clavier en appuyant sur la touche **[RIGHT]** du menu de partitions. **Permettre l'accès de sélection du groupe de partitions** doit être activé dans l'onglet **Options 1**, et **Contrôle groupe de partitions permis** doit être activé dans le groupe de menus de l'utilisateur.

  Si ce champ n'est pas défini toutes les partitions associées au contrôleur seront accessibles à partir de ce clavier, mais l'armement et le désarmement des groupes de partitions ne seront pas disponibles.
- **PGM de réinitialisation de fumée / groupe de sorties** : Cette sortie ou ce groupe de sorties est activé lorsqu'un utilisateur maintient les touches **[CLEAR]** et **[ENTER]** du clavier pendant 2 secondes. Ceci peut être utilisé pour activer un relais qui réinitialise le détecteur de fumée.

  Note : La sortie ou le groupe de sorties n'est pas désactivé automatiquement.
- **Durée de connexion de l'utilisateur** : Le temps (en secondes) pendant lequel un utilisateur peut être connecté au clavier sans appuyer sur aucune touche. Par exemple, si ce paramètre est réglé sur 20 secondes, après 20 secondes d'absence d'entrée, le clavier déconnecte automatiquement l'utilisateur.

  Ceci ne doit pas être réglé sur Ne jamais déconnecter, sauf à des fins de démonstration et de test. Les utilisateurs dont l'option **Groupe de menu installateur** est activée (**Groupes | Groupes de menus | Options**) peuvent rester connectés au clavier indéfiniment.

Claviers | Options 1

Options d'affichage

- **Afficher message personnalisé (lignes 1 et 2)** : Lorsque cette option est activée, si aucun utilisateur n'est connecté au clavier, affiche le texte défini dans **Défaut afficher ligne un/deux** (onglet **Général**).

  Cette option peut être remplacée par les options alternatives ci-dessous.
- **Afficher statut de partition primaire** : Avec cette option activée, si aucun utilisateur n'est connecté au clavier, affiche le statut de la partition primaire. La partition primaire est définie comme la partition **à laquelle appartient cet écran ACL** (onglet **Configuration**).
- **Afficher groupe de partitions défilant** : Avec cette option activée, lorsqu'aucun utilisateur n'est connecté, le clavier affichera les partitions comprises dans le **groupe de partitions de ce clavier** (onglet **Configuration**). Les utilisateurs peuvent faire défiler les partitions à l'aide des touches **[UP]** et **[DOWN]**.
- **Afficher message trouble** : Avec cette option activée, le clavier émet un bip et affiche le message « Trouble fault check system » en cas de problème de système.
- **Afficher message de contournement** : Lorsque cette option est activée, lorsqu'une partition a été armée avec une ou plusieurs entrées contournées, le clavier émet un bip et affiche le message « Le système a contourné une ou plusieurs entrées ».

  Ce message s'affiche uniquement lorsque la partition est armée.
- **Afficher message d'alarme** : Lorsque cette option est activée, chaque fois qu'une alarme est présente dans la mémoire d'alarme du clavier, ce dernier émet un signal sonore et affiche le message « Le système a une alarme en mémoire ».
- **Afficher messages de partition primaire seulement** : Lorsque cette option est activée, le clavier n'affiche que les messages relatifs à la partition primaire lorsqu'aucun utilisateur n'est connecté. Ceci s'applique aux options **Afficher message de contournement** et **Afficher message d'alarme**.

  Lorsque cette option est désactivée, des messages s'affichent pour toute partition incluse dans le groupe **Groupe de partitions pour ce clavier** (onglet **Configuration**).

  La partition primaire est définie comme la partition **à laquelle appartient cet écran ACL** (onglet **Configuration**).

- **Afficher messages d'avertissement de partition différée** : Avec cette option activée, lorsqu'une partition commence un cycle d'armement de porte en attente du mode Carte, le clavier émet un signal sonore et affiche le message « *AVERTISSEMENT* Le système est sur le point de S'ARMER! ». Le clavier doit faire partie du **Groupe de claviers différer avertissement** défini dans **Programmation | Partitions | Configuration**.

  Pour activer l'armement différé d'une partition, consulter **Reporter armement automatique (Programmation | Partitions | Options 2**).

- **Afficher les détails de temps et de présence** : Lorsque cette option est activée, chaque fois qu'un utilisateur accède à la porte associée, le clavier affiche son nom, l'heure actuelle et la date. Ceci est utile pour informer les employés de l'heure à laquelle ils sont arrivés au travail.

  La porte utilisée est définie comme la **porte connectée au clavier** (onglet **Configuration**).

- **Durée d'affichage du détail des présences** : Lorsque l'option **Afficher le détail temps et présence** est activée, il s'agit de la durée (en secondes) pendant laquelle le message de temps et de présence sera affichée sur le clavier.
- **Format du détail des présences** : Lorsque l'option **Afficher le détail du temps et des présences** est activée, ce champ définit le format qui sera utilisé pour la date. Choisissez entre les formats mois en premier ou jour en premier.

Options d'accès

- **Touche de fonction déverrouille la porte lorsque connecté (REX)** : Lorsque cette option est activée, les utilisateurs peuvent se connecter à un clavier en appuyant sur la touche **[FUNCTION]** (en maintenant la touche **[MENU]** pendant 2 secondes sur le PRT-KLCS). Vous pouvez définir **la porte connectée au clavier** dans l'onglet **Configuration**.
- **Clavier peut accéder seulement la partition primaire** : Lorsque cette option est activée, les utilisateurs peuvent uniquement afficher et contrôler la partition primaire du clavier (**partition à laquelle appartient cet ACL appartient** dans l'onglet **Configuration**), quel que soit le groupe de partitions attribué au clavier.
- **Permettre accès 24 heures de la partition** : Lorsque cette option est activée, les utilisateurs peuvent visualiser et contrôler les portions de 24 heures de toutes les portions disponibles sur le clavier. On y accède en appuyant sur la touche **[LEFT]** pendant la visualisation d'une partition.

  L'utilisateur doit également avoir activé l'option **Contrôle partition sabotage permis** dans son groupe de menus (**Groupes | Groupes de menus | Général**).

- **Permettre l'accès de sélection du groupe de partitions** : Lorsque cette option est activée, les utilisateurs peuvent visualiser et contrôler le groupe de partitions attribué à ce clavier (**Groupe de partitions pour ce clavier** dans l'onglet **Configuration**). On y accède en appuyant sur la touche **[RIGHT]** pendant la visualisation d'une partition.

  L'utilisateur doit également avoir activé l'option **Contrôle groupe de partitions permis** dans son groupe de menus (**Groupes | Groupes de menus | Général**).

- **Touche de fonction déverrouille la porte lorsque déconnecté (REX)** : Lorsque cette option est activée, les utilisateurs peuvent déverrouiller une porte en appuyant sur la touche **[FUNCTION]** (en maintenant la touche **[MENU]** pendant 2 secondes sur PRT-KLCS) sans se connecter au clavier. Vous pouvez définir **la porte connectée au clavier** dans l'onglet **Configuration**.
- **Déconnexion automatique après armement de l'utilisateur** : Lorsque cette option est activée, le clavier ferme automatiquement la session de l'utilisateur lorsqu'une partition est armée ou désarmée avec succès. Cela peut empêcher des tiers d'accéder au clavier si l'utilisateur oublie de se déconnecter.
- **Activer Sortie Niveau d'accès** : Lorsque cette option est activée, la ou les sorties associées au niveau d'accès de l'utilisateur seront activées lorsque l'utilisateur se connectera avec succès à ce clavier. Ces sorties sont définies dans les onglets **Utilisateurs | Niveaux d'accès | Sorties / Groupes de sorties**. L'option **Accès du clavier active la sortie** doit également être activée (**Utilisateurs | Niveaux d'accès | Général**).

  Par défaut, l'utilisateur doit avoir un accès valide aux menus du clavier à partir de son niveau d'accès. Pour enlever cette restriction, activez l'option **Toujours activer sortie de niveau d'accès** (onglet **Options 2**).

- **Verrouiller clavier sur tentatives excédentaires** : Lorsque cette option est activée, si quelqu'un tente à plusieurs reprises de se connecter avec un NIP d'utilisateur non valide, le clavier bloquera toute nouvelle tentative pendant une période déterminée. Lorsque le clavier est verrouillé, l'entrée trouble Trop de tentatives s'ouvre.

  Le **maximum d'entrées NIP invalides** et **la durée de verrouillage du clavier** sont définis dans l'onglet **Configuration**.

Claviers | Options 2

Options hors ligne

- **Accès hors ligne au menu d'automatisation** : Lorsque cette option est activée, les utilisateurs peuvent accéder au menu d'automatisation en appuyant sur **[MENU] [1]** sans se connecter au clavier. Les automatisations peuvent être liées à des sorties ou à des groupes de sorties, offrant ainsi aux utilisateurs une méthode pratique pour contrôler des dispositifs tels que l'éclairage, les arroseurs et le CVC.
- **Permettre l'accès au menu de vue trouble** : Lorsque cette option est activée, les utilisateurs peuvent accéder au menu d'affichage des troubles en appuyant sur **[MENU] [2]** sans se connecter au clavier. Ceci est pratique pour les techniciens qui diagnostiquent des problèmes dans le système.
- **Permettre l'accès au menu de révision d'événements** : Lorsque cette option est activée, les utilisateurs peuvent accéder au menu des événements en appuyant sur **[MENU] [3]** sans se connecter au clavier. Ceci est pratique pour les gardes qui passent en revue les événements récents.
- **Permettre l'accès au menu d'information** : Lorsque cette option est activée, les utilisateurs peuvent accéder au menu d'information en appuyant sur **[MENU] [4]** sans se connecter au clavier. Cela inclut des informations telles que la version du micrologiciel du contrôleur, le numéro de série du contrôleur, l'heure et la date.
- **Connexion clavier requiert carte** : Lorsque cette option est activée, les utilisateurs doivent présenter une carte et saisir un NIP pour accéder au clavier (authentification à deux facteurs).

  Le clavier doit être associé à un port du lecteur ou à un lecteur intelligent. Une fois qu'un utilisateur a passé son badge au lecteur, il peut saisir son NIP sur le clavier et appuyer sur **[ENTER]** pour se connecter. Les NIP ne peuvent pas être saisis directement au clavier sans présenter d'une carte au préalable.

  Pour activer cette fonctionnalité, il est nécessaire de configurer les options suivantes dans la programmation du module d'expansion du lecteur :
  - **Porte du lecteur 1/2** : Doit être défini sur une porte qui nécessite un accès par carte et code NIP pour l'entrée ou la sortie (correspondant au côté de la porte où se trouve le clavier).
  - **Type de clavier du lecteur 1/2** : Clavier ACL
  - **Clavier à utiliser pour NIPs du lecteur 1** : Ce clavier

En plus des options hors ligne décrites ci-dessus, il est également possible de visualiser toutes les entrées ouvertes dans la partition primaire du menu hors ligne, en ajoutant la commande `OfflineInputView = true`. Pour visualiser toutes les entrées dans la partition primaire, inclure également la commande `ClosedInputsInOfflineView = true`.

Options générales

- **Désactiver le signal sonore du clavier ACL** : Lorsque cette option est activée, le clavier ne produit pas de signal sonore lorsque vous appuyez sur les touches. Les autres opérations du signal sonore fonctionneront toujours.

  L'activation de ce réglage a priorité sur l'option **La touche Effacer peut désactiver le signal sonore de la touche** ci-dessous.

- **Entrées duplexes (4 entrées clavier)** : Lorsque cette option est activée, le clavier peut prendre en charge jusqu'à 4 entrées câblées en configuration duplex. Les entrées supplémentaires doivent être adressées comme entrées 3-4 sur le clavier.

  Pour les instructions de câblage, consulter le manuel d'installation du clavier correspondant.

- **Émettre un bip sur échec de communication** : Il s'agit d'une option héritée qui n'a aucun effet.
- **La touche Effacer peut désactiver le signal sonore de la touche** : Lorsque cette option est activée, les utilisateurs peuvent appuyer sur la touche**[CLEAR]** et la maintenir enfoncée pour désactiver le signal sonore du clavier. L'option désactive toutes les fonctions du signal sonore (par exemple, la réponse à la pression des touches, les alarmes et les délais d'entrée ou de sortie, le contrôle manuel, etc.). Appuyer encore une fois sur la touche **[CLEAR]** et la maintenir enfoncée pour activer le signal sonore.

  Ce réglage n'a aucun effet lorsque l'option **Désactiver le signal sonore du clavier ACL** ci-dessus est activée.
- **Module virtuel** : Activez cette option pour enregistrer le module en tant que module virtuel. Les modules virtuels agissent comme des emplacements dans le système, vous permettant de programmer des entrées et des sorties virtuelles à utiliser avec des fonctions programmables et d'autres fonctions avancées.

Options de sorties

- **Activer sortie de niveau d'accès seulement sur accès valide** : Cette option n'est pas utilisée. Ceci est le comportement par défaut pour les sorties de niveau d'accès.
- **Toujours activer sortie de niveau d'accès** : Lorsque cette option est activée, la sortie ou le groupe de sorties du niveau d'accès de l'utilisateur sera toujours activé(e) lorsqu'il saisit son code NIP sur le clavier, qu'il ait ou non accès à ce clavier. Cela peut permettre aux utilisateurs de contrôler une sortie ou un groupe de sorties spécifiques à partir du clavier sans leur donner accès au clavier.

  Activer sortie niveau d'accès (onglet **Options 1**) doit être activé. Les sorties de niveau d'accès sont attribuées dans **Utilisateurs | Niveaux d'accès | Sorties / Groupes de sorties**.

Commandes des claviers manuelles

Un clic droit sur un registre de clavier dans **Modules d'expansions | Claviers** ouvre un menu avec des commandes manuelles pour ce clavier.

Contrôle

- **Réinitialiser le**s utilisateursIl s'agit d'une option héritée qui n'a aucun effet. :
- **Mettre à jour le module** : Met à jour la programmation du clavier. Pour plus d'informations, consultez la section Mises à jour du module (la page 308).

Modules d'expansion analogiques

Les enregistrements des modules d'expansion analogiques sont utilisés pour surveiller et contrôler les canaux analogiques. Ils peuvent être configurés comme des entrées analogiques (réception de données) ou des sorties analogiques (envoi de données), en association avec des valeurs de données et des variables.

Protege Les modules d'expansion d'entrée analogiques et les modules d'expansion de sortie analogiques peuvent être utilisés pour connecter une variété de détecteurs analogiques (tels que les capteurs de température et d'humidité) et de dispositifs d'automatisation industrielle (tels que les modules HVAC) au système. Les canaux analogiques peuvent être surveillés directement dans Protege GX et peuvent contrôler ou être contrôlés par des fonctions programmables. Cela vous permet d'unifier les fonctions de sécurité et d'automatisation de votre site.

Pour plus d'informations sur la connexion des modules d'expansion analogiques, consultez le manuel d'installation correspondant.

Protege les alimentations électriques s'enregistrent comme des modules d'expansion analogiques dans le système. Cela vous permet de surveiller quatre canaux d'entrée : tension de base, tension V1, tension V2 et courant. Pour plus d'informations, consultez la section Surveillance de la tension et du courant de l'alimentation électrique (la page 317).

Modules d'expansions analogiques | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Personnalité du module d'expansion** : La personnalité du module d'expansion doit être réglée sur le code produit du Protege module connecté.

Configuration

- **Inverser sabotage de l'appareil** : Lorsque cette option est activée, l'entrée de sabotage du module sera inversée. Cette fonction doit être activée lorsque l'interrupteur d'altération a une configuration normalement ouverte.
- **Module virtuel** : Activez cette option pour enregistrer le module en tant que module virtuel. Les modules virtuels agissent comme des emplacements dans le système, vous permettant de programmer des entrées et des sorties virtuelles à utiliser avec des fonctions programmables et d'autres fonctions avancées.
- **Adresse physique** : L'adresse réseau du module sur le réseau du contrôleur. Les modules d'extension connectés peuvent être adressés avec la fonction **Adressage de module** du contrôleur (clic droit sur l'enregistrement du contrôleur).

  L'adresse physique maximale disponible pour les modules d'expansion analogiques est de 32.

Commandes

- Ce champ est utilisé pour envoyer des commandes de programmation à l'appareil. Il ne doit être utilisé que lorsqu'il est spécifiquement conseillé par la documentation ICT ou le support technique.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Modules d'expansions analogiques | Canal 1-4

Options

- **Activer le canal** : Lorsque cette option est activée, le module d'expansion analogique commencera à traiter le canal analogique. Le canal peut agir soit comme une sortie analogique (envoi de données), soit comme une entrée analogique (réception de données), selon le matériel. Lorsque cette option est désactivée, le canal ne remplira aucune fonction.
- **Canal utilise une entrée de 0-20mA (déactivée utiliser 0-10V)** : Chaque canal peut être configuré pour une opération en courant ou en tension. Par défaut, l'entrée ou la sortie fonctionnera en mode 0-10V. Lorsque cette option est activée, celui-ci fonctionnera en mode 0-20mA. L'option sélectionnée dépendra des appareils connectés.

  En mode courant, la marge de signal acceptable est de 0-20mA, ce qui permet de connecter des appareils standard 4-20mA.

- **Sortie de préréglage DAC mise sous tension** : Lorsque ce canal est utilisé pour une sortie analogique (DAC), activer cette option pour régler la sortie sur une valeur fixe lorsque le module est sous tension. La valeur préréglée est déterminée par l'option ci-dessous. Lorsque cette option est désactivée, lorsque la sortie est mise sous tension, elle est réglée sur la dernière valeur connue.
- **Préréglage à 100 pourcent (préréglage désactivé à 0)** : Lorsque **Sortie de préréglage DAC mise sous tension** est activé, cette option détermine l'état de la sortie analogique lorsque le module est mis sous tension. Lorsque cette option est activée, la sortie sera fixée à 100% (la valeur maximale). Lorsque cette option est désactivée, la sortie sera fixée à 0% (la valeur minimale).
- **Transmettre valeur ADC en mode diff**: Lorsque ce canal est utilisé pour une entrée analogique (ADC), cette option détermine comment les valeurs d'entrée sont envoyées au contrôleur.

  Par défaut (lorsque cette option est désactivée), la valeur analogique est envoyée au contrôleur à des intervalles définis. La fréquence des mises à jour est définie comme le **temps de mise à jour des canaux 1-4** ci-dessous.

  Lorsque cette option est activée, la valeur analogique est envoyée au contrôleur uniquement lorsqu'elle a changé d'une certaine quantité (la diff). Le chiffre que la valeur doit changer avant qu'une mise à jour soit envoyée est défini comme la **valeur de comparaison du canal diff** ci-dessous.
- **Enregistrer les données du canal**: Lorsque cette option est activée, toutes les mises à jour de données du canal sont enregistrées comme des événements. Ceci est utile pour la configuration initiale et le dépannage, mais doit être désactivée pendant le fonctionnement normal afin d'économiser le stockage des événements.

Paramètres du canal

- **Temps de mise à jour du canal** : Lorsque **Transmettre valeur ADC en mode diff** estdésactivé, le canal enverra des mises à jour au contrôleur à intervalles réguliers. Ce champ définit le temps entre les mises à jour (en secondes), et les données sont moyennées sur la période de temps qui est échantillonnée.

  Il est recommandé d'échelonner le temps de mise à jour en fonction du taux de changement prévu et du niveau de supervision requis. Un long temps de mise à jour est généralement suffisant et réduit le risque de "pics" dans les données.
- **Valeur de comparaison du canal diff** : Lorsque **Transmettre valeur ADC en mode diff** estactivé, le canal enverra des mises à jour au contrôleur lorsque la valeur a changé d'une quantité définie. Ce champ définit la valeur diff qui est utilisée pour comparer la valeur actuelle avec la mise à jour la plus récente.

  Par exemple, lors de la surveillance de la tension centrale d'une alimentation électrique, cette valeur peut être fixée à 10. Si la dernière valeur mise à jour est 1367 (13.67V), le canal n'enverra pas de mise à jour au contrôleur avant que la tension n'atteigne 1357 (13.57V) ou 1377 (13.77V).
- **Enregistrer les données du canal**: Chaque canal peut être affecté à une valeur de données, ce qui permet au système de définir et de stocker les données analogiques du canal. Lorsqu'elle est connectée à une entrée analogique, la valeur de données stocke et affiche les données provenant du canal. Lorsqu'elle est connectée à une sortie analogique, la valeur des données définit la valeur de sortie et l'envoie au matériel.

  Les valeurs des données sont programmées dans **Automatisation | Valeurs des données**.

Surveillance de la tension et du courant de l'alimentation électrique

Protege les alimentations électriques peuvent être traitées comme des modules d'expansion analogiques dans le système. Cela vous permet de configurer et de surveiller 4 canaux d'entrée analogiques représentant la tension et le courant dans l'alimentation électrique.

Les canaux représentent les informations suivantes :

Numéro de canal	Fonction
1	Tension de base
2	Tension V1
3	Tension V2
4	Courant

En utilisant des valeurs de données et des variables, il est possible de surveiller ces valeurs afin que les opérateurs puissent rester conscients de la consommation d'énergie du système.

