

# Setup Server 2019 Enterprise CA 4/5: Setup Group Policy

[vmlabblog.com/2019/09/setup-server-2019-enterprise-ca-4-5-setup-group-policy](https://vmlabblog.com/2019/09/setup-server-2019-enterprise-ca-4-5-setup-group-policy)

Aad Lutgert

September 25, 2019

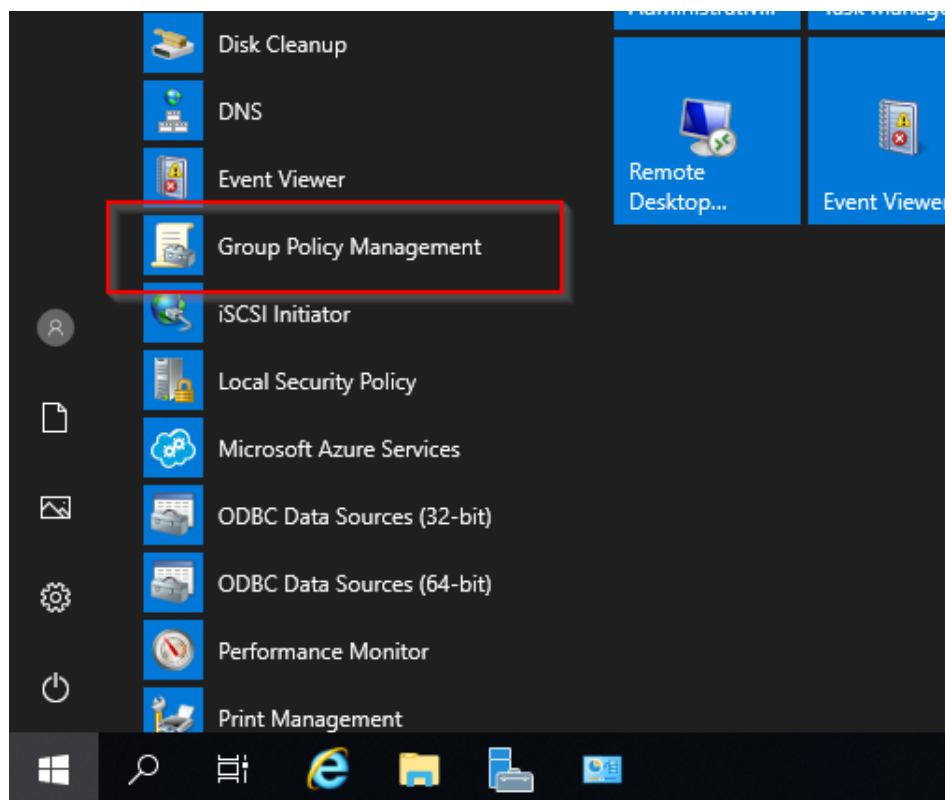
Previous: [Subordinate CA](#)

