Verschlüsselte Anmeldeinformationen

Übersicht

Die Paxton10 Encrypted Credentials sind ISO-Karten und Keyfobs, die mit einer 128-Bit-AES-Verschlüsselung gesichert sind. Das schützt sie vor dem Kopieren/Klonen und vor Replay-Angriffen auf Paxton10 Leser. Im Modus "Nur verschlüsselte Zugangsdaten" können die Systeme nur verschlüsselte Zugangsdaten registrieren, um sicherzustellen, dass keine anderen Zugangsdaten böswillig oder versehentlich eingeführt werden.

Jedes Paxton10-System verwendet seinen eigenen, eindeutigen Verschlüsselungsschlüssel. Das bedeutet, dass Zugangsdaten, die in einem System registriert werden, nicht in einem anderen System registriert werden können, da die Verschlüsselungsschlüssel der Standorte nicht übereinstimmen. Bei Bedarf können die Kunden ihren Standortschlüssel ändern und ihre Anmeldedaten aktualisieren.

In diesem Anwendungshinweis wird beschrieben, wie du die Verwendung von verschlüsselten Paxton10 Zugangsdaten aktivierst, den Standortschlüssel änderst und Paxlock-Geräte mit einem Paxton10 Standort verbindest, wenn du nur verschlüsselte Zugangsdaten verwendest.

Einrichten eines Paxton10-Systems für die Verwendung verschlüsselter Anmeldeinformationen

Um Paxton10 Encrypted Credentials auf einem System zu verwenden, müssen zunächst die folgenden Schritte durchgeführt werden. Wie du diese Schritte durchführst, erfährst du weiter unten in diesem Dokument.

1. Stelle sicher, dass auf dem System Paxton10 v.4.7 SR9 oder höher läuft.
- Ab dieser Version werden die Verschlüsselungsschlüssel automatisch auf dem Paxton10 Server generiert.

2. Vergewissere dich, dass alle auf dem System installierten Paxton Entry-Türstationen auf die Softwareversion xx.xx oder höher aktualisiert wurden.
- Verschlüsselte Anmeldeinformationen werden ab dieser Version unterstützt.

3. Lege den Standortverschlüsselungsschlüssel in den Desktop-Lesern mithilfe der Desktop-Leser-Konfigurationsanwendung fest.
- Es können nur Universal-Desktop-Leser (010-392) verwendet werden, Ältere Desktop-Leser (010-387) müssen ersetzt werden, da sie keine verschlüsselten Zugangsdaten unterstützen.

4. Erstelle die verschlüsselten Zugangsdaten wie gewohnt.

5. Stelle das Paxton10 System auf den Modus "Nur verschlüsselte Zugangsdaten" ein (optional).

Verwendung der Anwendung zur Konfiguration des Desktop-Lesers

Die Konfigurationsanwendung für den Desktop-Leser dient zur Verwaltung der Sicherheitsschlüssel, die für die Verschlüsselung der Anmeldeinformationen verwendet werden. Sie kann unter /PaxtonPortal/SoftwareDownload/#!/ heruntergeladen werden und wird benötigt, um Paxton10 Encrypted Tokens anzumelden. Die Anwendung wird verwendet, um die folgenden Aufgaben auszuführen:

- Festlegen des Standortverschlüsselungsschlüssels im Desktop-Leser
- Aktualisieren der Firmware im Desktop-Leser
- Ändern des Standortverschlüsselungsschlüssels
- Erstellen eines Paxlock-Binding-Tokens

Damit die Konfigurationsanwendung für den Desktop-Leser diese Aufgaben ausführen kann, muss sie auf einem PC installiert werden, der sich im gleichen Netzwerk wie der Paxton10-Server befindet. Der Desktop-Leser muss lokal über USB mit demselben PC verbunden sein.

Hinweis: Bei Installationen an mehreren Stand orten bedeutet dies, dass die Desktop-Leser in dem lokalen Netzwerk konfiguriert werden müssen, in dem sich der Server befindet.

Sobald die Desktop-Leser konfiguriert sind, können sie auf jedem Client-Arbeitsplatz wie bei den Vorgängerversionen verwendet werden. Die Anwendung muss also nur auf einem PC installiert und für die Konfiguration aller Desktop-Leser des Systems verwendet werden.

Um die Anwendung zu nutzen, ist ein Login des Systemingenieurs erforderlich.

