SC DAST 25.2 - FortifyConnect Certificate configuration.

01 September 2025 15:51

Version 25.2 the self-signed certificate is no longer generated. You have to generate self-signed certificate and configure it in FortifyConnect settings file.

Please follow the below steps to generate self-signed certificate on Linux OS and to configure the FortifyConnect settings file.

1. **Generate a Private Key**
   openssl genrsa -out server.key 2048

2. **Create a Certificate Signing Request (CSR)**
   openssl req -new -key server.key -out server.csr -subj "/C=<COUNTRY>/ST=<STATE>/L=<LOCATION>/O=OpenText/OU=IT/CN=fc.test.fortifyhosted.com"

3. **Generate the Self-Signed Certificate**
   openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt

4. **Combine into a .pem for Fortify**
   cat server.crt server.key > fortify-connect-api-certificate.pem

5. **Create folder and copy certificates.**
   mkdir -p /home/fortifyconnectsshuser/scdast/certificates/
   cp fortify-connect-api-certificate.pem .
   cp server.key fortify-connect-api-key.key

6. **Update certficate path in JSON file under Kestrel**
   nano FortifyConnectClientSettings_XX.json

   "Certificate": {
   "Path": "/home/fortifyconnectsshuser/scdast/certificates/fortify-connect-api-certificate.pem",
   "KeyPath": "/home/fortifyconnectsshuser/scdast/certificates/fortify-connect-api-key.key"
   }

```
"Kestrel": {
  "Endpoints": {
   "Https": {
    "Url": "https://127.0.0.1:35477",
    "SslProtocols": [
     "Tls12",
     "Tls13"
    ],
    "Certificate": {
     "Path": "/home/fortifyconnectsshuser/scdast/certificates/fortify-connect-api-certificate.pem",
     "KeyPath": "/home/fortifyconnectsshuser/scdast/certificates/fortify-connect-api-key.key"
    }
   }
  }
 }
```

7. **Run ./StartFortifyConnectClient_XX.sh**