Encrypted Credentials

Overview

The Paxton10 Encrypted credentials are ISO cards and keyfobs secured using128bit AES encryption. This protects them from copying/cloning as well as replay attacks on Paxton10 readers. With 'Encrypted credentials only' mode, systems can only enrol encrypted credentials, ensuring no other credentials are introduced maliciously or by accident.

Every Paxton10 system uses its own unique encryption key. This means that credentials enrolled onto a system cannot be enrolled onto any other system as the site encryption keys will not match. Should the need arise, customers are able to change their site encryption key and update their credentials.

This application note outlines how to enable the use of Paxton10 encrypted credentials, change the site encryption keys and connect Paxlock devices to a Paxton10 site when only using encrypted credentials.

Setting up a Paxton10 system to use Encrypted credentials

To use Paxton10 Encrypted credentials on a system the following steps must be performed first. Instructions for how to perform these steps are detailed later in the document.

1. Ensure the system is running Paxton10 v.4.7 SR9 or later.
   - From this version site encryption keys are automatically generated on the Paxton10 server

2. Ensure any Paxton Entry Panels that are installed on the system are upgraded to version xx.xx software or later.
   - Encrypted credentials are supported from this version.

3. Set the site encryption key in the Desktop reader(s) using the desktop reader configuration application.
   - Only Universal desktop readers (010-392), can be used, older desktop readers (010-387) must be replaced as they do not support encrypted credentials

4. Enrol the encrypted credentials in the normal way.

5. Set the Paxton10 system to 'Encrypted credentials only' mode (optional).

Using the Desktop reader Configuration Application

The Desktop reader configuration application is used to manage the security keys used in the encryption of the credentials. It can be downloaded from /PaxtonPortal/SoftwareDownload/#!/ and is required in order to enrol Paxton10 Encrypted tokens. The application is used to perform the following tasks,

- Set the site encryption key in the Desktop reader
- Update the firmware in the Desktop reader
- Change the site encryption key
- Create a Paxlock binding token

For the Desktop reader configuration application to perform these tasks it must be installed onto a PC that is on the same network as the Paxton10 server. The desktop reader needs to be connected locally via USB to the same PC.

Note: For multi-site installations this will mean configuring desktop readers on the local network where the server is located.

Once configured, Desktop readers can be used on any client workstation in the same way as with previous versions. So the application needs to only be installed on one PC and used to configure all of the Desktop readers for the system.

A system engineer login is required to use the application.

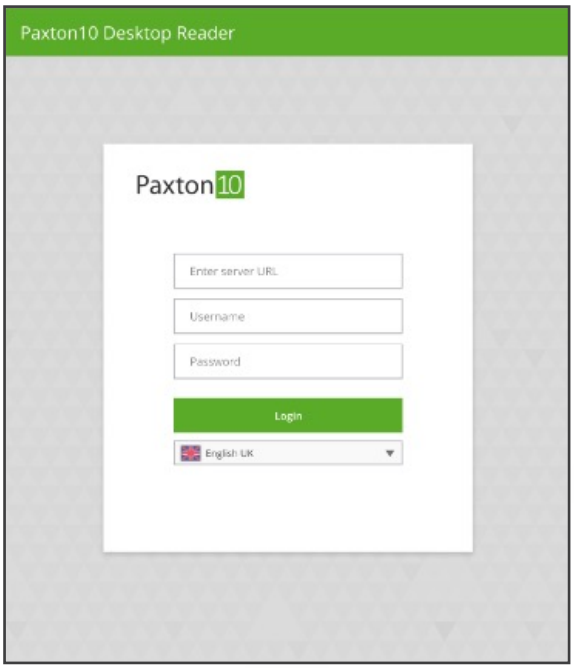
Setting the site encryption key in a Desktop reader

This is the most common use for the configuration application. All desktop readers that are required to enrol encrypted credentials must go through this simple process.

1. Ensure the desktop reader is connected before starting the application.

2. On running the application Paxton10 login details are requested.

3. Once logged in the application automatically looks for the attached desktop reader and transfers the site encryption keys to the device.



4. The application can now be closed and the desktop reader is ready to be used for enrolling encrypted credentials.

Updating a Desktop reader's firmware

The Paxton10 universal desktop reader has the ability to receive firmware upgrades using the desktop reader configuration application.

1. Ensure the desktop reader is connected.

2. On running the application Paxton10 login details are requested.

3. Once logged in the application automatically looks for the attached desktop reader and checks its current firmware version.

