

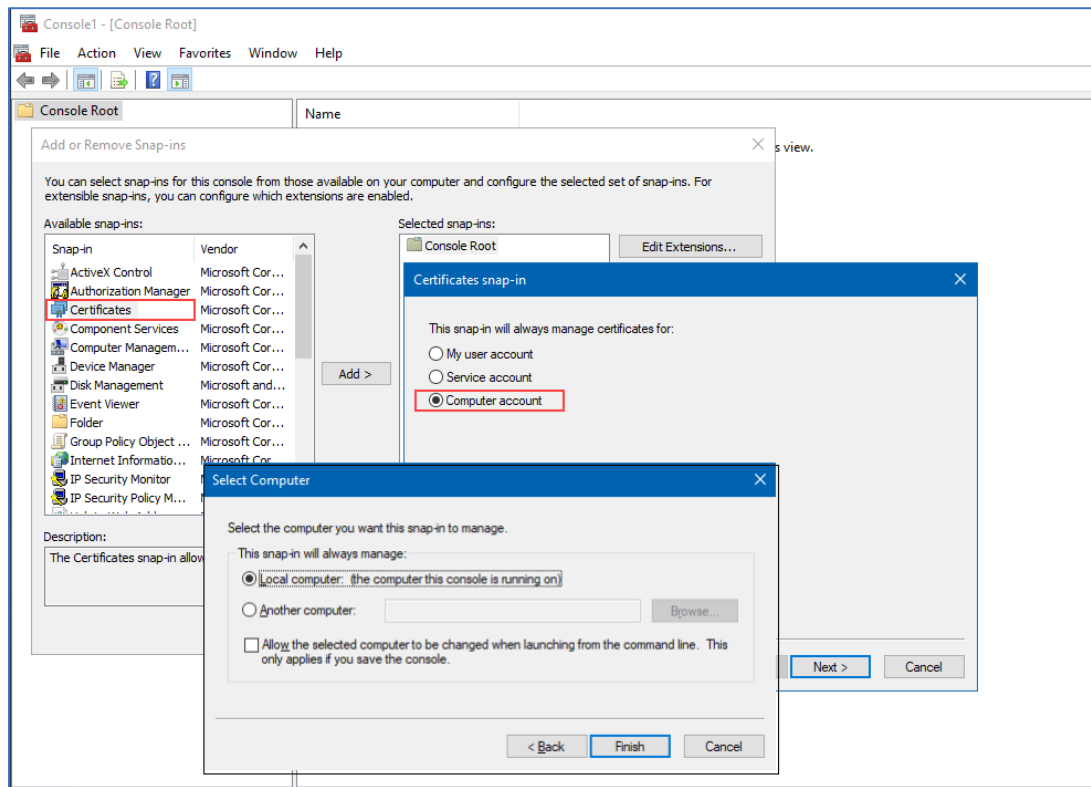
Implement Solr Certificates with XOSecurity RootCA

- 1. Create pfx file from XOSecurity Certificate**
- 2. Apply pfx to Solr Service**

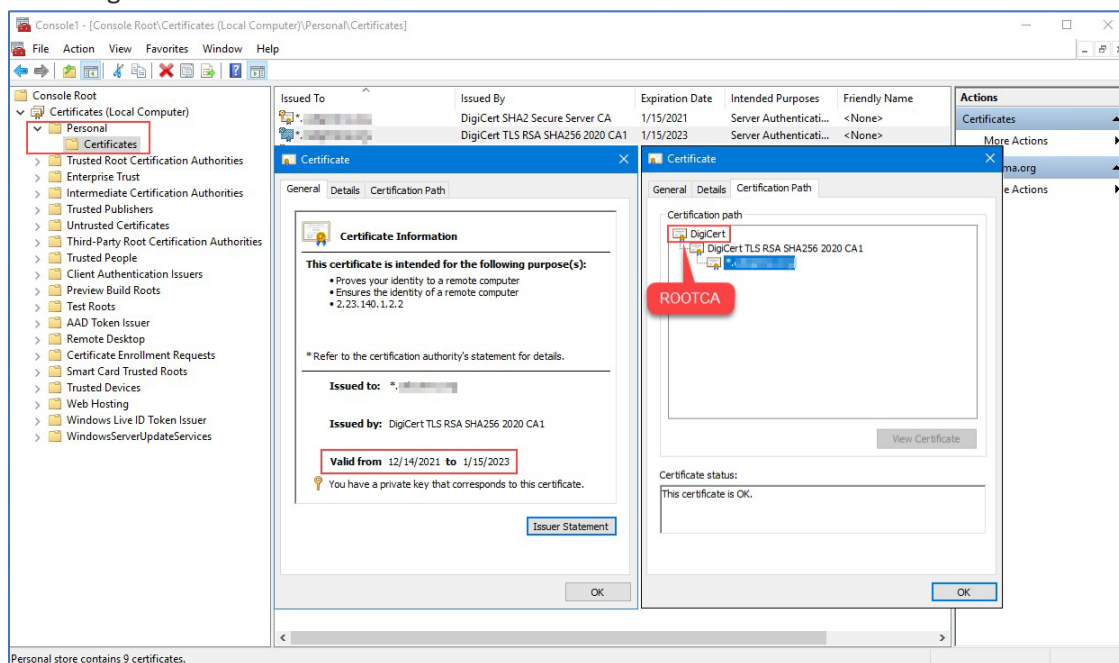
Implement Solr Certificates with XOSecurity RootCA

