Data Protection & Let's Encrypt SSL/TLS Certificates

PxPlus 2019 (v16)

Agenda

- Security on PxPlus Data
- Let’s Encrypt Support

SECURITY ON PXPLUS DATA

PASSWORD Directive

- To use PASSWORD directive, the file must be locked and empty
- Add a password to a data file

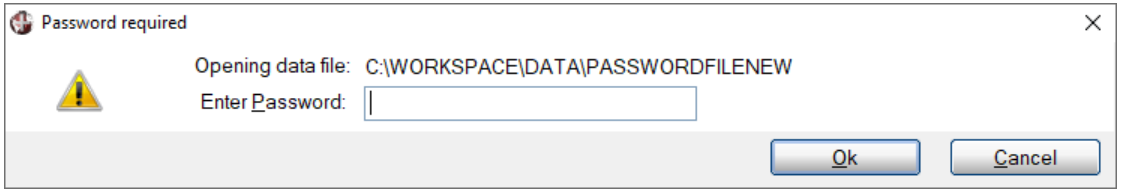
```
PASSWORD (chn) pwd$ REQUIRED FOR [OPEN|WRITE]
```

- Add a password to a data file and encrypt

```
PASSWORD (chn) pwd$ REQUIRED FOR [OPEN|WRITE] AND ON DATA
```

PASSWORD Directive

- Opening passworded/encrypted file prompts user for password



- To avoid prompt, use KEY=pwd$ with OPEN directive
  - Warning: to keep the password secret you must password protect the program

```
OPEN (chn, KEY=pwd$) filename$
```

Password/Encryption Types

New in PxPlus 2019

- Legacy
  - Passwords up to 8 characters, data beyond that ignored
  - PxPlus custom algorithm to hash password
  - PxPlus custom algorithm to encrypt data
  - Slightly faster

- Industry Standard
  - Passwords up to 128 characters, data beyond that ignored
  - Passwords salted then SHA-256 hashed
  - Data encrypted using AES-256
  - Compatible with PxPlus 2019 and up

Purpose of the Industry Standard Type

- Better protect customers' data
  - Longer passwords to prevent brute force
  - Proven resistance to cracking

- Security industry recognized
  - Security Audits
  - PCI Compliance

Select Password/Encryption Type

New in PxPlus 2019

- Encryption Algorithm 'EA' system parameter selects password/encryption type used for new passwords
  - Off = legacy (default)
  - On = industry standard

- Prefixing a password with "*AES:" allows using industry standard password/encryption on a per file basis when 'EA' is off

```
PASSWORD (HFN) "*AES:centuryraiselocationscientific" REQUIRED FOR OPEN AND ON DATA
```

LET’S ENCRYPT SUPPORT

Let’s Encrypt

- Let's Encrypt is a free and open certificate authority
  - Issues certificates to secure websites (HTTPS) and communications (SSL/TLS)
  - Certificates have a 90-day lifetime
  - Automated certificate renewal through client software
  - Run for public benefit

Reasons to Use Let's Encrypt

- Simplifies use of SSL/TLS by removing many barriers that prevented use
  - No cost
  - No Certificate Signing Request (CSR)
  - No company background check
  - Only need to prove you control the domain using client software
  - Much faster way to obtain a certificate and get up and running

- If it is easier to get a certificate, more people will use SSL/TLS improving security

Get a Let's Encrypt Certificate

- Install and run client on server where certificate is needed
  - UNIX/Linux client: Certbot
  - Windows client: Certify the Web
- Both clients setup automatic certificate renewal for you
- Certbot on older UNIX/Linux is the exception
  - Setup OS to run certbot renew command twice a day
- Let's Encrypt servers must access port 80 to verify control of the domain

Get a Let's Encrypt Certificate

- Certify the Web generates a new filename every time certificate is renewed
  - PxPlus 2019 ships with a script to handle this
  - Set Post-Request PS Script to the real path of script

```
PxPlus path: *ezweb\certifytheweb.ps1
Real path: C:\MyCompany\MyApp\lib\_ezweb\ certifytheweb.ps1
```

- New/Renewed Certificate file output
  - Certbot
    - /etc/letsencrypt/live/exp.com/fullchain.pem
    - /etc/letsencrypt/live/exp.com/privkey.pem
  - Certify the Web
    - C:\ProgramData\Certify\certes\assets\pfx\exp.com.pfx (no password)

More Info on Let's Encrypt

- This is only a rough outline of the process - for full details see:
  - PxPlus documentation
  - Let's Encrypt documentation
  - Certbot documentation
  - Certify the Web documentation

[TCP] Let's Encrypt Support

New in PxPlus 2019

- Certbot: use the [TCP] option PRIVKEY=pathname

```
OPEN (HFN) "[TCP];443;SECURE=/etc/letsencrypt/live/exp.com/fullchain.pem;PRIVKEY=/etc/letsencrypt/live/exp.com/privkey.pem"
```

- Certify the Web: use the *tools/pfxcertconvert utility

```
CALL "*tools/pfxcertconvert", "C:\ProgramData\Certify\certes\assets\pfx\exp.com.pfx", "", "converted.pem"
OPEN (HFN) "[TCP];443;SECURE=converted.pem"
```

EZWeb Let's Encrypt Support

New in PxPlus 2019

- EZWeb supports separate certificate/private key PEM files to allow use of Certbot generated certificates
  - New privkey=pathname option in the command line security argument

```
/app/pxplus "*ezweb/server" -arg 443 "/etc/letsencrypt/live/exp.com/fullchain.pem  privkey=/etc/letsencrypt/live/exp.com/privkey.pem"
```

  - New privkey pathname directive supported in the ezweb.conf configuration file

```
port 443
secure "/etc/letsencrypt/live/exp.com/fullchain.pem"
privkey "/etc/letsencrypt/live/exp.com/privkey.pem"
nobrowse
```

EZWeb Let's Encrypt Support

New in PxPlus 2019

- EZWeb supports passworded PFX certificate files to allow use of Certify the Web generated certificates
  - New pfxpswd=password option in the command line security argument

```
"C:\app\pxplus.exe" *ezweb\server -arg 443 "C:\ProgramData\Certify\certes\assets\pfx\exp.com.pfx pfxpswd="
```

  - New pfxpswd password directive supported in the ezweb.conf configuration file

```
port 443
secure "C:\ProgramData\Certify\certes\assets\pfx\exp.com.pfx"
pfxpswd ""
nobrowse
```

EZWeb Let's Encrypt Support

New in PxPlus 2019

- A restart of EZWeb is no longer required to use a renewed certificate
  - EZWeb will check for a renewed certificate as part of the first request after midnight
  - If a renewed certificate is found, EZWeb will automatically be updated to use it
  - Any new connections will use the renewed certificate
  - Any existing connections will become unresponsive; however, refreshing the page will restore the session using the renewed certificate

Recap

- Use the industry standard password/encryption to better protect data
- Let’s Encrypt is a free and simple way to secure your PxPlus applications network communications

Additional Resources

The help link(s) below refer to the current on-line help pages. The functionality may have been further updated since the PxPlus 2019 (version 16) release.

- PASSWORD Directive
- 'EA' Encryption Algorithm
- Let's Encrypt SSL/TLS Certificates with PxPlus
- Let's Encrypt Documentation
- Certbot
- Certify the Web
- [TCP] PRIVKEY Option
- *TOOLS/PFXCERTCONVERT
- EZWeb Server