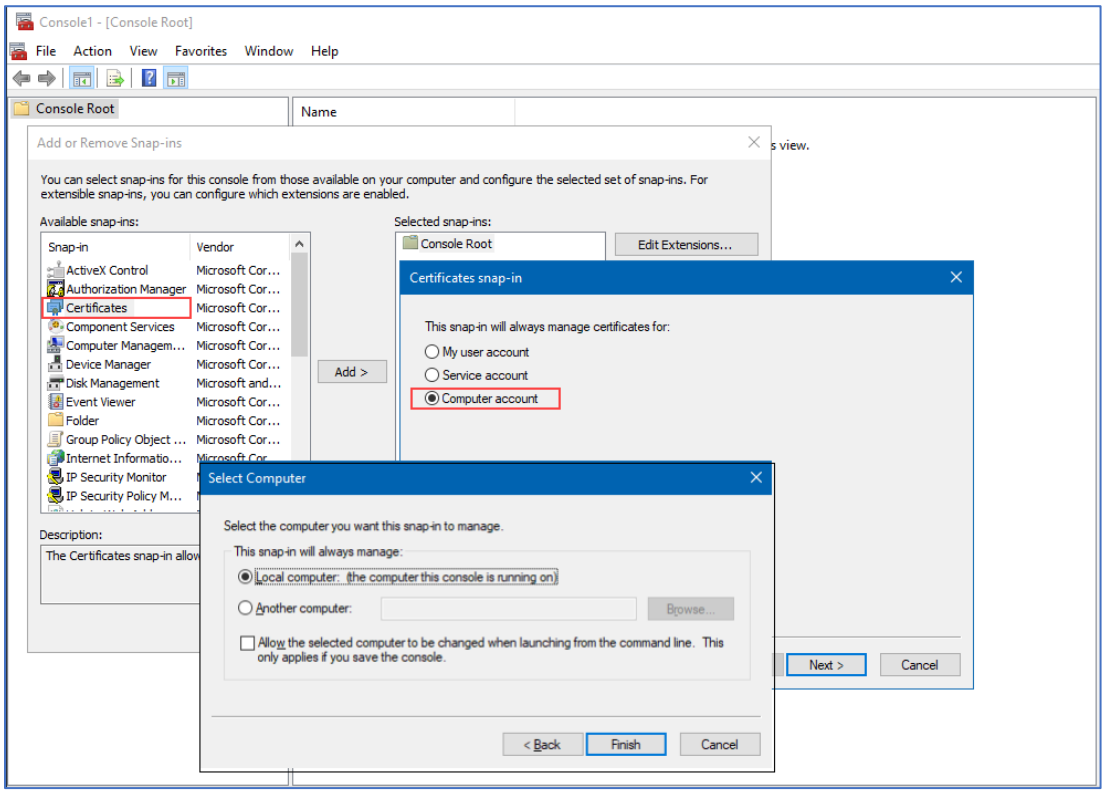
1. **Create pfx file from XOSecurity Certificate**

2. **Apply pfx to Solr Service**

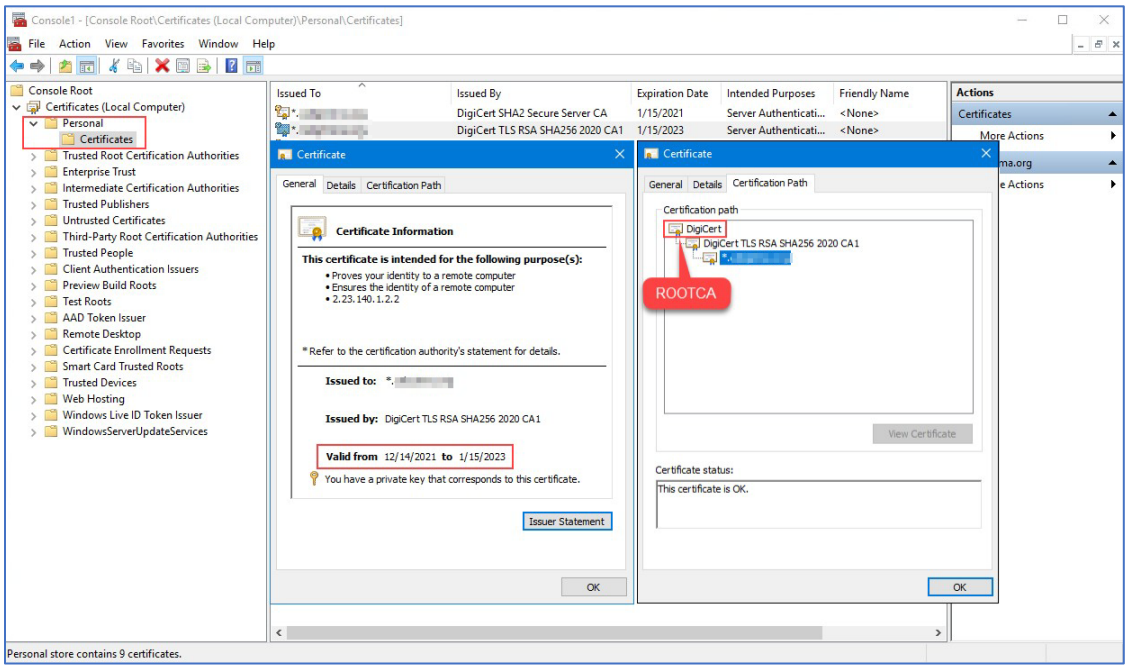
Create pfx file from XOSecurity Certificate

