

Paxton10 High Secure Kaarten en Tags programmeren

Algemeen

Paxton10 High Secure kaarten en tags zijn speciaal ontworpen voor gebruik met het Paxton10-systeem. Ze maken gebruik van AES-128 encryptie en 3-pass mutual authentication, waarbij kaart en lezer elkaar actief verifiëren. Dit voorkomt dat gegevens kunnen worden gekopieerd of onderschept. Dankzij deze geavanceerde techniek, communiceren de kaarten volledig versleuteld. En werken ze naadloos samen met alle Paxton10-kaart lezers, PaxLock deurbeslagen en Entry intercom panelen. Hierdoor kan de kaart of tag op alle lezers binnen het Paxton10 systeem gebruikt kan worden.

Om dit hoge niveau van beveiliging te kunnen bereiken genereert het Paxton10 systeem automatisch een unieke encryptiesleutel per systeem voor de High Secure kaarten en tags. Deze encryptiesleutel (Security key) wordt beveiligd opgeslagen op de Paxton10 Software controller. Zo hoeft u zelf geen encryptiesleutel op te slaan of te beheren waardoor de configuratie zeer eenvoudig is en er een optimale beveiliging is omdat de encryptiesleutel niet toegankelijk is.

In deze handleiding legt uit hoe u de High Secure credentials kunt gebruiken en programmeren

Een Paxton10 systeem instellen om de High Secure Credentials

Om de High Secure Credentials te kunnen gebruiken dient u in het Paxton10 systeem de volgende stappen uit te voeren. Deze stappen worden verderop in de handleiding uitgelegd.

1. Zorg dat uw systeem draait op Paxton10 software v4.9 SR1 of hoger.
 - Vanaf deze versie worden de encryptiesleutels automatisch in uw systeem gegenereerd.
2. Indien u Entry intercom gebruikt zorg er dan voor dat het Entry systeem geupdate is naar minimaal v4.1 of hoger.
3. Programmeer de desktop lezer via de Paxton10 desktop lezer configuratietool en installeer de unieke encryptiesleutel.
 - Alleen de Paxton10 High Secure desktop lezer (010-392) kan gebruikt worden in combinatie met de Paxton10 High secure kaarten en tags.
4. Indien u nog de Paxton10 desktop lezer(010-387) gebruikt dient u deze te vervangen
5. Sluit de Paxton10 desktop lezer configuratietool af, en open de Paxton10 software.
6. Voeg de High Secure credentials toe aan een gebruiker in de Paxton10 software.

De Paxton10 desktop lezer configuratietool gebruiken

De desktop-lezer configuratietool wordt gebruikt om de encryptiesleutels te programmeren op de desktop lezer. De tool kan via de Paxton10 software of via de Paxton Portal gedownload worden.

- De tool wordt voor de volgende doeleinden gebruikt
- De encryptiesleutel in de desktoplezer programmeren
- De firmware in de desktop lezer bijwerken
- De encryptiesleutel vernieuwen van de geprogrammeerde high secure kaarten en tags
- Een inleercredential voor de Paxlock programmeren

Deze software wordt op een PC geïnstalleerd die zich in hetzelfde netwerk bevindt als de Paxton10 Software controller.

De desktop lezer wordt lokaal via USB aangesloten op dezelfde PC.

Let op: Voor multi-site systemen betekent dit dat de desktop lezers geprogrammeerd moeten worden in het netwerk van de Paxton10 Software controller.