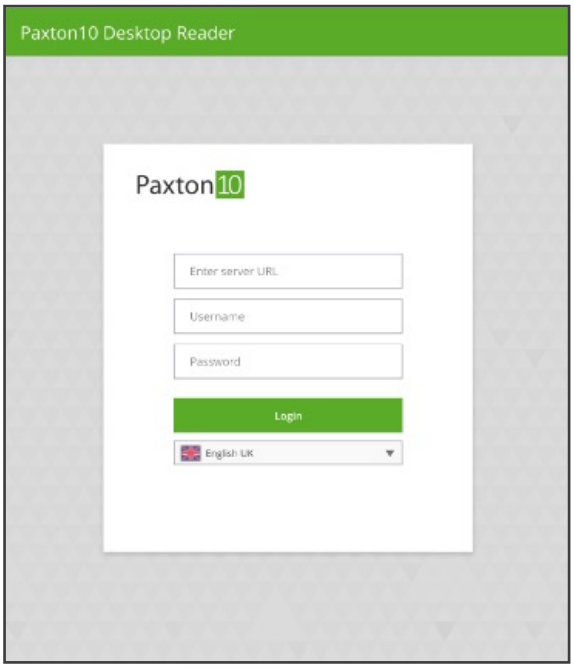
Festlegen des Verschlüsselungsschlüssels für die Standort in einem Desktop-Leser

Dies ist die häufigste Verwendung für die Konfigurationsanwendung. Alle Desktop-Leser, die verschlüsselte Anmeldedaten erfassen sollen, müssen diesen einfachen Prozess durchlaufen.

1. Stelle sicher, dass der Desktop-Leser angeschlossen ist, bevor du die Anwendung startest.

2. Wenn du die Anwendung startest, werden die Paxton10 Anmeldedaten abgefragt.

3. Sobald du eingeloggt bist, sucht die Anwendung automatisch nach dem angeschlossenen Desktop-Leser und überträgt die Verschlüsselungsschlüssel der Standort auf das Gerät.



4. Die Anwendung kann nun geschlossen werden und der Desktop-Leser ist bereit, um verschlüsselte Anmeldedaten zu erfassen.

Aktualisieren der Firmware eines Desktop-Lesers

Der universelle Desktop-Leser Paxton10 kann über die Konfigurationsanwendung des Desktop-Lesers Firmware-Upgrades empfangen.

1. Stelle sicher, dass der Desktop-Leser angeschlossen ist.

2. Wenn du die Anwendung aufrufst, werden die Paxton10 Anmeldedaten abgefragt.

3. Sobald du eingeloggt bist, sucht die Anwendung automatisch nach dem angeschlossenen Desktop-Leser und prüft dessen aktuelle Firmware-Version.

4. Wenn die Anwendung eine neuere Firmware-Version hat als die installierte, wird ein automatisches Update durchgeführt.

5. Nach der Aktualisierung kann die Anwendung geschlossen werden.

Ändern des Verschlüsselungscodes der Standort

Mit Hilfe der Konfigurationsanwendung kann der Verschlüsselungsschlüssel eines Standorts geändert werden. Dies kann geschehen, wenn die Schlüssel entdeckt werden oder wenn ein Standort sich regelmäßig entscheidet, seinen Schlüssel zu ändern.

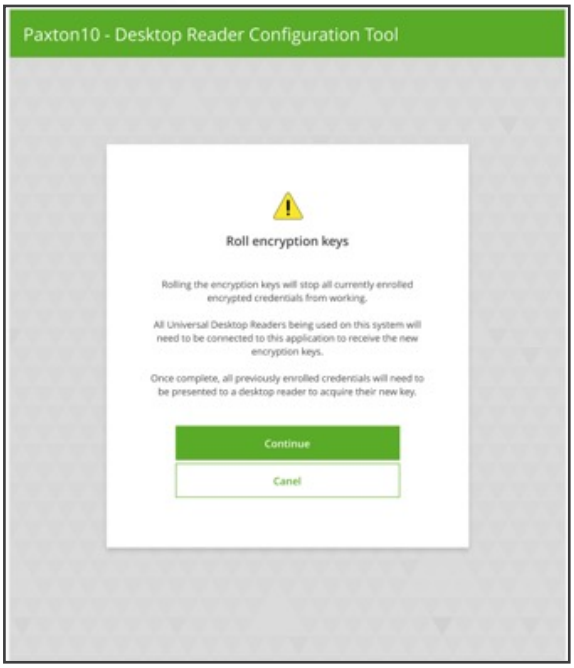
Sobald der Schlüssel eines Systems geändert wurde.

