Krypterade autentiseringsuppgifter

Översikt

Paxton10 Encrypted credentials är ISO-kort och nyckelbrickor som är säkrade med 128 bitars AES-kryptering. Detta skyddar dem mot kopiering/kloning samt mot upprepningsattacker på Paxton10 läsare. Med läget "Endast krypterade referenser" kan system endast registrera krypterade referenser, vilket säkerställer att inga andra referenser införs av misstag eller av misstag.

Varje Paxton10-system använder sin egen unika krypteringsnyckel. Detta innebär att inloggningsuppgifter som registreras i ett system inte kan registreras i något annat system eftersom krypteringsnycklarna inte matchar varandra. Om det skulle behövas kan kunderna ändra sin krypteringsnyckel för webbplatsen och uppdatera sina inloggningsuppgifter.

Den här applikationsnoten beskriver hur man aktiverar användningen av krypterade Paxton10-autentiseringsuppgifter, ändrar platsens krypteringsnycklar och ansluter Paxton10-enheter till en Paxton10-plats när man endast använder krypterade autentiseringsuppgifter.

Konfigurera ett Paxton10-system för att använda krypterade autentiseringsuppgifter

För att använda Paxton10 Encrypted credentials på ett system måste följande steg först utföras. Instruktioner för hur du utför dessa steg finns längre fram i dokumentet.

1. Se till att systemet kör Paxton10 v.4.7 SR9 eller senare.
   - Från och med denna version genereras krypteringsnycklar automatiskt på Paxton10-servern.

2. Se till att alla Paxton Entry-paneler som är installerade på systemet är uppgraderade till version xx.xx eller senare.
   - Krypterade autentiseringsuppgifter stöds från och med denna version.

3. Ställ in platsens krypteringsnyckel i Skrivbordsläsaren/läsarna med hjälp av programmet för konfiguration av Skrivbordsläsare.
   - Endast Universal Skrivbordsläsare (010-392) kan användas, äldre Skrivbordsläsare (010-387) måste bytas ut eftersom de inte stöder krypterade inloggningsuppgifter

4. Registrera de krypterade inloggningsuppgifterna på vanligt sätt.

5. Ställ in Paxton10-systemet i läget "Endast krypterade referenser" (valfritt).

Använda programmet för konfiguration av Skrivbordsläsare

Konfigurationsapplikationen för Skrivbordsläsare används för att hantera de säkerhetsnycklar som används vid kryptering av referenser. Den kan hämtas från /PaxtonPortal/SoftwareDownload/#!/ och krävs för att registrera Paxton10 Encrypted tokens. Programmet används för att utföra följande uppgifter,

- Ange platsens krypteringsnyckel i Skrivbordsläsaren
- Uppdatera den fasta programvaran i Skrivbordsläsaren
- Ändra platsens krypteringsnyckel
- Skapa en Paxlock-bindningstoken

För att programmet för konfiguration av Skrivbordsläsare ska kunna utföra dessa uppgifter måste det installeras på en dator som finns i samma nätverk som Paxton10-servern. Skrivbordsläsaren måste anslutas lokalt via USB till samma dator.

Obs: För installationer på flera platser innebär detta att skrivbordsläsare måste konfigureras i det lokala nätverk där servern finns.

När Skrivbordsläsarna har konfigurerats kan de användas på alla klientarbetsstationer på samma sätt som med tidigare versioner. Programmet behöver alltså bara installeras på en dator och användas för att konfigurera alla Skrivbordsläsare för systemet.

En inloggning för systemingenjörer krävs för att använda applikationen.

