On Premise: Opsætning af sikkerhedsprotokoller

Formål

Dette dokument vejleder i, hvilke krav XFlow stiller til jeres sikkerhedsprotokoller for at kunne integrere med eksterne services, samt hvordan disse kan opdateres, hvis det er nødvendigt.

Vejledning

- Windows Server skal understøtte de nyeste versioner af de gængse sikkerhedsprotokoller som fx TLS 1.2. Fuldt opdaterede Windows Server-versioner fra og med version 2008 R2 understøtter de nyeste protokoller
- I mange tilfælde skal protokollerne dog slås til, før de kan benyttes. Protokollerne kan slås til med værktøjet IIS Crypto, der kan indstille en Windows Server til at understøtte "best practice" for sikkerhedsprotokoller
- IIS Crypto kan downloades her, og der kan findes yderligere information om værktøjet her.
- Når du har hentet værktøjet, skal du gøre følgende:
    - Start IIS Crypto
    - Tryk på knappen "Best Practices"
    - Tryk på knappen "Apply"
    - Genstart serveren

- Det vil ofte være nødvendigt at indstille din Windows Server til at tvinge .NET applikationer til at benytte nyeste sikkerhedsprotokoller. Dette er især vigtigt for webapplikationer som XFlow.
- Dette gøres ved at udføre følgende PowerShell script:

```
# set strong cryptography on 64 bit .Net Framework (version 4 and above)
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Wow6432Node\Microsoft\.NetFramework\v4.0.30319' -Name 'SchUseStrongCrypto' -Value '1' -Type DWord

# set strong cryptography on 32 bit .Net Framework (version 4 and above)
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\.NetFramework\v4.0.30319' -Name 'SchUseStrongCrypto' -Value '1' -Type DWord
```