Références cryptées

Aperçu

Les identifiants chiffrés Paxton10 sont des cartes ISO et des porte-clés sécurisés à l'aide d'un chiffrement AES 128 bits. Cela les protège de la copie/du clonage ainsi que des attaques par rejeu sur les lecteurs Paxton10. Avec le mode "Références cryptées uniquement", les systèmes ne peuvent enregistrer que des références cryptées, ce qui garantit qu'aucune autre référence n'est introduite de manière malveillante ou accidentelle.

Chaque système Paxton10 utilise sa propre clé de cryptage. Cela signifie que les informations d'identification enregistrées sur un système ne peuvent pas être enregistrées sur un autre système, car les clés de cryptage des sites ne correspondent pas. En cas de besoin, les clients peuvent changer la clé de cryptage de leur site et mettre à jour leurs informations d'identification.

Cette note d'application explique comment activer l'utilisation des identifiants cryptés Paxton10, modifier les clés de cryptage du site et connecter les dispositifs Paxlock à un site Paxton10 lorsqu'on utilise uniquement des identifiants cryptés.

Configuration d'un système Paxton10 pour l'utilisation d'identifiants chiffrés.

Pour utiliser les identifiants chiffrés Paxton10 sur un système, les étapes suivantes doivent d'abord être effectuées. Les instructions pour réaliser ces étapes sont détaillées plus loin dans le document.

1. S'assurer que le système fonctionne avec Paxton10 v.4.7 SR9 ou une version ultérieure.
- À partir de cette version, les clés de cryptage du site sont automatiquement générées sur le serveur Paxton10

2. S'assurer que les Platine d'entrée Paxton qui sont installées sur le système sont mises à niveau vers la v.4.1 du logiciel ou une version ultérieure.
- Les informations d'identification cryptées sont prises en charge à partir de cette version.

3. Définir la clé de cryptage du site dans le(s) Lecteur(s) de bureau à l'aide de l'application de configuration du lecteur de bureau.
- Seuls les Lecteurs de bureau universels (010-392), peuvent être utilisés, les anciens lecteurs de bureau (010-387) doivent être remplacés car ils ne prennent pas en charge les identifiants cryptés

4. Enrôler les identifiants cryptés de manière normale.

5. Régler le système Paxton10 sur le mode '**Titres cryptés uniquement**' (facultatif).

Utilisation de l'application de configuration du Lecteur de bureau.

L'application de configuration du Lecteur de bureau permet de gérer les clés de sécurité utilisées pour le chiffrement des justificatifs. Elle peut être téléchargée à partir de www.Paxton.Info/9984 et est nécessaire pour enrôler les jetons cryptés Paxton10. L'application est utilisée pour effectuer les tâches suivantes,

Définir la clé de cryptage du site dans le lecteur de bureau

Mettre à jour le micrologiciel dans le lecteur de bureau

Modifier la clé de cryptage du site

Créer un jeton de liaison Paxlock

Pour que l'application de configuration du lecteur de bureau puisse effectuer ces tâches, elle doit être installée sur un PC qui se trouve sur le même réseau que le serveur Paxton10.Le Lecteur de bureau doit être connecté localement par USB au même PC.

Remarque : pour les installations multi-sites, cela signifie qu'il faudra configurer les lecteurs de bureau sur le réseau local où se trouve le serveur.

Une fois configurés, les Lecteurs de bureau peuvent être utilisés sur n'importe quel poste client de la même manière qu'avec les versions précédentes. L'application ne doit donc être installée que sur un seul PC et utilisée pour configurer tous les Lecteurs de bureau du système.

Un login d'ingénieur système est nécessaire pour utiliser l'application.

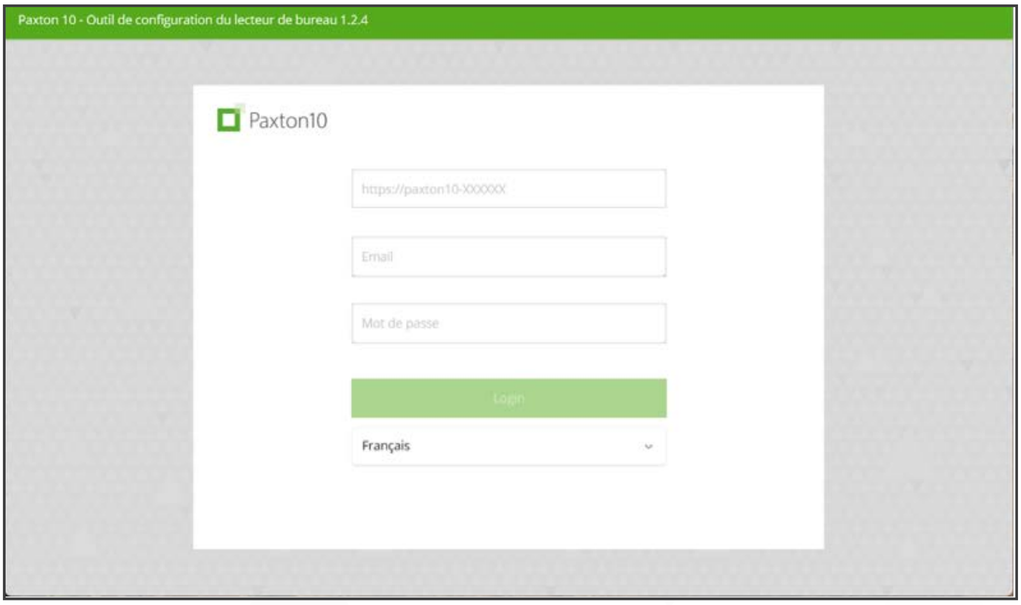
Paramétrage de la clé de cryptage du site dans un Lecteur de bureau.