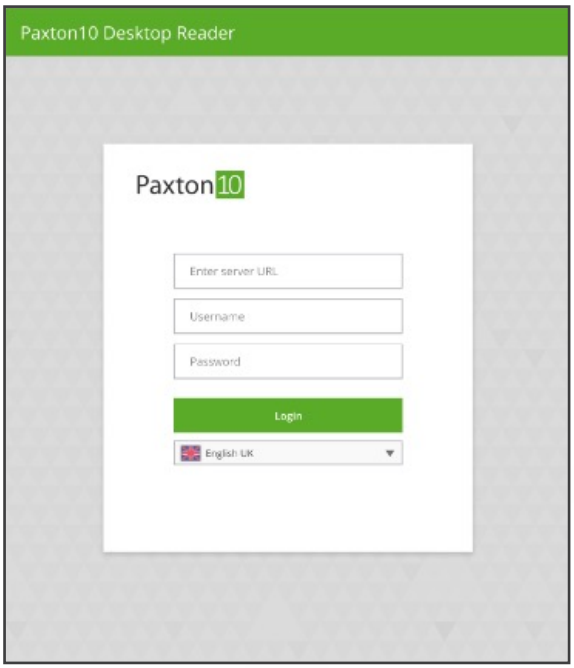
Ställa in krypteringsnyckeln för webbplatsen i en Skrivbordsläsare

Detta är det vanligaste användningsområdet för konfigurationsapplikationen. Alla Skrivbordsläsare som ska registrera krypterade autentiseringsuppgifter måste gå igenom denna enkla process.

1. Se till att skrivbordsläsaren är ansluten innan du startar applikationen.

2. När applikationen körs begärs inloggningsuppgifter för Paxton10.

3. När du har loggat in söker programmet automatiskt efter den anslutna Skrivbordsläsaren och överför webbplatsens krypteringsnycklar till enheten.



4. Applikationen kan nu stängas och skrivbordsläsaren är redo att användas för att registrera krypterade referenser.

Uppdatering av firmware för en Skrivbordsläsare

Den universella skrivbordsläsaren Paxton10 kan ta emot uppgraderingar av den fasta programvaran med hjälp av konfigurationsapplikationen för skrivbordsläsaren.

1. Se till att skrivbordsläsaren är ansluten.

2. När applikationen körs begärs inloggningsuppgifter för Paxton10.

3. När du har loggat in söker programmet automatiskt efter den anslutna skrivbordsläsaren och kontrollerar dess aktuella version av den fasta programvaran.

4. Om programmet har en nyare version av den fasta programvaran än den som är installerad kommer en automatisk

uppdatering att ske.

5. När uppdateringen är klar kan applikationen stängas.

Ändra krypteringsnyckeln för webbplatsen

Med hjälp av konfigurationsapplikationen är det möjligt att ändra den krypteringsnyckel som används på en anläggning. Detta kan göras i händelse av att nycklarna upptäcks eller om en anläggning regelbundet väljer att ändra sin nyckel.

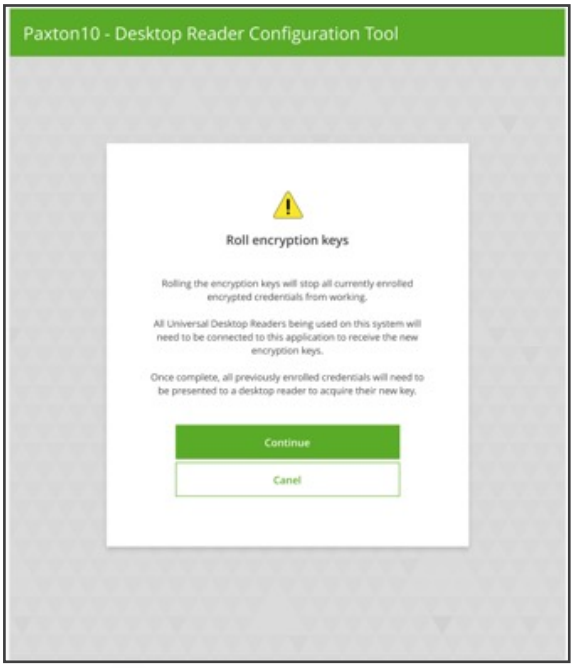
Det är viktigt att notera att när ett systems nyckel har ändrats måste

- varje skrivbordsläsare få sin krypteringsnyckel uppdaterad
- Alla krypterade referenser måste returneras till en uppdaterad skrivbordsläsare för att få sin krypteringsnyckel ändrad så att de fortsätter att fungera i systemet.
- Läsare i systemet kommer att få sin nyckel uppdaterad automatiskt