Create pfx file from XOSecurity Certificate

1. Open MMC
2. Add Certificates for “Computer Account”

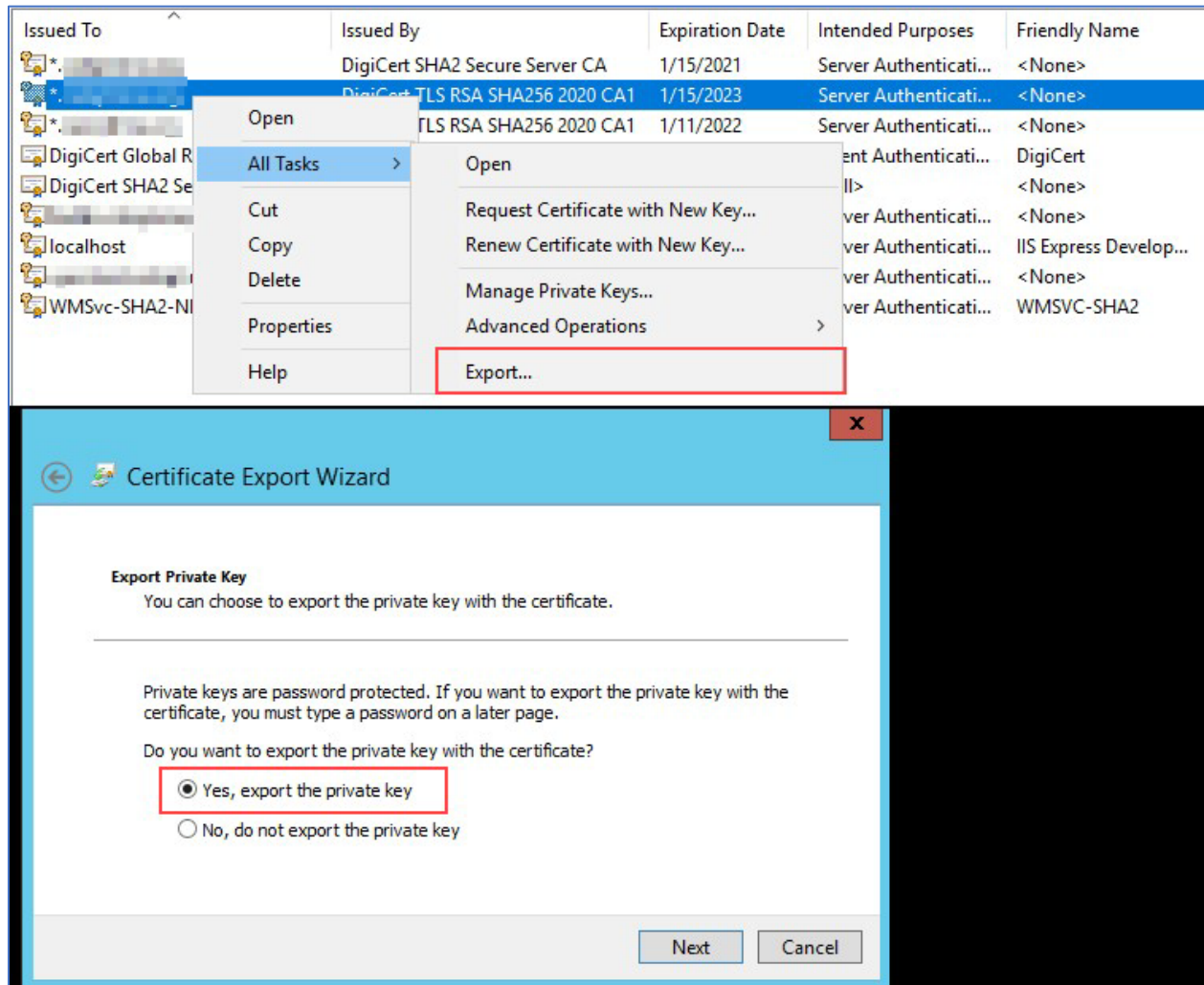


3. Check Right Certificate