4. If the application has a version of firmware more recent than the one installed, an automatic update will take place.

5. Once updated, the application can be closed.

Changing the Site encryption key

Using the configuration application, it is possible to change the encryption key being used on a site. This may be performed in the event that the keys are discovered or if a site periodically chooses to change their key.

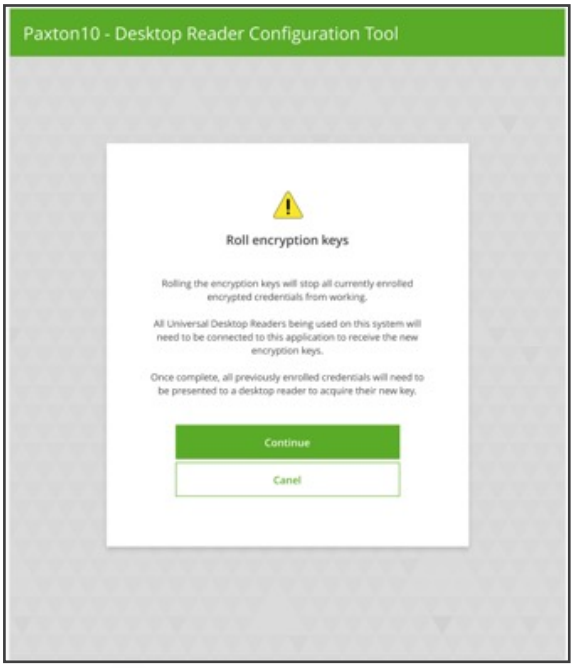
It is important to note that once a system's key has been changed,

- Each desktop reader needs to have its encryption key updated
- All encrypted credentials need to be returned to an updated desktop reader to have their encryption key changed so that they continue to function on the system.
- Readers on the system will have their key updated automatically

1. On running the application Paxton10 login details are requested.

2. Select the 'Roll keys' option.

3. A warning message is displayed describing what steps need to be taken once the keys have been changed.



4. Click 'Continue'. A new key is generated on the Paxton10 server and sent to the desktop reader (if one is connected)

5. The application can be closed.

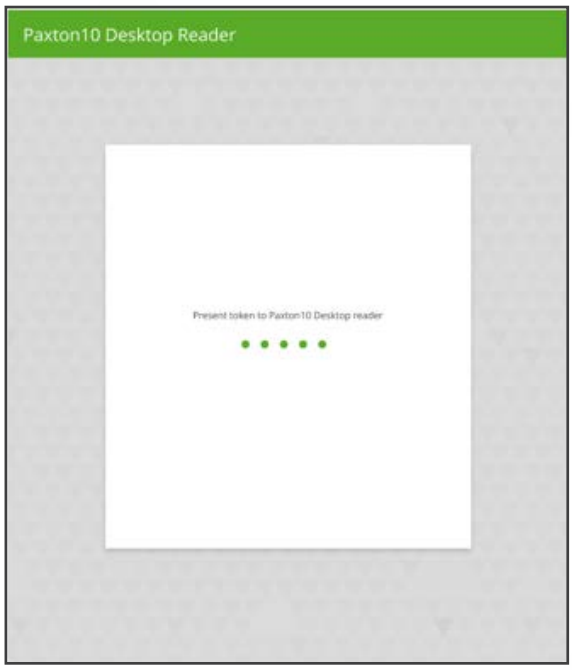
Creating a Paxlock Binding token

When operating in 'Encrypted credentials only' mode all of the readers need to hold the encryption keys in order to read the credentials. If a new Paxlock needs to be added to a system the normal method is to present a valid token from the system to the Paxlock. However, in encrypted credential only mode the Paxlock is unable to read any of the credentials until it has been bound to the system and sent the site encryption keys.

To get around this, the Desktop reader configuration application allows a Paxlock binding token to be created using one of the encrypted credentials. This allows new Paxlocks to be bound without compromising the 'encrypted only' integrity of the system.

1. Make sure a desktop reader is connected to the PC running the application.
2. On running the application Paxton10 login details are requested.
3. Select the 'Create Paxlock binding token' option.

4. Present an encrypted credential to the desktop reader.



5. The desktop reader converts the token into a Paxlock binding token which can now be used to connect new Paxlocks to the system.