1. När programmet körs begärs inloggningsuppgifter för Paxton10.

2. Välj alternativet "Rulla nycklar".

3. Ett varningsmeddelande visas som beskriver vilka åtgärder som måste vidtas när nycklarna har ändrats.



4. Klicka på "Fortsätt". En ny nyckel genereras på Paxton10-servern och skickas till skrivbordsläsaren (om en sådan är ansluten)

5. Applikationen kan stängas.

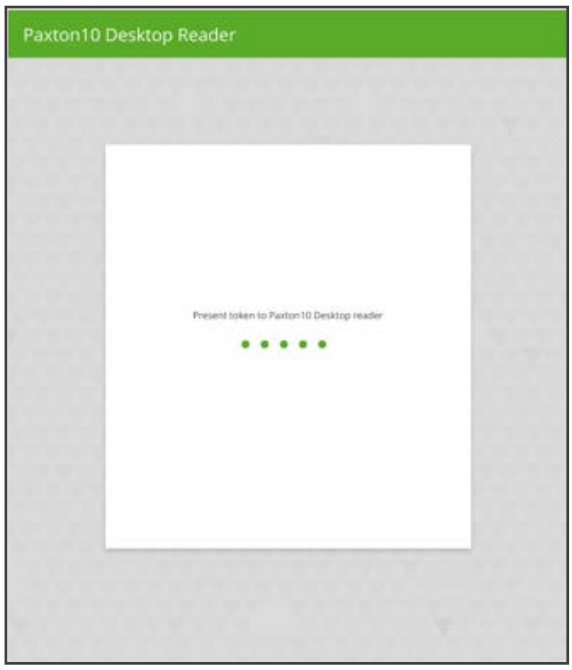
Skapa en Paxlock Binding-token

När man arbetar i läget "Endast krypterade referenser" måste alla läsare ha krypteringsnycklarna för att kunna läsa referenserna. Om ett nytt Paxlock behöver läggas till i ett system är den normala metoden att presentera en giltig token från systemet för Paxlock. Men i läget för endast krypterade autentiseringsuppgifter kan Paxlock inte läsa några autentiseringsuppgifter förrän det har bundits till systemet och fått webbplatsens krypteringsnycklar skickade till sig.

För att komma runt detta kan konfigurationsapplikationen för Skrivbordsläsare göra det möjligt att skapa en Paxlock-bindningstoken med hjälp av en av de krypterade autentiseringsuppgifterna. Detta gör det möjligt att binda nya Paxlock utan att äventyra systemets "endast krypterade"-integritet.

1. Se till att en Skrivbordsläsare är ansluten till den dator som kör programmet.
2. När programmet körs begärs inloggningsuppgifter för Paxton10.
3. Välj alternativet "Create Paxlock binding token".

4. Visa upp en krypterad autentiseringsuppgift för skrivbordsläsaren.



5. Skrivbordsläsaren omvandlar token till en Paxlock-bindningstoken som nu kan användas för att ansluta nya Paxlock till systemet.

6. Applikationen kan stängas.

Endast läge för krypterade autentiseringsuppgifter

Om du vill använda ett Paxton10-system i dess säkraste läge måste systemet konfigureras så att det endast läser helt krypterade referenser. Om du aktiverar "Endast läge för krypterade referenser" utförs följande åtgärder:

