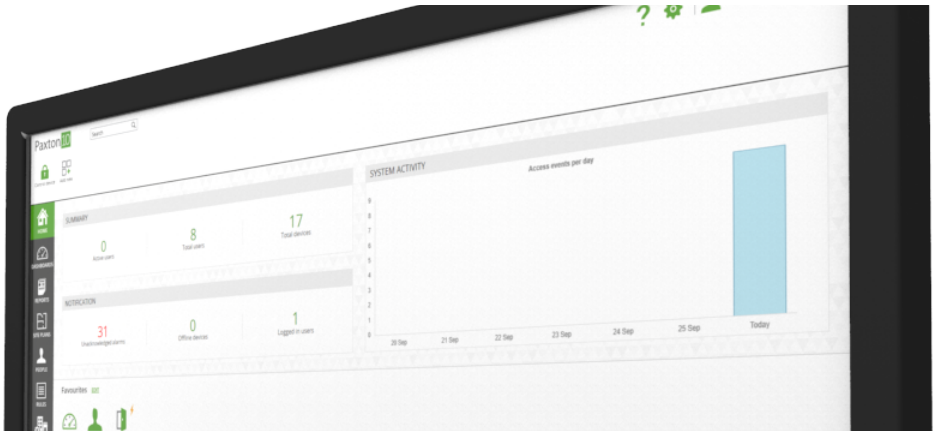

Tastaturleser mit Paxton10 verwenden

Übersicht

Tastatur-Leser können eine gute Möglichkeit sein, die Sicherheit zu erhöhen und vor verlorenen und gestohlenen Identifikationsmedien zu schützen. Tastatur-Leser erweitern einen Zutrittspunkt oder ein steuerbares Systemgerät um zusätzliche Leserbetriebsarten.

Betriebsmodus des Lesers	Benutzeraktion erforderlich	Benutzer Identifiziert
Nur Transponder	Einen gültigen Proximity-Transponder präsentieren.	J
Nur PIN	Benutzer-PIN über die Tastatur eingeben.	J
Nur Code	Einen der Systemgeräte-Codes über die Tastatur eingeben.	N
Transponder + PIN	Einen gültigen Proximity Transponder präsentieren und anschließend die Benutzer-PIN über die Tastatur eingeben. Der Transponder und die PIN muss zu demselben Benutzer gehören.	J
Transponder + Code	Einen gültigen Proximity Transponder präsentieren und anschließend einen der Systemgeräte-Codes über die Tastatur eingeben.	J
Transponder oder PIN	Einen gültigen Proximity-Transponder präsentieren ODER die Benutzer-PIN über die Tastatur eingeben.	J
Transponder oder Code	Einen gültigen Proximity-Transponder präsentieren ODER einen der Systemgeräte-Codes eingeben.	J/N
Transponder oder PIN oder Code	Einen gültigen Proximity-Transponder präsentieren ODER die Benutzer-PIN ODER einen der Systemgeräte-Codes eingeben.	J/N

Ein Code ist spezifisch für ein Systemgerät, während eine PIN spezifisch für einen Benutzer ist.

Wann wird eine Paxton10 Tastatur verwendet?

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

Security

Tastaturleser können verwendet werden, um eine zweite Authentifizierungsebene hinzuzufügen, indem Transponder-Inhaber aufgefordert werden, eine sekundäre Bestätigung zu liefern.

In der Betriebsart '**Transponder + PIN**' oder '**Transponder + Code**' würde ein verlorener Transponder oder zufällig abgehörter Code allein keinen Zugang zum Gebäude ermöglichen, um Zutritt zu erhalten, müsste ein Eindringling sowohl einen gültigen Transponder als auch den zugehörigen PIN- oder Tür-Code besitzen.

Convenience

Es ist nicht unüblich, dass Benutzer ihren Transponder vergessen, oder ihn auf dem Schreibtisch liegen lassen, was ihnen die Möglichkeit gibt, ausgesperrt zu werden. Die Betriebsart ‚**Transponder oder PIN**' oder ‚**Transponder oder Code**' ermöglicht dem Benutzer den Zugang ohne Transponder, was für Türen mit geringerem Sicherheitslevel ideal sein kann.

Berechtigungen

Bei Verwendung einer PIN oder eines Transponders wird der Zutritt durch die Gebäudeberechtigungen des Benutzers geregelt. Wenn nur ein Code verwendet wird, ist der Benutzer nicht bekannt und erhält daher nur Zutritt, wenn er den am Systemgerät gültigen Code eingeben kann.

Zuordnung eines Tastatur-Lesers

Tastaturleser werden genauso wie Proximity-Leser einem Gerät zugeordnet.

Siehe AN0006-D So fügen Sie einen Leser hinzu <www.paxton.info/6131>

Konfigurieren des Betriebsmodus eines Lesegeräts

1. Navigieren Sie zu dem Gerät, dem ein Leser zugeordnet ist.

2. Erweitern Sie in der Registerkarte ‚Konfiguration' den Abschnitt 'Leser'.

3. Aktivieren Sie das Kontrollkästchen neben den Authentifizierungsoptionen, um die Auswahl der Betriebsmodi zu aktivieren.

4. Wählen Sie den gewünschten Betriebsmodus.

Für Zugangspunkte, Eingangs- und Ausgangsleser können verschiedene Betriebsmodi haben (z. B. erfordern einen Transponder + PIN für das Betreten des Gebäudes, aber nur einen Transponder für das Verlassen des Gebäudes).