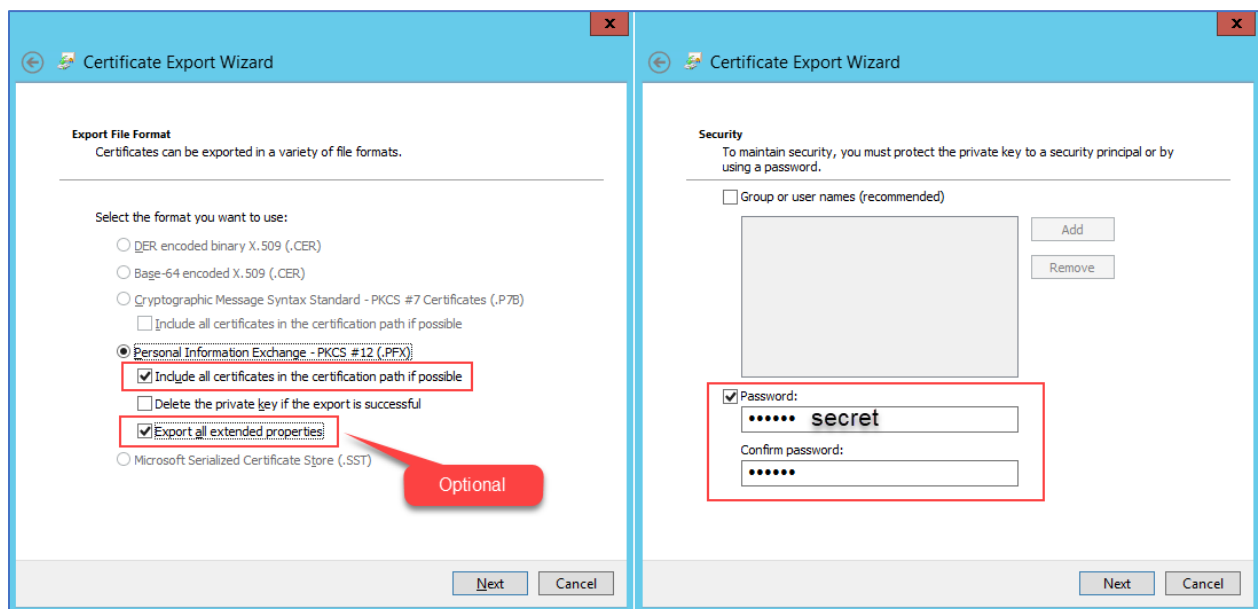


Implement Solr Certificates with XOSecurity RootCA

4. Export Private Key

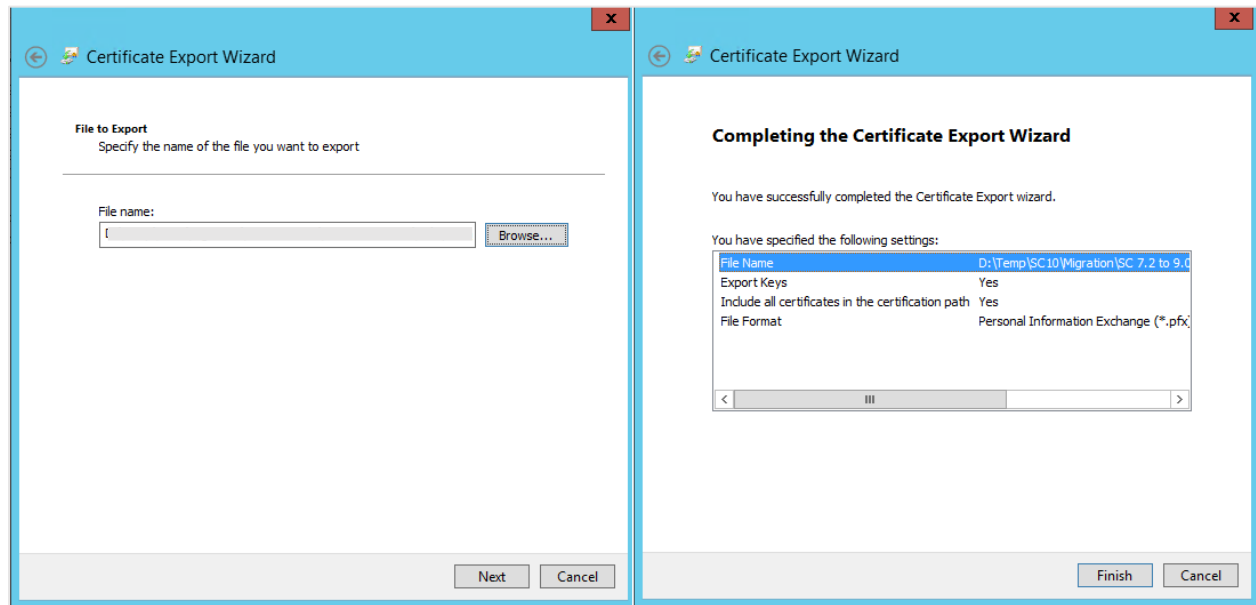