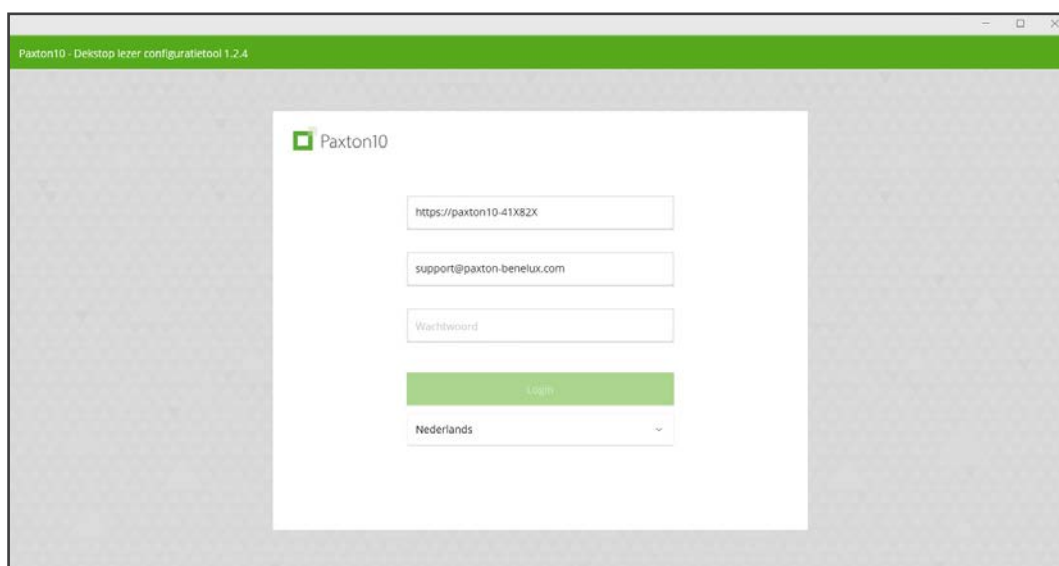
Enmaal geconfigureerd, kunnen Desktop lezers op elke client werkstation worden gebruikt op dezelfde manier als bij vorige versies. De applicatie hoeft dus slechts op één PC te worden geïnstalleerd. En wordt gebruikt om alle desktop lezers voor het systeem te configureren.

Software gebruiker met de bevoegdheid installateur is vereist om de applicatie te gebruiken.

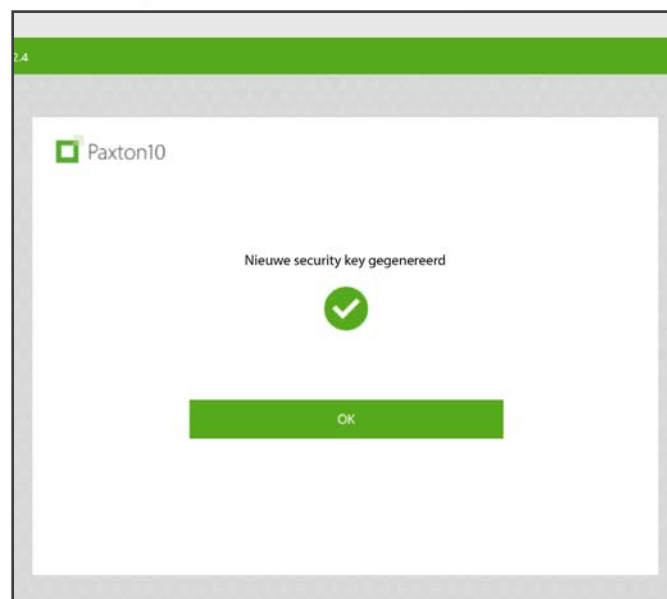
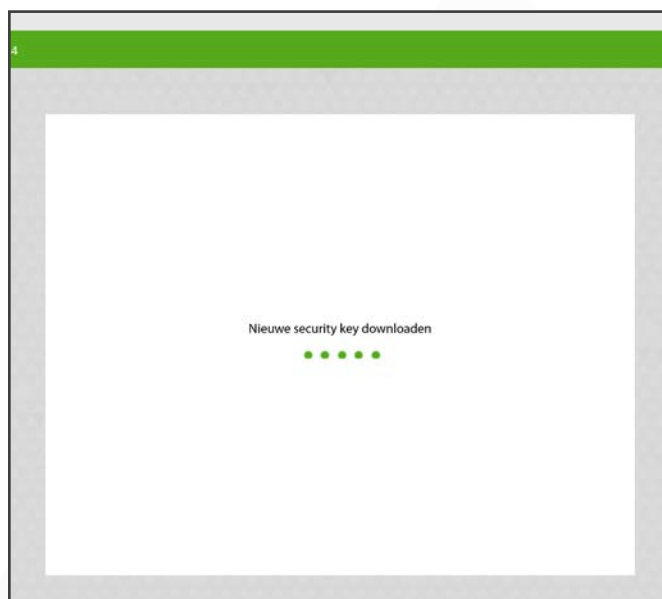
De encryptiesleutel programmeren in een desktop lezer

De Paxton10 desktop lezer configuratietool wordt voornamelijk gebruikt voor het programmeren van de encryptiesleutel in de desktop lezer. Alle Paxton10 desktop lezer die gebruikt gaan worden op locatie dienen via de configuratietool geprogrammeerd te worden.