1. Open MMC

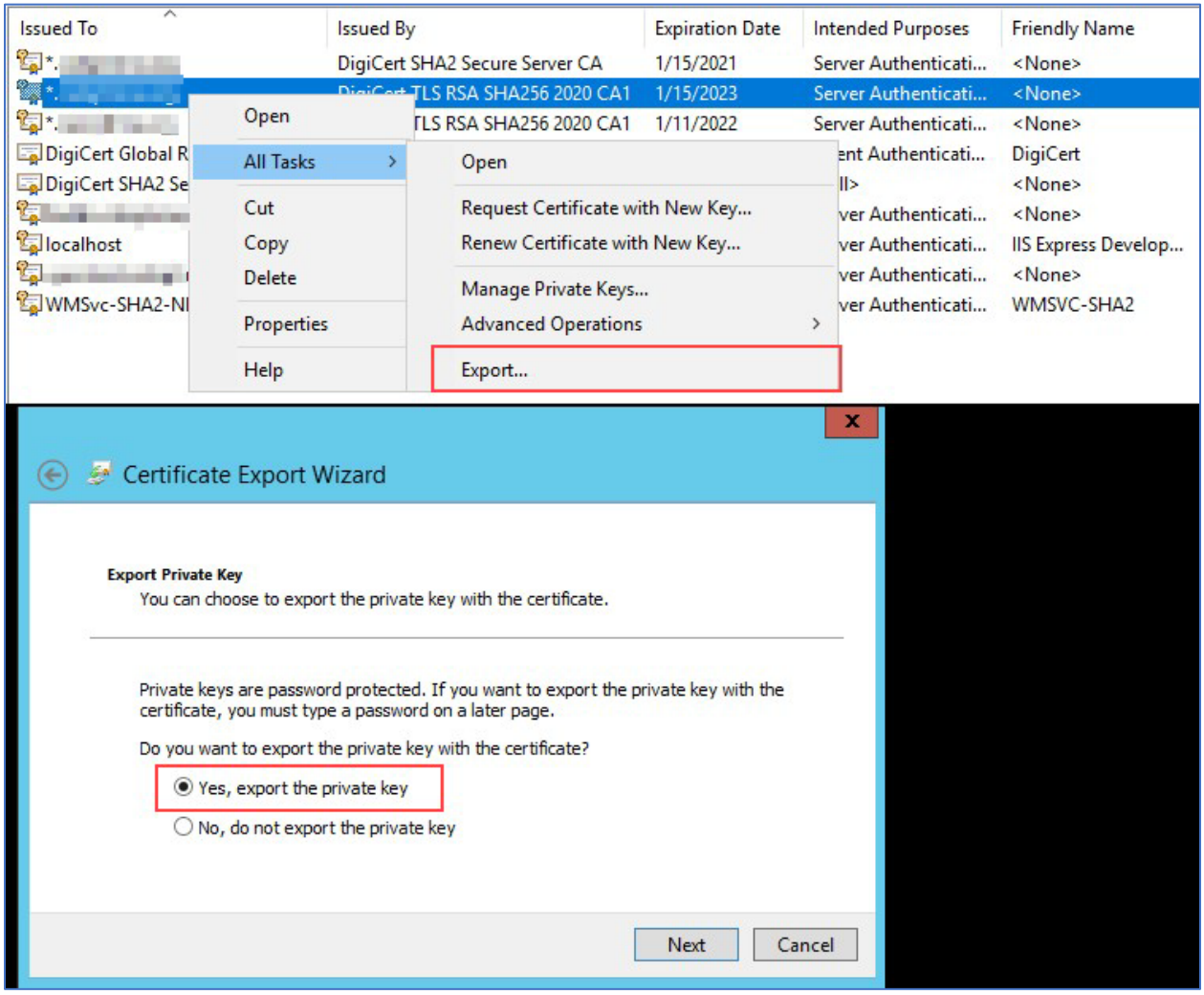
2. Add Certificates for “Computer Account”