C'est l'utilisation la plus courante de l'application de configuration. Tous les Lecteurs de bureau qui doivent enrôler des informations d'identification cryptées doivent passer par ce processus simple.

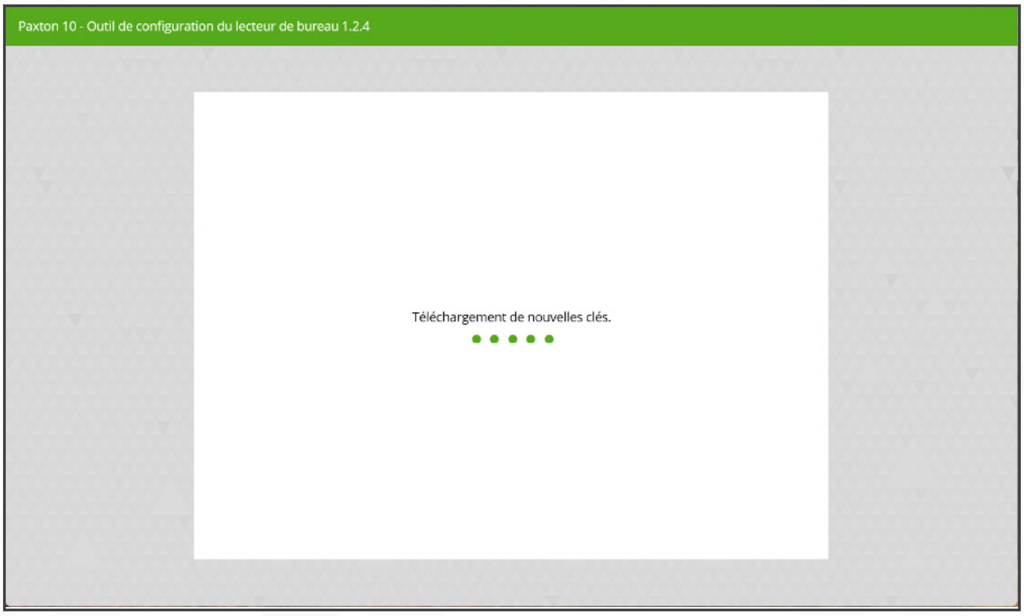
1. Veille à ce que le Lecteur de bureau soit connecté avant de lancer l'application.

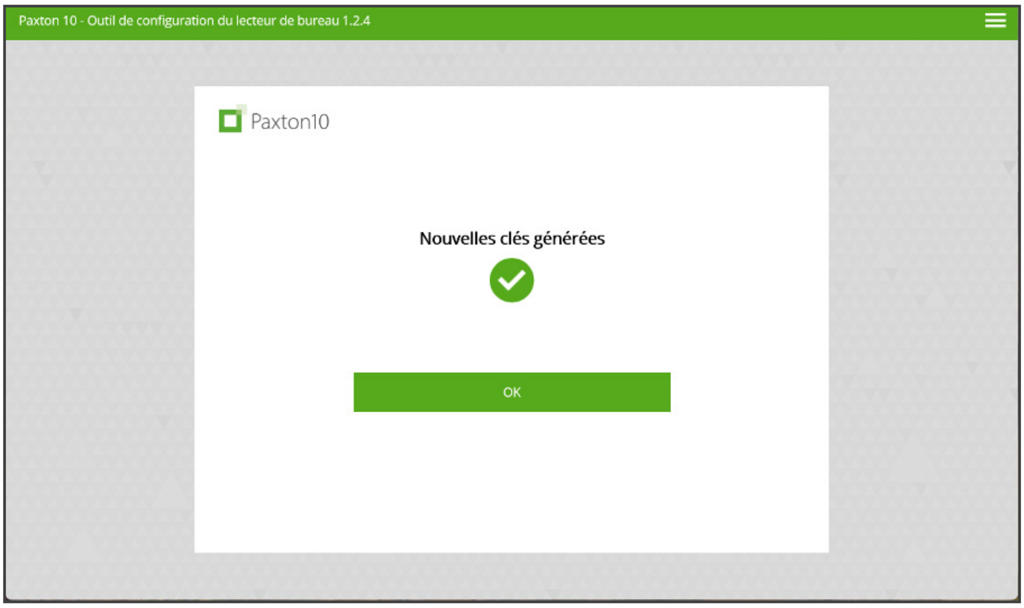
2. Lors du lancement de l'application, les informations de connexion de Paxton10 sont demandées.