1. Connecter l'alimentation électrique au réseau de module comme indiqué dans le manuel d'installation correspondant.
2. Identifier l'alimentation électrique comme un module d'expansion analogique (consultez la page 93).
3. Créer un enregistrement du module d'expansion analogique dans **Modules d'expansion | Modules d'expansion analogiques** avec une **adresse physique** correspondant à celle de l'alimentation électrique.
4. Régler la **Personnalité du module d'expansion** au type d'alimentation électrique connecté.
5. Dans l'onglet **Canal 1**, configurer les paramètres suivants pour le canal de tension de base :
   - **Activer le canal** : Activé
   - Pour mettre à jour la valeur à intervalles réguliers, désactiver **Transmettre valeur ADC en mode diff** et régler le **temps de mise à jour du canal 1**, OU
   - Pour mettre à jour la valeur à chaque fois qu'elle change d'un montant défini, activer **Transmettre valeur ADC en mode diff** et régler la **valeur de comparaison diff du canal 1**.
6. Une valeur de données doit être utilisée pour stocker les données. Cliquer sur l'ellipse **[...]** à côté **de la valeur de données du canal 1** pour ouvrir une fenêtre de rupture avec la programmation de la valeur de données. Créer une nouvelle valeur de données avec le nom Tension de base. Cliquez sur **Sauvegarder**.
7. Fermer la fenêtre de rupture et régler la valeur de données du **canal 1 sur la valeur** de données de la tension de base.
8. Répéter l'opération ci-dessus pour le canal 2 (tension V1), le canal 3 (tension V2) et le canal 4 (courant).
9. Cliquez sur **Sauvegarder**. Attendre que la programmation soit téléchargée sur le contrôleur, puis faire un clic droit sur l'enregistrement du module d'expansion analogique et cliquer sur **Mettre à jour le module**.
10. Des variables doivent être utilisées pour afficher les données du canal. Naviguer vers **Automatisation | Variables**. Créer quatre nouvelles variables avec les noms Tension de base Variable, V1 tension Variable, etc.
11. Pour chaque variable, régler **l'Échelle** sur 0,01 et la **Valeur de données** sur la valeur de données correspondante programmée ci-dessus. Cliquez sur **Sauvegarder**.
12. Les variables peuvent maintenant être affichées sur un plan d'étage. Naviguer vers **Surveillance | Configuration | Éditeur de plan d'étage** et sélectionner un plan d'étage existant ou en créer un nouveau.
13. Développer la section **Appareils** et cliquer sur **Ajouter**.
14. Définir le **type d'appareil** sur Variable et faire glisser les quatre variables sur le plan d'étage. Vous pouvez également ajouter du texte pour étiqueter chaque affichage de variable. Cliquez sur **Sauvegarder**.
15. Vous pouvez maintenant ouvrir le plan d'étage à partir de **Surveillance | Vue du plan d'étage** et surveiller les valeurs variables.

Modules d’expansion d’entrée

Les modules d’expansion d’entrée augmentent le nombre d’entrées disponibles dans le système, ce qui vous permet de surveiller davantage d’appareils tels que les contacts de porte, les entrées d’ascenseur, les PIR et les boutons de panique. Les module d’expansion d’entrée virtuels peuvent également être utilisés pour générer des alarmes via les fonctions programmables d’entrée suit sortie.

Pour les instructions de câblage, consulter le manuel d’installation correspondant.

Modules d’expansion d’entrée | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Configuration

- **Courant de charge élevée** : Lorsque cette option est activée, un module PCB hérité va permettre à la batterie connectée de se charger à 700 mA. Le régime de charge par défaut est de 350 mA. Cette option n'est pas utilisée pour les modules de rail DIN.
- **Module virtuel** : Activez cette option pour enregistrer le module en tant que module virtuel. Les modules virtuels agissent comme des emplacements dans le système, vous permettant de programmer des entrées et des sorties virtuelles à utiliser avec des fonctions programmables et d'autres fonctions avancées.
- **Inverser sabotage de l’appareil** : Lorsque cette option est activée, l’entrée de sabotage du module sera inversée. Cette fonction doit être activée lorsque l’interrupteur d’altération a une configuration normalement ouverte.
- **Adresse physique** : L'adresse réseau du module sur le réseau du contrôleur. Les modules d'extension connectés peuvent être adressés avec la fonction **Adressage de module** du contrôleur (clic droit sur l'enregistrement du contrôleur).

  Le nombre maximum d’adresses physiques disponibles pour les modules d’expansion d’entrée est de 248.

Commandes

- Ce champ est utilisé pour envoyer des commandes de programmation à l'appareil. Il ne doit être utilisé que lorsqu'il est spécifiquement conseillé par la documentation ICT ou le support technique.

Intégration externe

Cette section vous permet de configurer l’intégration Redwall ou Inovonics pour ce module d’expansion d’entrée. Les options disponibles dépendent du **type d’intégration** dans **Sites | Contrôleurs | Configuration**.

Pour plus d’informations, consulter la note de l’application 181 : Protege GX Intégration Redwall ou la note de l’application 183 : Protege GX Intégration Inovonics.

- **Redwall**
  - **Adresse IP du module** : L’adresse IP du module Redwall Redscan que ce registre de module d’expansion de partition représente.
- **Inovonics**

- **Numéro de série de module** : Le numéro de série de l'appareil sans fil Inovonics que représente ce module d'expansion d'entrée.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Modules d’expansion de sorties

Les modules d’expansion de sortie augmentent le nombre de sorties disponibles dans le système, ce qui vous permet de contrôler davantage de dispositifs tels que des relais de verrouillage, des pompes de porte, des DEL, des bips et des sirènes. Les modules d’expansion de sortie virtuels peuvent également faciliter une variété de fonctions de programmation avancées, telles que les fonctions programmables de contrôle logique.

Pour les instructions de câblage, consulter le manuel d’installation correspondant.

Modules d’expansion de sortie | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Configuration

- **Courant de charge élevée** : Lorsque cette option est activée, un module PCB hérité va permettre à la batterie connectée de se charger à 700 mA. Le régime de charge par défaut est de 350 mA. Cette option n'est pas utilisée pour les modules de rail DIN.
- **Inverser sabotage de l’appareil** : Lorsque cette option est activée, l’entrée de sabotage du module sera inversée. Cette fonction doit être activée lorsque l’interrupteur d’altération a une configuration normalement ouverte.
- **Module virtuel** : Activez cette option pour enregistrer le module en tant que module virtuel. Les modules virtuels agissent comme des emplacements dans le système, vous permettant de programmer des entrées et des sorties virtuelles à utiliser avec des fonctions programmables et d'autres fonctions avancées.
- **Adresse physique** : L'adresse réseau du module sur le réseau du contrôleur. Les modules d'extension connectés peuvent être adressés avec la fonction **Adressage de module** du contrôleur (clic droit sur l'enregistrement du contrôleur).

  Le nombre maximum d’adresses physiques disponibles pour les modules d’expansion de sortie est de 32.

Commandes

- Ce champ est utilisé pour envoyer des commandes de programmation à l'appareil. Il ne doit être utilisé que lorsqu'il est spécifiquement conseillé par la documentation ICT ou le support technique.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Modules d'expansion du lecteur

Les modules d'expansion du lecteur permettent d'augmenter le nombre d'appareils de lecture disponibles dans le système. Chaque module d'expansion du lecteur possède deux ports de lecteur, chacun pouvant être utilisé pour contrôler une porte ou une cabine d'ascenseur.

Un registre de module d'expansion du lecteur peut également être associé au module d'expansion du lecteur intégré du contrôleur. L'adresse de ce module d'expansion est définie dans le champ **Enregistrer comme module d'expansion de lecteur** (**Sites | Contrôleurs | Configuration**).

Pour les instructions de câblage, consulter le manuel d'installation correspondant.

Modules d'expansions du lecteur | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Configuration

- **Opération hors ligne** : Ce champ définit comment le module d'expansion du lecteur fonctionnera lorsqu'il perdra la connexion avec le contrôleur. Les options sont :
  - **Aucun utilisateur** : Le module d'expansion du lecteur n'accordera l'accès à aucun utilisateur.
  - **N'importe quelle carte** : Le module d'expansion du lecteur accordera l'accès à toute carte qui peut être lue. Cela permettra à toute personne possédant une carte au format correct d'accéder à la porte, même si la carte n'est pas programmée dans le système.
  - **Premiers 10 utilisateurs plus cache** : Avec cette option activée, le module d'expansion du lecteur stocke un certain nombre de cartes et accorde l'accès à ces cartes lorsqu'il est hors ligne. Toutes les autres cartes se verront refuser l'accès.
    - Le module d'expansion du lecteur accordera l'accès aux 10 premiers utilisateurs téléchargés sur le contrôleur. Il s'agit des 10 premiers utilisateurs par ID base de données ayant accès à tout ce qui se trouve sur le contrôleur, qu'ils aient ou non accès aux portes de ce module d'expansion. Seule la première carte programmée sera reconnue.
    - En outre, le module d'expansion du lecteur stockera les 150 cartes les plus récentes qui ont obtenu un accès à ce module d'expansion. Ces utilisateurs auront accès aux deux portes, quel que soit leur niveau d'accès normal.

  Lorsque le module d'expansion du lecteur est hors ligne, chaque fois qu'un accès est accordé, le lecteur émet quatre bips. L'utilisation du NIP n'est pas prise en charge par les modules d'expansion du lecteur hors ligne, et toutes les portes ne permettent qu'un accès par carte.
- **Opération Comm Esclave** : Certains anciens modules d'expansion du lecteur PCB possèdent un port RS-485 supplémentaire qui permet la connexion d'un réseau esclave. Cette option définit la fonction du réseau esclave. Cette option n'est pas utilisée pour les modules de rail DIN.
- **Étage de l'ascenseur divisé**: Lorsque **Opération Comm Esclave** est réglé sur 1 - 1 - Contrôle Étage Ascenseur, cette option définit où les relais d'étage sont répartis. Cette option n'est pas utilisée pour les modules de rail DIN.
- **Adresse physique** : L'adresse réseau du module sur le réseau du contrôleur. Les modules d'extension connectés peuvent être adressés avec la fonction **Adressage de module** du contrôleur (clic droit sur l'enregistrement du contrôleur).

Le nombre maximum d'adresses physiques disponibles pour les modules d'expansion du lecteur est de 64.

- **Type de réseau du port 1/2** : Ces champs déterminent le mode de fonctionnement de chaque port du lecteur (c'est-à-dire le type de données qu'il enverra et recevra). Les options sont :
  - **Wiegand** : Utilisé pour tout lecteur Wiegand standard.
  - **ICT RS-485** : Utilisé pour les lecteurs câblés en configuration RS-485 (recommandé).
  - **OSDP** : Utilisé lors de la connexion de lecteurs OSDP. Lorsque vous sélectionnez cette option, le logiciel crée automatiquement deux lecteurs intelligents dans **Modules d'expansion | Lecteurs intelligents** pour représenter les lecteurs de cartes OSDP d'entrée et de sortie sur ce port. Pour plus d'informations, consulter la note d'application 254 : Configuration des lecteurs OSDP dans Protege.
  - **Salto SALLIS** : Utilisé pour connecter un routeur SALLIS RS-485, qui peut contrôler jusqu'à 16 serrures sans fil (configurées comme des lecteurs intelligents). Pour plus de renseignements, consulter la note d'application 148 : intégration Salto SALLIS dans Protege GX.
  - **Aperio** : Utilisé pour connecter jusqu'à 15 concentrateurs de communication Aperio, qui peuvent contrôler jusqu'à 60 serrures sans fil (configurées comme des lecteurs intelligents). Pour plus de renseignements, consulter la Note d'application 147 : Protege GX intégration Aperio via RS-485.
  - **Série Allegion AD** : Utilisé pour connecter des PIM Allegion (jusqu'à 16 serrures sans fil prises en charge) ou des serrures câblées. Pour plus d'informations, consulter la note d'application 182 : Intégration Allegion avec Protege GX.
  - **Tierce Partie Générique** : Cette option vous permet de configurer le module d'expansion du lecteur pour qu'il reconnaisse les lecteurs tiers ou d'autres sources génériques de données série sur ce port de lecteur (consulter les options **Tierce Partie Générique** dans l'onglet **Lecteur 1/2**). Pour plus d'informations, consulter la note d'application 276 : Configuration des types d'informations d'identification dans Protege GX.
- **Type de réseau Ethernet** : Lorsque ce registre de module d'expansion du lecteur est utilisé pour le module d'expansion du lecteur intégré du contrôleur, vous pouvez définir ici la fonction du port Ethernet. Ceci est utilisé lorsqu'un système tiers envoie des données de lecteur au contrôleur.

  Les options sont :
  - **Carte désactivée** : Le port Ethernet n'est pas utilisé pour les données du lecteur. Cela n'a pas d'incidence sur la connexion du contrôleur au réseau IP.
  - **SALLIS** : Utilisé pour connecter un routeur SALLIS POE, qui peut contrôler jusqu'à 64 serrures sans fil (configurées comme des lecteurs intelligents). Des lecteurs intelligents sont requis pour configurer le contrôle de portes. Pour plus de renseignements, consulter la note d'application 148 : intégration Salto SALLIS dans Protege GX.
  - **Tierce Partie Générique** : Vous permet de connecter des sources de données personnalisées au contrôleur pour les utiliser comme lecteurs, via le réseau IP. Toute entrée de données qui peut être configurée comme un type d'informations d'identification peut être utilisée, avec un lecteur intelligent pour configurer le contrôle de portes. Pour plus d'informations, consulter la note d'application 276 : Configuration des types d'informations d'identification dans Protege GX.
  - **VingCard VisiOnline** : Utilisé pour se connecter à un serveur VingCard VisiOnline, qui communique avec des serrures sans fil (configurées comme des lecteurs intelligents). Pour plus d'informations, consulter la note d'application 215 : Intégration de VingCard VisiOnline dans Protege GX.
- **Port Ethernet** : Lorsque le **type de réseau Ethernet** ci-dessus est défini sur Tierce Partie Générique, ce champ définit le port TCP/IP sur lequel le contrôleur communiquera. Ce port est utilisé par les lecteurs intelligents pour recevoir des données de « lecteurs » tiers.

  Si le contrôleur doit écouter sur plusieurs ports pour différentes sources de données, saisir la commande `SmartReaderPortOffset = true` dans le champ **Commandes** ci-dessous. Le port utilisé par chaque lecteur intelligent correspond au **port Ethernet** plus l'**adresse configurée** (**Modules d'expansions | Lecteurs intelligents | Général**).
- **Port de routeur SALLIS** : Lorsque le **type de réseau Ethernet** ci-dessus est réglé sur SALLIS, ce champ définit le port utilisé pour communiquer avec le routeur SALLIS.

- **IP de routeur SALLIS** : Lorsque le **type de réseau Ethernet** ci-dessus est réglé sur SALLIS, ce champ définit l'adresse IP utilisée pour communiquer avec le routeur SALLIS.

Options

- **Option charge élevée** : Lorsque cette option est activée, un module PCB hérité va permettre à la batterie connectée de se charger à 700 mA. Le régime de charge par défaut est de 350 mA. Cette option n'est pas utilisée pour les modules de rail DIN.
- **Port 1/2 entrée lecteurs multiples** : Lorsque le **type de réseau du port 1/2** est réglé sur Wiegand, sélectionnez ces options pour activer le traitement de plusieurs lecteurs pour chaque port de lecteur. Cela vous permet de connecter deux lecteurs au port de lecteur spécifié pour servir de lecteurs d'entrée et de sortie. Lorsque ces options sont désactivées, le port du lecteur ne traite qu'un seul lecteur connecté.

  Ce réglage n'est pas nécessaire pour les connexions RS-485. Pour les instructions de câblage, consulter le manuel d'installation correspondant.
- **Module virtuel** : Activez cette option pour enregistrer le module en tant que module virtuel. Les modules virtuels agissent comme des emplacements dans le système, vous permettant de programmer des entrées et des sorties virtuelles à utiliser avec des fonctions programmables et d'autres fonctions avancées.
- **Inverser sabotage de l'appareil** : Lorsque cette option est activée, l'entrée de sabotage du module sera inversée. Cette fonction doit être activée lorsque l'interrupteur d'altération a une configuration normalement ouverte.

Options des données de cartes Ethernet

- **Clé de cryptage AES données de cartes** : Les cartes Salto SALLIS et Aperio peuvent être encodées avec les informations du site/de la carte via le client encodeur ICT. Ce champ définit la clé de décryptage afin que Protege GX puisse décrypter les données de ces cartes.

  Pour plus de renseignements, consulter la note d'application correspondante à chaque intégration.

  Ce champ définit la clé de cryptage pour les lecteurs SALLIS connectés à ce module d'expansion du lecteur.

Commandes

- Ce champ est utilisé pour envoyer des commandes de programmation à l'appareil. Il ne doit être utilisé que lorsqu'il est spécifiquement conseillé par la documentation ICT ou le support technique.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Modules d'expansion du lecteur | Lecteur 1/2

Ces onglets vous permettent de configurer le fonctionnement de chaque port du lecteur séparément. Différentes options seront disponibles en fonction du **type de réseau du Port 1/2** défini dans l'onglet **Général**.

Configuration

- **Format lecteur 1/2** : Ce champ définit le type de données que le port du lecteur recevra des lecteurs connectés. Les modules d'expansion du lecteur Protege prennent en charge une grande variété de protocoles disponibles publiquement, ainsi que certains protocoles spéciaux. Tout lecteur 26 ou 37 Bit conforme à la spécification du format standard fonctionnera avec le module d'expansion du lecteur.

  Les ports des modules d'expansion du lecteur prennent également en charge les informations d'identification personnalisées fournies par des appareils tiers :
  - L'option Format personnalisé utilise le format programmé dans **Sites | Contrôleurs | Format personnalisé du lecteur**.

- L'option Custom Credential utilise un type d'informations d'identification programmé dans **Sites | Types d'informations d'identification**. Le type d'informations d'identification utilisé est déterminé par le type de porte.

- **Location Lecteur 1/2** : La location indique au module d'expansion du lecteur si le lecteur connecté est installé du côté de l'entrée ou de la sortie de la porte. Ceci n'est pertinent que lorsque le **type de réseau du Port 1/2** est défini sur Wiegand, car la configuration du câblage est utilisée pour déterminer l'emplacement des connexions RS-485.

  Lorsque plusieurs lecteurs sont connectés à un port en configuration Wiegand, le lecteur qui est câblé au port secondaire est toujours compté comme le lecteur de sortie.

- **Mode du lecteur 1/2** : Chaque port du lecteur peut être configuré pour l'un des modes de fonctionnement suivants :
  - **Accès** : Contrôle l'accès par une porte. Définir la **porte du lecteur 1/2** selon les besoins. Ce mode doit également être utilisé pour contrôler un bouton d'appel d'ascenseur.
  - **Ascenseur** : Contrôle l'accès aux étages dans une cabine d'ascenseur. Définir l'**ascenseur du lecteur 1/2** selon les besoins.
  - **Contrôle de partition** : Contrôle l'armement et le désarmement de la partition uniquement. Définir la **partition de contrôle de la partition du lecteur 1/2**, tel que requis. Dans ce mode, le lecteur de cartes accepte les informations d'identification par carte ou par NIP. Les utilisateurs disposant des autorisations appropriées peuvent armer la partition en utilisant la méthode définie dans le **mode d'armement du lecteur 1/2**, et désarmer la partition en saisissant une fois leurs informations d'identification (lorsque l'option **Désarmer la partition pour la porte sur accès** est activée).

    Les ports de lecteur utilisés pour l'accès aux portes peuvent également être utilisés pour le contrôle de partition en définissant la **Partition à l'intérieur de la porte** et la **Partition à l'extérieur de la porte** (**Programmation | Portes | Général**).

- **Porte du lecteur 1/2** : Lorsque le **mode lecteur 1/2** est défini sur Accès, ce champ définit la porte qui est contrôlée par ce port du lecteur. Une même porte peut être contrôlée par plus d'un port du lecteur (entrée et sortie).
- **Type de clavier du lecteur 1/2** : Le port du lecteur prend en charge un certain nombre de formats de claviers NIP différents connectés en configuration Wiegand. Lorsqu'il est configuré pour un fonctionnement RS-485, seules les options ARK-501 et clavier ACL sont disponibles.
  - **Clavier ACL** : Cette option vous permet d'associer un module de clavier ACL à ce port du lecteur (le **Clavier à utiliser pour NIP du lecteur 1/2** ci-dessous). Lorsqu'un utilisateur présente son badge au lecteur, le clavier l'invite à saisir son NIP et à appuyer sur la touche **[FUNCTION]** pour déverrouiller la porte.

    Pour déverrouiller la porte, l'utilisateur **ne doit pas appuyer sur [ENTRÉE]** après avoir saisi son code NIP. La touche **[FONCTION]** doit suivre immédiatement le code NIP. Si l'utilisateur appuie sur **[ENTRÉE]**, le clavier le connectera (reportez-vous ci-dessous).

    En outre, cette option vous permet d'utiliser l'authentification à deux facteurs pour l'accès au clavier. Ceci est requis lorsque **Connexion clavier requiert carte** (**Module d'expansion| Claviers | Options 2**) est activé. Lorsque l'utilisateur passe sa carte, il peut saisir son NIP sur le clavier et appuyer sur **[ENTER]** pour se connecter au clavier.
  - **ARK-501** : Le format standard de Motorola® utilisé par lecteurs de carte ICT. Chaque pression sur une touche est codée sur 8 Bit de données, les 4 premiers Bit étant inversés par rapport aux 4 autres. L'utilisateur doit appuyer sur la touche **[ENTER]** ou **#** pour compléter le NIP.
  - **26 Bit (site 0)** : Format Wiegand 26 Bit utilisé par un clavier NIP connecté en parallèle avec le lecteur. Les données de clavier NIP ont un code de site de 0.

