PRT-GX-SRVR

Protege GX

Guide de l'utilisateur final

Dernière publication en 20-mars-25 13:35.

Contenu

Comprendre votre système Protege GX

Protege GX est une solution intégrée de contrôle d'accès, de détection d'intrusion et d'automatisation des bâtiments au niveau de l'entreprise, offrant un ensemble de fonctionnalités faciles à utiliser, simples à intégrer et extensibles sans effort.

Conçue pour l'utilisateur final, Protege GX offre une interface intuitive et conviviale avec des plans d'étage graphiques et des pages d'état hautement personnalisables pour contrôler et surveiller le système.

Des filtres d'alarme et d'événement personnalisables vous permettent de trier et de classer les données d'événement et d'alarme affichées, ainsi que d'afficher des informations pertinentes pour votre site et votre configuration.

Le système peut comprendre plusieurs éléments :

- Le **serveur de base de données** ou « serveur » qui stocke les données du système et fournit la connexion centralisée au reste du système. En fonction de votre site, le serveur sera généralement situé dans une salle de contrôle à accès restreint, et dans la plupart des cas, il n'y a aucune raison pour que quelqu'un d'autre que votre professionnel de la sécurité ou votre gestionnaire immobilier ait besoin d'un accès physique au serveur.
- Les ordinateurs **Protege GX clients** et l'interface **client web** qui fournissent l'interface utilisateur permettant aux opérateurs autorisés d'accéder au système pour ajouter et mettre à jour des registres et visualiser des informations sur le statut et les événements.
- Le **Protege GX contrôleur** qui est l'unité centrale de traitement du système. Le contrôleur sera installé dans une partition à l'écart, comme une pièce de service ou une armoire, et dans la plupart des cas, il n'y a aucune raison pour que quelqu'un d'autre que votre professionnel de la sécurité ou votre gestionnaire immobilier ait besoin d'un accès physique à cette unité.
- Divers **capteurs de détection** (appelés **entrées**), tels que les détecteurs de mouvement ou les contacts de porte qui sont connectés au contrôleur. Si votre système est armé et qu'un capteur est activé, l'entrée est « ouverte » et envoie un signal au contrôleur pour déclencher une alarme. Une sirène ou un autre appareil d'alarme est activé, et le contrôleur transmet automatiquement ces informations à votre poste de surveillance ou de garde. En entrant votre code d'accès et en désarmant le système, l'alarme est désactivée.
- Un ou plusieurs **claviers** qui sont utilisés pour armer/désarmer le système et afficher le statut actuel du système. Chaque clavier se trouve généralement dans un endroit pratique à l'intérieur de vos installations, près de la porte de sortie/d'entrée.
- Un ou plusieurs **lecteurs de cartes** et/ou **serrures sans fil** qui assurent le contrôle d'accès des portes de votre bâtiment. Ceux-ci peuvent être utilisés à l'aide de cartes d'accès, de téléphones mobiles, de codes NIP ou d'autres types d'informations d'identification.
  - Des lecteurs de cartes sont utilisés sur tous les sites. Ils sont reliés au système de sécurité, ce qui leur permet de vérifier instantanément les autorisations d'accès actuelles d'un utilisateur et d'accorder ou de refuser l'accès.
  - Certains sites tels que les immeubles d'habitation (copropriétés) peuvent utiliser des serrures sans fil hors ligne. Ceux-ci ne sont pas activement connectés au système de sécurité : au lieu de cela, la carte ou le téléphone mobile de chaque utilisateur porte les autorisations d'accès dont il a besoin (« données sur la carte »). Les données sont mises à jour chaque fois que l'utilisateur présente sa carte ou son téléphone à un lecteur de point de mise à jour câblé situé à la porte d'entrée ou à un autre endroit clé.

Avant de commencer

La flexibilité du système Protege permet à un intégrateur de programmer les fonctionnalités et le comportement du système en fonction du site. Ce guide vise à expliquer les paramètres les plus courants.

Votre système peut se comporter différemment selon la façon dont votre intégrateur l'a programmé. Consultez votre intégrateur pour obtenir des instructions d'utilisation plus détaillées.

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 Protege GX nom d'utilisateur d'opérateur.
   - **Mot de passe** : Votre Protege GX mot de passe d'opérateur.
   - **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**, saisissez 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.

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.

Modification du mot de passe de l'opérateur

1. Pour modifier votre mot de passe d'opérateur, cliquez sur le bouton **Modifier le mot de passe** sur la page d'accueil.
2. Cela ouvre la fenêtre **Modifier le mot de passe**.
3. Remplissez les champs **Ancien mot de passe**, **Nouveau mot de passe** et **Confirmer le nouveau mot de passe**

respectivement.

4. Cliquez sur **Ok**.

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 de registres peut avoir été restreint par l'administrateur de votre site.

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.
- **Déconnectez-vous** pour fermer Protege GX et revenez 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.

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 registres 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 registres sont classés dans un ordre relationnel, de sorte que vous pouvez localiser les registres en développant les catégories pertinentes.

Le navigateur système n'affiche que les registres 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 registres 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 registre pour visualiser les catégories associées à ce registre. Par exemple, développez un registre 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 registre pour ouvrir la fenêtre de programmation de cet élément. Par exemple, cliquez sur un registre de partition spécifique pour ouvrir la fenêtre de programmation **Programmation | Partitions** et mettre en évidence ce registre.
- Cliquez avec le bouton droit sur un registre 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 registre 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 registres 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 le registre 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 registres.
Site	Sélectionnez le site pour lequel vous souhaitez afficher les registres.
Ajouter	Créez un nouveau registre avec les paramètres par défaut.
Sauvegarder	Sauvegardez les changements apportés au registre actuel. Après la sauvegarde d'un registre, les modifications peuvent être téléchargées sur le contrôleur.
Trouver	Ouvrez l'outil de recherche pour filtrer la liste des registres. Pour plus d'informations, consultez la section Utiliser l'outil de recherche (page suivante).
Actualiser	Actualisez le registre actuel pour voir les mises à jour éventuelles.
Exporter	Exportez les registres affichés dans la liste des registres, y compris les informations des colonnes spécifiées. Vous pouvez exporter les données vers un fichier CSV ou vers le presse-papiers.
Copier	Copiez la configuration d'un registre spécifié sur le registre actuel. Cette fonction ne crée pas de copie du registre actuellement sélectionné. Au lieu de cela, elle écrase le registre actuellement sélectionné avec les paramètres d'un autre registre.
Effacer	Supprimez le registre de la base de données de programmation. Cela supprimera également tous les registres qui dépendent de ce registre. 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 simultanément des changements de programmation à un certain nombre de registres.

- Pour sélectionner plusieurs registres 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 Détachement (incrustation)

Le bouton **Détachement** (ou 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 de statut ou le plan d'étage souhaité, puis cliquez sur **Détachement** 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 comportent 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 registre individuel.

- **Onglet Historique** : Affiche l'historique d'audit du registre, vous permettant de voir quand le registre a été créé et modifié, et par quels opérateurs. Chaque fois que le registre 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 le registre est actuellement utilisé dans le logiciel. Par exemple, pour un registre 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 registres seront affectés si vous apportez une modification au registre. Il est recommandé de vérifier cet onglet avant de supprimer un registre, afin de s'assurer qu'il n'est pas utilisé ailleurs dans le système.
- **Onglet Événements** : Affiche les événements récents associés au registre. Par exemple, pour un registre 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 ce registre, 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.

Gestion des utilisateurs

Un **utilisateur** est une personne qui a besoin d'accéder à l'installation contrôlée par le système. Chaque utilisateur possède des informations d'identification uniques, tels que des cartes d'accès et des codes NIP, qu'il peut utiliser pour déverrouiller les portes et désarmer le système d'alarme.

Les **niveaux d'accès** sont utilisés pour contrôler ce que les utilisateurs peuvent faire, où ils peuvent aller et quand ils peuvent faire ces choses.