3. Une fois connectée, l'application recherche automatiquement le lecteur de bureau connecté et transfère les clés de cryptage du site sur l'appareil.



4. L'application peut maintenant être fermée et le Lecteur de bureau est prêt à être utilisé pour l'enregistrement des informations d'identification cryptées.

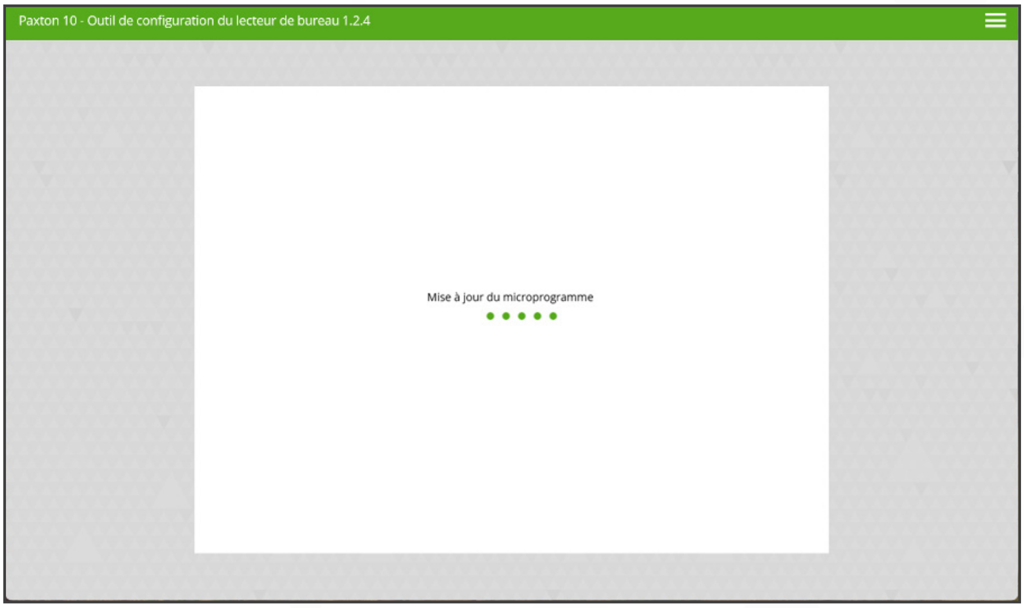


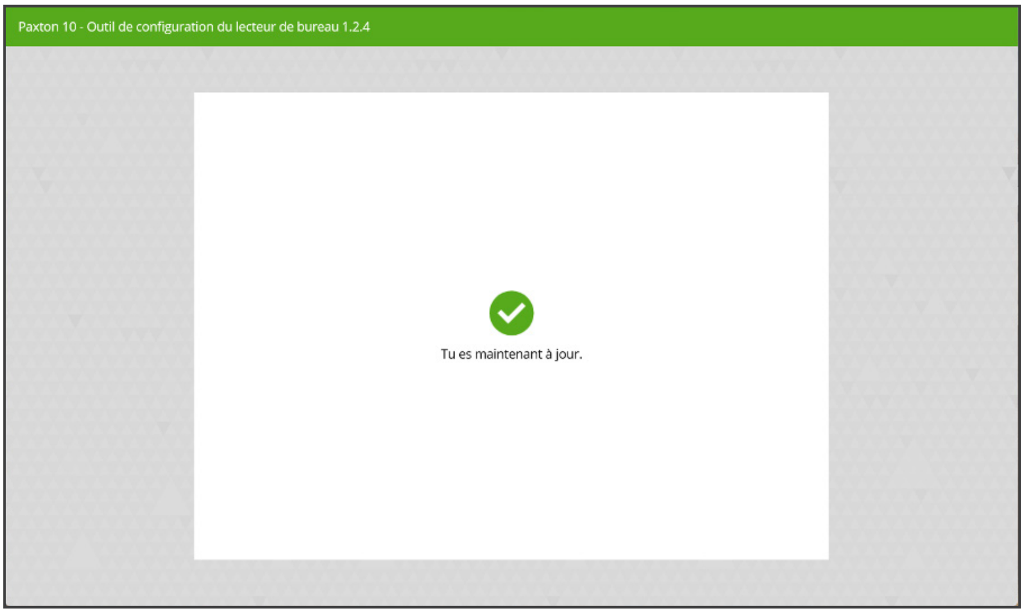


Mise à jour du micrologiciel d'un lecteur de bureau

Le lecteur de bureau universel Paxton10 a la possibilité de recevoir des mises à jour du micrologiciel à l'aide de l'application de configuration du lecteur de bureau.