1. Zorg ervoor dat de desktop lezer is aangesloten voor u de configuratietool opent.
2. Om de desktop lezer configuratietool te kunnen gebruiken zijn inlog gegevens van de Paxton10 software benodigd.
3. Wanneer u ingelogd bent in de desktop lezer configuratietool wordt de encryptiesleutel in de desktop lezer geprogrammeerd.



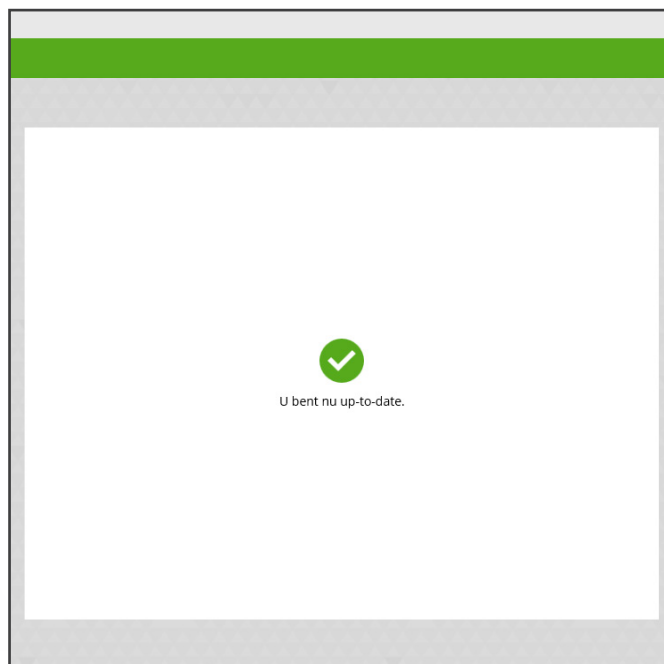
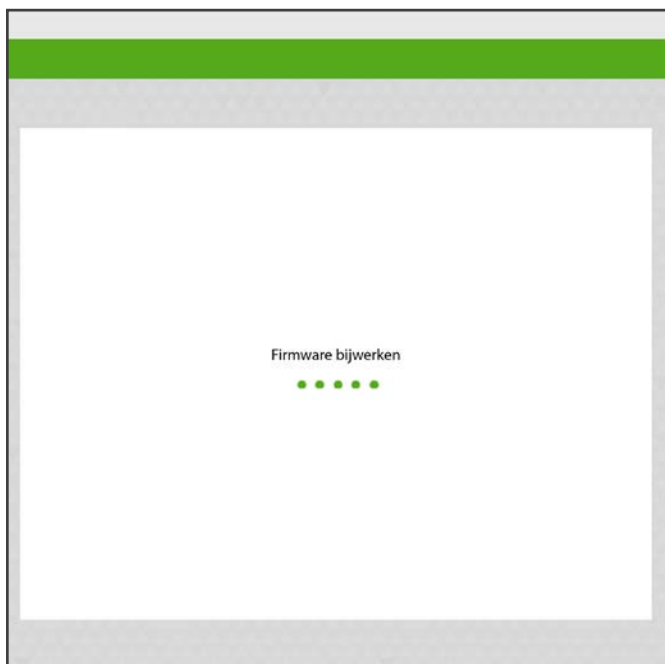
4. Wanneer dit gereed is kunt u de applicatie afsluiten en is de desktop lezer klaar voor gebruik.



Firmware van de desktop lezer bijwerken

De Paxton10 High Secure desktop lezer heeft de mogelijkheid om firmware updates te krijgen via de Paxton10 desktop lezer configuratietool.