Il existe plusieurs méthodes pour créer des utilisateurs. Ce guide décrit les étapes pour ajouter des utilisateurs à partir du menu « Utilisateurs ». Pour obtenir des instructions sur l'utilisation de méthodes alternatives, adressez-vous à votre installateur.

Chaque site ayant ses propres exigences en matière de registres d'utilisateur, consultez votre installateur ou votre administrateur système pour savoir quelles options sont utilisées dans votre système.

Ajout d'un utilisateur

1. Naviguez vers **Utilisateurs | Utilisateurs**, cliquez sur **Ajouter**.
2. Entrez un **prénom** et un **nom** pour l'utilisateur.
3. Le système remplit automatiquement le **Nom d'affichage** au format « Prénom Nom de famille » (par exemple, John Smith). Si votre site utilise un format différent (par exemple, Smith, J.), vous pouvez adapter le nom d'affichage.
4. En fonction de la configuration de votre site, il se peut que vous deviez sélectionner un **Groupe de registres** pour l'utilisateur. Cela détermine quels opérateurs Protege GX peuvent visualiser et modifier ce registre d'utilisateur.
5. Saisissez un **code NIP**. Il s'agit du numéro que l'utilisateur doit saisir lorsqu'il se connecte à un clavier ou accède à une porte qui nécessite des informations d'identification NIP.
6. Saisissez les informations d'identification de l'utilisateur en tapant les numéros correspondants de l'établissement et de la carte dans les champs disponibles.

   Chaque utilisateur peut avoir jusqu'à huit numéros de carte. Plusieurs numéros de carte permettent au même utilisateur d'avoir plusieurs informations d'identification (tels que les cartes, les porte-clés, les informations d'identification mobiles et les télécommandes sans fil), sans qu'il soit nécessaire de programmer des registres d'utilisateur en double.
7. Sélectionnez l'onglet **Niveaux d'accès** pour ajouter le ou les niveaux d'accès requis à l'utilisateur. Lorsque l'utilisateur effectue une action, le système vérifie le(s) niveau(x) d'accès pour s'assurer que l'utilisateur dispose des autorisations nécessaires pour effectuer l'action demandée.

   Pour plus d'informations, consultez la section Création d'un niveau d'accès (page suivante).
8. Cliquez sur **Ajouter**, sélectionnez le(s) niveau(x) d'accès approprié(s) et cliquez sur **OK**.
9. Dans l'onglet **Options**, il y a quelques paramètres communs que vous devrez peut-être activer :
   - **Traiter le NIP +1 de l'utilisateur sous contrainte** : L'utilisateur peut activer l'alarme de contrainte silencieuse en ajoutant 1 au dernier chiffre de son code NIP.
   - **L'utilisateur a des droits supérieurs et peut l'emporter sur l'anti-passback**: L'utilisateur peut ignorer les restrictions de verrouillage et d'antipassback.
   - **Utilisateur opère la fonction d'accès de porte prolongé** : L'utilisateur déverrouille les portes pour une durée plus longue (pour les personnes ayant des problèmes de mobilité).
10. Cliquez sur le bouton **Enregistrer** dans la barre d'outils pour enregistrer le nouvel utilisateur. L'utilisateur peut maintenant utiliser les informations d'identification et le NIP qui lui ont été attribués pour accéder aux portes, et armer et désarmer le système à partir d'un clavier.

Fixation des dates de début et d'expiration (facultatif)

Chaque utilisateur peut se voir attribuer un accès pour une période définie en cochant les options **Début** ou **Fin** (dans l'onglet **Général**) et en réglant une date et une heure.

Ainsi, vous pouvez émettre et envoyer des cartes avant que l'accès ne soit activé, par exemple dans le cas des employés qui n'ont pas encore commencé. Vous pouvez également définir des informations d'identification qui expirent automatiquement, par exemple lorsqu'un entrepreneur doit terminer à une date donnée.

Création d'un niveau d'accès

1. Accédez à **Utilisateurs | Niveaux d'accès**, cliquez sur **Ajouter**.
2. Saisissez un **Nom** pour le niveau d'accès.
3. Définir l'**Horaire d'opérateur**. Cela détermine les heures auxquelles l'utilisateur a accès aux portes, aux partitions et aux autres parties du niveau d'accès. Par défaut, cette valeur est réglée sur Toujours, ce qui autorise l'accès à tout moment. Par exemple, vous pouvez souhaiter limiter l'accès des employés aux seuls jours où ils travaillent.
4. Cliquez sur **Sauvegarder**.

Vous pouvez maintenant ajouter les parties du site auxquelles l'utilisateur est autorisé à accéder. Les exigences les plus courantes concernent les portes, les partitions et les groupes de menus.

Ajout de portes à un niveau d'accès

Les portes et les groupes de portes définissent les portes auxquelles un utilisateur a accès, ainsi que l'horaire qui détermine quand. Il est fort probable que votre installateur ait déjà programmé les portes requises pour votre site.

Les groupes de portes sont généralement utilisés sur les sites qui ont un grand nombre de portes contrôlées. Pour les petits sites, il est fréquent d'utiliser des portes individuelles. Selon la manière dont votre installateur a configuré votre système, vous pouvez ou non avoir des groupes de portes.

Pour ajouter des portes à un niveau d'accès :

1. Sélectionnez l'onglet **Portes** ou **Groupes de portes** et cliquez sur **Ajouter**.
2. Choisissez les portes ou groupes de portes concernés et cliquez sur **OK**.
3. Définissez l'**horaire** à utiliser. Par défaut, l'horaire est défini sur Toujours, ce qui signifie que l'accès aux portes sélectionnées est autorisé à tout moment. Vous pouvez attribuer un horaire pour restreindre l'accès à la ou aux portes à la période définie dans cet horaire. Par exemple, vous pouvez limiter l'accès à un bureau afin qu'il ne soit accessible que pendant les heures de bureau.
4. Enregistrez vos modifications.

Ajout de partitions à un niveau d'accès

Les groupes de partitions sont affectés à un niveau d'accès et servent à contrôler les partitions qu'un utilisateur peut armer et désarmer.

Pour ajouter un groupe de partitions à un niveau d'accès :

1. Sélectionnez l'onglet **Armement groupes de partitions** ou **Désarmement groupes de partitions** et cliquez sur **Ajouter**.

   Remarque : Si un utilisateur est autorisé à désarmer une partition, il est également autorisé à l'armer.

2. Choisissez le groupe de partitions concerné et cliquez sur **OK**.
3. Définissez l'**horaire** à utiliser. Par défaut, l'horaire est réglé sur Toujours, ce qui signifie que les utilisateurs peuvent à tout moment armer/désarmer les partitions de ce groupe. Vous pouvez attribuer un horaire pour

restreindre l'armement et le désarmement à la période définie dans l'horaire. Par exemple, vous pouvez ne pas souhaiter qu'un employé puisse désarmer une partition en dehors de ses heures de travail normales.

4. Enregistrez vos modifications.

Pour plus d'informations sur la programmation des groupes de partitions, consultez le Protege GX Manuel de référence de l'opérateur ou demandez à votre installateur.

Ajout d'un groupe de menus à un niveau d'accès

Les groupes de menus déterminent ce que l'utilisateur peut faire sur un clavier. En règle générale, la plupart des utilisateurs sont autorisés à armer/désarmer les partitions, mais les fonctions de menu utilisées pour le dépannage et le contrôle du système ne sont accessibles qu'aux installateurs.

Pour ajouter un groupe de menus à un niveau d'accès :

1. Sélectionnez l'onglet **Groupes de menus** et cliquez sur **Ajouter**.
2. Sélectionnez le groupe de menus concerné et cliquez sur **OK**.

   Vous ne pouvez ajouter qu'un seul groupe de menus à chaque niveau d'accès.

3. Enregistrez vos modifications.

Suppression des utilisateurs

Vous pouvez facilement supprimer les registres d'utilisateur qui ne sont plus nécessaires.