    Les codes NIP ne peuvent pas commencer par 0. Le NIP maximum pour ce format est 65535.

  - **4 Bit** : 4 Bit de données pour chaque pression sur une touche.
  - **Parité 4 Bit** : 4 Bits de données plus un Bit de parité pour chaque pression de touche.

- **4 Bit Buf** : 4 Bit de données à chaque appui de touche. Les données sont mises en mémoire tampon et envoyées uniquement lorsque l'utilisateur appuie sur la touche **[ENTER]** ou **#** pour compléter le code PIN.
- **4 Bit Buf & par** : 4 Bits de données plus un Bit de parité pour chaque pression de touche. Les données sont mises en mémoire tampon et envoyées uniquement lorsque l'utilisateur appuie sur la touche **[ENTER]** ou **#** pour compléter le code PIN.
- **36 Bit (IEI SO)** : Format Wiegand 36 Bit typique d'un clavier IEI, qui peut être configuré pour décoder les NIP de 0 à 999999.

  Les codes NIP ne peuvent pas commencer par 0. Le NIP maximum pour ce format est 999999.

- **Clavier à utiliser pour NIPs du lecteur 1/2** : Si le **type de clavier du lecteur 1/2** ci-dessus est réglé sur clavier ACL, ce clavier peut être utilisé pour la saisie du NIP à la porte.
- **Mode d'armement du lecteur 1/2** : La fonction définie dans ce champ permet aux utilisateurs d'armer des partitions ou de contrôler des sorties en saisissant leurs informations d'identification au niveau du lecteur de carte. Toutes les informations d'identification requises par le type de porte doivent être saisies à chaque fois. Le lecteur émet deux bips pour signaler que la fonction a réussi.

  Les options sont :
  - **Armer la partition sur 2 lectures** : Les utilisateurs peuvent saisir leurs identifiants deux fois pour armer la partition associée.
  - **Lecture et entrée 4/8 du module d'expansion** : Les utilisateurs peuvent maintenir l'entrée 4 (pour le port du lecteur 1) ou l'entrée 8 (pour le port du lecteur 2) et saisir leurs informations d'identification pour armer la partition associée.

    Si l'entrée 4/8 est surveillée par la partition en cours d'armement, l'armement peut échouer parce que l'entrée est ouverte. Pour éviter cela, assurez-vous que l'option **Entrée de sortie de l'allée ne pas la tester** est activée dans le type d'entrée attribué (**Programmation | Types d'entrée | Options (1)**).
  - **Armer la partition sur 3 lectures** : Les utilisateurs peuvent saisir leurs identifiants trois fois pour armer la partition associée.
  - **Basculer sortie de fonction sur 3 lectures** : Les utilisateurs peuvent saisir leurs identifiants trois fois pour activer ou désactiver la sortie ou le groupe de sorties de la fonction.
  - **Activer sortie de fonction sur 3 lectures** : Les utilisateurs peuvent saisir leurs informations d'identification trois fois pour activer la sortie ou le groupe de sorties de la fonction. La ou les sorties ne seront pas désactivées par cette fonction.

  Lorsque le **Mode Lecteur 1/2** est réglé sur Accès le lecteur d'entrée contrôle la **partition à l'intérieur de la porte** et le lecteur de sortie contrôle la **partition à l'extérieur de la porte** (réglage dans **Programmation | Portes | Général**). Lorsqu'il est réglé sur Contrôle de partition, les deux lecteurs contrôlent la **partition de contrôle de partition du lecteur 1/2** ci-dessous. Pour le options de contrôle des sorties, les deux lecteurs contrôlent la **sortie / le groupe de sorties de la fonction du lecteur 1/2**.

  L'utilisateur doit avoir coché **Autoriser l'armement multi-badge** dans **Utilisateurs | Niveaux d'accès | Général**. (indépendamment du fait que la fonction soit un contrôle de zone ou de sortie). Si les entrées du secteur peuvent être ouvertes, **Toujours armer en force à l'aide du lecteur de carte** peut être activé dans **Programmation | Secteurs | Options (2)**.
- **Partition de contrôle de partition du lecteur 1/2** : Lorsque le **mode lecteur 1/2** est réglé sur contrôle de partition, ce champ définit la partition qui est contrôlée par ce port du lecteur.
- **Ascenseur lecteur 1/2** : Lorsque le **mode lecteur 1/2** est réglé sur Ascenseur, ce champ définit la cabine d'ascenseur qui est contrôlée par ce port du lecteur.
- **Format secondaire du lecteur 1/2** : Le format de lecture secondaire est utilisé lorsque le module d'expansion du lecteur ne peut pas décoder une carte lue à l'aide du format primaire. Cette option est utile pour les sites qui utilisent plusieurs types de cartes.

  Pour plus d'informations sur les formats disponibles, consulter le **format de lecteur 1/2** ci-dessus.

- **Sortie / groupe de sorties de la fonction du lecteur 1/2** : Cette sortie ou ce groupe de sorties peut être activé (e) lorsque l'utilisateur saisit ses informations d'identification plusieurs fois, sur la base du **mode d'armement du lecteur 1/2** ci-dessus.
- **Sortie en attente d'authentification double du lecteur 1/2** : Cette sortie est activée lorsque le premier utilisateur saisit ses informations d'identification au niveau d'une porte qui nécessite une authentification double. C'est désactivé lorsque le **temps d'attente de l'authentification double du lecteur 1/2** ci-dessous expire ou que le deuxième utilisateur saisit ses informations d'identification.

  Pour les portes connectées au port Ethernet du contrôleur, utilisez la commande `DualAuthOutputEth = #`, où **#** est l'identifiant de base de données de la sortie.

- **Délai d'attente d'authentification double du lecteur 1/2** : Lorsqu'une porte est configurée pour nécessiter une l'authentification double, le module d'expansion du lecteur attendra pendant cette durée (en secondes), après que le premier utilisateur ait saisi ses informations d'identification. Le deuxième utilisateur peut saisir ses informations d'identification pendant cette période pour déverrouiller la porte. Si cette période expire, la porte ne se déverrouille pas et le processus doit être recommencé.

  Pour les portes connectées au port Ethernet du contrôleur, utilisez la commande `DualAuthTimeEth = #`, où **#** est le temps d'attente en secondes.

  Les paramètres d'authentification double sont configurés dans **Programmation | Types de portes | Option** .

Options du Lecteur

- **Permettre la lecture ouverte/déverrouillée** : Lorsque cette option est activée (par défaut), le module d'expansion du lecteur hors ligne traite les lectures de carte, même si la porte est déjà ouverte ou déverrouillée. Ceci est utile pour le fonctionnement correct de l'anti-passback, de temps et présence, des rapports Muster et du contrôle de partitions, car ça permet aux utilisateurs de s'enregistrer à la porte même si elle est déjà ouverte ou déverrouillée.

  Lorsque cette option est désactivée, toute lecture de carte reçue lorsque la porte est déverrouillée ou ouverte ne sera pas traitée et aucun événement ne sera généré.
- **Envoyer erreurs de format** : Lorsque cette option est activée, le module d'expansion du lecteur envoie des informations détaillées au contrôleur s'il lit une carte avec une erreur de format. Les erreurs de format comprennent le nombre de bits, le nombre d'octets, la parité, la somme de contrôle et les échecs de calcul LRC. Cette information apparaîtra dans le journal des événements.

  L'option **Enregistrer événements du lecteur** doit également être activée.
- **Mode de sabotage du lecteur intelligent** : Lecteurs de carte ICT offrent un fonctionnement de sabotage de lecteur intelligent. Lorsque cette fonction est activée à la fois dans le lecteur et dans le module d'expansion du lecteur, le lecteur de cartes effectuera un check in avec le module d'expansion du lecteur toutes les 30 secondes. Lorsque la connexion est perdue, l'entrée de trouble Lecteur 1/2 altéré/manquant est ouverte pour générer une alarme de sabotage.

  Cette option est toujours activée en mode RS-485.

Options données de cartes

- **Clé de cryptage AES données de cartes** : Les cartes Salto SALLIS et Aperio peuvent être encodées avec les informations du site/de la carte via le client encodeur ICT. Ce champ définit la clé de décryptage afin que Protege GX puisse décrypter les données de ces cartes.

  Pour plus de renseignements, consulter la note d'application correspondante à chaque intégration.

  Ce champ définit la clé de chiffrement pour les serrures connectées à ce port de lecteur.

Tierce partie générique :

Les options ci-dessous sont utilisées pour définir la structure des données en série génériques envoyées au port du lecteur. Cela peut être utilisé pour les lecteurs tiers et d'autres appareils.

Cette section ne s'affiche que lorsque le **type de réseau du port 1/2** est défini sur Tierce partie générique. Pour des exemples de programmation, consulter la note d'application 219 : Intégration d'interphone à l'aide de types d'informations d'identification dans Protege GX et note d'application 276 : Configuration des types d'informations d'identification dans Protege GX.

- **Ratio Baud Lecteur 1/2** : La vitesse à laquelle les données en série génériques sont transférées entre l'appareil tiers et le module d'expansion du lecteur.
- **Parité lecteur 1/2** : La méthode de calcul de la parité pour le bloc de données en série génériques. Ceci peut être pair, impair ou nul.
- **Bit d'arrêt Lecteur 1/2** : Les Bit d'arrêt pour les données en série génériques. C'est soit 1, 1,5 ou 2.
- **Délai d'attente inter-octet du lecteur 1/2** : Ce champ définit le temps (en millisecondes) autorisé entre la réception d'octets de données en série génériques.
- **Données non valides de journal du lecteur 1/2 reçues** : Activer cette option pour permettre au module d'expansion du lecteur d'enregistrer des informations détaillées sur tous les paquets de données invalides reçus d'un lecteur générique tiers.

Options misc

- **Désarmer la Partition pour la porte sur accès** : Lorsque cette option est activée, la partition associée sera automatiquement désarmée lorsqu'un utilisateur saisit des informations de connexion valides, à condition que l'utilisateur ait accès pour désarmer la partition. Lorsque le lecteur est utilisé pour le contrôle de portes, la partition derrière la porte sera désarmée. Lorsque le lecteur est utilisé pour le contrôle de partition, la partition de contrôle définie ci-dessus sera désarmée.
- **Permettre l'accès lorsque la Partition est armée** : Lorsque cette option est désactivée (par défaut), les utilisateurs peuvent se voir refuser l'accès à une porte lorsque la partition située derrière celle-ci est armée. L'accès ne leur sera permis que si ils ont la capacité de désarmer la partition.

  Cette option peut être activée pour permettre aux utilisateurs de passer par n'importe quelle porte à laquelle ils ont accès, quel que soit le statut de la partition. Sachez que cela peut facilement provoquer de fausses alarmes car les utilisateurs pourront entrer dans des partitions qu'ils ne peuvent pas désarmer.
- **Désarmer la partition d'usagers sur carte valide** : Cette option permet aux utilisateurs de désarmer une partition personnelle ou un groupe de partitions lorsqu'ils obtiennent l'accès au lecteur. Par exemple, cela pourrait être utilisé pour permettre à un seul lecteur de desservir une rangée de bureaux personnels que les utilisateurs peuvent armer et désarmer individuellement.

  Le réglage de la **zone Utilisateur** se fait dans **Utilisateurs | Utilisateurs | Général**, ou un groupe de partitions peut être réglé dans l'onglet **Groupes de partitions**. L'utilisateur doit avoir cette partition disponible dans **Utilisateurs | Niveaux d'accès | Désarmement groupes de partitions**.
- **Journaliser les événements du lecteur** : Activez cette option pour permettre au lecteur d'envoyer des informations sur les erreurs de format au contrôleur (avec l'option **Envoyer les erreurs de format** activée ci-dessus). Les autres événements du lecteur sont toujours envoyés au contrôleur.
- **Interchanger Affichage DEL de serrure**: Cette option n'est pas utilisée.
- **Activer Sortie Niveau d'accès** : Lorsque cette option est activée, la sortie ou le groupe de sorties attribué au niveau d'accès de l'utilisateur sera activé lorsque l'utilisateur aura accès à la porte.

  Les sorties sont affectées dans l'onglet **Sorties** ou **Groupes de sorties** de **Utilisateurs | Niveaux d'accès**. L'option **Accès du lecteur active la sortie** doit être activée dans **Utilisateurs | Niveaux d'accès | Général**, et d'autres configurations sont y sont disponibles.
- **Afficher détails de la carte lorsqu'invalide** : Lorsque cette option est activée (par défaut), le module d'expansion du lecteur envoie les détails de toute carte non reconnue (établissement et numéro de carte) au contrôleur. Le journal des événements affichera un événement « Lecture données brutes », permettant à un opérateur de faire un clic droit sur l'événement et d'attribuer la carte à un utilisateur.

Lorsque cette option est désactivée, les données de la carte ne sont pas sauvegardées et un événement « Carte pas trouvée » s'affiche dans le journal des événements.

- **Armer partition des utilisateurs** : Cette option permet aux utilisateurs de d'armer une partition personnelle ou un groupe de partitions au niveau du lecteur de cartes sur ce port du lecteur. Par exemple, cela pourrait être utilisé pour permettre à un seul lecteur de desservir une rangée de bureaux personnels que les utilisateurs peuvent armer et désarmer individuellement.

  L'action que l'utilisateur doit entreprendre pour armer la partition dépend du réglage du mode d'armement du **lecteur 1/2** ci-dessus.

  Le réglage de la **partition Utilisateur** se fait dans **Utilisateurs | Utilisateurs | Général**, ou un groupe de partitions peut être réglé dans l'onglet **Groupes de partitions**. L'utilisateur doit avoir coché la case **Activer l'armement multi-cartes** dans **Utilisateurs | Niveaux d'accès | Général**.

- **Activer les sorties Smart Reader améliorées** : Cette fonctionnalité est utilisée lorsque les lecteurs sont câblés en configuration RS-485. Les sorties BZ, L1 et L2 du module d'expansion du lecteur ne sont pas utilisées pour contrôler les bips et les DEL des lecteurs RS-485, mais par défaut elles sont réservées et ne peuvent pas être utilisées. Vous pouvez activer les sorties améliorées du lecteur intelligent pour « libérer » ces sorties physiques pour d'autres fonctions et obtenir un contrôle indépendant des sorties sur le lecteur RS-485 lui-même.

  Cette fonctionnalité modifie le fonctionnement des sorties du module d'expansion du lecteur à diverses adresses. Lecture Note d'application 295 : Sorties de lecteur intelligent amélioré dans Protege GX avant d'activer cette option.

  Cette fonctionnalité n'est pas liée aux lecteurs intelligents qui peuvent être programmés dans **Modules d'expansions | Lecteurs intelligents**.

Modules d'expansion du lecteur | Options du lecteur 1/2

Options

- **Inverser Relais d'étages** : Lorsque cette option est activée, le module d'expansion du lecteur PCB inversera toutes les sorties de relais sur les modules d'expansion de sorties PCB connectées qui sont utilisées pour le contrôle d'ascenseurs. Cette option n'est pas utilisée pour les modules de rail DIN.

  Les sorties relais d'étage d'ascenseur peuvent être inversées individuellement dans **Programmation | Sorties | Options**.

- **Contrôler relais sur échec de comm** : Lorsque cette option est activée, un module d'expansion de sortie PCB utilisé pour le contrôle d'ascenseurs contrôlera l'état des sorties de relais lorsque le module d'expansion est hors ligne. Sinon, les sorties relais resteront dans le même état lorsque le module d'expansion sera mis hors ligne. Cette option n'est pas utilisée pour les modules de rail DIN.
- **Relais activés en échec de comm**: Lorsque **Contrôler relais sur échec de comm** est activé, les sorties de relais sont désactivées par défaut lorsque le module d'expansion de sortie PCB est hors ligne. Activer cette option pour activer les sorties lorsque le module d'expansion passe hors ligne. Cette option n'est pas utilisée pour les modules de rail DIN.
- **Désactiver le traitement de la DEL rouge** : Lorsque cette option est activée, le module d'expansion du lecteur ne contrôle pas la sortie L2 et celle-ci peut être utilisée pour une autre fonction. Ceci est utile lorsque le lecteur est câblé en configuration DEL unique et n'utilise pas la sortie L2.

  Cette option n'est pertinente que pour les lecteurs en configuration Wiegand. Pour une fonction similaire pour les lecteurs RS-485, consulter **Activer les sorties Smart Reader améliorées** (onglet **Lecteur 1/2**)

- **Désactiver le traitement de la DEL verte** : Lorsque cette option est activée, la DEL verte du lecteur de cartes n'est pas activée lorsque la porte est déverrouillée. Lorsqu'il est utilisé avec des lecteurs Wiegand, le module d'expansion du lecteur ne contrôlera pas la sortie L1 et celle-ci pourra être utilisée pour une autre fonction.

  Cette fonctionnalité n'est pas disponible pour les lecteurs intelligents.

- **Désactiver traitement buzzer** : Lorsque cette option est activée, le module d'expansion du lecteur ne contrôle pas le bip du lecteur. Le lecteur émet un bip une fois lorsqu'une carte est lue, mais n'émet pas de bip supplémentaire pour indiquer que l'accès est accordé ou refusé. La sortie BZ peut être utilisée pour une autre fonction.
- **Utiliser expiration carte programmée** : Il s'agit d'une option héritée qui n'a aucun effet.

Options hors ligne

Les options ci-dessous déterminent le fonctionnement module d'expansion du lecteur lorsqu'il est hors ligne avec le contrôleur. Ils n'ont aucun effet sur le comportement en ligne. Veuillez noter qu'aucun événement n'est enregistré lorsque module d'expansion est hors ligne.

- **Détecteur de porte activé** : Lorsque cette option est activée, le module d'expansion du lecteur traite les fonctions du détecteur de porte de l'entrée 1 (port 1) ou 5 (port 2) lorsqu'il est hors ligne.
- **Entrée du détecteur de liaison activée** : Lorsque cette option est activée, le module d'expansion du lecteur traite les fonctions du détecteur de liaison de l'entrée 3 (port 1) ou 7 (port 2) lorsqu'il est hors ligne.
- **REX activé** : Lorsque cette option est activée, le module d'expansion du lecteur traite les fonctions REX de l'entrée 2 (port 1) ou 6 (port 2) lorsqu'il est hors ligne. Cela peut être utilisé pour déverrouiller la porte sans informations d'identification lorsque le module d'expansion est hors ligne.
- **REN activé** : Lorsque cette option est activée, le module d'expansion du lecteur traite les fonctions REN de l'entrée 4 (port 1) ou 8 (port 2) lorsqu'il est hors ligne. Cela peut être utilisé pour déverrouiller la porte sans informations d'identification lorsque le module d'expansion est hors ligne.
- **Activer fonction faisceau sur entrée 3/7** : Lorsque cette option est activée, le module d'expansion du lecteur traite les fonctions du détecteur de faisceau de l'entrée 3 (port 1) ou 7 (port 2) lorsqu'il est hors ligne. L'option **Sense de la porte activé** doit également être utilisée.
- **Inverser contrôle état porte R1/R2** : Si cette option est activée, l'entrée du détecteur de porte (entrée 1 ou 5) est inversée lorsque le module d'expansion du lecteur est hors ligne.
- **Inverser contrôle état détecteur** : Si cette option est activée, l'entrée du détecteur de liaison (entrée 3 ou 7) est inversée lorsque le module d'expansion du lecteur est hors ligne.
- **Inverser l'entrée REX** : Si cette option est activée, l'entrée REX (entrée 2 ou 6) est inversée lorsque le module d'expansion du lecteur est hors ligne.
- **Inverser l'entrée REN** : Avec cette option activée, l'entrée REN (entrée 4 ou 8) est inversée lorsque le module d'expansion du lecteur est hors ligne.
- **Toujours permettre REX** : Lorsque cette option est activée, un module d'expansion du lecteur hors ligne traite toujours le REX et déverrouille la porte, même si la porte est déjà ouverte.

  Pour le fonctionnement en ligne, voir l'option équivalente dans **Programmation | Portes | Entrées**.
- **Recycler temps d'ouverture de porte sur REX** : Il s'agit d'une option héritée qui n'a aucun effet.

  Pour le fonctionnement en ligne, voir l'option équivalente dans **Programmation | Portes | Entrées**.
- **Porte forcée envoie porte ouverte** : Il s'agit d'une option héritée qui n'a aucun effet.

  Pour le fonctionnement en ligne, voir l'option équivalente dans **Programmation | Portes | Entrées**.
- **Recycle temps REX** : Il s'agit d'une option héritée qui n'a aucun effet.

  Pour le fonctionnement en ligne, voir l'option équivalente dans **Programmation | Portes | Entrées**.

Commandes des modules d'expansion des lecteurs manuels

Un clic droit sur l'enregistrement d'un module d'expansion du lecteur dans **Modules d'expansion | Modules d'expansion du lecteur** ouvre un menu avec des commandes manuelles pour cet expandeur.

Contrôle

- **Mise à jour du module** : Met à jour la programmation dans le lecteur expanseur. Pour plus d'informations, consultez la section Mises à jour du module (la page 308).
- **Activer le mode d'installation OSDP** : Sélectionnez cette commande pour mettre le module d'expansion du lecteur en mode d'installation OSDP, ce qui lui permet de s'associer à tout lecteur de carte OSDP connecté qui est également en mode d'installation. Le module d'expansion du lecteur et le lecteur de carte établiront une clé de chiffrement partagée pour permettre une communication par canal sécurisé.