*Updated 11-12-2020: Updated filepath step 8 .*

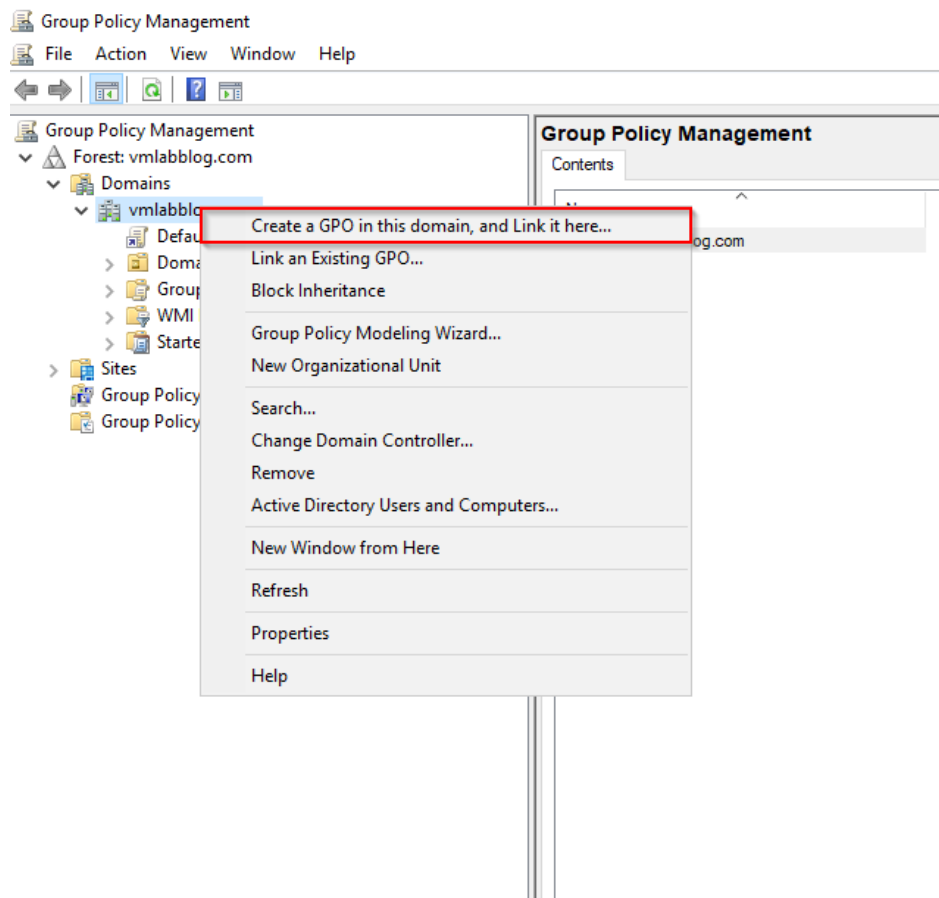
The CA Servers are now configured. Now the domain computers/servers need to trust the certificates which are created by the Subordinate Server. This is done by adding the Root CA certificate to the “Trusted Root Certification Authorities” store. The certificate can be added in multiple ways, but the easiest way is by adding it with a Group Policy. In this example a separate policy is created on the Domain Controller in the root of the domain. This is not required but just an example on how it’s possible.

## Setup Group Policy

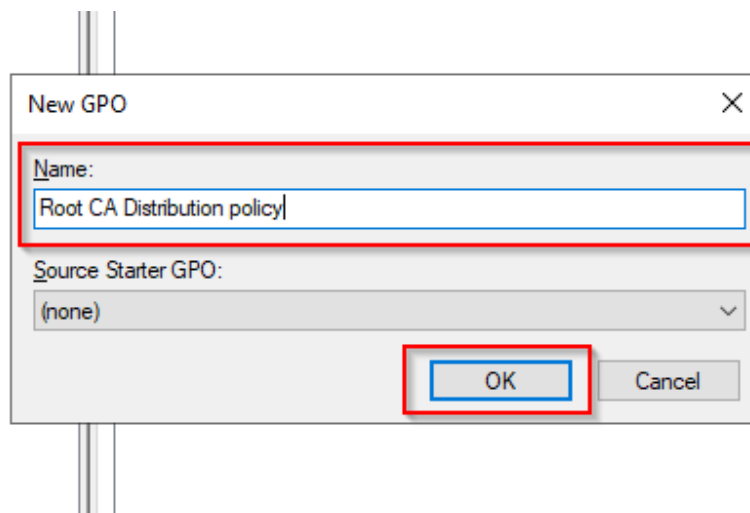
1. Open “Group Policy Management”



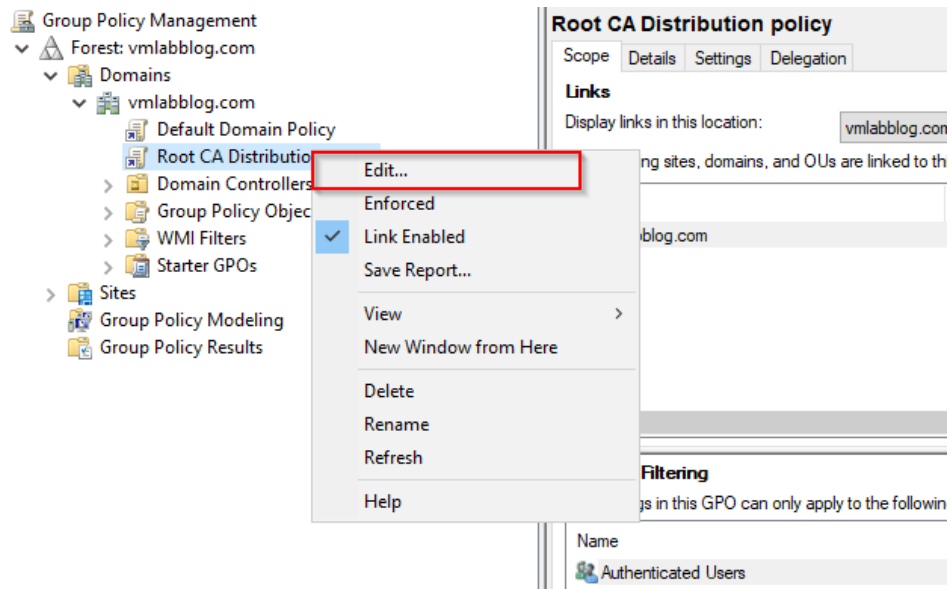
2. Expand “Group Policy Management” -> “Forest: <domain>” -> “Domains” and Rightclick your domain. Select “Create a GPO in this domain, and link it here...”