5. Set Password



Implement Solr Certificates with XOSecurity RootCA

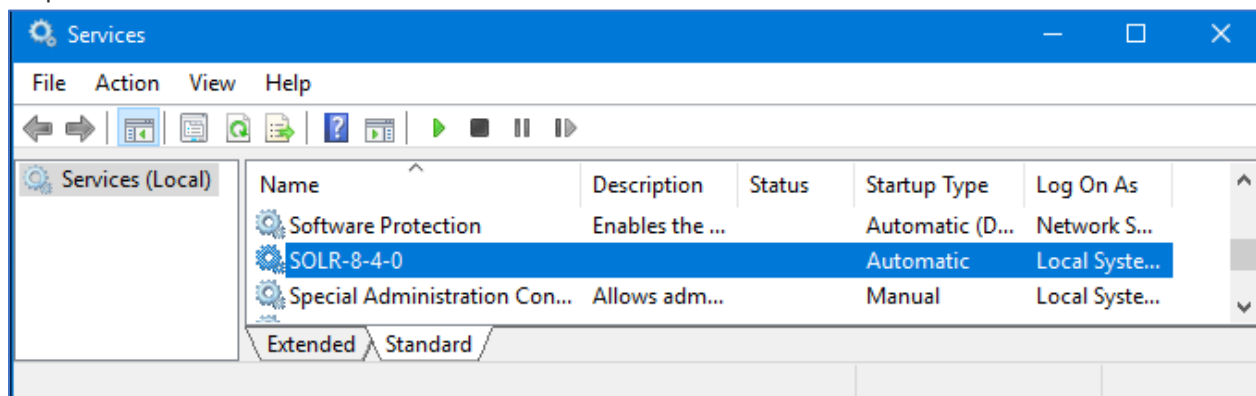
6. Save as pfx file



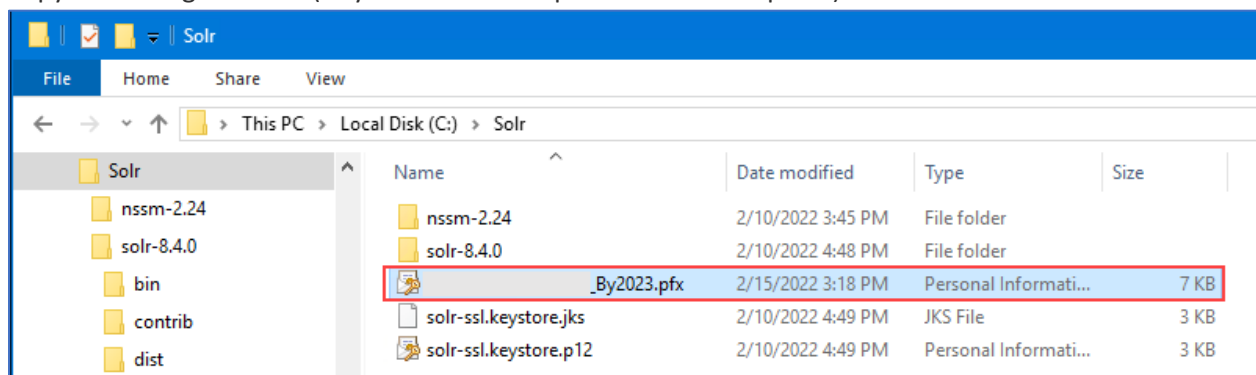
7.