  Pour plus d'informations, consulter la note d'application 254 : Configuration des lecteurs OSDP dans Protege.

Lecteurs intelligents

Les lecteurs intelligents sont des lecteurs non standard connectés Protege GX au système , ce qui leur permet d'exécuter les fonctions normales de contrôle des portes.

Outre les types d'informations d'identification, les lecteurs intelligents peuvent être utilisés pour interpréter une large variété de types de données personnalisées transmises par le port Ethernet embarqué du contrôleur. Par exemple, dans une intégration de reconnaissance de plaques d'immatriculation, chaque lecteur intelligent peut représenter une caméra qui envoie les données de la plaque d'immatriculation au contrôleur via la connexion IP. Par exemple, voir la note d'application 276 : Configuration des types d'informations d'identification dans Protege GX.

En outre, les lecteurs intelligents peuvent être associés au port de lecteur d'un élargisseur de lecteur, représentant des modules tiers connectés à ce port en configuration RS-485. Par exemple, lorsque le **type de réseau Port 1/2** du module d'expansion du lecteur est réglé sur OSDP, deux lecteurs intelligents sont automatiquement créés pour représenter les lecteurs d'entrée et de sortie sur ce port de lecteur. Pour plus d'informations et d'instructions de programmation, voir la Note d'application 254 : Configuration des lecteurs OSDP dans Protege.

Enfin, les lecteurs intelligents sont utilisés dans diverses intégrations tierces pour les dispositifs de verrouillage sans fil, comme Allegion, Aperio, Salto SALLIS et VingCard Visionline. Chaque lecteur intelligent représente un seul verrou sans fil. Pour plus d'informations et d'instructions de programmation, voir la note d'application correspondante.

Chaque lecteur intelligent est un élément sous licence (à l'exception des lecteurs OSDP). Les licences requises varient en fonction du type de connexion tierce requise. Contactez ICT l'assistance clientèle pour plus d'informations.

Lecteurs intelligents | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Configuration

- **Adresse Module d'expansion** : L'adresse du module d'expansion du lecteur intelligent est connecté à .
- **Port expander** : L'adresse du module d'expansion du lecteur intelligent est connecté à . Il peut s'agir d'un port de lecteur ou du port Ethernet du module d'expansion du lecteur

  Le **type de réseau Port 1/2** ou **le type de réseau Ethernet** détermine la fonction du lecteur intelligent. Par exemple, lorsqu'il est connecté à un port de lecteur réglé sur OSDP, le lecteur intelligent représente un lecteur OSDP connecté via RS-485. Lorsqu'il est connecté à un port Ethernet défini comme Tierce Partie Générique le lecteur intelligent représentera un lecteur IP tel qu'une caméra ou un scanner de codes-barres.

  Les lecteurs intelligents ne peuvent pas être connectés aux ports de lecteur réglés sur le fonctionnement Wiegand.

- **Adresse configurée** : L'adresse du module du lecteur intelligent dans le réseau du contrôleur. Cela peut être nécessaire pour correspondre à une adresse spécifique fournie par l'intégration du tiers.

  Pour les lecteurs intelligents connectés par le réseau Ethernet, la commande `SmartReaderPortOffset = true peut être saisie` dans la programmation du module d'expansion du lecteur Dans ce cas, le port IP utilisé par le lecteur intelligent est déterminé par le **port Ethernet** (**Expanders | Modules d'expansion |**

General) plus **l'adresse configurée** ici.

L'adresse maximale configurée disponible pour les lecteurs intelligents est de 248.

Intégration de VingCard Visionline

- **ID de porte VingCard Visionline**: Lorsque ce lecteur intelligent est utilisé pour l'intégration de VingCard Visionline, ce champ vous permet de saisir l'ID de verrouillage que ce lecteur intelligent représentera.

Commandes

- Ce champ est utilisé pour envoyer des commandes de programmation à l'appareil. Il ne doit être utilisé que lorsqu'il est spécifiquement conseillé par la documentation ICT ou le support technique.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Lecteurs intelligents | Lecteur

Différentes options sont disponibles sur cette page en fonction du type de lecteur intelligent à configurer. Toutes les options ne sont pas pertinentes pour toutes les intégrations.

Configuration

- **Format Lecteur Un** : Le type de données d'identification reçues, déterminé par l'appareil ou l'application tiers. En général, pour les lecteurs intelligents, le format est défini comme suit : Custom credential, qui représente un type d'informations d'identification spécifique :
  - Pour les lecteurs intelligents connectés en RS-485, le custom credential est déterminé par le ou les types d'informations d'identification définis dans le type de porte.
  - Pour les lecteurs intelligents connectés en Ethernet, le custom credential est défini dans le champ ci-dessous, intitulé **Types de correspondance des informations d'identification du lecteur**
- **Endroit Lecteur Un** : La location indique au lecteur intelligent si le lecteur connecté est installé du côté de l'entrée ou de la sortie de la porte.
- **Mode Lecteur Un** : Chaque lecteur intelligent peut être utilisé pour l'accès aux portes, le contrôle d'ascenseurs ou le contrôle de partition
- **Porte Lecteur Un** : Lorsque le **mode lecteur un** est défini sur Accès, ce champ définit la porte qui est contrôlée par ce lecteur intelligent. Une même porte peut être contrôlée par plus d'un lecteur intelligent ou d'un port de lecteur (entrée et sortie).

  Tous les types d'informations d'identification requis par le type de porte doivent être saisis dans le **champ Types de correspondance des informations d'identification du** lecteur ci-dessous.
- **Type de clavier Lecteur Un** : Si un identifiant NIP est requis par le type de porte associé, cette option vous permet de définir le type de saisie d'entrée NIP qui est utilisé. L'ARK-501 et les autres entrées NIP doivent être connectés à un port de lecteur avec la même **porte du lecteur 1/2** que le lecteur intelligent.

  Lorsque cette option est définie sur Clavier ACL , le **clavier à utiliser pour NIPs du lecteur 1** demandera un code NIP après la saisie de la première information d'identification. L'utilisateur peut saisir le code NIP et appuyer sur la touche **[FUNCTION]** pour déverrouiller la porte, ou **[ENTER]**pour se connecter au clavier. Pour plus d'informations, consultez **Connexion clavier requiert carte** (**Module d'expansion| Claviers | Options 2**).

  Pour déverrouiller la porte, l'utilisateur **ne doit pas appuyer sur [ENTRÉE]** après avoir saisi son code NIP. La touche **[FONCTION]** doit suivre immédiatement le code NIP. Si l'utilisateur appuie sur **[ENTRÉE]**, le clavier le connectera.
- **Clavier à utiliser pour NIPs du lecteur 1** : Si le **Type de clavier Lecteur** Un est réglé sur le clavier ACL, ce clavier demandera un NIP de l'utilisateur lorsque l'utilisateur saisira ses informations d'identification.

- **Mode d'armement Lecteur Un** : La fonction définie dans ce champ permet aux utilisateurs d'armer et de désarmer des partitions ou de contrôler une sortie ou un groupe de sorties programmables en saisissant leurs informations d'identification. Les utilisateurs doivent saisir la séquence complète d'identifiants plusieurs fois pour activer la fonction.
  - Lorsque le **Mode Lecteur Un**est réglé sur Accès le lecteur d'entrée contrôle la **partition à l'intérieur de la porte** et le lecteur de sortie contrôle la **partition à l'extérieur de la porte** (réglage dans **Programmation | Portes | Général**).
  - Lorsqu'il est réglé sur Contrôle de partitionle lecteur intelligent contrôle le **lecteur d'une zone de contrôle** en dessous.
  - Pour le contrôle des sorties, le lecteur intelligent contrôle la **sortie de fonction du lecteur un / groupe de sorties programmables**.

  L'utilisateur doit avoir coché **Autoriser l'armement multi-badge** dans **Utilisateurs | Niveaux d'accès | Général**. (indépendamment du fait que la fonction soit un contrôle de zone ou de sortie). Si les entrées du secteur peuvent être ouvertes, **Toujours armer en force à l'aide du lecteur de carte** peut être activé dans **Programmation | Secteurs | Options (2)**.
- **Zone de contrôle zone lecteur un** : Lorsque le **mode lecteur un** est réglé sur contrôle de partition, ce champ définit la partition qui est contrôlée par ce lecteur intelligent.
- **Ascenseur lecteur un** : Lorsque le **mode lecteur un** est réglé sur Ascenseur, ce champ définit la cabine d'ascenseur qui est contrôlée par ce lecteur intelligent.
- **Format secondaire lecteur un** : Le format de lecture secondaire est utilisé lorsque le lecteur intelligent ne peut pas décoder une carte lue à l'aide du format primaire. Cette option est utile pour les sites qui utilisent plusieurs types de cartes.
- **Sortie de fonction du lecteur un / Groupe de sorties programmables** : cette sortie programmable ou groupe de sorties programmables peut être activé lorsque l'utilisateur saisit trois fois ses informations d'identification sur un lecteur de cartes. Le mode **d'armement lecteur un** ci-dessus doit être réglé soit sur Basculer sortie de fonction sur 3 lectures ou soit Activer sortie de fonction sur 3 lectures.

Options du Lecteur

- **Permettre la lecture ouverte/déverrouillée** : Cette option n'est pas utilisée. Les portes connectées à des lecteurs intelligents permettent toujours la lecture lorsqu'elles sont ouvertes ou déverrouillées.
- **Sense de la porte activé**: Cette option n'est pas utilisée. La détection de la porte est configurée **dans Programmation | Portes | Entrées**.
- **Entrée Bond Sense activée**: Cette option n'est pas utilisée. La détection de la liaison est **configurée dans Programmation | Portes | Entrées**.
- **REX activé** : Cette option n'est pas utilisée. L'entrée REX est configurée dans **Programmation | Portes | Entrées**.
- **REN activé**: Cette option n'est pas utilisée. L'entrée REN est configurée dans**Programmation | Portes | Entrées** .
- **Envoyer erreurs de format** : Lorsque cette option est activée, le lecteur intelligent enverra des informations détaillées au contrôleur s'il lit une carte avec une erreur de format. Les erreurs de format comprennent le nombre de bits, le nombre d'octets, la parité, la somme de contrôle et les échecs de calcul LRC. Cette information apparaîtra dans le journal des événements.

  L'option **Enregistrer événements du lecteur** doit également être activée.
- **Mode de sabotage du lecteur intelligent**: Cette option n'est pas utilisée.

Options données de cartes

- **Clé de cryptage AES données de cartes** : Les cartes Salto SALLIS et Aperio peuvent être encodées avec les informations du site/de la carte via le client encodeur ICT. Ce champ définit la clé de décryptage afin que Protege GX puisse décrypter les données de ces cartes.

  Pour plus de renseignements, consulter la note d'application correspondante à chaque intégration.

Ce champ définit la clé de cryptage pour ce verrou sans fil uniquement.

- **Lecture des ICT données du secteur non programmé** : L'activation de cette option permet au verrou sans fil de lire les données de secteur de la carte qui ne sont pas programmées par ICT ; toutefois, le verrou ne lira plus les données de secteur programmées par ICT. Ceci est utilisé dans les intégrations Salto SALLIS et Aperio.

N'activez pas cette option si vous souhaitez que le verrou lise à la fois ICT les données du secteur programmé et les données du secteur supplémentaire.

Options misc

- **Désarmer la Partition pour la porte sur accès** : Lorsque cette option est activée, la partition associée sera automatiquement désarmée lorsqu'un utilisateur saisit des informations de connexion valides, à condition que l'utilisateur ait accès pour désarmer la partition. Lorsque le lecteur est utilisé pour le contrôle de portes, la partition derrière la porte sera désarmée. Lorsque le lecteur est utilisé pour le contrôle de partition, la partition de contrôle définie ci-dessus sera désarmée.
- **Permettre l'accès lorsque la Partition est armée** : Lorsque cette option est désactivée (par défaut), les utilisateurs peuvent se voir refuser l'accès à une porte lorsque la partition située derrière celle-ci est armée. L'accès ne leur sera permis que si ils ont la capacité de désarmer la partition.

  Cette option peut être activée pour permettre aux utilisateurs de passer par n'importe quelle porte à laquelle ils ont accès, quel que soit le statut de la partition. Sachez que cela peut facilement provoquer de fausses alarmes car les utilisateurs pourront entrer dans des partitions qu'ils ne peuvent pas désarmer.
- **Désarmer la partition d'usagers sur carte valide** : Cette option permet aux utilisateurs de désarmer une partition personnelle ou un groupe de partitions lorsqu'ils obtiennent l'accès au lecteur. Par exemple, cela pourrait être utilisé pour permettre à un seul lecteur de desservir une rangée de bureaux personnels que les utilisateurs peuvent armer et désarmer individuellement.

Le réglage de la **zone Utilisateur** se fait dans **Utilisateurs | Utilisateurs | Général**, ou un groupe de partitions peut être réglé dans l'onglet **Groupes de partitions**. L'utilisateur doit avoir cette partition disponible dans **Utilisateurs | Niveaux d'accès | Désarmement groupes de partitions**.

- **Journaliser les événements du lecteur** : Activez cette option pour permettre au lecteur d'envoyer des informations sur les erreurs de format au contrôleur (avec l'option **Envoyer les erreurs de format** activée ci-dessus). Les autres événements du lecteur sont toujours envoyés au contrôleur.
- **Interchanger Affichage DEL de serrure**: Cette option n'est pas utilisée.
- **Activer Sortie Niveau d'accès** : Lorsque cette option est activée, la sortie ou le groupe de sorties attribué au niveau d'accès de l'utilisateur sera activé lorsque l'utilisateur aura accès à la porte.

  Les sorties sont affectées dans l'onglet **Sorties** ou **Groupes de sorties** de **Utilisateurs | Niveaux d'accès**. L'option **Accès du lecteur active la sortie** doit être activée dans **Utilisateurs | Niveaux d'accès | Général**, et d'autres configurations sont y sont disponibles.
- **Afficher le détail de la carte lorsqu'elle est invalide** : Lorsque cette option est activée, les données brutes de tout justificatif d'identité non reconnu seront enregistrées dans le journal des événements. Un opérateur peut cliquer avec le bouton droit de la souris sur l'événement "Lire les informations d'identification brutes" pour attribuer l'identification à un utilisateur. L'identifiant sera automatiquement attribuée au type d'identifiant correct en fonction **des types de correspondance des informations d'identification du lecteur** programmés ci-dessous.
- **Activer la fonction faisceau sur l'entrée 3**: Cette option n'est pas utilisée. Vous pouvez définir une entrée de faisceau pour la porte dans **Programmation | Portes | Entrées** .
- **Toujours permettre REX**: Cette option n'est pas utilisée. Voir l'option équivalente dans **Programmation | Portes | Entrées**. .
- **Recycler le temps REX**: Cette option n'est pas utilisée. Voir l'option équivalente dans **Programmation | Portes | Entrées** .

Types de correspondance des informations d'identification du lecteur

Lors de la configuration des lecteurs intelligents connectés au port Ethernet du contrôleur, il est nécessaire de spécifier un ou plusieurs types d'informations d'identification que le lecteur intelligent utilisera. Cela permet au contrôleur d'interpréter les données reçues sur le réseau IP.

Si le **Mode Lecteur un** est réglé sur Accès, les types d'informations d'identification définis ici doivent correspondre à ceux requis par le type de porte. S'il est défini sur contrôle de l'ascenseur ou de la partition, n'importe quel type d'informations d'identification défini ici peut être utilisé pour accéder à l'ascenseur ou contrôler la partition.

Les types d'informations d'identification peuvent être programmés dans **Sites | Types d'informations d'identification**.

Menu Visiteur

Le Protege GX système de gestion des visiteurs (VMS) vous permet de suivre et de contrôler l'accès des visiteurs sur un site. Il fonctionne comme une version spéciale du Protege GX client qui gère l'inscription et la déconnexion des visiteurs.

Dans ce menu, vous pouvez configurer le fonctionnement et l'apparence du client de gestion des visiteurs, les exigences relatives à la procédure d'inscription, les postes de travail qui exécuteront le VMS et les cartes d'accès qui seront remises aux visiteurs.

Le système de gestion des visiteurs est une fonction sous licence. Pour plus d'informations et des instructions de programmation complètes, voir la note d'application 287 : Protege GX Système de gestion des visiteurs.

Modèles

Les paramètres, le contenu et la gestion des visiteurs du client de gestion des visiteurs sont configurés par le biais d'un modèle VMS. Il est possible de créer plusieurs modèles de VMS et de les appliquer à différentes stations de travail, ce qui permet de s'adapter aux besoins de différents points d'enregistrement des visiteurs sur un même site.

Par exemple, la réception et l'entrée de l'entrepôt peuvent exiger des détails différents de la part des visiteurs, ou des bureaux différents sur le même site peuvent avoir des exigences différentes en matière d'image de marque.

Modèles | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Configuration

- **Modèle de carte** : Le modèle de conception utilisé pour imprimer des étiquettes ou des cartes pour visiteurs. Ces informations sont nécessaires au fonctionnement du système de gestion des visiteurs et peuvent inclure des éléments tels que des détails sur le visiteur, des informations d'identification, une photo de l'utilisateur et un code à barres pour une déconnexion rapide. Les modèles de cartes peuvent être programmés dans **Utilisateurs | Éditeur de modèles de cartes**.
- **Mode Checkout** : Règle ce qui arrive à l'enregistrement de l'utilisateur créé pour un visiteur lorsqu'il se déconnecte du VMS.
  - Un utilisateur désactivé enlèvera les informations d'identification de l'enregistrement utilisateur du visiteur.
  - Supprimer l'utilisateur effacera l'enregistrement de l'utilisateur.

  Les visiteurs désactivés ne sont pas réactivés s'ils se connectent à nouveau au VMS : un double des enregistrements sera créé. Toutefois, le visiteur peut être « réactivé » en lui attribuant manuellement des informations d'identification dans Protege GX.

- **Nécessite une validation** : Cette option n'est pas utilisée.
- **Exige une photo** : Si cette option est activée, le VMS se connectera à une webcam ou à une caméra intégrée pour prendre une photo du visiteur pendant le processus d'inscription. Cette photo sera stockée dans l'onglet **Photo** de l'enregistrement de l'utilisateur, et pourra être imprimée sur une étiquette visiteur avec un modèle de carte approprié.
- **Étirer la photo pour la remplir** : Lorsque cette option est activée, les photos des visiteurs seront étirées pour occuper tout l'espace alloué dans le modèle de carte. Le rapport hauteur/largeur ne sera pas préservé, ce qui peut entraîner des images déformées.
- **Télécharger Utilisateur vers Contrôleurs** : Cette option doit être activée pour le bon fonctionnement du VMS.
- **Afficher le dialogue d'impression** : Si ce paramètre est activé, le VMS affichera un dialogue d'impression, permettant à l'utilisateur de sélectionner une imprimante pour l'étiquette visiteur. S'il est désactivé, l'imprimante par défaut de l'ordinateur sera utilisée. Cette option est utile pour les tests car elle vous permet d'annuler l'impression de toute étiquette.
- **Afficher le bouton de maximisation**: Lorsque cette option est activée, l'interface VMS comprendra des boutons d'agrandissement, de réduction et de fermeture. Le logo ICT s'affiche dans le coin supérieur gauche.
- **Maximiser la fenêtre** : En activant cette option, la fenêtre du VMS sera automatiquement maximisée, quels que soient les paramètres du poste de travail.
- **Envoyer courriel des Exceptions** : Cette option n'est pas utilisée.

Se déconnecter

L'une ou l'autre de ces options peut être utilisée.

- **Scanner le code barres** : Le visiteur devra scanner un code à barres sur son étiquette imprimée pour signer son départ. Les codes barres peuvent être ajoutés aux étiquettes dans le modèle de carte.
- **Sélectionnez le nom dans la liste déroulante** : Le visiteur sera invité à sélectionner son nom dans un menu déroulant pour se déconnecter.

Modèles | Pages

- **Pages VMS** : Ajoutez des pages personnalisées supplémentaires au processus de connexion au VMS. Celles-ci peuvent inclure des informations supplémentaires ou des champs personnalisés pour la saisie. Les pages VMS peuvent être créées dans **Visiteur | Pages**.

Modèles | Courriel

- **Opérateurs** : Tous les opérateurs ajoutés à cette section recevront des e-mails chaque fois qu'un visiteur s'inscrit à l'aide de ce modèle VMS.

  Les fonctions de courrier électronique automatisées dans Protege GX exigent qu'un serveur de courrier SMTP soit configuré dans **Global | Paramètres globaux | Paramètres de courrier électronique**. Chaque opérateur doit avoir une adresse électronique entrée sous **Global | Opérateurs**.

Templates | Display

Après avoir apporté des modifications à l'interface VMS, vous devez fermer et redémarrer tous les clients ouverts pour mettre en œuvre les modifications.

- **Images** : Sélectionnez des images pour le fond, le logo, les boutons de connexion/déconnexion et les images de publicité. Cliquez sur le bouton ellipsis **[...]** pour naviguer instantanément vers **Visiteur | Images** afin d'ajouter toute image VMS requise.
  - **Image de fond** : Affiché comme fond pour tous les écrans dans le VMS. Ceci remplacera le réglage de la **couleur de fond**.
  - **Logo** : Affiché au-dessus des boutons de connexion/déconnexion, centré horizontalement.

- **Image de connexion/déconnexion** : Affiché au-dessus du texte dans les boutons de connexion/déconnexion respectivement.
- **Image d'annonce 1-4** : Affiché au bas de l'écran d'accueil du VMS. Cette option permet d'ajouter jusqu'à quatre bannières publicitaires à l'interface VMS. Si plusieurs images publicitaires sont configurées, la page d'accueil fera défiler les différentes images au fil du temps.