6. The application can be closed.

Encrypted Credentials Only Mode

To operate a Paxton10 system in its most secure mode, the system needs to be configured to only read credentials that are fully encrypted. Enabling 'Encrypted credentials only mode' causes the following actions to be performed,

1. All credentials that are not encrypted are deleted from the system database.

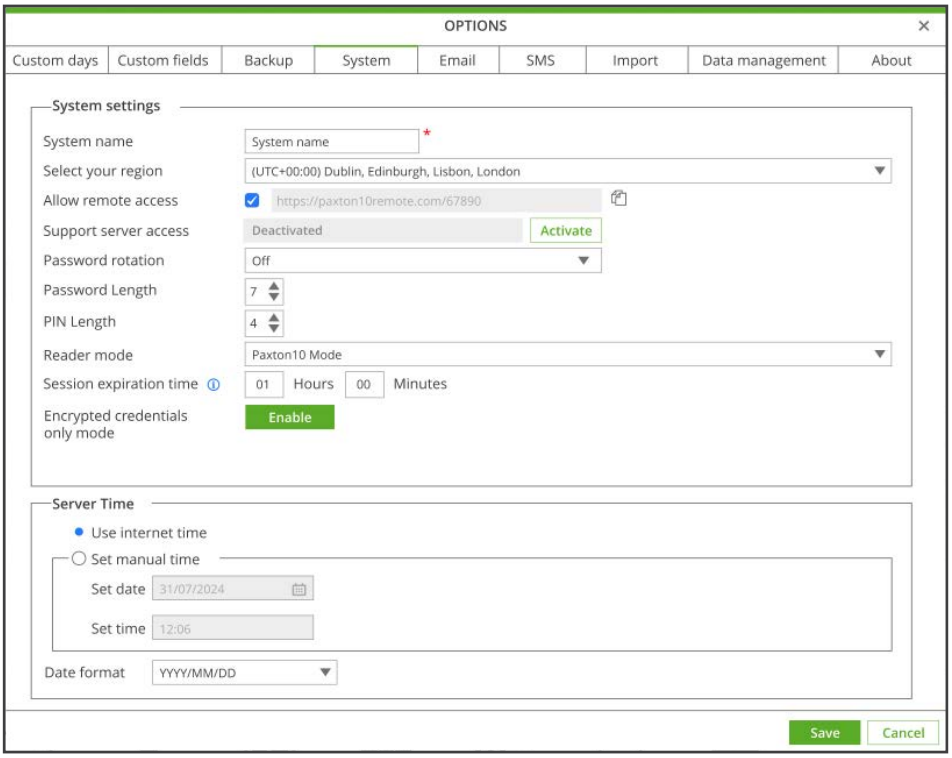
2. Readers on the system will no longer read tokens that are not encrypted.

3. The desktop reader will no longer enrol tokens that are not encrypted.

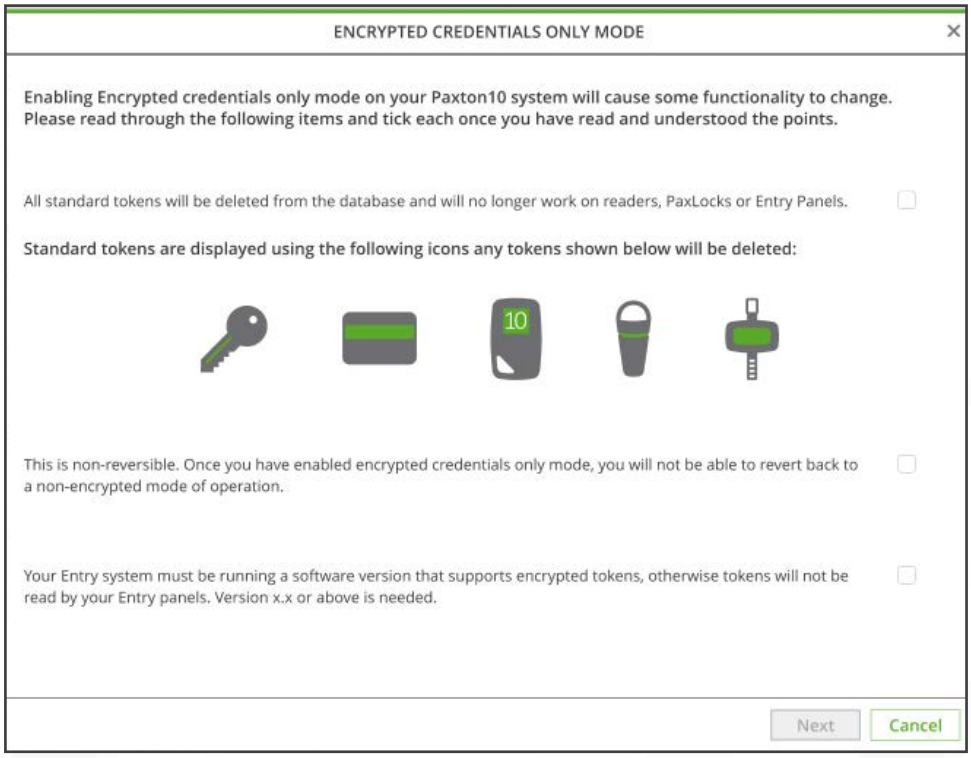
The switch to 'Encrypted credentials only' mode is a one way path. Once this mode is enabled it cannot be reversed.