Apply pfx to Solr Service

1. Stop Solr Service

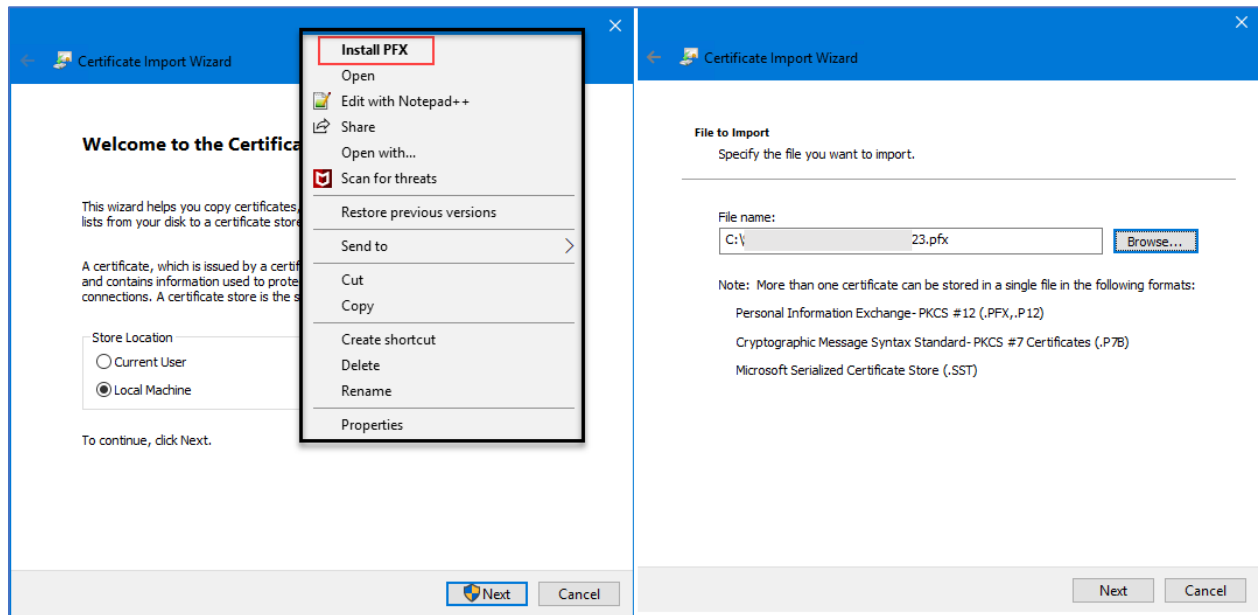


2. Copy file to target folder (Any location is acceptable in this computer)

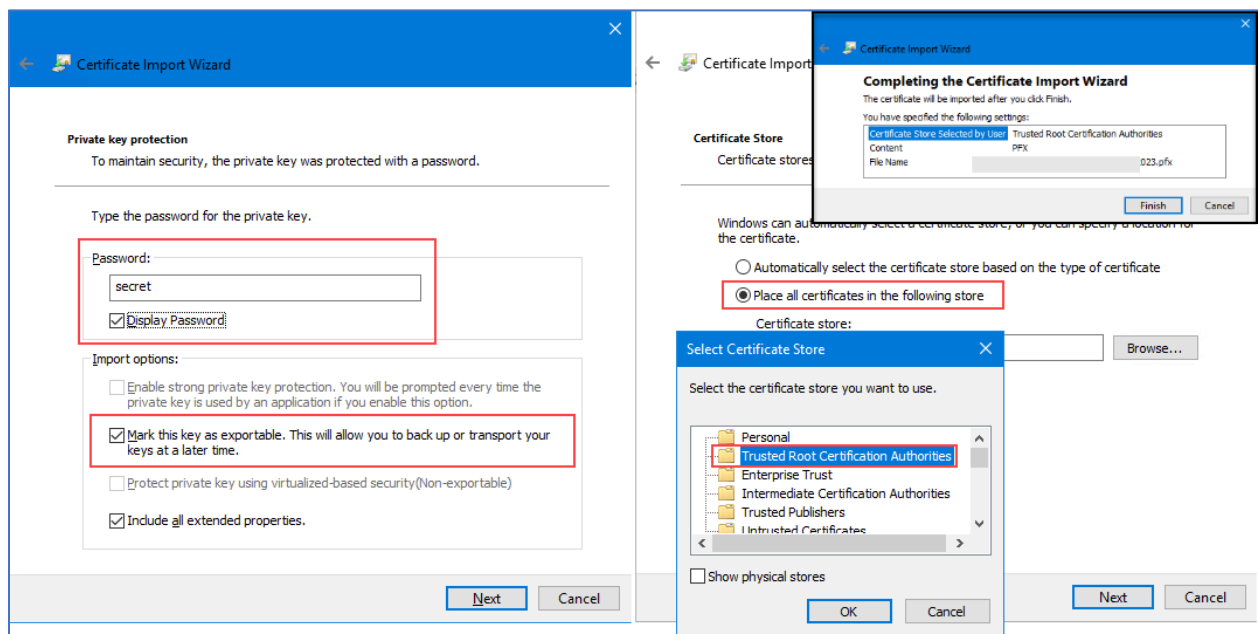


Implement Solr Certificates with XOSecurity RootCA

3. Install into Certificates Root Folder

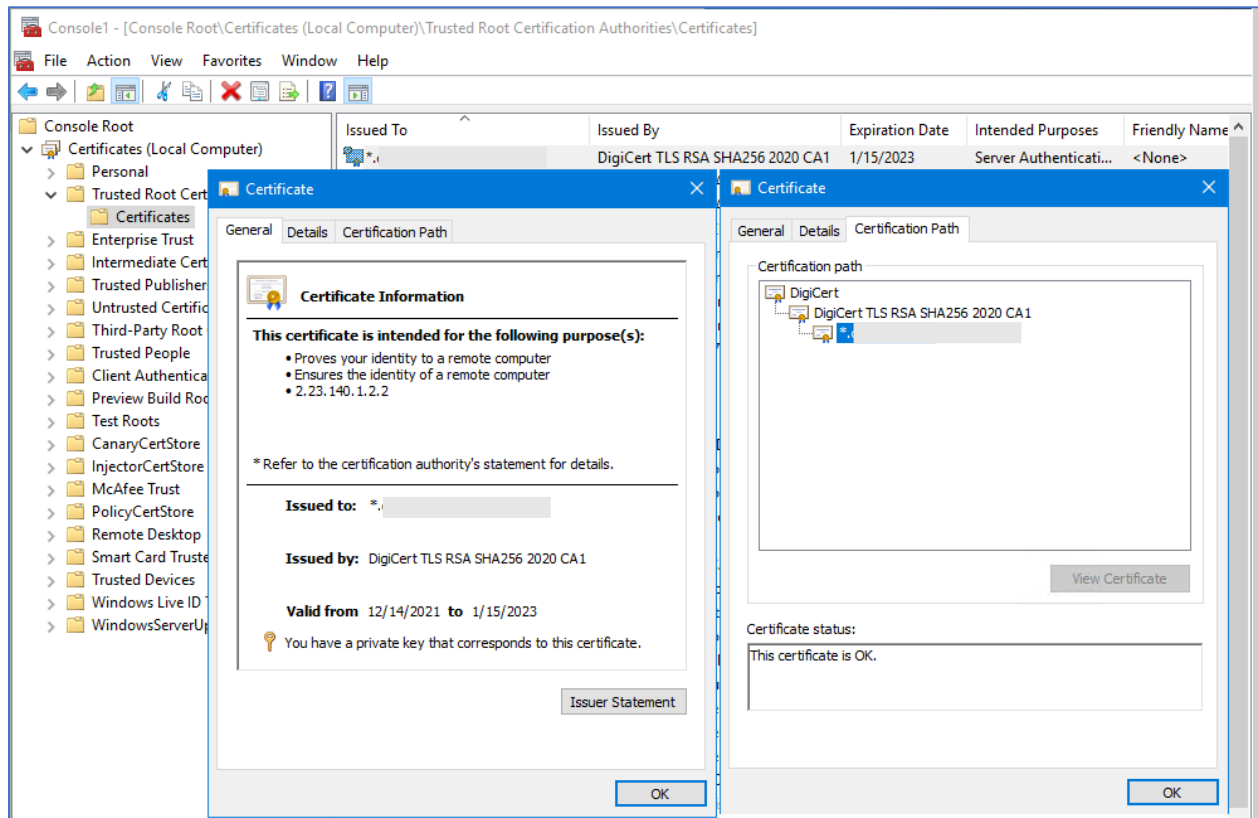


4. Set Password

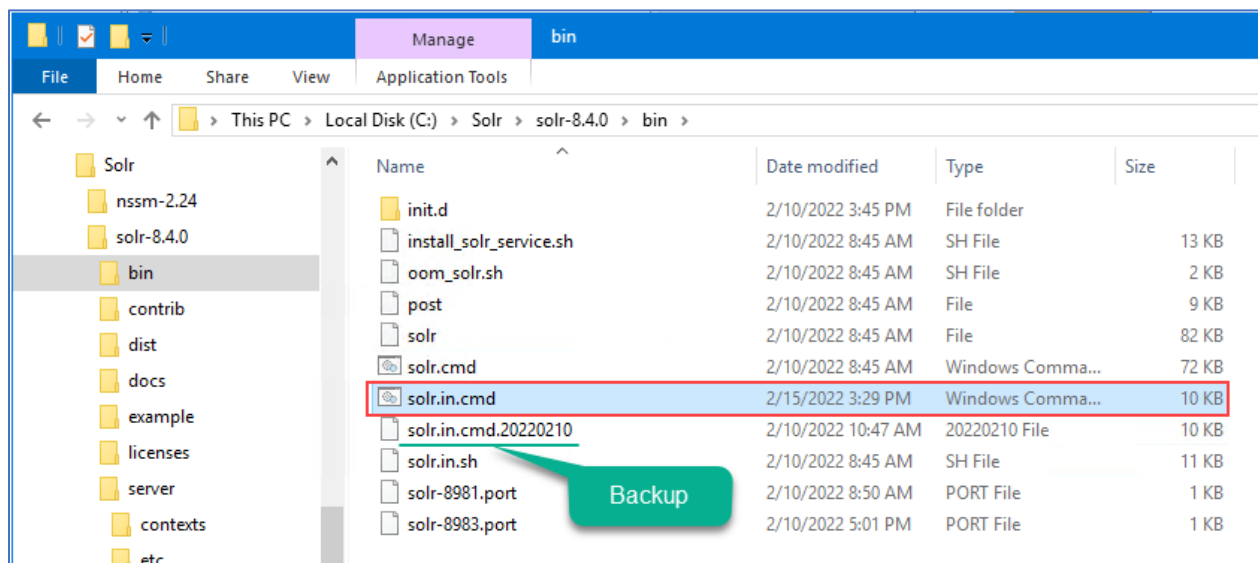


Implement Solr Certificates with XOSecurity RootCA

5. Check Certification



6. Edit solr.in.cmd



Implement Solr Certificates with XOSecurity RootCA

7. Set pfx file location and Store Type

```