1. Vérifie que le Lecteur de bureau est connecté lors de l'exécution de l'application,
2. Les données de connexion de Paxton10 sont demandées.
3. Une fois connectée, l'application recherche automatiquement le lecteur de bureau connecté et vérifie la version actuelle de son micrologiciel.
4. Si l'application dispose d'une version du micrologiciel plus récente que celle installée, une mise à jour automatique aura lieu.





5. Une fois la mise à jour effectuée, l'application peut être fermée.

Changer la clé de cryptage du site

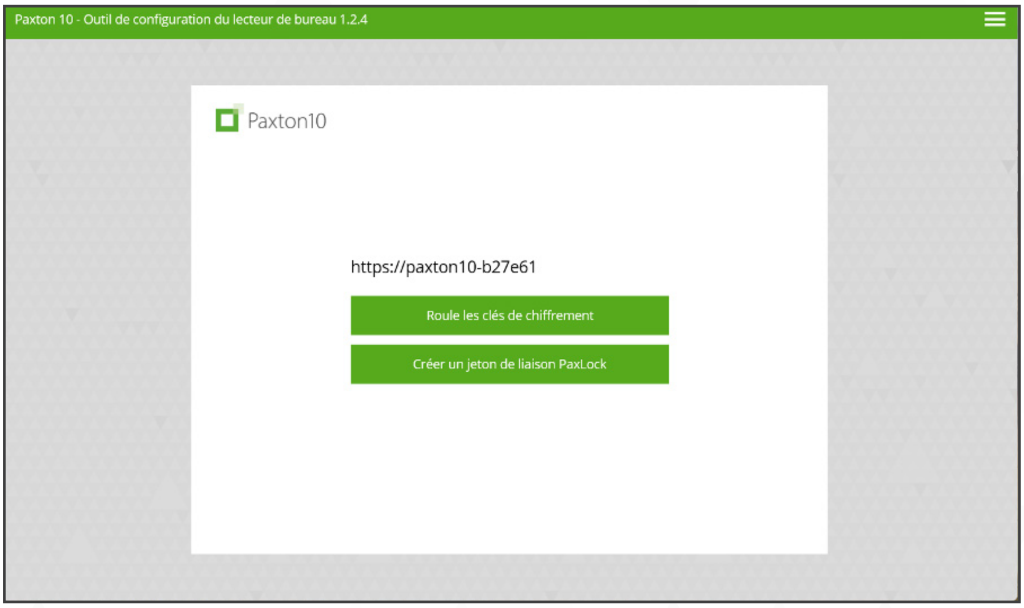
À l'aide de l'application de configuration, il est possible de changer la clé de cryptage utilisée sur un site. Cette opération peut être effectuée dans le cas où les clés sont découvertes ou si un site choisit périodiquement de changer sa clé.

Il est important de noter qu'une fois que la clé d'un système a été changée,

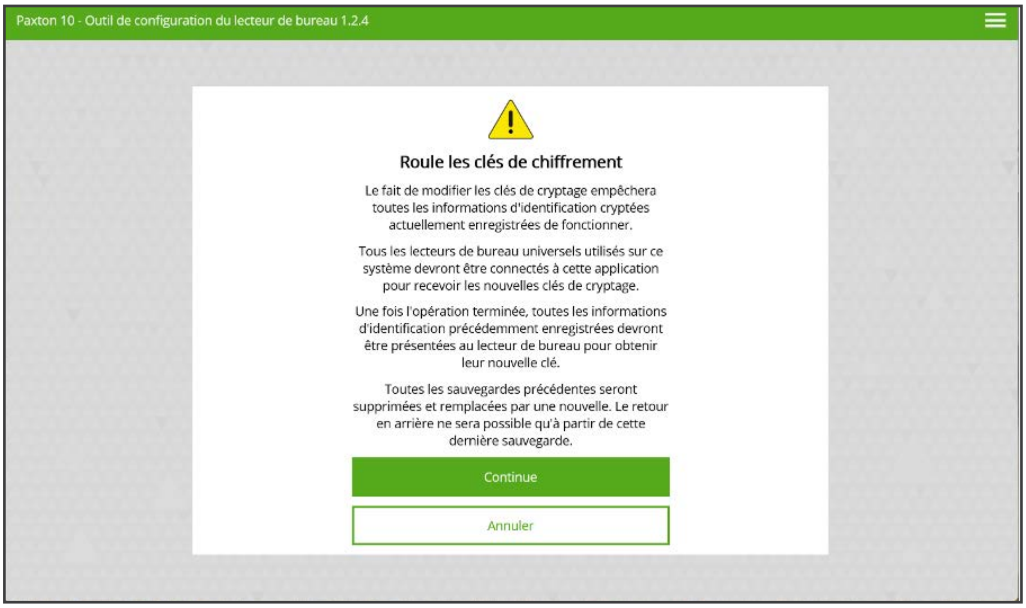
- Chaque lecteur de bureau doit avoir sa clé de cryptage mise à jour
- Toutes les informations d'identification cryptées doivent être renvoyées à un lecteur de bureau mis à jour pour que leur clé de cryptage soit changée afin qu'elles continuent à fonctionner sur le système.
- Les lecteurs présents sur le système verront leur clé mise à jour automatiquement