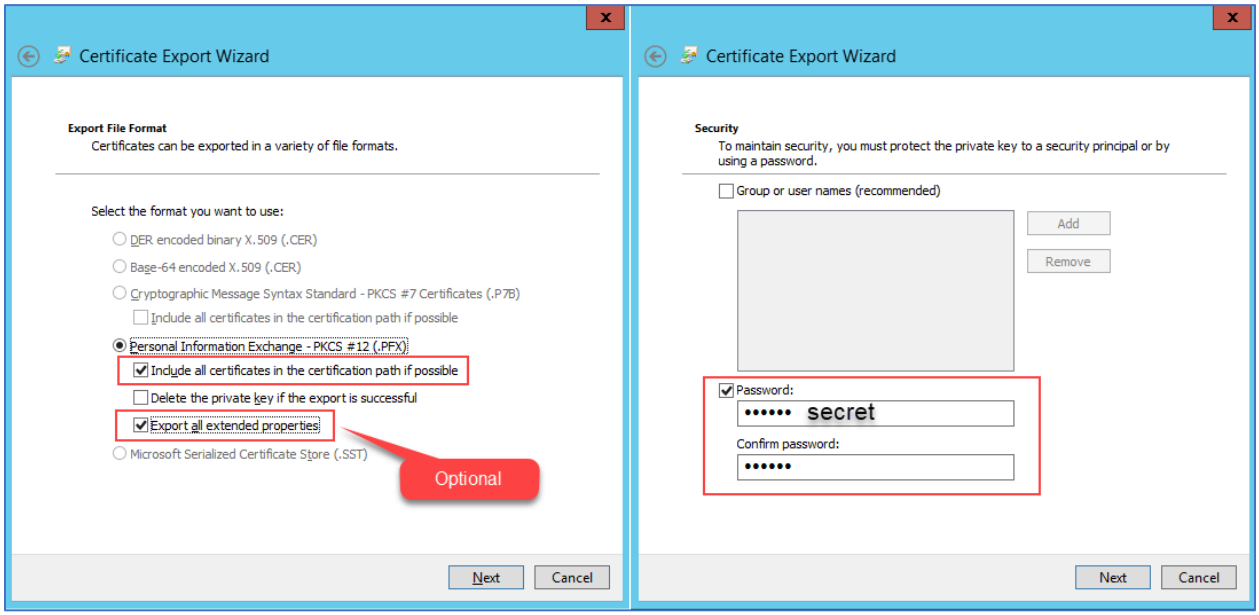
3. Check Right Certificate



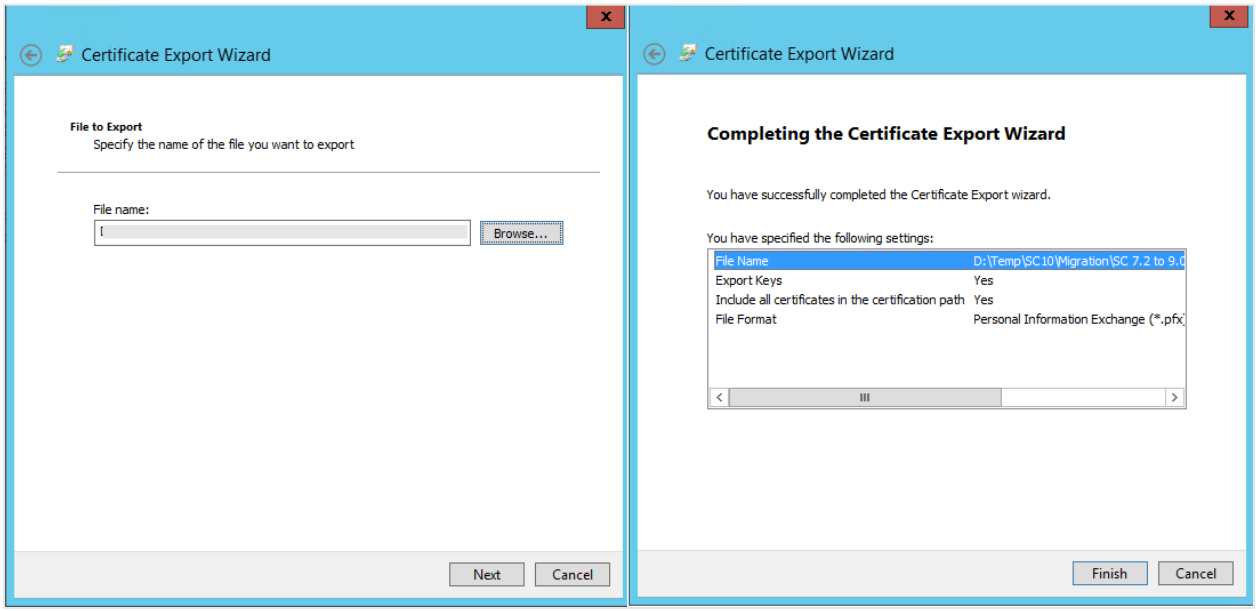
4. Export Private Key



5. Set Password



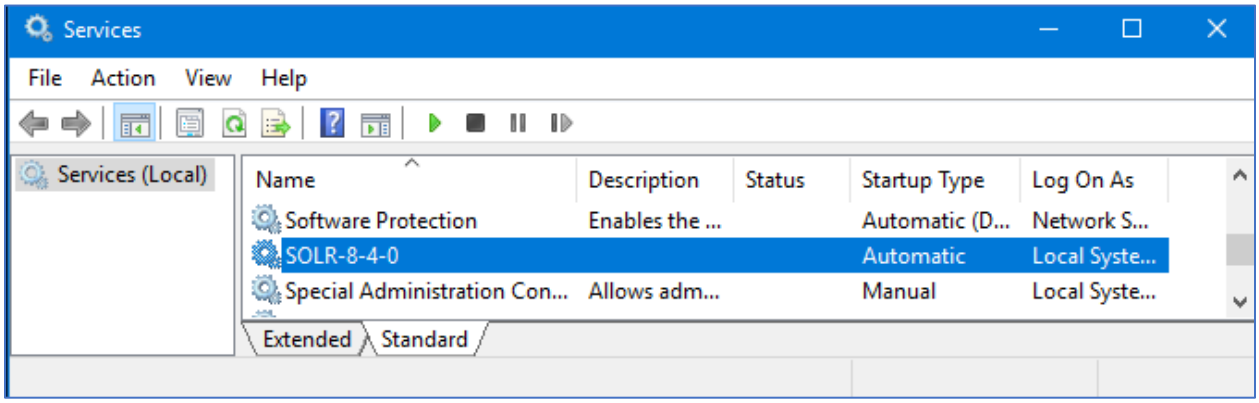
6. Save as pfx file



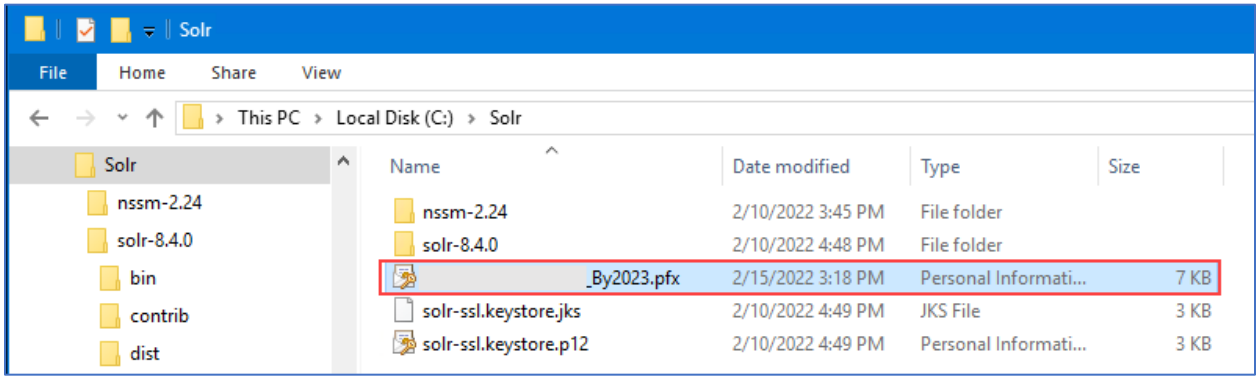
7.

