PureConnect®

2022 R2

Generated:

27-July-2022

Content last updated:

See Change Log for summary of changes.

GENESYS™

SSO, SA, and Certificate Improvements

User's Guide

Abstract

This document describes how to implement and configure SA and SSO with respect to improvements in Third party certificates, which allows secure connection to Interaction Connect.

For the latest version of this document, see the PureConnect Documentation Library at: http://help.genesys.com/pureconnect.

For copyright and trademark information, see https://help.genesys.com/pureconnect/desktop/copyright_and_trademark_information.htm.

Table of Contents

Introduction to SA, SSO, and Third-Party Certificates

The SA, SSO and CI technical reference is for technical and management staff who need an overview of communication with IC with respect to Single Sign On using Third-party certificates instead of CIC certificates for secure communication.

SA is used to configure CIC Server in a new installation and to configure and install the certificates.

Single Sign-On is an industry term for using one instance of user identity authentication across multiple applications and systems. SAML SSO works by transferring the user's identity from one place (the identity provider) to another (the service provider). This is done through an exchange of digitally signed XML documents.

The third-party certificates ensures that the corporate data is encrypted in such a way, that only the recipient who owns the certificate can decrypt it.

CIC provides many options to allow administrators to choose a necessary security level that is appropriate for each environment in which IC resides. IC enables many Pureconnect Security Features by default while other security features require licensing. Administrators enable and configure those features through one or more CIC applications.

All components of an IC System use asymmetric Public-Key cryptography and a form of Public-Key Infrastructure (PKI) with certificates to validate every connection between them. CIC Subsystems, such as Interaction Media Server, Session Manager, and Interaction SIP Proxy, use this security schema to validate connections with other subsystems, CIC client applications, and the IC server. The IC System validates most of these connections automatically without visual notifications and requires little to no configuration efforts by an administrator.

Certificates Overview

Digital certificates show that devices, organizations, and people are who they say they are. No security measure is fool proof, but digital certificates provide a reliable way to stop unauthorized access to computer devices and networks.

- Digital signatures use identity certificates to combine your public key with other identifying information for your authentication.
- Certificates contain a public key and information about the owner of the public key.
- Certificates bind the public key to a distinguished name, MAC address, e-mail address, or alternative name.
- A Certificate Authority (CA) validates (signs) the contents of a certificate.
- Validation hashes the data in the certificate and signs it with the CA private key.
- The CA public key is available for consumers of the certificate to validate its authenticity.
- CIC generates or obtains the most standard certificates automatically.
- TLS allows authenticated, encrypted communication between parties previously unknown to each other. Public key cryptography facilitates this process using certificates. When a 'client' (any application, local or remote server process that connects to the CIC Server) starts TLS communication with a server, it follows a handshaking process.
- The client sends a request for TLS communication to the server.
- The server responds by providing its digital certificate to the client and (optionally) requesting a certificate from the client for client authentication.
- The client validates the certificate by using the server certificate CA public key.
- If a certificate of the server is valid, the client then creates a master secret key for use in future communication. It encrypts the key with the public key of the server (from a certificate of the server) and transmits it to the server.
- If the server requested client authentication, the client also includes its own digital certificate.
- If the client transmitted a certificate, the server verifies the identity of the client using the CA client certificate's public key.
- Client and server both use the master secret key to generate the symmetric session keys.
- All future communication takes place using symmetric encryption.
- During the initial steps of the handshaking process, the client and server also negotiate the exact cryptographic algorithms to secure the session.

Certificates usage in IC

CIC uses the following certificate types, each for a different purpose:

- Subsystem certificates: Validate data connections using TLS between local and remote CIC Subsystems and the CIC Server, and CIC application connections to the CIC Server.
- Line certificates: Validate SIP connections using TLS between CIC and SIP devices.
- E-mail certificates: There are two types of e-mail certificates. One type uses SSL/TLS to validate e-mail transmissions between the CIC Server and the e-mail server. The other type uses S/MIME to secure e-mail between individual e-mail senders and receivers. You can use one or both types.
- Web Server certificates: Validates that apps (such as iPad Supervisor) have connected to the web server on a trusted CIC Server

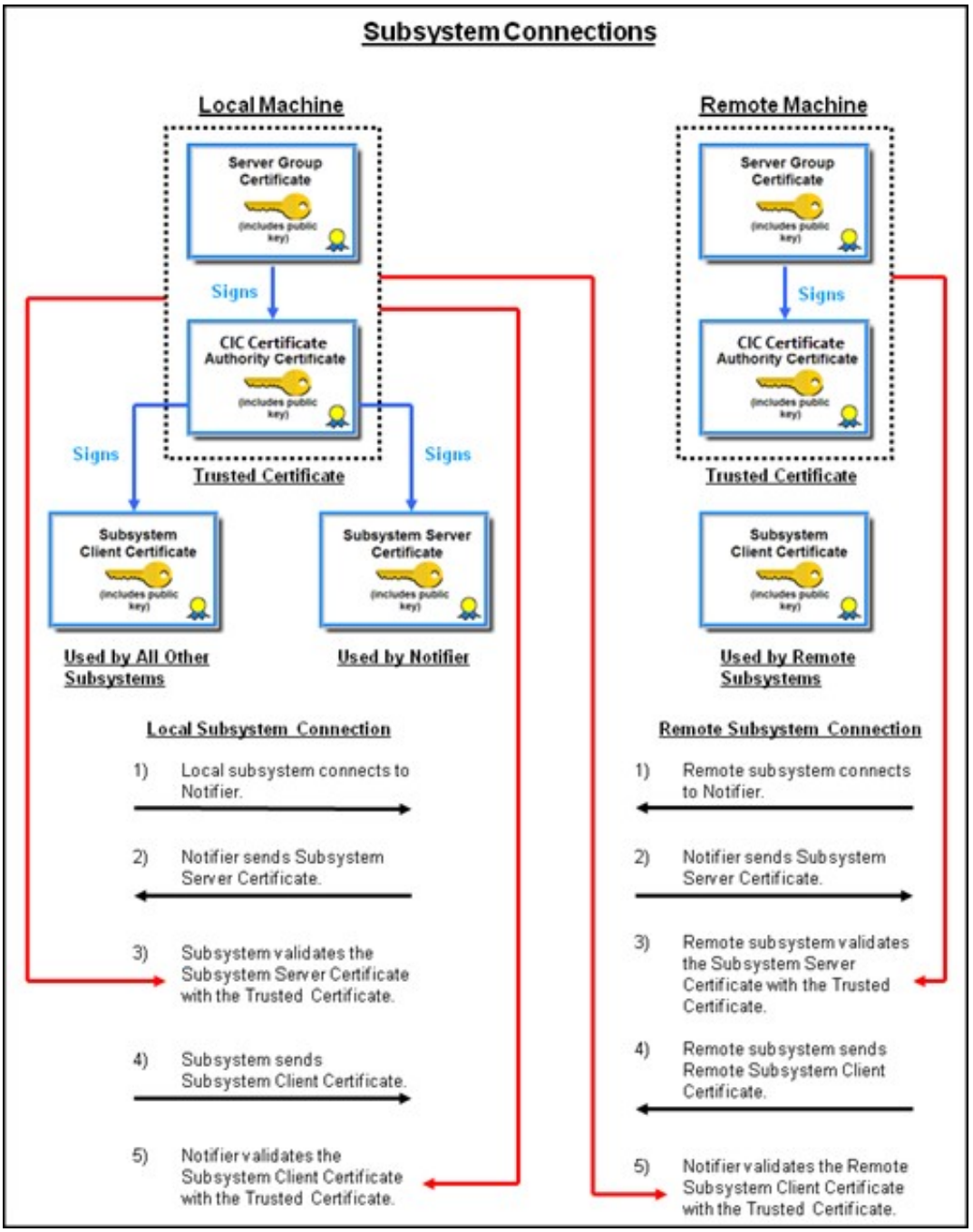
IC Subsystem Certificates

Genesys is the authority behind the certificates installed by default with CIC. If you use the provided subsystem certificates, they require little configuration. If you choose to use your certificate authority (CA), it requires extra configuration.

- CIC Servers automatically use TLS protocol-enabled connections and public/private key certificates for communication with remote subsystems. For example, communications between CIC Servers, Interaction Media Servers, and ASR servers all use secure, encrypted TLS connections with digitally signed certificates for secure validation between them.
- These certificates should be trusted in IA for communication.
- Genesys installs its server group (root) certificate authority that issues certificates to all authorized remote connections and applications.
- Switchover Server pairs must use the same server group (root) certificate and private key so remote connections can have immediate access to both the primary and backup servers.
- Multi-site CIC Servers that do not share common subsystems each have their server group (root) certificate to issue private keys to the local subsystems at each site.

Subsystem certificate generation

The IC installation program and Setup Assistant generate all of the needed IC subsystem, server, client, and line certificates when you use the CIC System as the certificate authority. The certificates are unique to each IC Server. Switchover servers must share a server group, certificates, and private keys. When configuring the backup server in a switchover pair, safely copy the server group certificates and private key from one server to another.



CIC subsystem certificate files

The default CIC certificates are generated and stored under the \I3\IC\Certificates folder on the CIC Server. Each type of certificate is stored in the appropriately named subfolder. The following table contains a summary of the CIC Server's subsystem and application certificates along with their public/private keys.

Subfolder Under \I3\IC\Certificates and Subsystem Certificate Files	Description
\ServerGroup	
ServerGroupCertificate.cer	The server group certificate authority is the root of the trust chain, and it issues the CIC Certificate Authority (CA) certificates
ServerGroupPrivateKey.bin	The server group private key (most important to protect this file).
ServerGroupPublicKey.bin	The server group public key.
\ICCertificateAuthority	
<icserver>_ICCertficateAuthorityCertificate.cer	The CIC Server Certificate Authority (CA) issues all other CIC subsystem certificates.
<icserver>_ICCertficateAuthorityPrivateKey.bin	The CA private key (protect this file)!
<icserver>_ICCertficateAuthorityPublicKey.bin	The CA public key
\Client\Local_Subsystem	
<icserver>_ServerCertificate.cer	The server certificate the CIC Server uses in the mutual authentication of a subsystem or client application
<icserver>_ServerPrivateKey.bin	The server private key
<icserver>_ServerPublicKey.bin	The server public key
<icserver>_ClientCertificate.cer	Use the client certificate for the mutual authentication of a local subsystem.
<icserver>_ClientPrivateKey.bin	The client's private key
<icserver>_ClientPublicKey.bin	The client's public key
<icserver>_TrustedCertificate.cer	Use the CIC Server trusted certificate to validate both the <icserver>_ClientCertificate.cer and the <icserver>_ServerCertificate.cer.
\Client\Remote_Subsystem\<icserver2>*	
<icserver>_ClientCertificate.cer	The client certificate enabling <icserver> to connect to <icserver2>
<icserver>_ClientPrivateKey.bin	The client's private key
<icserver>_ClientPublicKey.bin	The client's public key
<icserver>_TrustedCertificate.cer	The trusted certificate is used to validate the certificate from <icserver2>.
\Client\Remote_Client\<icserver>	
<icserver>_TrustedCertificate.cer	The trusted certificate is used to authenticate remote CIC Servers for local client applications. It uses this certificate to validate the certificate from the remote CIC Server. In a SwitchoverServer pair, there are two <icserver> folders named for each CIC Server in the pair.

Certificate map file

The <icserver>_ININ_Certificates.xml file in the \I3\IC\certificates directory on the CIC Server contains a map of all the subsystem and client certificates created on the server. It does not include the SIP line certificates. For example:

```
- <ININCertificates>
  - <Notifiers>
    - <ServerGroupCertificate>
        <PublicKeyPath>D:\I3\IC\Certificates\ServerGroup\ServerGroupPublicKey.bin</PublicKeyPath>
        <PrivateKeyPath>D:\I3\IC\Certificates\ServerGroup\ServerGroupPrivateKey.bin</PrivateKeyPath>
        <CertificatePath>D:\I3\IC\Certificates\ServerGroup\ServerGroupCertificate.cer</CertificatePath>
        <Password />
        <TrustedCertificatePath />
      </ServerGroupCertificate>
    - <Notifier Name="Jasper">
      - <SubsystemsRemoteClientCertificate>
          <PublicKeyPath>D:\I3\IC\Certificates\Client\Remote_Subsystems\Jasper\LAKE_ClientPublicKey.bin</PublicKeyPath>
          <PrivateKeyPath>D:\I3\IC\Certificates\Client\Remote_Subsystems\Jasper\LAKE_ClientPrivateKey.bin</PrivateKeyPath>
          <CertificatePath>D:\I3\IC\Certificates\Client\Remote_Subsystems\Jasper\LAKE_ClientCertificate.cer</CertificatePath>
          <Password />
          <TrustedCertificatePath>D:\I3
            \IC\Certificates\Client\Remote_Subsystems\Jasper\LAKE_TrustedCertificate.cer</TrustedCertificatePath>
        </SubsystemsRemoteClientCertificate>
      - <RemoteClientCertificate>
          <PublicKeyPath />
          <PrivateKeyPath />
          <CertificatePath />
          <Password />
          <TrustedCertificatePath>D:\I3\IC\Certificates\Client\Remote_Client\jasper\LAKE_TrustedCertificate.cer</TrustedCertificatePath>
        </RemoteClientCertificate>
      </Notifier>
    - <Notifier Name="LAKE">
      - <ICCertificateAuthority>
          <PublicKeyPath>D:\I3\IC\Certificates\ICCertificateAuthority\LAKE_ICCertificateAuthorityPublicKey.bin</PublicKeyPath>
          <PrivateKeyPath>D:\I3\IC\Certificates\ICCertificateAuthority\LAKE_ICCertificateAuthorityPrivateKey.bin</PrivateKeyPath>
          <CertificatePath>D:\I3\IC\Certificates\ICCertificateAuthority\LAKE_ICCertificateAuthorityCertificate.cer</CertificatePath>
          <Password />
          <TrustedCertificatePath />
        </ICCertificateAuthority>
      - <SubsystemsServerCertificate>
          <PublicKeyPath>D:\I3\IC\Certificates\Client\Local_Subsystems\LAKE_ServerPublicKey.bin</PublicKeyPath>
          <PrivateKeyPath>D:\I3\IC\Certificates\Client\Local_Subsystems\LAKE_ServerPrivateKey.bin</PrivateKeyPath>
          <CertificatePath>D:\I3\IC\Certificates\Client\Local_Subsystems\LAKE_ServerCertificate.cer</CertificatePath>
          <Password />
          <TrustedCertificatePath>D:\I3\IC\Certificates\Client\Local_Subsystems\LAKE_TrustedCertificate.cer</TrustedCertificatePath>
        </SubsystemsServerCertificate>
      - <SubsystemsRemoteClientCertificate>
          <PublicKeyPath>D:\I3\IC\Certificates\Client\Local_Subsystems\LAKE_ClientPublicKey.bin</PublicKeyPath>
          <PrivateKeyPath>D:\I3\IC\Certificates\Client\Local_Subsystems\LAKE_ClientPrivateKey.bin</PrivateKeyPath>
          <CertificatePath>D:\I3\IC\Certificates\Client\Local_Subsystems\LAKE_ClientCertificate.cer</CertificatePath>
          <Password />
          <TrustedCertificatePath>D:\I3\IC\Certificates\Client\Local_Subsystems\LAKE_TrustedCertificate.cer</TrustedCertificatePath>
        </SubsystemsRemoteClientCertificate>
      - <RemoteClientCertificate>
          <PublicKeyPath />
          <PrivateKeyPath />
          <CertificatePath />
          <Password />
          <TrustedCertificatePath>D:\I3\IC\Certificates\Client\Remote_Client\lake\LAKE_TrustedCertificate.cer</TrustedCertificatePath>
        </RemoteClientCertificate>
      </Notifier>
    </Notifiers>
    <SIPDevices />
  </ININCertificates>
```

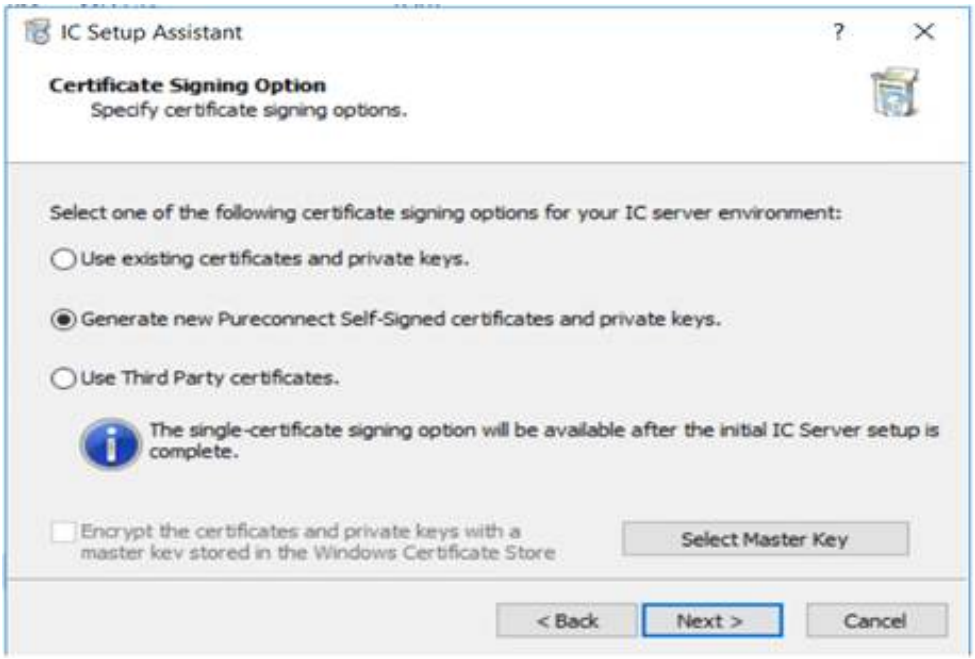
Certificate signing options

CIC Servers require certificates and private keys for secure communications with remote subsystems such as ASR servers and Web servers.

CIC Servers in multiple CIC Server environments, for example, a Switchover pair, require identical certificates and private keys to connect to remote subsystems. Depending on this CIC Server's role in your CIC Server environment, you can complete this process on each CIC Server.

First Run of IC Setup Assistant

Following is how the *Certificate Signing Option* page appears the first time you run IC Setup Assistant



Use Existing certificates and private keys

If selected, you prefer to leave the current certificate structure as it is. This selection bypasses any further setup for certificates and continues with the next step in IC Setup Assistant.

Generate new PureConnect Self-Signed certificates and private keys

If selected, the system generates new PureConnect self-signed certificates and private keys. For more information see section *Generate new PureConnect Self-Signed certificates and private key.*

Use Third Party certificates

Note:You can use this option only during a Re-run of the Setup Assistant. DO NOT use this procedure for the first run of the Setup Assistant.

If selected, the system uses certificates that a third-party certificate authority signed. This option requires you to select the certificate use type for which to create a certificate signing request. After you receive the signed certificate from the certificate authority, run IC Setup Assistant again and select this option again to import the signed certificate and private key. For more information, see section *Use Third Party Certificates.*

Select Master Key

This procedure allows you to specify a separate master certificate and private key to use to encrypt the certificate folder. The Windows Certificate Store stores the master certificate. You can use Select Master Key with all three certificate signing options. After you use the **Import Certificate** dialog box to import the master certificate and private key, **Encrypt the certificates and private keys with a master key stored in the Windows Certificate Store** option appears selected.

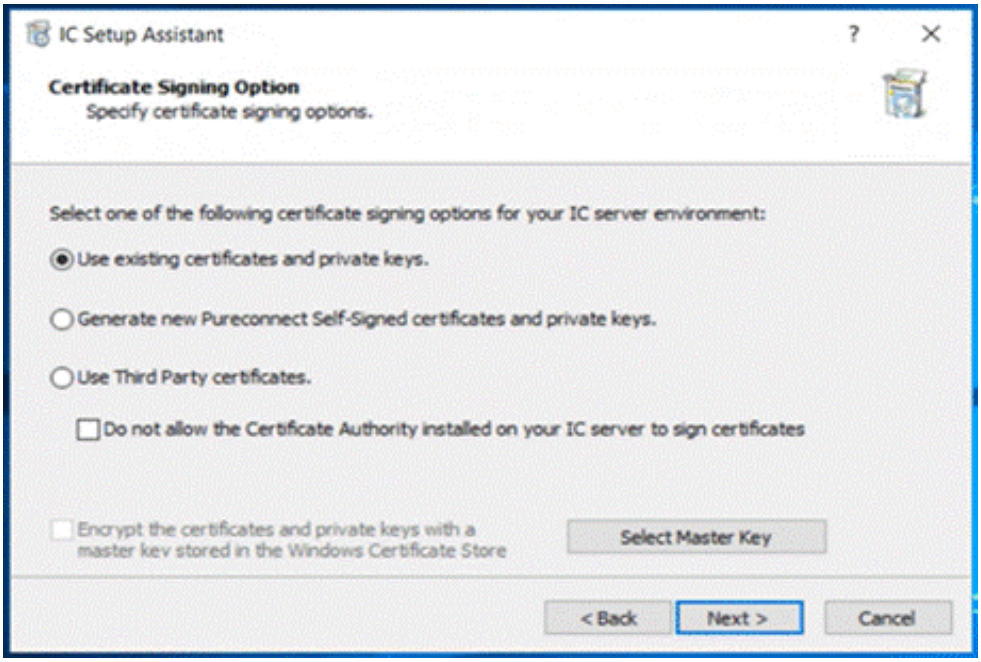
Encrypt the certificates and private keys with a master key stored in the Windows Certificate Store

If you used Select Master Key to import a certificate and private key to use as a master key, Setup Assistant selects this option. If you don't want to use a certificate and private key to encrypt the certificate folder, clear this option.

Important! This option disables further certificate generation on this computer until you run IC Setup Assistant again and remove the check mark to clear this option.

Subsequent runs of IC Setup Assistant

Following is how the Certificate Signing Option page appears when you rerun IC Setup Assistant.



Use Existing certificates and private keys

If selected, you prefer to leave the current certificate structure as is. This selection bypasses any further setup for certificates and continues with the next step in IC Setup Assistant.

Generate new PureConnect Self-Signed certificates and private keys

If selected, the system generates new PureConnect self-signed certificates and private keys. For more information see section *Generate new PureConnect Self-Signed certificates and private key.*

Use Third Party certificates

If selected, the system uses certificates that a third-party certificate authority signed. This option requires you to select the certificate use type for which to create a certificate signing request. After you receive the signed certificate from the certificate authority, run IC Setup Assistant again and select this option again to import the signed certificate and private key. For more information, see section *Use Third Party Certificates.*

Do not allow the Certificate Authority installed on your IC Server to sign certificates

If selected, the system prevents the certificate authority installed on the IC Server from generating certificates. You must generate and manage all certificates in your environment. This option only appears when you **rerun** IC Setup Assistant.

Note:When using a single-server certificate for all certificate use types and the single certificate becomes compromised for one certificate use type, the other certificate use types cannot use the certificate.

Select Master Key

Allows you to specify the master certificate and private key to use to encrypt the certificate folder. The Windows Certificate Store stores the master certificate. You can use **Select Master Key** with all three certificate signing options.

After you use the Import Certificate dialog box to import the master certificate and private key, **Encrypt the certificates and private keys with a master key stored in the Windows Certificate Store** option appears selected.

Encrypt the certificates and private keys with a master key stored in the Windows Certificate Store

If you used **Select Master Key** to import a certificate and private key to use as a master key, Setup Assistant selects this option. If you don't want to use a certificate and private key to encrypt the certificate folder, clear this option.

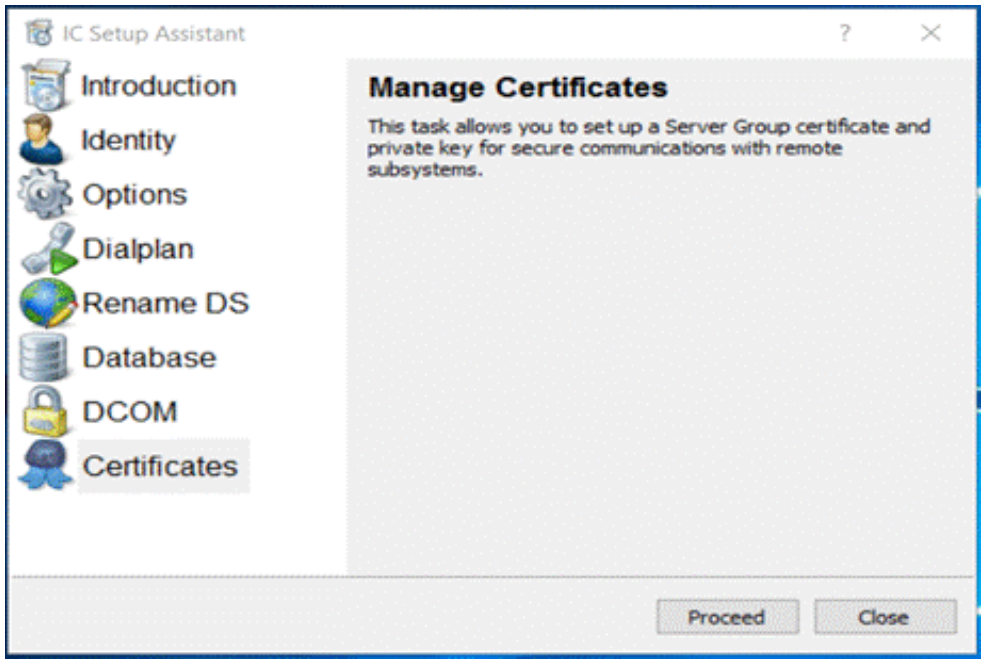
Important! This option disables further certificate generation on this computer until you run IC Setup Assistant again and remove the check mark to clear this option.

Generate new PureConnect Self-Signed certificates and private keys

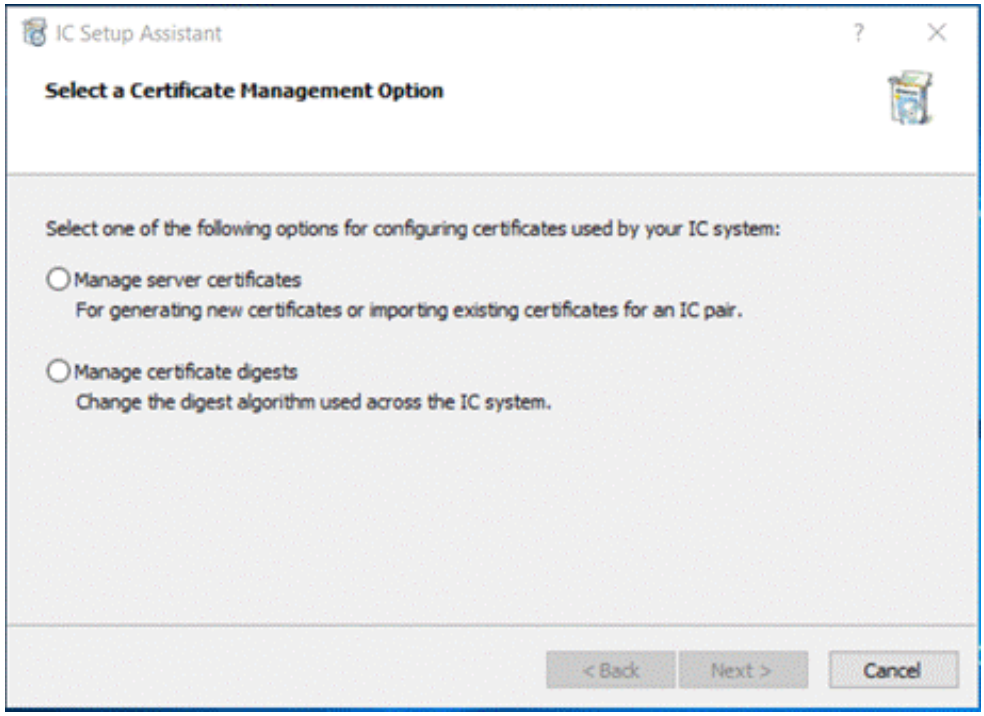
CIC Servers in multiple CIC Server environments, such as Switchover pairs, require identical Server Group certificates and private keys to connect to remote subsystems. Some CIC Server roles require an extra procedure to fulfil this requirement. As an example, the following information describes the options to select for the initial active and backup servers in a Switchover pair.

To select the certificate management option for your IC Server environment:

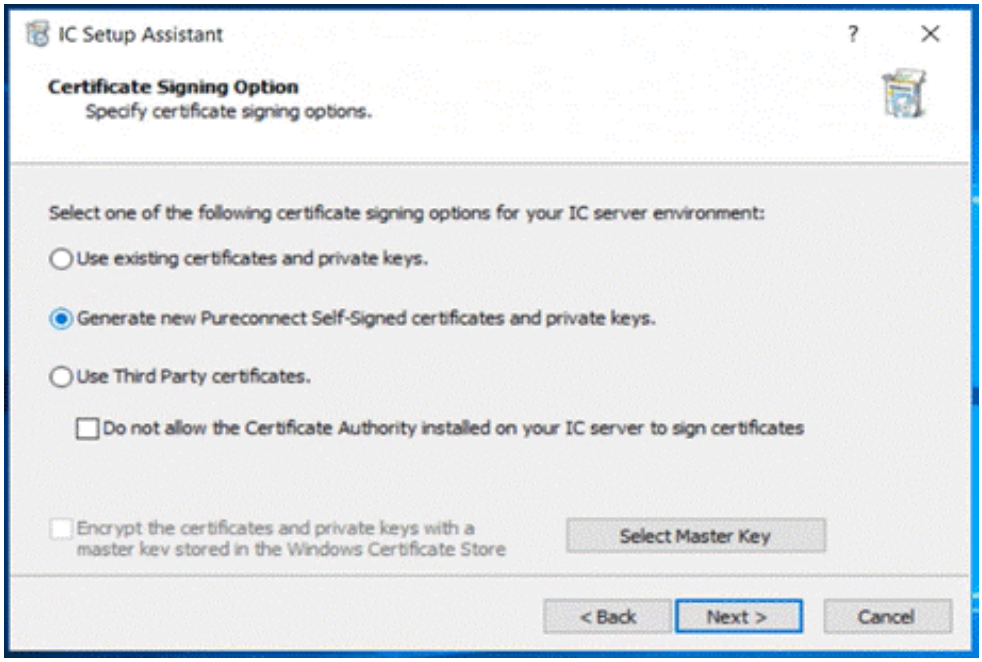
1. Open IC Setup Assistant and then click **Certificates**. The *Manage Certificates* page appears.



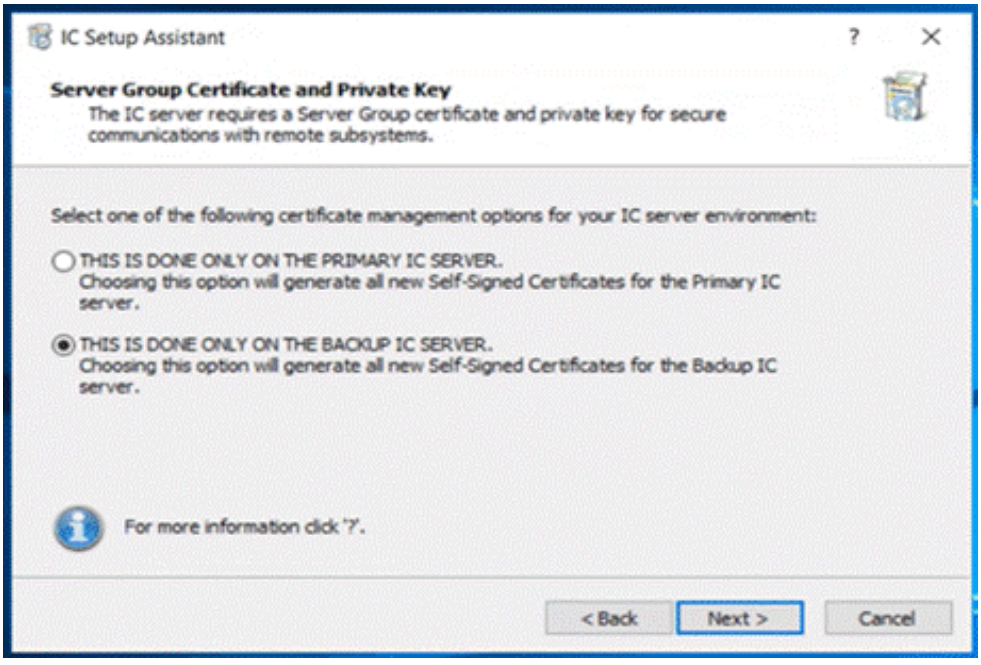
2. Click **Proceed**. The *Select a Certificate Management Option* page appears.



3. Select **Manage server certificates** and then click **Next**. The *Certificate Signing Option* page appears.



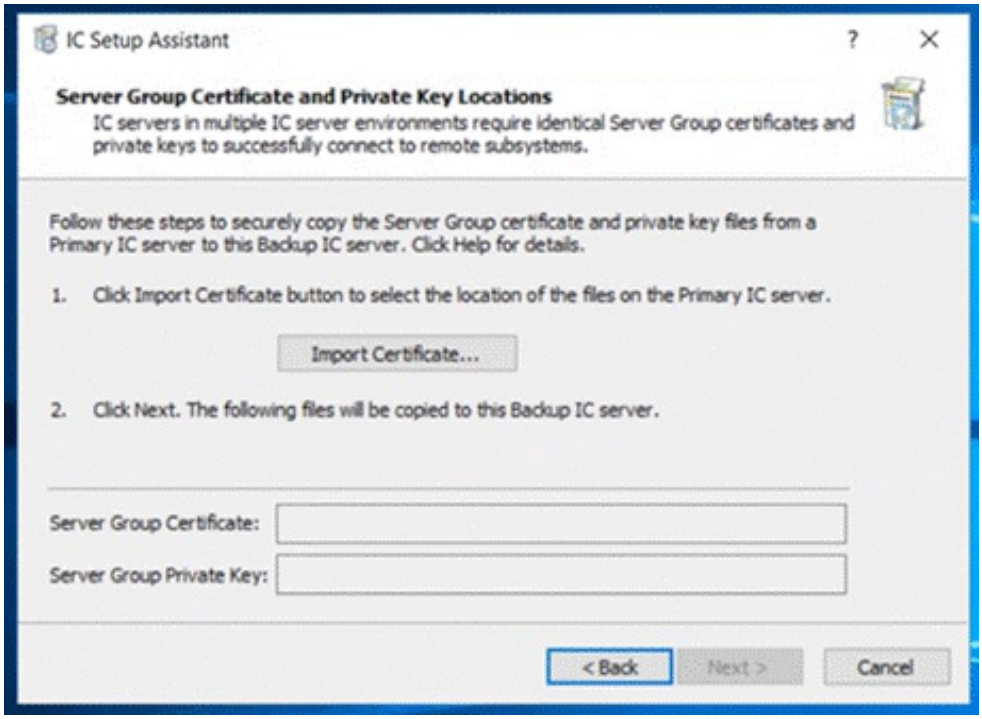
4. Select **Generate new PureConnect Self-Signed certificates and private keys** and then click **Next**. The *Server Group Certificate and Private Key* page appears.