1. Lors de l'exécution de l'application, les informations de connexion de Paxton10 sont demandées.

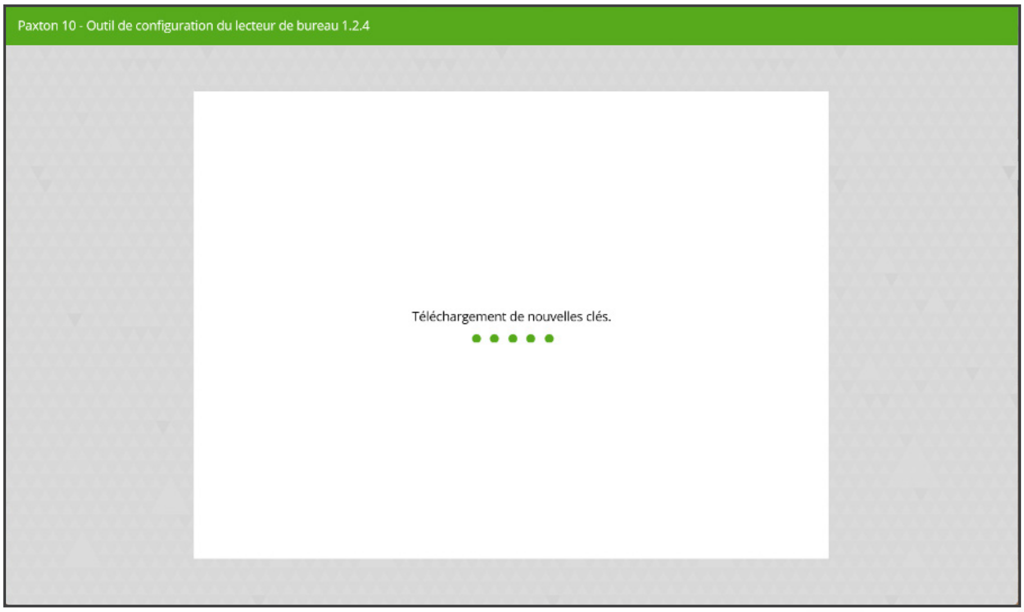
2. Sélectionne l'option "**Rouler les clés**".

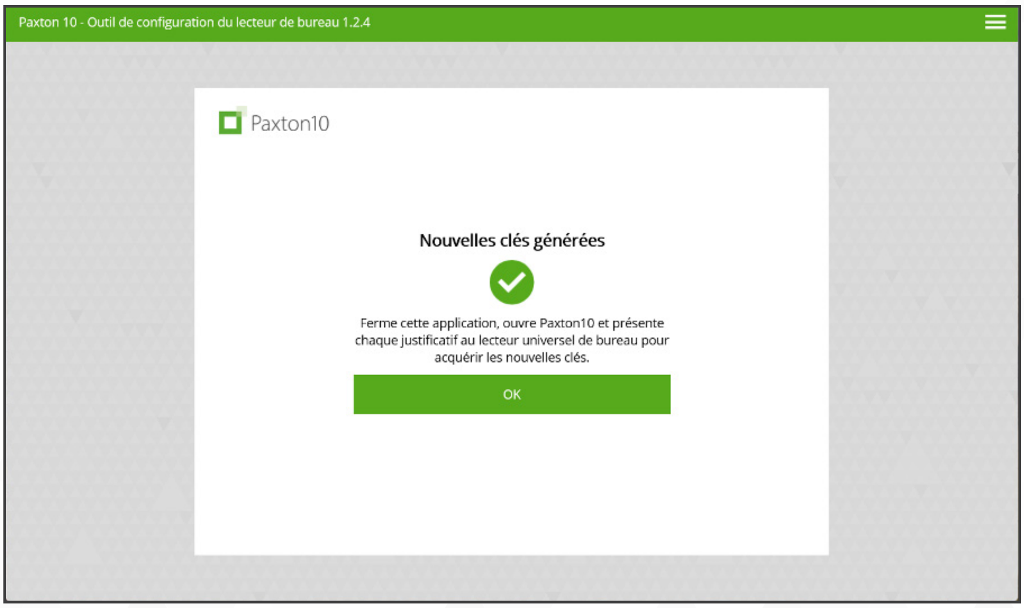


3. Un message d'avertissement s'affiche, décrivant les mesures à prendre une fois que les clés ont été modifiées.



4. Clique sur '**Continuer**'. Une nouvelle clé est générée sur le serveur Paxton10 et envoyée au Lecteur de bureau (s'il est connecté)