Apply pfx to Solr Service

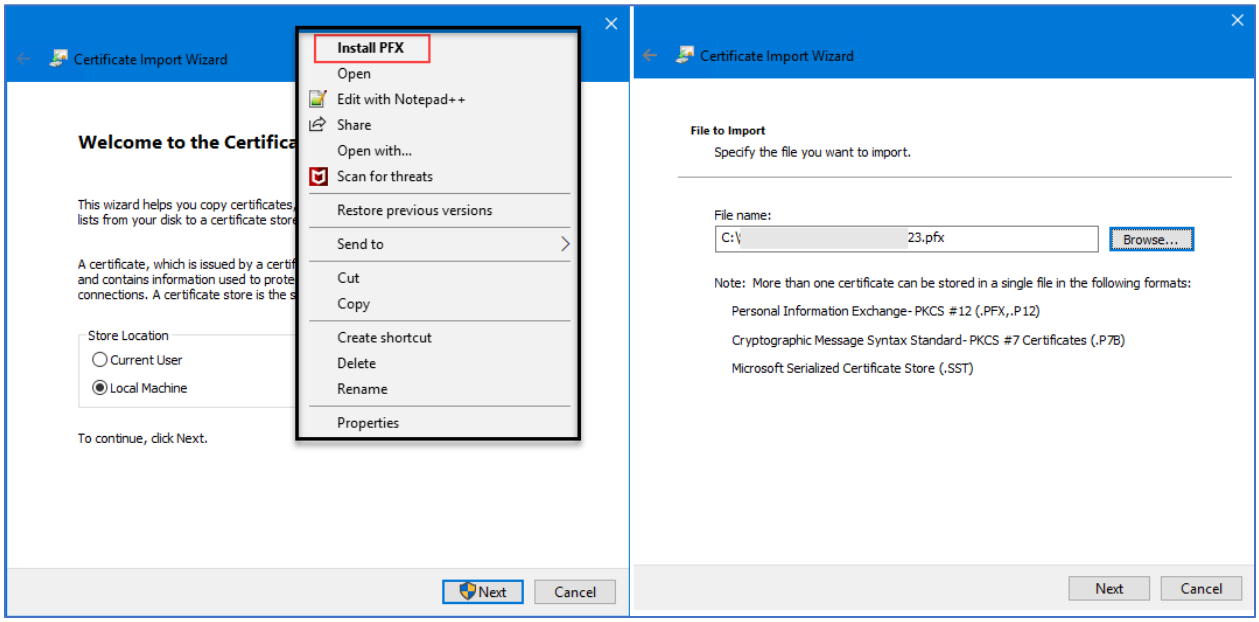
1. Stop Solr Service



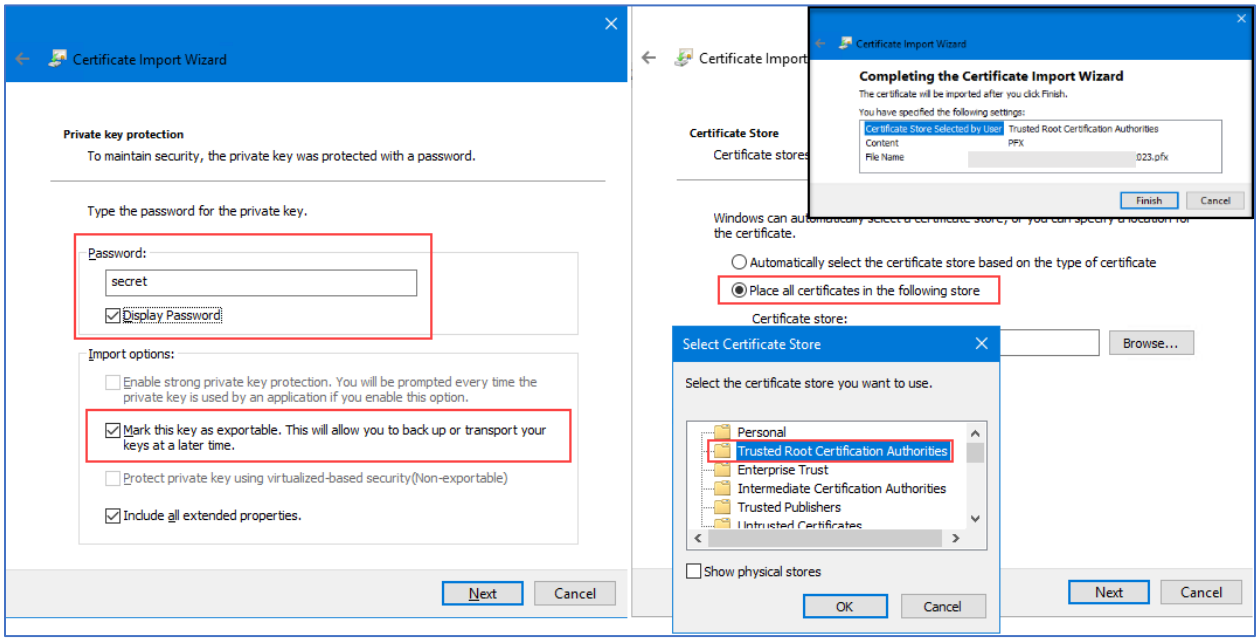
