Outil de protection des données Blue Prism

L'outil de protection des données Blue Prism est utilisé pour déchiffrer et chiffrer les chaînes de connexion stockées dans le fichier appsettings.json. Pour des raisons de sécurité, les chaînes de connexion sont chiffrées et l'outil de protection des données Blue Prism permet de les déchiffrer, afin qu'elles puissent être modifiées si nécessaire, puis chiffrées à nouveau.

L'outil BluePrismDataProtector.Console est un outil de ligne de commande et doit être utilisé avec Windows PowerShell s'exécutant en tant qu'administrateur.

Déchiffrer une chaîne de connexion

Pour utiliser l'outil pour déchiffrer une chaîne de connexion :

1. Téléchargez le fichier BluePrismDataProtector.Console.exe à partir du portail Blue Prism et enregistrez-le à un emplacement pratique sur votre appareil.
2. Ouvrez PowerShell en tant qu'administrateur dans le dossier où se trouve BluePrismDataProtector.Console.exe.
   La fenêtre Administrateur : Windows PowerShell s'affiche.

   > Si vous tapez *.\BluePrismDataProtector.Console.exe* sur la ligne de commande et appuyez sur Entrée, une liste des commandes possibles s'affiche.

3. Dans l'Explorateur Windows, ouvrez le fichier appsettings.json qui contient la chaîne que vous souhaitez déchiffrer et copiez-la. Par exemple :


```
"HubServiceBus": {
  "Connection": "CfDJ8LadX9spUNhMhvbxTcsxZYTHFA3m8Tyl-Z_EZ0Zn16mYfv_23Q2D2waPDTBXaz4-viNO2Akk-S5C73dNjOdGHifGCxSIftwExJ3O4FuDXHpbNo0be-xyQtlD1-j7rosuYw",
  "Topic": "thttopic",
  "Subscription": "Hub",
```


4. Dans PowerShell, saisissez les informations suivantes :

```
.\BluePrismDataProtector.Console.exe unprotect -v "[string]" -p "[path]"
```

   Où :

   `[string]` = la chaîne copiée à partir du fichier

   `[path]` = le chemin d'accès à DataProtectionKeys. Généralement, C:\Program Files (x86)\Blue Prism\DataProtectionKeys

   Par exemple :

```
.\BluePrismDataProtector.Console.exe unprotect -v "CfDJ8LadX9spUNhMhvbxTcsxZYTHFA3m8Tyl-Z_
EZ0Zn16mYfv_23Q2D2waPDTBXaz4-viNO2Akk-S5C73dNjOdGHifGCxSIftwExJ3O4FuDXHpbNo0be-xyQtlD1-
j7rosuYw" -p "C:\Program Files (x86)\Blue Prism\DataProtectionKeys"
```

5. Appuyez sur **Entrée**.
   La chaîne est déchiffrée et la valeur non chiffrée s'affiche dans PowerShell.

Chiffrer une chaîne de connexion

Pour utiliser l'outil pour chiffrer une chaîne de connexion :

1. Ouvrez PowerShell en tant qu'administrateur dans le dossier où se trouve BluePrismDataProtector.Console.exe.
   La fenêtre Administrateur : Windows PowerShell s'affiche.

   > Si vous tapez *.\BluePrismDataProtector.Console.exe* sur la ligne de commande et appuyez sur Entrée, une liste des commandes possibles s'affiche.

2. Dans PowerShell, saisissez les informations suivantes :

   ```
   .\BluePrismDataProtector.Console.exe protect -v "[string]" -p "[path]"
   ```

   Où :

   `[string]` = la chaîne que vous souhaitez chiffrer

   `[path]` = le chemin d'accès à DataProtectionKeys. Généralement, C:\Program Files (x86)\Blue Prism\DataProtectionKeys

   Par exemple :

   ```
   .\BluePrismDataProtector.Console.exe unprotect -v "Str0ngP@SsW0rD" -p "C:\Program Files (x86)\Blue Prism\DataProtectionKeys"
   ```

3. Appuyez sur **Entrée**.
   La chaîne est chiffrée et la valeur s'affiche dans PowerShell, par exemple :
   `CfDJ8LadX9spUNhMhvbxTcsxZYTHFA3m8Tyl-Z_EZ0Znl6mYfv_23Q2D2waPDTBXaz4-viNO2Akk-S5C73dNjOdGHifGCxSIftwExJ3O4FuDXHpbNo0be-xyQtlD1-j7rosuYw`

4. Copiez la chaîne chiffrée à l'emplacement approprié dans le fichier appsettings.json et enregistrez le fichier.

5. Ouvrez le gestionnaire d'IIS et redémarrez le pool d'applications approprié pour vous assurer qu'il utilise la nouvelle chaîne de connexion.

> Si des caractères dans votre chaîne sont associés à des commandes dans PowerShell même, vous devrez ajouter un caractère d'échappement à votre chaîne afin que PowerShell honore la chaîne comme prévu. Exemple :
>
> - ` et $ auront besoin d'un ` (backtick) avant le caractère. Par exemple, Str0ng`P@$$W0rD devra être saisi comme « Str0ng``P@`$`$W0rD » sur la ligne de commande.
> - " aura besoin de \` avant. Par exemple, P@$"W0rD devra être saisi comme « P@`$\`"W0rD » sur la ligne de commande.
>
> Ces caractères d'échappement supplémentaires maintiennent l'intégrité de la chaîne. Si la valeur chiffrée résultante est à nouveau déchiffrée, la valeur correspond à la chaîne d'origine plutôt qu'à la version de ligne de commande.