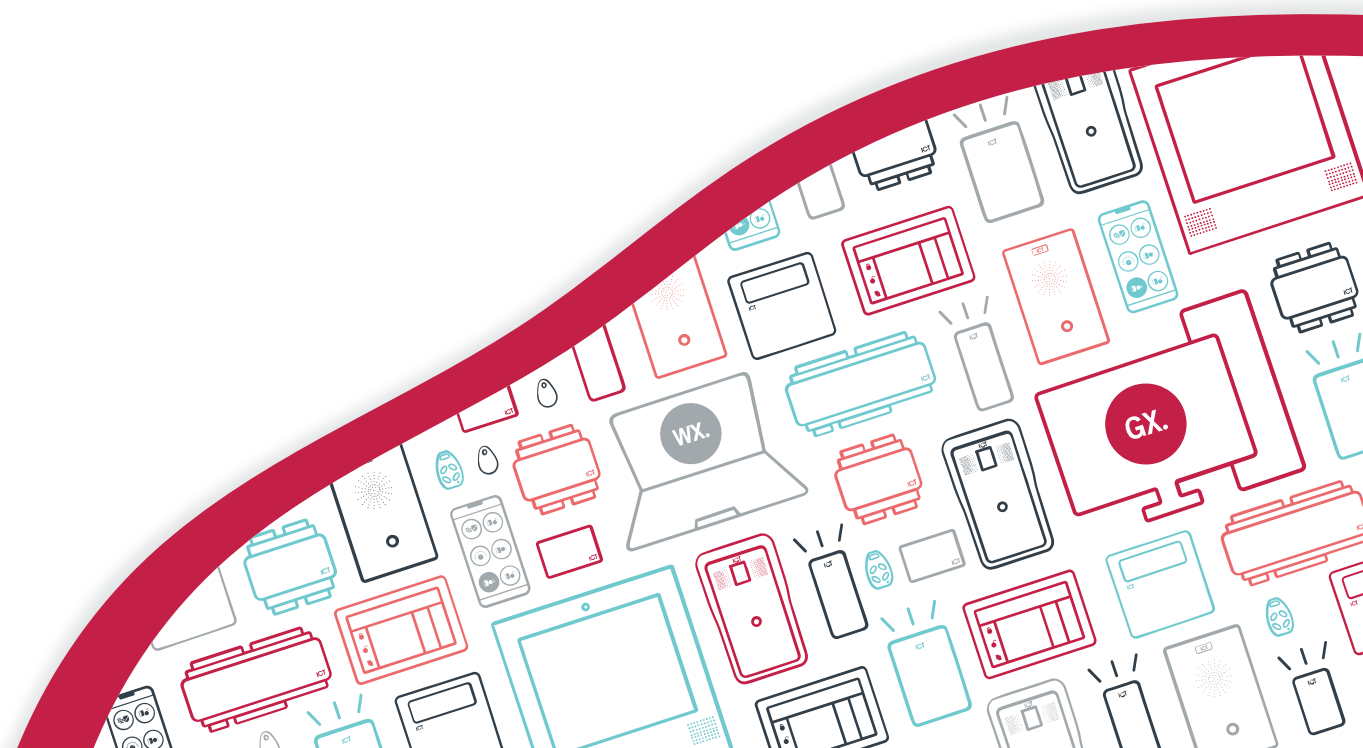
PRT-WX-DIN

Protege WX

Guide de l'utilisateur final



Dernière publication en 04-juil.-22 08:52.

Contenu

Comprendre votre système Protege WX

Protege WX est un système flexible basé sur le Web qui vous permet de programmer, de surveiller et de contrôler un site à partir de n'importe quel téléphone intelligent, tablette ou ordinateur disposant d'une connexion réseau fixe ou mobile. Il combine le contrôle d'accès, l'intrusion par alarme, l'automatisation et le contrôle, le tout dans un seul ensemble unifié.

Le système peut comprendre plusieurs éléments :

- Le **contrôleur Protege WX**, 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 l'état actuel du système. Chaque clavier se trouve généralement dans un endroit pratique à l'intérieur de vos installations, près de la porte de sortie et d'entrée.
- Un ou plusieurs **lecteurs de cartes** qui sont utilisés pour contrôler l'accès à la ou aux portes de votre bâtiment.

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.

Ouverture de session

Pour accéder au système après la configuration initiale, vous devez vous connecter avec un nom d'utilisateur et un mot de passe d'opérateur valides.

1. Ouvrez un navigateur Web et entrez l'adresse IP du contrôleur, avec le préfixe https:// (par exemple, https://192.168.1.2).