1. Zorg ervoor dat de desktop lezer is aangesloten voor u de configuratietool opent.
2. Om de desktop lezer configuratietool te kunnen gebruiken zijn inlog gegevens van de Paxton10 software benodigd.
3. Wanneer u bent ingelogged kijkt de configuratietool naar firmware versie van de aangesloten desktop lezer.
4. Indien nieuwe firmware beschikbaar is zal de firmware van de desktop lezer bijgewerkt worden.



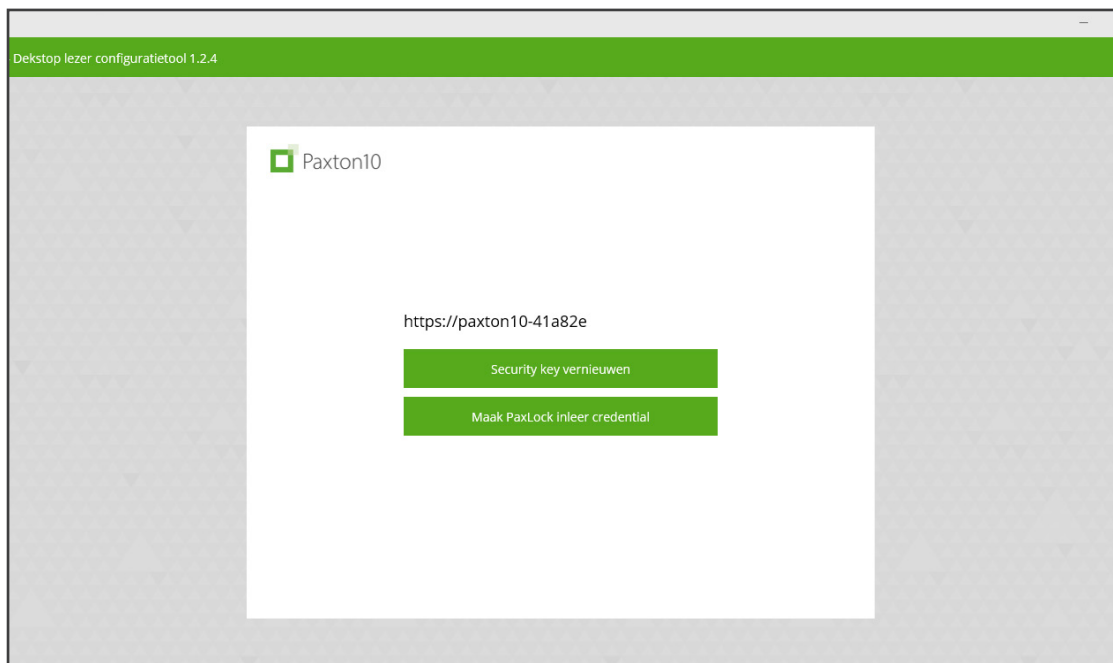
5. Als de firmware is bijgewerkt kan de applicatie afgesloten worden