- Muss der Verschlüsselungsschlüssel jedes Desktop-Lesers aktualisiert werden.
- Alle verschlüsselten Zugangsdaten müssen an einen aktualisierten Desktop-Leser zurückgegeben werden, damit ihr Verschlüsselungsschlüssel geändert wird und sie weiterhin im System funktionieren.
- Bei den Lesern im System wird der Schlüssel automatisch aktualisiert.

1. Beim Ausführen der Anwendung werden die Paxton10 Anmeldedaten abgefragt.

2. Wähle die Option "Schlüssel ändern".

3. Es wird eine Warnmeldung angezeigt, in der beschrieben wird, welche Schritte nach der Änderung der Schlüssel unternommen werden müssen.



4. Klicke auf "Weiter". Ein neuer Schlüssel wird auf dem Paxton10 Server generiert und an den Desktop-Leser gesendet (falls ein solcher angeschlossen ist)

5. Die Anwendung kann geschlossen werden.

Ein Paxlock Binding Token erstellen

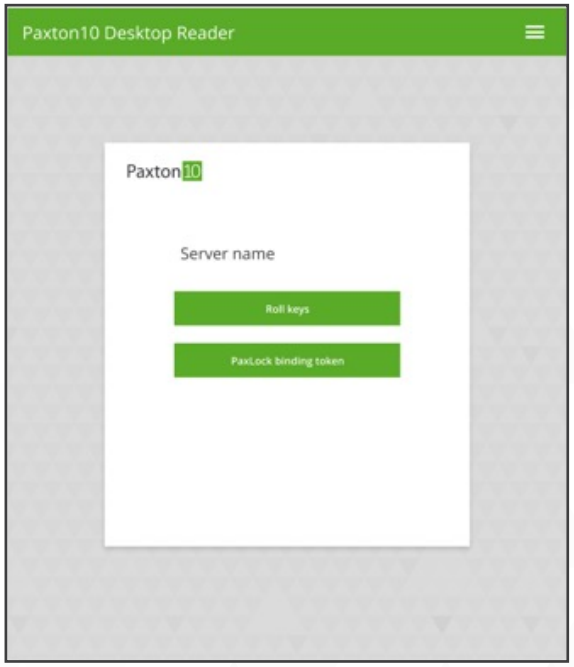
Wenn du im Modus "Nur verschlüsselte Zugangsdaten" arbeitest, müssen alle Leser die Verschlüsselungsschlüssel besitzen, um die Zugangsdaten lesen zu können. Wenn ein neues Paxlock zu einem System hinzugefügt werden muss, ist die normale Methode, dem Paxlock ein gültiges Token vom System vorzulegen. Im Modus "Nur verschlüsselte Zugangsdaten" kann das Paxlock die Zugangsdaten jedoch erst lesen, wenn es an das System gebunden ist und die Verschlüsselungsschlüssel der Standort erhalten hat.

Um dies zu umgehen, kann mit der Konfigurationsanwendung des Desktop-Lesers ein Paxlock-Bindungs-Token mit einem der verschlüsselten Zugangsdaten erstellt werden. So können neue Paxlocks gebunden werden, ohne die Integrität des Systems zu gefährden, das nur verschlüsselt ist.

1. Stelle sicher, dass ein Desktop-Leser an den PC angeschlossen ist, auf dem die Anwendung läuft.

2. Wenn du die Anwendung startest, werden die Paxton10 Anmeldedaten abgefragt.

3. Wähle die Option "Paxlock Binding Token erstellen".



4. Lege dem Desktop-Leser einen verschlüsselten Berechtigungsnachweis vor.

5. Der Desktop-Leser wandelt das Token in ein Paxlock-Binding-Token um, mit dem nun neue Paxlocks mit dem System verbunden werden können.

6. Die Anwendung kann geschlossen werden.

Modus "Nur verschlüsselte Anmeldeinformationen

Um ein Paxton10 System in seinem sichersten Modus zu betreiben, muss das System so konfiguriert werden, dass es nur vollständig verschlüsselte Anmeldedaten liest. Wenn du den Modus "Nur verschlüsselte Berechtigungsnachweise" aktivierst, werden die folgenden Aktionen ausgeführt:

Alle unverschlüsselten Berechtigungsnachweise werden aus der Systemdatenbank gelöscht.