   Si vous ne pouvez pas accéder au contrôleur avec cette URL, supprimez le préfixe https:// (par exemple, 192.168.1.2).

2. Si un avertissement de sécurité s'affiche lorsque vous accédez à la page Web HTTPS, utilisez les options avancées pour accéder à la page Web du contrôleur.
3. La fenêtre **Connexion** s'affiche.
4. Entrez votre **nom d'utilisateur** et votre **mot de passe** de l'opérateur .
5. Cliquez sur **Connexion**.

La saisie répétée de mots de passe incorrects dans la fenêtre d'ouverture de session entraîne l'arrêt de la connexion. Trois tentatives incorrectes consécutives entraînent le verrouillage de la fenêtre d'ouverture de session pendant cinq secondes. Si trois autres tentatives échouent, l'identification en cours est verrouillée pendant 60 secondes entre toutes les tentatives suivantes jusqu'à ce qu'une connexion valide soit effectuée. Il n'est pas possible de configurer la durée de l'interruption de la connexion.

Les contrôleurs à une porte peuvent nécessiter des étapes supplémentaires pour accéder à l'interface Web. Pour plus d'informations, consultez la section Navigation vers les contrôleurs à une porte (ci-dessous).

Navigation vers les contrôleurs à une porte

Les contrôleurs à une porte utilisent un ancien type de matériel qui ne prend pas en charge les protocoles de sécurité et les suites de chiffrement plus récents. Ainsi, les navigateurs Web modernes ne font pas confiance à tout contrôleur à une porte sur lequel un certificat de sécurité est installé. La plupart des navigateurs Web ne permettront pas aux utilisateurs d'accéder aux pages d'interface Web de ces contrôleurs, même si les utilisateurs font confiance au site et acceptent le risque.

Si vous avez un contrôleur à une porte, vous pouvez voir l'une des erreurs suivantes lorsque vous tentez d'accéder à l'interface Web :

- **Chrome** : « Ce site ne peut être atteint »
- **Edge** : « Mmmm... Impossible d'atteindre cette page »
- **Firefox** : « La connexion sécurisée a échoué » (PR_END_OF_FILE_ERROR)

Dans cette situation, la solution recommandée est d'autoriser l'accès à l'interface Web du contrôleur en créant un profil Firefox avec une sécurité réduite.

Pour éviter les failles de sécurité, il est recommandé d'utiliser ce profil uniquement pour accéder aux contrôleurs à une porte.

1. Téléchargez et installez Firefox à partir du site Web de Mozilla si vous ne l'avez pas déjà.
2. Ouvrez Firefox, tapez **about:profiles** dans la barre URL et appuyez sur **Entrée**.
3. Cliquez sur **Créer un nouveau profil** pour ouvrir l'assistant.
4. Cliquez sur **Suivant**.
5. Entrez un nom de profil descriptif (par exemple, Contrôleur).
6. Cliquez sur **Terminer**.
7. Cliquez sur **Lancer le profil dans un nouveau navigateur**.

   Vous pouvez revenir à la page **about:profiles** à tout moment pour passer d'un profil à l'autre ou définir un profil par défaut.
8. Dans le nouveau navigateur, tapez **about:config** dans la barre URL et appuyez sur **Entrée**.
9. Cliquez sur **Accepter le risque et continuer**.
10. Dans la barre de recherche, entrez **security.tls.version.enable-deprecated**.
11. Par défaut, cette valeur est définie sur false. Cliquez sur le bouton à bascule à droite pour le définir sur true.
12. Essayez de naviguer vers votre contrôleur sur https://192.168.1.2 (utilisez l'adresse configurée de votre contrôleur si elle a été modifiée par rapport à la valeur par défaut). Firefox signalera qu'il existe un risque potentiel de sécurité, car le contrôleur possède un certificat auto-signé.
13. Cliquez sur **Avancé...**
14. Cliquez sur **Accepter le risque et continuer**.
15. Le navigateur présente l'écran de connexion du contrôleur. À l'avenir, vous devriez être en mesure de naviguer vers ce contrôleur en utilisant ce profil d'utilisateur Firefox.

Gestion des utilisateurs

Un **utilisateur** est une personne qui a besoin d'accéder à l'installation contrôlée par le système. Chaque utilisateur possède des identifiants 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.

Ajout d'un utilisateur

1. Naviguez vers **Utilisateurs | Utilisateurs**, cliquez sur **Ajouter**.
2. Entrez un **prénom** et un **nom** pour l'utilisateur.
3. Saisissez un **code NIP**. Il s'agit du numéro que l'utilisateur doit entrer lorsqu'il se connecte à un clavier ou accède à une porte qui nécessite un code NIP.
4. Saisissez l'identifiant (les identifiants) de l'utilisateur en tapant les numéros d'installation et de carte correspondants dans les champs disponibles.