De Encryptiesleutel vernieuwen

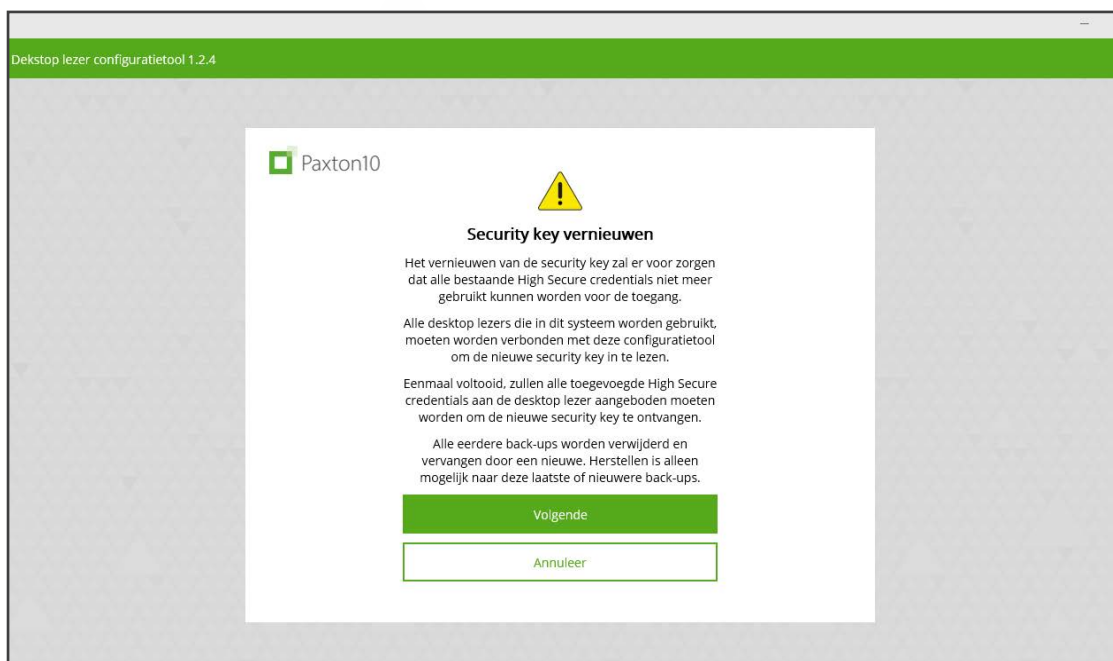
Via de desktop lezer configuratietool is het mogelijk om de encryptiesleutels te vernieuwen. Dit kan gedaan worden in het geval dat de locatie ervoor kiest om periodiek de encryptiesleutel te vernieuwen.

Er zijn een aantal belangrijke punten om rekening mee te houden als u de encryptiesleutel ververst;

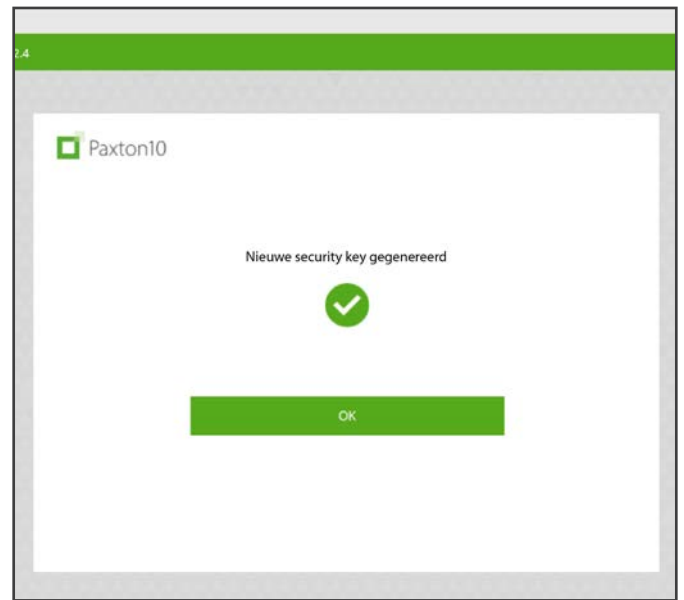
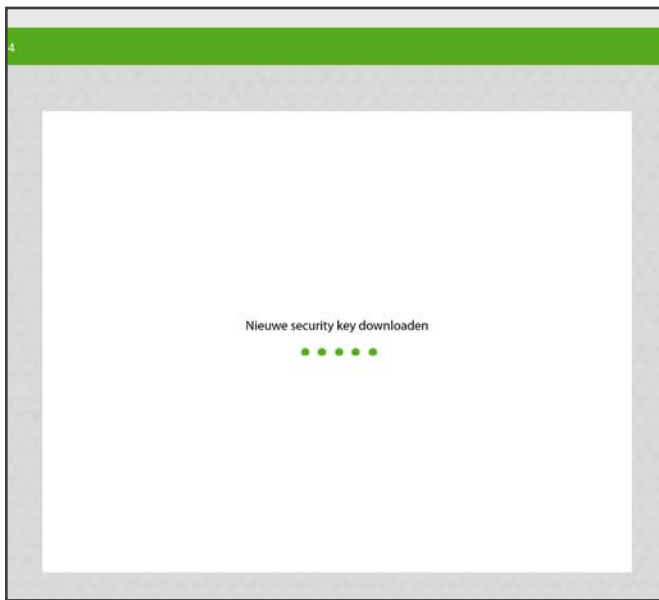
- Elke desktoplezer dient via de desktop lezer configuratie tool bijgewerkt te worden met de nieuwe encryptiesleutel.
 - Alle High Secure credentials dienen via de bijgewerkte desktoplezer opnieuw geprogrammeerd te worden om de nieuwe encryptiesleutel te ontvangen.
 - Alle lezers in het Paxton10 systeem worden automatisch bijgewerkt met de nieuwe encryptiesleutel.
1. Zorg ervoor dat de desktop lezer is aangesloten voor u de configuratietool opent. Om de desktop lezer configuratietool te kunnen gebruiken zijn inlog gegevens van de Paxton10 software benodigd.
 2. Zodra u ingelogged bent klikt u op Security key(encryptiesleutel) vernieuwen.



