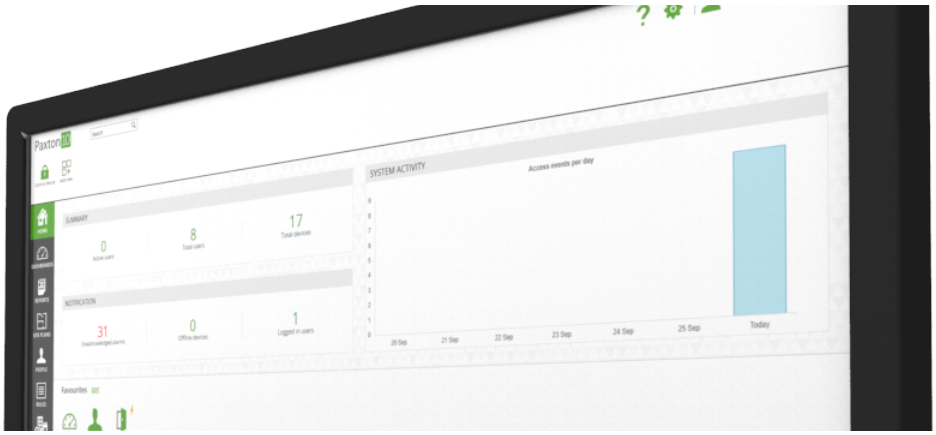

Utilisation de clavier avec Paxton10

Présentation

Les lecteurs clavier peuvent être un excellent moyen de renforcer la sécurité et d'assurer une protection contre l'utilisation d'authentification perdue ou volée. Les lecteurs clavier ajoutent des modes de fonctionnement de lecteur supplémentaires à un point d'accès ou un appareil contrôlable.

Mode de fonctionnement du lecteur	Action utilisateur requise	Utilisateur identifié
Badge uniquement	Présentez un badge de proximité valide.	O
PIN uniquement	Saisissez le PIN de l'utilisateur sur le clavier.	O
Code uniquement	Saisissez l'un des codes de l'appareil sur le clavier.	N
Badge + PIN	Présentez un badge de proximité valide, puis saisissez le PIN de l'utilisateur. Le titulaire du badge et le PIN doivent appartenir au même utilisateur.	O
Badge + code	Présentez un badge de proximité valide, puis saisissez l'un des codes de l'appareil.	O
Badge ou PIN	Présentez un badge de proximité valide, OU saisissez le PIN de l'utilisateur.	O
Badge ou code	Présentez un badge de proximité valide, OU saisissez l'un des codes de l'appareil.	O/N
Badge ou PIN ou code	Présentez un badge de proximité valide, OU saisissez le PIN de l'utilisateur, OU saisissez l'un des codes de l'appareil.	O/N

Un code est spécifique à un appareil alors qu'un PIN est spécifique à un utilisateur.

Quand utiliser un lecteur Paxton10

A Paxton10 keypad reader can be installed in place of any existing Paxton10 reader.

Security

Les lecteurs clavier peuvent être utilisés pour ajouter un deuxième niveau d'authentification en exigeant des détenteurs de badge qu'ils fournissent une deuxième confirmation.

Lorsqu'utilisé en mode de fonctionnement « **badge + PIN** » ou « **badge + code** », un badge perdu ou un code entendu tout seul n'autoriserait pas l'accès au bâtiment, afin de pouvoir entrer, un intrus devrait posséder à la fois un badge valide ET son PIN associé ou son code de porte.

Convenience

Il est courant que les utilisateurs oublient leur badge, ou le laissent au travail sur leur bureau, ce qui les empêche parfois de rentrer à nouveau. Utiliser un mode de fonctionnement « **badge ou PIN** » ou « **badge ou code** » permet aux utilisateurs d'obtenir l'accès sans leur badge, ce qui peut être idéal pour les portes à basse sécurité.

Autorisations

Lorsqu'un PIN ou un badge est utilisé, l'accès est accordé par les autorisations d'accès au bâtiment de l'utilisateur. Lorsqu'un code est utilisé seul, l'utilisateur n'est pas connu et il se verra donc accordé l'accès à condition que le code soit valide sur l'appareil.

Mapper un lecteur clavier

Les lecteurs clavier sont mappés sur un appareil de la même façon que les lecteurs de proximité.

Voir AN0006-F - Comment ajouter un lecteur <www.paxton.info/6130>

Configuration d'un mode de fonctionnement du lecteur

1. Accédez à l'appareil sur lequel un lecteur est mappé
2. Dans l'onglet « **Configuration** », développez la section « **Lecteurs** »
3. Cochez la case à côté des options d'authentification pour activer la sélection du mode de fonctionnement
4. Sélectionnez le mode de fonctionnement requis

Pour les points d'accès, les lecteurs d'entrée et de sortie peuvent avoir différents modes de fonctionnement (par exemple, exiger un badge + PIN pour entrer dans le bâtiment, mais seulement un badge pour quitter le bâtiment).