5. L'application peut être fermée.

Création d'un jeton de liaison Paxlock

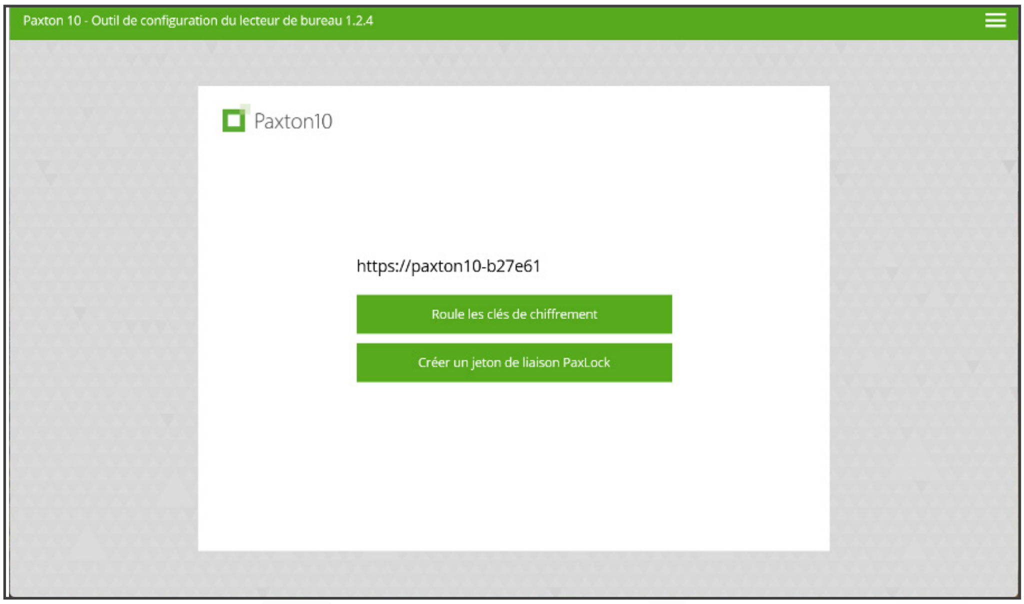
Lorsqu'ils fonctionnent en mode "Identifiants chiffrés uniquement", tous les Lecteurs doivent détenir les clés de chiffrement pour pouvoir lire les identifiants. Si un nouveau Paxlock doit être ajouté à un système, la méthode normale consiste à présenter un jeton valide du système au Paxlock. Cependant, en mode crypté, le Paxlock ne peut pas lire les informations d'identification tant qu'il n'a pas été lié au système et que les clés de cryptage du site ne lui ont pas été envoyées.

Pour contourner ce problème, l'application de configuration du Lecteur bureau permet de créer un jeton de liaison Paxlock à l'aide de l'une des informations d'identification cryptées. Cela permet de lier de nouveaux Paxlocks sans compromettre l'intégrité "cryptée uniquement" du système.

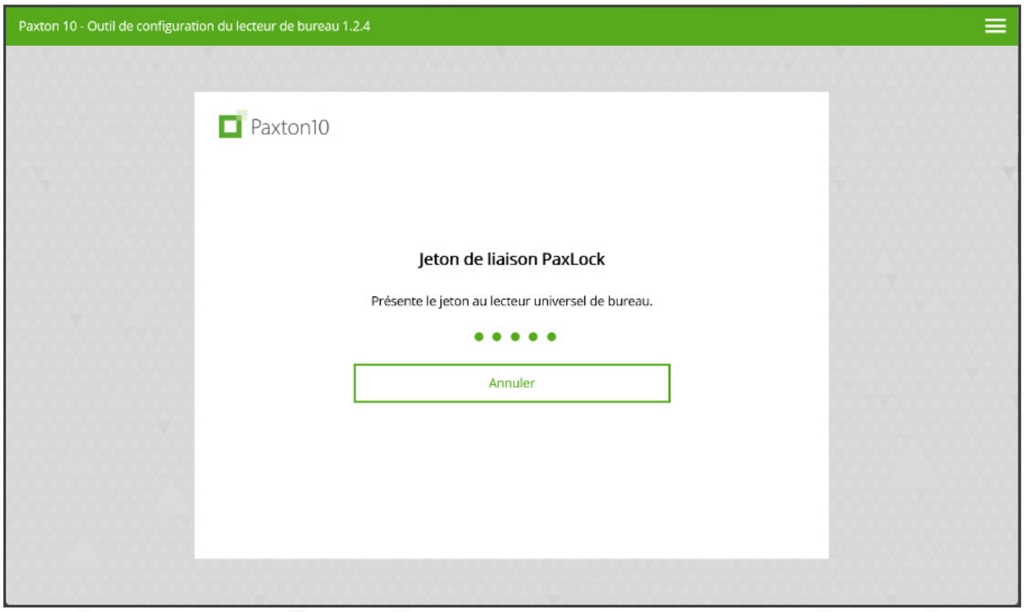
1. Assure-toi qu'un Lecteur de bureau est connecté au PC qui exécute l'application.