3. Er wordt een melding getoond met de stappen die u dient uit te voeren zodra de encryptiesleutel vernieuwt is.



4. Klik op volgende, er zal nu een nieuwe encryptiesleutel gegenereerd worden op de Paxton10 software controller en deze zal geprogrammeerd worden in de desktop lezer.



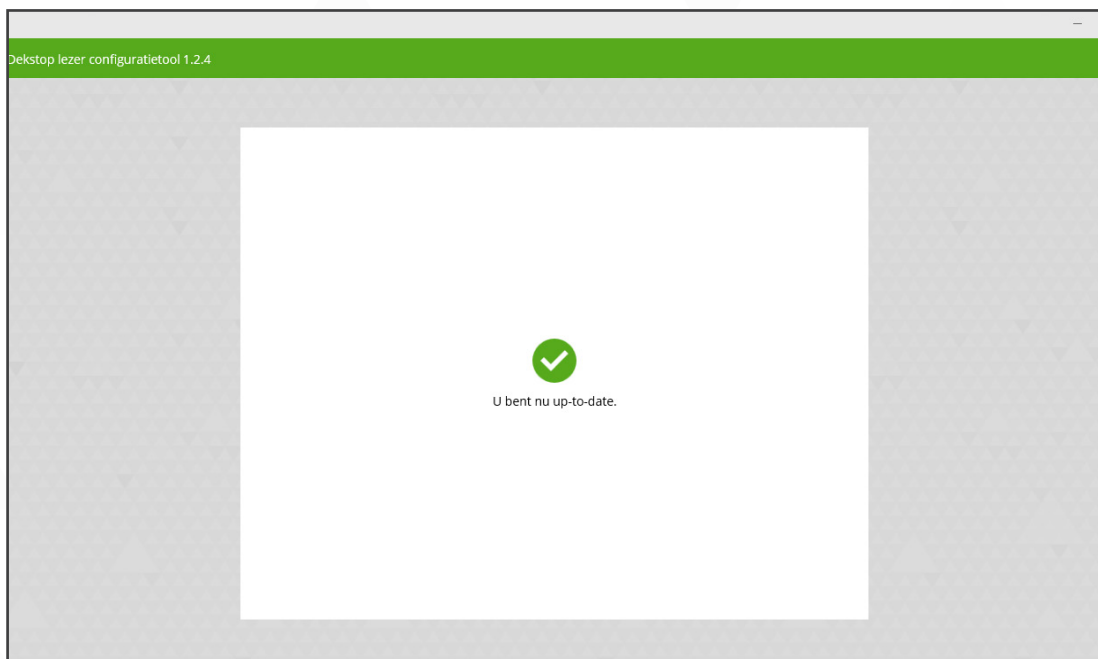
5. De configuratietool kan nu afgesloten worden.