5. Do one of the following:
   - If this CIC Server is the initial active server, click **THIS IS DONE ONLY ON THE PRIMARY IC Server**
   - No further configuration is necessary. IC Setup Assistant uses the Server Group certificate and a private key that generated automatically during the CIC Server installation.
   - If this CIC Server is the initial backup server, click **THIS IS DONE ON THE BACKUP IC Server**

- If you plan to use a third-party certificate authority, click the question mark **(?)** for instructions.

6. Click **Next**. If selected the second option, **THIS IS DONE ON THE BACKUP IC Server** the *Server Group Certificate and Private Key Locations* page appears.



7. Do the following:

   a. Open the \I3\IC\Certificates directory on the initial active server.

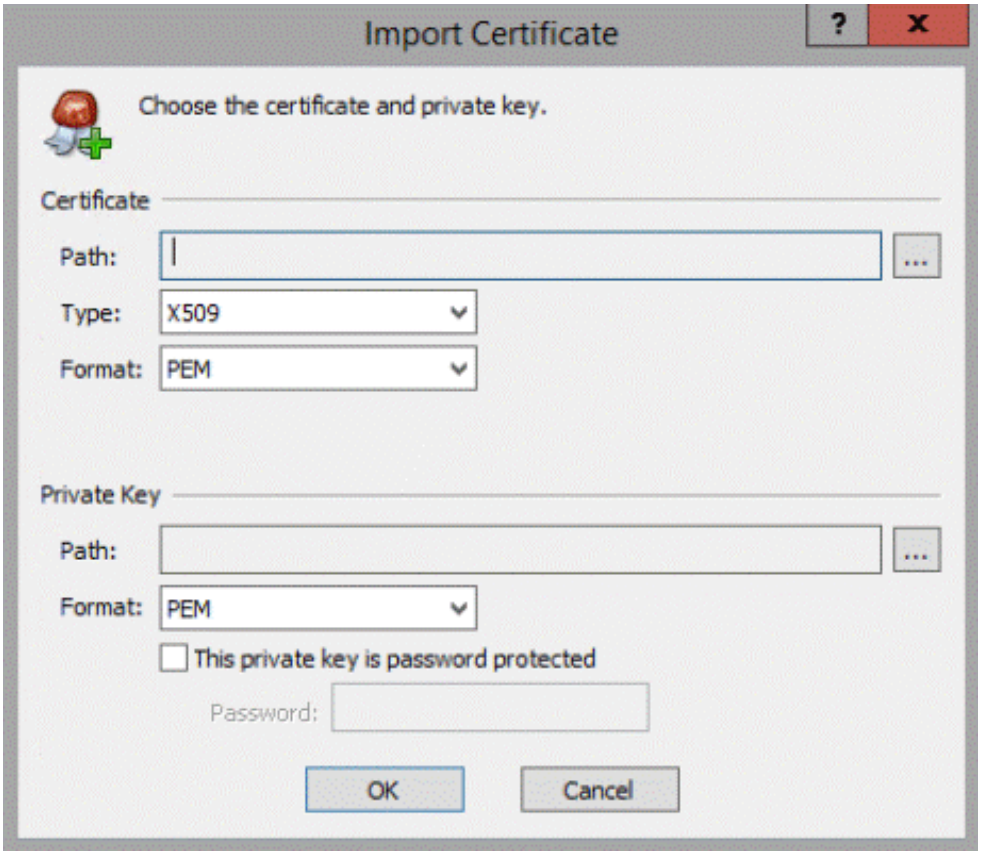
      Note: To use your ServerGroup certificate and private key, locate the Server Group Certificate (ServerGroupCertificate.cer) and Server Group Private key (ServerGroupPrivateKey.bin) to use.

   b. Copy the entire \I3\IC\Certificates directory

      Note: If you are using your ServerGroup certificate and private key, copy the Server Group Certificate (ServerGroupCertificate.cer) and Server Group Private key (ServerGroupPrivateKey.bin) that you want to use.

   c. Paste the Certificate Directory into the initial backup server.

   d. On the *Server Group Certificate and Private Key Locations* page, click Import Certificate. The Import Certificate dialog box appears.



Certificate Path:

Location of the Server Group certificate on the USB key. For example, F:\ServerGroup\ServerGroupCertificate.cer.

Type:

Certificate type. If you are using your own Server Group certificate, specify the type; otherwise, leave the default setting.

Format:

Certificate format. If you are using your own Server Group certificate, specify the format; otherwise, leave the default setting.

Private Key Path:

Location of the private key files on the USB key. For example, F:\ServerGroup\ServerGroupPrivateKey.bin.

Format:

Private key format. If you are using your private key, specify the format; otherwise, leave the default setting.

This private key is password protected:

If selected and you are using your private key, the private key is password protect

Password:

Password for the private key, when protected.

e. Complete the information and then click **OK**. IC Setup Assistant returns to the *Server Group Certificate and Private Key Locations* page. It displays the paths of the Server Group certificate and private key files on the backup server to copy to this CIC Server.

Note: IC Setup Assistant backs up the existing certificate and private key files before overwriting them.

f. Click **Next.**

g. Close IC Setup Assistant.

h. Store the key containing the \Certificates directory in a safe place for backup purposes.

Troubleshooting

Do not copy the Server Group certificate and private key files manually from the designated existing CIC Server to this CIC Server. Manual copying can lead to errors.

Important! If errors occur, rerun IC Setup Assistant, and do the procedures again. If IC Setup Assistant fails to start Notifier, DS Server, and AdminServer, regenerate the default certificates.

Note: Before you perform any Certificate work on the IC Server for use within the DOD, you must install the latest version of the "InstallRoot" application and run the application to install the correct DoD certificates on all of your PureConnect Windows Servers (IC, Media, SQL and so on). InstallRoot is designed to facilitate the management of DoD PKI Certification Authority (CA) certificates and other PKI CA certificates that may be necessary the conduct any DoD business across a variety of different certificate stores. Please contact your DoD Customer to obtain this application. For Federal Agencies, install the Agencies Root Certificate Authority Certificate and any additional Intermediate certificates as well before doing anything else.

Server Group Certificate and Private Key backup information

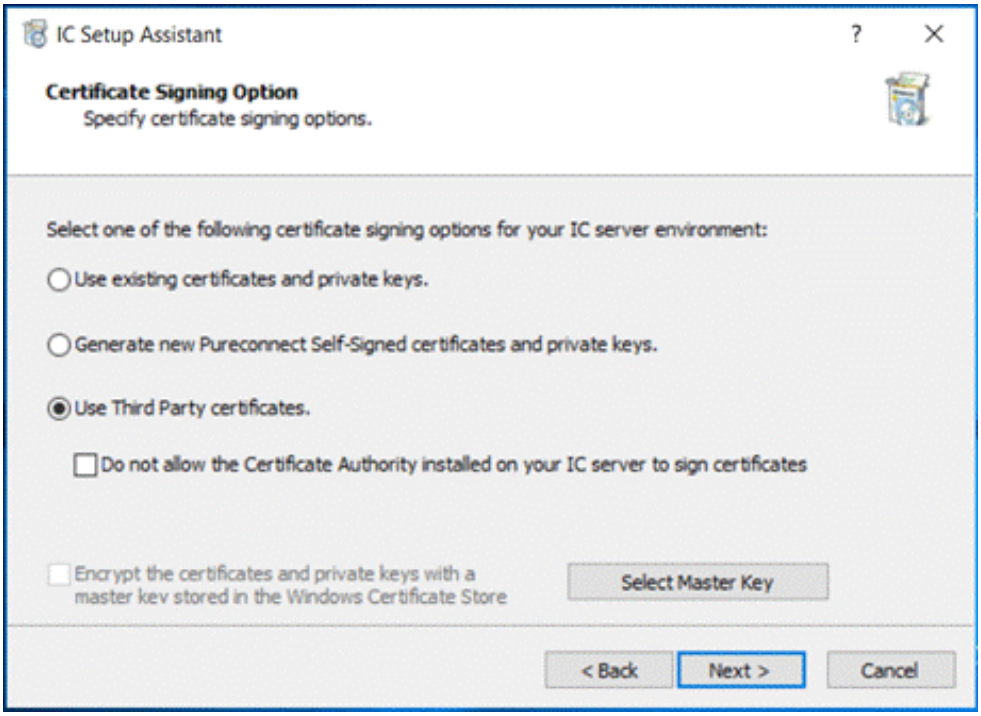
IC Setup Assistant backs up the existing Server Group certificate and private key files in the \I3\IC\Certificates\ServerGroup directory. It overwrites them with the certificate and private key you specify in the Import Certificates dialog box.The backed-up files have the same name as the original files, with the <BackupNumber> extension. For example:

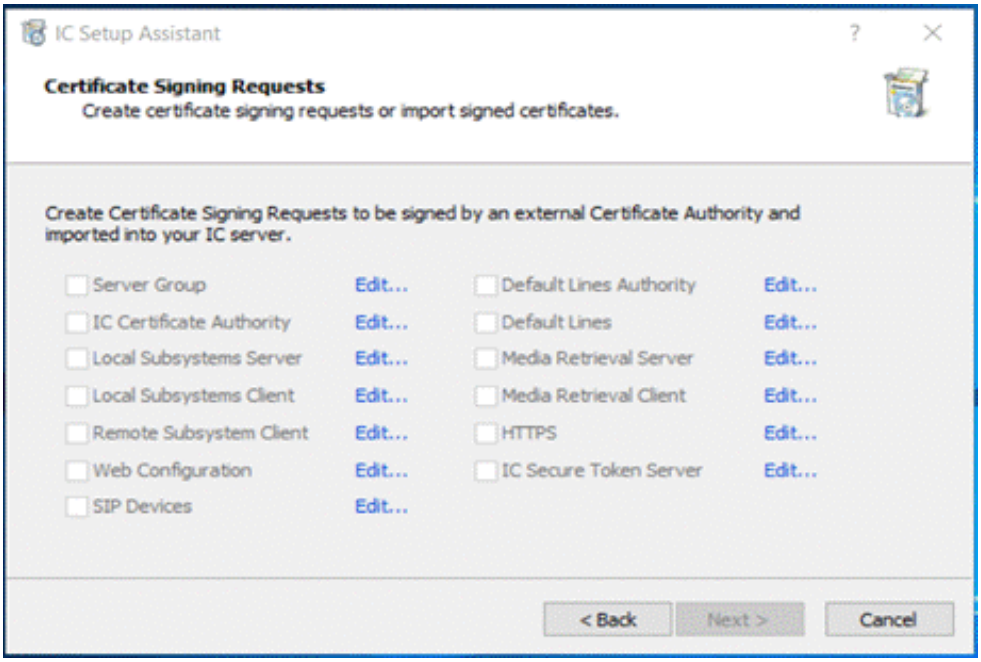
ServerGroupCertificate.cer.1 on the first backup

ServerGroupCertificate.cer.2 on the second backup

Use Third Party Certificates

Click the **Use Third party Certificates** option to use certificates signed by a third-party certificate authority. This option displays the Certificate Signing Requests page to allow you to select the certificate use type for which to create a certificate signing request.





The first time you run IC Setup Assistant:

- If you do not plan to use a single certificate for all certificate uses, use the *Certificate Signing Requests* page to create certificate signing requests for all the certificate use types. We recommend that you use a Single Certificate to simplify the process.
- If you plan to use a single certificate for all certificate uses, use the *Certificate Signing Requests* page to create a certificate signing request for the Server Group certificate use type or select a signed certificate from the Windows Certificate Store for the Server Group certificate use type.
- When you create a certificate signing request, it creates a certificate signing request file and a private key. Send the certificate signing request file to a certificate authority. Keep the private key to use when you import the signed certificate that you receive from the certificate authority.

  Note: Do not send the private key to the certificate authority. Do not copy the private key unless you create a secure copy.
- When you receive the signed certificate from the certificate authority, run IC Setup Assistant again and use this page to import the signed certificate and private key.

When you rerun IC Setup Assistant:

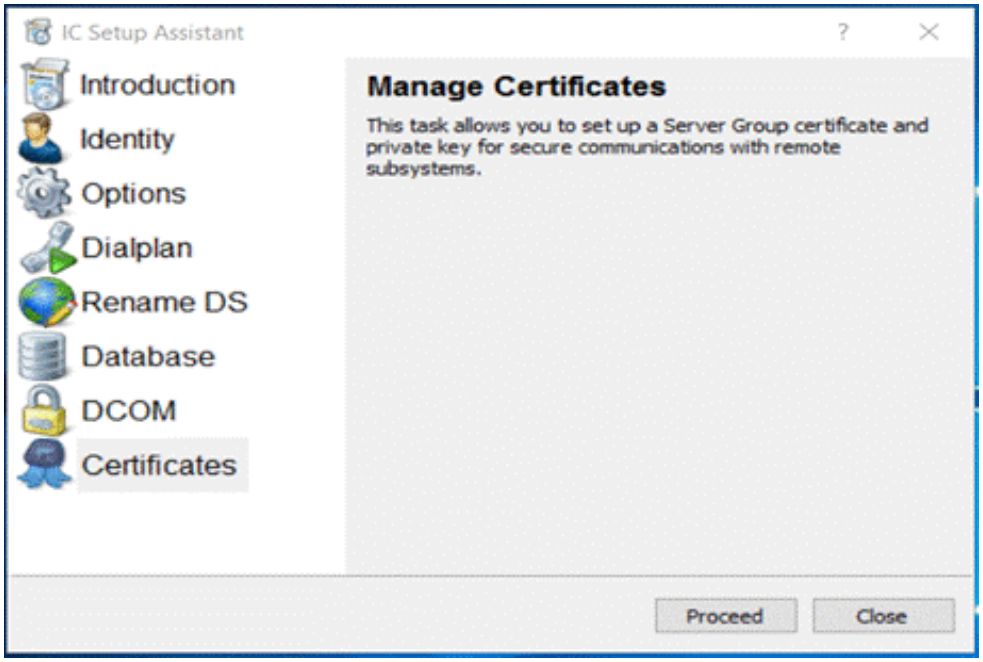
- If you selected **Do not allow the Certificate Authority installed on your IC Server to sign certificates** to use a single certificate for all certificate uses, you import a signed certificate for all the certificate use types.
- If you did not select **Do not allow the Certificate Authority installed on your IC Server to sign certificates** to use a single certificate for all certificate uses, you import a signed certificate for the Server Group certificate use type.

CIC Servers in multiple CIC Server environments, for example, a Switchover pair, require identical certificates and private keys to connect to remote subsystems. Depending on this CIC Server's role in your CIC Server environment, you can complete this process on each CIC Server.

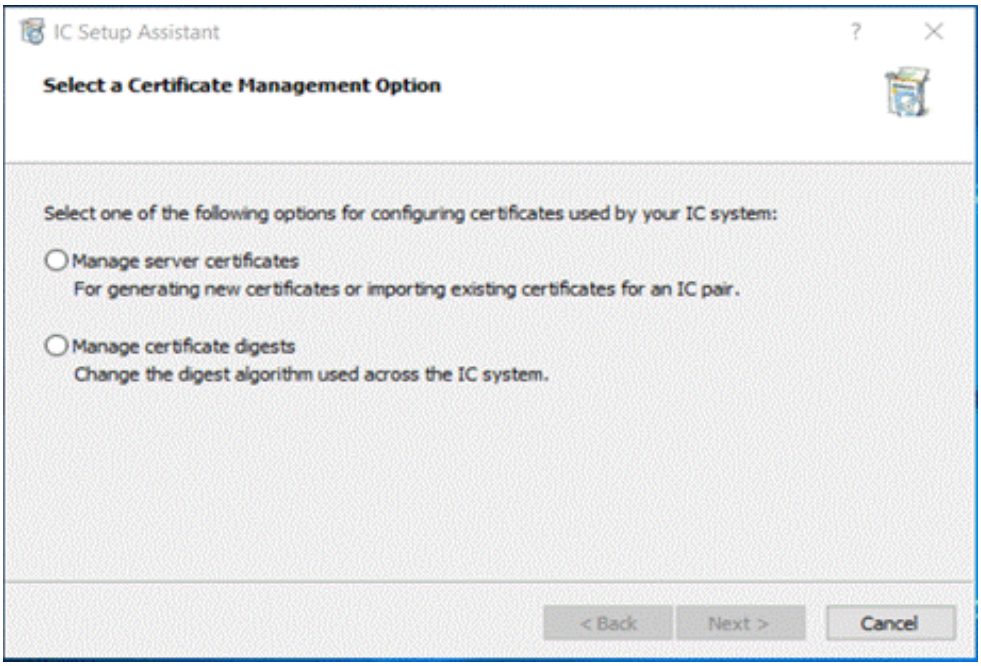
Create a Certificate Signing Request

Important! If you plan to use a single certificate for all certificate uses, you must create a certificate signing request for the Server Group certificate use type. If you do not plan to use a single certificate for all certificate uses, you must create certificate signing requests for all the certificate use types.

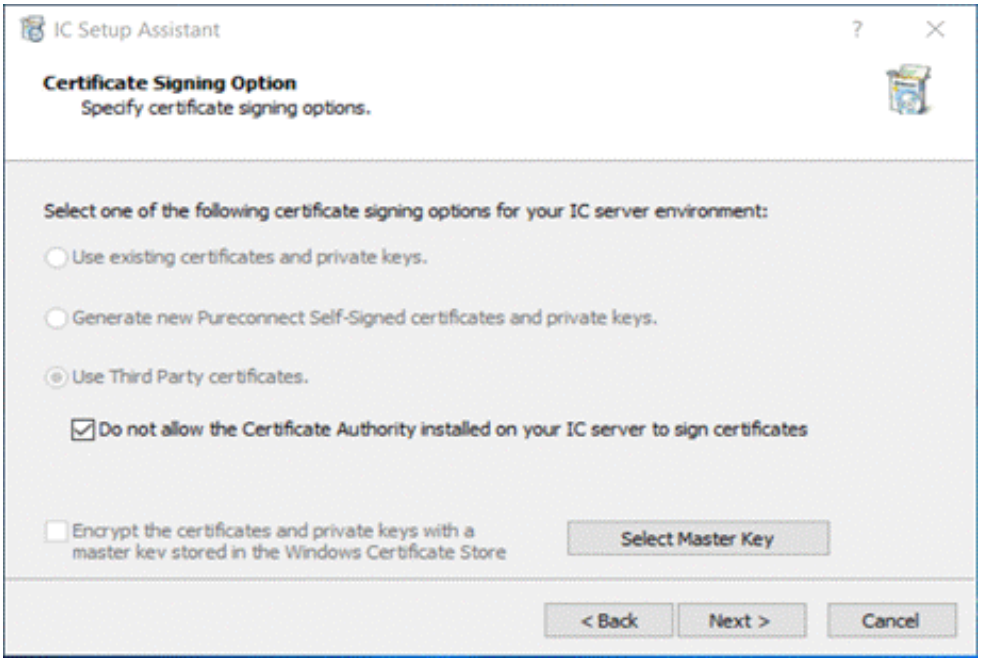
1. Open IC Setup Assistant and then click Certificates. The *Manage Certificates* page appears.



2. Click **Proceed**. The *Select a Certificate Management Option* page appears.

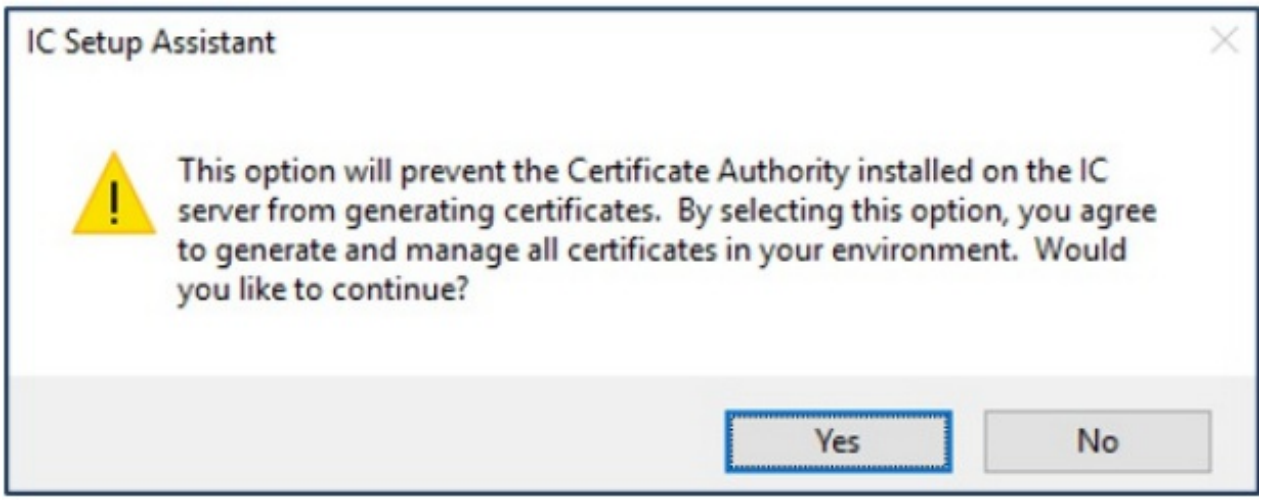


3. Click **Manage certificates** and then click **Next**. The *Certificate Signing Option* page appears.

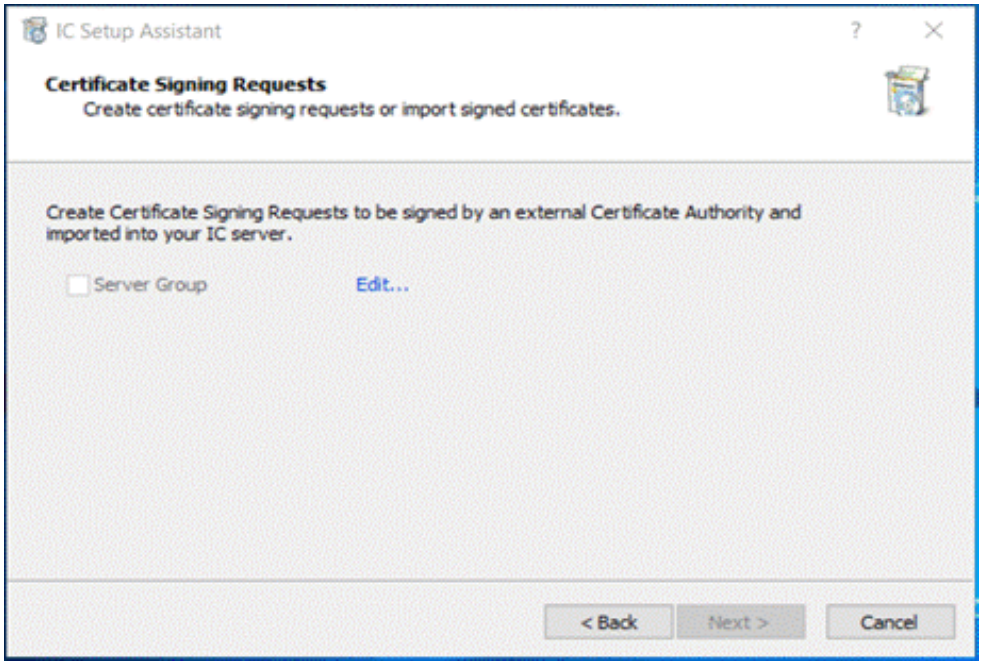


4. Click **Use Third Party Certificates** and check **Do not allow the Certificate Authority installed on your IC Server to sign certificate** checkbox.

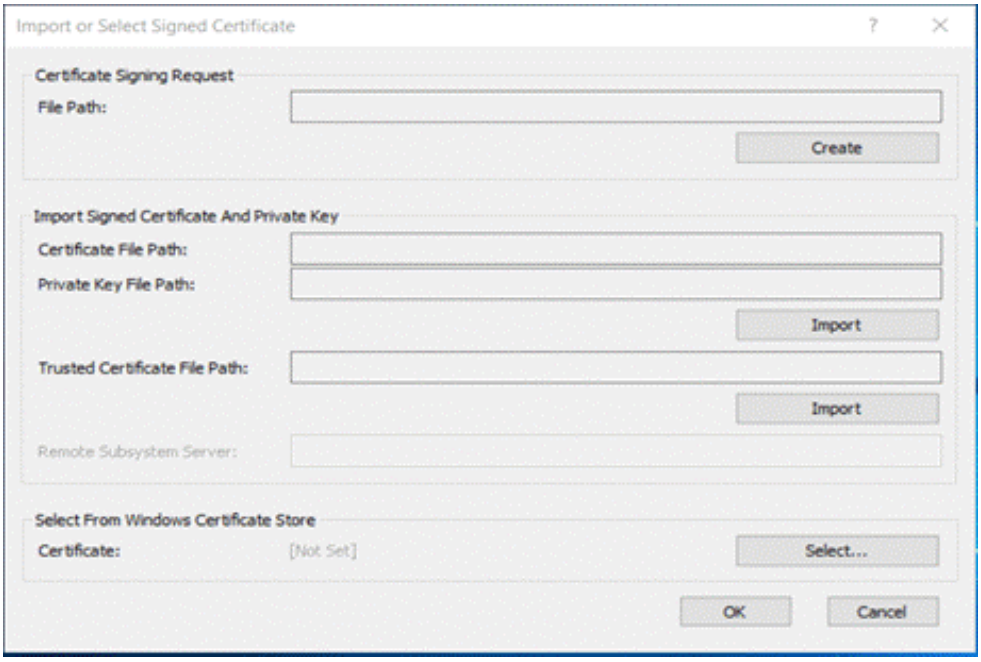
5. Click **Next**. The *Certificate Signing Requests* page appears. Click **Yes** on the Warning Message.



If you chose to use a single-server certificate for all certificate use types, only one certificate use type appears on this page. Otherwise, all certificate use types appear.

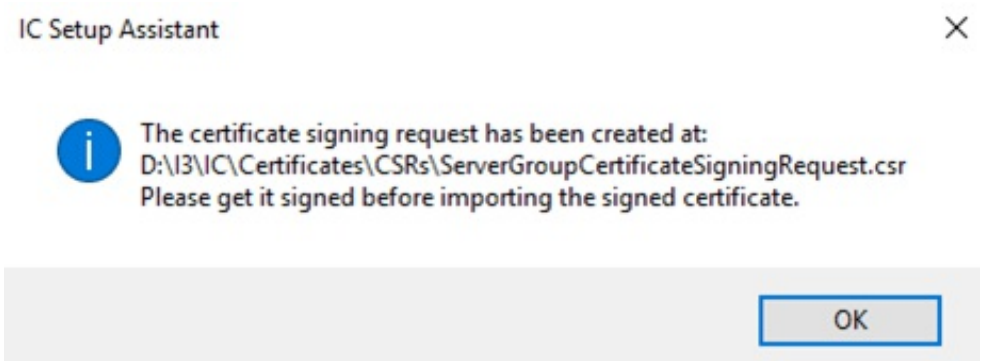


6. To create a certificate signing request for a certificate use type, click the **ellipsis (...)** next to the certificate use type. The *Import or Select Signed Certificate* page appears.



7. Click **Create**. IC Setup Assistant displays a message to indicate that you successfully created the request. The **File Path** field indicates the path to the certificate signing request file and the private key.

Note: Remember the path to the certificate signing request file and private key so that you can send the file to the certificate authority and specify the private key during import.



8. Click OK. On the Certificate Signing Requests page, the IC Setup Assistant place a checkmark next to the certificate use type for which you created a certificate signing request.

9. If you chose to use a separate server certificate for each certificate use type, create a certificate signing request for the remaining certificate use types and then click **Next**.

Importing Signed Certificate

After you create the certificate signing requests, send the certificate signing request file or files to your certificate authority. Don't send the private key to the certificate authority and don't copy the private key unless you create a secure copy.

When you receive the signed certificate back from the certificate authority, run IC Setup Assistant again and do the following to import the signed certificate and private key: There are two ways to do this.

- Importing signed certificate and Private Keys.
- Importing from Windows Certificate Store.

a. Importing signed certificate and Private Keys

1. On the *Certificate Signing Option* page, select the **Use Third Party Certificates** option.

2. If you selected the **Do not allow the Certificate Authority installed on your IC Server to sign certificate** check box, when you created your certificate signing requests, select the check box again. Otherwise, clear the check box.

3. Click **Next**. The *Certificate Signing Requests* page appears.

4. Click the **ellipsis (…)** next to a certificate use type to import a signed certificate and private key for that certificate use type. *Import or Select Signed Certificate* page appears.

5. Click **Import** to import the certificate file and private key. The *Import Certificate* page appears.

6. Complete the information and then click **OK**, for going back to *Import or Select Signed Certificate* page. The **Certificate File Path** and **Private Key File Path** boxes display the location from which you imported.

7. Click **Import** to import the **Trusted certificate**. The *Import Certificate* page appears. If you selected the "Local Subsystems Server," "Local Subsystems Client," "Remote Subsystem Client," or "HTTPS" certificate use type on the *Create*

Certificate Signing Request and Import Signed Certificate page, you can select Import to import a trusted certificate.

8. Complete the information and then click **OK**, for going back to *Create Certificate Signing Request and Import Signed Certificate* page. The **Trusted Certificate File Path** box displays the location from which you imported.

9. In the **Remote Subsystem Server** box, type the name of the server. If you selected the "Remote Subsystem Client" certificate use type on the *Create Certificate Signing Request and Import Signed Certificate page*, you can access the **Remote Subsystem** Server box.

10. Click **OK**. The *Certificate Signing Requests* page appears. IC Setup Assistant places a checkmark next to the certificate use type that you just completed.

11. If you chose to use a separate server certificate for each certificate use type, import the signed certificate and private key for the remaining certificate use types.

12. Click **Next**.

13. Select **Restart IC.**

14. Select **Commit.**

The certificate process will run and once completed select **Close** and you will have the option to start the Interaction Center Service now or at a later time.

15. **Reboot** the IC Server once to validate that the IC Server Service starts.

b. Importing from Windows Certificate Store

Once you have received the Signed Certificate back from the Signing Authority, you will need to convert it into a .PFX format and then import that PFX certificate into the Local Servers Windows Certificate Store under "Trusted Devices".

1. On the *Certificate Signing Option* page, select the **Use Third Party Certificates**.

2. If you selected the **Do not allow the Certificate Authority installed on your IC Server to sign certificate** check box when you created your certificate signing requests, select the check box again. Otherwise, clear the check box.

3. Click **Next**. The *Certificate Signing Requests* page appears

4. Click the **ellipsis (…)** next to a certificate use type to import a signed certificate and private key for that certificate use type. *Import or Select Signed Certificate* page appears.

5. In the *Import or Select Signed Certificate* window choose the Select box under the **Select from Windows Certificates Store** option

6. Select the **Local Machine** radio button and then choose the "**Trusted Device**" option in the pull-down arrow.

7. Click on the **Select** button.

8. The Confirm Certificate window will appear, make sure that the correct Certificate is chosen.

9. Select **OK.**

10. The next window will pop up and it wants you to validate that you have chosen the certificate you want.

11. Click **OK**.

12. The certificate now shows up in the **Select from Windows Certificates Store** field.

13. Click **OK.** The *Certificate Signing Requests* page appears. IC Setup Assistant places a checkmark next to the certificate use type that you just completed.

14. Click **Next.**

15. Select **Restart IC.**

16. Select **Commit.**

The certificate process will run and once completed select “Close” and you will have the option to start the Interaction Center Service now or at a later time.

17. **Reboot** the IC Server once to validate that the IC Server Service starts.

Using the Single Third-Party Certificate Mode for PureConnect IC 2022 R2

Third-party certificates can be used with all the below off-server components

1. CIC Server
2. Media Server
3. OSSM
4. Scheduled Reports
5. SIP Proxy
6. Interaction Recorder
7. RCS (Remote Content Server)
8. Dialer
9. Campaign Server
10. SIP Softphone
11. ICWS-based applications
12. IceLib-based applications
13. IPA (Interaction Process Automation)
14. CX Insights
15. Multisite (EMS Server)
16. Director

Note: We are not considering Schedule Reports and Director, because based on the understanding and knowledge we gather about Schedule Reports, it is concluded that the Third-Party certificates are not required for Schedule Reports as it uses the native Notifier connection between CIC and schedule report server and works on internal network TLS certificates and so the SQL DB is already secured. Also, for "Director" the release testing was stopped for almost 3-4 years because of no customers and due to the complexity of the test environment.

Interaction Center version 2018 R5 and later can operate on a Single Third-Party Certificate to run the PureConnect applications and associated subsystems. You may now store your Third Party Signed Certificates in the local Server's "Windows Certificate Store" to minimize human certificate manipulation. The PureConnect Certificate Wizard can import those Third Party Signed Certificates from the local Windows Certificate Store and to encrypt the Certificates with a Master Key. Depending on your requirements, Master Key encryption may or may not be required. Check with the appropriate vulnerability security personal before determining your agency's requirements.