- **Couleur** : Entrez le code de la couleur souhaitée sous forme hexadécimale, ou cliquez sur le bouton ellipsis **[...]** pour ouvrir un sélecteur de couleurs.

Pages

Le menu des pages VMS vous permet d'ajouter des pages supplémentaires à la section d'ouverture de session du client VMS. Ces pages peuvent être utilisées pour demander des informations supplémentaires aux visiteurs et afficher des avis importants, tels que des avertissements en matière de santé et d'avertissement.

Les pages VMS peuvent être ajoutées à un modèle VMS dans l'onglet **Visiteur | Modèles | Pages**.

Pages | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Image de fond texte

- **Image de fond** : Le texte saisi ici sera affiché sur cette page du VMS. Cette fonction est utile pour afficher des avis importants à l'intention des visiteurs, tels que les politiques de santé et de sécurité, les coordonnées de contact et d'autres informations sur le site.
- **Afficher le bouton d'accusé de réception sur la page** : Lorsque cette option est activée, les visiteurs devront reconnaître qu'ils ont lu **l'image de fond**avant de pouvoir se connecter. Cela permet de garantir la conformité lorsque les personnes arrivent sur le site.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Pages | Champs personnalisés

Champs

L'ajout de champs personnalisés à une page VMS vous permet de demander des informations supplémentaires aux visiteurs à leur arrivée. Ces informations seront sauvegardées dans l'enregistrement de l'utilisateur qui est créé lorsque le visiteur termine le processus de connexion. Appuyez sur **Ajouter** pour ajouter des champs personnalisés.

Les informations saisies dans les champs personnalisés ne seront pas enregistrées dans la fiche du visiteur, sauf si le même champ est inclus dans un onglet de champ personnalisé. Assurez-vous que chaque champ a l'onglet **Champ personnalisé** défini dans **Utilisateurs | Champs personnalisés | Général**.

Stations de travail

Les postes de travail VMS sont des ordinateurs qui peuvent ouvrir le Protege GX client de gestion des visiteurs. Lorsqu'un opérateur se connecte au client sur ces stations de travail, il a la possibilité d'utiliser le client comme VMS.

Stations de travail | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Configuration

- **Nom de l'ordinateur** : Le nom de la station de travail qui exécutera le VMS. Il doit s'agir d'un ordinateur sur lequel le client Protege GX est installé. Il s'agit généralement d'une station d'entrée ou d'un PC de réception.
- **Modèle de gestion des visiteurs** : Ce champ définit le modèle de VMS qui sera utilisé par cette station de travail. Chaque station de travail peut avoir un modèle de VMS différent.
- **Groupe de registres de l'utilisateur** : Toute fiche de visiteur créée par le VMS à partir de ce poste de travail sera automatiquement affectée à ce groupe de registres. Ceci est utile pour trouver, filtrer et faire des rapports sur les visiteurs d'un site.

Cartes

Les visiteurs qui se connectent au VMS se verront attribuer une carte (ou un justificatif similaire) provenant du groupe de cartes VMS créé ici. Il doit s'agir d'informations d'identification de rechange qui ne sont attribuées à aucun utilisateur. Lorsque le visiteur se déconnecte, la carte VMS n'est plus attribuée et peut être utilisée par un autre visiteur.

Les enregistrements de cartes VMS doivent être créés même si les justificatifs physiques ne sont pas requis, car le VMS ne permettra pas à un visiteur de se connecter sans carte VMS disponible.

Cartes| Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Numéro d'établissement/de carte

- **Numéro d'établissement** : Le numéro de l'établissement ou du site de cette carte de visiteur.
- **Numéro de Carte** : Le numéro de la carte de ce visiteur. Il est utile de créer une séquence de cartes uniques qui seront attribuées aux visiteurs.

  Les cartes VMS sont attribuées aux visiteurs dans l'ordre de leur création, et non par ordre de numéro de carte.
- **Carte en utilisation** : Ce champ est en lecture seulement. Cette case est cochée lorsque cette carte VMS a été attribuée à un visiteur, et décochée lorsque la carte est disponible pour être utilisée.

Images

Les images VMS vous permettent de personnaliser l'apparence du VMS pour répondre aux exigences de l'image de marque de l'entreprise. Vous pouvez ajouter des images de fond, des logos centraux, des icônes de boutons d'entrée/sortie et des bannières publicitaires.

Des images peuvent être ajoutées à un modèle VMS dans l'onglet **Visiteur | Modèles | Affichage**.

Images | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Image

- **Image** : Pour ajouter une image, cliquez sur le bouton**[...]** représentant une ellipse en bas à droite.
  - Si l'image est déjà stockée sur le réseau, sélectionnez l'ellipse **[...]** à côté de **Path** pour naviguer vers l'image. L'image doit être accessible depuis la machine serveur.
  - Si l'image n'existe pas encore, définissez le champ **Source de l'image** pour capturer une nouvelle image. Vous pouvez capturer une image à partir d'une webcam connectée ou d'un bloc de signature Topaz.
  - Lorsque vous avez terminé, cliquez sur **Suivant**.

  Vous pouvez ensuite recadrer l'image si nécessaire :
  - Ajustez la taille et la position du rectangle pointillé pour inclure la section de l'image que vous souhaitez conserver. Cochez l'option **Aspect** pour fixer le rapport d'aspect du rectangle.
  - Pour recadrer l'image, cochez la case **Crop**.
  - Cliquez sur **Ok**.

  L'image complétée s'affiche dans la boîte à images.

  Assurez-vous que l'image est stockée sur le serveur ou à un autre endroit accessible à tous les stations de travail qui exécutent le VMS.

Menu Automatisation

Les fonctions avancées relatives au contrôle et à l'automatisation des constructions se trouvent dans le menu Automatisation.

Automatisation

Les automatisations (également appelées points d'automatisation) sont des "interrupteurs" numériques du système qui peuvent être utilisés pour commander des sorties. Les utilisateurs peuvent activer et désactiver les automatismes à partir d'un clavier, ce qui en fait un moyen pratique de contrôler les dispositifs qui doivent être actionnés régulièrement. Par exemple, une automatisation peut être utilisée pour contrôler l'éclairage extérieur, l'irrigation ou les systèmes CVCA (chauffage, ventilation et climatisation).

Les utilisateurs peuvent activer les automatisations à partir d'un clavier en se connectant et en appuyant sur **[MENU] [5] [5]** . Sélectionner une automatisation et appuyer sur **[1]** pour l'activer pendant une durée définie, **[2]** pour la désactiver et **[3]** pour l'activer indéfiniment. Il est également possible de visualiser et de contrôler les automatisations à partir du menu hors ligne du clavier (voir **Modules d'expansion | Claviers | Options 2**).

Les automatisations sont également utilisés dans l'intégration C-Bus pour connecter les entrées et les sorties aux groupes C-Bus. Cela permet aux entrées et sorties de contrôler les groupes C-Bus et les groupes C-Bus de contrôler les sorties, en intégrant pleinement les systèmes de sécurité et d'automatisation du bâtiment.

Pour plus d'informations et d'instructions de programmation, consulter la note d'application 289 : Intégration C-Bus avec Protege GX et Protege WX.

Automatisation | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Nom d'affichage du clavier** : Le nom qui sera téléchargé vers le contrôleur. Ce dernier sera affiché sur le clavier et dans les rapports des services de surveillance IP. Le clavier ne peut afficher que les 16 premiers caractères du nom. Il doit donc décrire de manière concise l'emplacement physique et la fonction de l'appareil.

Configuration

- **Heure de sortie d'automatisation** : Lorsque l'automatisation est activée, en pressant **[1]** sur un clavier ou par l'intégration du C-Bus, elle reste allumée pendant cette durée (en secondes). Toutes les sorties activées par l'automatisation seront également désactivées après ce délai.

  Lorsque ce champ est défini sur 0, l'automatisation restera active indéfiniment et la sortie ou le groupe de sortie utilisera le temps d'activation défini dans sa propre programmation.

  Dans l'intégration C-Bus, cette option n'est pertinente que dans le cas où un groupe C-Bus contrôle une Protege sortie.

- **Sortie d'automatisation / groupe de sortie**: En fonctionnement normal, cette sortie ou ce groupe de sortie est activé lorsque l'automatisation est activée par le clavier. Il est désactivé lorsque l'automatisation est désactivée.

  Dans l'intégration C-Bus, cette sortie ou ce groupe de sorties peut soit contrôler le groupe C-Bus, soit être contrôlé par le groupe C-Bus. L'utilisation dépend du paramètre de **sortie d'automatisation C-Bus** dans l'onglet **Options**.

- **Code d'application C-Bus** : L'adresse de l'application C-Bus avec laquelle l'automatisation communiquera. Les codes d'application se trouvent dans la documentation du logiciel C-Bus ou du système.
- **Code de groupe C-Bus** : L'adresse du groupe C-Bus avec laquelle l'automatisation communiquera. Les codes de groupe se trouvent dans la documentation du logiciel C-Bus ou du système.
- **Service C-Bus** : Le service utilisé pour la communication entre Protege GX et l'interface réseau C-Bus. Le service est configuré dans **Programmation | Services** avec le **type de service** défini sur C-Bus.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Automatisation | Options

Options

- **Affichage de l'état inversé** : Il s'agit d'une option héritée qui n'a aucun effet.
- **Activer les fonctions d'automatisation C-Bus** : Lorsque cette option est activée, l'automatisation contrôle ou est contrôlée par le groupe C-Bus attribué.

  Cette option est nécessaire pour que l'automatisation commence à communiquer avec le C-Bus.
- **Sortie d'automatisation C-Bus** : Lorsque cette option est activée, l'automatisation contrôlera le groupe C-Bus attribué. Lorsque cette option est désactivée, l'automatisation sera contrôlée par le groupe C-Bus attribué.
- **Utiliser l'état des sorties dans la fonction C-Bus**: Lorsque cette option est activée, l'automatisation modifie ou transmet le statut de sa sortie d'automatisation ou de son groupe de sorties plutôt que le statut de l'automatisation elle-même.
- **C-Bus fonctionne sur la bordure montante** : Le traitement C-Bus s'active sur la bordure montante d'un changement d'état de la sortie/entrée, c'est-à-dire le passage de off à on. Si l'option est désactivée, le processus C-Bus ignore ces changements.
- **C-Bus fonctionne sur la bordure descendante** : Le traitement C-Bus s'active sur la bordure descendante d'un changement d'état de la sortie/entrée, c'est-à-dire le passage de on à off. Si l'option est désactivée, le processus C-Bus ignore ces changements.

Fonctions programmables

Les fonctions programmables sont des processus automatisés spéciaux qui peuvent être programmés dans le système. En général, ces processus ont un déclencheur - comme l'activation d'une sortie ou une valeur de donnée atteignant un nombre défini - qui amène le contrôleur à activer le processus.

Ces fonctions présentent une grande variété d'applications pour le contrôle et l'automatisation. Par exemple, vous pouvez les utiliser pour armer une partition en fonction de l'état d'une sortie, faire fonctionner une série complexe de dispositifs chaque fois qu'une porte spécifique est déverrouillée, régler la température en fonction du nombre de personnes présentes dans une partition ou déverrouiller les portes en cas d'alarme incendie.

Pour des exemples de programmation avancée utilisant des fonctions programmables, consulter les notes d'application suivantes :

- Note d'application 208 : Programmation d'évacuation d'urgence et de verrouillage
- Note d'application 278 : Comptage des partitions par niveau d'accès dans Protege GX
- Note d'application 282 : Programmation des mécanismes de porte dans Protege GX
- Note d'application 307 : Programmation d'un interrupteur d'homme mort dans Protege GX
- Note d'application 334 : Programmation des tours de garde dans Protege GX

Démarrage et arrêt des fonctions programmables

Un clic droit sur un registre de fonction programmable dans **Automatisation | Fonctions programmables** ouvre un menu avec des commandes manuelles pour cette fonction programmable.

Contrôle

- **Début** : Démarre la fonction programmable sur le contrôleur. Le processus s'exécutera lorsque les conditions de déclenchement seront remplies.
- **Arrêter** : Arrête la fonction programmable sur le contrôleur. Le contrôleur génère un message d'état de santé indiquant que la fonction a été arrêtée.

Avant d'apporter des changements à une fonction programmable, vous devez d'abord **arrêter** la fonction. Lorsque les changements ont été téléchargés dans le contrôleur, vous devez **relancer** la fonction. Si cette procédure n'est pas suivie, le contrôleur risque de ne pas mettre en œuvre correctement les modifications.

Fonctions programmables | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.
- **Supporter commandes manuelles** : Lorsque cette option est activée, un opérateur disposant des autorisations appropriées peut cliquer avec le bouton droit de la souris sur la fonction programmable pour commencer ou arrêter le processus.

Type

- **Type** : Le type de fonction programmable détermine le type d'opération qu'elle va effectuer. Chaque type de fonction dispose de différents onglets de programmation et d'options disponibles.

- **Aucun** : La fonction n'effectuera aucune action.
- **Contrôle logique** : Contrôle une sortie ou un groupe de sorties en fonction de l'état d'une ou deux sorties de déclenchement. Plusieurs opérations logiques sont disponibles.
- **Contrôle de partition** : Arme ou désarme une partition ou un groupe de partitions en fonction de l'état d'une sortie.
- **Paquet de chaleur toit** : Gère un système CVC avec jusqu'à 4 niveaux de chauffage et de refroidissement et deux niveaux de déshumidification.
- **Étage temporaire** : Gère un système thermique d'air avec chauffage et refroidissement à un seul niveau.
- **Valeur comparer** : Compare deux valeurs de données et active les sorties en fonction de leurs quantités relatives. Par exemple, ceci peut être utilisé pour contrôler les circuits d'éclairage en fonction des entrées des détecteurs de lumière du jour.
- **Sortie d'ondulation** : Active une série de sorties dans un modèle d'ondulation basé sur une seule sortie de déclenchement. Ceci peut être utilisé pour installer des appareils à courant important et des circuits d'éclairage multiples.
- **Contrôle de portes** : Verrouille ou déverrouille une porte ou un groupe de portes en fonction de l'état d'une sortie. Peut également être utilisé pour déclencher une évacuation d'urgence ou un verrouillage des portes.
- **Porte virtuelle** : Permet à des entrées et sorties définies d'agir comme une porte sans programmation d'un registre de porte. Utile pour les portes qui n'ont pas de lecteurs et qui ne sont pas surveillées par un module d'expansion du lecteur mais qui nécessitent un certain traitement de la porte.
- **Entrée suit Sortie** : Contrôle une entrée en fonction de l'état d'une sortie. Peut être utilisé pour activer des alarmes basées sur l'état d'une sortie.
- **Contrôle d'ascenseurs** : Verrouille ou déverrouille une cabine d'ascenseur ou un groupe d'ascenseurs en fonction de l'état d'une sortie.
- **Enregistrer compteur** : Augmente ou diminue une valeur de données en fonction de l'état d'une entrée.
- **Moyenne** : Calcule la moyenne d'un maximum de 8 valeurs de données d'entrée et l'écrit dans une valeur de données de sortie. Par exemple, cela peut être utilisé pour prendre une moyenne de plusieurs détecteurs de température.
- **Sortie variable comparer** : Compare une seule valeur de données d'entrée avec une série de valeurs de données à « point fixe ». Lorsque la valeur d'entrée atteint chaque point fixe, une valeur de données de sortie est mise à jour avec une quantité connue.

- **Mode** : Lorsque cette option est réglée sur Normal, la fonction programmable s'exécute chaque fois que ses conditions de déclenchement sont réunies. Si le contrôleur est redémarré, la fonction reprend. Lorsqu'elle est réglée sur Exécutez une fois seulement, la fonction programmable s'exécute une fois lorsque les conditions de déclenchement sont remplies, puis s'arrête.
- **État** : Il s'agit d'une option héritée qui n'a aucun effet.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Contrôle logique

Une fonction de contrôle logique évalue l'état d'une ou deux sorties et applique une opération logique pour contrôler l'état d'une autre sortie ou d'un groupe de sorties (appelé la sortie de contrôle). Une gamme de programmation logique est disponible, y compris le suivi/suivi inversé (avec des options continues et pulsées), OR, AND, NOR, NAND et XOR.

Configuration

- **Mode de fonction logique** : Ce champ détermine le type d'opération logique qui sera utilisé pour contrôler l'état de la sortie de contrôle ou du groupe de sorties.

  Le mode de contrôle peut être continu (options 0 à 1, 6 à 10) ou pulsé (options 2 à 5). Les modes de contrôle continu vérifient l'état de la sortie toutes les 30 secondes. Si l'état n'est pas correct, la fonction réaffirme le contrôle et active/désactive la partition. Les modes de déclenchement pulsé ou par front d'impulsion ne modifient l'état de sortie que lorsque les conditions de déclenchement sont réunies, et ne l'affectent pas à d'autres moments..

  Les options de contrôle disponibles sont les suivantes :

  - **0 - Suivre et tester la première sortie** : La sortie de contrôle de partition suit en permanence l'état de la première sortie. Lorsque la première sortie est ON, la sortie de contrôle est ON. Lorsque la première sortie est OFF, la sortie de contrôle est OFF.
  - **1 - Suivre et tester la première sortie inversée** : La sortie de contrôle de partition suit en permanence l'état de la première sortie de manière inversée. Lorsque la première sortie est ON, la sortie de contrôle est OFF. Lorsque la première sortie est OFF, la sortie de contrôle est ON.
  - **2 - Suivre Impulsion sur première sortie** : La sortie de contrôle suit la bordure montante de la première sortie. Lorsque la première sortie est ON, la sortie de contrôle passe sur ON.
  - **3 - Suivre impulsion sur première sortie inversée** : La sortie de contrôle suit la bordure montante de la première sortie de manière inversée. Lorsque la première sortie est ON, la sortie de contrôle passe sur OFF.
  - **4 - Suivre impulsion à partir première sortie** : La sortie de commande est activée sur la bordure descendante de la première sortie. Lorsque la première sortie est OFF, la sortie de contrôle passe sur ON.
  - **5 - Suivre impulsion à partir première sortie inversée** : La sortie de commande est désactivée sur la bordure descendante de la première sortie. Lorsque la première sortie est OFF, la sortie de contrôle passe sur OFF.
  - **6 - Suivre logique OR** : La fonction effectue une opération logique OR pour déterminer l'état de la sortie de contrôle. Si la première ou la deuxième sortie est ON, la sortie de contrôle est ON. Si la première et la deuxième sortie sont toutes deux OFF, la sortie de contrôle est OFF.

Première sortie	Deuxième sortie	Sortie de contrôle
✓	✓	✓
✓	✗	✓
✗	✓	✓
✗	✗	✗

  - **7 - Suivre logique AND** : La fonction effectue une opération logique AND pour déterminer l'état de la sortie de contrôle. Si la première et la deuxième sortie sont toutes deux ON, la sortie de contrôle est ON. Si la première ou la deuxième sortie est OFF, la sortie de contrôle est OFF.

Première sortie	Deuxième sortie	Sortie de contrôle
✓	✓	✓

Première sortie	Deuxième sortie	Sortie de contrôle
✓	✗	✗
✗	✓	✗
✗	✗	✗

- **8 - Suivre logique NOR** : La fonction effectue une opération logique NOR pour déterminer l'état de la sortie de contrôle. Si la première ou la deuxième sortie est ON, la sortie de contrôle est OFF. Si la première et la deuxième sortie sont toutes deux OFF, la sortie de contrôle est ON.

Première sortie	Deuxième sortie	Sortie de contrôle
✓	✓	✗
✓	✗	✗
✗	✓	✗
✗	✗	✓

- **9 - Suivre logique NAND** : La fonction effectue une opération logique NAND pour déterminer l'état de la sortie de contrôle. Si la première et la deuxième sortie sont toutes deux ON, la sortie de contrôle est OFF. Si la première ou la deuxième sortie est OFF, la sortie de contrôle est ON.

Première sortie	Deuxième sortie	Sortie de contrôle
✓	✓	✗
✓	✗	✓
✗	✓	✓
✗	✗	✓

- **10 - Suivre logique XOR** : La fonction effectue une opération logique XOR pour déterminer l'état de la sortie de contrôle. Si la première et la deuxième sortie sont dans le même état (toutes deux ON ou OFF), la sortie de contrôle est OFF. Si la première et la deuxième sortie sont dans des états différents (une ON, une OFF), la sortie de contrôle est ON.

Première sortie	Deuxième sortie	Sortie de contrôle
✓	✓	✗
✓	✗	✓
✗	✓	✓
✗	✗	✗

- **Première sortie à vérifier** : La première sortie qui est utilisée pour définir l'état de sortie de contrôle. Ce champ doit être défini pour tous les modes de fonctions logiques.
- **Deuxième sortie à vérifier** : La deuxième sortie qui est utilisée pour définir l'état de sortie de la partition. Ce champ n'est pas nécessaire pour les modes de fonction logique 0-5.

- **Sortie / groupe de sorties à contrôler** : Cette sortie ou ce groupe de sorties est la sortie de contrôle de la fonction de contrôle logique. Cette option est activée et désactivée en fonction des états des première et deuxième sorties et du **mode de fonction logique** sélectionné ci-dessus.

  Vous pouvez définir soit une sortie, soit un groupe de sorties. Si les deux sont réglés, seule la sortie sera contrôlée par la fonction.