5. Si les informations d'identification Bluetooth (appareils intelligents ou porte-clés mains libres Paxton10) sont en cours d'utilisation, sélectionnez la portée de lecture de ces identifiants et cochez « **Vérification** » si l es utilisateurs de périphériques intelligents doivent disposer d'un code PIN ou d'une configuration biométrique sur leur appareil pour qu'ils soient valides.

Voir : AN0006-F - Comment ajouter un lecteur <www.paxton.info/6130> pour plus d'informations sur les identifiants Bluetooth.

Si un mode de fonctionnement différent est requis à une heure spécifiée, « **Authentification chronométrée** » peut être utilisée.

6. Effectuez les étapes ci-dessus pour « **Options d'authentification** »
7. Cochez la case « **Authentification chronométrée** » pour activer les modes de fonctionnement supplémentaires
8. Cliquez sur « **Sélectionner** » et choisissez le profil horaire requis pour un fonctionnement différent
9. Configurez le mode de fonctionnement du lecteur, le mode Bluetooth et les paramètres de vérification à appliquer pendant le profil horaire sélectionné

(Par exemple, les options d'authentification peuvent être définies sur un mode badge + code sécurisé, mais pendant les heures de travail quand il y a toujours des gens dans le bâtiment, une option de badge ou de code est peut être plus appropriée)

Lorsque les options d'authentification ne sont pas cochées, les lecteurs fonctionneront en mode badge uniquement.

Gestion des codes

Les codes sont gérés par appareil et peuvent être utilisés par n'importe quel utilisateur.

Lorsqu'un mode de fonctionnement par code a été sélectionné, cliquez sur « **Gérer les codes** » dans la section « **Lecteurs** » de l'appareil pour créer un code pour cet appareil. Saisissez un code, puis cliquez sur « **Ajouter** », ou sélectionnez un code existant et cliquez sur « **Supprimer** » pour le supprimer.

Chaque appareil peut avoir plusieurs codes.

Gestion des PIN

Les PIN sont uniques à chaque utilisateur et sont considérés comme une authentification dans le profil de l'utilisateur.

Pour donner une authentification PIN à un utilisateur :

1. Ouvrez le profil de l'utilisateur, et cliquez sur l'onglet « **Authentifications** »
2. Cliquez sur « **Ajouter une authentification** »
3. Sélectionnez « **PIN** » dans le menu déroulant
4. Saisissez un nouveau numéro de PIN ou acceptez celui généré aléatoirement
5. Cliquez sur « **OK** »

La longueur du PIN peut se changer dans les options du système.

Questions fréquemment posées

Quelle est la différence entre un PIN et un code ?

Un numéro d'identification personnel (PIN) est unique à chaque utilisateur. Chaque utilisateur aura son propre code PIN, et son PIN ne donnera accès qu'aux appareils pour lesquels il a les autorisations d'accès au bâtiment.

En comparaison, un code est défini sur chaque appareil et peut être utilisé par plusieurs utilisateurs. Un code ne peut pas être utilisé pour identifier un utilisateur et ne sont donc pas contraints par les autorisations d'accès au bâtiment.

Quelle est la longueur d'un PIN ?

La longueur du code PIN doit être comprise entre 4 et 8 chiffres ; ceci est configuré dans les options système. Tous les PIN d'un système doivent être de la même longueur.

Je n'ai plus de PIN uniques, que dois-je faire ?

La longueur du PIN peut être modifiée dans les options du système. L'augmentation de la longueur du code PIN augmentera le nombre possible de combinaisons de codes PIN, ce qui augmentera également la sécurité du système.

Remarque : L'augmentation de la longueur du PIN du système ajoutera « 0 » à la fin de tous les PIN existants afin de répondre à la nouvelle exigence de longueur.

Attention ! La réduction de la longueur du code confidentiel du système supprimera tous les identifiants PIN.

Quelle est la longueur d'un code ?

Les codes doivent être compris entre 4 et 8 chiffres. Des codes de longueurs différentes peuvent exister.

Pourquoi un appareil peut-il avoir plusieurs codes ?

Il existe de nombreux scénarios où plusieurs codes peuvent être donnés à un appareil, par exemple :

- Un code pour la barrière de parking donné aux visiteurs, qui change de manière hebdomadaire. Alors que le code utilisé par les employés reste constant.
- Différents codes pour représenter différents niveaux d'accès, tels que les cadres supérieurs utilisant un code qui fonctionne sur chaque appareil, et les agents de nettoyage utilisant un code différent qui ne fonctionne que sur certains appareils.

L'utilisation d'un mode de fonctionnement de code affecte-t-elle l'anti-passback ou l'appel ?

Lorsque vous utilisez le mode de fonctionnement « code uniquement », l'utilisateur n'est pas connu et la position de l'utilisateur ne peut donc pas être déterminée. Pour les rapports d'appel et la restriction anti-passback, un mode de fonctionnement comprenant un identifiant utilisateur (badge ou PIN) est requis.