You can generate a single server certificate through the Setup Assistant for the PureConnect IC Server or use the GenSSLCertsU Command Line tool for the other Off IC Server components such as the Media servers, RCS, and Off Host Session manager servers. This option forces all xIC subsystems to use the single server certificate and private key for all uses. While this option reduces the complexity of managing certificates and private keys, all xIC subsystems become insecure if the single server private key becomes compromised.

Please note that if you select to use the single server certificate option, you will not be able to generate new certificates and private keys, until you **Re-run the Setup Assistant or the GenSSLCertsU tool and select a different certificate signing option.**

For Third-Party Certificate deployments, you may need to create a Domain User account named "ICService" on the Customers Domain that we use to log on to and install or upgrade the PureConnect IC Server applications (we use this same account on other IC sub-system peripheral servers as well. This "ICService" account becomes the "Service" account that Windows uses to run PureConnect as a service. This "Service" account will have the required ACLs and permissions to encrypt and run PureConnect in the Master Key mode should you need this level of security. Note, only the "ICService" account will have the required permissions to enable and run PureConnect IC applications once you start using Third-Party certificates.

The "ICService" account can be named anything you want it to be named. Just be sure that this account is the account that you must use to log onto the PureConnect IC Server and install the PureConnect IC applications as a complete system.

For more information about using the GenSSLCertU tool, refer to the Generating Certificates Manually with GenSSLCertsU help section.

Note: For Internal Testing purposes, it is highly recommended to use the Default IC Self Signed Certificate process done at the initial installation of PureConnect to validate that you have a fully functional IC System that you have verified that everything is up and running and switchover is fully functional before performing any other certificate work. That also means that the Media Server and any other Peripheral Off Host IC Sub-systems have been installed, Trusted, and functionality tested before you are satisfied that you have a fully functional IC system, then you can proceed with generating a new CSR for the Third Party Signed Certificate Mode use and then continue with any subsequent updating of the PureConnect Certificates.

Overview of the Process

The procedures to use a Third-Party signed certificate within the PureConnect applications is not complex; it is just a matter of generating new Certificate Signing Requests (CSRs) and importing the Signed Certificate, Private Key back into the system. The steps below walk you through the process:

1. Start the PureConnect Certificate Setup Assistant Wizard on the IC Server to generate the Certificate Signing Requests (CSR) and import the Signed Certificate, Private Key, and Root CA (Trusted Certificate Authority (CA) Certificate back into the IC System.

2. New stand-alone Certificate UI utility on ALL other Off Host IC Subsystems (Media Server, RCS, Off Host Session Manager, and so on) to generate new Certificate Signing Requests (CSR) and import the Signed Certificate, Private Key, and Root CA (Trusted Certificate Authority (CA) Certificate back into the IC System using GenSSLCertsU.exe command-line utility.

3. Use GenSSLCertsU.exe command-line utility on ALL other Off Host IC Subsystems (Media Server, RCS, Off Host Session Manager, and so on) to generate the CSR and import the Signed Certificate, Private Key, and Root CA (Trusted Certificate Authority (CA) Certificate back into the Media Server or other Off Host IC sub-system

Note: During the initial installation of the PureConnect Interaction Center system and other Off Host Sub-systems, you may be prompted to select an option to use SHA-1 or SHA 256 (SHA-2) certificates. You MUST select the SHA 256 (SHA-256) option.

Note: It is highly recommended to use the New stand-alone Certificate GUI application to generate Certificate Signing Requests (CSR) so that the process is quicker and less error-prone. For more information, see CSR Tool User's Guide

Note: For Internal Testing purposes, it is highly recommended to use the Default IC Self Signed Certificate process done at the initial installation of PureConnect to validate that you have a fully functional IC System that you have verified that everything is up and running and switchover is fully functional before performing any other certificate work. That also means that the Media Server and any other Peripheral Off Host IC Sub-systems have been installed, Trusted, and functionality tested before you are satisfied that you have a fully functional IC system, then you can proceed with generating a new CSR for the Third Party Signed Certificate Mode use and then continue with any subsequent updating of the PureConnect Certificates.

Using the Single existing certificate management process

CIC server connection security features include:

- IC Servers automatically use TLS protocol-enabled connections and public/private key certificates for communication with remote subsystems. For example, communications between CIC Servers, Interaction Media Servers, and ASR servers all use digitally signed certificates to authenticate the endpoints and establish TLS connections.
- Genesys provides its own "server group" (root) certificate authority that issues connection certificates to all authorized remote connections and applications. During the CIC Server installation, the installation creates a Server Group certificate authority file and a Server Group private key file automatically in \I3\IC\Certificates\ServerGroup directory on the CIC Server. You configure them using Setup Assistant, and they require only a simple post-install step to trust remote subsystem connections.
- SwitchoverServer pairs must use the same server group (root) certificate and private key so that remote connections can have immediate access to both the primary and backup servers.
- Multi-site CIC Servers that do not share common subsystems each have their server group (root) certificate to issue certificates to the local subsystems at each site.
- Mutual authentication requires the server and trusted computer to have either a certificate from the same certificate authority or the CA certificate of the other system's certificate.

Note: Before you perform any Certificate work on the IC Server for use within the DOD, you must install the latest version of the "InstallRoot" application and run the application to install the correct DoD certificates on all of your PureConnect Windows Servers (IC, Media, SQL and so on). InstallRoot is designed to facilitate the management of DoD PKI Certification Authority (CA) certificates and other PKI CA certificates that may be necessary to conduct any DoD business across a variety of different certificate stores. Please contact your DoD Customer to obtain this application. For Federal Agencies, install the Agencies Root Certificate Authority Certificate and any additional Intermediate certificates as well before doing anything else.

Procedures

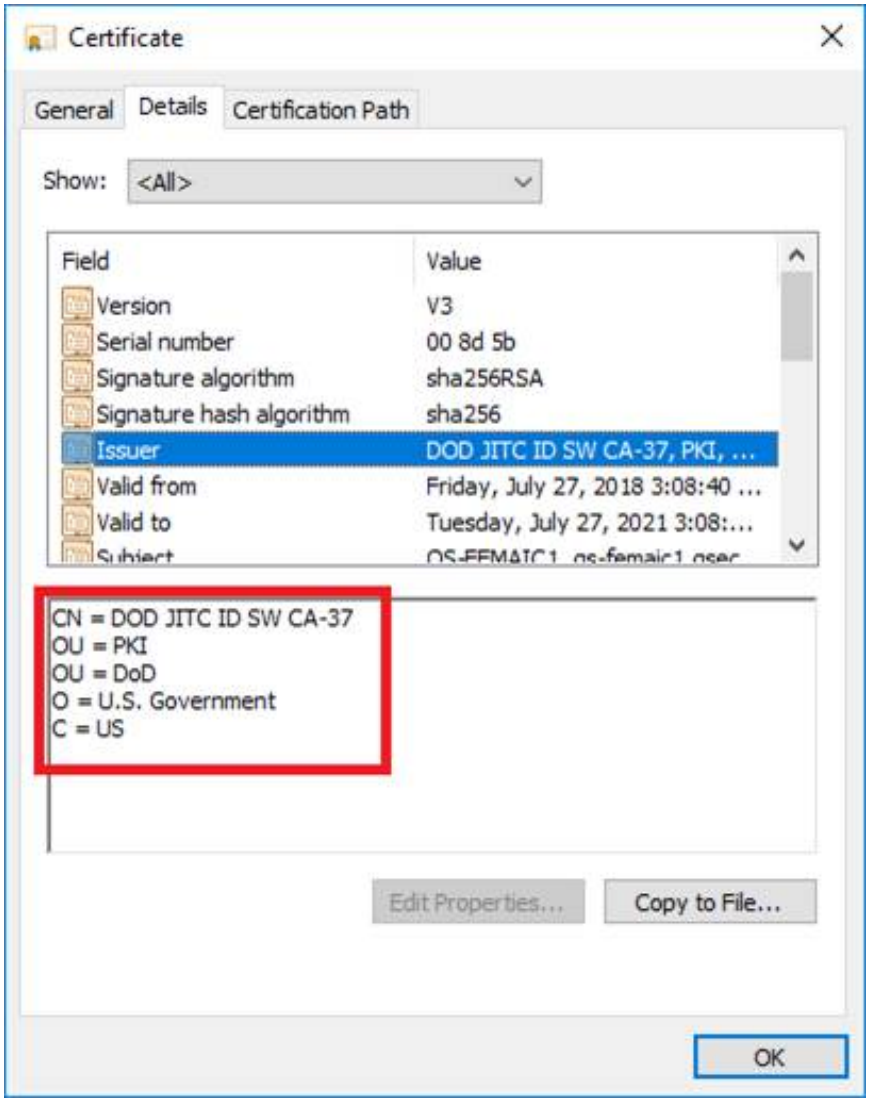
This document contains the instructions on how to enable and use a Third Party Signed Certificate. The procedures are outlined below define the steps and the order of the procedures that we will use to transition the IC System to Third Party Certificates:

1. Regenerate new Certificate Signing Requests (CSRs) for specific PureConnect Servers and any Off Host Servers (Media Server, RCS, Off Host Session Manager Servers).
2. Send the CSRs to the appropriate Certificate Signing Authority.
3. The Certificate Signing Authority signs the CSRs.
4. Retrieve the Signed Certificate and Root CA (Trusted Certificate Authority) Certificate then save them locally and import them into the local windows certificate store.
5. Run the IC Certificate Setup Assistant Wizard or GenSSLCertsU.exe utility to import the Signed Certificate and Private Key back into the IC System
6. Perform System and Post Certificate configuration tasks.
7. Test and validate to see if IC is still operational and functional

Note: Always backup your original Certificate Directory at the location D:\I3\IC Certificates. If something goes wrong during the process you can always revert to the original Certificates.

Pre CSR Tasks

Companies and Government Agencies often require that certain information be included in the Certificate Signing Request. In the example below, the DoD requires a specific Organizational Unit (OU) and other information when the CSR is generated:



O	**: Organization Name**
OU	**: Organizational Unit**
SAN	**: Subject Alternative Name**
CN	**: Common Name**
C	**: Country**
S	**: State**
L	**: Locality or City**

To ensure that the appropriate OU, O and C entries are correct for your company or agency, you will need to edit a configuration file and drop that file into the D:\IC\Server Directory on the PureConnect Server or Off Host Server. That edited file is named "OpenSSL.cnf" and it ensures that the appropriate entries are incorporated into the CSR.

Note: If you use the CSR Utility, you will be able to directly enter the correct information and set them in the correct order. If you use the CSR utility, the steps in the paragraph below are NOT needed or required and you can move on to the next set of procedures.

Open SSL.cnf file example

The "**# req_extentions=v3_req #**" section is the area that you will need to edit to ensure that the appropriate elements are set to the Agencies requirements. In the example below, in this case of JITC, they expect to see the following elements within the CSR.

CN = (PureConnect Server Name)

OU = Contractor

OU = PKI

OU = DoD

O = U.S. Government

C = US

So, the # req_extensions = v3_req # section of the OpenSSL.cnf file has been edited to ensure that those required elements are set to a Default value. Without the Default value entered in the OpenSSL.cnf, those entries will not be part of the CSR. Those elements are highlighted in Yellow.

Please edit the correct fields with the appropriate OU entry that your US Govt Customer expects before you drop the OpenSSL.cnf file into the d:\I3\IC\Server directory

The extensions to add to a certificate request

[req_distinguished_name] = Country Name (2 letter code)

countryName_default = US

countryName_min = 2

countryName_max = 2

stateOrProvinceName = State or Province Name (full name)

localityName = Locality Name (eg, city)

0.organizationName = Organization Name (eg, company)

0.organizationName_default = U.S. Government

0.organizationalUnitName = Organizational Unit Name 1 (eg, section)

0.organizationalUnitName_default = DoD

1.organizationalUnitName = Organizational Unit Name 2 (eg, section)

1.organizationalUnitName_default = PKI

2.organizationalUnitName = Organizational Unit Name 3 (eg, section)

2.organizationalUnitName_default = CONTRACTOR

commonName = Common Name (eg, YOUR name)

commonName_max = 64

Note: This is where our Certificate Wizard stand-alone UI needs to allow the Customer to configure the CSR Entries like O, OU, CN, Subject Alternative Names, City, State, Country, and so forth with the UI. Please see this link to understand what kind of entries are needed : CSR Tool User's Guide.

Note: If you are using the New stand-alone Wizard-type GUI application to generate Certificate Signing Requests (CSR) this step can be done with ease and less error-prone along with the CSR generation.

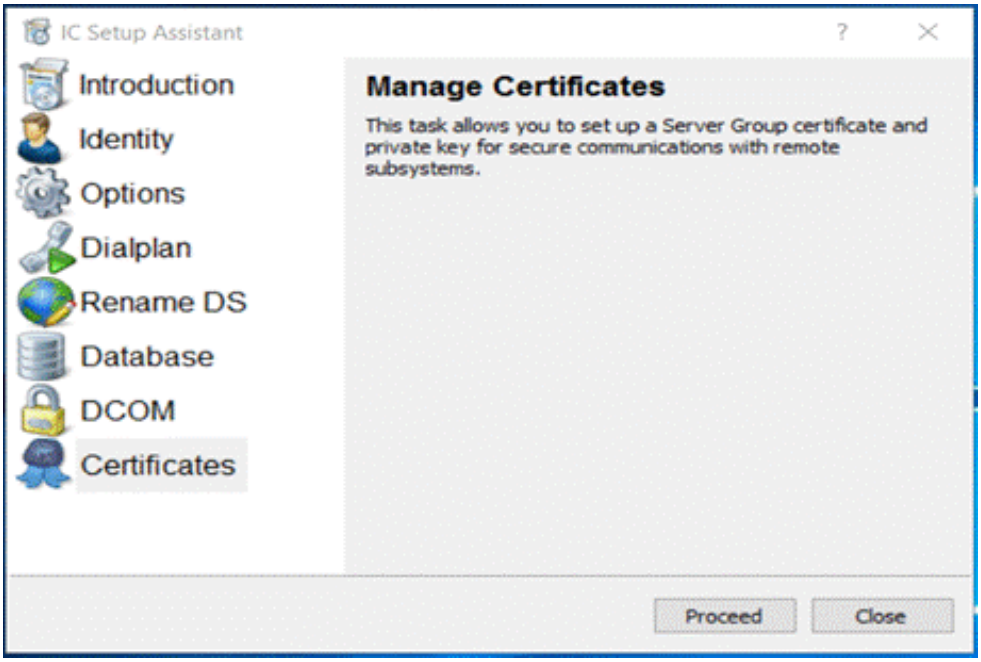
Generating the PureConnect Third Party Certificate for the IC Server

You can create certificate signing requests by using IC Setup Assistant, CSR Generation tool, or the GenSSLCertsU tool. Use this option to use certificates signed by a third-party certificate authority. Creating a certificate signing request creates a certificate signing request file and a private key. Send the file to a certificate authority. Keep the private key to use when you import the signed certificate that you receive from the certificate authority. When you receive the signed certificate from the certificate authority, re-run IC Setup Assistant to import the signed certificate and private key.

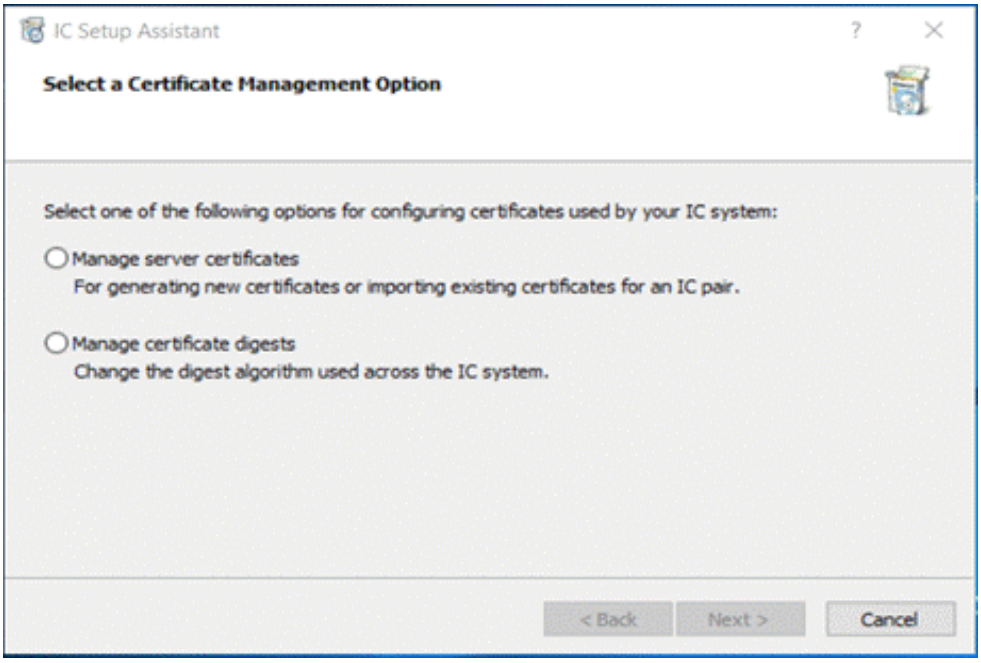
Generating a CSR for the Primary and backup IC Servers

Follow the steps outlined below to generate the Certificate Signing Request (CSR) for the PureConnect IC Server Primary and Backup Servers using the Setup Assistant:

1. Open the IC Setup Assistant, Select **Certificates** and click **Proceed**.

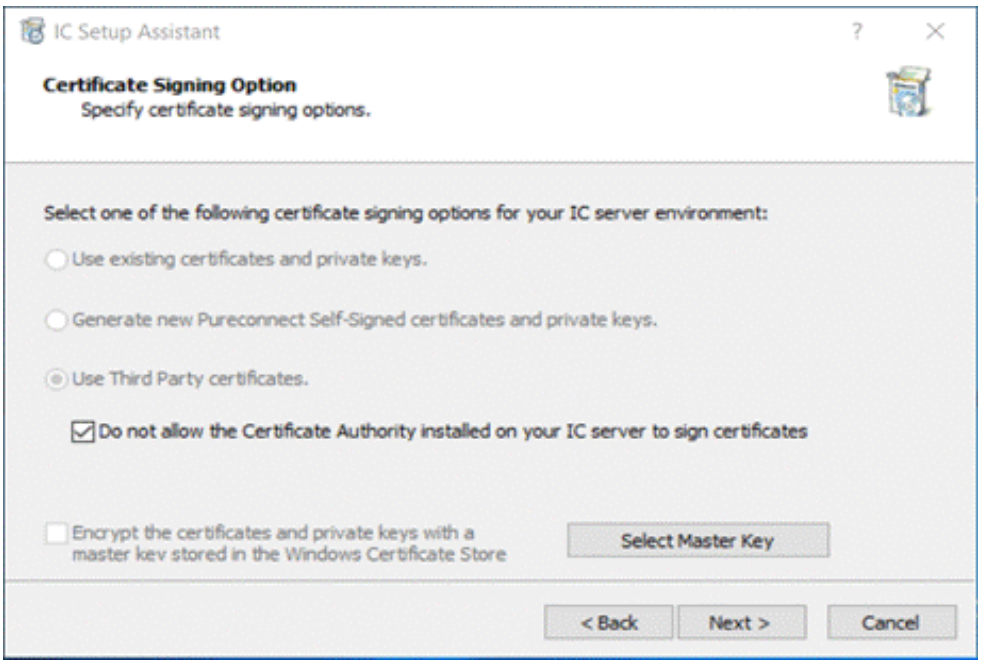


2. Select **Manage server certificates** and click **Next**.

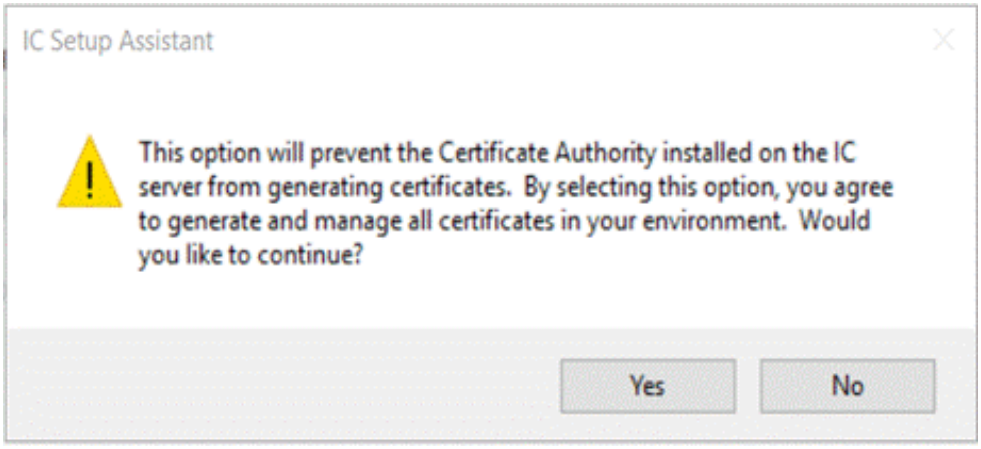


3. Select **Use Third Party Certificates** and ensure the **"Do not allow the Certificate Authority installed on your IC Server**

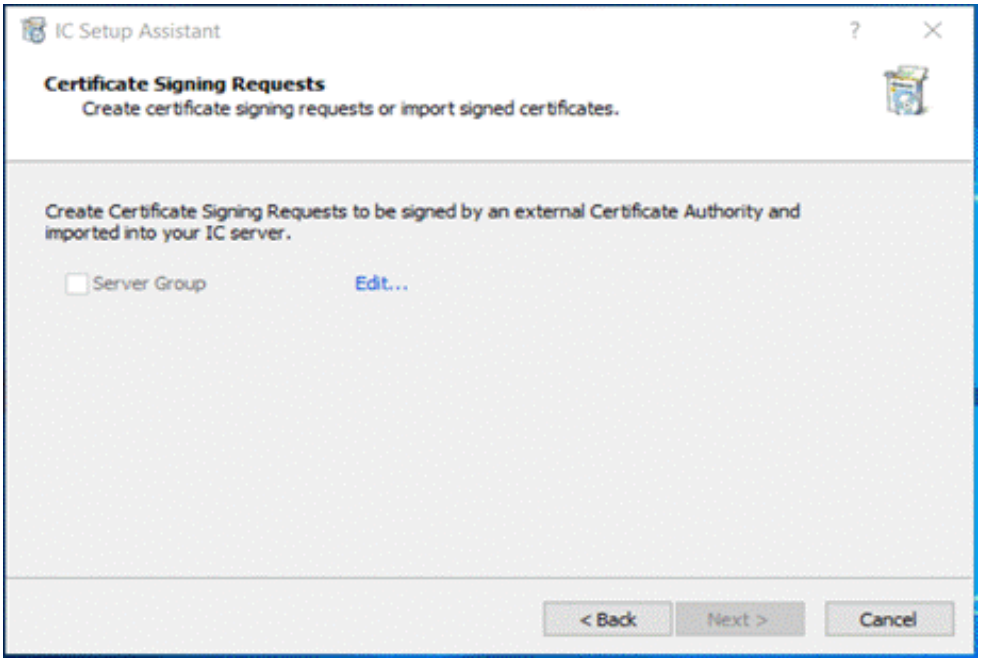
to sign certificates" checkbox is checked.



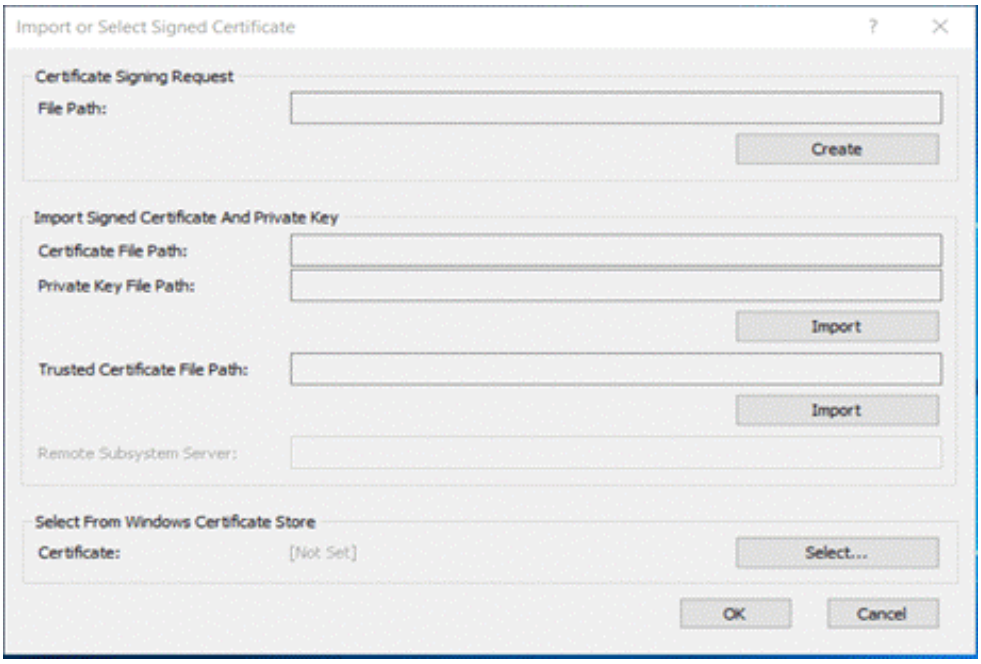
4. You will receive this warning, select **Yes** to continue.



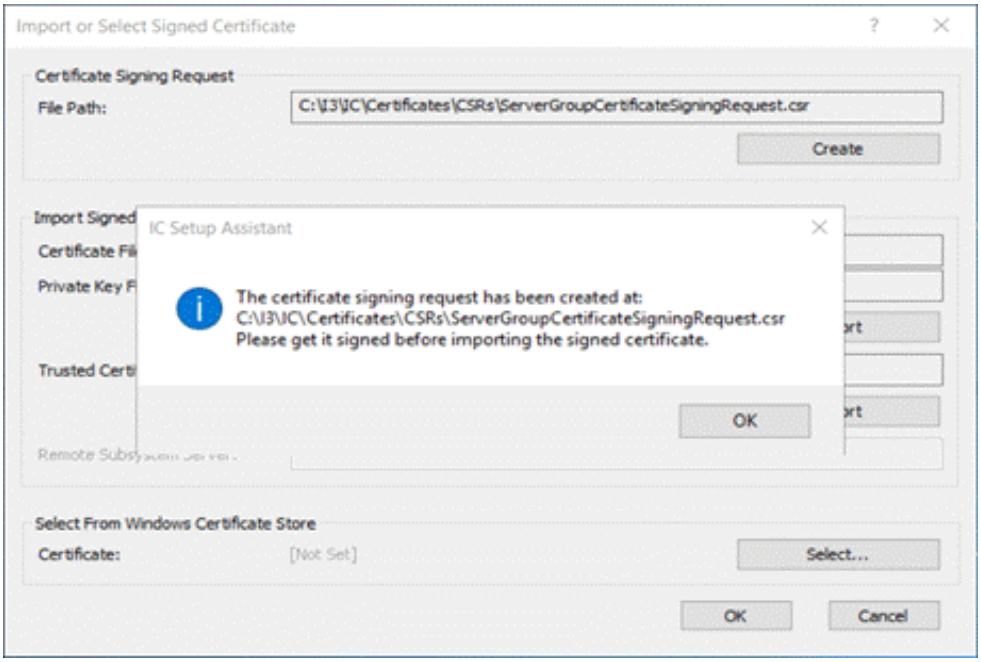
5. Click **ellipsis (…)** box to continue



6. Click **Create** under Certificate Signing Request.



7. Once you see the IC Setup Assistant Warning, click **OK**.

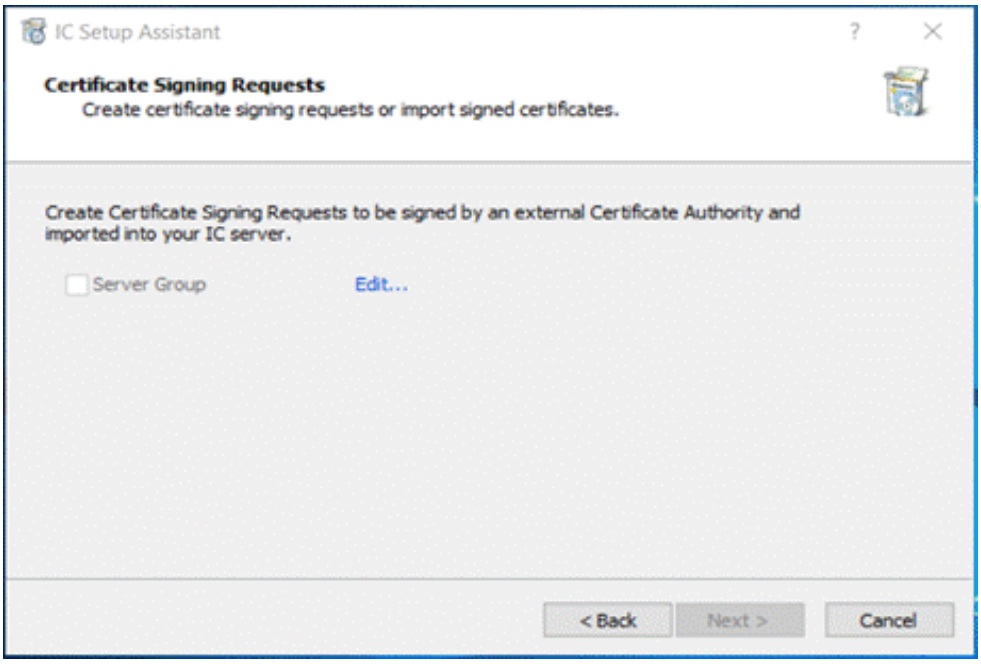


The CSR has been created at this point and there are no additional steps needed, so we will close out and get out of the Setup Assistant Wizard for now. We will return to the Certificate Setup Assistant Wizard later to Import the Signed Certificate.

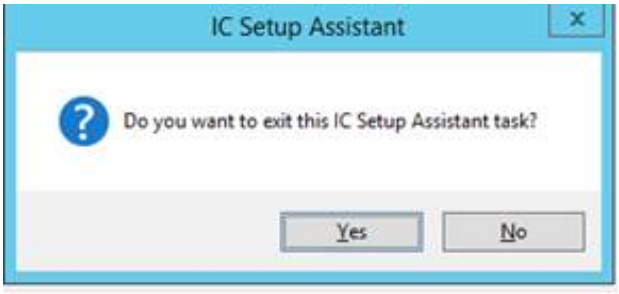
8. Then select **Cancel**.

Note: the location of the CSR is identified in the File Path as shown above. This is the Directory that you will navigate to so that you can get the CSR and send it off to the signing Authority.

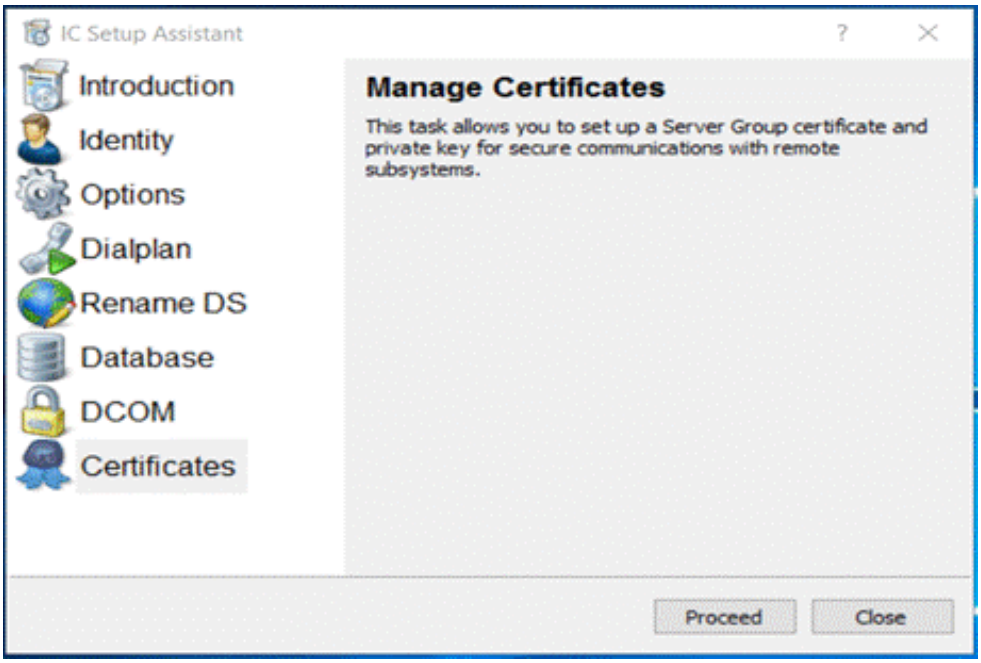
9. Select **Cancel**, again.



10. We will now close the IC Setup Assistant Wizard, so click **Yes**.



11. Click **Close**.

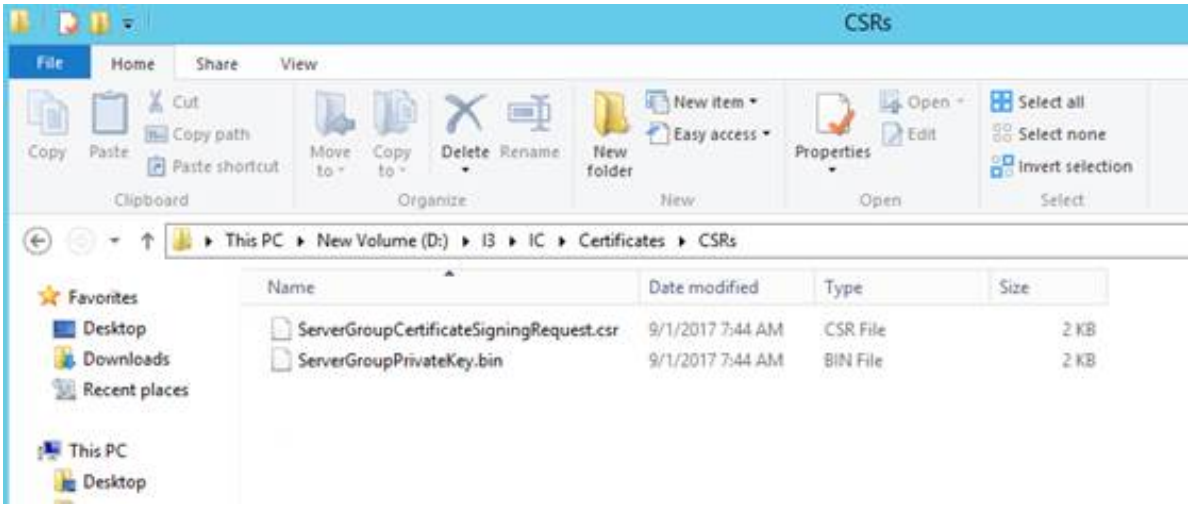


At this point, you will need to send the CSR to the Certificate Signing Authority so that they can sign it.