2. Lors de l'exécution de l'application, les informations de connexion de Paxton10 sont demandées.

3. Sélectionne l'option "**Créer un jeton de liaison Paxlock**".



4. Présente un justificatif d'identité crypté au lecteur de bureau.



5. Le Lecteur de bureau convertit le jeton en jeton de liaison Paxlock qui peut maintenant être utilisé pour connecter de nouveaux Paxlocks au système.

6. L'application peut être fermée.

Mode d'authentification cryptée uniquement

Pour faire fonctionner un système Paxton10 dans son mode le plus sécurisé, le système doit être configuré pour ne lire que les informations d'identification qui sont entièrement cryptées. L'activation de l'option 'Encrypted credentials only mode' entraîne les actions suivantes :

1. Toutes les informations d'identification qui ne sont pas cryptées sont supprimées de la base de données du système.

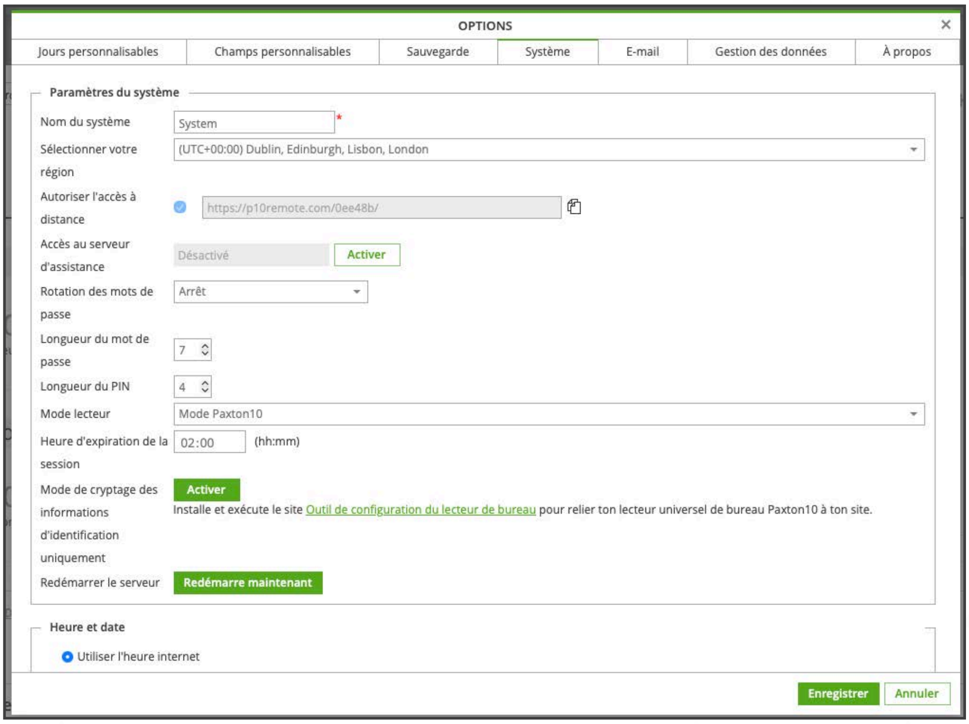
2. Les lecteurs du système ne liront plus les justificatifs qui ne sont pas cryptés.

3. Lecteur de bureau n'enrôlera plus les jetons qui ne sont pas cryptés.

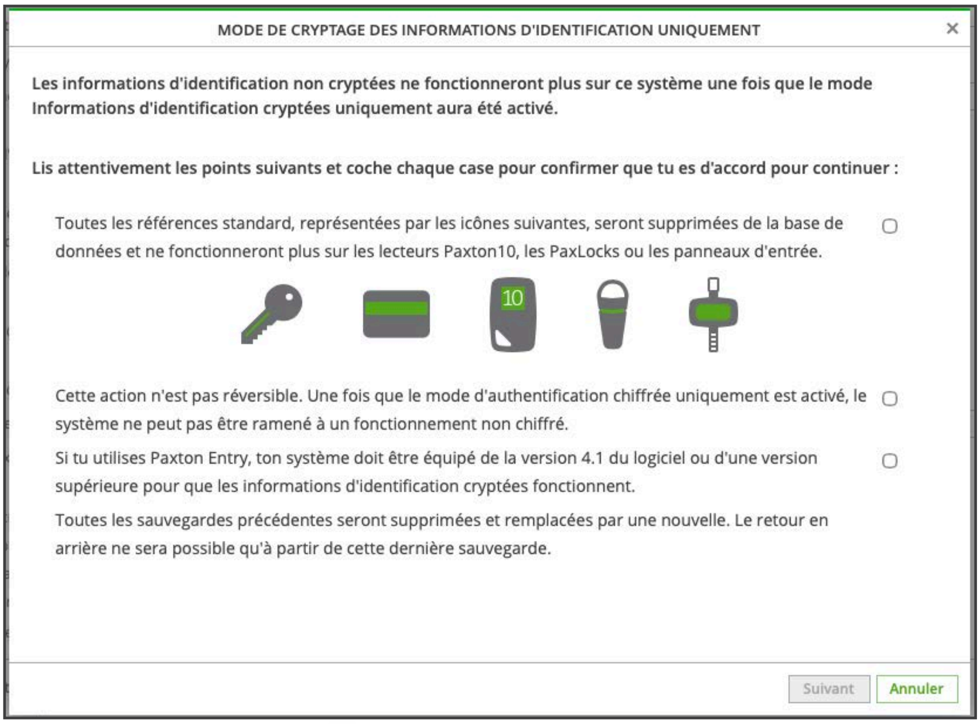
Le passage au mode "Informations d'identification cryptées uniquement" est un chemin à sens unique. Une fois que ce mode est activé, il ne peut pas être inversé.