1. Alla referenser som inte är krypterade raderas från systemets databas.

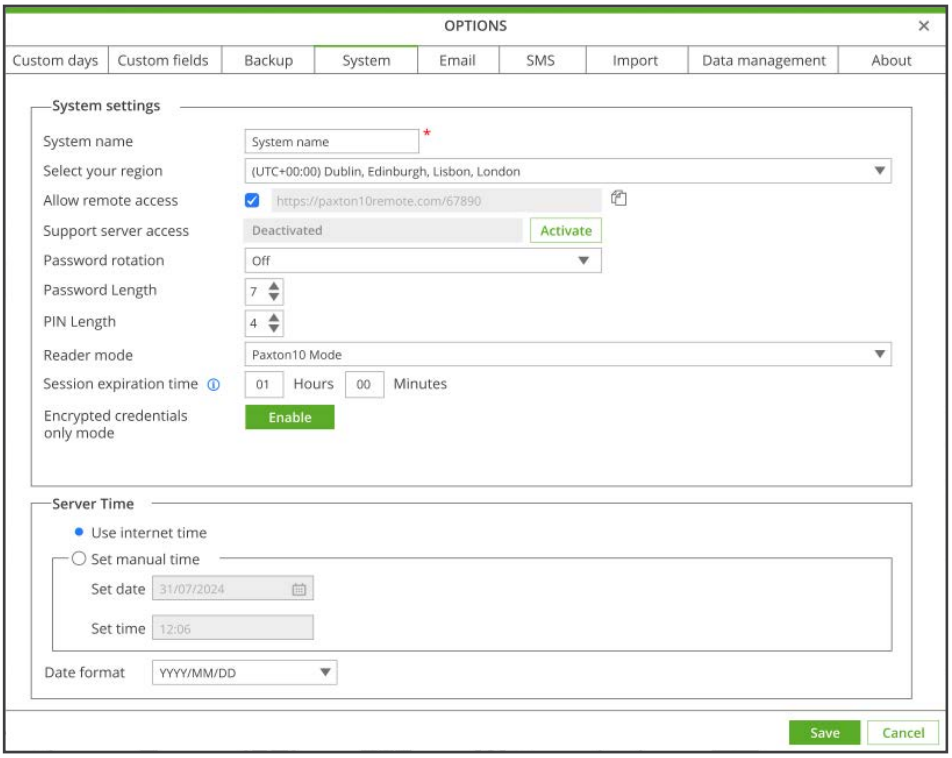
2. Läsare på systemet kommer inte längre att läsa tokens som inte är krypterade.

3. Skrivbordsläsaren kommer inte längre att registrera tokens som inte är krypterade.

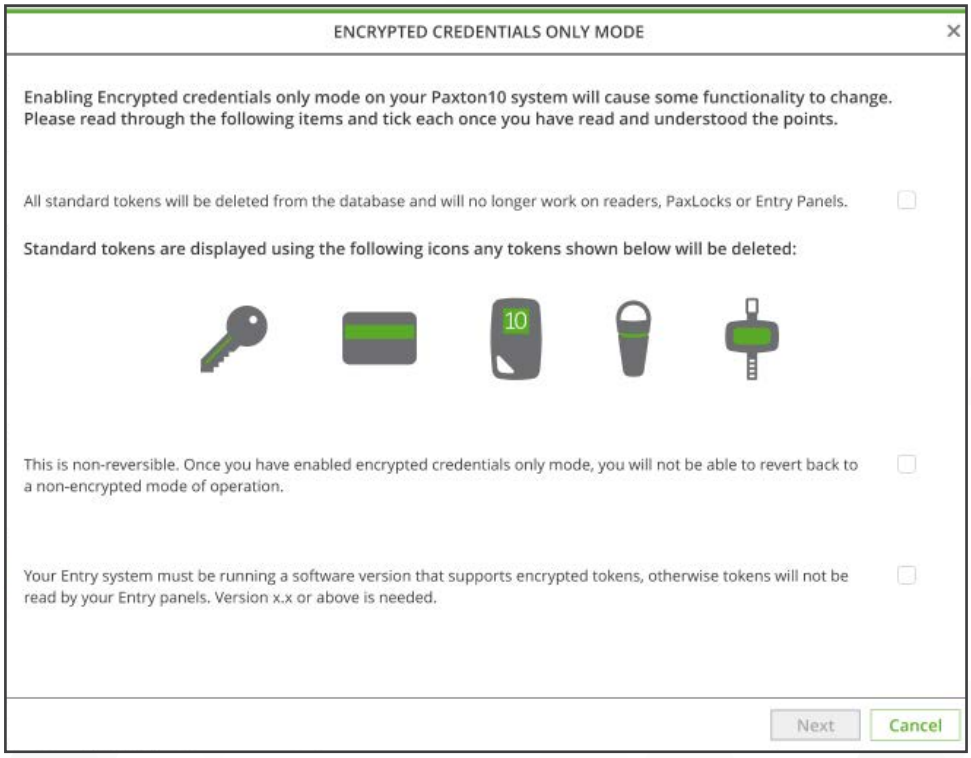
Växlingen till läget "Endast krypterade referenser" är en enkelriktad väg. När detta läge har aktiverats kan det inte återställas.
4.