Contrôle de partition

Les fonctions programmables de contrôle de partition peuvent armer et désarmer une partition ou un groupe de partitions (appelé contrôle de partition) en fonction de l'état d'une sortie. Vous pouvez configurer un contrôle continu (la fonction vérifie toujours l'état de la sortie et maintient l'état de la partition) ou un contrôle par impulsions (la fonction ne contrôle l'état de la partition que lorsque la sortie change d'état).

Cela peut être utilisé pour des applications telles que l'armement d'une partition après une période d'inactivité ou l'utilisation d'un interrupteur à clé pour désarmer une partition.

Configuration

- **Fonction de partition** : Ce champ détermine comment le contrôle de partition ou le groupe de partition sera contrôlé en fonction de l'état de la sortie.

  Le mode de contrôle peut être continu (options 0 à 1) ou pulsé (options 2 à 5). Les modes de contrôle continu vérifient l'état de la partition toutes les 30 secondes. Si l'état n'est pas correct, la fonction réaffirme le contrôle et arme/désarme la partition. Les modes de déclenchement pulsé ou par front d'impulsion ne modifient l'état de la partition que lorsque les conditions de déclenchement sont réunies, et ne l'affectent pas à d'autres moments..

  - **0 - La partition suit l'état de la sortie** : Le contrôle de partition suit en permanence l'état de la sortie. Lorsque la sortie est ON, le contrôle de partition est ARMÉ. Lorsque la sortie est OFF, le contrôle de partition est DÉSARMÉ.
  - **1 - La partition suit l'état de la sortie inversé** : Le contrôle de partition suit en permanence l'état de la sortie de manière inversée. Lorsque la sortie est ON, le contrôle de partition est DÉSARMÉ. Lorsque la sortie est OFF, le contrôle de partition est ARMÉ.
  - **2 - La partition arme sur sortie allumée** : Le contrôle de partition est armé sur le front montant de l'état de sortie. Lorsque la sortie S'ACTIVE, le contrôle de partition est ARMÉ.
  - **3 - La partition désarme sur sortie allumée** : Le contrôle de partition est désarmé sur le front montant de l'état de sortie. Lorsque la sortie S'ACTIVE, le contrôle de partition est DÉSARMÉ.
  - **4 - La partition arme sur sortie éteinte** : Le contrôle de partition est armé sur le front descendant de l'état de sortie. Lorsque la sortie SE DÉSACTIVE, le contrôle de partition est ARMÉ.
  - **5 - La partition désarme sur sortie éteinte** : Le contrôle de partition est armé sur le front descendant de l'état de sortie. Lorsque la sortie SE DÉSACTIVE, le contrôle de partition est DÉSARMÉ.
- **Sortie à vérifier** : La sortie qui est utilisée pour définir l'état de contrôle de la partition.
- **Partition / Groupe de partitions à contrôler** : Cette partition ou ce groupe de partition est le contrôle de partition de la de la fonction programmable. Celui-ci est armé ou désarmé en fonction de l'état de la **Sortie à vérifier** et de la **Fonction de partition** sélectionnée ci-dessus.

  Vous pouvez définir soit une partition, soit un groupe de partition. Si les deux sont réglés, seule la partition sera contrôlée par la fonction.

Système de chauffage du toit

Ce type de fonction programmable gère un système de climatisation de type système de chauffage sur le toit (RTHP) avec jusqu'à quatre niveaux de chauffage et de refroidissement et jusqu'à deux niveaux de déshumidification Cette fonction surveille la température et l'humidité (via les canaux d'entrée analogiques) et active les sorties de chauffage, de refroidissement et de déshumidification de l'unité de climatisation pour atteindre la température et l'humidité de consigne.

Chaque fonction programmable de ce type peut gérer l'ensemble du système de climatisation d'un bâtiment. Vous pouvez programmer plusieurs versions de cette fonction qui s'exécutent sous certaines conditions. Par exemple, vous pouvez avoir des fonctions alternatives pour le jour et la nuit en fonction du calendrier d'occupation prévu du bâtiment. Une programmation efficace peut augmenter considérablement l'efficacité énergétique du bâtiment.

La programmation de cette fonction nécessite une compréhension des systèmes CVC à plusieurs niveaux.

Configuration

- **Niveau de refroidissement**: Le nombre d'étapes de refroidissement gérés par le RTHP.
- **Étape de chauffage**: Le nombre d'étapes de chauffage gérés par le RTHP.
- **Étapes de déshumidification**: Le nombre d'étapes de déshumidification gérées par le RTHP. Seule une déshumidification en 1 ou 2 étapes peut être programmée.
- **Commande toujours le ventilateur (circuler)**: Lorsque cette option est activée, la sortie / le groupe de sortie **du ventilateur principal** sera toujours activé pour faire circuler l'air.
- **Extinction rapide du feu**: Lorsque cette option est activée, en cas d'incendie, le RTHP s'arrête rapidement pour empêcher la circulation du fumée. Cela se produit lorsque **l'entrée de sortie de contrôle d'incendie** est activée.
- **Étape de dépannage rapide désactivée**: Lorsque cette option est activée, le RTHP s'arrête rapidement en cas de défaillance. Cela se produit lorsque l'entrée **de sortie par défaut** est activée.
- **Retard entre les étapes du refroidissement**: Lorsque le RTHP augmente le refroidissement de l'étape 1 à 4, il s'agit du délai (en secondes) entre l'activation de chaque étape.
- **Retard entre les étapes du chauffage**: Lorsque le RTHP augmente le chauffage de l'étape 1 à 4, il s'agit du délai (en secondes) entre l'activation de chaque étape.
- **Retard entre les étapes de déshumidification**: Lorsque le RTHP fait passer la déshumidification de l'étape 1 à l'étape 2, il s'agit du délai (en secondes) entre l'activation de chaque étape.
- **Retard de l'étape du registre de l'économiseur** : Le délai (en secondes) avant l'activation de l'économiseur (volet).
- **Temps de refroidissement de l'air frais**: La durée pendant laquelle le système va tenter d'utiliser l'air frais pour le refroidissement. Si le point de consigne de refroidissement n'est pas atteint dans ce délai, le refroidissement régulier sera activé.
- **Délai d'arrêt entre les étapes de refroidissement**: Lorsque le RTHP réduit le refroidissement de l'étape 4 à 1, il s'agit du délai (en secondes) entre la désactivation de chaque étape.
- **Retard de l'arrêt entre les étapes de chauffage**: Lorsque le RTHP réduit le chauffage du niveau 4 au niveau 1, il s'agit du délai (en secondes) entre la désactivation de chaque niveau.
- **Délai de désactivation entre les étapes de déshumidification**: Lorsque le RTHP réduit la déshumidification du niveau 2 au niveau 1, il s'agit du délai (en secondes) entre la désactivation de chaque niveau.

Variables de données

- **Valeur du point de consigne de la chaleur**: Cette valeur de données détermine la température à laquelle le RTHP chauffera l'espace. Elle est comparée au **Registre variable données température de l'espace** pour déterminer si un chauffage est nécessaire.
- **Valeur des données du point de consigne de refroidissement**: Cette valeur détermine la température à laquelle le RTHP refroidira l'espace. Elle est comparée au **Registre variable données température de l'espace** pour déterminer si un refroidissement est nécessaire.

- **Valeur des données du point de consigne de l'humidité**: Cette valeur de données détermine le niveau d'humidité qui déclenchera le RTHP pour commencer à diminuer l'humidité. La valeur d'humidité actuelle est déterminée par le **registre variable de données d'humidité de l'espace**.
- **Valeur des données de l'hystérésis de la chaleur**: Cette valeur de données est ajoutée à la **valeur de données du point de consigne de la chaleur** pour définir une plage acceptable de chauffage. Cela permet au chauffage d'aller légèrement au-delà du point de consigne (hystérésis), l'empêchant d'osciller entre la bande neutre et le mode chauffage.
- **Valeur des données de l'hystérésis de refroidissement**: Cette valeur de données est ajoutée à la **valeur de données du point de consigne de refroidissement** pour définir une plage acceptable de refroidissement. Cela permet au refroidissement d'aller légèrement au-delà du point de consigne (hystérésis), l'empêchant d'osciller entre la bande neutre et les modes de refroidissement.
- **Valeur des données de l'hystérésis d'humidité**: Cette valeur est soustraite ou ajoutée à la **valeur du point de consigne d'humidité**, selon que l'humidité a déjà dépassé le point de consigne. Cela permet au processus de déshumidification de ne fonctionner que lorsque l'humidité est à un niveau défini au-dessus du point de consigne, et de conduire la déshumidification en dessous du point de consigne, évitant ainsi toute oscillation.
- **Valeur des données du point de consigne de réchauffement**: Si le point de consigne de réchauffement n'est pas égal à 0, le système vérifiera la température interne par rapport au point de consigne de réchauffement lorsque le RTHP démarre. Si la température interne est inférieure au point de consigne de chauffage, le système ferme le volet d'air frais et fait fonctionner le chauffage pour atteindre le point de consigne de chauffage dans le temps le plus court possible. Une fois que le point de consigne de chauffage est atteint, l'unité fonctionnera normalement.
- **Valeur des données du point de consigne de rafraîchissement**: Si le point de consigne de refroidissement de l'air frais n'est pas égal à 0, le système vérifiera la température de l'air frais lorsqu'une demande de refroidissement existe et modulera les volets pour permettre un refroidissement naturel. Le système reste en mode de refroidissement naturel pendant la durée définie par la **durée de refroidissement de l'air frais**.
- **Valeur des données de demande de l'étape 1 à 4** : Les valeurs des données de demande sont utilisées pour calculer l'étape de chauffage ou de refroidissement nécessaire. La valeur actuelle **des données d'erreur de sortie** est confrontée à chaque valeur pour déterminer le niveau de chauffage ou de refroidissement nécessaire. Par exemple, si l'erreur de l'installation dépasse la valeur de demande de l'étape 3, le RTHP activera la troisième étape de refroidissement ou de chauffage.
- **Valeur des données du mode actuel**: Cette valeur de données est définie par la fonction pour vous permettre de contrôler l'état actuel du système RTHP. Vous pouvez associer la valeur des données à une variable, visualiser la variable sur un plan d'étage ou une page du statut, et comparer la valeur avec le tableau des statuts (consultez la page 354) pour déterminer l'état actuel du système RTHP.
- **Valeur des données d'erreur de l'usine**: L'erreur de l'installation est la différence entre la température actuelle (**Variable de données de température spatiale**) et la valeur du point de consigne de chauffage ou de refroidissement. La fonction écrit cette valeur de données au fur et à mesure que la température change, et l'utilise pour calculer **L'erreur de sortie**. Cette valeur de données peut être associée à une variable et affichée sur un plan d'étage pour être utilisée dans le réglage des points de consigne de chauffage, de refroidissement et de demande.
- **Valeur des données d'erreur de sortie**: L'erreur de sortie est le résultat d'un calcul personnalisé de la boucle PID. Elle est dérivée de l'erreur de l'usine et des termes intégraux calculés. Ces données sont comparées aux points de consigne de la demande pour déterminer le niveau de chauffage ou de refroidissement nécessaire.
- **Valeur des données de consigne de la fraîcheur du volet**: Ce champ définit la valeur par défaut du registre **variable de données du volet de l'économiseur** ci-dessous. Ceci définit la position normale du volet de l'économiseur lorsque le RTHP n'est ni en mode réchauffement ni en mode refroidissement libre. La position du volet détermine le volume d'air frais qui est aspiré dans le bâtiment.
- **Registre de variable de données d'humidité de l'espace**: Cette valeur de données enregistre l'humidité actuelle à l'intérieur de l'espace contrôlé par le RTHP. La valeur est actualisée par un capteur d'humidité connecté à un canal d'entrée analogique.
- **Registre variable des données de température de l'espace** : Cette valeur de données enregistre la température actuelle à l'intérieur de l'espace contrôlé par le climatiseur. La valeur est actualisée par un thermomètre connecté à un canal d'entrée analogique.

- **Registre variable des données de température de l'air frais**: Cette valeur de données enregistre la température actuelle de l'air frais à l'extérieur de l'espace contrôlé par le conditionneur d'air. La valeur est actualisée par un thermomètre connecté à un canal d'entrée analogique, généralement situé dans l'entrée d'air frais. Si la température extérieure est suffisamment fraîche, le registre de l'économiseur pourrait s'ouvrir pour permettre à l'air frais de refroidir le bâtiment.
- **Registre des données variables du volet de l'économiseur**: Cette valeur de données contrôle la position du volet d'air frais. Cette valeur de données est connectée à un canal de sortie analogique qui commande le volet physique. La valeur par défaut est la valeur de consigne de la fraîcheur **du volet** ci-dessus.

  Lorsque le refroidissement est nécessaire et que l'air frais extérieur est froid, le volet s'ouvre pour permettre à l'air frais d'entrer directement dans le système. Lorsque le système nécessite un chauffage ou que l'air extérieur est chaud, le volet se ferme pour limiter le flux d'air frais.

Système de chauffage du toit | Sorties

Ventilateur principal

- **Sortie du ventilateur principal / groupe de sortie**: Cette sortie est utilisée pour commander les ventilateurs du système de climatisation. Il est activé 30 secondes avant que le RTHP ne commence tout processus de chauffage, de refroidissement ou de déshumidification.

Activé

- **Entrée de sortie activée**: Cette sortie est contrôlée par la fonction. Lorsque cette sortie est activée, cette fonction exécute et contrôle le système RTHP. Lorsque cette sortie est désactivée, la fonction ne marchera pas.

  Par exemple, cette sortie peut être liée à un programme afin que le RTHP ne fonctionne que lorsque le bâtiment est occupé. Une fonction distincte peut être exécutée aux moments où le bâtiment n'est pas occupé.

  S'il n'y a pas de sortie définie, cette fonction marchera de façon continue.

Défaut

- **Entrée de sortie par défaut**: Cette sortie est surveillée par la fonction et doit être utilisée pour indiquer lorsqu'il y a un défaut dans le système RTHP. Si l'option **Arrêt rapide par défaut** est activée, lorsque cette sortie est activée, le RTHP s'arrête dans le délai le plus court possible pour éviter d'endommager le système.

Contrôle des incendies

- **Entrée de sortie du contrôle d'incendie**: Cette sortie est contrôlée par la fonction et doit être utilisée pour indiquer la présence d'un incendie dans le bâtiment. Si l'option **Arrêt rapide d'incendie** est activée, lorsque cette sortie est activée, le RTHP s'arrête et interrompt la climatisation jusqu'à ce que l'alarme incendie soit supprimée.

Étape de refroidissement

- **Étape de refroidissement une à quatre sorties / groupe de sorties**: Ces sorties et groupes de sorties sont utilisés pour contrôler chaque étage de refroidissement du système RTHP. Par exemple, lorsque la deuxième étape de refroidissement est requise, la sortie **Étape de refroidissement deux / groupe de sortie** est activée.

Étape de chauffage

- **Étape de chauffage une à quatre sorties / groupe de sortie**: Ces sorties et groupes de sorties sont utilisés pour contrôler chaque étape de chauffage du système RTHP. Par exemple, lorsque la deuxième étape de chauffage est requise, la sortie **Étape de chauffage deux / groupe de sortie** est activée.

Étape de déshumidification

- **Étape de déshumidification une-deux sortie / groupe de sortie**: Ces sorties et groupes de sorties sont utilisés pour contrôler chaque étape de déshumidification du système RTHP. Par exemple, lorsque la deuxième étape de déshumidification est requise, la sortie / le groupe de sortie**s de la deuxième étape de déshumidification** est activée. Ceux-ci sont généralement connectés aux vannes de réchauffage des gaz chauds situées dans l'unité RTHP.

État du système de chauffage du toit

La valeur de la **Valeur des données du mode actuel** (onglet du**système de chauffage du toit**) indique l'état actuel du système RTHP. Pour surveiller l'état du système, associez une variable à cette valeur de données et visualisez-la sur un plan d'étage ou sur une page du statut

Valeur	Statuts	Description
0	État inactif du RTHP	La fonction programmable est à l'arrêt et aucun traitement n'est en cours.
1	RTHP en attente du signal de démarrage	L'entrée de sortie **Activée** n'est pas activée. La fonction est inactive.
2	Vérification du chauffage RTHP	Si le RTHP est programmé pour entrer dans un état de réchauffement au début du fonctionnement, il vérifie d'abord la température pour voir si la température interne actuelle est inférieure au point de consigne de réchauffement. Si c'est le cas, le RTHP passe en mode de réchauffement.
3	Espace de réchauffement du RTHP	En mode de chauffage, le RTHP fonctionne à pleine capacité pour amener l'espace au-dessus du point de consigne de chauffage le plus rapidement possible. Lorsque la température atteint ce niveau, le système fonctionne normalement.
4	Processus de bande neutre du RTHP	Aucun chauffage, refroidissement ou déshumidification n'est nécessaire. Le RTHP attendra une condition qui est en dehors des points de consigne.
5	Sur appel pour le réchauffement des locaux	La température ambiante est inférieure au point de consigne du chauffage et la fonction de démarrage du processus de chauffage est active. Cela activera les étapes nécessaires pour amener la température au point de consigne du chauffage.
6	Sur appel pour le refroidissement des locaux	La température des locaux est supérieure au point de consigne de refroidissement et la fonction de démarrage du processus de refroidissement est active. Cela activera les étapes nécessaires pour ramener la température au point de consigne de refroidissement.
7	Sur appel pour le refroidissement des locaux à l'air frais	La température des locaux est supérieure au point de consigne de refroidissement et l'air extérieur est inférieur au point de consigne de refroidissement de l'air libre. Le RTHP fera osciller l'économiseur d'air frais pour refroidir l'espace en utilisant l'entrée d'air frais. Cette fonction restera active jusqu'à ce que la température soit inférieure au point de consigne de refroidissement. Si le refroidissement naturel ne parvient pas à atteindre le point de consigne dans le **temps de refroidissement de l'air frais**, le mode 6 sera activé.
8	Arrêt de l'étape de chauffage	Les étages de chauffage s'éteignent progressivement en raison de l'atteinte du point de consigne.
9	Arrêt de l'étape de refroidissement	Les étapes de refroidissement sont désactivées progressivement en raison de l'atteinte du point de consigne.

Valeur	Statuts	Description
10	Déshumidification Refroidissement plus Réchauffage	Une déshumidification est nécessaire et le point de consigne actuel est supérieur au point de consigne de refroidissement. L'étape de déshumidification sera activée pour réduire l'humidité.
11	Passage à la déshumidification	Le processus de déshumidification est en transition entre les besoins de déshumidification et le refroidissement.
12	Chauffage de déshumidification	Une déshumidification est nécessaire et le point de consigne actuel est inférieur au point de consigne du chauffage. L'étape de déshumidification sera activée pour réduire l'humidité, ainsi qu'une étape de chauffage.
13	Désactivation du chauffage de déshumidification	Les étapes de déshumidification et de chauffage sont désactivées parce que l'humidité a été maîtrisée ou que le point de consigne de refroidissement (de l'autre côté du réglage de la bande neutre) a été atteint.
14	Désactivation du refroidissement de la déshumidification	Les étapes de déshumidification et de refroidissement sont désactivées parce que l'humidité a été réduite ou que le point de consigne de chauffage (de l'autre côté du réglage de la bande neutre) a été atteint.
15	Déshumidification désactivée	Les étapes de déshumidification sont désactivés car l'humidité a atteint le point de consigne et la déshumidification n'est plus nécessaire.
16	Fermeture du RTHP	Le RTHP est en train d'effectuer un arrêt ordonné des étapes actuellement activées et des commandes du ventilateur.
17	Condition de défaillance	Une condition de défaillance s'est activée et a provoqué l'arrêt du RTHP.
18	Situation d'incendie	Une alarme incendie a été activée et a provoqué l'arrêt du RTHP.

Étage temporaire

Ce type de fonction programmable permet de gérer un système thermique au sol (ou de l'air) avec un chauffage et un refroidissement à une étape. La fonction utilise les entrées de température du conduit et du sol, et peut gérer les modes de ventilation avant et arrière.

Sorties

- **Sortie / groupe de sorties programmables du conduit du ventilateur** : Cette sortie ou ce groupe de sorties programmables est utilisé pour activer le conduit ventilateur. Il est activé 30 secondes avant tout chauffage ou refroidissement.

  La direction du ventilateur (avant ou arrière) est déterminée par les sorties de ventilateur vers avant et de ventilateur vers l'arrière ci-dessous. Si un signal de mise en marche du ventilateur n'est pas nécessaire, les sorties avant et arrière doivent être utilisées pour commander les contacteurs appropriés.
- **Sortie pour activer cette fonction** : Cette sortie est contrôlée par la fonction. Lorsque cette sortie est activée, cette fonction s'exécute et contrôle le système thermique. Lorsque cette sortie est désactivée, la fonction n'est pas exécutée.

  Par exemple, cette sortie pourrait être liée à un horaire afin que le système thermique ne fonctionne que lorsque le bâtiment est occupé. Une fonction distincte peut être exécutée aux moments où le bâtiment n'est pas occupé.