Il vous suffit de sélectionner les registres à supprimer, puis de cliquer sur le bouton **Supprimer** de la barre d'outils.

Désactivation des utilisateurs

Le paramètre **Désactiver l'utilisateur** (situé sous l'onglet **Options**) supprime immédiatement l'accès tout en conservant le registre d'utilisateur et ses détails. Cette fonction est idéale pour supprimer temporairement l'accès, par exemple lorsque le personnel est en congé prolongé, ou pour supprimer l'accès tout en conservant les informations de l'utilisateur.

Gestion des utilisateurs à l'aide de serrures sans fil hors ligne

Il existe quelques différences essentielles en matière de gestion des utilisateurs entre les systèmes standard et les systèmes dotés de serrures sans fil hors ligne.

Les serrures sans fil hors ligne n'étant pas activement connectées au reste du système, lorsque vous ajoutez un utilisateur ou mettez à jour ses paramètres, vous devez charger ces paramètres sur les informations d'identification de l'utilisateur. Pour ce faire, vous pouvez utiliser soit un **encodeur de bureau** connecté à l'ordinateur, soit un **lecteur de point de mise à jour** situé à la porte d'entrée ou à un autre endroit clé du bâtiment.

Aucune des fonctions liées à d'autres parties du système de sécurité (par exemple, désarmer une partition en fonction de l'accès à la porte) n'est disponible sur les serrures hors ligne. Certains paramètres de contrôle d'accès peuvent également ne pas fonctionner comme prévu.

Ajout d'un niveau d'accès

1. Accédez à **Utilisateurs | Niveaux d'accès** et cliquez sur **Ajouter**.
2. Dans l'onglet **Portes** ou **Groupes de portes**, ajoutez les portes et les groupes auxquels l'utilisateur aura accès.
3. Groupez l'**Horaire** pour chaque porte et groupe de portes.
4. Cliquez sur **Sauvegarder**.

Ajout d'un nouvel utilisateur

1. Accédez à **Utilisateurs | Utilisateurs** et cliquez sur **Ajouter**.
2. Programmez les paramètres de l'utilisateur normalement :
   - Nom
   - Niveaux d'accès
   - Dates d'expiration sous **Date/heure d'expiration de l'utilisateur** (facultatif).
3. La **Période de mise à jour** (onglet **Général**) détermine la fréquence à laquelle l'utilisateur doit renouveler ses données d'accès en présentant sa carte à un lecteur de point de mise à jour. Si ce délai expire, l'utilisateur ne pourra plus accéder aux serrures hors ligne jusqu'à ce qu'il remette sa carte à jour.
4. Sélectionnez **Activer le déverrouillage du bureau** (onglet **Général**) pour permettre à l'utilisateur de basculer la serrure lorsque la porte est en mode bureau (consultez la page 35).
5. Avant que l'utilisateur puisse utiliser sa carte ou ses informations d'identification mobiles dans une serrure hors ligne, vous devez l'initialiser pour télécharger les données d'accès. Il existe deux méthodes pour initialiser des informations d'identification :

   Utilisation d'un encodeur de bureau (cartes uniquement) :
   - Sauvegarder le registre d'utilisateur.
   - Dans l'onglet **Général**, descendez jusqu'à la section **Informations d'identification** et sélectionnez le type d'informations d'identification ICT Verrouillage sans fil.
   - Définissez les dates d'expiration de **Début** et de **Fin** si nécessaire.
   - Placez la carte sur l'encodeur de bureau.
   - Cliquez sur **Carte de programme**. Protege GX va encoder la carte, télécharger les données d'accès et sauvegarder l'installation et le numéro de la carte dans le dossier de l'utilisateur.

   Utilisation d'un lecteur de point de mise à jour (cartes et informations d'identification mobiles) :
   - Dans l'onglet **Général**, descendez jusqu'à la section **Informations d'identification** et sélectionnez le type d'informations d'identification ICT Verrouillage sans fil.
   - Sous **Informations d'identification**, saisissez le numéro de l'établissement et le numéro de la carte ou les informations d'identification mobile de l'utilisateur, séparés par deux points (par exemple 10636:7482).
   - Définissez les dates d'expiration de **Début** et de **Fin** si nécessaire.
   - Cliquez sur **Sauvegarder**.
   - Attendez que la programmation soit téléchargée dans le contrôleur.
   - Badgez la carte ou l'appareil mobile sur un lecteur de point de mise à jour pour encoder la carte et télécharger les données d'accès.

L'utilisateur peut désormais utiliser sa carte ou son téléphone mobile pour accéder aux serrures sans fil hors ligne.

Mise à jour des utilisateurs

Lorsque vous mettez à jour les paramètres d'un utilisateur, tels que les niveaux d'accès ou les horaires, l'utilisateur doit badger sa carte sur un lecteur de point de mise à jour avant que les nouveaux paramètres ne soient disponibles.

Désactivation des utilisateurs

Pour désactiver un registre d'utilisateur, vous pouvez :

- Définir la **Date/heure d'expiration de l'utilisateur** ou la date de **Fin** des informations d'identification sur une date non valide (par exemple, hier).
- Supprimer ou modifier les niveaux d'accès qui permettent d'accéder aux serrures sans fil.

Le paramètre **Désactiver l'utilisateur** dans **Utilisateurs | Utilisateurs | Options** ne fonctionne pas avec les serrures hors ligne.

Désactivation des utilisateurs

Lorsque vous supprimez un registre d'utilisateur ou des informations d'identification, cela est ajouté à la **liste de blocage** qui est chargée sur toutes les informations d'identification d'utilisateur. Au fur et à mesure que les utilisateurs se déplacent dans le système, ils mettent à jour la liste de blocage stockée sur chaque serrure sans fil. Cela réduit le risque que des informations d'identification supprimées permettent d'obtenir un accès non autorisé.

Les informations d'identification figurant sur la liste de blocage ne peuvent pas être réaffectées à un autre utilisateur tant qu'elles n'ont pas expiré. En règle générale, après l'ajout d'informations d'identification à la liste de blocage, vous devez la mettre de côté pendant deux fois la **Période de mise à jour** (par exemple 60 jours) avant de la réaffecter à un autre utilisateur.

Ne supprimez pas en une seule fois un grand nombre de registres d'utilisateur ou d'informations d'identification (par exemple, plus de 100). Au lieu de cela, désactivez les registres à l'aide des méthodes ci-dessus, puis supprimez les registres d'utilisateur sur une période plus longue.

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.

Création de groupes de jours fériés

Avant de créer un horaire, il est convenable de programmer un ou plusieurs groupes de jours fériés qui s'y appliquent. Ceux-ci doivent inclure les jours fériés nationaux, locaux et autres, qui peuvent entraîner un fonctionnement différent de votre site ; par exemple, un commerce de détail peut avoir des horaires plus courts (ou plus longs) un jour férié.

Il n'est pas nécessaire de programmer les fins de semaine en tant que groupes de jours fériés.

1. Naviguez à **Sites | Groupes fériés** et cliquez sur **Ajouter**.
2. Entrez un **Nom** pour le groupe de vacances.
3. Sélectionnez l'onglet **Groupes Fériés** et **Ajoutez** des vacances au groupe.
   - Activez l'option **Répéter** pour les jours fériés qui ont lieu le même jour chaque année.
   - Pour les périodes de vacances qui s'étendent sur plusieurs jours (comme le jour de Noël et le lendemain de Noël), définissez les dates de début (premier jour) et de fin (dernier jour).
   - En ce qui concerne les jours fériés qui tombent un jour différent chaque année (comme Pâques), ceux-ci doivent être programmés pour chaque occurrence annuelle car les dates ne se répètent pas. Toutefois, en ajoutant plusieurs entrées, vous pouvez programmer plusieurs années à l'avance.
4. Cliquez sur **Sauvegarder**. Une fois que vous avez programmé votre ou vos groupes de jours fériés, ils peuvent être appliqués à vos horaires.