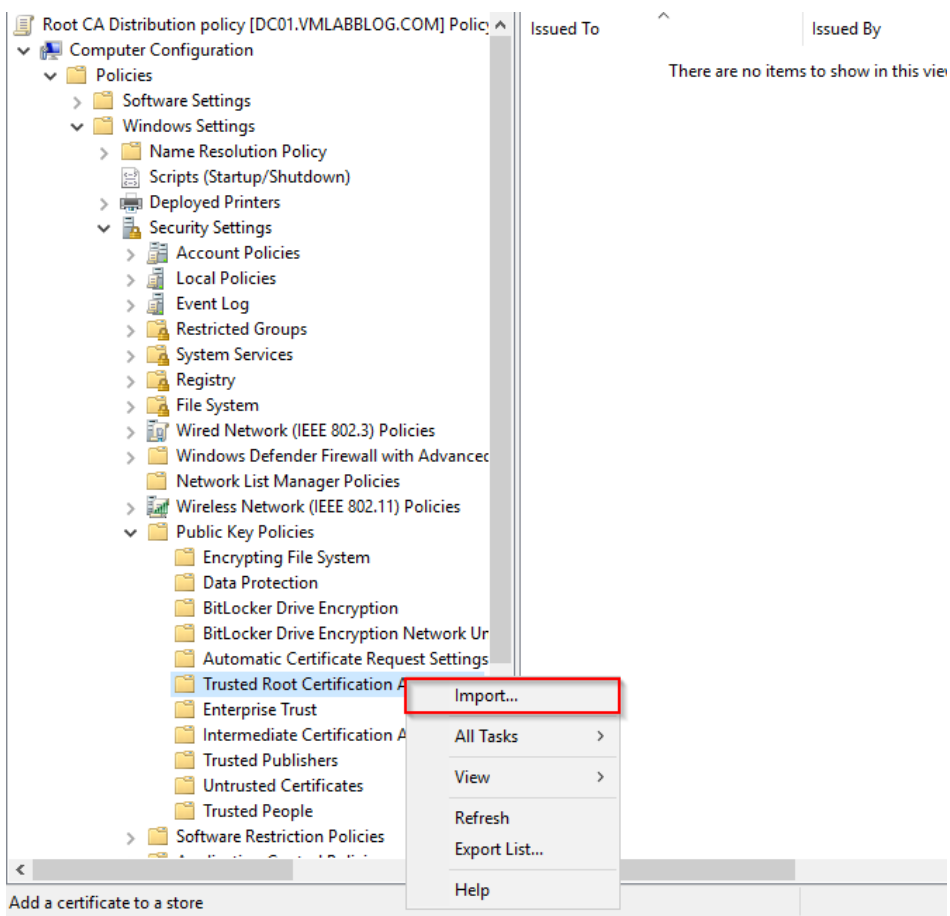
3. Enter a name for the policy for example “Root CA Distribution policy” and press “OK”



4. Select the created policy and press “Edit”



5. Go to: “Computer Configuration” -> “Policies” -> “Windows Settings” -> “Security Settings” -> “Public Key Policies” and Rightclick “Trusted Root Certification Authorities” and select “Import”



6. Press “Next” to continue

## Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

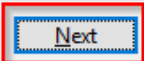
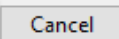
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

☐ Current User

☒ Local Machine

To continue, click Next.

### 7. Press “Browse”

#### File to Import

Specify the file you want to import.