Validating the PureConnect IC CSR

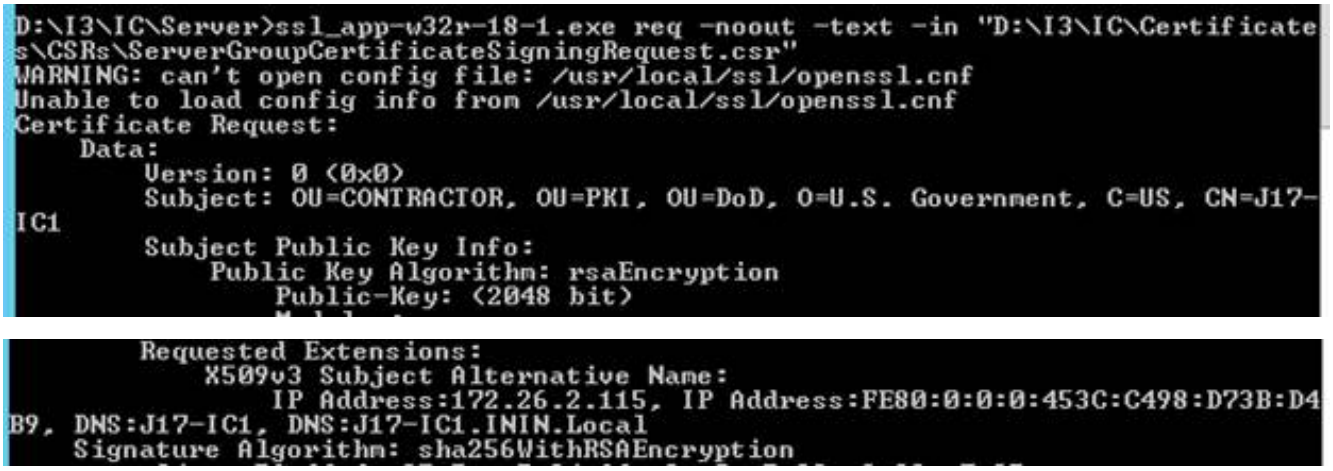
At this Point in time, we need to validate that the CSR has been generated properly with the appropriate data elements as well as any Certificate properties are assigned. Please follow the steps below:

1. Browse to your CSR Location D:\I3\IC\Certificates\CSRs to validate that CSRs have been created.



To validate that your CSRs were generated properly, open a CMD prompt as an administrator and change the path in the command prompt to D:\I3\IC\Server:

2. **Run** the following command to validate the Certificates as shown below:



CMD:

ssl_app-w32r-18-5.exe req -noout -text -in "D:\I3\IC\Certificates\CSRs\ServerGroupCertificateSigningRequest.csr"

Note: The ssl_app-w32r-xx-x.exe version will change with time. So, while running this command check the version and change the cmd accordingly.

The main items that we are reviewing are to ensure that the SubjectAltName(s) IP Address(s), and DNS names are correct as well as any Agency specific OU elements have been created. These will be specific to your organizational requirements.

Once you have validated the CSR and you deem it correct, you can now submit the CSR to the proper Certificate Signing Authority within your organization to get the certificate signed.

Importing the Signed Certificate to PureConnect IC

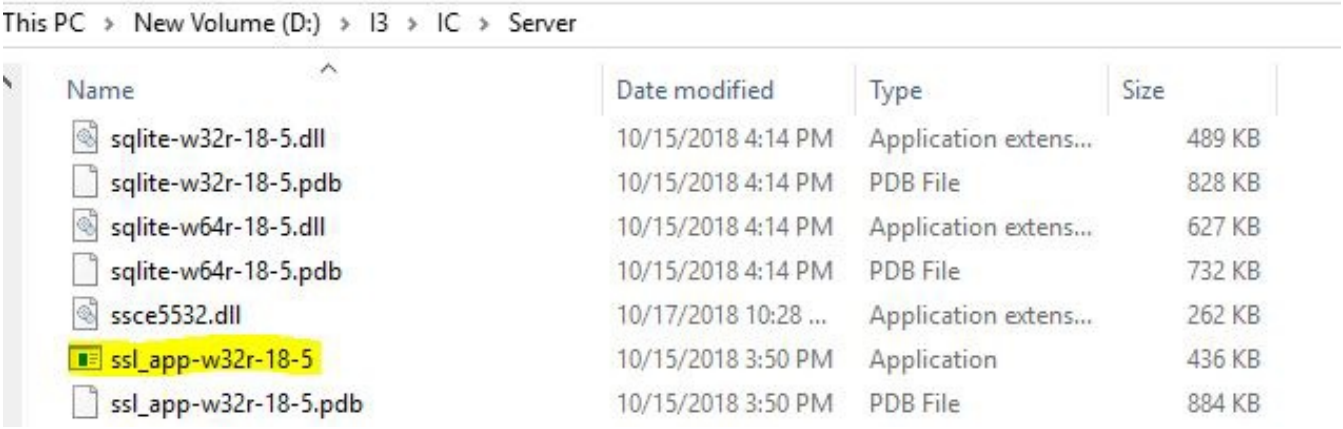
Once you have received the signed certificate, you will paste or copy it back into the folder with your Private Key that was generated during the Certificate Signing Request Process along with the Root CA (Trusted Certificate Authority) Certificate. In this example, we will be using D:\I3\IC\CSRs. We will have to convert the Signed Certificate into .PFX file so that we can import it into the Windows Certificate Store.

Converting the Signed Certificate for Importing

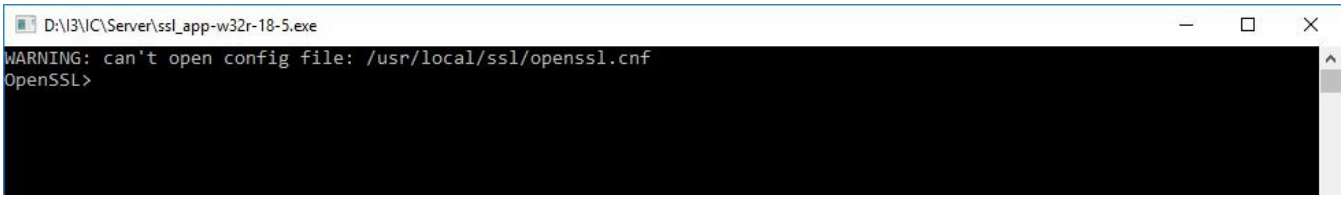
To import and use the Signed Certificate, we will need to convert it into a .PFX format.

1. Navigate to the D:\I3\IC\server directory and locate the "ssl_app-w32-8-5. Exe" file.

   Note: The version of ssl_app_w32r_xx_x.exe may change with time.



2. You will receive a warning that the "openssl.cnf" file cannot be opened, ignore the warning.



3. In the openssl command line, enter the following command:

pkcs12 -export -in "D:\I3\IC\Certificates\CSRs\winstorms1.cer" -inkey "D:\I3\IC\Certificates\CSRs\ServerGroupPrivateKey.bin" -out "D:\I3\IC\Certificates\CSRs\winstorms1.pfx"

```
OpenSSL> pkcs12 -export -in D:\I3\IC\Certificates\CSRs\winstoric2.cer -inkey D:\I3\IC\Certificates\CSRs\ServerGroupPrivateKey
.bin -out D:\I3\IC\Certificates\CSRs\winstoric2.pfx
```

In our example above the name of the certificate and the private key is "winstoric2cer" and "ServerGroupPrivateKey.bin". please use your server names within the Command line

The command line points to the signed certificate so that it can be converted into the .PFX format. If there are any spaces within the directory name, place at the beginning and end of the directory name.

4. Enter a Password, and please note or maintain that password for future use.

```
Enter Export Password:
```

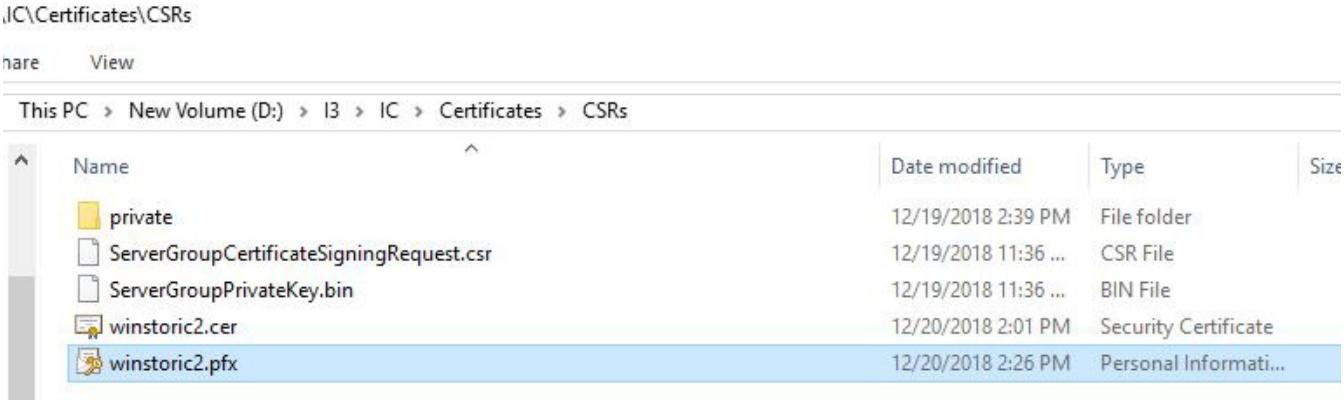
5. Verify Password

```
Verifying - Enter Export Password:
```

6. Conversion completed:

```
OpenSSL> pkcs12 -export -in D:\I3\IC\Certificates\CSRs\winstoric2.cer -inkey D:\I3\IC\Certificates\CSRs\ServerGroupPriva
teKey.bin -out D:\I3\IC\Certificates\CSRs\winstoric2.pfx
Enter Export Password:
Verifying - Enter Export Password:
OpenSSL>
```

7. Check the .PFX file:

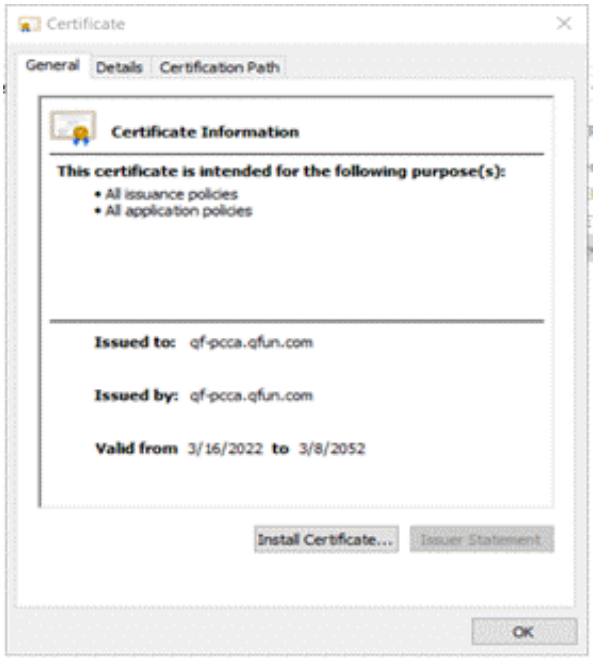


Importing the Signed Certificate and Root CA Certificate into the Windows Certificate Store

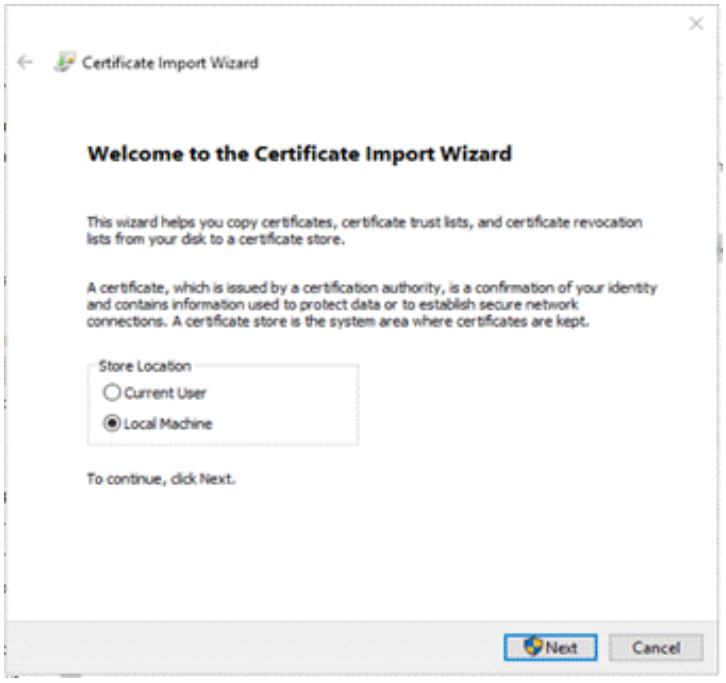
Importing Root CA

Now you will import the Root CA (Trusted Certificate Authority) Certificate into the local server's Windows Certificate Store.

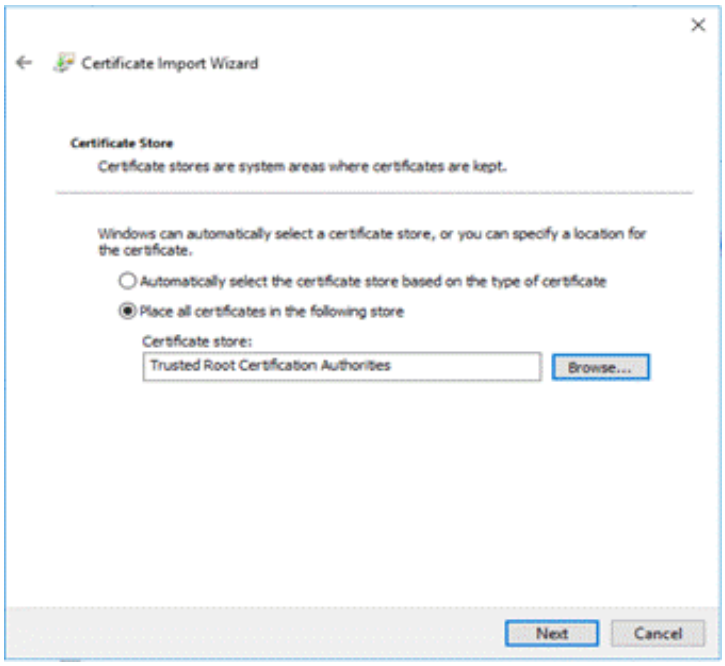
1. Navigate to the D:\I3\IC\Certitifcates\CSR directory and locate the Root CA Certificate you have copied from CA.
2. Double Click on the file.
3. Select **Install Certificate...** from the Certificate.



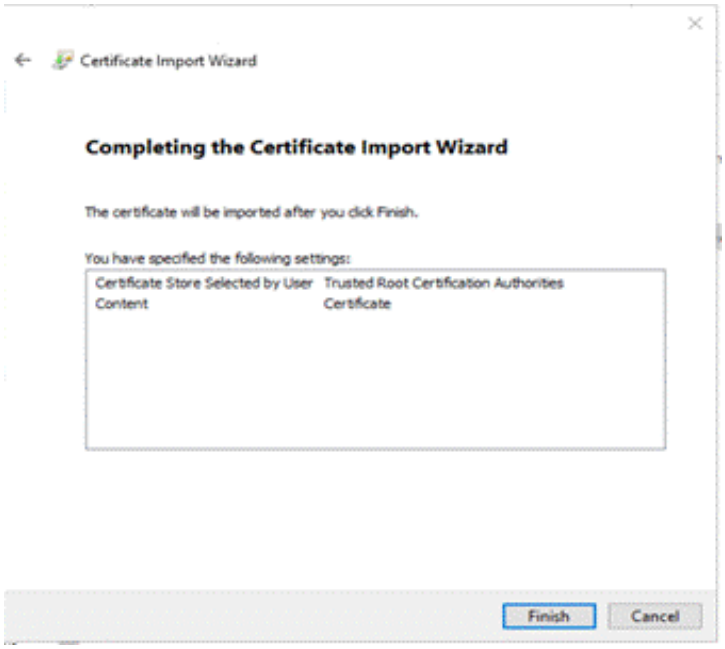
4. A new window appears, select **Local Machine** radio button and click **Next**.



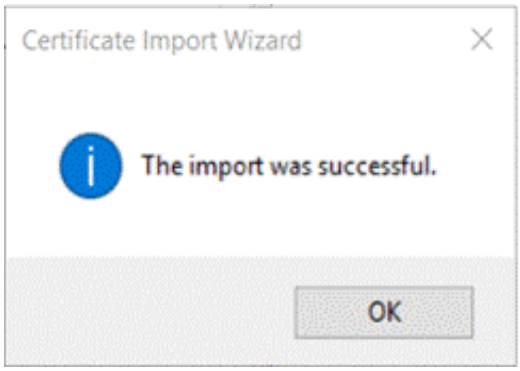
5. Select **Place all certificates in the following store** and select **Trusted Root Certification Authorities** from the list.



6. Click **Next**.
7. Completing the Import, verify that you have imported the correct Certificate and select **Finish**.



8. After the successful import, select **OK** to close the window.

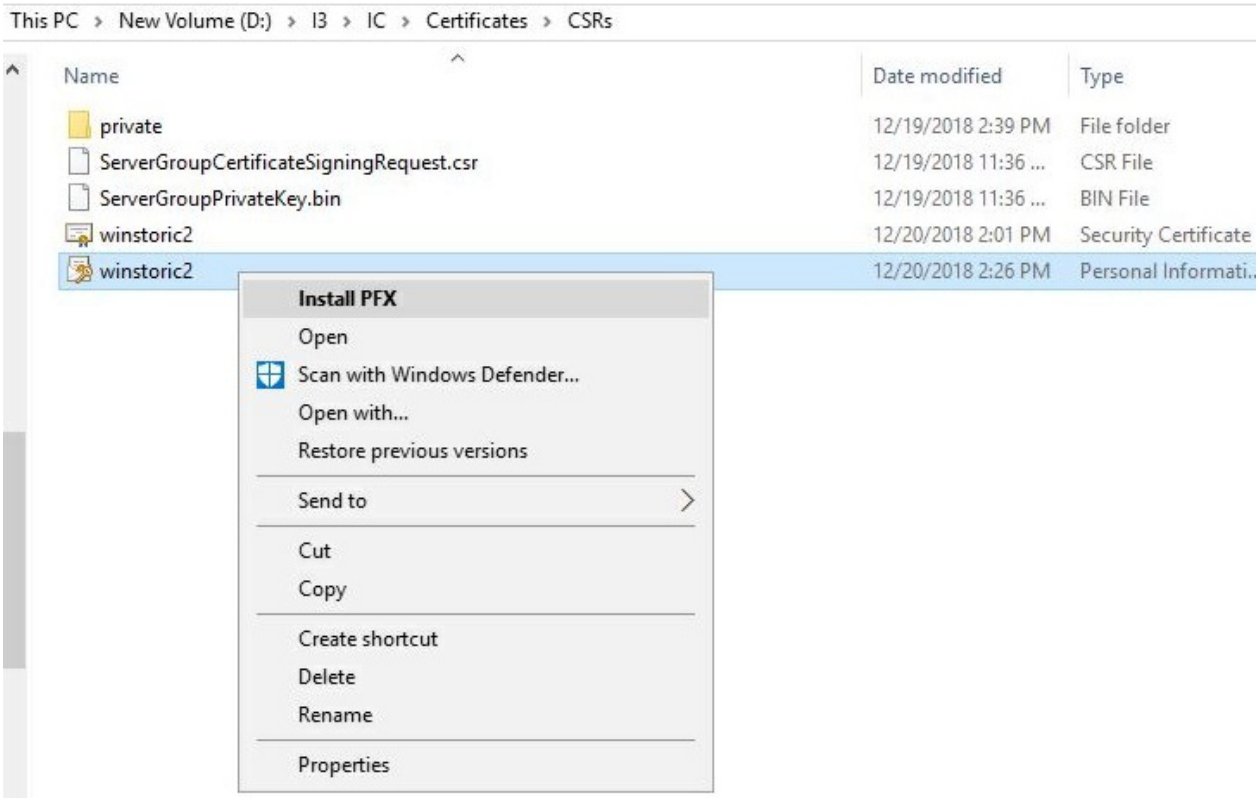


Importing Signed Certificate

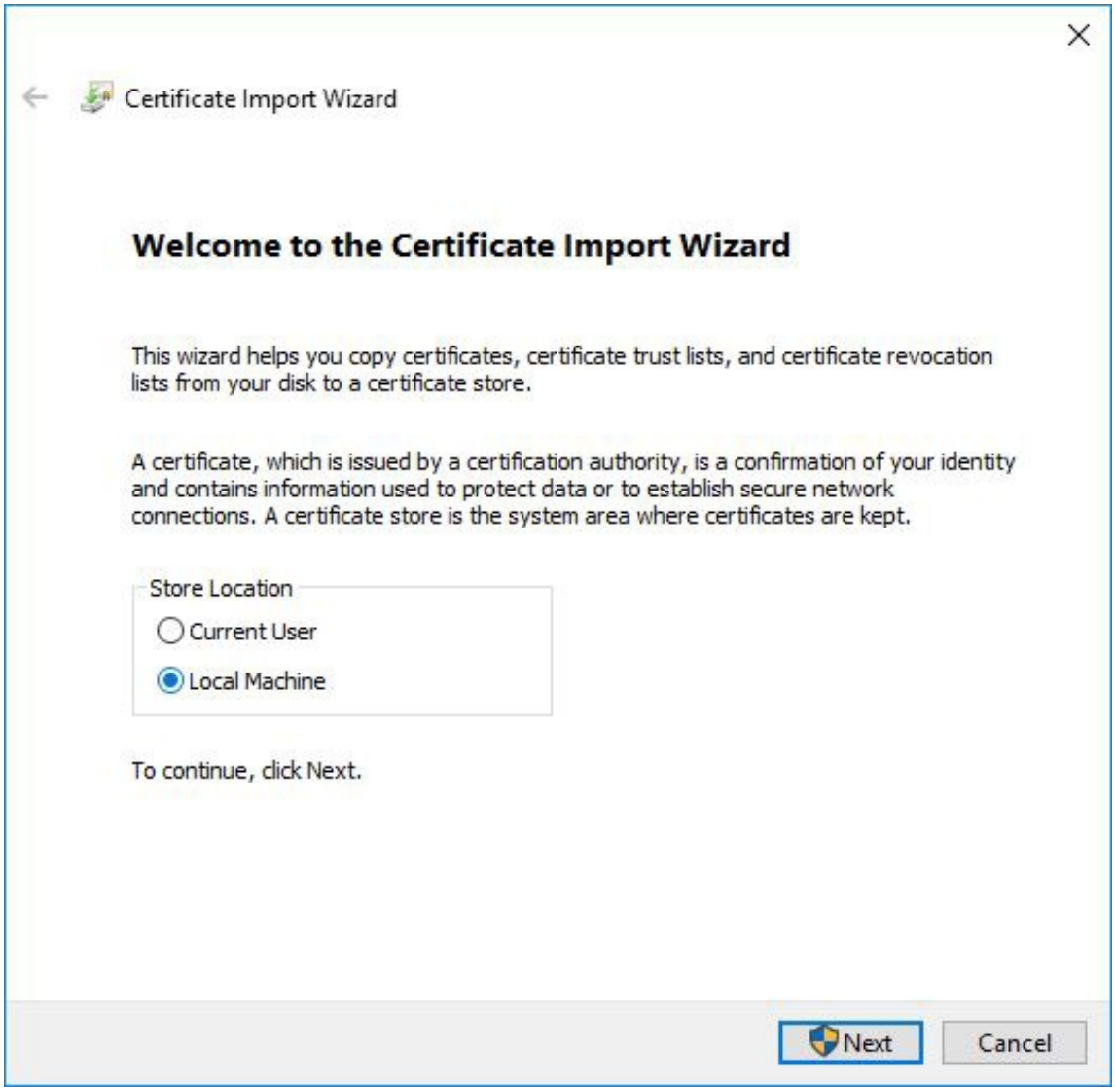
The Signed Certificate has been converted into .pfx, now you will import the Certificate.PFX into the local server's Windows Certificate Store.

1. Navigate to the D:\I3\IC\Certitifcates\CSR directory and locate the newly created .pfx file that you perform in the previous steps.