   Chaque utilisateur peut avoir jusqu'à huit numéros de carte. Les numéros de carte multiples permettent au même utilisateur d'avoir plusieurs identifiants (tels que les cartes, les porte-clés, les identifiants mobiles et les télécommandes sans fil), sans qu'il soit nécessaire de programmer des enregistrements d'utilisateurs en double.
5. 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 (ci-dessous).
6. Cliquez sur **Ajouter**, sélectionnez le(s) niveau(x) d'accès approprié(s) et cliquez sur **OK**.
7. Cliquez sur le bouton **Enregistrer** dans la barre d'outils pour enregistrer le nouvel utilisateur. L'utilisateur peut maintenant utiliser les identifiants 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 **Expiration** et en définissant 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 identifiants 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 et cliquez sur **Enregistrer**.

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.

Si le mode avancé est activé, les groupes de partitions d'un niveau d'accès sont séparés en **groupes de partitions d'armement** et **groupes de partitions de désarmement**, ce qui vous permet de différencier les partitions qu'un utilisateur est autorisé à armer ou à désarmer. Par exemple, les nettoyeurs peuvent être autorisés à armer une partition mais pas à la désarmer.

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

1. Sélectionnez l'onglet **Groupes de partitions** et cliquez sur **Ajouter**.
2. Choisissez le groupe de partitions concerné et cliquez sur **OK**.
3. Définissez l'**horaire** à utiliser. Par défaut, l'horaire est fixé à 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 zones, reportez-vous au Manuel de référence de programmation Protege WX ou demandez à votre installateur.

Suppression des utilisateurs

Vous pouvez facilement supprimer les enregistrements d'utilisateurs qui ne sont plus nécessaires.

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

Important : la suppression d'un utilisateur supprime **toute** référence à cet utilisateur dans le journal des événements. La méthode recommandée pour supprimer un utilisateur actif est de le désactiver d'abord (voir ci-dessous) jusqu'à ce que ses événements ne soient plus nécessaires.

Désactivation des utilisateurs

Le paramètre **Désactiver l'utilisateur** (situé sous l'onglet **Options**) supprime immédiatement l'accès tout en conservant l'enregistrement 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.

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 jusqu'à **Horaire | Groupes de jours fériés** et cliquez sur **Ajouter**.
2. Entrez un **Nom** pour le groupe de vacances.
   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.
3. Cliquez sur **Enregistrer**. 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 vers **Horaire | Horairesi**.
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 12).

   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 **que** 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. Naviguer vers **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 (consultez la page 8) 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 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.

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 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.

Travailler avec les rapports

Les rapports d'événements permettent à un opérateur de créer, de visualiser et d'exporter des rapports personnalisés en fonction des utilisateurs, des portes et des partitions.

Création d'un rapport d'événement

1. Naviguez vers **Surveillance | Rapports | Rapports d'événement** et entrez un **Nom** pour le rapport.

   Un nom n'est nécessaire que si vous souhaitez enregistrer le rapport. Si vous souhaitez simplement visualiser les événements au fur et à mesure qu'ils se produisent, la saisie d'un nom est facultative.

2. Entrez une **date de début** et une **date de fin** valides.
3. Pour inclure tous les événements, il suffit de cliquer sur **Enregistrer**, **Voir** ou **Exporter**.

   ou-

   Pour filtrer en fonction des utilisateurs, des portes ou des partitions, utilisez les onglets supplémentaires. Un certain nombre de scénarios de rapport fréquents, ainsi que les critères de filtrage requis, sont présentés ci-dessous.

   La limite du nombre d'enregistrements que vous pouvez sélectionner est de 1 500. Si vous sélectionnez plus que ce nombre d'enregistrements et essayez de sauvegarder le rapport, vous verrez une erreur. En raison d'une limitation connue, il n'est pas possible de supprimer les enregistrements excédentaires et de sauvegarder le rapport à nouveau; vous devrez recréer le rapport à partir de zéro.

4. Cliquez sur **Voir** pour afficher les événements pertinents.
5. Cliquez sur **Exporter** pour enregistrer les événements au format CSV, ce qui vous permet d'extraire des données d'événements qui peuvent ensuite être formatées et manipulées selon les besoins.

   En fonction des paramètres de votre navigateur, vous pouvez être invité à enregistrer le fichier. Sinon, il sera automatiquement téléchargé dans votre dossier « Téléchargements ».