  S'il n'y a pas de sortie définie, cette fonction est exécutée en continu.
- **Sortie pour activer fermeture par défaut** : Cette sortie est surveillée par la fonction et doit être utilisée pour indiquer la présence d'une anomalie dans le système thermique. Lorsque cette sortie est activée, le système thermique s'arrête dans les plus brefs délais pour éviter d'endommager le système.
- **Sortie pour activer arrêt d'incendie** : Cette sortie est contrôlée par la fonction et doit être utilisée pour indiquer la présence d'un incendie dans le bâtiment. Lorsque cette sortie est activée, le système thermique s'arrête et cesse la climatisation jusqu'à ce que l'alarme incendie soit levée.
- **Sortie / groupe de sorties programmables de refroidissement** : Cette sortie ou ce groupe de sorties programmables est activé lorsqu'il y a un besoin de refroidissement actif. Ne définissez pas ce champ si le système thermique n'est pas équipé d'un compresseur de refroidissement.
- **Sortie / groupe de sorties programmables de chauffage** : Cette sortie ou ce groupe de sorties programmables est activé lorsqu'il y a un besoin de chauffage actif. Il est uniquement activé dans le sens avant.
- **Sortie / groupe de sorties programmables activer vers l'avant le ventilateur** : Cette sortie ou ce groupe de sorties programmables est utilisé pour entraîner le ventilateur dans le sens avant. Lorsque la température au sol est inférieure au point de consigne, le ventilateur avant est utilisé pour faire circuler l'air du conduit à travers l'élément chauffant et vers le sol.
- **Sortie / groupe de sorties programmables renverser le ventilateur** : Cette sortie ou ce groupe de sorties programmables est utilisé pour entraîner le ventilateur dans le sens arrière. Lorsque la température au sol est supérieure au point de consigne, le ventilateur arrière est utilisé pour faire circuler l'air chaud du sol vers l'extérieur par le conduit.
- **Sortie pour contrôler chauffage manuel** : Cette sortie est contrôlée par la fonction. Lorsqu'elle est activée, le ventilateur fonctionne en mode avant (chauffage) quelle que soit la température du sol.

  Si les sorties de chauffage manuel et de refroidissement manuel sont toutes deux activées, le ventilateur fonctionne en mode avant.
- **Sortie pour contrôler refroidissement manuel** : Cette sortie est contrôlée par la fonction. Lorsque cette fonction est activée, le ventilateur fonctionne en mode arrière (refroidissement), quelle que soit la température du sol.

  Si les sorties de chauffage manuel et de refroidissement manuel sont toutes deux activées, le ventilateur fonctionne en mode avant.

Variables de données

- **Sortie variable données d'entrée de température d'étage** : Cette valeur de donnée enregistre la température actuelle au niveau du sol. La valeur est actualisée par un thermomètre connecté à un canal d'entrée analogique.
- **Sortie variable donnée d'entrée température de conduit** : Cette valeur de données enregistre la température actuelle au niveau du conduit. La valeur est actualisée par un thermomètre connecté à un canal d'entrée analogique. Il est généralement situé dans le conduit en aval du conduit ventilateur (en mode avant).
- **Valeur de données point de consigne d'étage** : Cette valeur de donnée détermine la température souhaitée au niveau du sol. Cette valeur est comparée à la température du sol pour déterminer si un chauffage ou un refroidissement est nécessaire, ainsi que la direction du ventilateur.
- **Valeur de données hystérésis d'étage** : Cette valeur de donnée est ajoutée ou soustraite à la **Valeur de données point de consigne d'étage** pour définir une plage acceptable de chauffage ou de refroidissement. Cela permet au système thermique d'aller légèrement au-delà du point de consigne (hystérésis), ce qui l'empêche d'osciller entre différents modes.
- **Valeur de données point de consigne de conduit** : Cette valeur de donnée définit la température maximale pour le capteur du conduit. Elle est comparée à la température du conduit pour contrôler le chauffage de l'air du conduit.
- **Valeur de données hystérésis de conduit** : Cette valeur de donnée est ajoutée à la **Valeur de données point de consigne de conduit** pour définir une plage acceptable de chauffage. Cela permet au système thermique d'aller légèrement au-delà du point de consigne (hystérésis), ce qui l'empêche d'osciller entre différents modes.
- **Valeur de données mode actuel** : Cette valeur de donnée est définie par la fonction pour vous permettre de surveiller l'état actuel du système thermique. Vous pouvez associer la valeur des donnée à une variable, visualiser la variable sur un plan d'étage ou une page du statut, et comparer la valeur avec le tableau des statuts (consultez ci-dessous) pour connaître le statut actuel du système thermique.

Status de l'étage temporaire

La valeur de la **Valeur de données mode actuel** indique l'état actuel du système thermique. Pour surveiller l'état du système, associez une variable à cette valeur de données et visualisez-la sur un plan d'étage ou une page du statut.

Valeur	État	Description
0	Condition d'inactivité de l'étage temporaire	La fonction programmable est arrêtée et aucun traitement n'est en cours.
1	Étage temporaire en attente du signal de départ	La **Sortie pour activer cette fonction** n'est pas activée. La fonction est inactive.
2	Étage temporaire en attente de vérification	Le système thermique au sol détermine s'il doit fonctionner en mode manuel ou automatique.
3	Étage temporaire processus de zone morte	Aucun chauffage ou refroidissement n'est nécessaire. Le système thermique attend une condition qui se situe en dehors des points de consigne.
4	Chauffage d'étage	La température du sol est inférieure au point de consigne et le processus de chauffage est actif. Cela active le ventilateur et le chauffage avant qui sont nécessaires pour amener la température au point de consigne du sol.

Valeur	État	Description
5	Refroidissement d'étage	La température du sol est supérieure au point de consigne et le processus de refroidissement est actif. Cela active le ventilateur arrière et (le cas échéant) le compresseur de refroidissement pour ramener la température en dessous du point de consigne.
6	Chauffage avant manuel	La sortie de chauffage manuel est activée et le système thermique est en mode chauffage, quelle que soit la température du sol.
7	Refroidissement arrière manuel	La sortie de refroidissememt manuel est activée et le système thermique est en mode refroidissement, quelle que soit la température du sol.
8	Étage temporaire en cours d'arrêt	Le système thermique termine un arrêt ordonné des sorties actuellement activées et des commandes du ventilateur.
9	Condition d'anomalie	Une condition d'anomalie a été activée et a provoqué l'arrêt du système thermique.
10	Condition d'incendie	Une condition d'alarme incendie a été activée et a provoqué l'arrêt du système thermique.
11	Délai du mode	Le mode est passé du mode manuel au mode automatique ou inversement et la fonction est entrée dans une période de délai.

Valeur comparer

Ce type de fonction programmable vous permet de comparer deux valeurs de données (une valeur d'entrée et une valeur de consigne) et d'activer des sorties lorsque l'une est supérieure ou inférieure à l'autre. Cela pourrait servir à activer des circuits d'éclairage en fonction de capteurs de lumière du jour ou à activer des sorties spécifiques en fonction du nombre d'utilisateurs dans une partition.

Configuration

- **Sortie pour activer cette fonction** : Lorsque cette sortie est activée, la fonction compare les valeurs et active les sorties qui en résultent. Lorsque cette sortie est désactivée, la fonction de comparaison de valeurs ne fonctionne pas. Si aucune sortie n'est définie ici, la fonction sera toujours exécutée.
- **Activer la sortie / groupe de sorties programmables lorsque le point de consigne est dépassé** : La sortie haute ou le groupe de sorties est activé lorsque la valeur des données d'entrée est supérieure à la valeur des données du point de consigne (une fois les réglages de l'hystérésis pris en compte). Il est désactivé lorsque la valeur des données d'entrée est égale ou inférieure au point de consigne.
- **Activer la sortie / groupe de sorties programmables lorsque en dessous du point de consigne** : La sortie basse ou le groupe de sorties est activé lorsque la valeur des données d'entrée est inférieure à la valeur des données du point de consigne (une fois les réglages de l'hystérésis pris en compte). Il est désactivé lorsque la valeur des données d'entrée est égale ou supérieure au point de consigne.
- **Registre variable données d'entrée analogique** : Cette valeur de données est la valeur d'entrée variable qui est comparée. Elle peut provenir d'un canal d'entrée analogique mesurant une quantité telle que la température, le courant ou détails de l'opérateur.
- **Chronométreur d'hystérésis**: Cette option n'est pas utilisée.
- **Valeur de données point de consigne** : Cette valeur de données est la valeur d'entrée variable qui est comparée.
- **Valeur de données hystérésis** : Cette valeur de données fixe est ajoutée et soustraite au point de consigne pour définir une plage de valeurs. Les sorties haute et basse ne sont activées que lorsque la valeur d'entrée est en dehors de cette plage. Par exemple, lors de la surveillance du courant, cela peut être utilisé pour définir une bande de courants acceptables, de sorte que les sorties ne soient activées que lorsque le courant dépasse cette bande.
- **Valeur de données de temps d'hystérésis** : Cette valeur de données définit un temps de retard (par intervalles de 500 millisecondes) avant que la fonction ne réagisse à tout changement d'état. Si un changement de la valeur d'entrée déclenche un changement de sortie, il ne se produira pas avant que cette période ne se soit écoulée. Les changements de sortie multiples seront espacés d'un même intervalle. Si la valeur d'entrée revient dans les limites acceptables dans ce délai, les sorties ne changeront pas.

  Par exemple, la valeur de la donnée de temps d'hystérésis peut être réglée sur 10, c'est-à-dire 5 secondes (en utilisant **l'option Valeur** prédéfinie). Si la valeur d'entrée passe d'une valeur basse à une valeur haute, la sortie basse sera désactivée après cinq secondes. Après cinq secondes supplémentaires, la sortie haute sera activée. Cependant, si la valeur d'entrée revient à une quantité faible dans les cinq secondes, aucune sortie ne changera.

Sortie d'ondulation

Cette fonction programmable permet d'activer ou de désactiver une série de sorties lorsqu'une sortie de déclenchement change d'état. Elle est idéale pour mettre en scène des appareils à fort courant ou des circuits d'éclairage multiples.

Configuration

- **Sortie pour activer cette fonction**: Lorsque cette sortie est activée, la fonction active les sorties contrôlées en séquence (vers le haut). Lorsque cette sortie est désactivée, la fonction désactive les sorties contrôlées en séquence (vers le bas).
- **Sortie de l'étage 1 à 8 / groupe de sortie programmable**: Ces champs définissent jusqu'à 8 sorties ou groupes de sorties programmable qui sont contrôlés par cette fonction. Lorsque la **Sortie pour activer cette fonction** est activée, la fonction active ces sorties en séquence de 1 à 8, séparées par le **temps d'ondulation de l'étape intermédiaire**. Lorsque la **sortie permettant d'activer cette fonction** est désactivée, la fonction désactive ces sorties en séquence inverse de 8 à 1, séparées par le **temps d'ondulation de l'étape intermédiaire**.
- **Temps d'ondulation de l'étape intermédiaire**: Lorsque les sorties contrôlées sont intensifiées, il s'agit du délai entre chaque activation de sortie (en secondes).
- **Temps d'ondulation de l'arrêt de l'étape intermédiaire**: Lorsque les sorties contrôlées sont abaissées, il s'agit du délai entre chaque désactivation de sortie (en secondes).

Contrôle de portes

La fonction programmable de contrôle de portes vous permet de verrouiller et de déverrouiller une porte ou un groupe de portes en fonction de l'état d'une sortie. Elle permet également d'appliquer les états de déverrouillage incendie (évacuation d'urgence) et de verrouillage sur une porte ou un groupe de portes.

Configuration

- **Mode de fonction de porte** : Ce champ définit la manière dont la porte ou le groupe de portes répond à l'état de la sortie, c'est-à-dire si la sortie active ou désactive le mode de contrôle de porte sélectionné. Cette relation entre l'état de la sortie et la fonction de contrôle de portes s'appelle le déclencheur.

  Par exemple, avec le réglage 4 - sortie suivre impulsion off, le déclencheur est activé lorsque la sortie passe sur OFF. Lorsque le déclencheur est activé, la porte peut se déverrouiller, déverrouiller le loquet, se déverrouiller pour incendie ou se verrouiller en fonction du mode de contrôle de porte. Lorsque le déclencheur est désactivé, la porte peut se verrouiller ou canceller le confinement.

  Le mode de contrôle peut être continu (options 0-1) ou pulsé (options 2-5). Les modes de contrôle continu vérifient l'état de la porte toutes les 30 secondes. Si l'état n'est pas correct, la fonction réaffirme le contrôle et met à jour l'état de la porte. Les modes de déclenchement pulsé ou par front d'impulsion ne modifient l'état de la porte que lorsque les conditions de déclenchement sont remplies, et ne l'affectent pas le reste du temps.

  Les options sont :

  - **0 - suivre et tester sortie** : La porte suit en permanence l'état de la sortie. Lorsque la sortie est sur ON, le déclencheur est activé. Lorsque la sortie est sur OFF, le déclencheur est OFF.
  - **1 - suivre et tester sortie inversé** : La porte suit en permanence l'état de la sortie de manière inversée. Lorsque la sortie est sur ON, le déclencheur est OFF. Lorsque la sortie est sur OFF, le déclencheur est ON.
  - **2 - suivre impulsion sur sortie** : La porte suit le front montant de l'état de la sortie. Lorsque la sortie est mise sous tension, le déclencheur s'active.
  - **3 - suivre impulsion sur sortie inversé** : La porte suit le front montant de l'état de la sortie de manière inversée. Lorsque la sortie est mise sur ON, le déclencheur passe sur OFF.
  - **4 - sortie suivre impulsion off** : La porte suit le front descendant de l'état de la sortie. Lorsque la sortie est mise sur OFF, le déclencheur passe sur ON.
  - **5 - sortie suivre impulsion off inversée** : La porte suit le front descendant de l'état de la sortie de manière inversée. Lorsque la sortie est mise sur OFF, le déclencheur passe sur OFF.
- **Mode de contrôle de porte** : Ce champ définit l'action de la porte ou du groupe de portes lorsque le déclencheur est activé ou désactivé.
  - **0 - Imiter menu de déverrouillage** : Lorsque le déclencheur est activé, la porte est déverrouillée pendant la durée du **Temps d'activation du verrouillage** (**Programmation | Portes | Sorties**). Cela a le même effet que de déverrouiller la porte via le REX ou les informations d'identification. Lorsque le déclencheur est désactivé, la porte est verrouillée.

    La porte ne se déverrouille que temporairement, même si le **Mode de fonction de porte** est réglé sur un mode continu.
  - **1 - déverrouiller porte verrouillée** : Lorsque le déclencheur est activé, le loquet de la porte est déverrouillé. Lorsque le déclencheur est désactivé, la porte est verrouillée.
  - **2 - Déverrouiller porte de contrôle d'incendie** : Lorsque le déclencheur est activé, le loquet de la porte est déverrouillé indéfiniment. Cette commande a priorité sur les autres fonctions qui pourraient maintenir la porte verrouillée, comme le statut de la partition. Lorsque le déclencheur est désactivé, la porte revient à son statut précédent.
  - **3 - Verrouillage de portes (Refuser Entrée + Sortie)** : Lorsque le déclencheur est activé, la porte est verrouillée et l'accès est refusé à tous les utilisateurs dans les deux sens. Lorsque le déclencheur est désactivé, le verrouillage est supprimé et la porte revient à son état précédent.
  - **4 - Verrouillage de portes (permettre entrée)** : Lorsque le déclencheur est activé, la porte est verrouillée. L'accès est uniquement autorisé dans la direction de l'entrée (y compris le REN). Lorsque le déclencheur est désactivé, le verrouillage est supprimé et la porte revient à son état précédent.

- **5 - Verrouillage de portes (permettre sortie)** : Lorsque le déclencheur est activé, la porte est verrouillée. L'accès est uniquement autorisé dans la direction de la sortie (y compris le REX). Lorsque le déclencheur est désactivé, le verrouillage est supprimé et la porte revient à son état précédent.
- **6 - Verrouillage de portes (Permettre Entrée + Sortie)** : Lorsque le déclencheur est activé, la porte est verrouillée. L'accès est autorisé dans les deux directions (y compris le REX et le REN). Lorsque le déclencheur est désactivé, le verrouillage est supprimé et la porte revient à son état précédent.

- **Sortie à vérifier** : Cette sortie est utilisée pour contrôler la porte ou le groupe de portes. La relation entre la sortie et l'état de la porte est déterminée par le **Mode de fonction de porte** ci-dessus.
- **Porte / Groupe de portes à contrôler** : Cette porte ou ce groupe de portes est commandé par la fonction programmable. Si une porte et un groupe de portes sont sélectionnés, seule la porte est contrôlée.

Porte virtuelle

Cette fonction vous permet de configurer des entrées et des sorties définies pour qu'elles fonctionnent comme une porte. Cette option est utile lorsque certains aspects du traitement des portes sont nécessaires mais qu'aucun lecteur ou port d'extension de lecteur n'est disponible. Par exemple, les portes roulantes sans lecteur peuvent nécessiter des verrous, un bouton REX et un contrôle de l'ouverture. Il est également possible de lier une porte virtuelle à une porte normale, ce qui permet de commander deux portes à partir du même lecteur.

Note : Une autre façon d'obtenir le même effet consiste à créer un enregistrement de porte qui n'est associé à aucun module d'expansion du lecteur Cette méthode permet d'obtenir la plupart des caractéristiques des portes habituelles, tandis que la méthode des fonctions programmables est plus limitée. Cependant, la méthode alternative exige une licence de porte pour chaque nouvel enregistrement de porte.

Configuration

- **Demande pour sortir de l'entrée** : Lorsque cette entrée est ouverte, un REX (demande de sortie) est envoyé à la porte virtuelle. La fonction programmable active alors la sortie verrou et autorise l'accès.

  La fonction programmable inverse l'entrée REX par défaut. Par conséquent, le **type de contact** dans **Programmation | Entrées | Options** doit être réglé sur l'opposé du câblage physique. Si l'entrée REX est câblée normalement ouverte, le **type de contact** doit être réglé sur Normalement fermé. Si l'entrée REX est câblée normalement fermée, elle doit être réglée sur Normalement ouverte .

- **Entrée état de porte** : Cette entrée représente le contact de porte ou l'entrée de position de porte pour la porte virtuelle. Lorsque l'entrée est ouverte, la porte est considérée comme ouverte. Lorsque l'entrée est fermée, la porte est considérée comme fermée.
- **Entrée porte laissée ouverte à contrôler** : Cette entrée est ouverte lorsque la porte est restée ouverte trop longtemps (comme défini par le **temps d'ouverture maximum** ci-dessous). Il peut être programmé avec une partition et un type d'entrée pour lui permettre de signaler les événements de porte laissée ouverte à partir de la porte virtuelle (au lieu de l'entrée de dérangement disponible sur une porte normale).

  Il convient d'utiliser une entrée virtuelle à cette fin plutôt qu'une entrée physique.

- **Entrée de porte forcée pour le contrôle** : Cette entrée est ouverte lorsque la porte est forcée en position ouverte. Il peut être programmé avec une partition et un type d'entrée pour lui permettre de signaler les événements de forçage de porte à partir de la porte virtuelle (au lieu de l'entrée de trouble disponible sur une porte normale).

  Il convient d'utiliser une entrée virtuelle à cette fin plutôt qu'une entrée physique.

- **Heure de déverrouillage** : La durée (en secondes) pendant laquelle le verrou sera activé lorsque la porte virtuelle est déverrouillée.
- **Temps d'ouverture maximal** : La durée (en secondes) pendant laquelle la porte virtuelle peut être ouverte avant de passer à l'état de porte ouverte.
- **Sortie de verrouillage / groupe de sorties programmables** : Cette sortie ou ce groupe de sorties contrôle le verrou physique de la porte.
- **Sortie d'alarme / Groupe de sorties programmables** : Cette sortie ou ce groupe de sorties est activé lorsque la porte virtuelle entre dans une condition d'ouverture ou de forçage. Il doit s'agir d'un signal sonore ou d'une autre sortie audible/visible qui peut avertir les utilisateurs de fermer la porte. Il est désactivé lorsque la porte est fermée.

  Les options requises **Activer la sortie d'alarme** doivent être activées ci-dessous.

- **Activer sortie d'alarme sur porte laissée ouverte** : Lorsque cette option est activée, la **sortie d'alarme / le groupe de sorties programmable** sera activé(e) lorsque la porte reste ouverte trop longtemps.
- **Pulser sortie d'alarme sur porte laissée ouverte** : Par défaut, la sortie d'alarme est activée en permanence lorsque la porte est laissée ouverte. Lorsque cette option est activée, elle s'allume et s'éteint par intervalles de 5 secondes.

L'activation de la sortie d'alarme sur une porte laissée ouverte doit également être activée.

- **Activer sortie d'alarme sur porte forcée**: Lorsque cette option est activée la **sortie d'alarme / le groupe** de sorties programmables d'alarme est activé(e) lorsque la porte est forcée.
- **Pulser sortie d'alarme sur porte forcée** : Par défaut, la sortie d'alarme est activée en permanence lorsque la porte est forcée en position ouverte. Lorsque cette option est activée, elle s'allume et s'éteint par intervalles de 5 secondes.

L'activation de la sortie d'alarme en cas de porte forcée doit également être activée.

- **Enregistre événement d'entrée de porte laissée ouverte** : Il s'agit d'une option héritée qui n'a aucun effet. Un événement est toujours enregistré lorsque la porte virtuelle est laissée ouverte trop longtemps.
- **Enregistrer événement d'entrée de porte forcée**: Il s'agit d'une option héritée qui n'a aucun effet. Un événement est toujours enregistré lorsque la porte virtuelle est forcée.
- **Lien vers la porte** : Cette option vous permet d'associer la porte virtuelle à une porte ordinaire. Chaque fois que la porte normale est déverrouillée par un accès, un clavier ou un opérateur, la porte virtuelle est également déverrouillée. Chaque fois que la porte virtuelle est déverrouillée par le REX, la porte normale est également déverrouillée. Cela permet de commander deux portes à partir d'un seul lecteur.