5. Wenn Bluetooth-Berechtigungsnachweise (Smart-Geräte oder Paxton10-Freisprech-Schlüsselanhänger) verwendet werden, wählen Sie den Lesebereich dieser Berechtigungsnachweise aus und markieren Sie ‚Verifizierung', wenn Benutzer von Smart-Geräten eine PIN oder eine biometrische Einrichtung auf ihrem Gerät benötigen, um gültig zu sein.

Siehe: AN0006 - Wie man ein Lesegerät hinzufügt <www.paxton.info/6131> für weitere Informationen über Bluetooth-Identifikationsmedien.

Wenn zu einer bestimmten Zeit ein anderer Betriebsmodus erforderlich ist, kann eine ‚zeitgesteuerte Authentifizierung' verwendet werden.

6. Führen Sie die oben genannten Schritte für ‚**Authentifizierungsoptionen**' durch.

7. Aktivieren Sie das Kästchen neben ‚Zeitgesteuerte Authentifizierung', um die zusätzlichen Betriebsmodi zu aktivieren.

8. Klicken Sie auf ‚**Auswählen**' und wählen Sie das für verschiedene Operationen erforderliche Zeitprofil.

9. Konfigurieren Sie den Betriebsmodus des Lesegeräts, den Bluetooth-Modus und die Authentifizierungsoptionen, die während des gewählten Zeitprofils gelten sollen.

(Zum Beispiel können die Authentifizierungsoptionen auf einen sicheren Transponder + Code-Modus eingestellt werden, aber während der Arbeitszeiten, wenn sich ständig Personen im Gebäude aufhalten, kann eine bequemere Token- oder Code-Option angebracht sein.)

Wenn die Authentifizierungsoptionen nicht aktiviert sind, arbeiten die Lesegeräte nur mit dem Transponder.

Codes verwalten

Die Codes werden pro Gerät verwaltet und können von jedem Benutzer verwendet werden.

Wenn eine Code-Betriebsmodus eingestellt wurde, klicken Sie auf‚Codes verwalten' in der Registerkarte‚Leser', um einen Code für dieses Gerät zu erstellen. Geben Sie einen Code ein, klicken Sie dann auf‚**Hinzufügen**', oder wählen Sie einen vorhandenen Code aus und klicken Sie auf‚Entfernen', um ihn zu löschen.

Jedes Gerät kann mehrere Codes haben.

PINs Verwalten

PINs sind für jeden Benutzer eindeutig und werden als Berechtigungsnachweis innerhalb des Benutzerdatensatzes behandelt.

Um einem Benutzer eine PIN zu geben:

1. Öffnen Sie den Datensatz des Benutzers und klicken Sie auf die Registerkarte "**Identifikationsmedien**".
2. Klicken Sie auf '**Identifikationsmedium hinzufügen**'.
3. Wählen Sie 'PIN' aus dem Drop-Down-Menü.
4. Geben Sie eine neue PIN-Nummer ein oder akzeptieren Sie die zufällig generierte.
5. Klicken Sie auf '**OK**'.

Die PIN-Länge kann in den Systemoptionen geändert werden.

Häufig gestellte Fragen

Was ist der Unterschied zwischen einer PIN und einem Code?

Eine persönliche Identifikationsnummer (PIN) ist für jeden Benutzer einzigartig. Jeder Benutzer hat seine eigene PIN, und die PIN gibt nur Zugang zu Systemgeräten frei, für die er eine Gebäudegenehmigung besitzt.

Im Vergleich wird an jedem Systemgerät ein Code festgelegt, der von mehreren Benutzern verwendet werden kann. Ein Code kann nicht verwendet werden, um einen Benutzer zu identifizieren, und ist daher nicht durch Gebäudegenehmigungen eingeschränkt.

Wie lang ist eine PIN?

Die Länge der PIN muss zwischen 4 und 8 Ziffern betragen; dies wird in den Systemoptionen konfiguriert. Alle PINs auf einem System müssen gleich lang sein.

Ich habe keine eindeutigen PIN-Nummern mehr, was soll ich tun?

Die Länge der PIN kann in den Systemoptionen geändert werden. Eine Erhöhung der PIN-Länge erhöht die Anzahl der möglichen PIN-Kombinationen und damit auch die Systemsicherheit.

Hinweis: Durch die Erhöhung der Länge der System-PINs werden am Ende aller bestehenden PINs‚0' hinzugefügt, um die neue Längenanforderung zu erfüllen.

Warnung! Eine Verringerung der Länge der System-PINs löscht alle PIN-Zugangsdaten.

Was ist die Länge eines Codes?

Codes muss zwischen 4 und 8 Ziffern sein. Es können Codes unterschiedlicher Länge existieren.

Warum kann ein Systemgerät mehrere Codes besitzen?

In vielen Szenarien in denen z.B. mehrere Codes an ein Gerät vergeben werden können:

- Ein Code für die Parkplatzschranke, der den Besuchern ausgehändigt wird und der sich wöchentlich ändert. Während der von den Mitarbeitern verwendete Code konstant bleibt.

- Unterschiedliche Codes zur Darstellung verschiedener Zugangsebenen, wie z.B. das höhere Management, das einen Code verwendet, der an jedem Gerät funktioniert, und Reinigungsunternehmen, die einen anderen Code verwenden, der nur an einigen Geräten funktioniert.

Wirkt sich die Verwendung eines Code-Betriebsmodus auf die Funktion Anti-Passback oder Benutzerlokalisierung aus?

Im Betriebsmodus ‚Nur Code' ist der Benutzer nicht bekannt, und daher kann die Position des Benutzers nicht bestimmt werden. Für Berichte zur Benutzerlokalisierung sowie Anti-Passback-Einschränkungen ist ein Betriebsmodus erforderlich, die ein Identifikationsmedium (Transponder oder PIN) enthält.