Création et modification des horaires

1. Naviguez jusqu'à **Sites | Horaires**.
2. Cliquez sur **Ajouter** et entrez un **Nom** pour le programme, ou sélectionnez le programme que vous souhaitez modifier.
3. Chaque horaire comporte plusieurs périodes qui peuvent être programmées et qui peuvent être utilisées pour différents jours de la semaine ou jours fériés. Pour chaque période, entrez les heures de début et de fin pour lesquelles vous souhaitez que l'horaire fonctionne, et cochez les cases des jours de la semaine requis.

   Pour plus d'informations, consultez la section Horaires et périodes multiples (la page 20).

   Notez comment la **vue graphique** se met à jour pour indiquer quand l'horaire sera valable.

4. Pour chaque période, sélectionnez le **mode jours fériés** pour définir quel sera le fonctionnement de l'horaire pendant une période de jours fériés. Choisissez parmi :
   - **Désactivé lors des jours fériés** : lorsque cette option est sélectionnée, la période ne valide **pas** l'horaire lors d'un jour férié. En d'autres termes, si une porte est programmée pour se déverrouiller selon cet horaire, elle ne se déverrouille pas un jour férié lorsque cette option est sélectionnée. Il s'agit du mode de fonctionnement par défaut pour les horaires
   - **Activé lors des jours fériés** : lorsque cette option est sélectionnée, la période ne valide pas l'horaire **uniquement** lors d'un jour férié. Par exemple, un utilisateur peut avoir des heures d'accès différentes un jour férié par rapport à un jour normal.
   - **Ignorer les jours fériés** : lorsque cette option est sélectionnée, la période valide l'horaire **indépendamment** du fait que le jour soit un jour férié ou non. Par exemple, le gestionnaire peut avoir accès au bâtiment à tout moment, qu'il soit jour férié ou non.
5. Sélectionnez l'onglet **Groupes de jours fériés**. Cliquez sur **Ajouter** et sélectionnez les groupes de jours fériés que vous souhaitez appliquer à l'horaire.

   Ainsi, vous indiquez à l'horaire les jours qui sont fériés, mais vous n'indiquez pas à l'horaire ce qu'il faut faire s'il s'agit d'un jour férié. Ce paramètre est défini par le **mode jours fériés** ci-dessus.
6. Cliquez sur **Enregistrer** pour terminer la création de votre horaire.

Utilisation d'un horaire pour déverrouiller automatiquement une porte

L'attribution d'un horaire de déverrouillage à une porte déterminera le moment où cette porte se déverrouillera. Par exemple, si vous avez une porte d'entrée de bureau que vous devez déverrouiller à 8 h et verrouiller à nouveau à 17 h, vous devez créer un horaire pour les heures d'ouverture, puis attribuer cet horaire à la porte.

1. Naviguez jusqu'à **Programmation | Portes**.
2. Choisissez la porte que vous souhaitez contrôler et définissez l'**horaire de déverrouillage**.
3. Enregistrez vos modifications.

   Dans de nombreux cas, vous devrez également empêcher la porte de se déverrouiller si personne ne se présente au travail. Un moyen simple de le faire est d'utiliser la fonction L'horaire fonctionne en retard pour ouvrir.
4. Sélectionnez l'onglet **Options** et activez l'option **L'horaire fonctionne en retard pour ouvrir** et enregistrez vos modifications

   Ainsi, la porte ne se déverrouille pas avant que le premier utilisateur n'y accède.

Il existe de nombreuses autres options de porte qui peuvent être programmées, mais elles dépassent la portée de ce guide. Pour plus d'informations, et avant d'apporter des modifications, nous vous recommandons de vous adresser à votre installateur.

Utilisation d'un horaire pour contrôler l'accès des utilisateurs

Les horaires sont utilisés pour contrôler **le moment où** un utilisateur peut faire quelque chose. L'attribution d'un horaire de fonctionnement à un niveau d'accès détermine le moment où le niveau d'accès est valide et celui où les utilisateurs peuvent accéder aux options programmées dans le niveau d'accès.

1. Accédez à **Utilisateurs | Niveaux d'accès**.
2. Sélectionnez le niveau d'accès auquel vous souhaitez ajouter l'horaire et définissez l'**horaire d'opération**
3. Enregistrez vos modifications.

Vous pouvez également attribuer un horaire aux portes d'un niveau d'accès pour restreindre l'accès aux heures définies ou aux des groupes de partitions pour restreindre l'armement/le désarmement à une période spécifique. Cette option offre une plus grande flexibilité en vous permettant de définir l'accès de manière plus détaillée. Par exemple, vous pourriez vouloir limiter l'accès à un groupe de portes aux heures de bureau prévues, mais autoriser l'accès à un autre groupe en dehors de ces heures.

Les horaires ont de nombreuses autres utilisations. Pour plus d'informations, nous vous recommandons de vous adresser à votre installateur.

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 jours fériés** sur Activé durant jours fériés.

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.

Périodes de chevauchement

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

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.

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 fériés doit être appliqué au calendrier dans l'onglet **Groupes de fériés**.
3. Le **Mode jours fériés** pour la période de programmation doit être réglé sur Désactivé durant jours fériés.

Mise à jour des serrures hors ligne

Les serrures hors ligne n'étant pas connectées au système, toute modification de leur configuration doit être transférée à la serrure par un installateur ou un administrateur autorisé à l'aide de l'application de configuration Protege. Il s'agit notamment des modifications de :

- Paramètres de porte
- Horaires pour l'accès des utilisateurs ou le déverrouillage automatique
- Groupes fériés
- Groupes de portes pour l'accès des utilisateurs

N'oubliez pas que les fonctions liées à d'autres parties du système de sécurité (par exemple, désarmer une partition en fonction de l'accès à la porte) ne sont pas disponibles sur les serrures hors ligne.

Contactez votre installateur si vous devez mettre à jour les horaires ou tout autre paramètre de vos serrures sans fil hors ligne.

Travailler avec les rapports

Le menu Rapports permet d'afficher une série de rapports sur le système.

De puissantes options de filtrage et de rapports flexibles sont standard dans l'application Protege GX, ce qui vous permet d'obtenir facilement des informations détaillées et pertinentes sur les événements et les utilisateurs. Tous les rapports permettent de filtrer, de trier, d'imprimer, d'envoyer par courrier électronique et d'exporter les informations obtenues dans divers formats de fichiers.

Rapports d'événements

Les rapports d'événements permettent à l'opérateur de visualiser facilement ce qui se passe dans le système. Les événements sont classés par catégories pour faciliter leur identification et les détails sont facilement accessibles.

Par défaut, trois rapports d'événements sont déjà préconfigurés :

- Tous les événements
- Toutes les alarmes
- Toutes les alarmes reconnues

Votre administrateur système peut avoir créé des rapports personnalisés pour votre site spécifique.

Visualisation d'un rapport d'événement

1. Naviguez jusqu'à **Rapports | Événement**.
2. Sélectionnez un rapport d'événement à exécuter dans la liste disponible et cliquez sur **Exécuter.**.
3. Saisissez les détails de la période pour laquelle vous souhaitez répertorier les événements et cliquez sur **Ok**.

   Une liste d'événements est renvoyée et affichée dans une liste allant de l'événement le plus récent à l'événement le plus ancien.
4. Cette liste peut être triée et filtrée pour afficher un sous-ensemble d'événements plutôt que de les afficher tous en même temps. Vous pouvez également modifier la liste pour afficher ou masquer certaines colonnes, ou pour redimensionner 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.
5. Si plus de 200 événements sont retournés, utilisez les boutons **Précédent** et **Suivant** pour naviguer entre les résultats qui couvrent plusieurs pages.
6. Utilisez le bouton **Imprimer** pour ouvrir la fenêtre d'aperçu avant impression dans laquelle vous pouvez imprimer, exporter ou envoyer les résultats par courrier électronique.
7. Utilisez la vue en grille pour trier, grouper et filtrer davantage les résultats affichés.