2. Right click on the file, in our example we right-clicked on the "winstoric2.pfx" file.

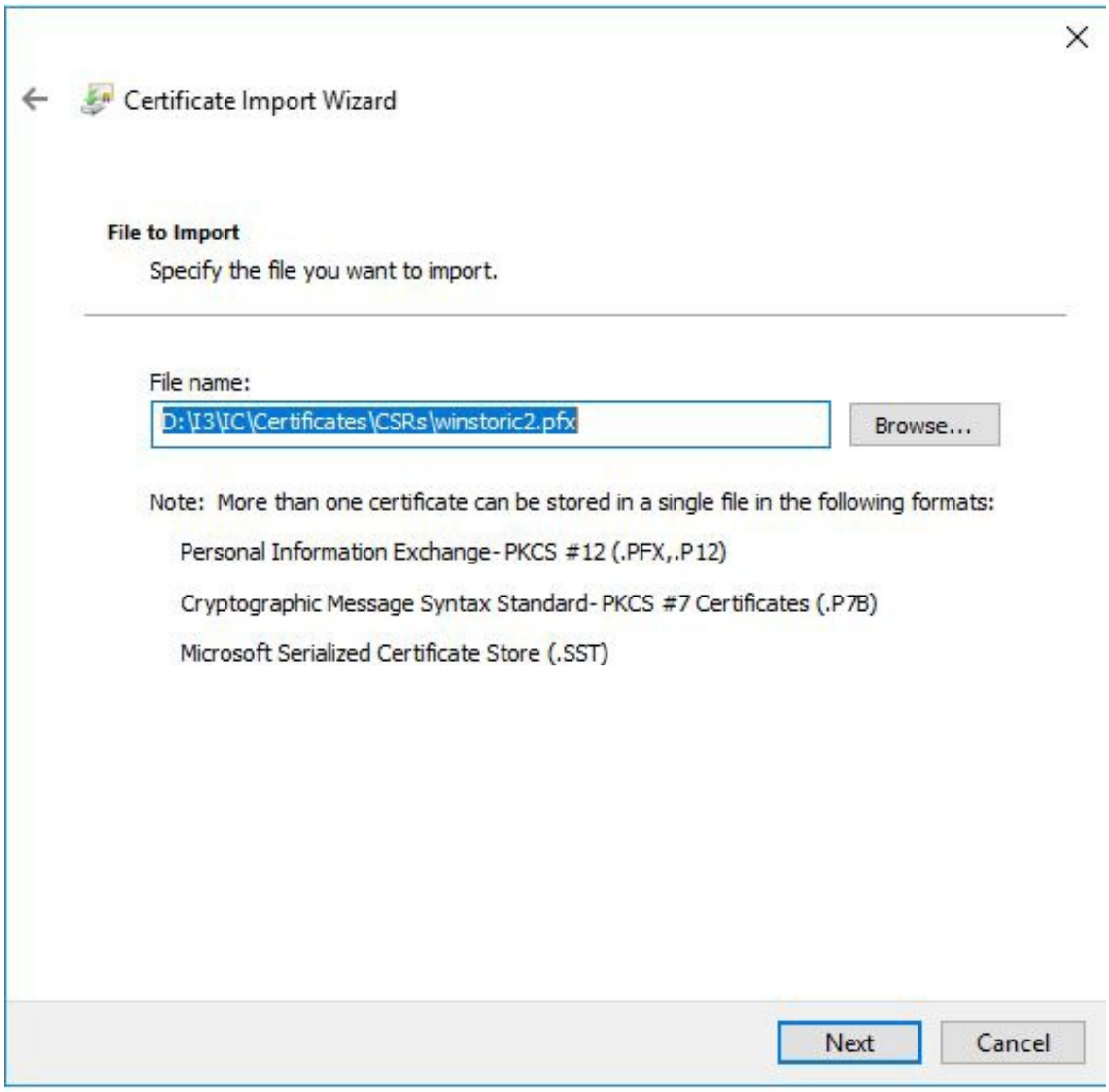


3. Select **Install PFX** from the menu.
4. A new window appears, select **Local Machine** radio button.

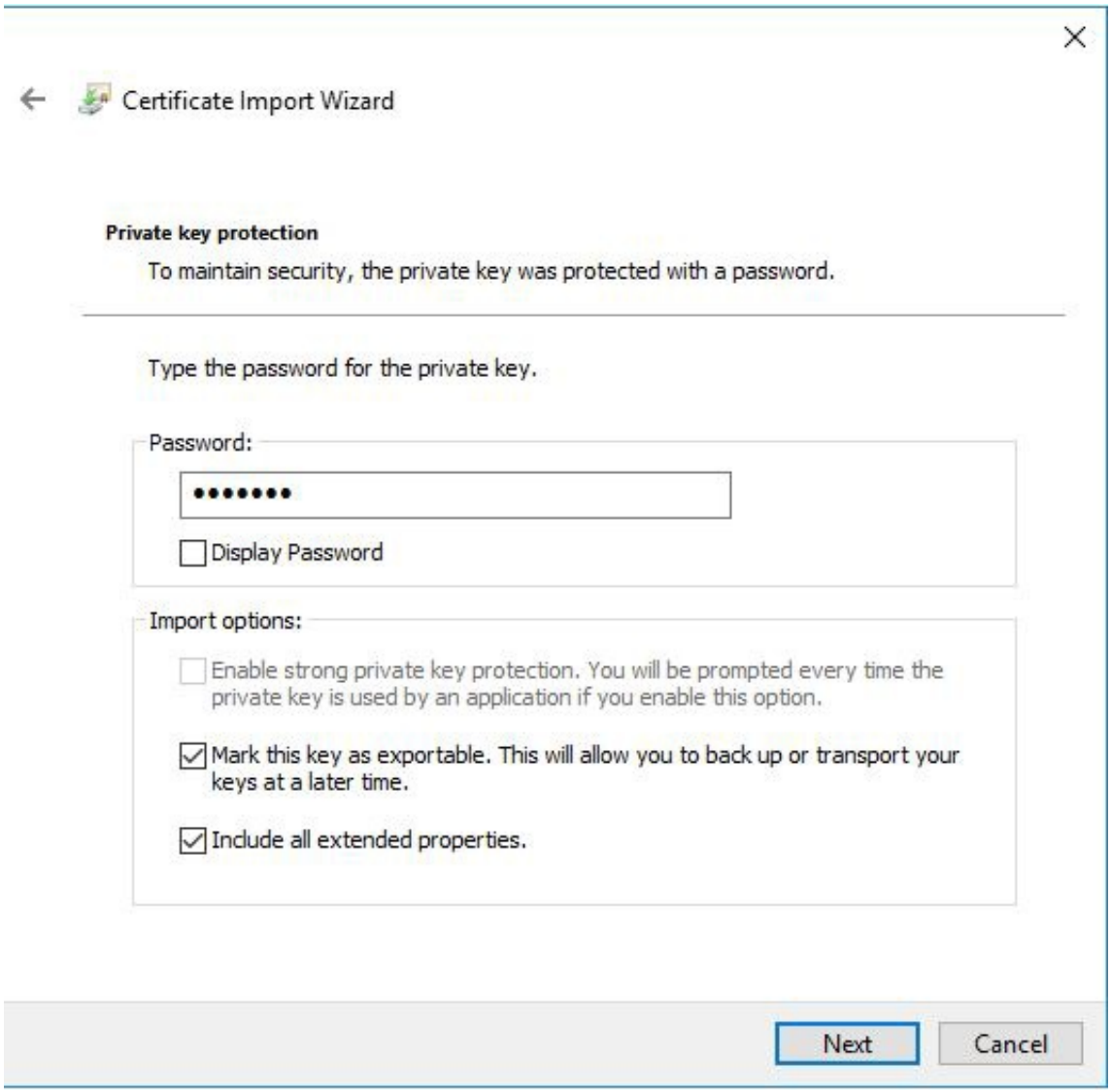


5. Click **Next**.

6. Browse and specify the file you want to import and click **Next**.

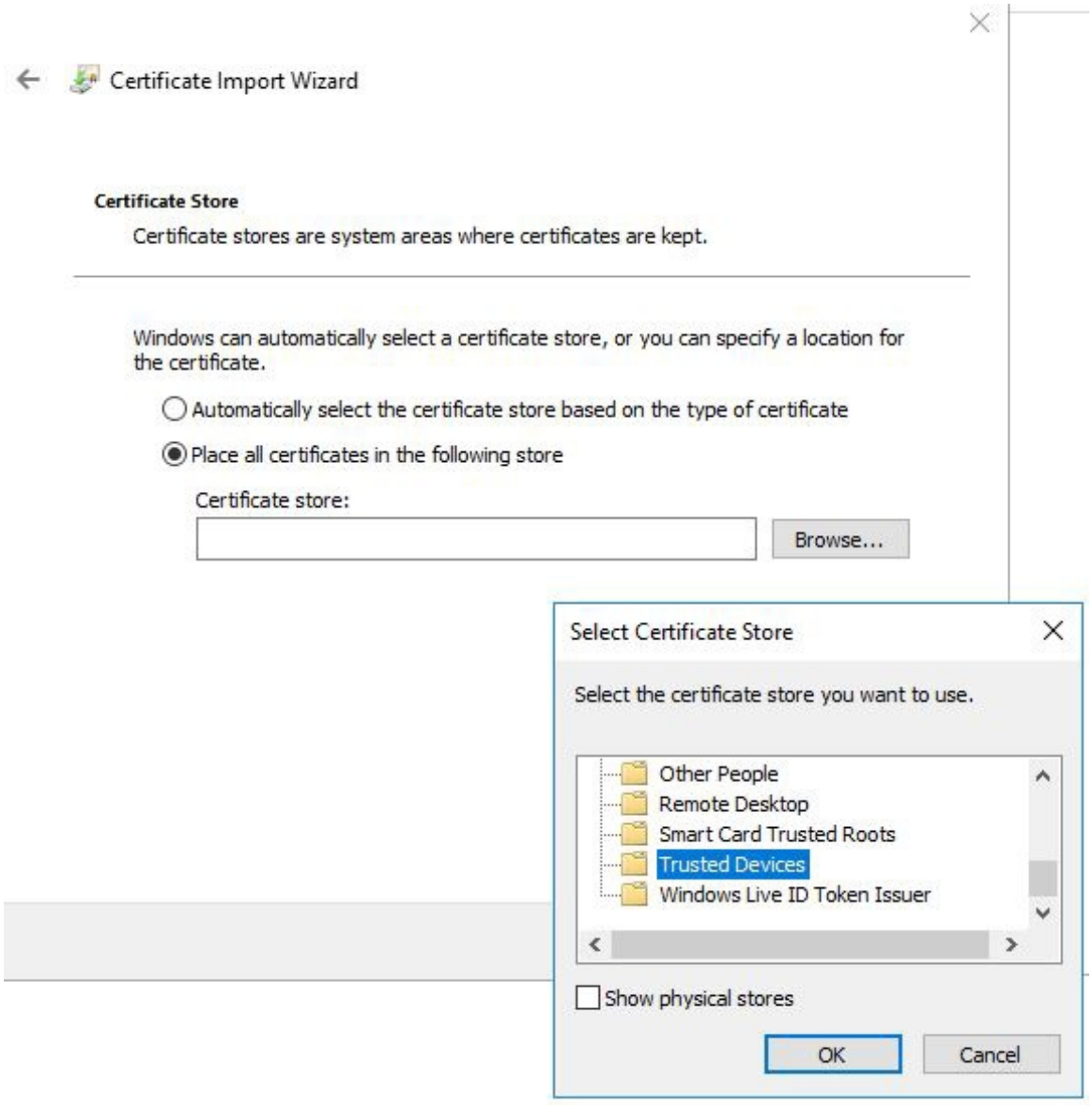


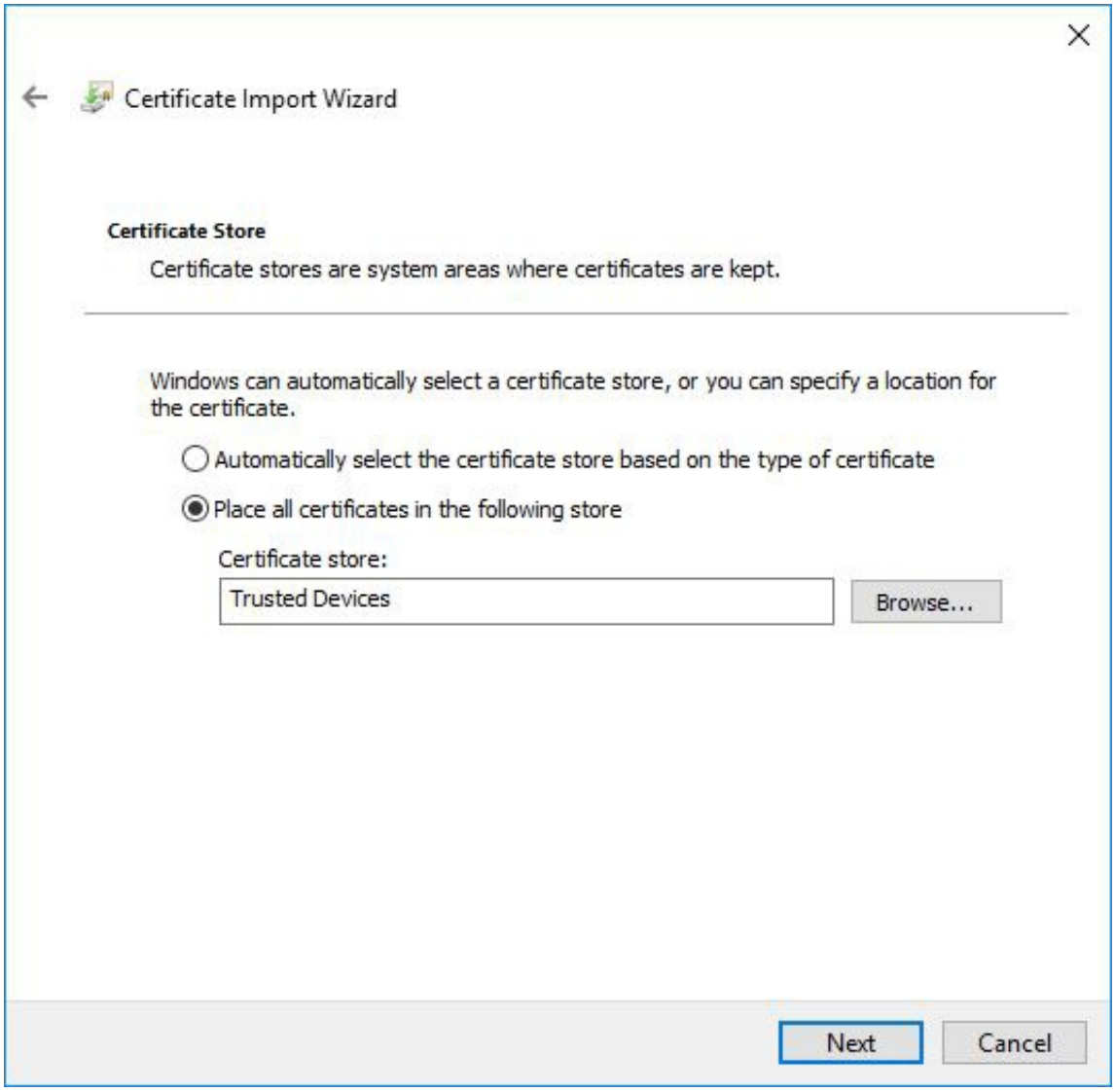
7. Enter the password, which was created in the step 4 of section *"Converting the Signed Certificate for Importing"* .



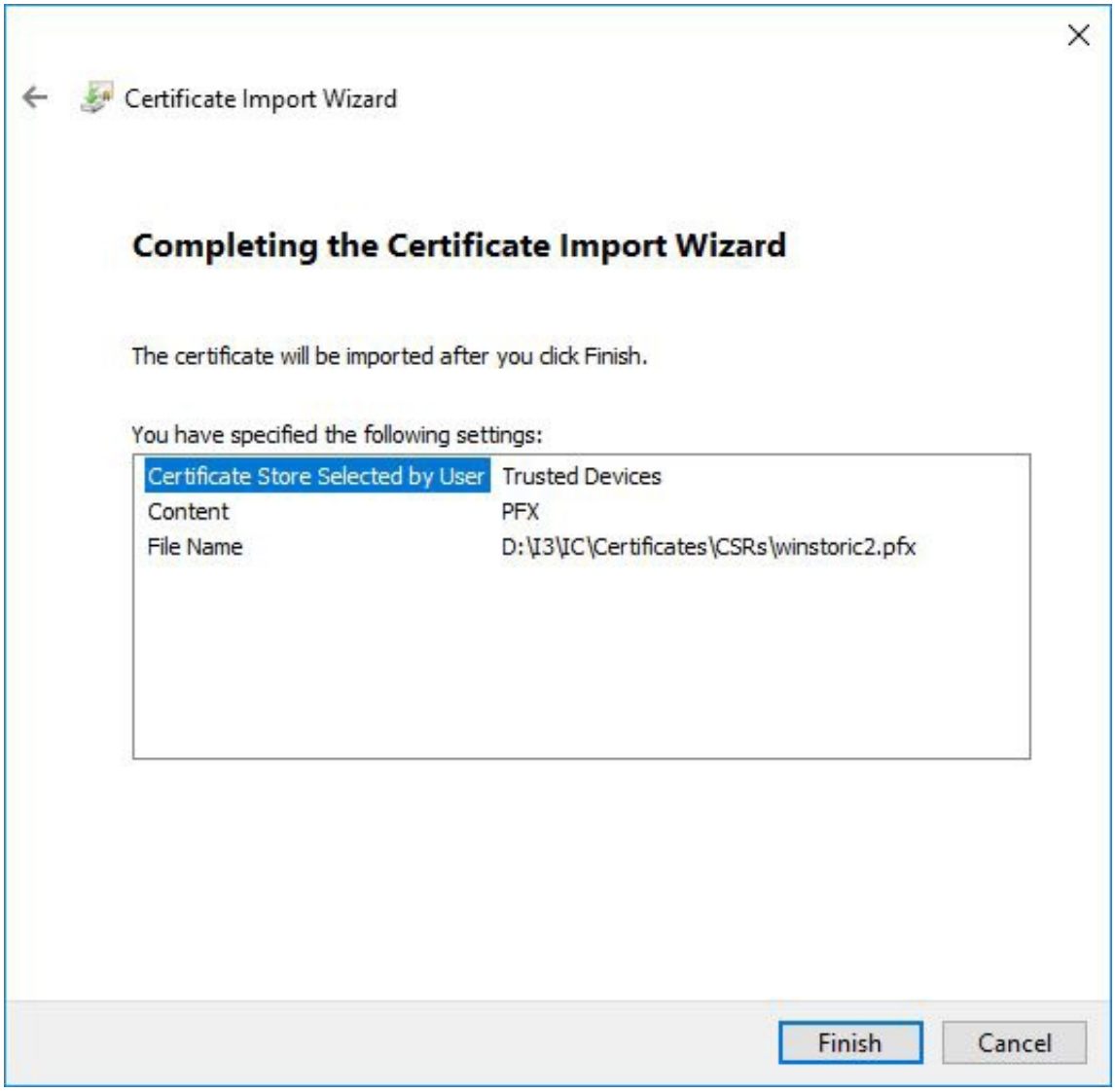
Note: you must mark this certificate as exportable or the PureConnect application cannot use or register with this certificate. Please mark the extended properties checkbox as well.

8. Select **Place all certificates in the following store** and select **Trusted Devices** area.

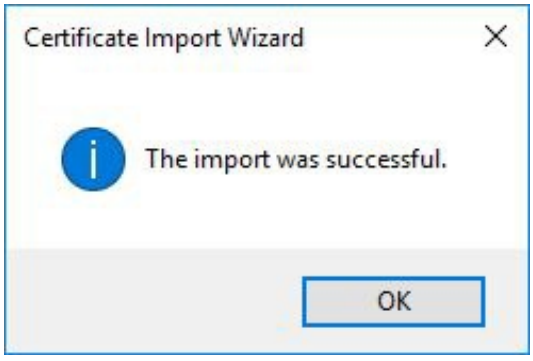

Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
Select Certificate Store
Select the certificate store you want to use.
Other People
Remote Desktop
Smart Card Trusted Roots
Trusted Devices
Windows Live ID Token Issuer
Show physical stores
OK
Cancel



9. Completing the Import, verify that you have imported the correct Certificate and select **Finish**.



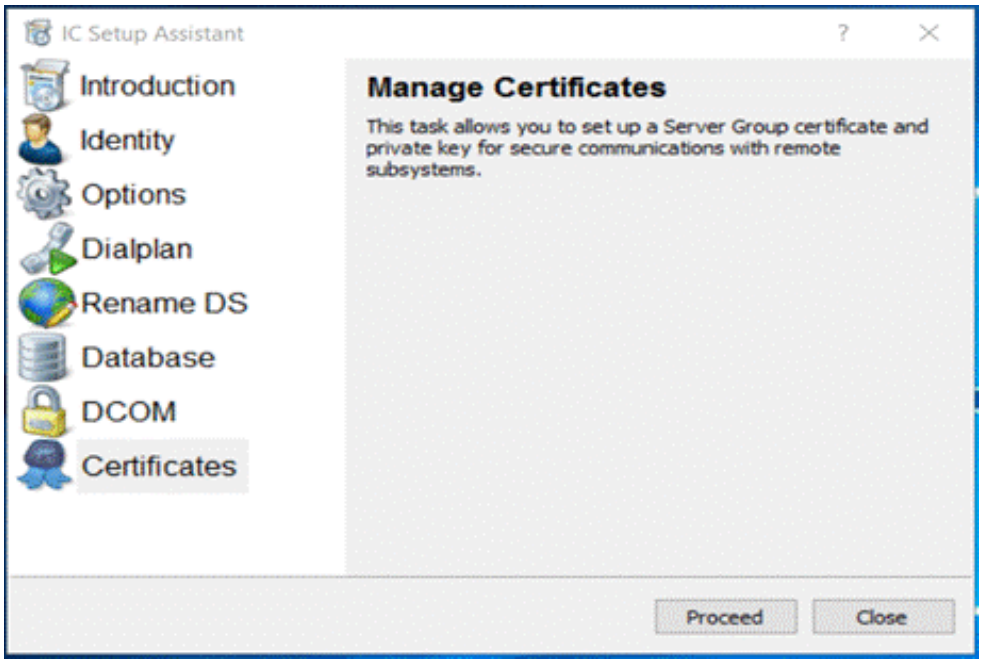
10. Completing the Import, verify that you have imported the correct Certificate and select **Finish**.



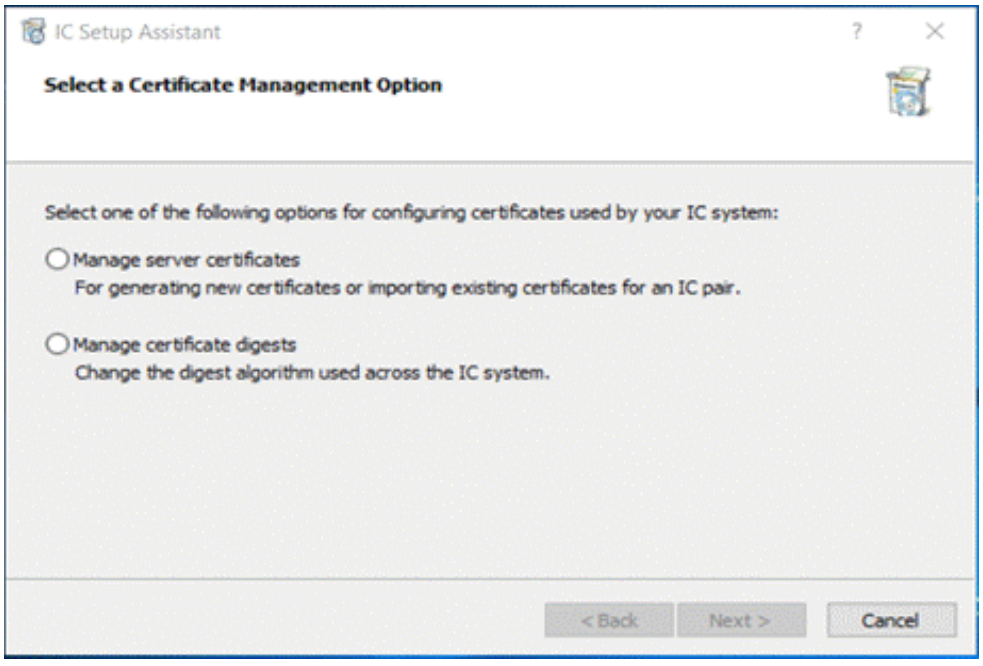
Importing the PureConnect Certificate from the Windows Certificate Store into the PureConnect

We will now import the signed certificate file that is in the Windows Certificate Store so that the PureConnect Server can register the application to the Certificate.P lease follow the directions below to complete the Import process.

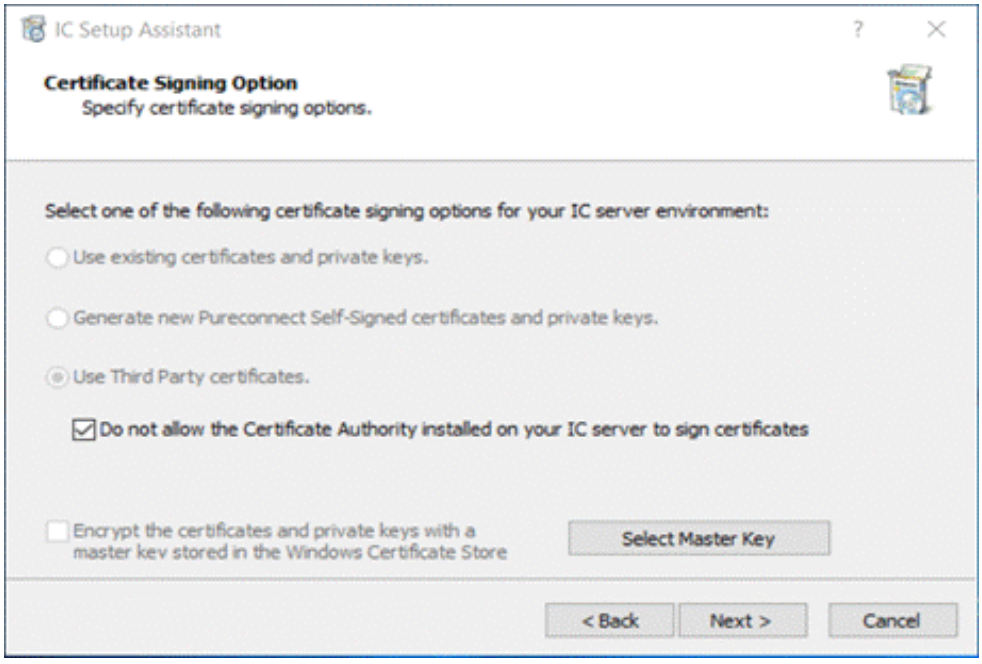
1. Open IC Setup Assistant, Select **Certificates** and click **Proceed**.



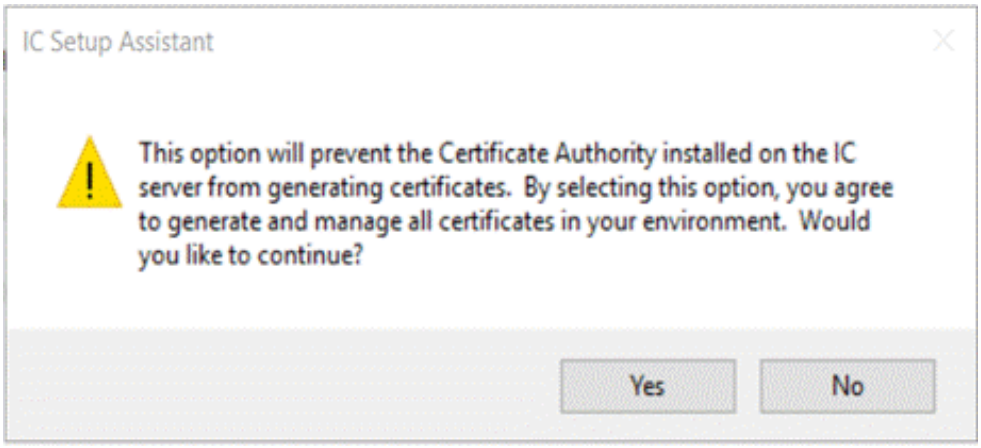
2. Select **Manage server group certificates** and click **Next**.



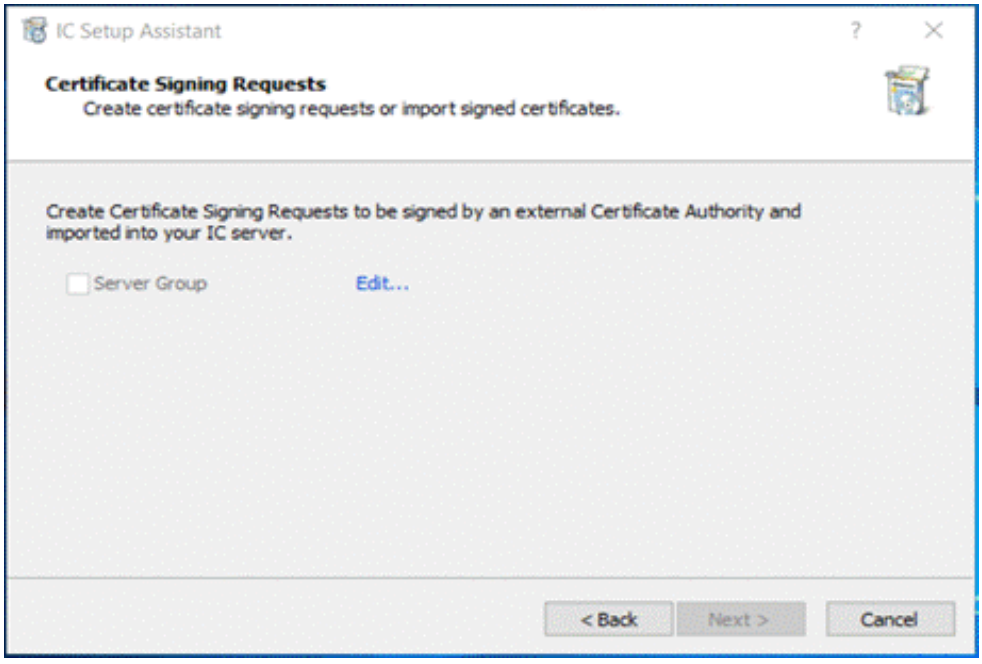
3. Select **Use Third Party certificates** and ensure the **"Do not allow the Certificate Authority installed on your IC Server to sign certificates"** checkbox is checked.



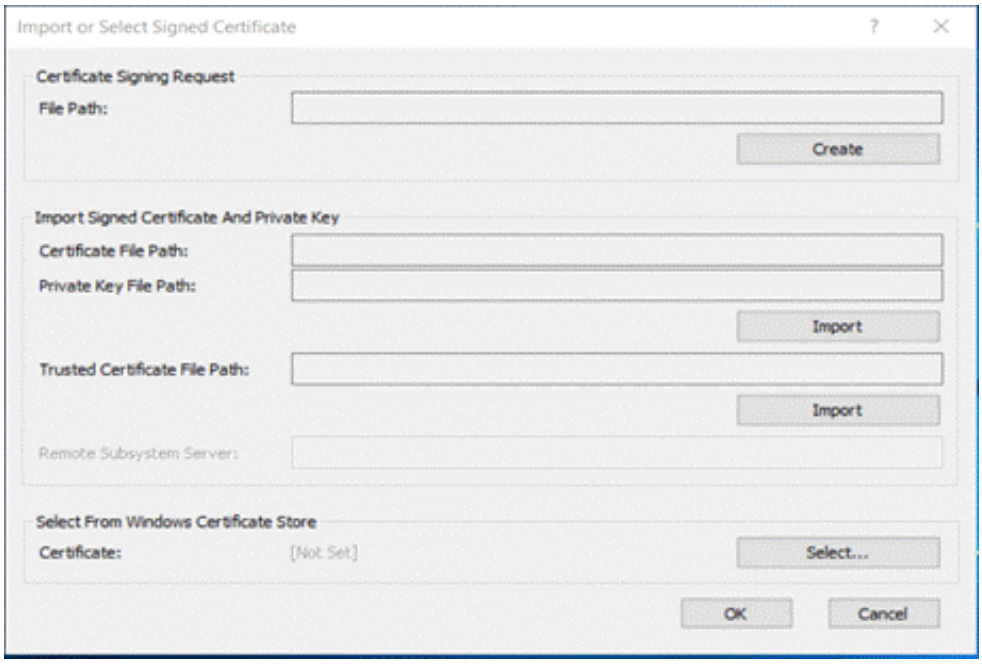
You will receive this warning, select **Yes** to continue.



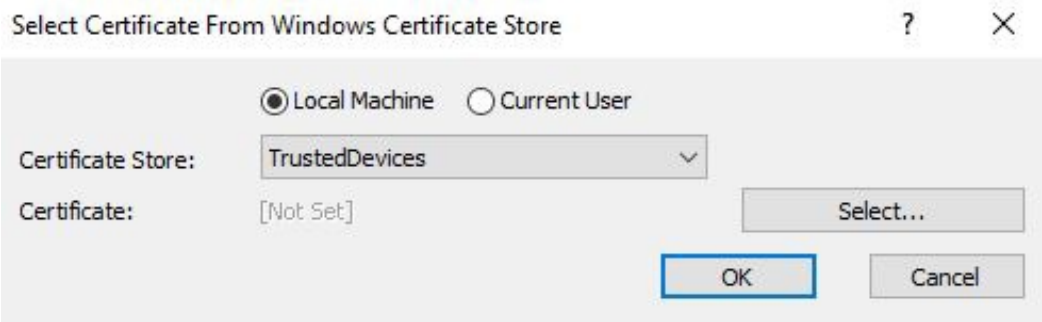
4. Click on the **ellipsis (…)** box to continue.



5. In the **Import or Select Signed Certificate** windows, choose the **"Select"** box under the **Select from Windows Certificate Store** option.

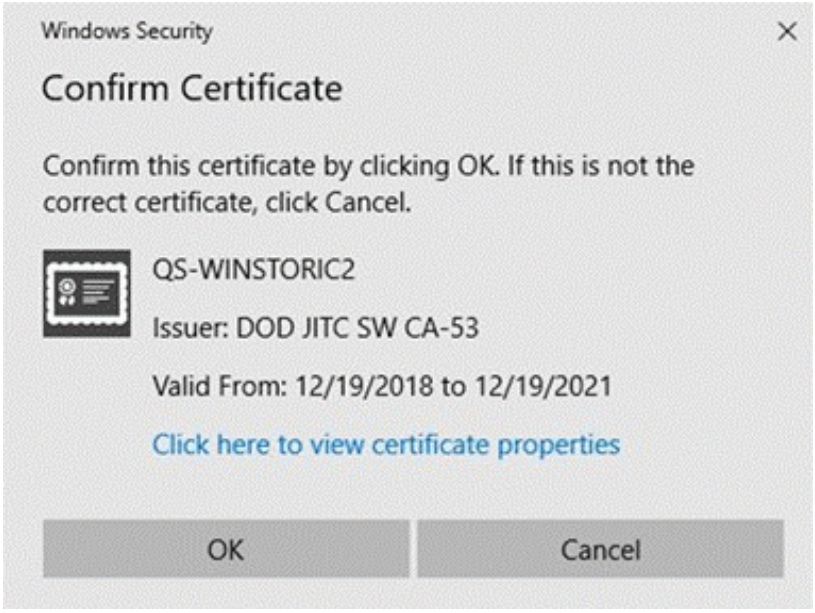


6. Select the **Local Machine** radio button and then choose the **TrustedDevice** option in the pull down arrow.



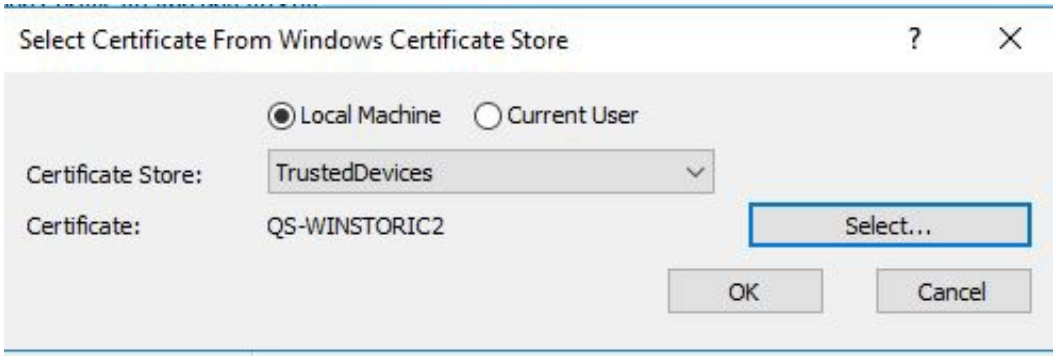
7. Click **Select** .

The Confirm Certificate window will appear, make sure that the correct Certificate is chosen. In our case it will be the “QS-Winstoric2” certificate that we placed in the Windows Store in earlier procedures.



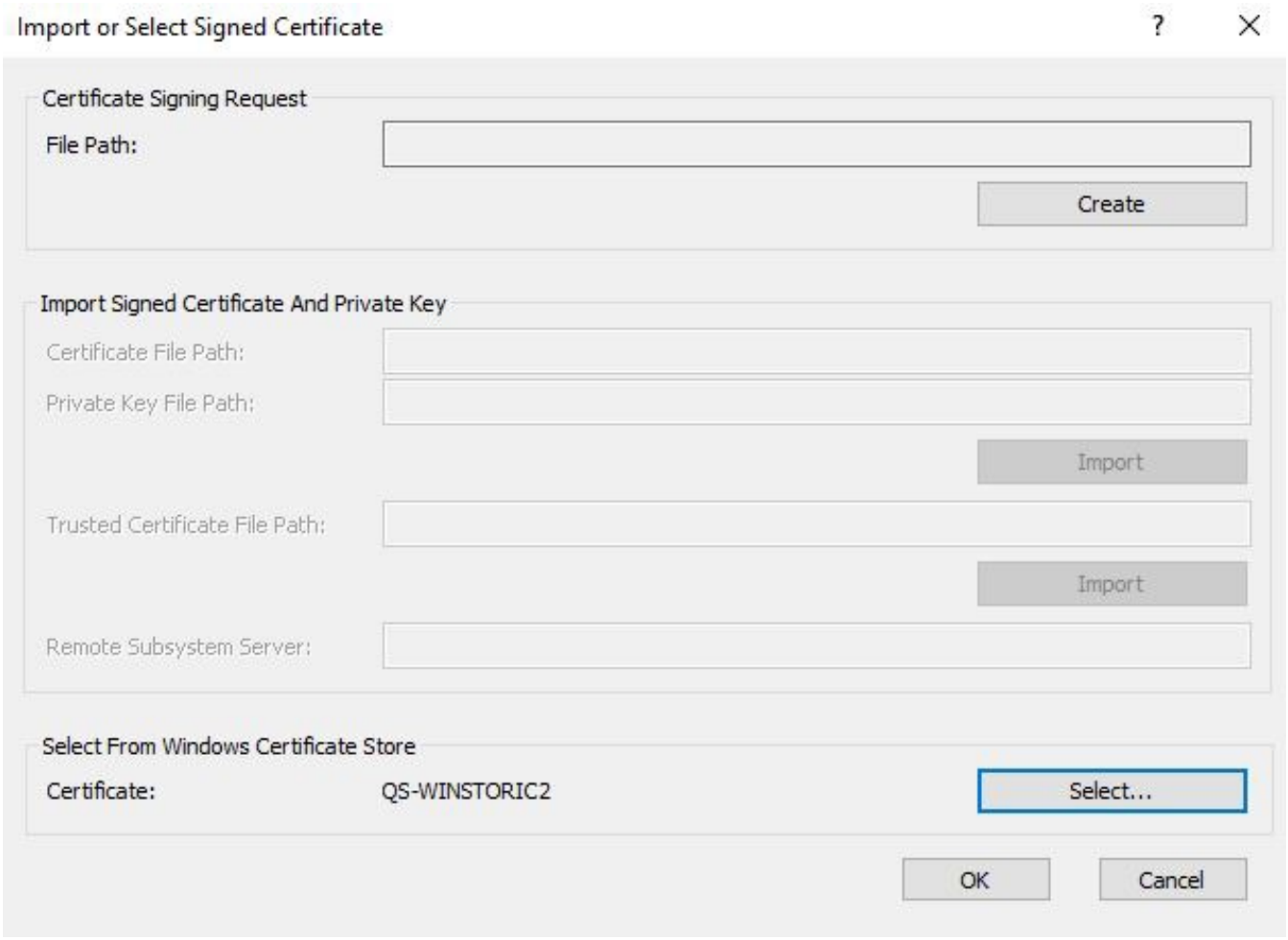
8. Select **OK.**

The next window will pop up and it wants you to validate that you have chosen the certitifcate you want. In our case the QS-Winstoric2 name appears in the Certificate Field as shown in our example below:

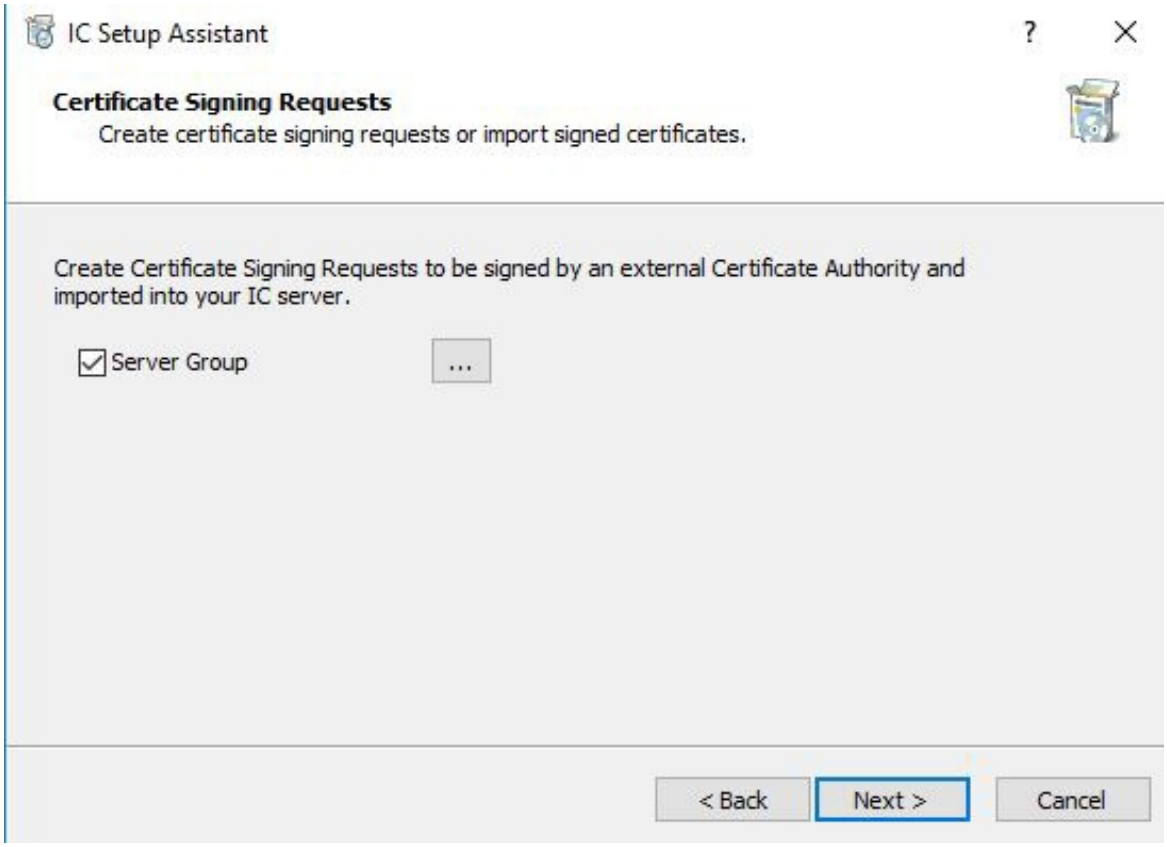


9. Click **OK** .

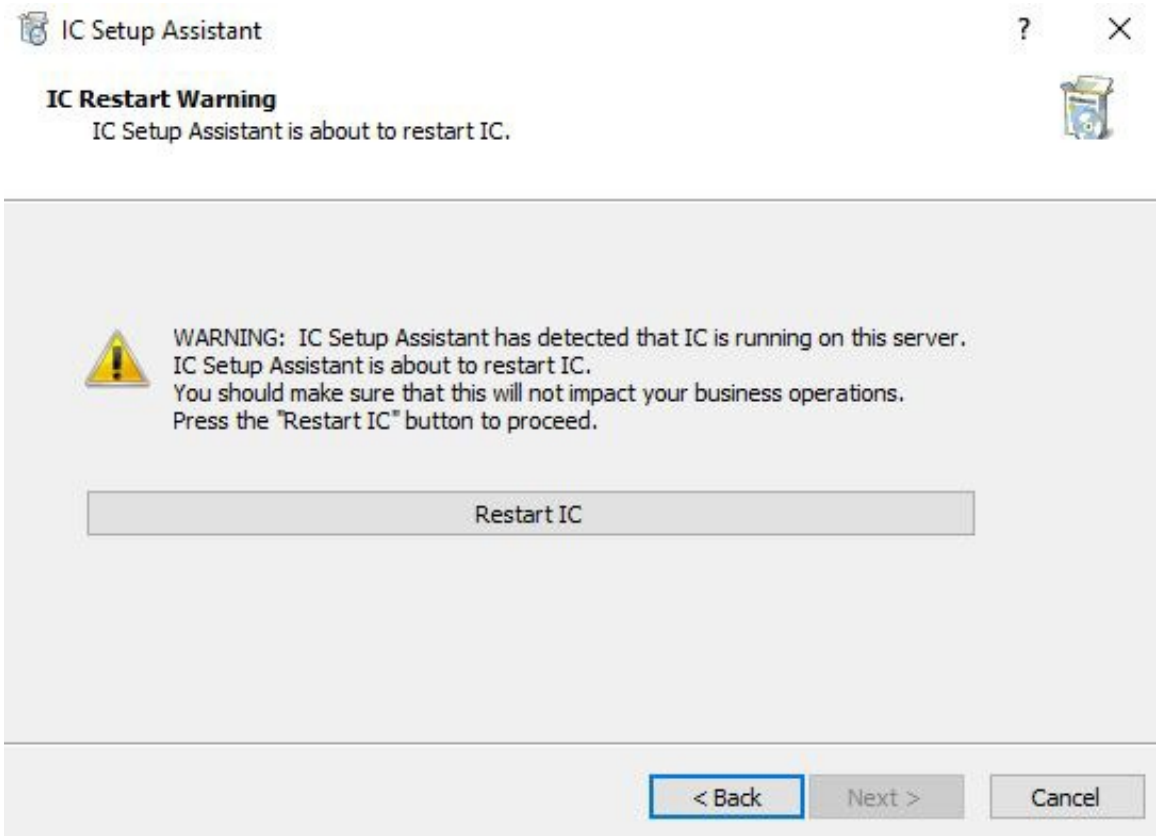
The “QS-Winstoric2” now shows up in the “Select From Windows Certificate Store” Certificate field as shown below:



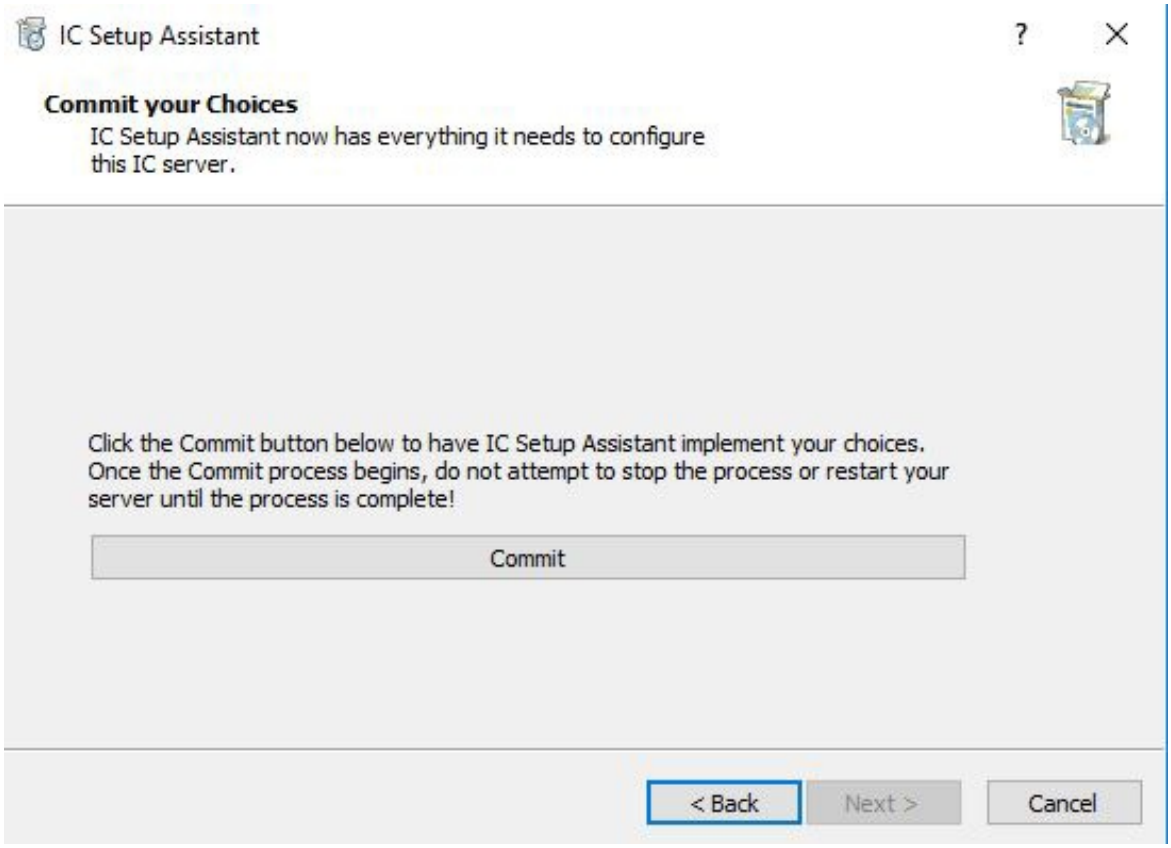
10. Select **Next** to return the the the beginning of the Wizard.



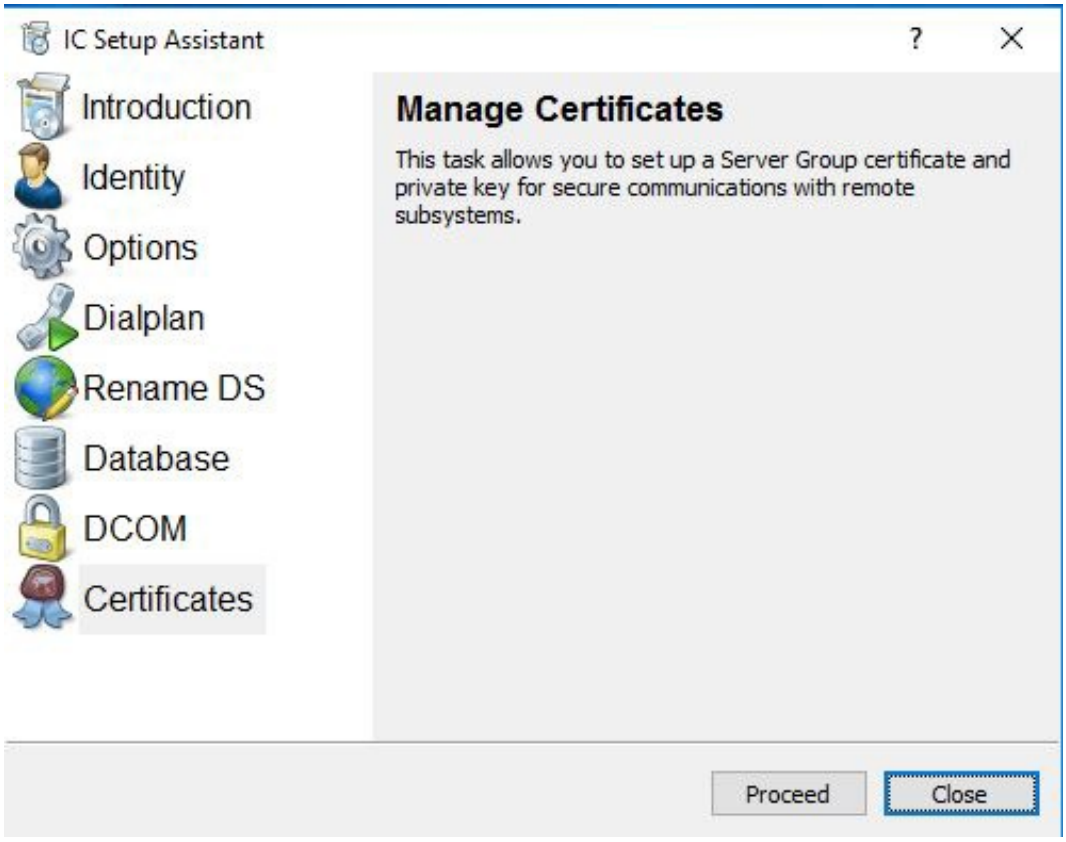
11. Select **Restart IC**.



12. Select **Commit**.



The certificate process will run and once completed select **Close** and you will have the option to start the Interaction Center Service now or at a later time.



13. Reboot the IC Server once to validate that the IC Server Service starts.

Backup IC Server Configuration with Third-Party Certificates

1. Copy the Private Key used for IC Primary Server to the Backup IC Server.

2. Go to the Backup server and do the same steps mentioned for IC Server. But while Creating CSR, use the same Private Key used for IC Primary Server for SSO with Third-Party Certificates.

Note: Please refer to the CSR Tool User's Guide for using the existing private key for the CSR Generation.

3. Reboot the Backup IC Server.

4. Check to see if the IC service started.

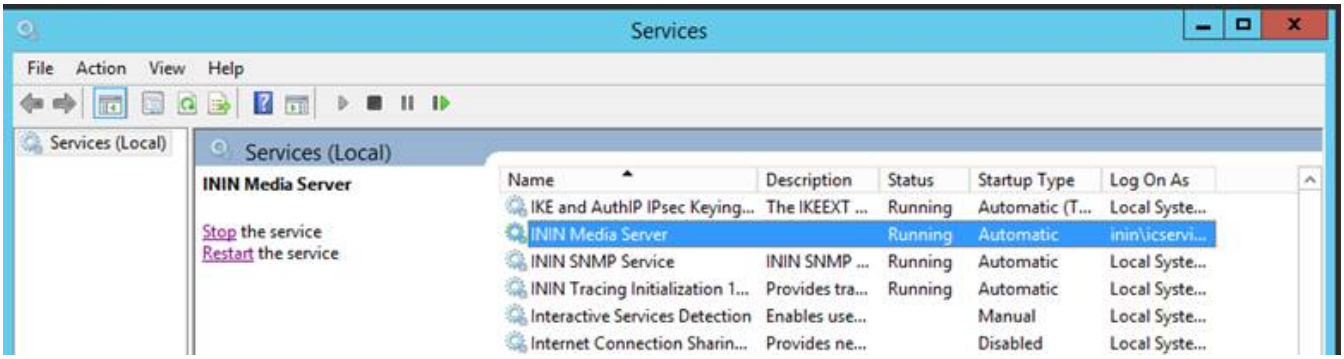
> WARNING:
>
> Each time you perform an install or add an IC option, the I3 system generates new Certificates that will override your Certificates. You may over-write your good working certificates.
>
> Always, maintain a backup copy of the IC Certificate folder after you have a working system

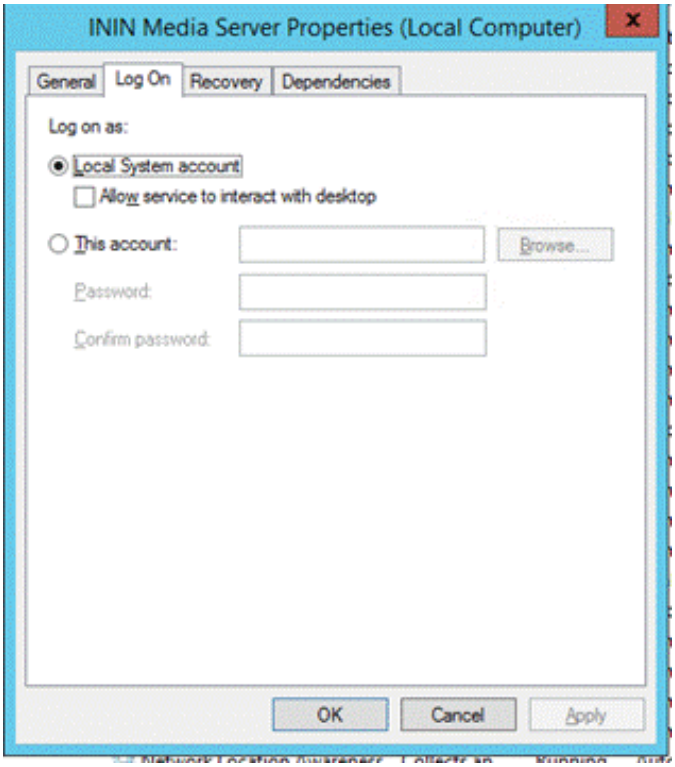
Certificates for the IC Media Server, RCS, OHSM and other Off- Server Components1

The Media Server and other peripheral devices also can operate using a Single Certificate. Since the PureConnect Off Host servers do not have a “Setup Assistant Wizard”, we will be using a Command Line utilty, which will perform tha same task that we did with the Setup Assistant Wizard on the IC Server. Please follow the directions below for all of the associated devices.

Before You begin

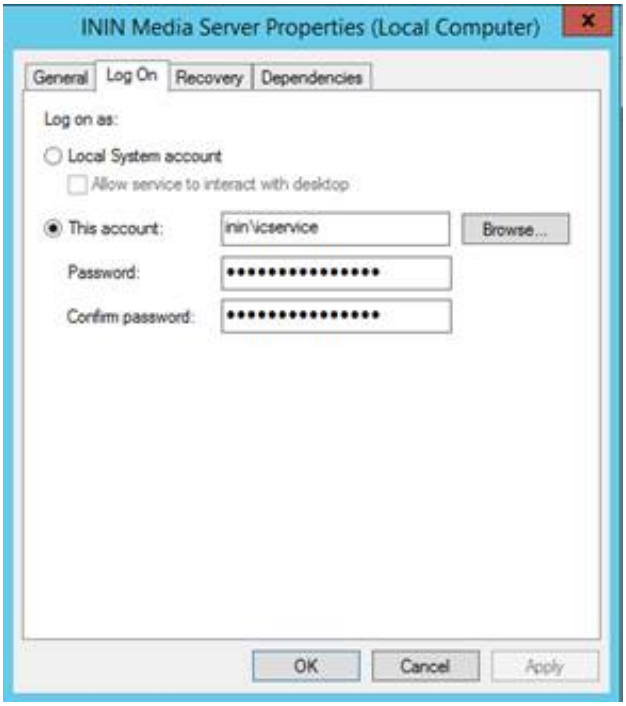
The Media Server and other or other Off Host C sub-systems need to use the Local System account to run as a service.



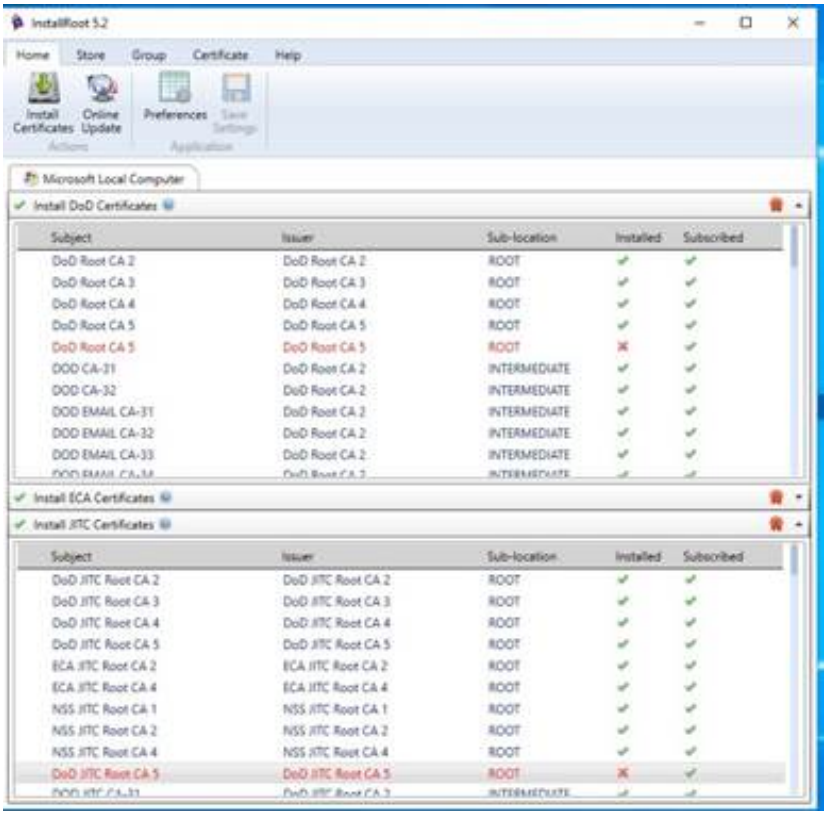


This account does not have any access controls or permissions to perform the tasks that we will need to perform.

You will need to change that entry to an account that has the proper ACLs and permissions to perform the Certificate tasks and process the required Certificate requests. In our example below, we are using a Domain (inin) account named “ICService”. This account is a normal domain user account.



Note: Before you perform any Certificate work on the IC Server, you must install the latest version of the “InstallRoot” application and run the application to install the correct certificates on all of your PureConnect Windows Servers _ (IC, Media[TM1] , SQL and so on) InstallRoot is designed to facilitate the management of PKI Certification Authority (CA) or Other Federal Agency certificates and other PKI CA certificates that may be necessary to the conduct any business across a variety of different certificate stores. Please contact your Agency or Customer to obtain this application or certificates.



Also, please ensure that the approriate **OU**, **O**, and **C** entries are correct for your agency, you will need to edit a configuration file and drop that file into the D:\IC\Server Directory on the PureConnect Server or Media Server.That edited file is named “OpenSSL.cnf” and it ensures that the appropriate entries are incorporated into the CSR

Generate the CSR

You can generate the CSR for an off-server component in two ways.

- Using CSR Generation Tool (Recommended Procedure)
- Using GenSSLCertsU.exe commands

a.Using CSR Generation Tool

Please refer following link to know how to generate the CSR using CSR tool.

b. Using GenSSLCertsU.exe

Note: It is recommended to use the new stand-alone Wizard-type CSR Generation Tool to generate Certificate Signing Requests (CSR) so that the process is quicker and less error-prone. Refer CSR Tool User's Guide for more info.

Depending on how you installed the Media Server/RCS or other Off Host IC sub-system, you will **Open a Command Prompt as an Administrator** and change the root starting point of where the install package installed the application.

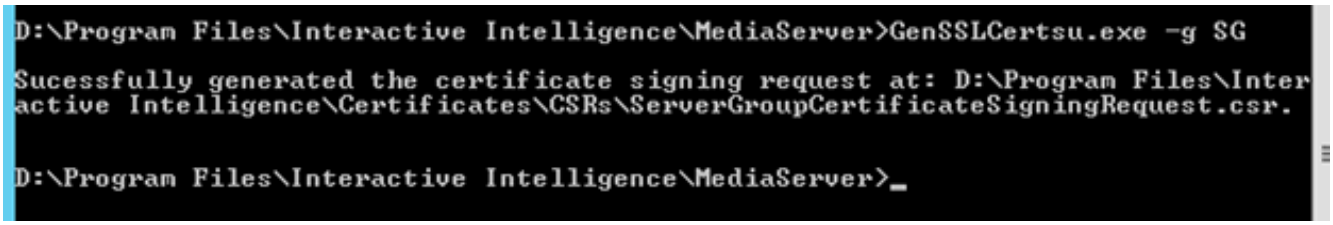
In our example below, the appropriate directory that the Media Server was installed into :

D:\Program Files\Interactive Intelligence\MediaServer

(Again, this is the directory location where the install package for the IC sub-system installed the application executable, so you may have to direct the "Command Prompt" to the appropriate application Directory.)

1. Run the following command to generate the CSR:

*C*MD: GenSSLCertsU.exe -g SG -f



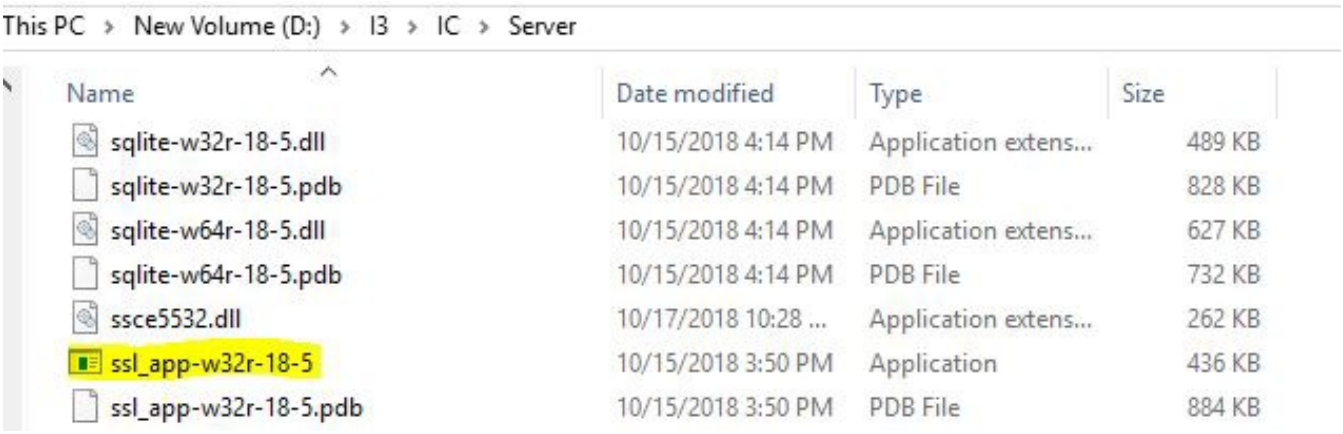
2. Browse to the appropriate Certificate Directory, in our case "D:\Program Files\Interactive Intelligence\Certificates\CSRs", to validate the CSR.

Once validated, submit the CSR to the proper Signing Authority for your organization. Once the Certificate is signed, return it to the CSR directory so that we can convert it and the private key into a .pfx file.

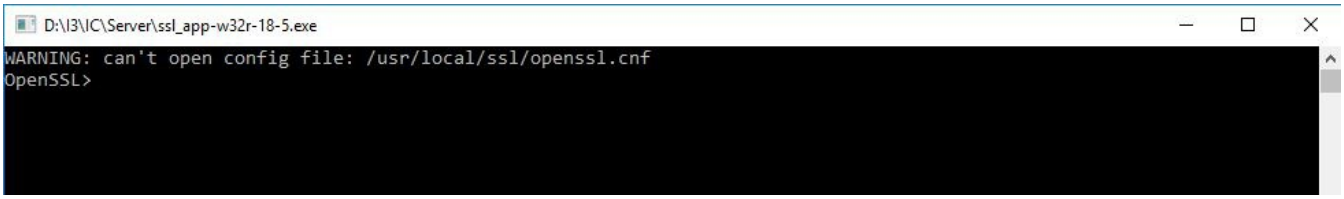
Converting a Signed Off Host Server Certificate into a PFX file

Once you have received the Signed Certificate back from the Signing Authority, we will need to convert it into a **.PFX** format for the Windows Certificate Store.

Navigate to the Media Server directory, in most cases, it will be in the "D:\Program Files\Interactive Intelligence\MediaServer" directory and locate the "ssl_app-w32-8-5. Exe file.



You will receive a warning that the “openssl.cnf” file cannot be opened, ignore the warning.



In the openssl command line, enter the following command:

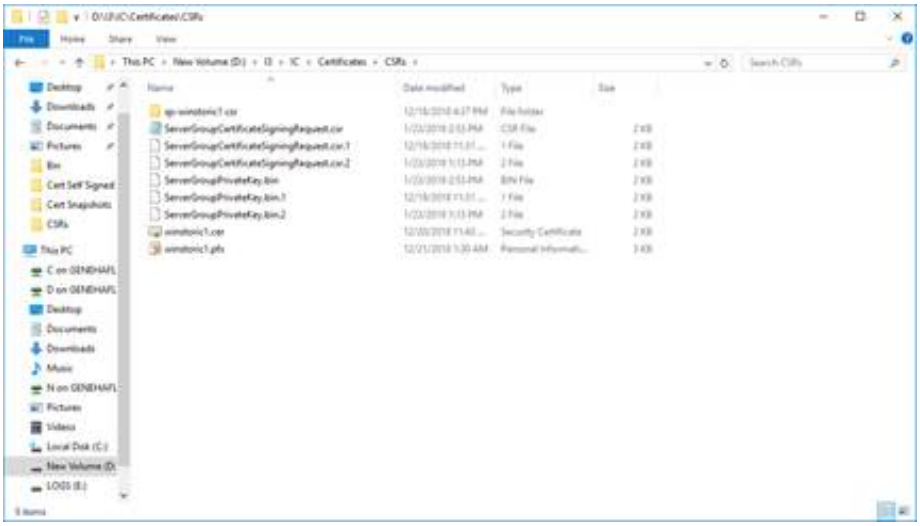
pkcs12 -export -in " D:\Program Files\Interactive Intelligence\Certificates\CSRs\winstorms1.cer" -inkey " D:\Program Files\Interactive Intelligence\Certificates\CSRs\ServerGroupPrivateKey.bin" -out " D:\Program Files\Interactive Intelligence\Certificates\CSRs\winstorms1.pfx"

```
OpenSSL> pkcs12 -export -in D:\I3\IC\Certificates\CSRs\winstoric2.cer -inkey D:\I3\IC\Certificates\CSRs\ServerGroupPrivateKey
.bin -out D:\I3\IC\Certificates\CSRs\winstoric2.pfx
```

In our example above the name of the certificate is “winstorms1.cer” and the private key is named “ServerGroupPrivateKey.bin”.

Please use and or substitute your server’s name within the Command line.

In most cases, the Media Server Certificate is located in the D:\Program Files\Interactive Intelligence\Certificates directory. Your Certificate Directory may be different based on how you installed the system. In any case, please use the correct directory location for your server when using the Command Line entries.



The command line points to the signed certificate so that it can be converted into the **.PFX** format.

If there are any spaces within the directory name, place at the beginning and end of the directory name.
Enter a Password, and please note or maintain that password for future use.

```
Enter Export Password:
```

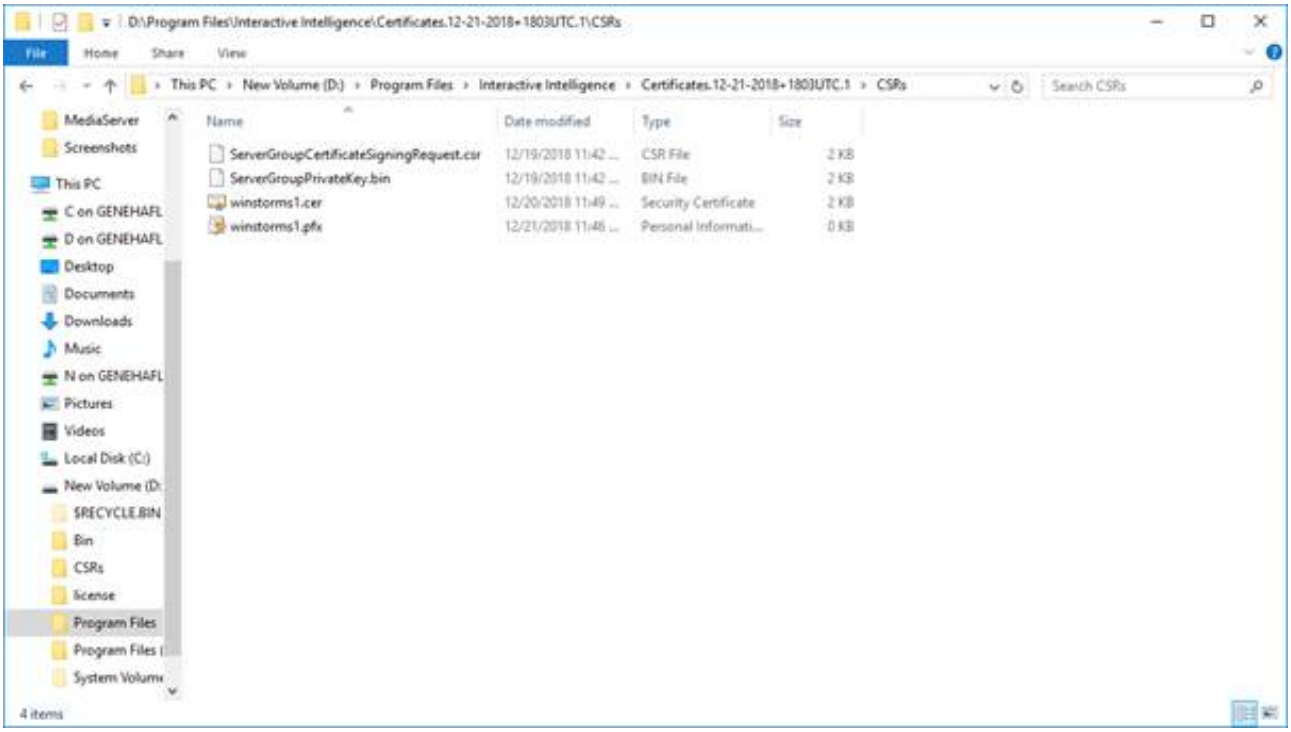
Verify Password

```
Verifying - Enter Export Password:
```

Conversion completed:

```
OpenSSL> pkcs12 -export -in D:\I3\IC\Certificates\CSRs\winstoric2.cer -inkey D:\I3\IC\Certificates\CSRs\ServerGroupPriva
teKey.bin -out D:\I3\IC\Certificates\CSRs\winstoric2.pfx
Enter Export Password:
Verifying - Enter Export Password:
OpenSSL>
```

Check the **.PFX** file, again please go to the appropriate certificate directory for your server:

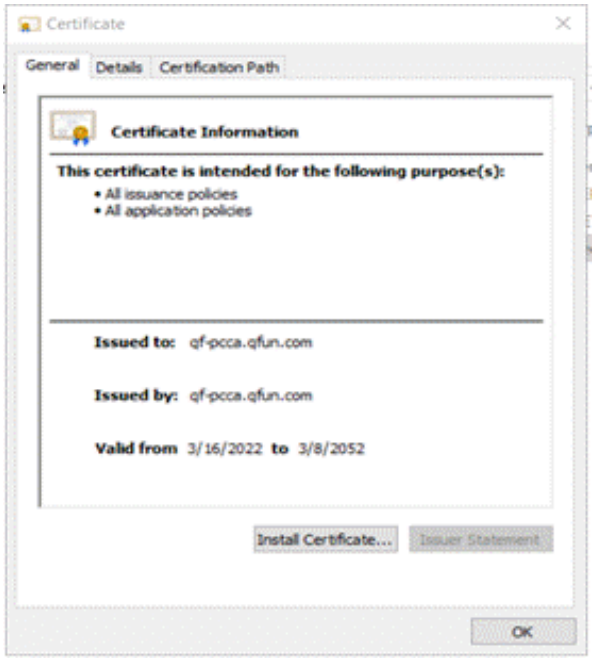


Importing the Off Host Server Signed Certificate and Root CA into the Local Windows

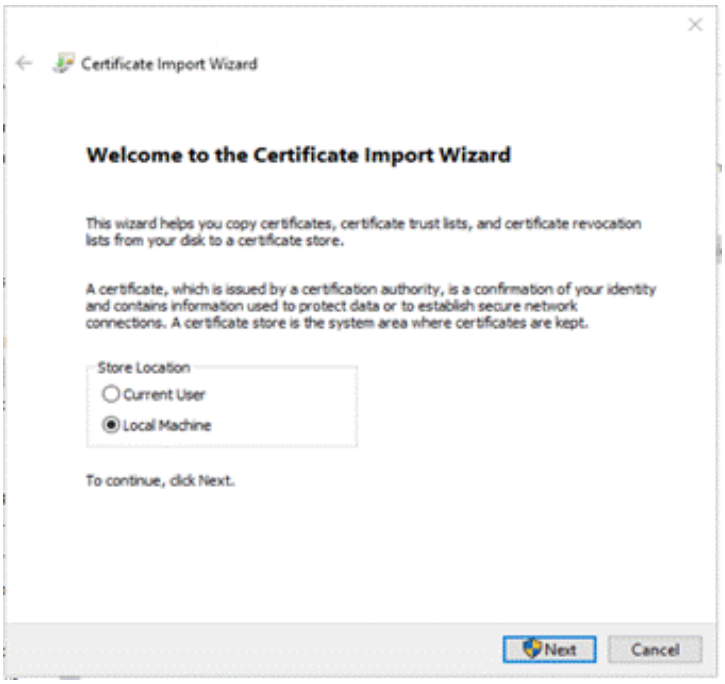
Importing Root CA

Now you will import the Root CA (Trusted Certificate Authority (CA)) Certificate into the local server's Windows Store.

