Blue Prism Data Protector Tool

Das Blue Prism Data Protector Tool wird verwendet, um in der Datei appsettings.json gespeicherte Verbindungszeichenfolgen zu entschlüsseln und zu verschlüsseln. Aus Sicherheitsgründen werden die Verbindungszeichenfolgen verschlüsselt. Das Blue Prism Data Protector Tool ermöglicht es, sie zu entschlüsseln, damit sie bei Bedarf geändert und dann erneut verschlüsselt werden können.

Das Tool BluePrismDataProtector.Console ist ein Befehlszeilen-Tool und sollte mit Windows PowerShell im Administratormodus ausgeführt werden.

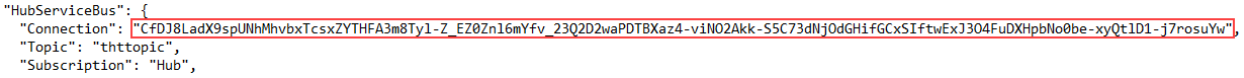
Verbindungszeichenfolgen entschlüsseln

So verwenden Sie das Tool zum Entschlüsseln einer Verbindungszeichenfolge:

1. Laden Sie die Datei BluePrismDataProtector.Console.exe vom Blue Prism Portal herunter und speichern Sie sie auf Ihrem Gerät.
2. Öffnen Sie PowerShell als Administrator im Ordner, in dem sich BluePrismDataProtector.Console.exe befindet.
   Das Fenster „Administrator: Windows PowerShell“ wird angezeigt.

   > Wenn Sie *.\BluePrismDataProtector.Console.exe* in der Befehlszeile eingeben und die Eingabetaste drücken, wird eine Liste der möglichen Befehle angezeigt.

3. Öffnen Sie im Windows Explorer die Datei appsettings.json, die die Verbindungszeichenfolge enthält, die Sie entschlüsseln und kopieren möchten. Zum Beispiel:



4. Geben Sie in PowerShell Folgendes ein:

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

   Dabei gilt:

   `[string]` = die kopierte Zeichenfolge aus der Datei

   `[path]` = der Pfad zu DataProtectionKeys. Typischerweise C:\Program Files (x86)\Blue Prism\DataProtectionKeys

   Zum Beispiel:

```
.\BluePrismDataProtector.Console.exe unprotect -v "CfDJ8LadX9spUNhMhvbxTcsxZYTHFA3m8Tyl-Z_
EZ0Znl6mYfv_23Q2D2waPDTBXaz4-viNO2Akk-S5C73dNjOdGHifGCxSIftwExJ3O4FuDXHpbNo0be-xyQtlD1-
j7rosuYw" -p "C:\Program Files (x86)\Blue Prism\DataProtectionKeys"
```

5. Drücken Sie die **Eingabetaste**.
   Die Zeichenfolge wird entschlüsselt und der unverschlüsselte Wert wird in PowerShell angezeigt.

Verbindungszeichenfolgen verschlüsseln

So verwenden Sie das Tool zum Verschlüsseln einer Verbindungszeichenfolge:

1. Öffnen Sie PowerShell als Administrator im Ordner, in dem sich BluePrismDataProtector.Console.exe befindet.
   Das Fenster „Administrator: Windows PowerShell“ wird angezeigt.

   > Wenn Sie *.\BluePrismDataProtector.Console.exe* in der Befehlszeile eingeben und die Eingabetaste drücken, wird eine Liste der möglichen Befehle angezeigt.

2. Geben Sie in PowerShell Folgendes ein:

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

   Dabei gilt:

   `[string]` = die Zeichenfolge, die Sie verschlüsseln möchten

   `[path]` = der Pfad zu DataProtectionKeys. Typischerweise C:\Program Files (x86)\Blue Prism\DataProtectionKeys

   Zum Beispiel:

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

3. Drücken Sie die **Eingabetaste**.
   Die Zeichenfolge wird verschlüsselt und der Wert wird in PowerShell angezeigt, zum Beispiel:
   `CfDJ8LadX9spUNhMhvbxTcsxZYTHFA3m8Tyl-Z_EZ0Znl6mYfv_23Q2D2waPDTBXaz4-viNO2Akk-S5C73dNjOdGHifGCxSIftwExJ3O4FuDXHpbNo0be-xyQtlD1-j7rosuYw`
4. Kopieren Sie die verschlüsselte Zeichenfolge an den entsprechenden Platz in der Datei appsettings.json und speichern Sie die Datei.
5. Öffnen Sie IIS Manager und starten Sie den entsprechenden Anwendungspool neu, um sicherzustellen, dass er die neue Verbindungszeichenfolge verwendet.

Wenn sich Zeichen in Ihrer Zeichenfolge befinden, die Befehlen in PowerShell zugeordnet sind, müssen Sie Ihrer Zeichenfolge ein Escapezeichen hinzufügen, damit PowerShell sie korrekt interpretiert. Zum Beispiel:

- ` und $ benötigen ein ` (Backtick) vor dem Zeichen, zum Beispiel, Str0ng`P@$$W0rD müsste als „Str0ng``P@`$`$W0rD“ in die Befehlszeile eingegeben werden.
- " muss ein \` vorangestellt sein, zum Beispiel müsste P@$"W0rD als „P@`$\`"W0rD“ in der Befehlszeile eingegeben werden.

Diese zusätzlichen Escapezeichen wahren die Integrität der Zeichenfolge. Wenn der resultierende verschlüsselte Wert wieder entschlüsselt wird, entspricht der Wert der ursprünglichen Zeichenfolge und nicht der Befehlszeilenversion.