Recherche d'événement

La recherche d'événement permet de visualiser simplement ce qui se passe dans le système.

La recherche d'un événement génère un rapport temporaire « unique » qui peut être imprimé ou exporté, mais ne peut pas être sauvegardé.

1. Naviguez jusqu'à **Événements | Recherche d'événement**.
2. Sélectionnez la période dont vous souhaitez inclure les événements.
   - Choisissez une période dans la liste disponible ou saisissez une date et une heure de début spécifiques.
   - Si nécessaire, sélectionnez une date et une heure de fin spécifiques.
3. Vous pouvez sélectionner **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, vous devrez définir les types d'événements à inclure.
   - Cliquez sur **Ajouter** pour ouvrir la fenêtre **Sélectionner les types d'événements**.
   - Sélectionnez les types d'événement concernés et cliquez sur **Ok**.
5. Cliquez sur l'onglet **Registres** pour créer jusqu'à deux filtres de registre (facultatifs) qui vous permettent de restreindre davantage les résultats renvoyés.
6. Cliquez sur **Ajouter** pour ouvrir la fenêtre **Sélectionner les appareils**.
   - Sélectionnez le **Type d'appareil** et le **Contrôleur**, puis sélectionnez les **Appareils** parmi ceux disponibles.
   - Répétez cette procédure pour créer un second filtre de registre si nécessaire.
7. Cliquez sur **Trouver** pour commencer la recherche.
8. Un rapport temporaire est généré et affiché dans une fenêtre séparée. Vous pouvez ajuster la liste pour 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.
9. Si plus de 200 événements sont retournés, utilisez les boutons **Précédent** et **Suivant** pour naviguer entre les résultats qui couvrent plusieurs pages.
10. Utilisez le bouton **Imprimer** pour ouvrir la fenêtre d'aperçu avant impression dans laquelle vous pouvez imprimer, exporter ou envoyer les résultats par courrier électronique.
11. Utilisez la vue en grille pour trier, grouper et filtrer davantage les résultats affichés.

Création d'un rapport d'utilisateur

Les rapports sur les utilisateurs contiennent des informations détaillées sur les utilisateurs de votre système. En créant des rapports d'utilisateur pour les informations dont vous avez besoin, vous pouvez rapidement identifier des détails importants tels que les utilisateurs qui ont accès aux portes sélectionnées, qui ont déclenché des événements définis ou dont les cartes arrivent à expiration.

1. Dans le menu principal, sélectionnez **Rapports | Configuration | Utilisateur**.
2. Cliquez sur le bouton **Ajouter** et saisissez un nom pour le rapport.
3. Sélectionnez le **Type de rapport** à exécuter parmi ceux qui sont énumérés. Choisissez parmi :
   - Tous les utilisateurs
   - Tous les utilisateurs ayant accès aux portes sélectionnées
   - Tous les utilisateurs inclus dans les niveaux d'accès suivants
   - Tous les utilisateurs par événement
   - Tous les utilisateurs par groupe de registres
   - Utilisateurs par type d'événement/portes

- Cartes sur le point d'expirer
- Derniers utilisateurs à avoir franchi les portes
- Tous les utilisateurs ne participant pas à des événements
- Tous les visiteurs actuels
- Tous les visiteurs en retard
- Tous les visiteurs par date
- Rapport sur l'historique des modifications enregistrées

Lorsque le type de rapport est sélectionné, l'écran est mis à jour, ce qui vous permet de définir les options supplémentaires pertinentes pour ce type de rapport (telles que les portes, les niveaux d'accès, les types d'événements, etc.)

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.
   - **Grouper par** : Regroupe les données retournées selon la colonne définie.
5. Cliquez sur l'onglet **Colonnes** pour choisir les colonnes à inclure dans le rapport. Par défaut, seuls le nom et le prénom sont inclus.
6. Cliquez sur **Ajouter** pour ouvrir la fenêtre **Champs d'utilisateur**. Sélectionnez les colonnes à inclure, puis cliquez sur **OK**.
7. Les colonnes sont ajoutées par ordre alphabétique. Pour modifier l'ordre, 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 l'onglet **Courriel** pour saisir les détails concernant la personne et la date à laquelle le rapport doit être envoyé par courrier électronique.
9. - **Opérateurs** : Ajouter le ou les opérateurs à qui envoyer le rapport.
   - **Rapport de courriel** : Sélectionnez cette option pour activer le courrier électronique. Notez que l'opérateur doit avoir une adresse électronique définie dans ses paramètres et que le serveur SMTP doit être défini dans les paramètres globaux, faute de quoi l'envoi du courriel échouera.
   - **Format du rapport** : Définit le format du fichier si le rapport qui sera envoyé. Choisir parmi les formats PDF, CSV, Texte ou XLS.
   - **Heure** : Définit l'heure et le(s) jour(s) d'envoi du rapport.
   - **Heure actuelle du serveur :** Définit l'heure locale actuelle du serveur ou l'heure locale actuelle où les Protege GX services sont exécutés.
10. Cliquez sur **Sauvegarder** pour sauvegarder le rapport.

Exécution d'un rapport de l'utilisateur

1. Naviguez jusqu'à **Rapports | Utilisateur**.
2. Sélectionnez un rapport de l'utilisateur à exécuter dans la liste disponible et cliquez sur **Exécuter**.
3. Une liste d'utilisateurs est renvoyée et affichée à l'aide de la vue en grille.

   Vous pouvez ajuster la liste pour afficher ou masquer certaines colonnes, ou pour redimensionner 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.

4. Utilisez le bouton **Imprimer** pour ouvrir la fenêtre d'aperçu avant impression dans laquelle vous pouvez imprimer, exporter ou envoyer les résultats par courrier électronique.
5. Utilisez la vue en grille pour trier, grouper et filtrer davantage les résultats affichés.

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	Sauvegarde le fichier de prévisualisation du rapport actuel au format .prnx pour stocker temporairement les rapports à 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.
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.

Bouton	Fonction
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**.

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 de la page de statut

Les pages de statut offrent une vue d'ensemble intuitive et efficace de votre système et chaque page est entièrement personnalisable pour inclure les informations que vous souhaitez, avec un contenu pertinent pour votre site. Une page de statut peut inclure des dispositifs tels que des portes, des partitions, des entrées et des sorties, des listes d'événements en direct, des flux de caméra et des plans d'étage.

Pour visualiser une page de statut

1. À partir du menu, sélectionnez **Surveillance | Vue de la page de statut**.
2. La page de statut par défaut s'affiche. Sélectionnez une autre page de statut dans la liste déroulante si nécessaire.
3. L'écran se met automatiquement à jour pour afficher la page sélectionnée.
4. Un clic droit sur un dispositif tel qu'une porte ou une partition sur la page d'état ouvre un menu dans lequel vous pouvez contrôler manuellement le dispositif. Par exemple, vous pouvez l'utiliser pour déverrouiller une porte, activer une entrée ou armer une partition.

Vue du plan d'étage

Les plans d'étages vous 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 objets 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 visualiser un plan d'étage

1. Naviguez jusqu'à **Surveillance | Vue du plan d'étage**.
2. Le plan d'étage par défaut est affiché. Sélectionnez un autre plan d'étage dans la liste déroulante si nécessaire.
3. Le plan d'étage comprend les composantes suivantes :
   - Une représentation graphique du plan d'étage.
   - Une liste d'état qui se met dynamiquement à jour pour afficher l'état en temps réel des appareils utilisés sur le plan d'étage.
   - Une fenêtre d'événement affichant une liste d'événements du plan d'étage, et éventuellement d'autres onglets d'événements personnalisés.
4. Un clic droit sur un appareil dans le plan d'étage ouvre un menu dans lequel vous pouvez contrôler manuellement l'appareil en sélectionnant l'action requise dans le menu.