File name:

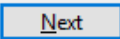
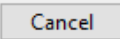


Note: More than one certificate can be stored in a single file in the following formats:

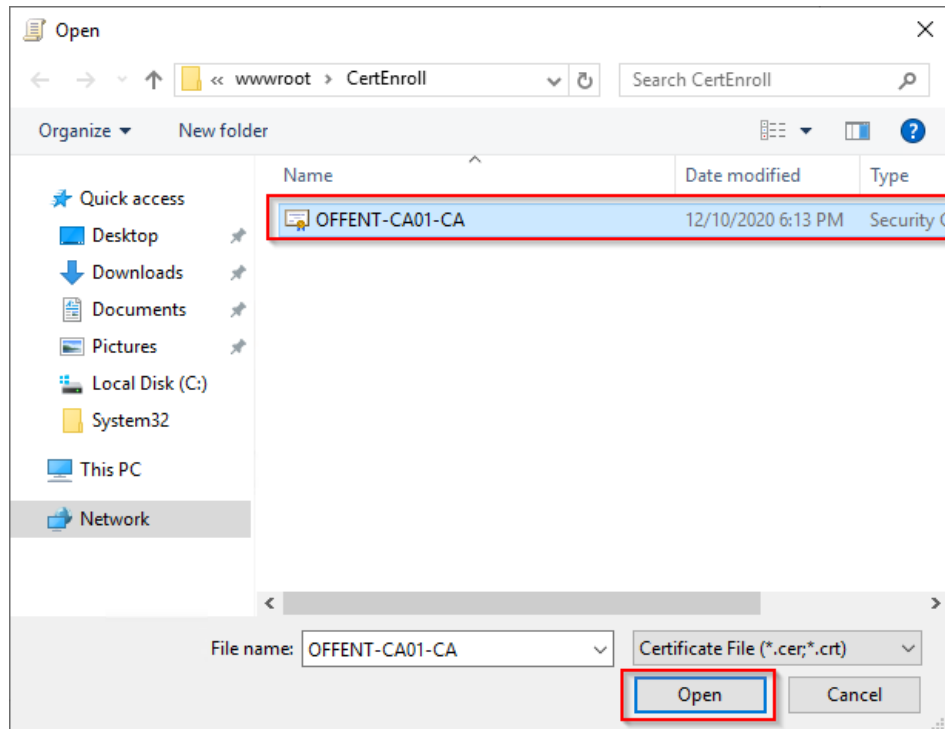
Personal Information Exchange - PKCS #12 (.PFX, .P12)

Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

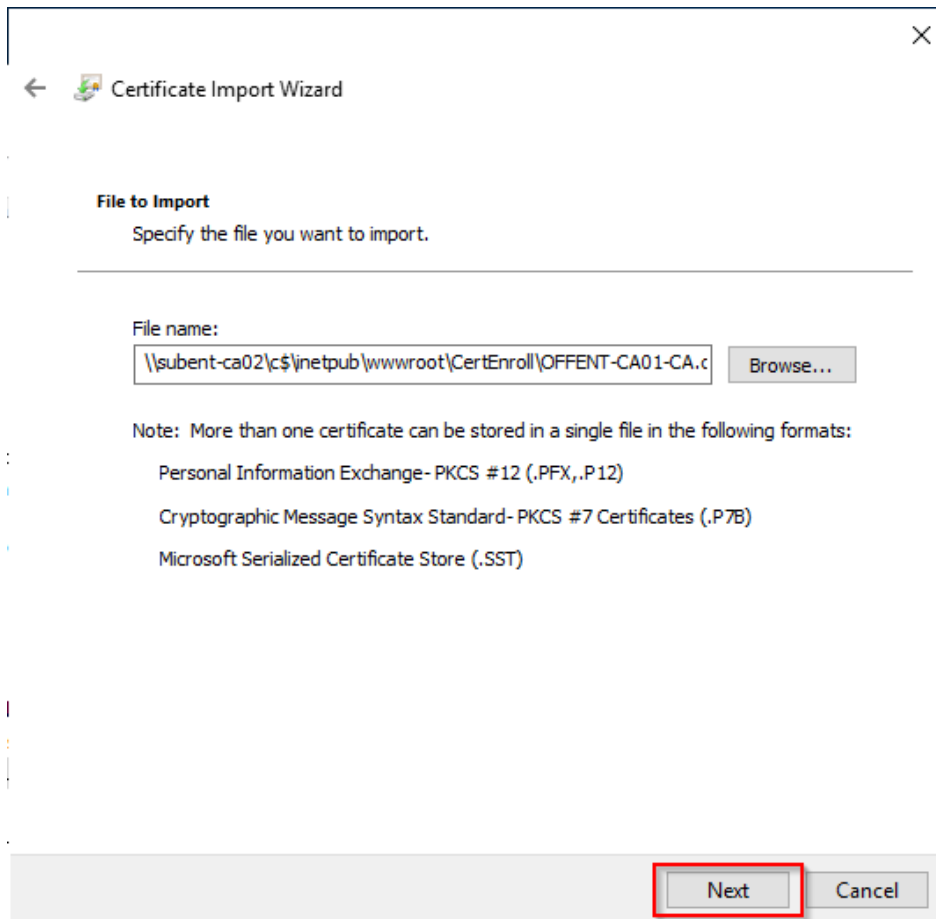
Microsoft Serialized Certificate Store (.SST)