Note: If any Paxton Entry panels are installed on the system they must be upgraded to v.4.1 before enabling Encrypted credential only mode.

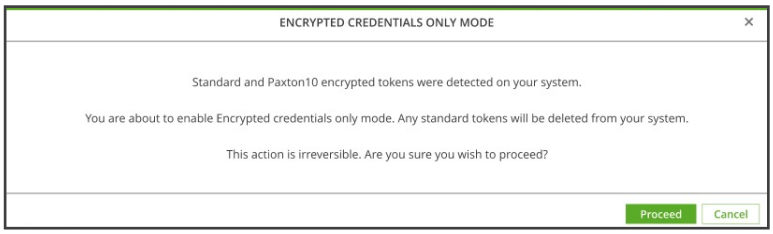
1. To enable the mode go to the 'Options' modal and select the 'System' tab. Click the 'Enable' button.



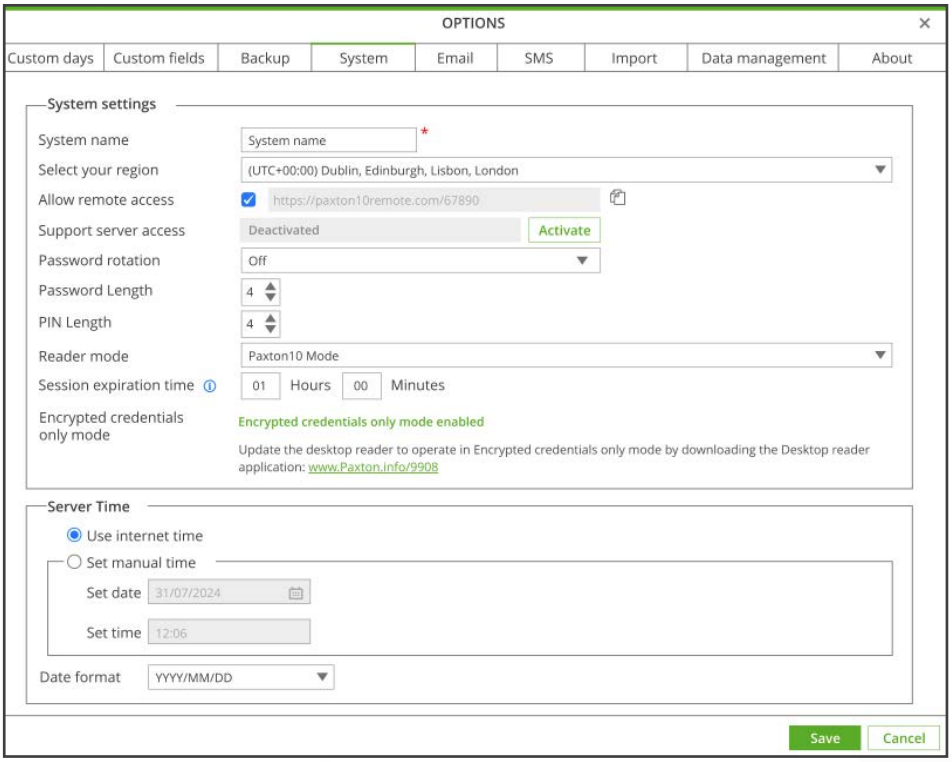
2. Details of the implications of enabling Secure credentials only mode will be displayed and you are asked to confirm that each step is understood.



3. One last chance to cancel as this step is not reversible!



4. The 'System' tab now shows that the system has Encrypted credentials only mode enabled.



The site is now configured to only accept encrypted credentials, in all other respects the system will function as normal.