2. Copy file to target folder (Any location is acceptable in this computer)



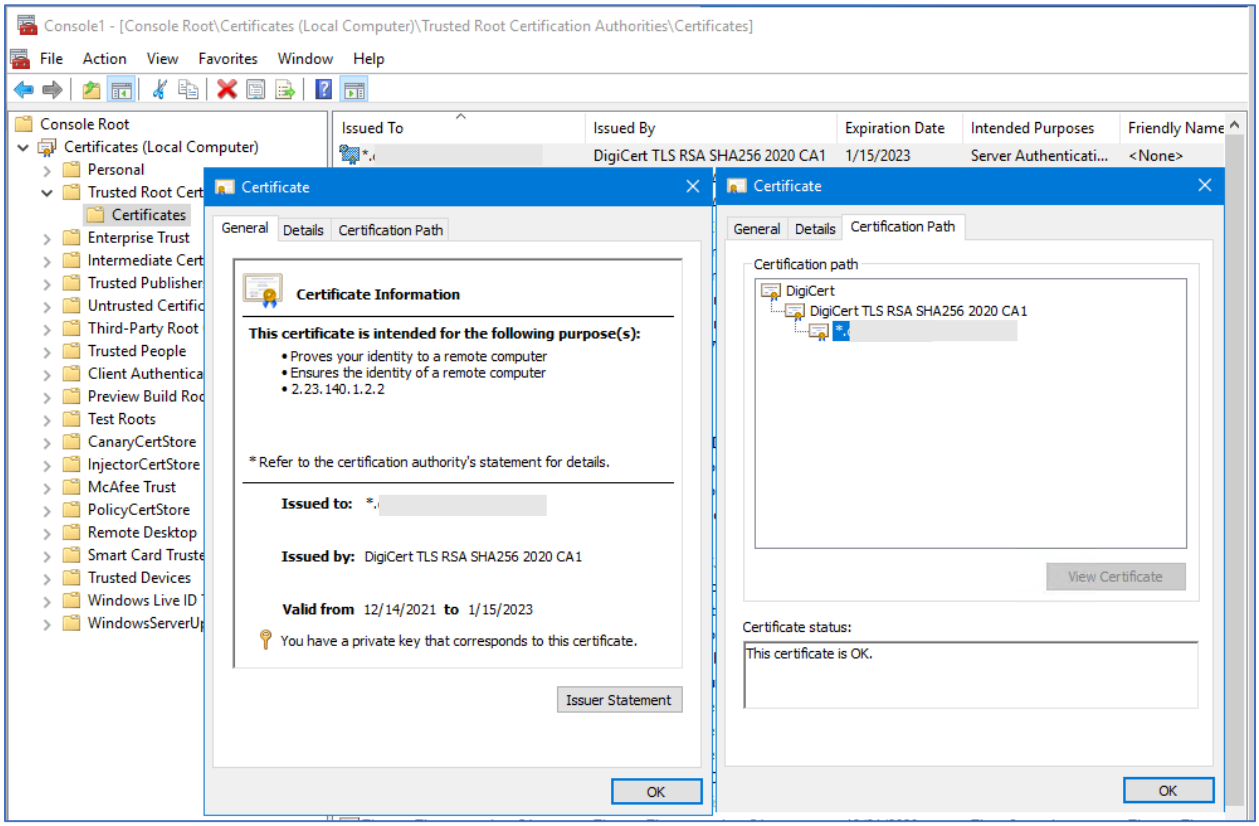
3. Install into Certificates Root Folder