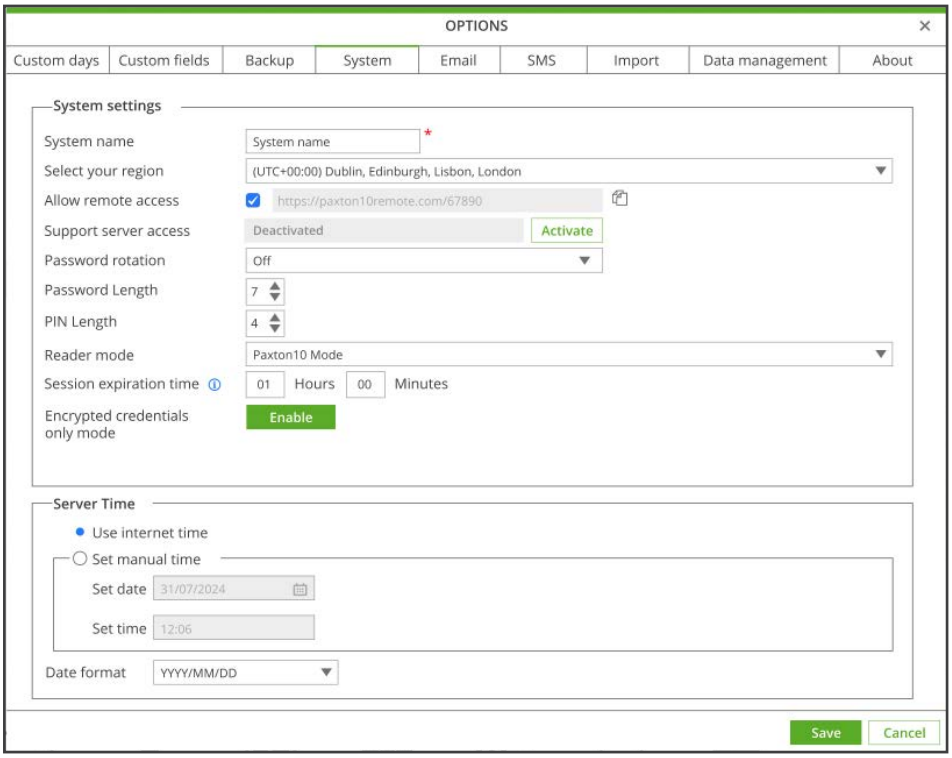
Die Leser im System lesen keine unverschlüsselten Token mehr.

Der Desktop-Leser trägt keine unverschlüsselten Token mehr ein.

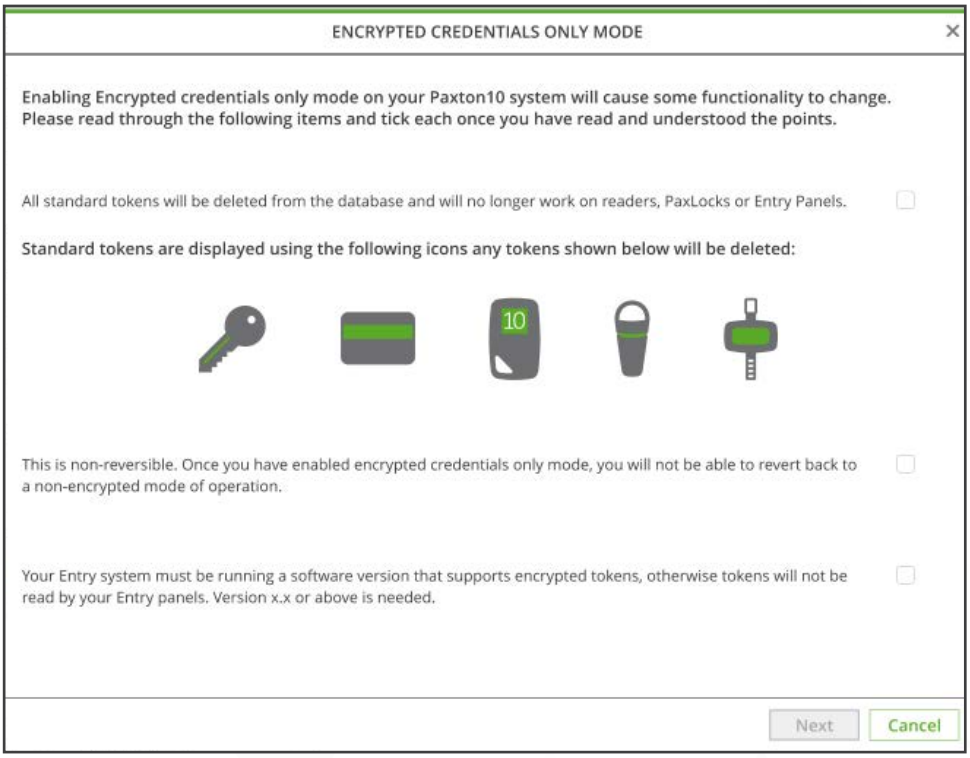
Die Umstellung auf den Modus "Nur verschlüsselte Anmeldedaten" ist eine Einbahnstraße. Sobald dieser Modus aktiviert ist, kann er nicht mehr rückgängig gemacht werden.