8. Browse to <subordinate-ca>\c\$\inetpub\wwwroot\CertEnroll and select the RootCA certificate. Press “Open” to continue



9. Press “Next” to continue



← Certificate Import Wizard

**File to Import**  
Specify the file you want to import.

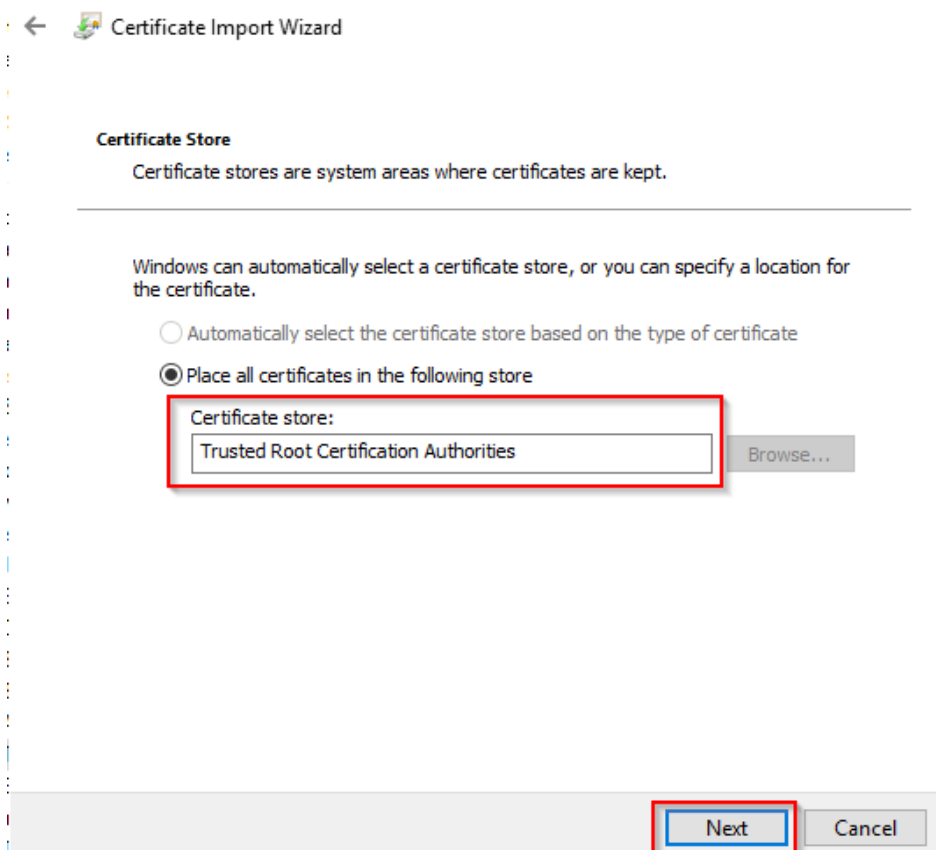
---

File name:

Note: More than one certificate can be stored in a single file in the following formats:

- Personal Information Exchange- PKCS #12 (.PFX, .P12)
- Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
- Microsoft Serialized Certificate Store (.SST)