Een PaxLock inleer credential maken

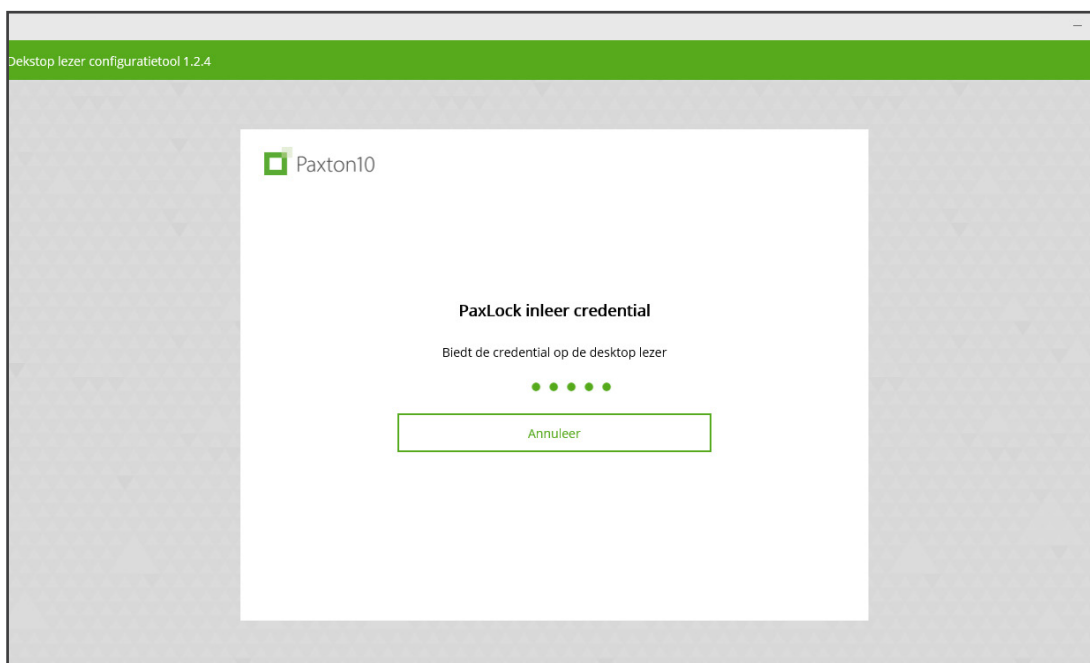
Wanneer Paxton10 is ingesteld in de High Secure mode dienen alle lezers voorzien te zijn van de encryptiesleutel om de High Secure credentials te kunnen lezen. Om een PaxLock toe te voegen aan het systeem biedt u normaliter een geldige tag aan op de PaxLock. Echter wanneer in Paxton10 High Secure mode is ingesteld kan een PaxLock niet gekoppeld worden met een normale kaart of tag omdat de PaxLock nog niet geprogrammeerd is met de encryptiesleutel.

Om dit op te lossen is het via de Paxton10 desktop lezer configuratietool mogelijk om een inleer credential aan te maken om een PaxLock toe te kunnen voegen aan Paxton10.

1. Zorg ervoor dat de desktop lezer is aangesloten voor u de configuratietool opent.
2. Om de desktop lezer configuratietool te kunnen gebruiken zijn inlog gegevens van de Paxton10 software benodigd.
3. Zodra u ingelogged bent klikt u op security key maak PaxLock inleer credential.



4. Biedt een High Secure kaart of tag aan op de Paxton10 desktop lezer



5. De desktoplezer programmeert de High Secure credential zodat deze gebruikt kan worden om een nieuwe PaxLock aan het systeem te koppelen
6. De configuratietool kan nu afgesloten worden.

High Secure mode inschakelen

Voor extra beveiliging kunt u uw Paxton10-systeem instellen op High Secure Mode. In deze modus accepteren alle Paxton10 kaartlezers uitsluitend High Secure kaarten, tags en Paxton10 Smart Credentials. Andere kaarttechnieken worden op de Paxton10 lezers uitgeschakeld. Voor u High Secure mode inschakeld is het belangrijk om met de volgende punten rekening te houden;

1. Bij inschakelen zullen alle niet High Secure kaarten en tags uit het systeem worden verwijderd.
2. Alle Paxton10 kaart lezers, PaxLock deurbeslagen en Entry intercom panelen lezen uitsluitend High Secure kaarten, tags en Paxton10 Smart Credentials.
3. Andere kaarttechnieken worden uitgeschakeld.