Hinweis: Wenn Paxton Entry-Türstationen im System installiert sind, müssen sie auf Version 4.1 aktualisiert werden, bevor der Modus "Nur verschlüsselte Zugangsdaten" aktiviert werden kann.

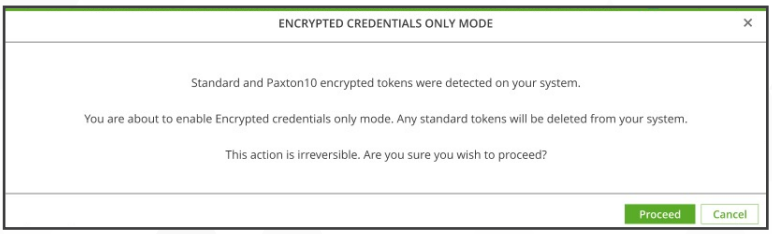
1. Um den Modus zu aktivieren, gehst du zum Modal "Optionen" und wählst die Registerkarte "System". Klicke auf die Schaltfläche "Aktivieren".



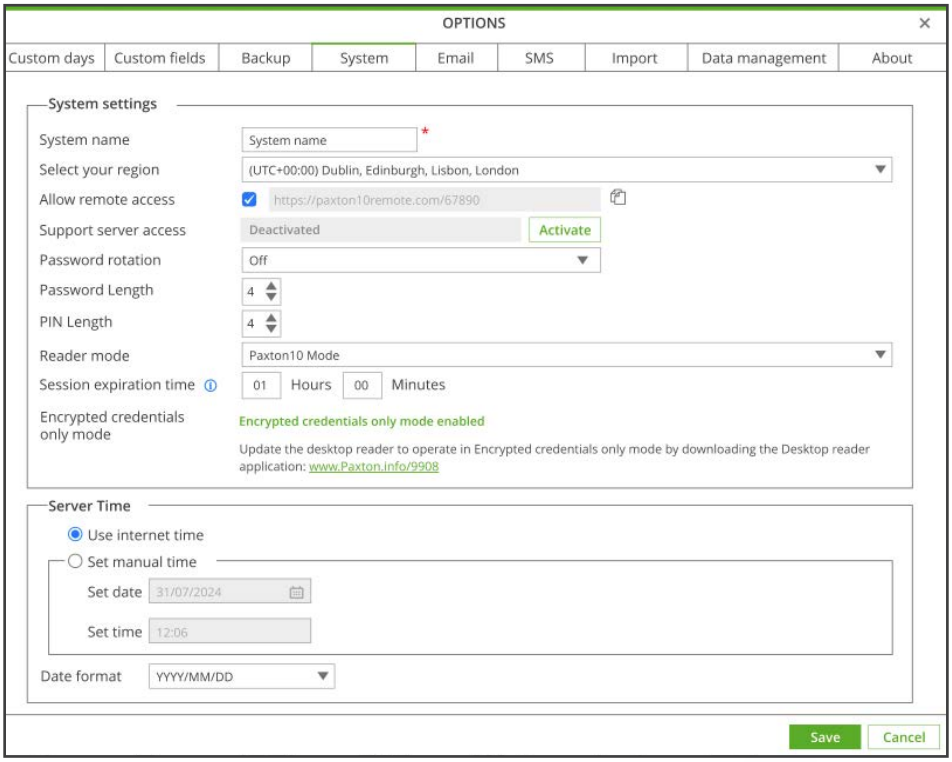
2. Es werden Details zu den Auswirkungen der Aktivierung des Modus "Nur verschlüsselte Anmeldeinformationen" angezeigt und du wirst aufgefordert, zu bestätigen, dass du jeden Schritt verstanden hast.



3. Eine letzte Chance zum Abbrechen, denn dieser Schritt ist nicht umkehrbar!



4. Auf der Registerkarte "System" wird nun angezeigt, dass im System der Modus "Nur verschlüsselte Anmeldeinformationen" aktiviert ist.



Die Standort ist jetzt so konfiguriert, dass sie nur verschlüsselte Anmeldedaten akzeptiert, ansonsten funktioniert das System ganz normal.