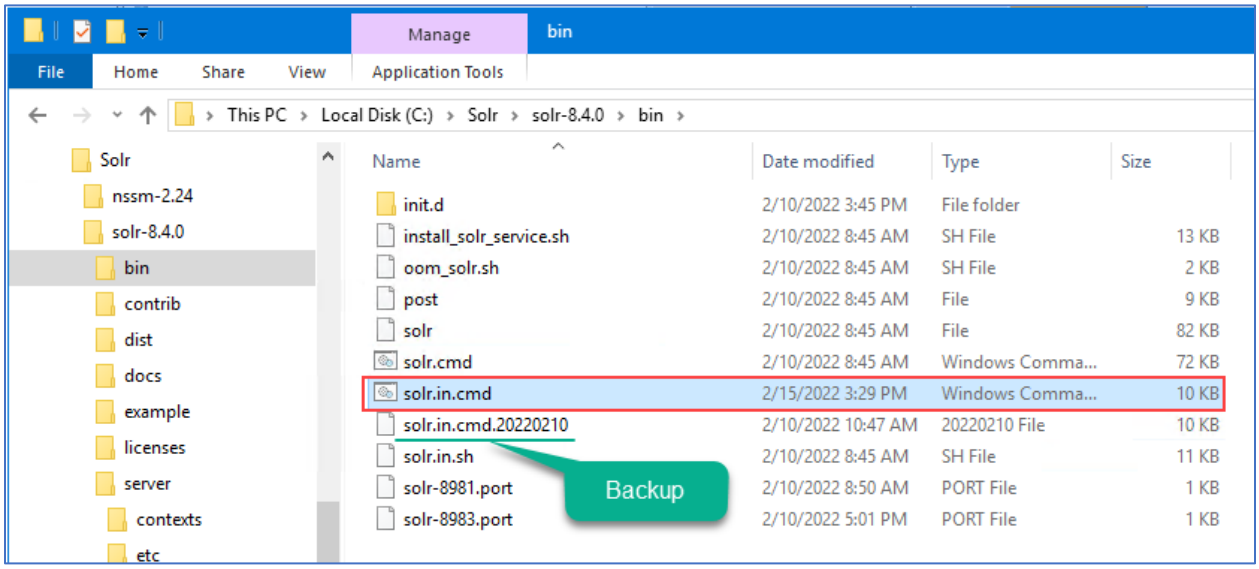
4. Set Password



5. Check Certification



6. Edit solr.in.cmd

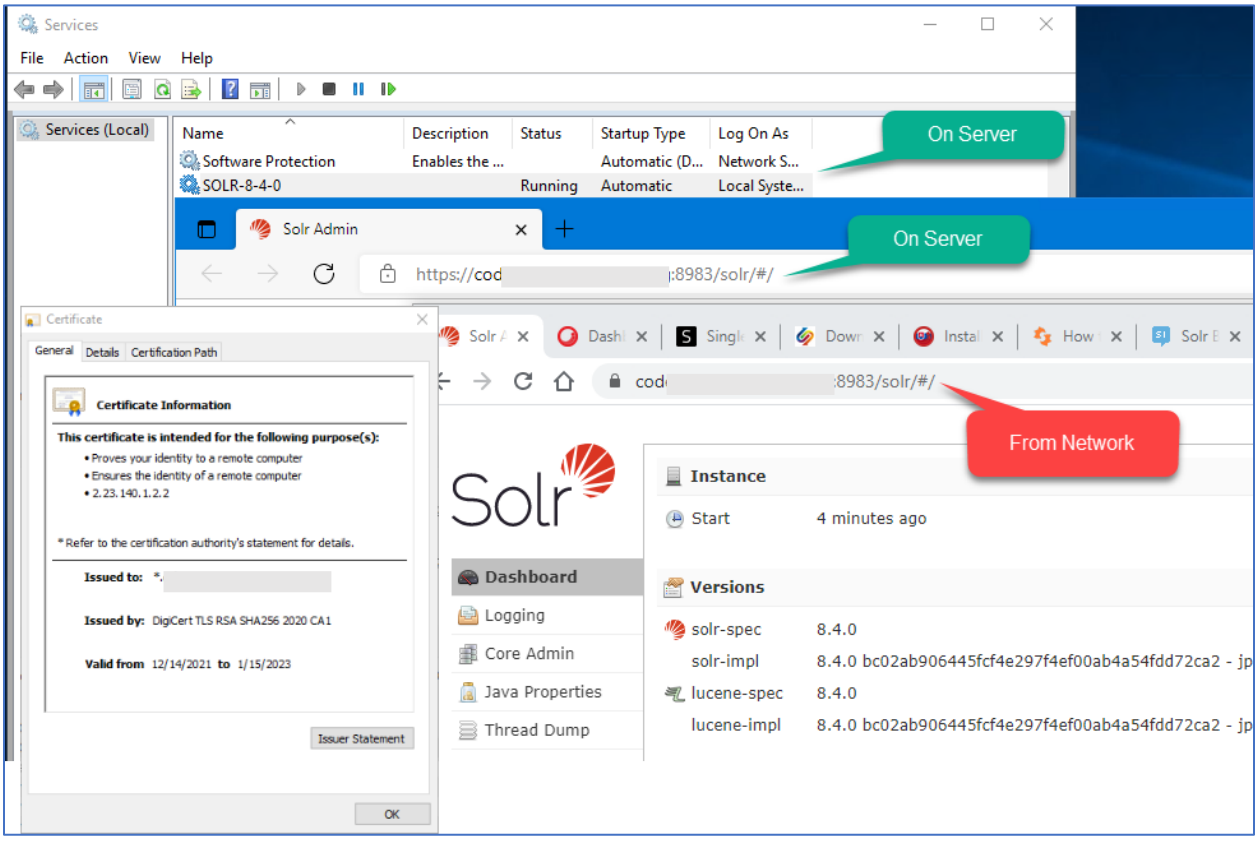


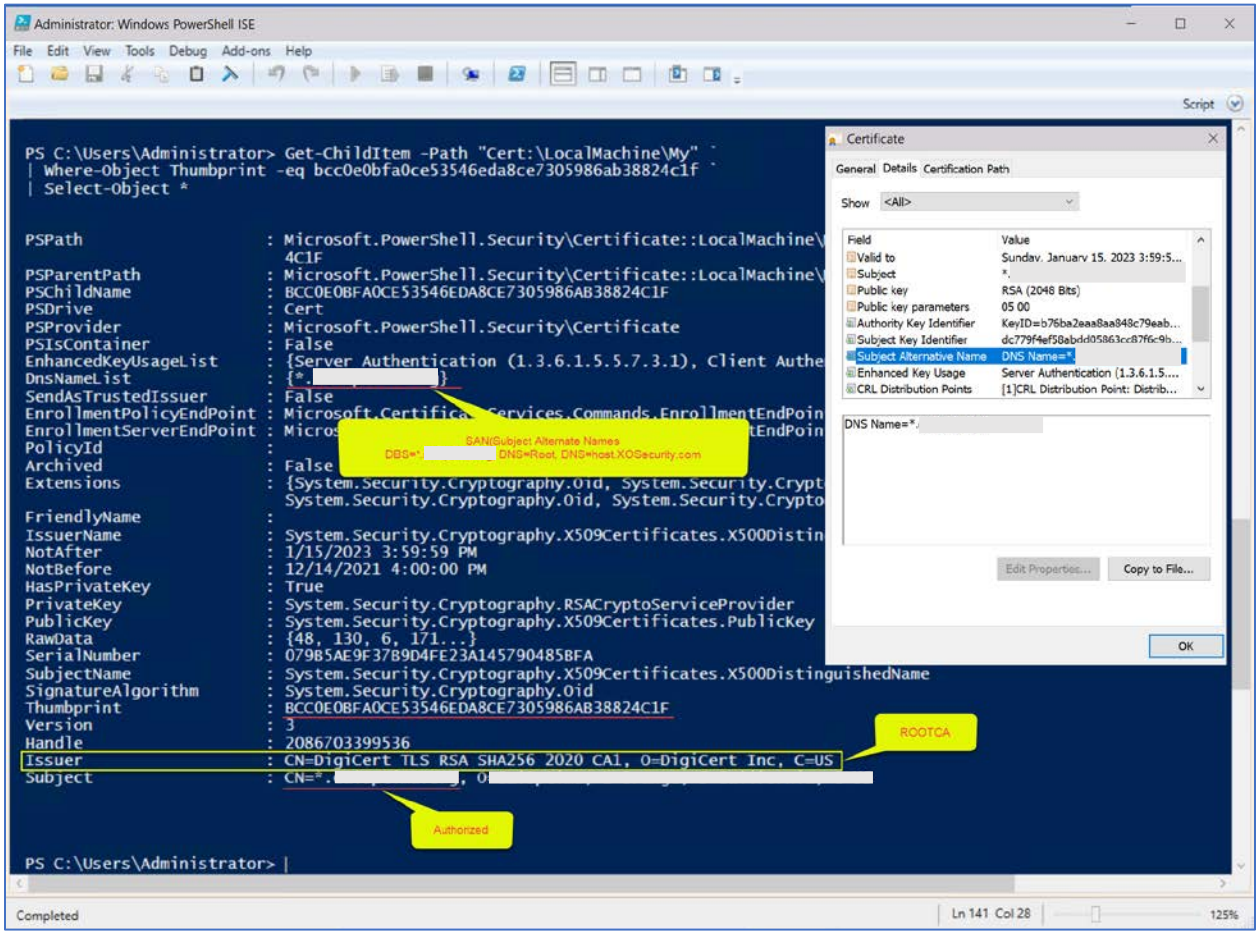
7. Set pfx file location and Store Type

```
REM Sets the port Solr binds to, default is 8983
set SOLR_PORT=8983

REM Enables HTTPS. It is implictly true if you set SOLR_SSL_KEY_STORE. Use this config
REM to enable https module with custom jetty configuration.
set SOLR_SSL_ENABLED=true
REM Uncomment to set SSL-related system properties
REM Be sure to update the paths to the correct keystore for your environment
set SOLR_SSL_KEY_STORE=C:\Solr\                tCA_By2023.pfx
set SOLR_SSL_KEY_STORE_PASSWORD=secret
set SOLR_SSL_TRUST_STORE=C:\Solr\              tCA_By2023.pfx
set SOLR_SSL_TRUST_STORE_PASSWORD=secret
REM Require clients to authenticate
set SOLR_SSL_NEED_CLIENT_AUTH=false
REM Enable clients to authenticate (but not require)
set SOLR_SSL_WANT_CLIENT_AUTH=false
REM Verify client hostname during SSL handshake
set SOLR_SSL_CLIENT_HOSTNAME_VERIFICATION=false
REM SSL Certificates contain host/ip "peer name" information that is validated by defau
REM this to false can be useful to disable these checks when re-using a certificate on
set SOLR_SSL_CHECK_PEER_NAME=true
REM Override Key/Trust Store types if necessary
set SOLR_SSL_KEY_STORE_TYPE=PKCS12
set SOLR_SSL_TRUST_STORE_TYPE=PKCS12
```