Remarque : si des Platine d'entrée sont installées sur le système, elles doivent être mises à niveau vers la version 4.1 avant d'activer le mode " Références cryptées uniquement ".

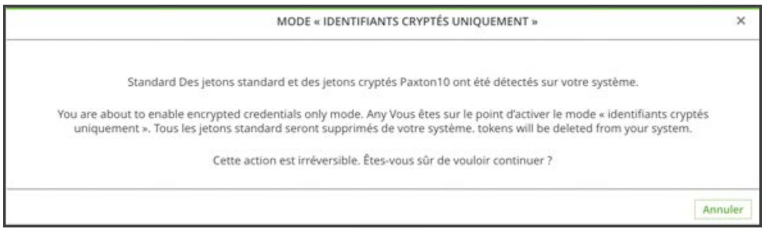
1. Pour activer le mode, va dans la fenêtre modale '**Options**' et sélectionne l'onglet '**Système**'. Clique sur le bouton "**Activer**".



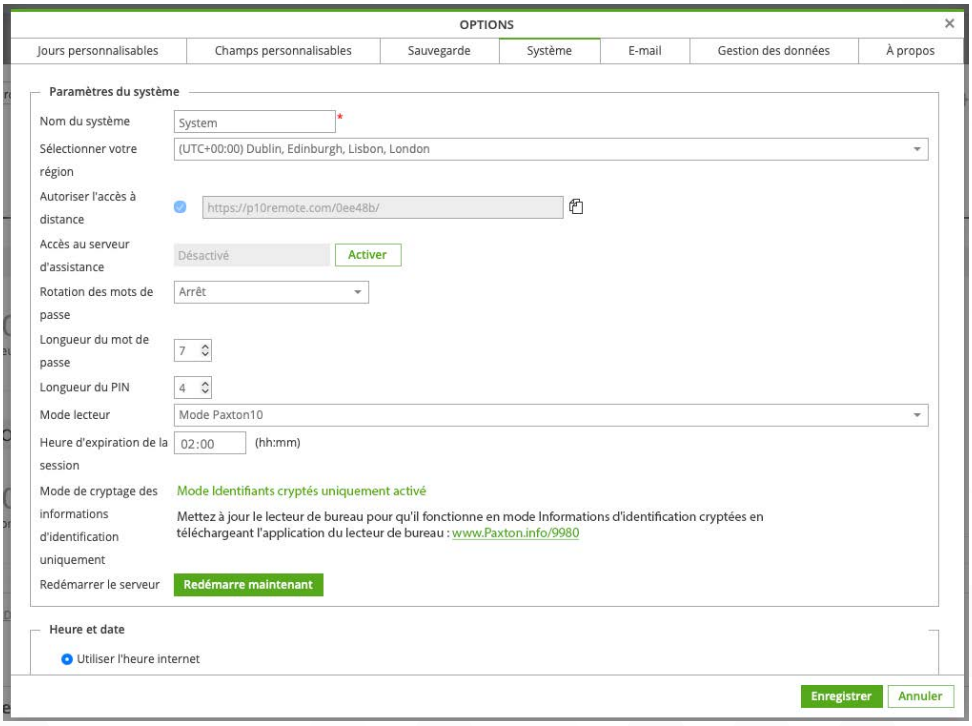
2. Les détails des implications de l'activation du mode Informations d'identification sécurisées uniquement s'affichent et il t'est demandé de confirmer que chaque étape est comprise.



3. Tu as une dernière chance d'annuler, car cette étape n'est pas réversible !



4. L'onglet '**Système**' indique maintenant que le système a activé le mode d'authentification cryptée uniquement.



Le site est maintenant configuré pour n'accepter que les informations d'identification cryptées ; pour le reste, le système fonctionnera normalement.