10. Use the default settings and press “Next”



← Certificate Import Wizard

**Certificate Store**  
Certificate stores are system areas where certificates are kept.

---

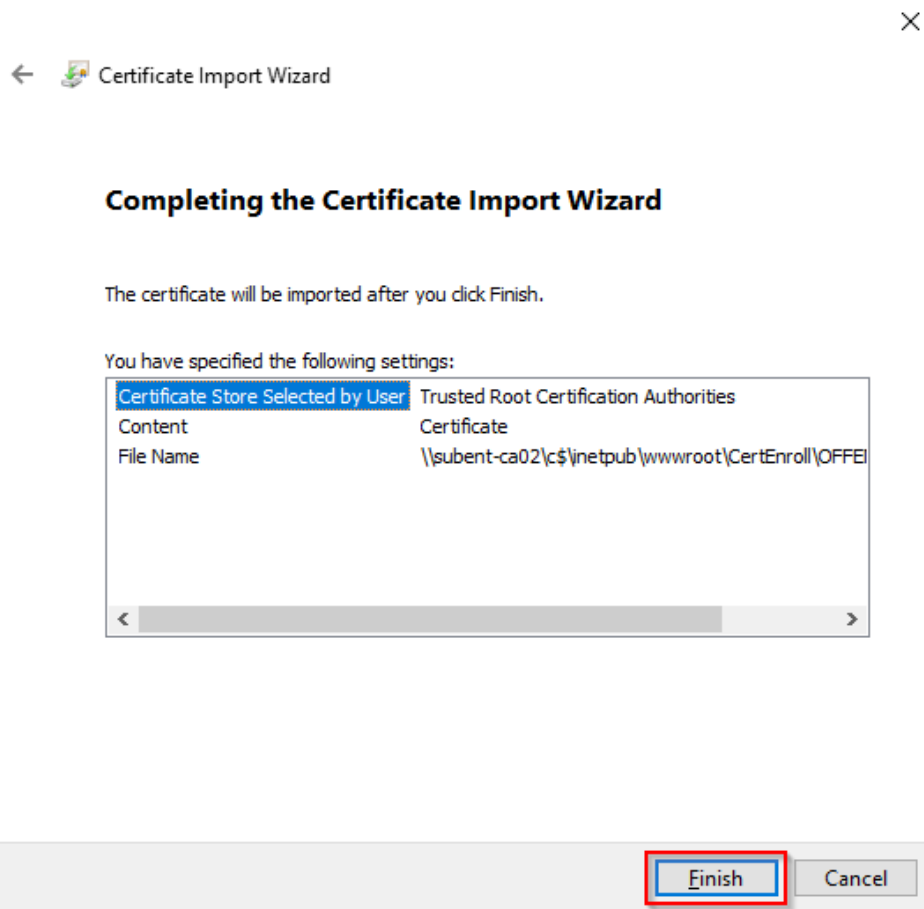
Windows can automatically select a certificate store, or you can specify a location for the certificate.

☐ Automatically select the certificate store based on the type of certificate

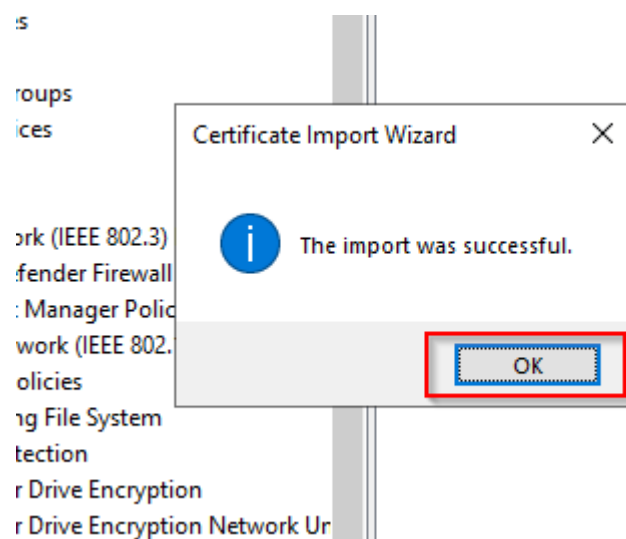
☒ Place all certificates in the following store

Certificate store:

11. Press “Finish” to import the Root CA Certificate.



12. After some time when the import has finished a popup will appear. Press “OK” to continue



The Root CA Certificate is now distributed to all domain devices.

Next: [Deploy Policy Templates](#)