Utilisation d'un clavier pour armer/désarmer votre système

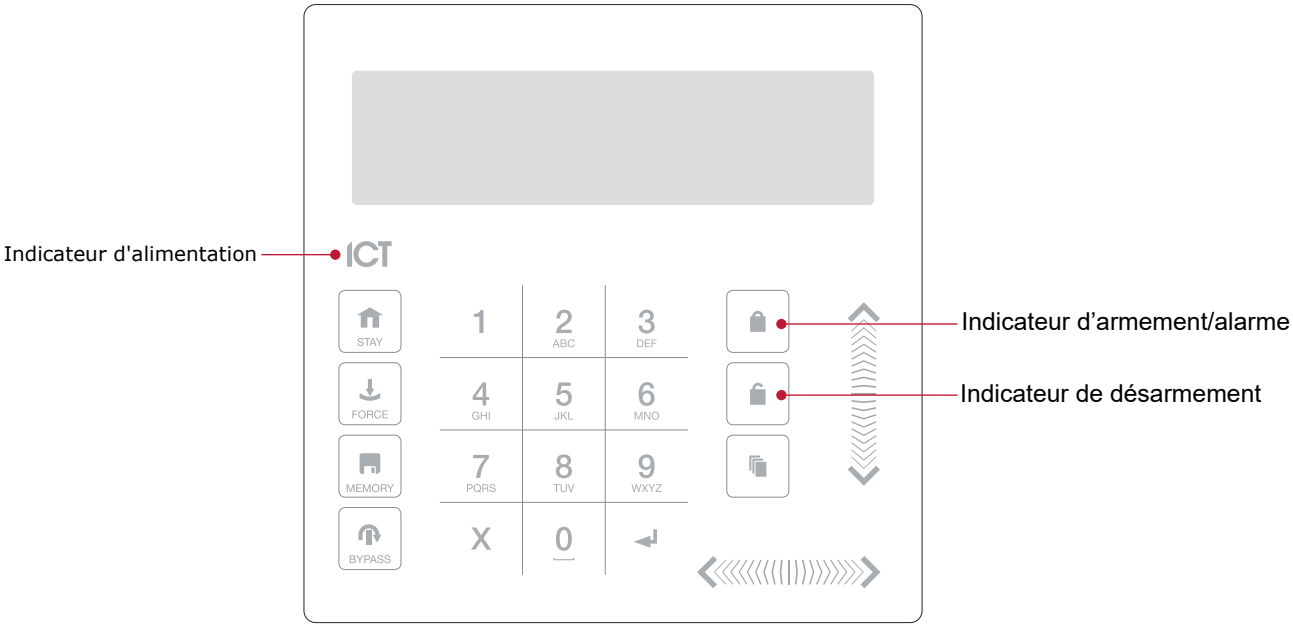
Les claviers sont généralement situés près d'une entrée ou d'une porte pour permettre d'armer et de désarmer les partitions du système.

Les instructions suivantes donnent un aperçu du clavier et de la manière dont il est utilisé pour armer et désarmer votre système. Il existe un certain nombre de fonctions du clavier qui ne sont disponibles que lorsque l'option a été activée par votre installateur. Votre installateur ou votre professionnel de la sécurité peut vous fournir de plus amples informations sur ces fonctions.

Pour plus d'informations, consultez le manuel d'utilisation de votre modèle de clavier.

Indicateurs d'état

Le clavier comporte trois voyants d'indication de l'état montrant l'état du système Protege.



Indicateur d'alimentation

Quand l'indicateur d'alimentation est **allumé**, le système est alimenté et fonctionne normalement. En cas de panne de courant complète, cet indicateur sera **éteint**.

Indicateur d'armement/alarme

Quand l'indicateur d'armement/alarme **clignote**, le système est en alarme et vous devez entrer votre code d'utilisateur pour faire cesser l'alarme. Quand il est **allumé**, le système est armé.

Cet indicateur est programmable et peut ne pas fonctionner comme décrit ici. Vérifiez le fonctionnement avec votre compagnie d'installation ou votre professionnel de la sécurité.

Indicateur de désarmement

Quand l'indicateur de désarmement est **allumé**, le système est désarmé. Par ailleurs, lorsque l'indicateur de désarmement est **allumé**, le système pourrait être prêt à être armé (toutes les entrées sont sécurisées). Entrer votre code pour armer.

Cet indicateur est programmable et peut ne pas fonctionner comme décrit ici. Vérifiez le fonctionnement avec votre compagnie d'installation ou votre professionnel de la sécurité.

Mode de confidentialité

Les claviers comprennent un mode de confidentialité où toutes les lumières (alimentation, activation, désactivation et rétro-éclairage ACL) s'éteignent lorsque le clavier n'est pas utilisé. Le mode de confidentialité peut être activé par votre installateur.

Retour audible

Quand vous enfoncez une touche, cela émet une courte tonalité audible. D'autres tonalités sont générées quand certaines fonctions sont utilisées.

Tonalité de confirmation

Quand une opération est correctement réalisée, le clavier génère une séquence de quatre tonalités audibles.

Tonalité de refus

Quand le système expire ou quand une opération est entrée de manière incorrecte, le clavier émet une tonalité audible pendant trois secondes.

Les tonalités peuvent être désactivées au besoin en appuyant et en maintenant enfoncée la touche **[CLEAR]** pendant trois secondes. Cette option doit activée par votre professionnel de la sécurité ou votre administrateur système.

Fonctions du clavier

Touche	Fonction
0-9	La principale fonction des touches numériques est de saisir les codes utilisateurs. Lors du contrôle des appareils, la touche **[1]** allume l'appareil, la touche **[2]** l'éteint, et lorsqu'il est allumé, la touche **[3]** verrouille l'appareil.
	La touche **[ARM]** est utilisée pour lancer le processus d'armement pour une partition.
	La touche **[DISARM]** est utilisée pour faire taire l'alarme, désarmer la partition, et annuler une séquence d'armement.
	La touche **[MENU]** est utilisée pour accéder au menu et peut être suivie de touches de sélection de raccourci de menu qui représentent un élément du menu. Lorsque la touche **[MENU]** est maintenue enfoncée pendant 2 secondes, le clavier la reconnaîtra comme la touche **[FUNCTION]** qui peut être programmée pour déverrouiller une porte.
	La touche **[STAY]** est utilisée pour initier le processus d'armement en mode partiel pour une partition.
	La touche **[FORCE]** est utilisée pour forcer l'armement d'une partition.
	La touche **[MEMORY]** mènera directement l'utilisateur au menu mémoire.
	La touche **[BYPASS]** peut être enfoncée lorsqu'il y a une intrusion sur une partition pendant un processus d'armement pour contourner l'entrée affichée.
	La touche **[CLEAR]** déconnecte l'utilisateur présentement connecté au clavier. Quand elle est pressée sans qu'il n'y ait de connexion, l'affichage est rafraîchi.
	La touche **[ENTER]** est utilisée pour confirmer une action sur le clavier, reconnaître les informations sur la mémoire et l'alarme, et passer à l'écran de programmation suivant.
TOUCHES DIRECTIONNELLES	Les touches directionnelles sont utilisées pour faire défiler le menu, déplacer la sélection d'une fenêtre de programmation vers l'écran suivant, et déplacer le curseur quand vous programmez ou modifiez des valeurs.

Connexion au clavier

Identifiant unique

1. Pour vous connecter, entrez votre code **NIP** et appuyez sur **[ENTER]**.

Une fois qu'un NIP valide a été saisi, un écran de bienvenue, l'état de la partition ou le menu disponible s'affiche.

Double identifiant

Vous devrez peut-être saisir un double identifiant pour vous connecter au clavier, si celui-ci a été configuré par votre installateur.

1. Pour vous connecter en utilisant une double authentification d'informations d'identification, saisissez le code d'informations d'identification de votre **ID utilisateur** et appuyez sur **[ENTER]**.
2. Lorsque vous y êtes invité, entrez votre code **NIP** et appuyez sur **[ENTER]**.

Une fois qu'un NIP valide a été saisi, un écran de bienvenue, l'état de la partition ou le menu disponible s'affiche.

