Blue Prism Data Protector Tool

The Blue Prism Data Protector tool is used to decrypt and encrypt connection strings stored in the appsettings.json file. For security reasons, the connection strings are encrypted and the Blue Prism Data Protector tool allows the strings to be decrypted, so they can be altered if needed, and then encrypted again.

The BluePrismDataProtector.Console tool is a command line tool and should be used with Windows PowerShell running as an administrator.

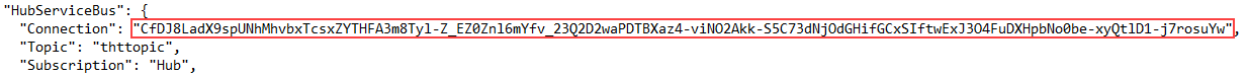
Decrypt a connection string

To use the tool to decrypt a connection string:

1. Download the BluePrismDataProtector.Console.exe file from the Blue Prism Portal and save to a convenient location on your device.
2. Open PowerShell as an administrator in the folder where BluePrismDataProtector.Console.exe is located.
   The Administrator: Windows PowerShell window displays.

   > If you type *.\BluePrismDataProtector.Console.exe* at the command line and press Enter, a list of possible commands will display.

3. From Windows Explorer, open the appsettings.json file that contains the string you want to decrypt and copy it. For example:



4. In PowerShell, type the following:

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

   Where:

   `[string]` = the copied string from the file

   `[path]` = the path to DataProtectionKeys. Typically, C:\Program Files (x86)\Blue Prism\DataProtectionKeys

   For example:

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

5. Press **Enter**.
   The string is decrypted and the unencrypted value displays in PowerShell.

Encrypt a connection string

To use the tool to encrypt a connection string:

1. Open PowerShell as an administrator in the folder where BluePrismDataProtector.Console.exe is located.
   The Administrator: Windows PowerShell window displays.

   If you type *.\BluePrismDataProtector.Console.exe* at the command line and press Enter, a list of possible commands will display.

2. In PowerShell, type the following:

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

   Where:

   `[string]` = the string that you want to encrypt

   `[path]` = the path to DataProtectionKeys. Typically, C:\Program Files (x86)\Blue Prism\DataProtectionKeys

   For example:

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

3. Press **Enter**.
   The string is encrypted and the value displays in PowerShell, for example:
   `CfDJ8LadX9spUNhMhvbxTcsxZYTHFA3m8Tyl-Z_EZ0Znl6mYfv_23Q2D2waPDTBXaz4-viNO2Akk-S5C73dNjOdGHifGCxSIftwExJ3O4FuDXHpbNo0be-xyQtlD1-j7rosuYw`

4. Copy the encrypted string into the appropriate place in the appsettings.json file and save the file.

5. Open IIS Manager and restart the appropriate Application Pool to ensure it uses the new connection string.

If there are characters in your string which are associated with commands in PowerShell itself, you will need to add an escape character to your string so that PowerShell honors the string as intended. Such as:

- ` and $ will need a ` (backtick) before the character, for example, Str0ng`P@$$W0rD would need to be entered as "Str0ng``P@`$`$W0rD" on the command line.
- " will need \` before it, for example, P@$"W0rD would need to be entered as "P@`$\`"W0rD" on the command line.

These additional escape characters maintain the integrity of the string. If the resulting encrypted value is decrypted again, the value would match the original string rather than the command line version.