8. Restart Solr Service & Check




Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Script
PS C:\Users\Administrator> Get-ChildItem -Path "Cert:\LocalMachine\My"
| Where-Object Thumbprint -eq bcc0e0bfa0ce53546eda8ce7305986ab38824c1f
| Select-Object *
PSPath : Microsoft.PowerShell.Security\Certificate::LocalMachine\My\BCC0E0BFA0CE53546EDA8CE7305986AB38824C1F
PSParentPath : Microsoft.PowerShell.Security\Certificate::LocalMachine\My
PSChildName : BCC0E0BFA0CE53546EDA8CE7305986AB38824C1F
PSDrive : Cert
PSProvider : Microsoft.PowerShell.Security\Certificate
PSIsContainer : False
EnhancedKeyUsageList : {Server Authentication (1.3.6.1.5.5.7.3.1), Client Authe
DnsNameList : {*.
SendAsTrustedIssuer : False
EnrollmentPolicyEndPoint : Microsoft.Certificate Services.Commands.EnrollmentEndPoin
EnrollmentServerEndPoint : Micros tEndPoin
PolicyId :
Archived : False
Extensions : {System.Security.Cryptography.Oid, System.Security.Crypt
System.Security.Cryptography.Oid, System.Security.Crypto
FriendlyName :
IssuerName : System.Security.Cryptography.X509Certificates.X500Distin
NotAfter : 1/15/2023 3:59:59 PM
NotBefore : 12/14/2021 4:00:00 PM
HasPrivateKey : True
PrivateKey : System.Security.Cryptography.RSACryptoServiceProvider
PublicKey : System.Security.Cryptography.X509Certificates.PublicKey
RawData : {48, 130, 6, 171...}
SerialNumber : 079B5AE9F3789D4FE23A145790485BFA
SubjectName : System.Security.Cryptography.X509Certificates.X500DistinguishedName
SignatureAlgorithm : System.Security.Cryptography.Oid
Thumbprint : BCC0E0BFA0CE53546EDA8CE7305986AB38824C1F
Version : 3
Handle : 2086703399536
Issuer : CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US
Subject : CN=*.
SAN(Subject Alternate Names
DNS=*. DNS=Root, DNS=host.XOSecurity.com
ROOTCA
Authorized
PS C:\Users\Administrator>
Certificate
General Details Certification Path
Show <All>
Field Value
Valid to Sunday, January 15, 2023 3:59:5...
Subject *.
Public key RSA (2048 Bits)
Public key parameters 05 00
Authority Key Identifier KeyID=b76ba2eaa8aa848c79eab...
Subject Key Identifier dc779f4ef58abdd05863cc87f6c9b...
Subject Alternative Name DNS Name=*.
Enhanced Key Usage Server Authentication (1.3.6.1.5....
CRL Distribution Points [1]CRL Distribution Point: Distrib...
DNS Name=*.
Edit Properties... Copy to File...
OK
Completed
Ln 141 Col 28
125%