Si l'option **Verrouiller clavier sur tentatives excédentaires** a été autorisée sur votre système, entrer un code d'utilisateur invalide trois fois verrouillera le clavier pendant une courte période, empêchant les nouvelles tentatives de connections pour tout utilisateur. Le moment de déverrouillage est défini pendant la programmation du clavier.

Déconnexion

Vous serez déconnecté automatiquement après une courte période d'inactivité, ou si la touche **[CLEAR]** est enfoncée pendant que vous êtes connecté.

La période d'inactivité est définie par l'installateur. Même si le système a été programmé pour vous déconnecter automatiquement, pour des raisons de sécurité, il est bon de prendre l'habitude de vous déconnecter lorsque vous quittez le clavier. Ainsi, vous éviterez que des inconnus n'utilisent votre connexion pour désarmer la partition.

Armement de votre système

Lorsque vous quittez votre bâtiment, vous devez armer (ou activer) les partitions de votre système. Vous pouvez avoir une seule partition ou plusieurs partitions qui peuvent être armées indépendamment.

1. Entrez votre **[CODE UTILISATEUR]** et appuyez sur **[ENTER]** pour vous connecter au système.
2. Un message d'accueil s'affiche. Appuyez sur n'importe quelle touche pour continuer ou attendez que le message d'accueil s'arrête.
3. Une partition et un état s'affichent. Si vous avez accès à plus d'une partition, utilisez les touches haut et bas pour faire défiler les partitions disponibles et localiser la partition que vous souhaitez armer.
4. Appuyez sur la touche **[ARM]** pour lancer le processus d'armement.
5. Le système vérifie que toutes les entrées (telles que les détecteurs de mouvement et les loquets de porte) sont fermées avant de commencer à armer la partition. Si vous tentez d'armer le système alors qu'une entrée est ouverte, le clavier émet un bip et affiche un message d'avertissement à l'écran. Vous devrez soit fermer l'entrée avant de pouvoir procéder à l'armement du système, soit choisir de **contourner** l'entrée.

   Le fait de contourner une entrée indique au système d'ignorer temporairement cette entrée jusqu'au prochain armement du système. Par exemple, vous pouvez souhaiter désarmer un capteur dans une pièce où vous effectuez des réparations ou des rénovations, ou garder une fenêtre ouverte pour permettre l'entrée d'air frais.
6. Pour contourner une entrée ouverte, appuyez sur **[BYPASS]**. Une invite apparaît pour vous informer que le système a un certain nombre d'entrées contournées. Appuyez sur **[ARM]** pour confirmer l'action ou sur **[DISARM]** pour arrêter le processus d'armement et remettre la partition en état désarmé.
7. La partition commencera le délai de sortie. Ainsi, vous disposez de suffisamment de temps pour quitter la partition avant que le système ne s'arme complètement. Le clavier ou le lecteur de cartes émettront des bips pendant la période de délai de sortie.
8. Appuyez sur **[CLEAR]** pour vous déconnecter. Quittez la partition avant la fin du délai de sortie et l'armement de la partition.

Armer une partition en mode partiel

L'armement de séjour est une option qui doit être activée par votre installateur.

L'armement de séjour vous permet de rester dans une partition alors qu'elle est partiellement armée. En sélectionnant ce mode, vous armez uniquement les capteurs extérieurs et non les capteurs intérieurs, ce qui vous permet de vous déplacer librement à l'intérieur sans déclencher l'alarme. Par exemple, si vous travaillez tard, vous pouvez armer une partie du bâtiment pour protéger les fenêtres et les portes sans armer les autres entrées.

1. Entrez votre **[CODE UTILISATEUR]** et appuyez sur **[ENTER]** pour vous connecter au système.
2. Un message d'accueil s'affiche. Appuyez sur n'importe quelle touche pour continuer ou attendez quelques secondes pour que le message d'accueil s'arrête.
3. Appuyez sur la touche **[STAY]** pour lancer le processus d'armement de séjour.
4. Le système vérifie que les capteurs extérieurs de la partition sont fermés tout en contournant les capteurs intérieurs.
5. Si toutes les entrées extérieures sont fermées, la partition passe en délai de sortie. Une fois le délai de sortie terminé, la partition est en mode partiel armé.

Forcer l'armement d'une partition

Forcer l'armement est une option devant être autorisée par votre installateur.

Forcer l'armement vous permet d'armer le système sans attendre que toutes les entrées dans le système soient fermées. Il est couramment utilisé lorsqu'un détecteur de mouvement surveille l'espace où se trouve le clavier. Si le détecteur de mouvement a été programmé sur entrée forcée, le système vous permettra d'armer même si l'entrée est ouverte. Lorsque vous quittez le champ d'action du détecteur de mouvement, l'entrée se ferme et le système commence à la surveiller.

1. Entrez votre **[CODE UTILISATEUR]** et appuyez sur **[ENTER]** pour vous connecter au système.
2. Un message d'accueil s'affiche. Appuyez sur n'importe quelle touche pour continuer ou attendez quelques secondes pour que le message d'accueil s'arrête.
3. Appuyez sur la touche **[FORCE]** pour lancer le processus d'armement de force.
4. Le système vérifie si les entrées dans la partition sont fermées, en sautant automatiquement toute entrée ouverte qui peut être armée de force.
5. Si toutes les entrées sont fermées, la partition entre dans son délai de sortie. Une fois le délai de sortie terminé, la partition est armée de force.

Désarmement de votre système

En entrant dans les locaux, vous devrez désarmer (ou désactiver) le système.

Les points d'entrée, tels que la porte d'entrée, sont programmés avec un délai d'entrée. Lorsqu'un point d'entrée est ouvert, le clavier émet une tonalité continue jusqu'à ce que vous désarmiez le système. Votre système ne générera pas d'alarme tant que ce délai ne sera pas écoulé.

1. Entrez votre **[CODE UTILISATEUR]** et appuyez sur **[ENTER]** pour vous connecter au système.
2. Un message d'accueil s'affiche. Appuyez sur n'importe quelle touche pour continuer, ou attendez quelques secondes pour que le message d'accueil s'éteigne.
3. Une partition et un état s'affichent. Si vous avez accès à plus d'une partition, utilisez les touches haut et bas pour faire défiler les partitions disponibles et localiser la partition que vous souhaitez désarmer.
4. Appuyez sur la touche **[DISARM]** pour désarmer la partition.

Si une alarme a été déclenchée alors que votre système était armé, un message s'affiche à l'écran. Pour acquitter une alarme, il suffit d'appuyer sur **[ENTER]** et de poursuivre le processus de désarmement.

Saisie d'un code de contrainte

Si vous êtes contraint d'armer ou de désarmer votre système ou de déverrouiller une porte, vous pouvez entrer un **code de contrainte**, qui complétera l'action et transmettra immédiatement un message d'alerte silencieux à la station de surveillance.

Selon la configuration de votre système, vous pouvez avoir l'un des deux types de code de contrainte courants :

- Un code de contrainte d'utilisateur désigné qui s'applique généralement à l'ensemble du site.
- Un code de contrainte spécifique qui est égal à votre code d'utilisateur habituel plus un. Par exemple, si votre NIP est 1234, le code de contrainte sera 1235.

  Notez que le compteur +1 ne s'applique qu'au dernier chiffre. Ainsi, si le NIP de l'utilisateur est 1239, le NIP pour déclencher un code de contrainte sera 1230.

Les fonctions du code de contrainte doivent être activées avant de pouvoir être utilisées. Votre installateur peut confirmer laquelle de ces options a été configurée et vous fournir des instructions d'utilisation supplémentaires.

Acquittement d'une alarme

Les alarmes sont stockées en mémoire jusqu'à ce qu'elles soient acquittées.

- Pour acquitter une alarme, il suffit d'appuyer sur **[ENTER]** et de poursuivre le processus de désarmement.
- Si vous procédez au désarmement sans acquitter l'alarme, vous pouvez la visualiser plus tard en appuyant sur **[MENU]** + **[MEMORY]** et **[ENTER]** puis en utilisant les touches fléchées pour visualiser les détails. Appuyez sur **[ENTER]** pour acquitter et effacer l'alarme de la mémoire.