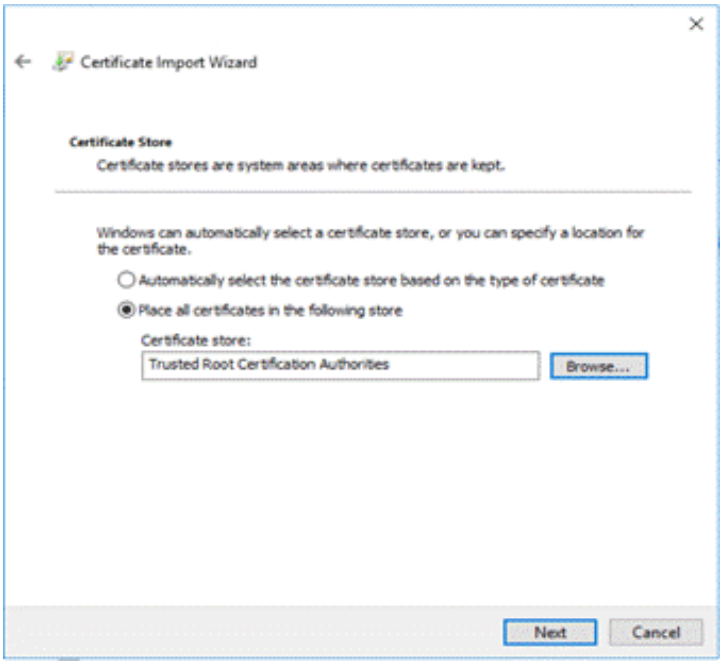
1. Navigate to the D:\I3\IC\Certitifcates\CSR directory and locate the Root CA Certificate you have copied from CA.
2. Double Click on the file.
3. Select "**Install Certificate...**" from the Certificate.



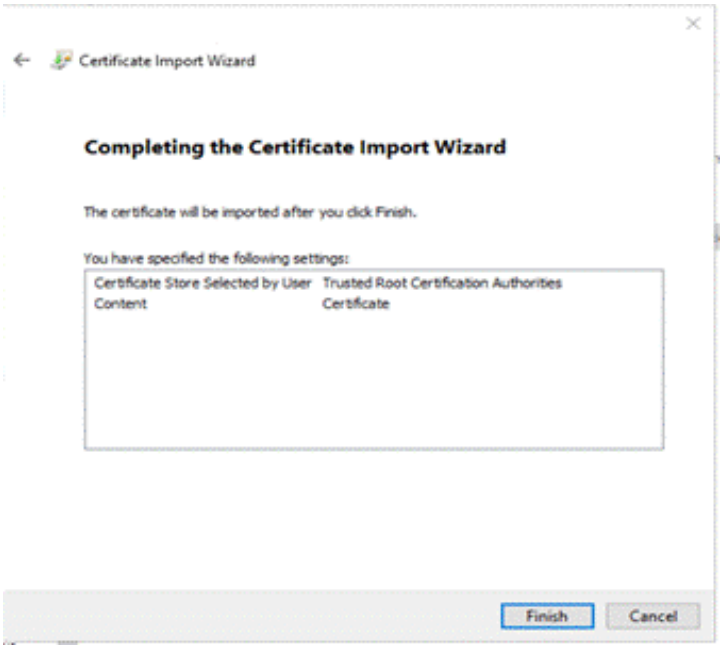
4. A new window appears, select **Local Machine** radio button and click on **Next**.



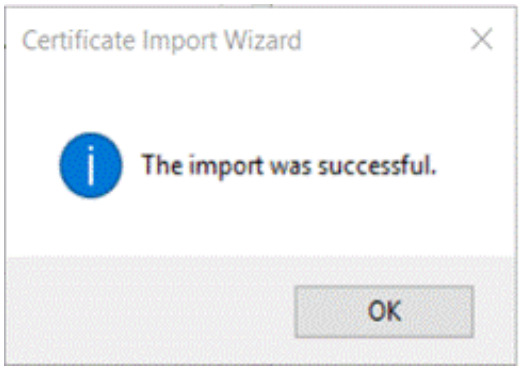
5. Select **Place all certificates in the following store** and select **Trusted Root Certification Authorities** area:



6. After completing the Import, verify that you have imported the correct Certificate and click **Finish**.



7. After the successful Import, click **OK** to close the window.

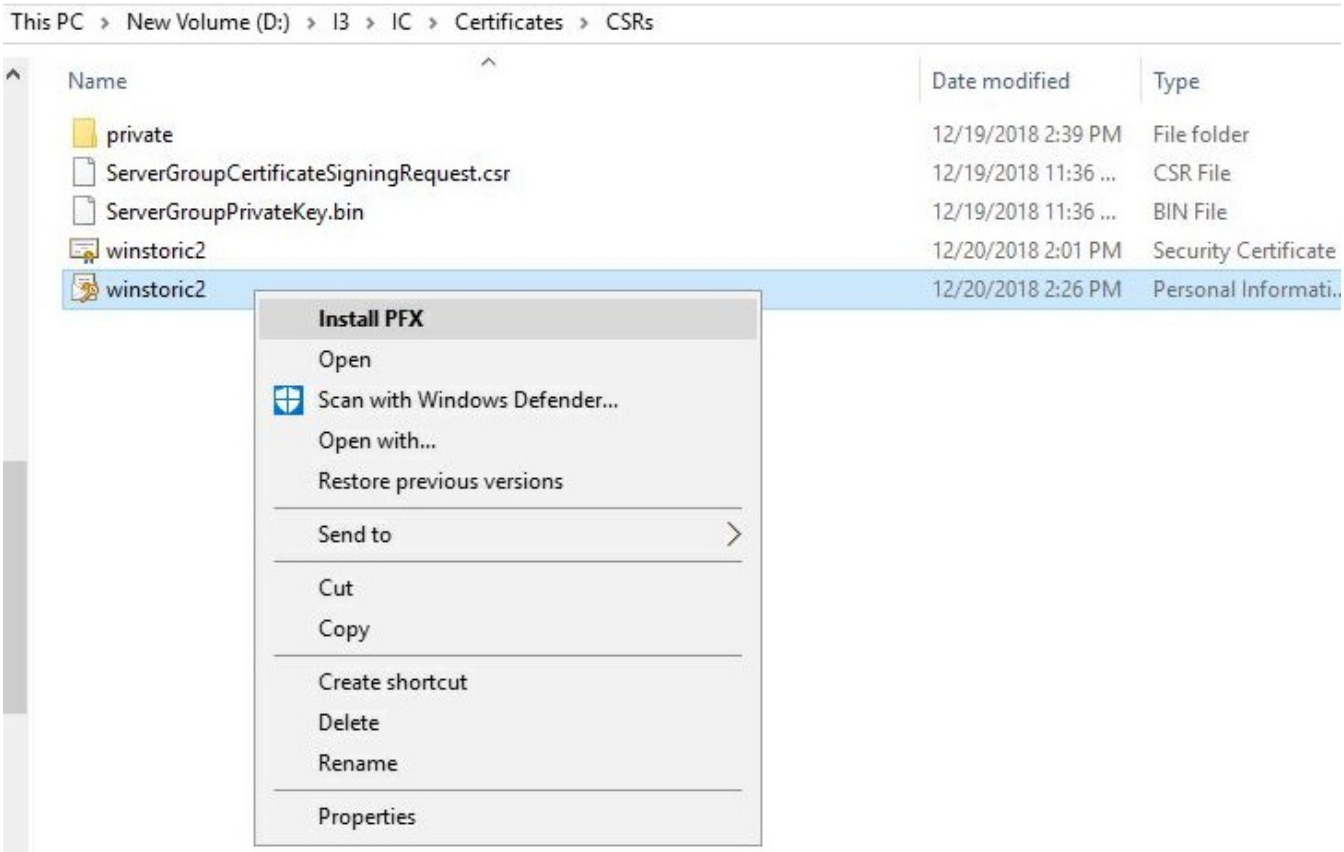


Importing the Signed Certificate

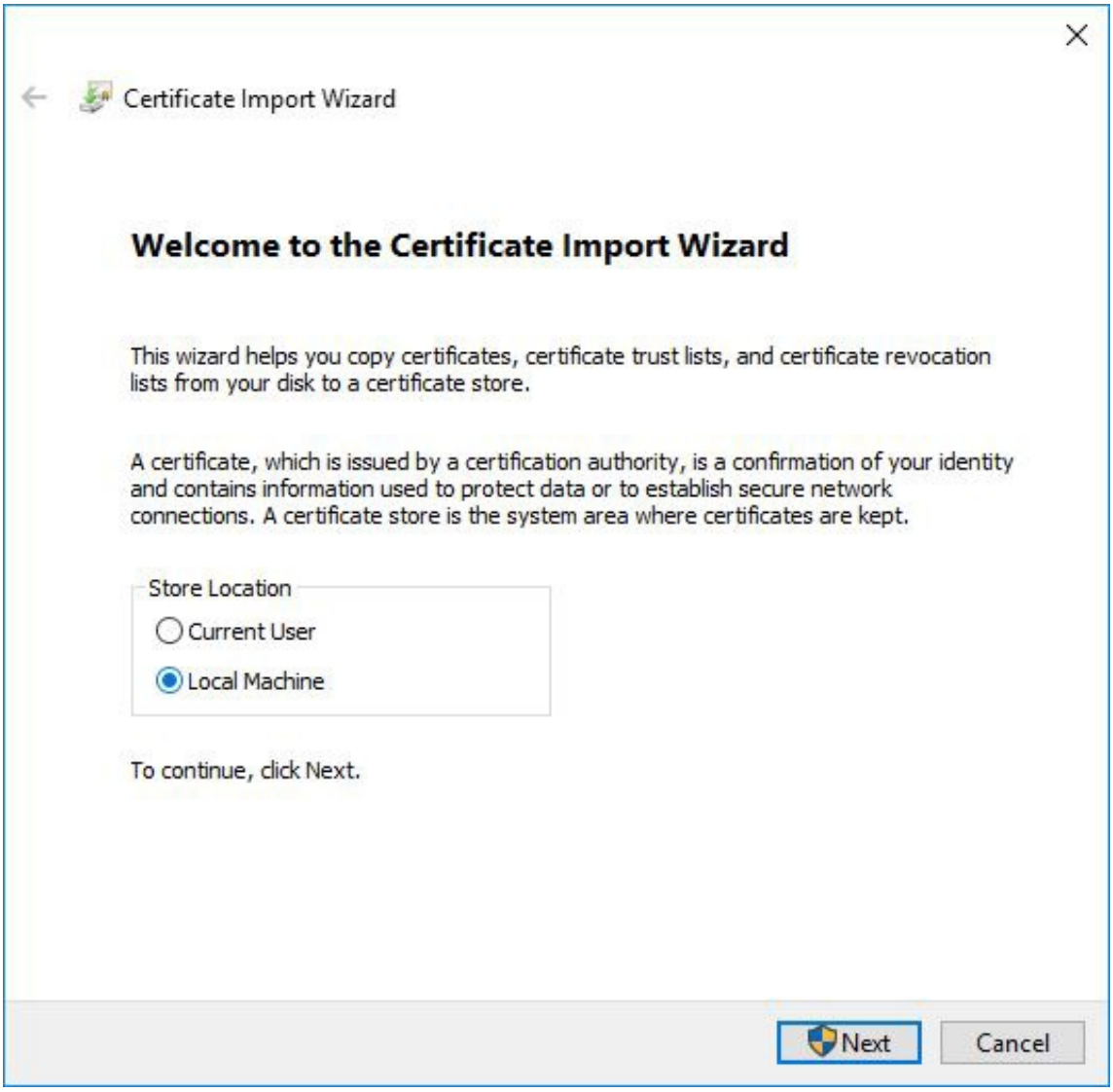
Now that the Signed Certificate has been signed and converted, you will import the PFX Certificate into the local server's Windows Certificate Store.

1. Navigate to the "D:\Program Files\Interactive Intelligence\Certificates\CSRs" directory or whatever CSR directory you have and locate the newly created certificate .pfx file that you performed in the previous steps.

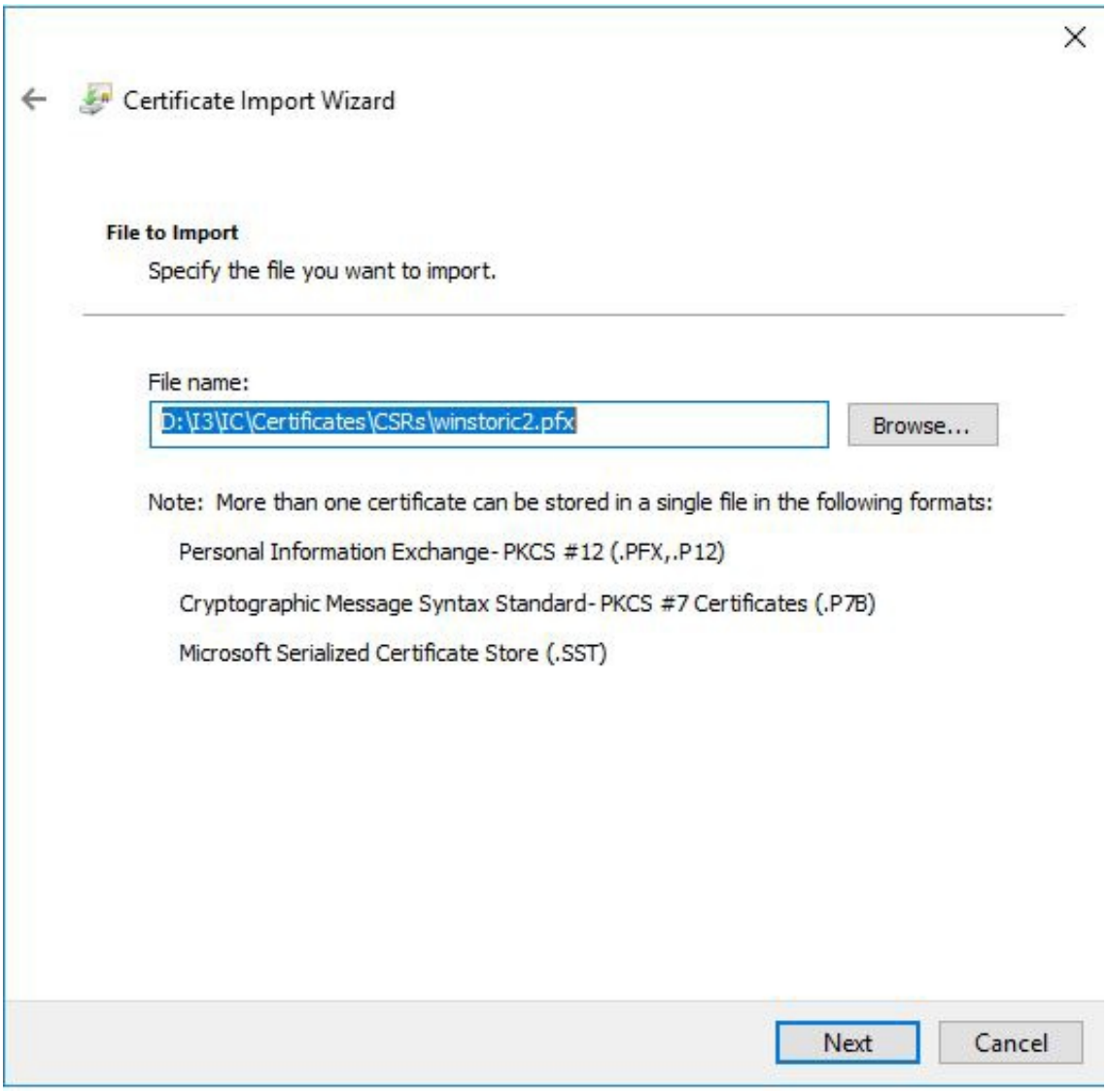
2. Right click on the file, in our example we right-clicked on the "winstoric2.pfx" file.



3. Select **Install PFX** from the menu. A new window appears, select **Local Machine** radio button

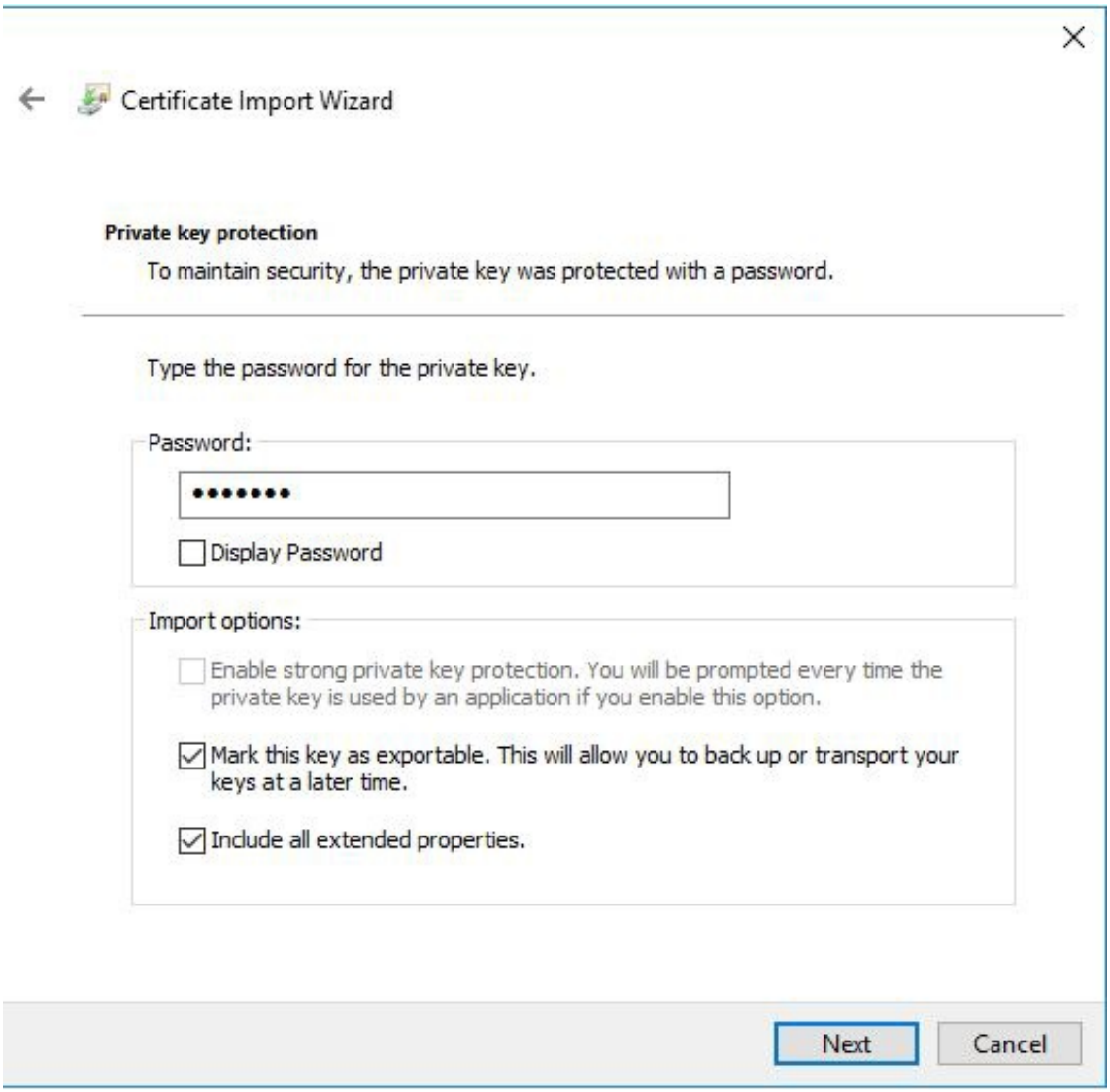


4. Browse to and specify the file you want to import:

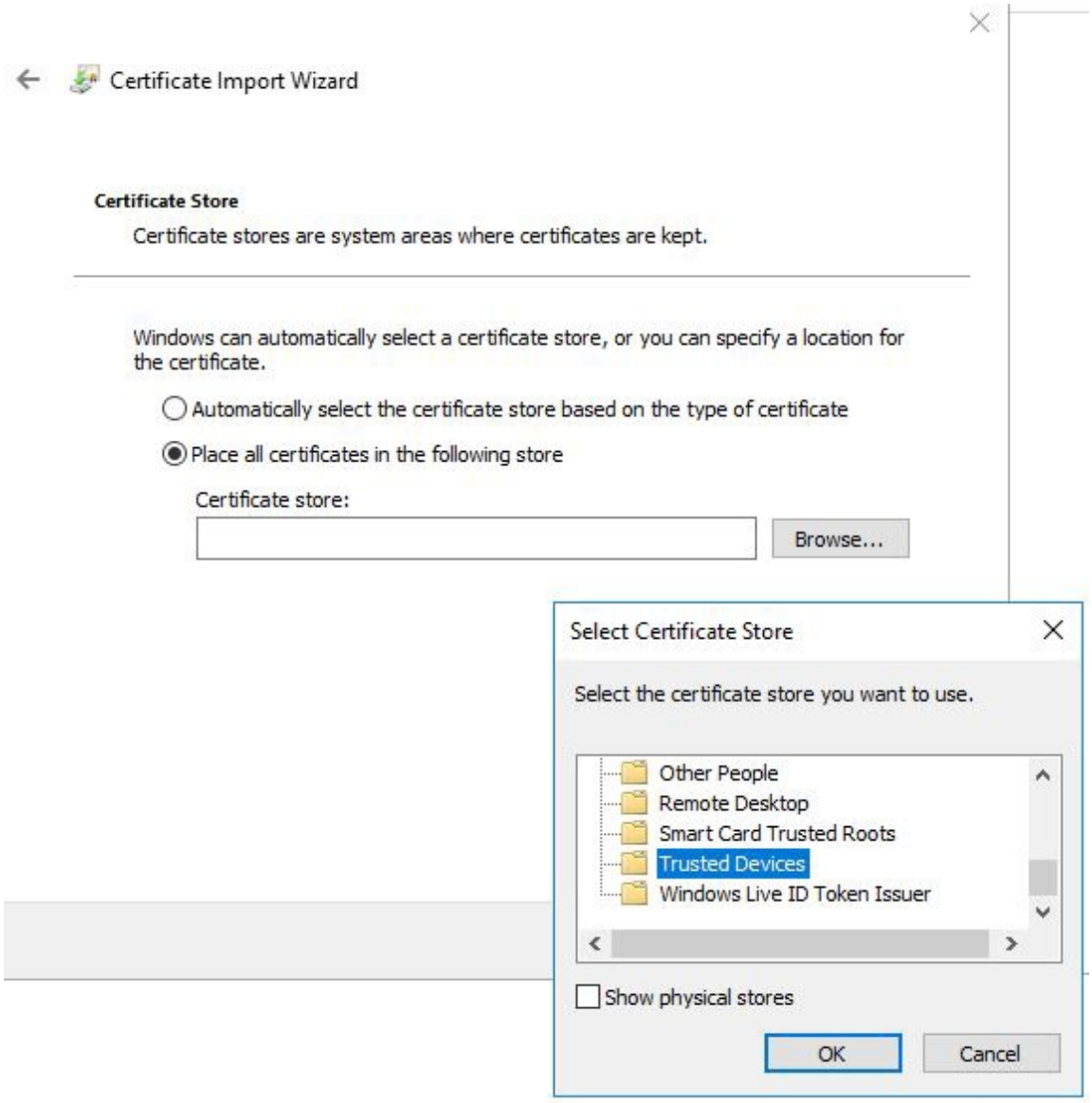


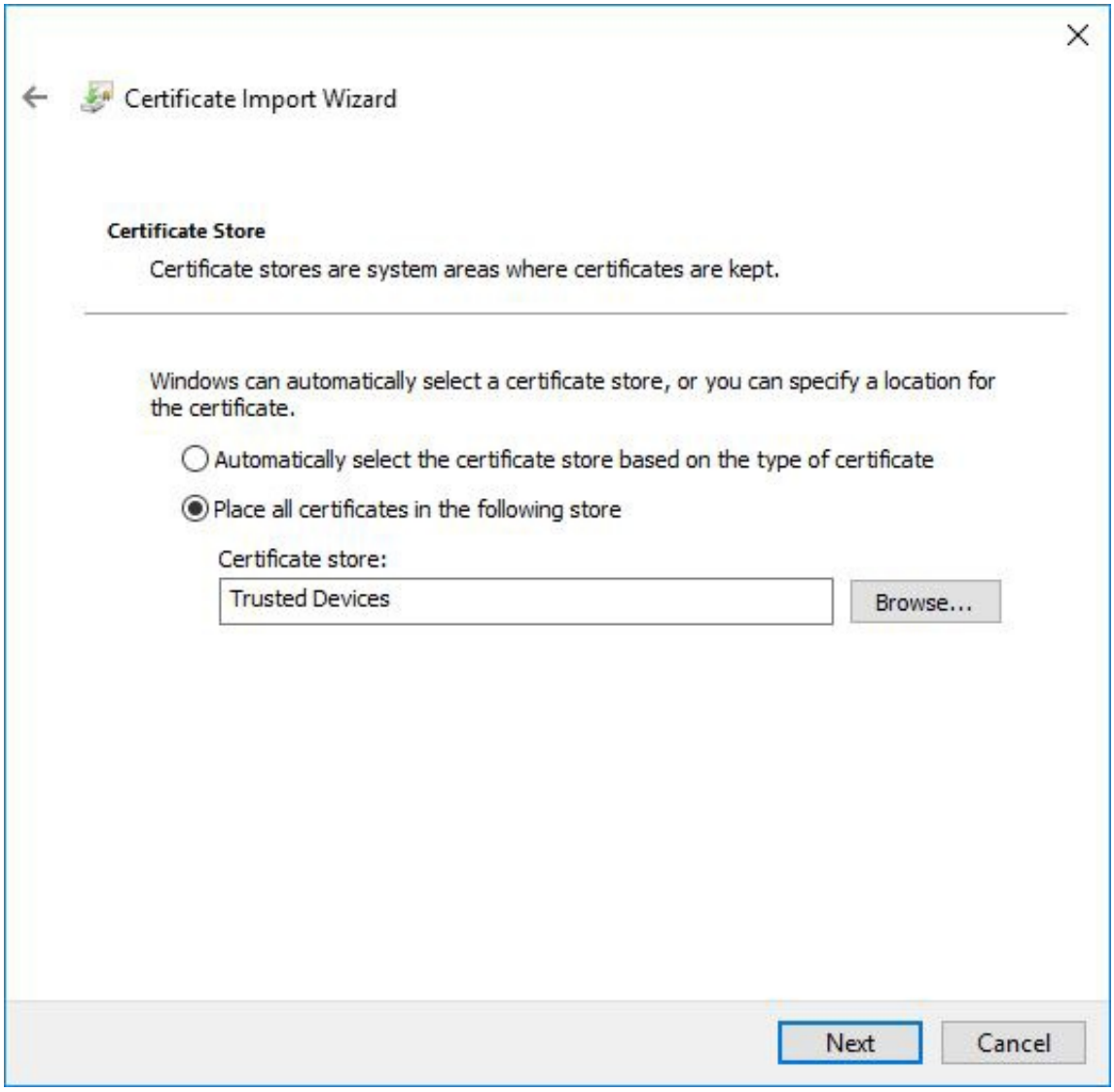
5. Enter the Password, which was created in the step 4 of section *"Converting the Signed Certificate for Importing"*

Note: you must mark this certificate as exportable or the PureConnect application cannot use or register with this certificate. Please mark the extended properties checkbox as well.

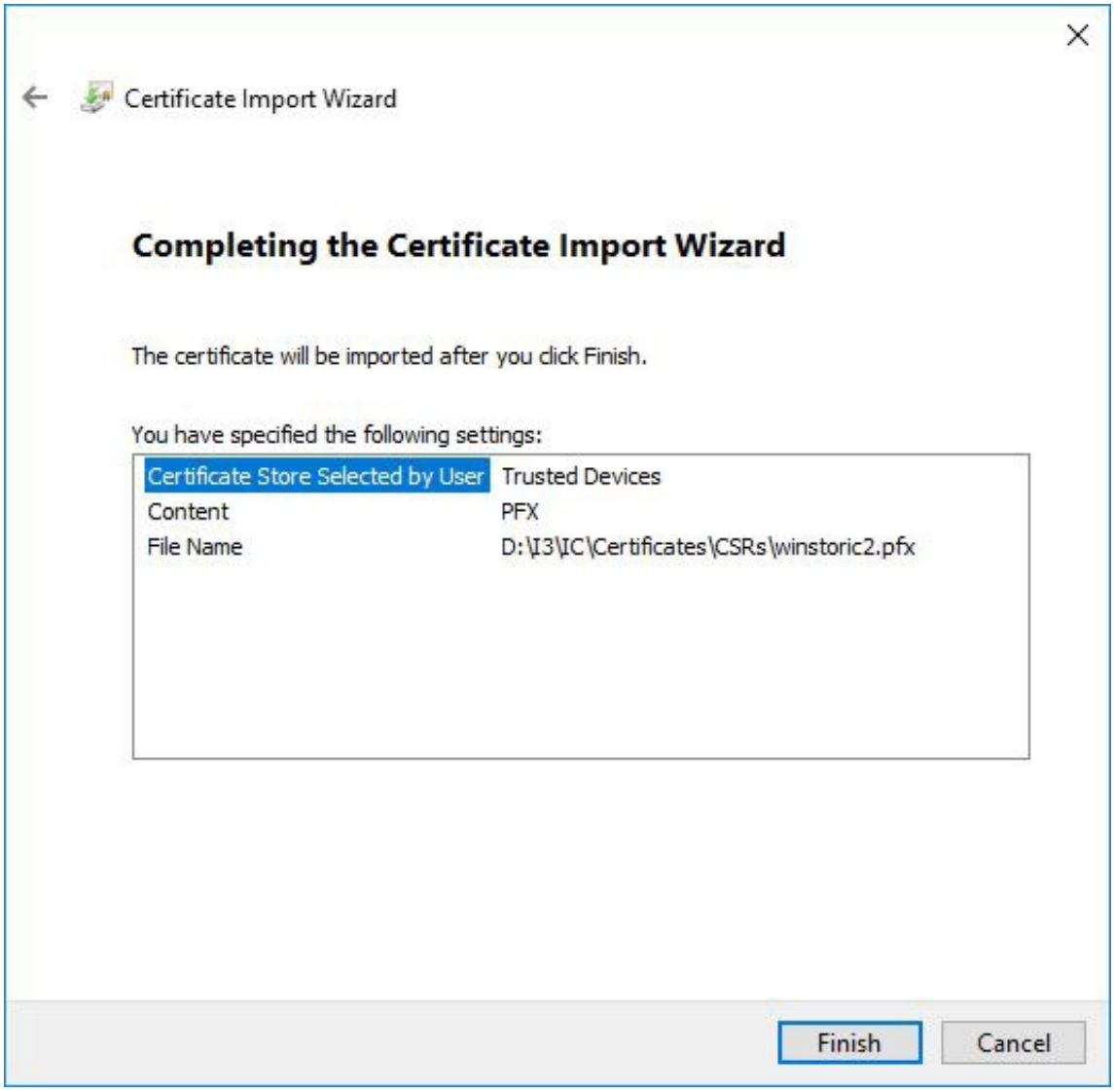


6. Select **Place all certificates** in the "Trusted Devices" area:

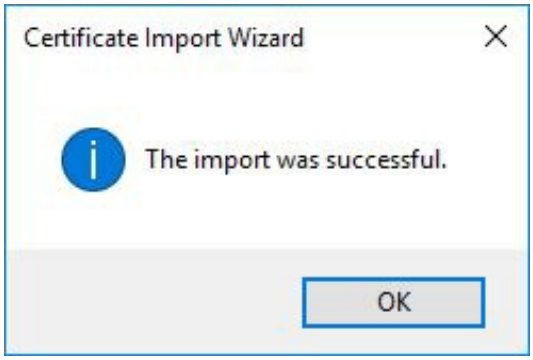

Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
Select Certificate Store
Select the certificate store you want to use.
Other People
Remote Desktop
Smart Card Trusted Roots
Trusted Devices
Windows Live ID Token Issuer
Show physical stores
OK
Cancel



7. After completing the Import, verify that you have imported the correct Certificate and click **Finish**.



8. After the successful import, click **OK** to close the window.



Importing the Off- Server Sub-systems Certificates from Windows Certificate Store to Server

This section covers the procedures of importing the Signed Certificate for Media, RCS, or other peripheral IC sub-system back into that server.

Now that the Signed Certificates have been returned and you have exported in into the Local Windows Certificate Store, we will import the Signed Certificate from the Windows Certificate store so that the Media Server or other Off Host servers can register PureConnect with the Certificate.

Open a Command Prompt Running as Administrator -> browse to D:\Program Files\Interactive Intelligence\MediaServer (Replacing Media Server with appropriate application Directory).