109 REM Sets the port Solr binds to, default is 8983
110 set SOLR_PORT=8983
111
112 REM Enables HTTPS. It is implicitly true if you set SOLR_SSL_KEY_STORE. Use this config
113 REM to enable https module with custom jetty configuration.
114 set SOLR_SSL_ENABLED=true
115 REM Uncomment to set SSL-related system properties
116 REM Be sure to update the paths to the correct keystore for your environment
117 set SOLR_SSL_KEY_STORE=C:\Solr\(\ )tCA_By2023.pfx
118 set SOLR_SSL_KEY_STORE_PASSWORD=secret
119 set SOLR_SSL_TRUST_STORE=C:\Solr\(\ )tCA_By2023.pfx
120 set SOLR_SSL_TRUST_STORE_PASSWORD=secret
121 REM Require clients to authenticate
122 set SOLR_SSL_NEED_CLIENT_AUTH=false
123 REM Enable clients to authenticate (but not require)
124 set SOLR_SSL_WANT_CLIENT_AUTH=false
125 REM Verify client hostname during SSL handshake
126 set SOLR_SSL_CLIENT_HOSTNAME_VERIFICATION=false
127 REM SSL Certificates contain host/ip "peer name" information that is validated by default
128 REM this to false can be useful to disable these checks when re-using a certificate on
129 set SOLR_SSL_CHECK_PEER_NAME=true
130 REM Override Key/Trust Store types if necessary
131 set SOLR_SSL_KEY_STORE_TYPE=PKCS12
132 set SOLR_SSL_TRUST_STORE_TYPE=PKCS12
```