Scénarios de rapport communs

Les scénarios suivants concernent les exigences communes en matière de rapports et les options à choisir :

- Pour visualiser l'activité d'**un ou de plusieurs utilisateurs** particuliers, définissez une plage de dates/heures et sélectionnez les utilisateurs concernés.
- Pour visualiser l'activité d'**une ou de plusieurs portes** particulières, définissez une plage de dates/heures et sélectionnez les portes concernées.
- Pour déterminer si un **utilisateur spécifique a eu accès à une porte particulière**, définissez une plage de dates/heures et sélectionnez l'utilisateur et la porte concernés.
- Pour déterminer **quel utilisateur a armé ou désarmé une partition**, définissez une plage de dates/heures et sélectionnez la partition concernée.
- Pour déterminer si un **utilisateur spécifique a armé ou désarmé une partition** particulière, définissez une plage de dates/heures et sélectionnez l'utilisateur et la partition concernés.

Utilisation d'un clavier pour armer/désarmer votre système

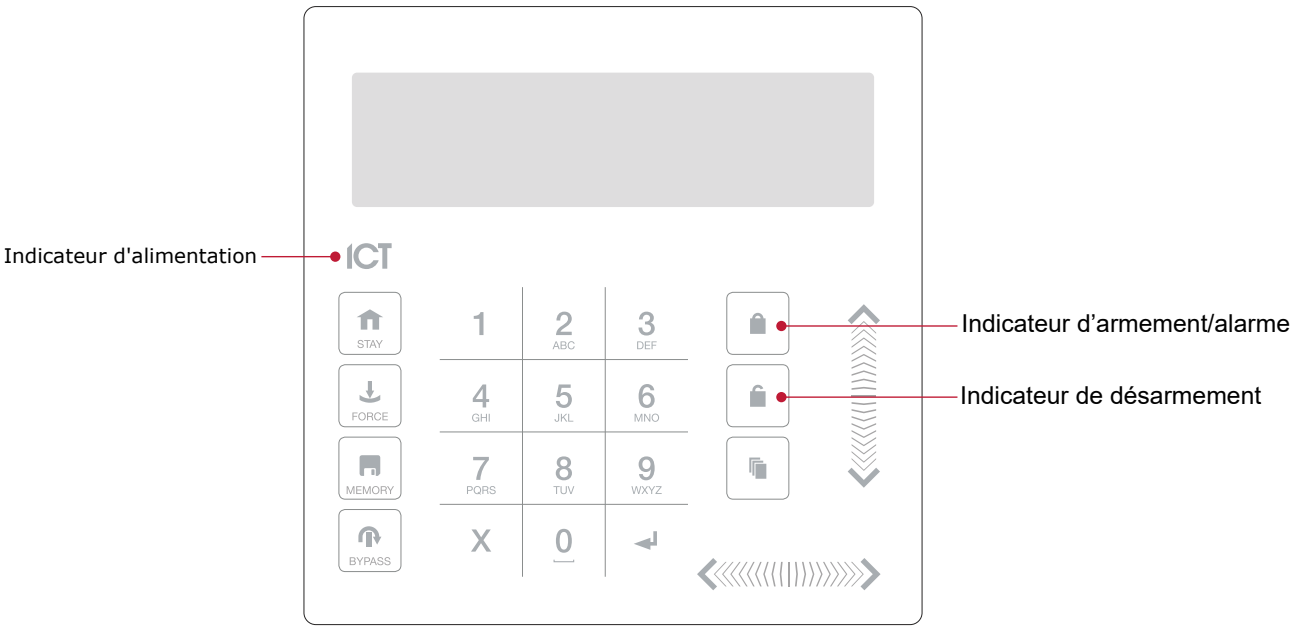
Les claviers sont généralement situés près d'une entrée ou d'une porte pour permettre d'armer et de désarmer les partitions du système.

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 de 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 **étient**.

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 tonalite 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 deux secondes, le clavier la reconnaît comme étant 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'affichent.

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, entrez le code 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.

Déconnection

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 **[ARMER]** 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 **[ENTRÉE]** 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]** + **[MEMOIRE]** et **[ENTRÉE]** puis en utilisant les touches fléchées pour visualiser les détails. Appuyez sur **[ENTRÉE]** 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) à courte portée. Lorsqu'une carte d'accès se trouve à portée de ce champ, une puce intégrée à la carte renvoie un numéro de carte au lecteur, qui transmet ces informations au système, qui vous accorde ou vous refuse l'accès en fonction de vos autorisations.

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 identifiants, 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.

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. Il s'agit notamment des éléments suivants :

- **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 différents identifiants 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.

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