Utilisation des lecteurs de cartes

Les lecteurs de proximité fonctionnent en émettant constamment un champ de radiofréquences (RF) de courte portée. Lorsqu'une carte d'accès se trouve à portée de ce champ, une puce intégrée dans la carte transmet un numéro de carte au lecteur.Le lecteur envoie ces détails au système de sécurité, qui vous accorde ou vous refuse l'accès en fonction de vos autorisations.

De nombreux lecteurs de cartes sont également dotés de capacités Bluetooth® et NFC, ce qui permet aux utilisateurs d'obtenir un accès avec des informations d'identification mobiles à l'aide de l'application mobile Protege.

Présentation des cartes

Il peut être utile de considérer un lecteur de carte en tant qu'agent de sécurité. Lors d'une demande d'accès, le lecteur doit être muni de vos informations d'identification, tout comme un agent de sécurité peut inspecter une carte d'identité. Pour accéder à une partition par une porte munie d'un lecteur de cartes d'accès, il suffit de présenter votre carte d'accès au lecteur.

Si vous utilisez l'application mobile Protege, vous pouvez déverrouiller les portes avec votre téléphone en utilisant le Bluetooth® ou la NFC. Pour déverrouiller une porte, connectez-vous à l'appli et gardez-la ouverte ou réduite sur votre téléphone, puis présentez votre téléphone au lecteur de carte. Pour déverrouiller la porte à de plus grandes distances, augmentez la **portée Bluetooth** ou utilisez la fonction **Shake to Unlock (secouer pour déverrouiller)**.

Types de cartes

Il existe un certain nombre d'options pour les cartes de proximité modernes : 125 kHz, MIFARE et DESFire. Bien qu'il y ait peu de différences visibles entre les différents types de cartes, ce qui se passe en coulisses est très différent.

Historiquement, les systèmes de contrôle d'accès par carte étaient basés sur une carte avec une bande magnétique qui devait être glissée dans un lecteur de carte magnétique pour accéder à une porte. Ces cartes présentaient un certain nombre d'inconvénients, notamment un taux d'usure élevé et une très faible sécurité.

Les technologies de proximité plus récentes permettent de lire les cartes sans contact physique avec le lecteur et, outre la fréquence utilisée pour transmettre les données, il existe des différences essentielles en matière de sécurité et de portée de lecture des cartes.

- Les cartes à 125 kHz offrent une bonne portée de lecture (environ 10 cm) et un temps de lecture court, ce qui signifie que vous pouvez effectivement présenter, faire glisser ou agiter votre carte dans la direction générale du lecteur pour obtenir une lecture réussie.
- MIFARE a une portée de lecture légèrement réduite (environ 7 cm) et un temps de lecture plus long, ce qui signifie qu'en général, une carte MIFARE ne peut pas être simplement glissée ou agitée sur un lecteur de carte, mais doit être présentée.
- DESFire est le plus haut standard de sécurité de carte actuellement disponible, cependant il a une portée de lecture encore réduite de 1 à 2 cm. Ainsi, une carte DESFire doit être fermement présentée au lecteur et maintenue en place jusqu'à ce que l'accès soit autorisé. Si vous agitez ou faites glisser une carte DESFire, la lecture ne sera pas réussie.

Discutez avec votre installateur de la technologie de carte d'accès utilisée sur votre site.

Mode d'entrée

Votre installateur aura programmé les portes de votre système avec un mode d'entrée qui contrôle le fonctionnement d'une porte. Cela inclut :

- **Carte uniquement** : un passe à carte est tout ce qui est nécessaire pour déverrouiller la porte.
- **Carte et NIP** : un passe à carte et un NIP sont tous deux nécessaires pour déverrouiller la porte.
- **Carte ou NIP** : un passe à carte ou un NIP peut être utilisé pour déverrouiller la porte.
- **NIP uniquement** : un NIP est tout ce qui est nécessaire pour déverrouiller la porte.

Le mode utilisé peut varier en fonction des exigences de votre système et peut également être programmé en fonction de l'heure de la journée, ce qui permet d'utiliser différentes informations d'identification de sécurité. Par exemple, une porte peut être programmée pour n'exiger qu'un accès par carte entre les heures normales de bureau (de 8 h à 17 h), mais nécessiter une carte et un NIP en dehors de ces heures pour plus de sécurité.

Armement et désarmement à partir d'un lecteur de cartes

En fonction de la programmation de votre système, vous pourrez peut-être désarmer la partition derrière une porte, simplement en faisant glisser votre carte pour déverrouiller la porte. Ainsi, vous n'aurez plus besoin de désarmer la partition à l'aide d'un clavier après être entré.

En général, les systèmes sont configurés pour vous permettre d'armer la partition derrière une porte à partir d'un lecteur de carte. Il existe quelques options courantes :

- Faites glisser sur le lecteur deux fois pour armer la partition.
- Faites glisser sur le lecteur trois fois pour armer la partition.
- Tenez un bouton et un passe sur le lecteur pour armer la partition.

Votre installateur peut confirmer si ces options sont activées.

Utilisation de serrures hors ligne

Les serrures sans fil hors ligne fonctionnent différemment des lecteurs de cartes câblés du système. Au lieu d'envoyer vos informations d'identification au système pour validation, les serrures hors ligne utilisent les données d'accès stockées sur votre carte ou votre téléphone mobile pour valider vos autorisations d'accès.

Les lecteurs des points de mise à jour situés à des endroits clés tels que la porte d'entrée sont utilisés pour mettre à jour et renouveler les données stockées sur vos informations d'identification. Vous devez présenter régulièrement vos informations d'identification au lecteur du point de mise à jour, car les données expirent au bout d'un certain temps (généralement tous les 30 jours). Le lecteur clignote rapidement en violet pendant qu'il met à jour vos données, puis clignote en vert et émet un signal sonore lorsqu'il déverrouille la porte.

Patientez pendant que le lecteur de point de mise à jour met à jour la carte. Ne retirez pas la carte tant que le lecteur n'a pas cessé de clignoter en violet.

Les serrures sans fil ont différents modes de fonctionnement :

- **Standard** : Lorsque vous obtenez l'accès, la porte se déverrouille temporairement.
- **Déverrouillage sur horaire** : La porte se déverrouille en fonction d'un horaire spécifique (par exemple, les heures de travail).
- **Déverrouillage du bureau** : Tout utilisateur autorisé peut déverrouiller la porte temporairement, mais des utilisateurs spécifiques (par exemple les responsables) peuvent déverrouiller la porte indéfiniment en maintenant la poignée intérieure enfoncée et en présentant des informations d'identification au lecteur. Répétez la procédure pour reverrouiller la porte.
- **Basculer** : Chaque fois qu'un utilisateur autorisé accède à la porte, la serrure bascule entre marche arrêt.
- **La sortie laisse la porte déverrouillée** : Lorsque quelqu'un sort par la porte en utilisant la poignée intérieure, celle-ci reste déverrouillée. Selon les réglages, elle se verrouille à nouveau après un certain temps ou reste déverrouillé jusqu'à ce que quelqu'un badge une carte.

Chaque serrure peut utiliser différents modes en fonction de différents horaires (par exemple, le mode de déverrouillage du bureau pendant les heures de bureau, puis le mode standard après les heures de bureau).

En outre, avec certains modèles de serrure, vous pouvez utiliser la molette intérieure ou la clé pour activer le **mode privé**. Ainsi, toute personne essayant de déverrouiller la porte depuis l'extérieur se verra refuser l'accès, à moins qu'elle ne dispose d'une clé ou de droits de super-utilisateur.

Concepteurs et fabricants de produits électroniques intégrés de contrôle d'accès, de sécurité et d'automatisation.
Conçus et fabriqués par Integrated Control Technology Ltd.