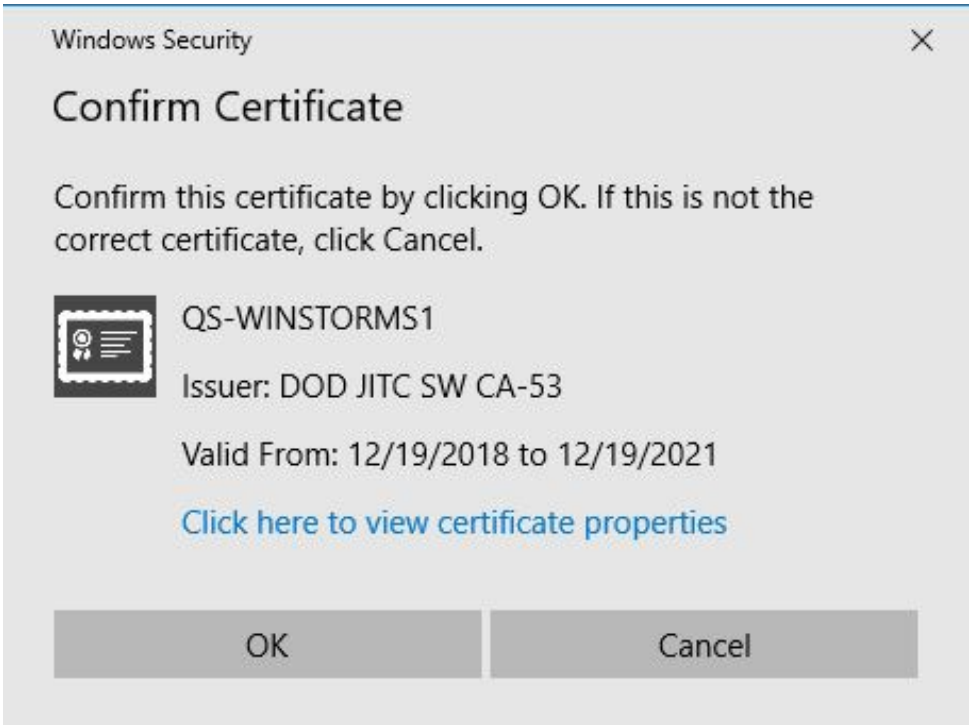
1. Run the command below from the D:\Program Files\Interactive Intelligence\MediaServer directory:

   GenSSLCertsU.exe -o -w -f

```
D:\Program Files\Interactive Intelligence\MediaServer>GenSSLCertsU.exe -o -w -f
```

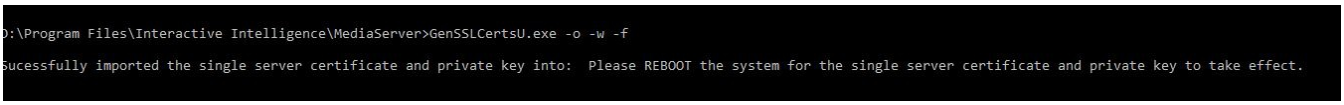
2. Select **Trusted Devices** and then click on the **Select** button to choose your Server Certificate:

3. Confirm and click **OK**.



4. Check to make sure your Server name is in the Certificate field and then click **OK**.

5. The Command-Line shows that you have successfully imported the Cert from the Windows Certificate Store.



6. Close the Command-Line and Reboot the Server.

The Signed Certificate as well as the Private Key and Trusted certificates have been imported into the IC certificate Directory. Please validate that the certificates are in that Certificate directory.

Reboot the server once you are satisfied that the certificates are in the correct location.

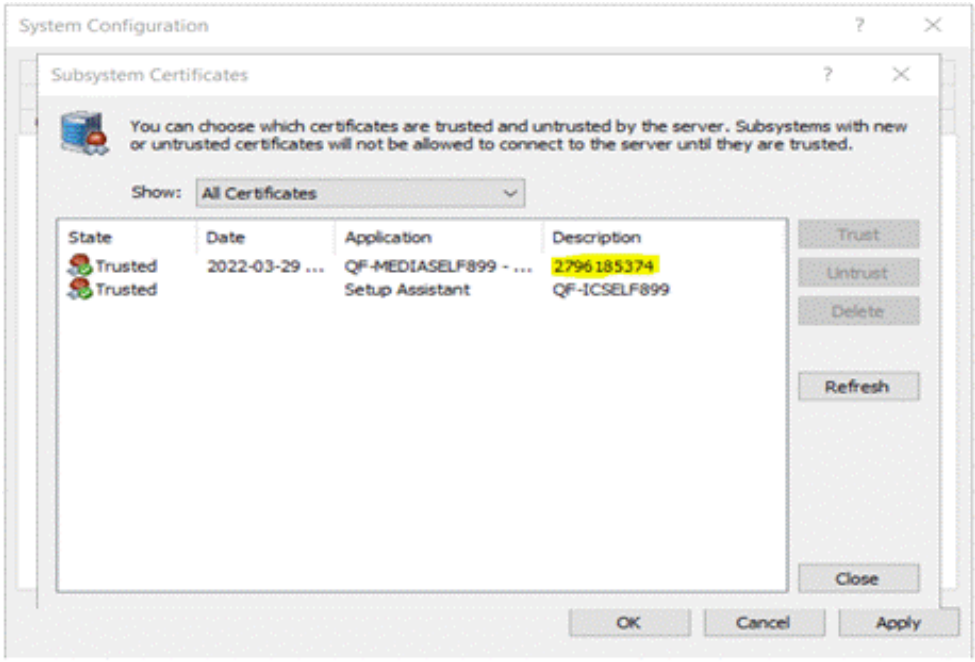
Validate that the appropriate Service starts, and the Media Server or other Off Host IC Sub-system service are running and that the application is functioning correctly.

Registry Fixes for the Media Server, RCS, PASv2 or OHSM

The Media Server, Remote Content Server (RCS), PASv2(Process Automation Server), and or other Off Host Session Manager (OHSM) servers have been Trusted in the Interaction Administrator application during the initial install and setup. These servers used the IC Self Signed certificates to validate that IC and it associated Off Host Sub-systems are functioning correctly. At that time, those Off Host Sub-systems were identified within the Interaction Administrator by an IC serialized number you will have to change within the Registry of the IC Server. The following procedures lead you step by step to update those entries on the PureConnect IC Server.

This step is important for all Sub-System which has been Trusted Certificate in the Interaction Administrator application during the initial installation and setup.

1. Open the Interaction Administrator utility on the PureConnect server.
2. Navigate down to the System Configuration container.
3. Open Configuration Container in the “Right” pane of the utility.
4. Open the Certificate Management Tab.
5. Select the Subsystem Certificates Configuration modify button.
6. Look for the name of your Off-host Server or ASR server:

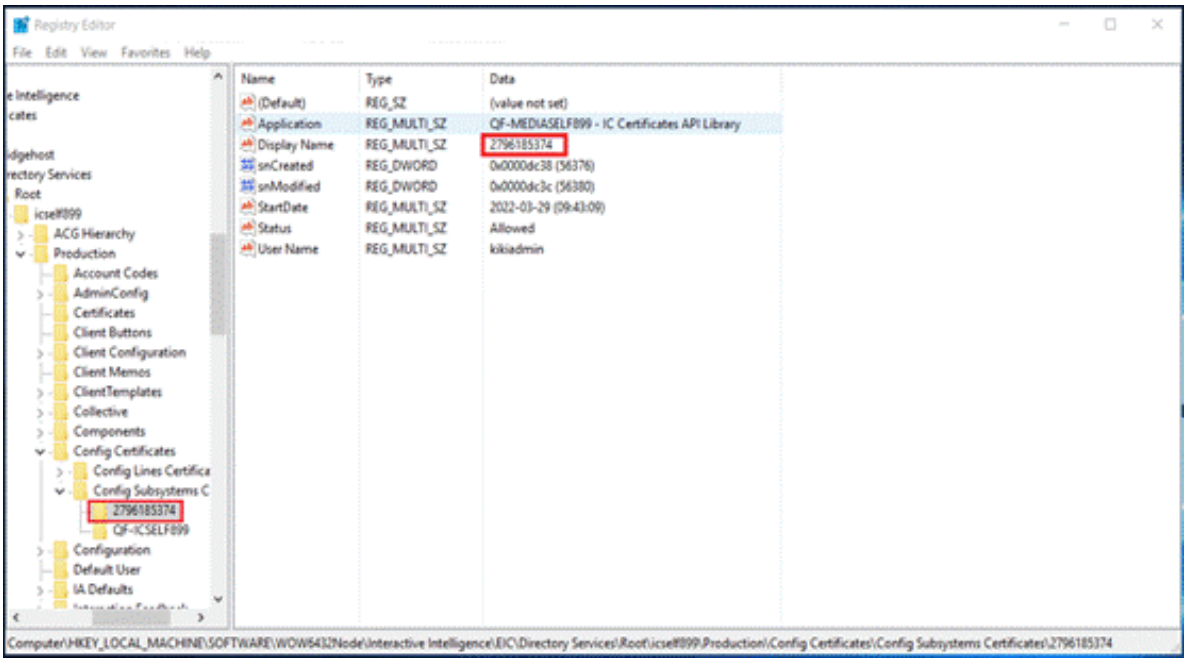


7. Record or write down the numbers that are listed in the “Description” label. We will need to find and edit those in a later task. If you have more than one Media server “Trusted”, record those numbers also.

8. If you have an ASR server that has been “Trusted” also, record or write down the numbers that are listed in the “Description” label for each ASR server. We will need to find and edit those in a later task as well.

9. Open the Windows Registry editor on the PureConnect server (regedit.exe) and navigate to:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Interactive Intelligence\EIC\Directory Services\Root\Customer Site\Production\Config Certificates\Config Subsystems Certificates\



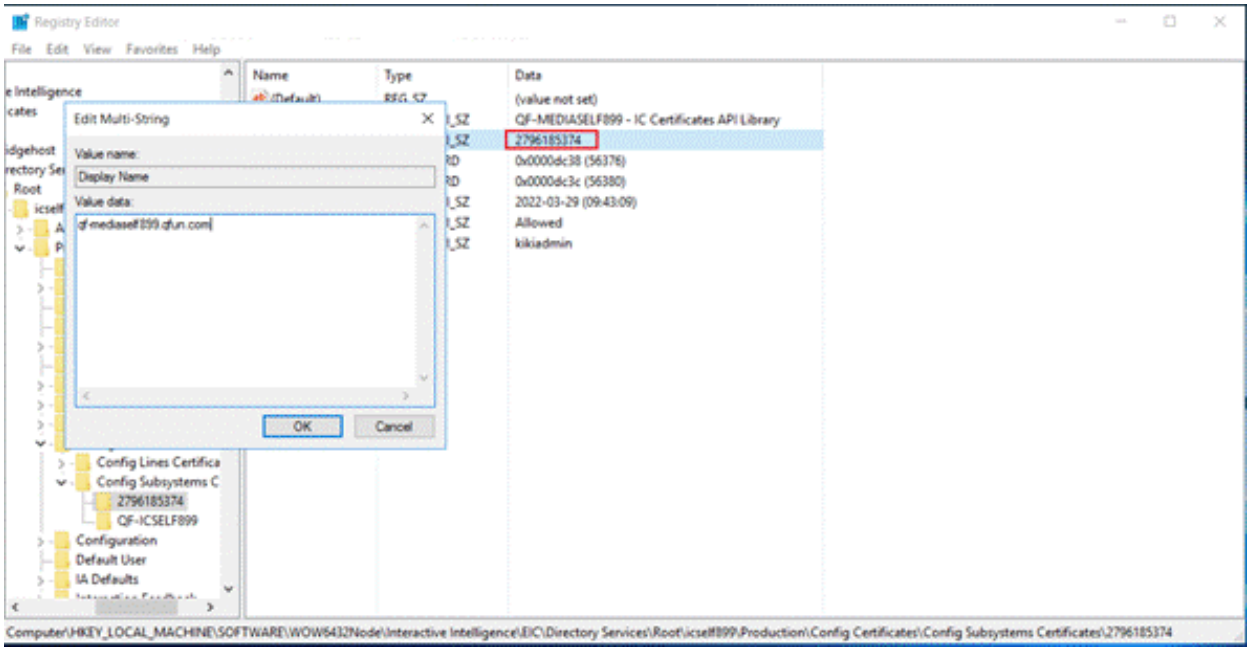
10. Look for the “Description” number that represents your Media Server. You want to look for the numeric entry that represents

the “Trusted” Certificate name used in the Interaction Administrator when the Media server was first connected to the PureConnect Server. In our example in the Figure below shows that Media Server QF-MEDIASELF899 has a “Description” of 2796185374. Look for the “Description” number that represents your Media Server.

11. Double Click or Select the “Display Name” entry that represents your Media Server so that we can modify this entry.

12. An “Edit Multi-String” window will open.

13. You may need to change or edit the entry with the Host Name (FQDN) of the Media\ASR server. If the Hostname was correct when you opened it, you can move on to the next step. Please note that any changes you make here will overwrite the number that used to appear in that position.

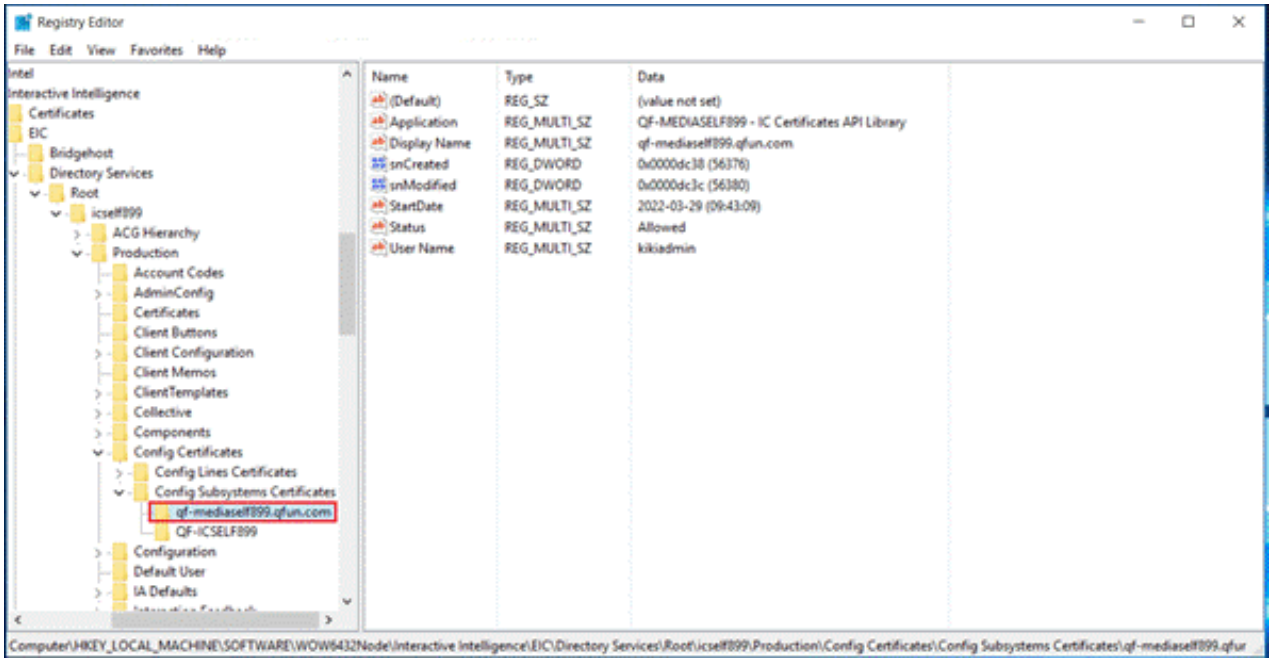


14. Click **OK** button.

15. Navigate back to the original Number that represents this Certificate as shown in the figure below.

16. Right click on the Number that represents this Media Server Certificate and select **Rename**.

17. Rename the Folder with the same Hostname which we used in Step 13.



18. Repeat Steps 1 through 11 until all the Media\ASR server entries have the correct FQDN instead of the previously used numbers.

19. Follow steps 1 thru 17 for on the Backup Media Server.

20. Startup IC service now.

21. Once the PureConnect server as started, start the Media\ASR server's service on those respective machines.

22. Make a backup of the working Media or ASR Federal or modified Certificate folder and retain/store it in a safe location.

At this time check your connection of the Media Server if it does not connect; Reboot the CIC Server.

Final PureConnect Server Certificate Procedures

1. Reboot the IC Servers. Once they are up and running. Place the PureConnect or Interaction Center Service back in “Automatic” mode” and Start the IC service now.

2. When the IC system restarts, make a Backup copy of the newly modified Certificate folder on all PureConnect servers in this solution and store them in a location that can be safeguarded.

3. Should the IC system fail to start, check the Window Event Logs for any Certificate related errors or if CIC fails to start? Navigate to the D:\I3\IC\Certificates folder and rename it to Certificate X.

4. If the IC system fail to start, check the Window Event Logs for any Certificate related errors or Navigate to the D:\I3\IC\Certificates folder and rename it to Certificate X.

5. Copy the original, modified IC Certificate folder back into its original location. You may have to rename it back to “Certificates”.

6. Reboot the CIC Server.

7. The CIC Server should start since we have reverted to the original CIC Certificate folder that was working priorbeforemodifications.

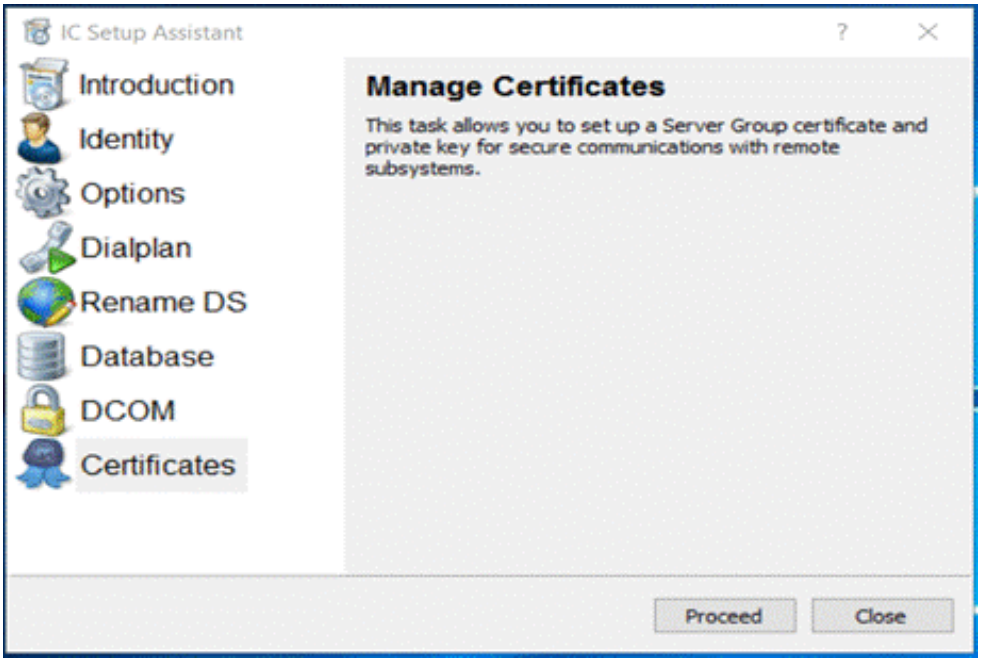
8. Contact GENESYS Support if you cannot get the modified Certificates to work.

Manage Certificate Digest

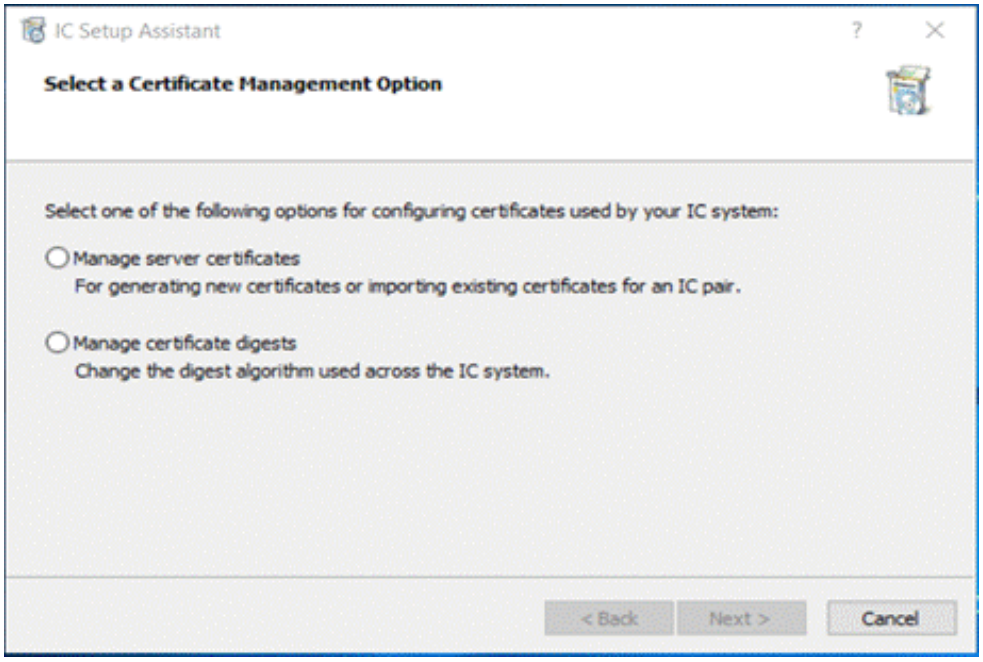
For existing IC Server installs, the certificate signatures will need to be converted to SHA-256 with an option in the Certificates wizard found in Setup Assistant. When the "Manage certificate digests" option is chosen, it will prompt you to choose between SHA-1 or SHA-256 as the signature digest. **The current Server Group certificate digest will be chosen by default**. After the choice is confirmed, the wizard will convert all existing certificates that are not signed with the chosen digest to the new digest algorithm.

Digest Conversion from SHA-1 to SHA-256

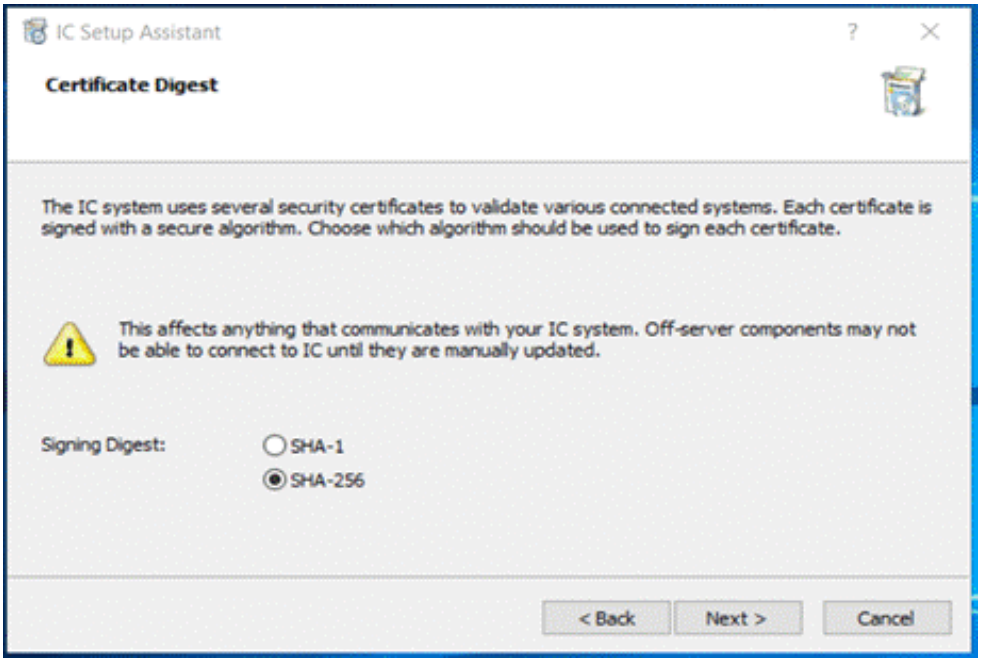
1. Backup the Certificates currently in place.
2. Place the Original Certificates into the appropriate Directory for both the PureConnect and Off-Host Server(s).
3. Get the Off-Host Server connected to the PureConnect server with the Original Certificates.
4. Test and validate.
5. Run Setup Assistant for upgrading the Certificates to SHA-256.
6. Select Certificates

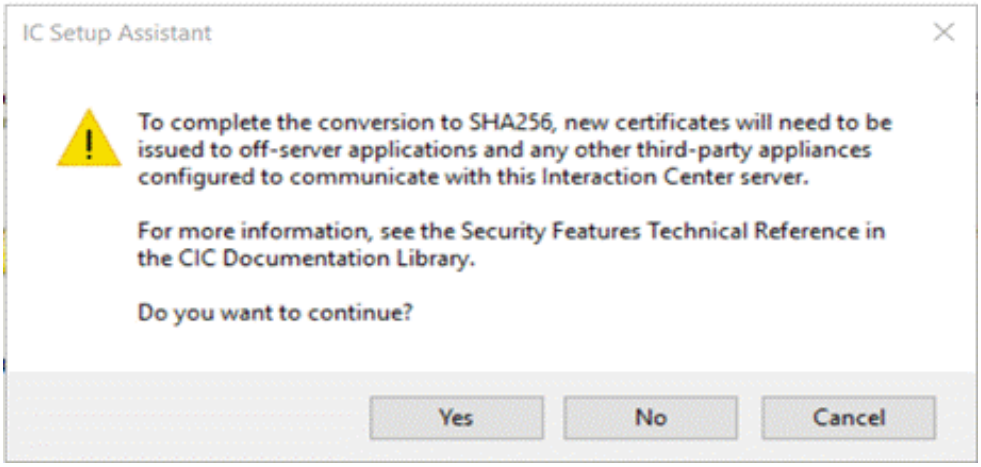


7. Select **Manage Certificate Digests**.



8. Select **SHA-256** and Click **Yes** on the Warning.

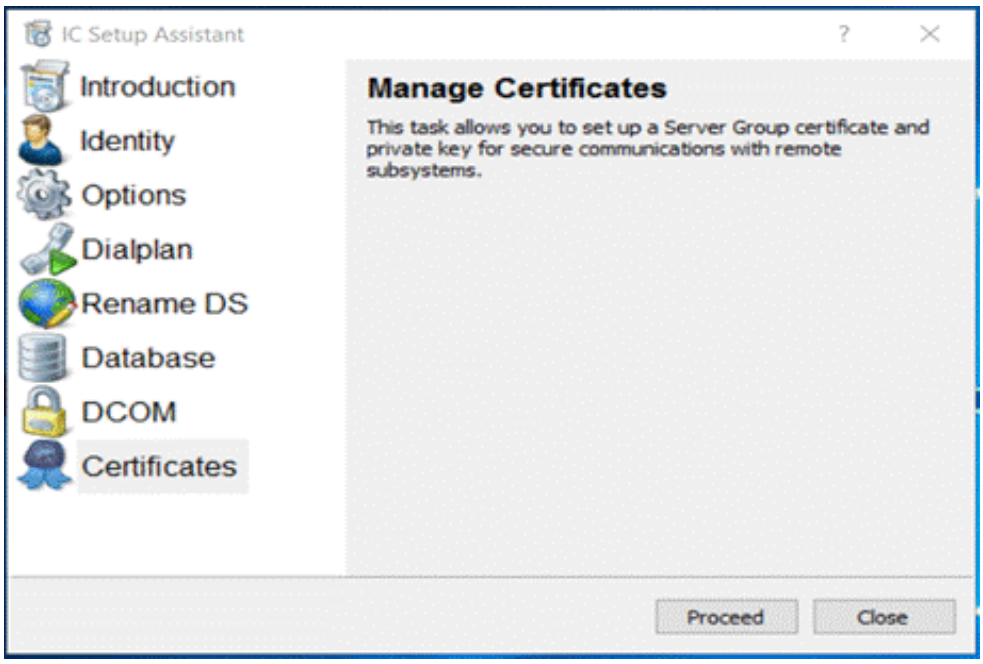




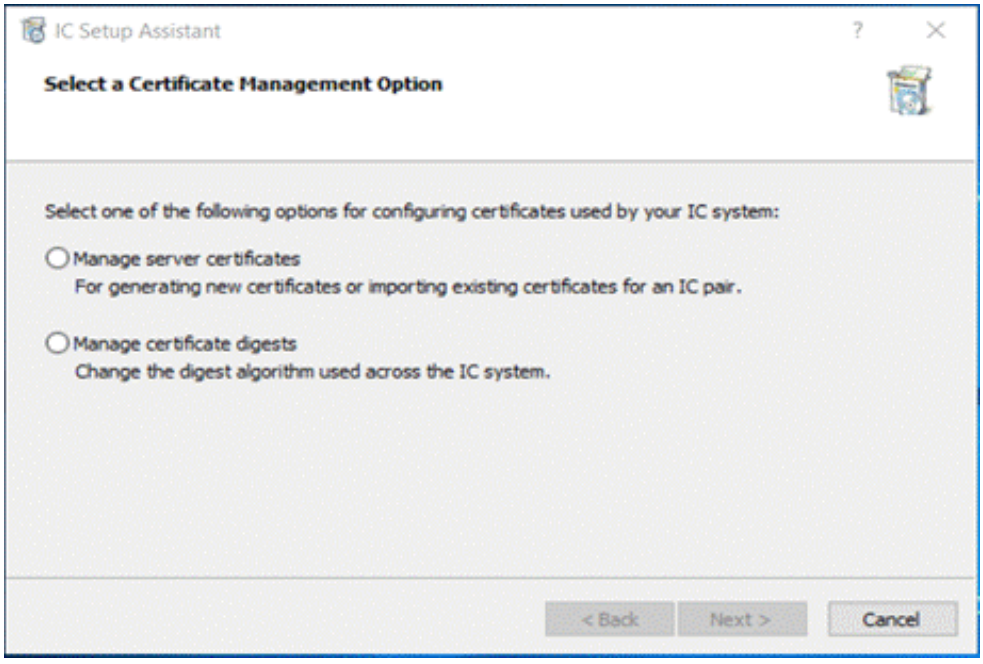
9. Complete the Setup Assistant. Validate and test your system.
10. Place your SHA-256 signed Certificates into the Certificate Directory for all PureConnect and Media Servers and reboot.

Digest Conversion from SHA-256 to SHA-1

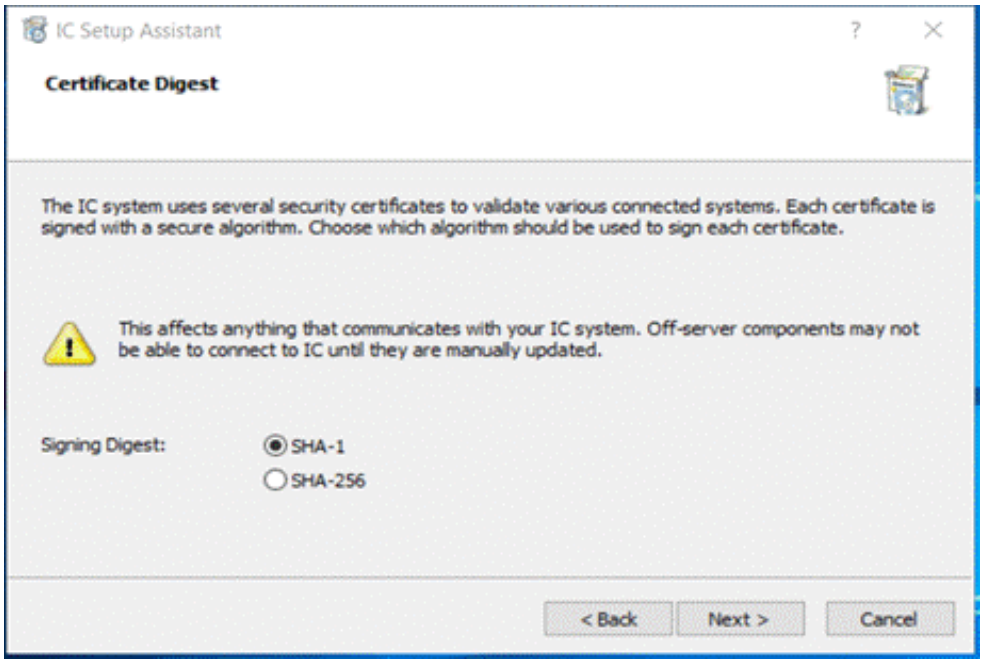
1. Backup the Certificates currently in place.
2. Place the Original Certificates into the appropriate Directory for both the PureConnect and Off-Host Server(s).
3. Get the Off-Host Server connected to the PureConnect server with the Original Certificates.
4. Test and validate.
5. Run Setup Assistant for converting the Certificates into SHA-1
6. Select Certificates

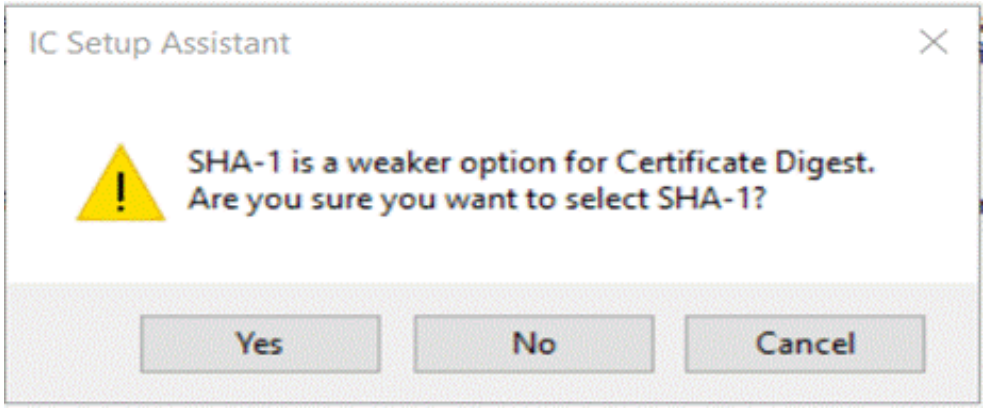


7. Select **Manage Certificate Digests**.



8. Select **SHA-1** and Click **Yes** on the Warning.





9. Complete the Setup Assistant. Validate and test your system.

10. Place your SHA-1 signed Certificates into the Certificate Directory for all PureConnect and Off-Host Servers and reboot.