Entrée suit Sortie

Cette fonction permet à une entrée d'être déclenchée par une sortie. Ceci est utile pour générer des alarmes basées sur l'état d'une sortie plutôt que sur une entrée physique.

Configuration

- **Entrée suit Sortie** : Cette entrée de contrôle est ouverte lorsque la **sortie à suivre** est activée, et fermée lorsque la sortie est désactivée. En programmant l'entrée dans une partition avec un type d'entrée, elle peut être utilisée pour le signalement d'alarmes.

  Il convient d'utiliser une entrée virtuelle plutôt qu'une entrée physique.

- **Sortie à suivre** : Cette sortie est surveillée par la fonction et contrôle l'état de l'entrée de contrôle. Ceci peut être défini sur n'importe quelle sortie physique ou virtuelle qui doit déclencher un état d'alarme.
- **Enregistrer événements d'entrée** : Lorsque cette option est activée, un événement est généré chaque fois que l'entrée change d'état en raison de cette fonction programmable. Lorsque cette option est désactivée, aucun événement n'est généré.

Contrôle d'ascenseurs

Ce type de fonction programmable est utilisé pour verrouiller et déverrouiller les étages d'un groupe d'ascenseurs spécifique en fonction de l'état d'une sortie. Elle permet également d'appliquer l'état de déverrouillage incendie (évacuation d'urgence) aux étages.

Configuration

- **Mode de fonction d'ascenseur** : Ce champ définit la manière dont le groupe d'étages répond à l'état de la sortie, c'est-à-dire si la sortie active ou désactive le mode contrôle d'ascenseur sélectionné. Cette relation entre l'état de la sortie et la fonction de contrôle d'ascenseurs s'appelle le déclencheur.

  Par exemple, avec le réglage 4 - sortie suivre impulsion off, le déclencheur est activé lorsque la sortie passe sur OFF. Lorsque le déclencheur est activé, les étages peuvent se déverrouiller, déverrouiller le loquet ou se déverrouiller pour incendie selon le **Mode contrôle d'ascenseur**. Lorsque le déclencheur est désactivé, les étages se verrouillent.

  Le mode de contrôle peut être continu (options 0-1) ou pulsé (options 2-5). Les modes de contrôle continu vérifient l'état de l'étage toutes les 30 secondes. Si l'état n'est pas correct, la fonction réaffirme le contrôle et met à jour l'état de l'étage. Les modes de déclenchement pulsé ou par front d'impulsion ne modifient l'état de l'étage que lorsque les conditions de déclenchement sont remplies, et ne l'affectent pas le reste du temps.

  Les options sont :

  - **0 - suivre et tester sortie** : L'étage suit en permanence l'état de la sortie. Lorsque la sortie est sur ON, le déclencheur est activé. Lorsque la sortie est sur OFF, le déclencheur est OFF.
  - **1 - suivre et tester sortie inversé** : Les étages suivent en permanence l'état de la sortie de manière inversée. Lorsque la sortie est sur ON, le déclencheur est OFF. Lorsque la sortie est sur OFF, le déclencheur est ON.
  - **2 - suivre impulsion sur sortie** : Les étages suivent le front montant de l'état de la sortie. Lorsque la sortie est mise sous tension, le déclencheur s'active.
  - **3 - suivre impulsion sur sortie inversé** : Les étages suivent le front montant de l'état de la sortie de manière inversée. Lorsque la sortie est mise sur ON, le déclencheur passe sur OFF.
  - **4 - sortie suivre impulsion off** : Les étages suivent le front descendant de l'état de la sortie. Lorsque la sortie est mise sur OFF, le déclencheur passe sur ON.
  - **5 - sortie suivre impulsion off inversée** : Les étages suivent le front descendant de l'état de la sortie. Lorsque la sortie est mise sur OFF, le déclencheur passe sur OFF.
- **Mode contrôle d'ascenseur** : Ce champ définit l'action que prend le groupe d'étages lorsque le déclencheur est activé ou désactivé.
  - **0 - Imiter menu de déverrouillage** : Lorsque le déclencheur est activé, le groupe d'étages est déverrouillé pendant le **Temps de jeton** (ci-dessous). Lorsque le déclencheur est désactivé, le groupe d'étages est verrouillé.

    Le groupe d'étages ne se déverrouille que temporairement, même si le **Mode de fonction d'ascenseur** est réglé sur un mode de suivi continu.

  - **1 - déverrouiller ascenseur verrouillé** : Lorsque le déclencheur est activé, le groupe d'étages déverrouille le loquet. Lorsque le déclencheur est désactivé, le groupe d'étages est verrouillé.
  - **2 - déverrouiller ascenseur pour contrôle d'incendie** : Lorsque le déclencheur est activé, le groupe d'étages déverrouille le loquet indéfiniment. Cette commande a priorité sur les autres caractéristiques qui pourraient verrouiller les étages, comme le statut de la partition. Lorsque le déclencheur est désactivé, le groupe d'étages revient à son état précédent.
- **Sortie à vérifier** : Cette sortie permet de contrôler le groupe d'étages. La relation entre la sortie et l'état de l'étage est définie par le **Mode de fonction de porte** ci-dessus.
- **Groupe d'ascenseurs** : Le groupe d'étages contrôlé par cette fonction est verrouillé/déverrouillé par les cabines d'ascenseurs de ce groupe d'ascenseurs. Par exemple, une fonction programmable peut être utilisée pour déverrouiller les loquets des étages dans les ascenseurs publics mais pas dans les ascenseurs de maintenance.

- **Groupe d'étages** : Les étages qui sont contrôlés par cette fonction.
- **Temps de jeton** : Si le **Mode contrôle d'ascenseur** est réglé sur 0 - Imiter menu de déverrouillage, les étages sont déverrouillés pendant cette durée (en secondes) lorsque le déclencheur est activé.

Registre compteur

La fonction de registre compteur est utilisée pour incrémenter ou décrémenter une valeur de données en fonction de l'état d'une entrée. Par exemple, vous pouvez mettre en place une valeur de données enregistrant le nombre de fois qu'un contact de porte est ouvert afin d'estimer le nombre total de personnes passant par là sur une certaine période.

Configuration

- **Appliquer au compteur**: Cette entrée est contrôlée par la fonction programmable. Lorsque l'entrée change d'état, le compteur est incrémenté ou décrémenté.

  Pour compter les activations d'une entrée ou d'autres fonctions, cette fonction pourrait être associée à une fonction d'entrée suivant les sorties programmables pour déclencher les activations d'entrée requises.

- **Registre compteur** Cette valeur de données est incrémentée ou décrémentée par la fonction, selon des options définies ci-dessous.

  La valeur des données du compteur peut stocker une valeur maximale de 65 535. Chaque fois que le compte dépasse cette valeur, le **Registre de débordement** est incrémenté de 1. Par conséquent, le nombre total peut être calculé comme suit : Total = Compteur + (dépassement de capacité x 65 535).
- **Registre de débordement**: Cette valeur de données est incrémentée de 1 à chaque fois que la valeur de données du compteur déborde. Chaque 1 dans la valeur des données de débordement représente un compte de 65 535.
- **Incrément sur entrée ouverte**: Lorsque cette option est activée, le compteur s'incrémente à chaque fois que l'entrée s'ouvre.
- **Incrément sur entrée fermée**: Lorsque cette option est activée, le compteur s'incrémente à chaque fois que l'entrée se ferme.
- **Enregistrer les événements du compteur:** Lorsqu'elle est activée, la fonction enregistre un événement pour chaque incrément.
- **Incrément sur entrée ouverte**: Lorsque cette option est activée, le compteur se décrémente à chaque fois que l'entrée s'ouvre.

  La valeur des données ne peut pas stocker de valeurs négatives. Si le compte passe en dessous de zéro, le décompte « reviendra » jusqu'à 65 535.

- **Décrément sur entrée fermée**: Lorsque cette option est activée, le compteur se décrémente à chaque fois que l'entrée se ferme.

  La valeur des données ne peut pas stocker de valeurs négatives. Si le compte passe en dessous de zéro, le décompte « reviendra » jusqu'à 65 535.

- **Pas de débordement de registre**: Lorsque cette option est activée, la valeur des données du compteur ne débordera pas dans la valeur des données de débordement. Cela signifie que le compte a un total maximum de 65 535.
- **Réinitialiser la sortie**: Lorsque cette sortie est activée, les valeurs du compteur et des données de débordement sont mises à zéro. Lorsque cela se produit, un événement est enregistré avec le compte total.

  Par exemple, pour enregistrer le total hebdomadaire d'une valeur de données, vous pouvez créer une sortie virtuelle avec un **calendrier d'activation** qui l'active une fois par semaine.

Moyenne

Cette fonction programmable prend la moyenne d'un maximum de huit valeurs de données d'entrée et écrit ce nombre dans une valeur de données de sortie. Par exemple, cette fonction peut être utilisée pour surveiller une pièce équipée de plusieurs capteurs de température, la moyenne étant utilisée pour déterminer le chauffage ou le refroidissement souhaité.

Configuration

- **Temps de mise à jour** : Le temps (en secondes) entre les mises à jour de la valeur des données de sortie.
- **Sortie** : La valeur de données dans laquelle la moyenne sera écrite.

  La sortie de cette fonction est toujours un nombre entier, et sera arrondie vers le haut ou vers le bas si nécessaire.

- **Moyenne 1 à 8** : Les valeurs des données d'entrée qui sont utilisées pour calculer la moyenne.

Sortie variable comparer

Ce type de fonction vous permet de comparer une valeur de données d'entrée à une série de points de consigne et de définir une valeur de données de sortie spécifique en fonction du résultat. La valeur d'entrée est comparée à chaque valeur de comparaison (jusqu'à 16) et la valeur de sortie correspondante est copiée dans la valeur des données de sortie.

Configuration

- **Temps de mise à jour** : Le temps (en secondes) entre les mises à jour de la valeur des données de sortie.
- **Entrée** : La valeur des données d'entrée est contrôlée par la fonction et comparée aux valeurs de comparaison ci-dessous.
- **Sortie** : La valeur des données de sortie est définie par la fonction en fonction de la valeur de **sortie 1-16** ci-dessous.

Comparer

- **Comparer les valeurs 1-16** : Il s'agit d'une série de valeurs de données du point de consigne auxquelles la valeur d'entrée est comparée. La valeur de comparaison dont la valeur d'entrée est la plus proche détermine quelle valeur de sortie (ci-dessous) est définie pour la sortie.

  Par exemple, réglez la valeur de **comparaison 1** sur 5 et la valeur de **comparaison 2** sur 10 . Lorsque la valeur d'entrée est inférieure, égale ou juste supérieure à 5, **la valeur de sortie 1** est utilisée. Lorsque la valeur d'entrée est supérieure à 5 (7 ou plus), égale à 10 ou supérieure à 10,, **la valeur de sortie 2**est utilisée.

  La valeur d'entrée peut dépasser la valeur de comparaison inférieure d'un certain montant avant que la valeur de sortie ne change. Cela dépend de l'intervalle total entre les deux valeurs de comparaison consécutives. Il est recommandé de tester l'opération avant de l'utiliser.

- **Valeur de sortie 1-16** : Il s'agit d'une série de valeurs de données du point de consigne qui déterminent la valeur de la sortie. Pour chaque valeur de comparaison, il doit y avoir une valeur de sortie. Lorsque la valeur d'entrée correspond à une valeur de comparaison particulière, la valeur de sortie correspondante est copiée dans la valeur des données de sortie.

Valeurs de données

Les valeurs de données (parfois appelées registres) sont utilisées par le système pour stocker des valeurs numériques afin de surveiller les entrées analogiques, de contrôler les sorties analogiques ou pour utilisation dans des fonctions programmables. Par exemple, chaque canal d'un module d'expansion analogique peut être représenté par une valeur de donnée qui stocke une quantité telle que le courant ou la tension. Les valeurs de données peuvent également être associées à des variables, ce qui permet de mettre la valeur à l'échelle par une équation linéaire, de la surveiller et de la contrôler.

Plusieurs types de fonctions programmables surveillent ou manipulent spécifiquement les valeurs de données, comme la valeur comparer, l'enregistrer compteur, la moyenne et la sortie variable comparer. Cela vous permet d'utiliser les valeurs de données pour un grand nombre de fonctions avancées.

Pour la surveillance des canaux analogiques à l'aide de valeurs de données, reportez-vous à la section des modules d'expansion analogiques (consultez la page 317). Pour une application de programmation avancée, consulter la Note d'application 278 : Comptage des partitions par niveau d'accès dans Protege GX.

Si une valeur de données n'est pas générée par un module physique tel qu'un module d'expansion analogique, il peut être nécessaire de la définir comme **valeur de données de canal** pour un module d'expansion analogique virtuel (**Modules d'expansions | Modules d'expansion analogiques | Canal 1-4**) pour s'assurer qu'elle est téléchargée vers le contrôleur.

Valeurs de données | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Configuration

- **Prédéfinir alimentation** : Lorsque cette option est activée, la valeur des données est réglée sur la **Valeur prédéfinie** chaque fois que le contrôleur est mis sous tension. Lorsque cette option est désactivée, la valeur des données revient à la dernière valeur connue lorsque le contrôleur est mis sous tension.
- **Valeur prédéfinie** : Lorsque cette option est activée, la valeur des données est réglée sur la **Valeur prédéfinie** chaque fois que la programmation est téléchargée vers le contrôleur. Cela crée une valeur constante qui peut fournir un point fixe ou de consigne pour la comparaison.

  Cette option ne doit pas être utilisée pour les valeurs de données qui contrôlent les canaux d'entrée analogiques.
- **Valeur prédéfinie** : Si l'une ou l'autre ou les deux options **Prédéfinir alimentation** et **Valeur prédéfinie** sont activées, la valeur des données sera réglée sur ce chiffre.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Variables

Les variables vous permettent d'afficher les informations stockées par les valeurs de données sous une forme lisible par l'homme. La valeur des données peut être mise à l'échelle par une équation linéaire pour rendre la valeur plus facile à lire.

Les variables peuvent être affichées sur les plans d'étage ou les pages d'état (via une liste d'état). Lorsqu'elle est affichée sur un plan d'étage, vous pouvez faire un clic droit sur la variable, saisir une valeur et cliquer sur **Régler la variable** pour modifier manuellement la valeur de la variable.

Pour un exemple de configuration de variable, voir la section sur le module d'expansion analogique(consultez la page 317).

Variables | Général

Général

- **Nom** : Le nom de l'enregistrement en anglais. Ce nom est utilisé partout où l'enregistrement apparaît dans la version anglaise du logiciel.
- **Nom (deuxième langue)** : Le nom de l'enregistrement dans la deuxième langue (telle qu'installée avec le logiciel). Ce nom est utilisé partout où l'enregistrement apparaît dans la version du logiciel en deuxième langue. Il est également possible d'inclure dans ce champ des informations supplémentaires sur l'enregistrement.

Configuration

- **Échelle** : La valeur des données est multipliée par l'échelle pour calculer la variable Cette fonction peut être utilisée pour convertir une valeur en une unité plus lisible, par exemple de millivolts en volts.
- **Offset** : L'offset est ajouté à la valeur des données pour calculer la variable. Il peut s'agir d'une valeur positive ou négative.

  L'échelle est appliquée avant le décalage, de sorte que l'offset n'est pas multiplié.

- **Valeur minimale / maximale** : Lorsque la variable est affichée sur un plan d'étage, elle peut être affichée sur une jauge linéaire. Ces options déterminent les valeurs minimales et maximales qui peuvent être affichées sur cette jauge. Réglez-les à des valeurs raisonnables pour que la jauge soit facile à lire d'un coup d'œil.

  Ces options n'affectent pas la valeur de la variable elle-même.

- **Valeur des données** : La valeur de la donnée qui fournit la valeur de base de la variable.
- **Supporter commandes manuelles** : Lorsque cette option est activée, les opérateurs peuvent faire un clic droit sur cette variable sur un plan d'étage et définir manuellement la valeur. Cette option ne doit pas être utilisée pour les variables destinées à servir de constantes ou à surveiller les entrées physiques.

Historique des enregistrements

Chaque enregistrement affiche l'historique de sa programmation, y compris l'heure et la date de sa création, l'heure et la date de sa dernière modification et l'opérateur qui l'a modifié en dernier.

Variables| Enregistrer

- **Enregistrer les données**: Cette option vous permet d'enregistrer la valeur de la variable dans le journal des événements à intervalles réguliers.

  Vous pouvez également activer la journalisation des données brutes dans **Modules d'expansions| Module d'expansion analogique | Canal 1-4** .

Menu À propos

Le menu À propos est utilisé pour enregistrer et mettre à jour la licence de votre logiciel, ainsi que pour visualiser les informations sur la version.

Aide

Le menu **À propos de | Aide** vous permet d'accéder facilement au manuel de référence de l'opérateur en format électronique directement à partir du client Protege GX.

L'accès à Internet n'est pas nécessaire.

Licence

Cette page vous permet de visualiser les détails de votre Protege GX licence actuelle et de mettre à jour votre licence.

Licence | Information

La fenêtre d'information sur la licence s'affiche :

- Le numéro de série du logiciel (SSN) actuellement utilisé.
- La durée restante du contrat de maintenance de votre logiciel
- La version de l'application principale (logiciel) que vous utilisez
- La version de la licence dont vous disposez
- Les fonctions sous licence qui sont activées sur votre SSN
- Le nombre d'éléments sous licence limitée qui sont utilisés dans le système par rapport au plafond de licence (par exemple, 10 portes utilisées sur 50 disponibles).
- Les dates d'expiration des fonctions sous licence actuellement activées (pour les afficher, cliquez sur la flèche à bascule située à côté de l'élément sous licence concerné).

Licence | Détails du site

L'onglet des détails du site affiche les détails du site et de l'installateur qui sont enregistrés pour cette licence dans le système de licences de Protege GX.

Enregistrement et mise à jour de votre licence d'utilisation du logiciel

Avant de pouvoir utiliser Protege GX, vous devez enregistrer votre licence logicielle auprès de ICT. Vous devez également répéter ce processus pour mettre à jour votre fichier de licence chaque fois que vous ajoutez de nouveaux éléments ou de nouvelles fonctionnalités à la licence.

Conditions requises pour l'enregistrement ou la mise à jour de la licence

Pour enregistrer ou mettre à jour votre licence Protege GX, vous aurez besoin des éléments suivants :

- Un appareil avec un accès à Internet. Deux méthodes d'octroi de licence sont disponibles, en fonction de la connectivité Internet du réseau :
  - Si le serveur Protege GX ou tout client Protege GX dispose d'un accès Internet, vous pouvez utiliser la méthode de licence **automatique**.
  - Si aucune machine Protege GX n'a d'accès à Internet, vous devez utiliser la méthode de licence **manuelle**. Vous devrez utiliser le serveur Protege GX et un autre appareil pouvant accéder à Internet.

- L'opérateur qui active ou met à jour la licence doit avoir accès à **tous les sites** du système.
- Le compte Windows utilisé doit avoir des privilèges d'administration locale.

Activation automatique de votre licence

1. Connectez-vous à Protege GX sur n'importe quelle machine ayant accès à Internet.
2. Dans le menu principal, naviguez jusqu'à **À propos | Licence**.
3. Sélectionnez l'onglet **Mise à jour de licence**.
4. Cliquez sur **Télécharger la licence**.
5. Saisissez les informations requises et sélectionnez **OK**.
   L'application Protege transmet vos coordonnées au service d'enregistrement Web de ICT, puis active automatiquement votre logiciel.
6. Fermez et redémarrez le logiciel Protege GX pour mettre en oeuvre la nouvelle licence.

Activation manuelle de votre licence

1. Connectez-vous à Protege GX **sur la machine serveur**.
2. Dans le menu principal, naviguez jusqu'à **À propos | Licence**.
3. Sélectionnez l'onglet **Mise à jour de licence**.
4. Cliquez sur **Générer** pour créer un fichier de demande de licence. Lorsque vous y êtes invité, enregistrez le fichier **ICT_LicenceRequest.req** dans un dossier de votre réseau ou sur un lecteur portable.
5. Notez le lien affiché à côté de « Téléchargez votre licence via le site Web ».
6. Transférez le fichier de demande de licence sur un appareil ayant accès à Internet.
7. Ouvrez un navigateur Web et naviguez jusqu'au lien que vous avez noté ci-dessus.
8. Saisissez les informations requises et transférez le fichier de demande de licence, puis cliquez sur **Envoyer**.
   Vos détails sont ensuite transmis au service d'enregistrement Web de ICT. Une fois que l'enregistrement est complété, vous serez demandé de télécharger votre fichier de licence(.lic).
9. Transférez le fichier de licence vers le serveur Protege GX.
10. Dans l'onglet **Mise à jour de la licence**, cliquez sur **Naviguer...** et sélectionnez le fichier de licence.
11. Fermez et redémarrez le logiciel Protege GX pour mettre en oeuvre la nouvelle licence.

Visualisation des informations sur la version

Lorsque vous enregistrez un ticket d'assistance, il vous est généralement demandé de fournir les détails de la version du logiciel que vous utilisez. Pour visualiser les informations relatives à la version, naviguez vers **À propos | Version**..

Concepteurs et fabricants de produits électroniques intégrés de contrôle d'accès, de sécurité et d'automatisation.
Conçus et fabriqués par Integrated Control Technology Lté.