8. Restart Solr Service & Check

The screenshot shows the Windows Services console with the 'SOLR-8-4-0' service running. Below it, the Solr Admin web interface is open in a browser at <https://localhost:8983/solr/#/>. A 'Certificate Information' dialog box is also open, showing details for a certificate issued by 'DigCert TLS RSA SHA256 2020 CA1'.

Services (Local)

Name	Description	Status	Startup Type	Log On As
Software Protection	Enables the ...	Running	Automatic (D...	Network S...
SOLR-8-4-0		Running	Automatic	Local Syste...

Solr Admin

https://localhost:8983/solr/#/

Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.23.140.1.2.2

* Refer to the certification authority's statement for details.

Issued to: *

Issued by: DigCert TLS RSA SHA256 2020 CA1

Valid from: 12/14/2021 to 1/15/2023

Issuer Statement

OK

Implement Solr Certificates with XOSecurity RootCA

The screenshot displays a Windows PowerShell ISE window with the following commands and output:

```
PS C:\Users\Administrator> Get-ChildItem -Path "Cert:\LocalMachine\My" -Where-Object Thumbprint -eq bcc0e0bfa0ce53546eda8ce7305986ab38824c1f | Select-Object *
```

The output lists various properties of the certificate, including:

- PSPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My\4C1F
- PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My
- PSChildName: BCC0E0BFA0CE53546EDA8CE7305986AB38824C1F
- PSDrive: Cert
- PSProvider: Microsoft.PowerShell.Security\Certificate
- PSIsContainer: False
- EnhancedKeyUsageList: {Server Authentication (1.3.6.1.5.7.3.1), Client Authentication (1.3.6.1.5.7.3.2)}
- DnsNameList: {*}
- SendAsTrustedIssuer: False
- EnrollmentPolicyEndPoint: Microsoft.CertificateServices.Commands.EnrollmentEndpoint
- EnrollmentServerEndPoint: Microsoft.CertificateServices.Commands.EnrollmentEndpoint
- PolicyId: 00000000-0000-0000-0000-000000000000
- Archived: False
- Extensions: {System.Security.Cryptography.Oid, System.Security.Cryptography.Oid, System.Security.Cryptography.Oid, System.Security.Cryptography.Oid}
- FriendlyName:
- IssuerName: System.Security.Cryptography.X509Certificates.X500DistinguishedName
- 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: 07985AE9F3789D4FE23A145790485BFA
- 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=*, O=*

The Certificate Properties dialog box is open, showing the following details:

- Field: Valid to, Value: Sunday, January 15, 2023 3:59:59 PM
- Field: Subject, Value: *
- Field: Public key, Value: RSA (2048 Bits)
- Field: Public key parameters, Value: 05 00
- Field: Authority Key Identifier, Value: KeyID=b76ba2aaa8aa948c79eab...
- Field: Subject Key Identifier, Value: dc779f4ef58abd05863cc87f6c9b...
- Field: Subject Alternative Name, Value: DNS Name=*
- Field: Enhanced Key Usage, Value: Server Authentication (1.3.6.1.5.7.3.1), Client Authentication (1.3.6.1.5.7.3.2)
- Field: CRL Distribution Points, Value: [1]CRL Distribution Point: Distrib...

Yellow callouts highlight the following information:

- "Authorized" pointing to the Subject field in the PowerShell output.
- "ROOTCA" pointing to the Issuer field in the PowerShell output.
- A yellow box containing the text: SAN: Subject: Alternate Names, DNS=*, DNS=Root, DNS=host.XOSecurity.com