Via de desktop lezer is het niet langer mogelijk om niet High secure kaarten en tags in te leren.

Let op: Voordat u High Secure mode inschakeld dient u ervoor te zorgen dat uw Entry intercomsysteem geupdate is naar minimaal v4.1 of hoger.

Let op: High Secure mode is niet uit te schakelen wanneer dit eenmaal is ingeschakeld op het systeem

1. Om high secure mode in te schakelen gaat u naar het menu 'systeeminstellingen' en klik op de knop inschakelen naast High Secure mode

SYSTEEMINSTELLINGEN

Specifieke dagen | Gebruikersvelden | Back-up | **Systeem** | E-mail | Gegevensbeheer | Over

Systeeminstellingen

Systeemnaam:

Uw tijdzone selecteren: (UTC+00:00) Dublin, Edinburgh, Lisbon, London

Remote toegang: ☐

Server toegang support:

Verplicht wijzigen van het wachtwoord:

Lengte wachtwoord:

Lengte PIN:

Type kaart leesmodus:

Automatisch uitloggen na een inactiviteit van: (hh:mm)

High Secure mode:
 Installeer de [Desktop lezer configuratietool](#) om de High Secure Paxton10 Desktop lezer te programmeren met de unieke security key

Software controller opnieuw opstarten:

Tijd en datum

☒ Internettijd gebruiken

☐ Handmatige tijd instellen

Selecteer datum:

Selecteer tijd:

2. In de pop-up worden alle punten getoond waar u rekening mee dient te houden, lees deze goed door en bevestig deze door de punten aan te vinken.

HIGH SECURE MODE

Het is niet langer mogelijk om standaard credentials te gebruiken als High Secure mode is ingeschakeld.

Lees de volgende punten zorgvuldig door en vink elk vakje aan om te bevestigen dat u dit gelezen heeft:

Alle standaard credentials, weergegeven door de volgende iconen, zullen worden verwijderd uit de database. Het is niet langer mogelijk deze credentials te gebruiken op Paxton10 Lezers, PaxLocks of Entry Buitenposten. ☐

High Secure mode wordt permanent ingeschakeld! Wanneer High Secure mode is ingeschakeld kan deze niet meer uitgeschakeld worden. ☐

Als Paxton Entry gebruikt wordt in dit systeem, dient u Entry te updaten naar minimaal v4.1 om de High Secure credentials te kunnen gebruiken. ☐

Alle huidige back-ups worden verwijderd wanneer High Secure mode wordt ingeschakeld! Na het inschakelen wordt er een nieuwe back-up gemaakt van het systeem.

U kunt nu High Secure mode inschakelen.

WAARSCHUWING

Er zijn standaard credentials toegevoegd aan dit Paxton10 systeem. Deze standaard credentials zullen verwijderd worden uit het systeem voor High Secure mode ingeschakeld kan worden.

Wilt u doorgaan?

Let op dit is permanent en is niet uit te schakelen

SYSTEEMINSTELLINGEN

Specifieke dagen

Gebruikersvelden

Back-up

Systeem

E-mail

Gegevensbeheer

Over

Systeeminstellingen

Systeemnaam

System

Uw tijdzone selecteren

(UTC+00:00) Dublin, Edinburgh, Lisbon, London

Remote toegang

☐

Server toegang support

Uitgeschakeld

Activeren

Verplicht wijzigen van het wachtwoord

Uit

Lengte wachtwoord

7

Lengte PIN

4

Type kaart leesmodus

Paxton10

Automatisch uitloggen na een inactiviteit van

02:00 (hh:mm)

High Secure mode

Modus alleen versleutelde referenties ingeschakeld

Installeer de [Desktop lezer configuratietool](#) om de High Secure Paxton10 Desktop lezer te programmeren met de unieke security key

Software controller opnieuw opstarten

Nu herstarten

Tijd en datum

☒ Internettijd gebruiken

☐ Handmatige tijd instellen

Selecteer datum

16/02/2026

Selecteer tijd

08:50

Selecteer tijd

Opslaan

Annuleren