Obs: Om några Paxton Entry-paneler är installerade i systemet måste de uppgraderas till v.4.1 innan du aktiverar läget "Endast krypterade referenser".

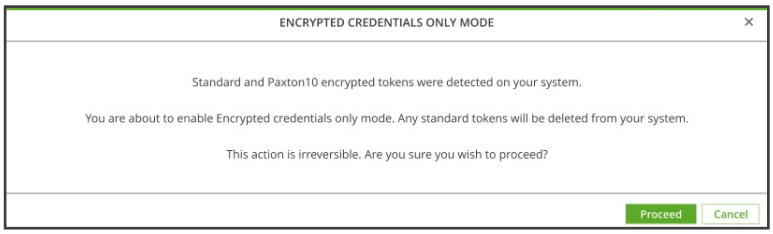
1. För att aktivera läget går du till modalen "Alternativ" och väljer fliken "System". Klicka på knappen "Enable".



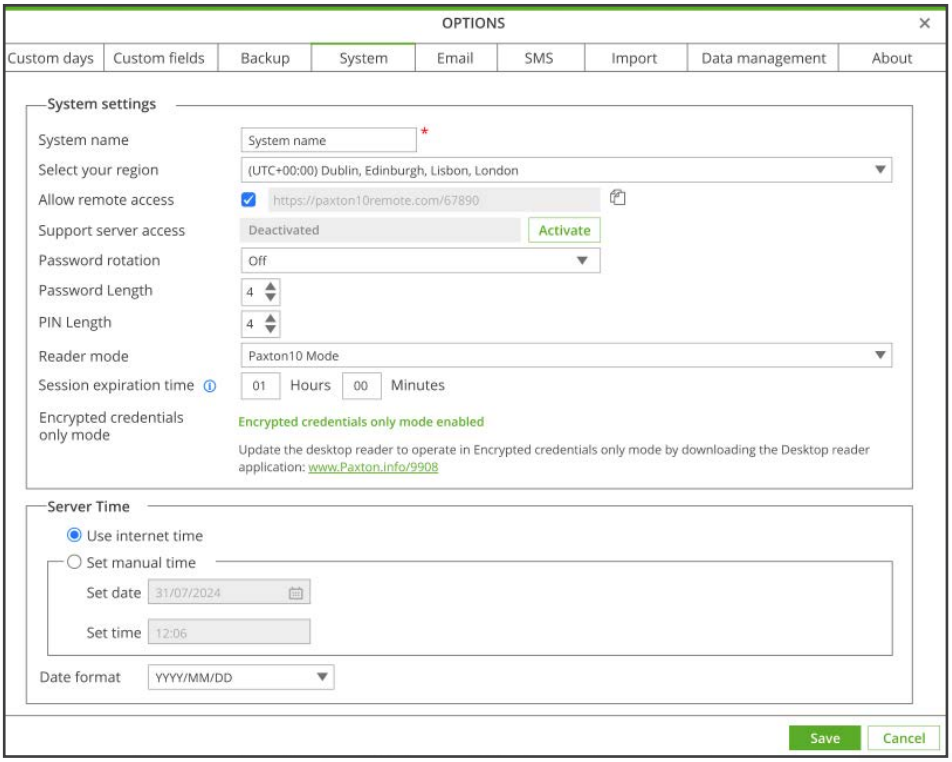
2. Detaljer om konsekvenserna av att aktivera läget Secure credentials only visas och du ombeds bekräfta att du har förstått varje steg



3. .En sista chans att avbryta eftersom det här steget inte är reversibelt!



4. På fliken "System" visas nu att systemet har läget Encrypted credentials only aktiverat.



5. Webbplatsen är nu konfigurerad för att endast acceptera krypterade inloggningsuppgifter, i övrigt fungerar systemet som vanligt.