

# Active Directory Certification

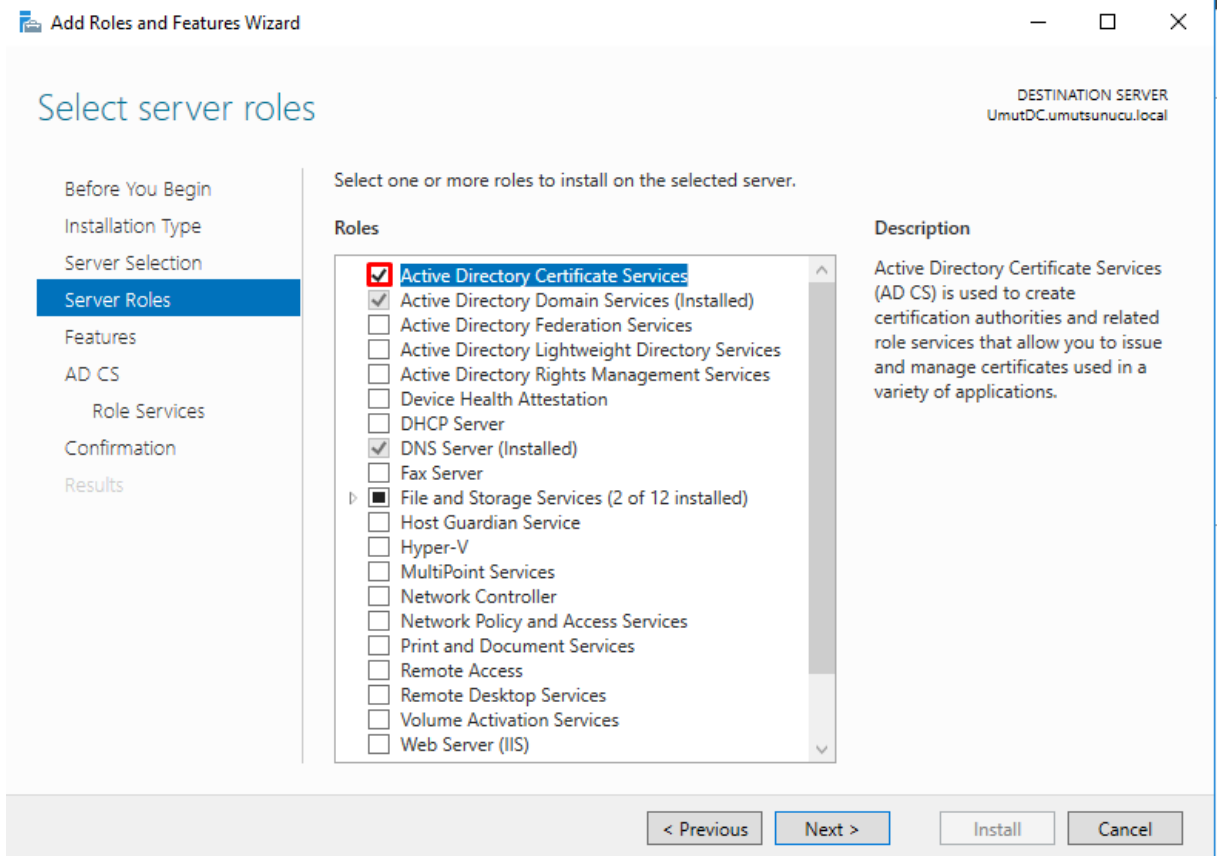
Umut Geer

- 1) Ama
- 2) Eklemeler ve Enterprise CA Kurulumu
- 3) User Kısımındaki Kurulumlar
- 4) Sonu

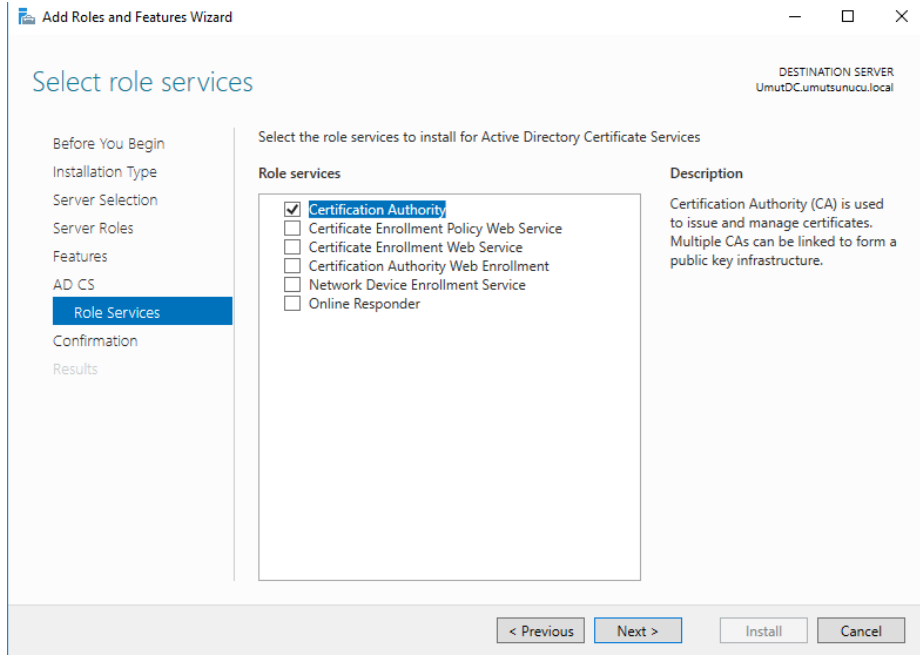
## 1) Amaç

Bu projemizde amaç, domain'imize bağlı host'lar arasında sertifikası olan/olmayan host gruplandırması yaparak, o host'lara belli yaptırımlar uygulamak ya da erişimi engellemektir.

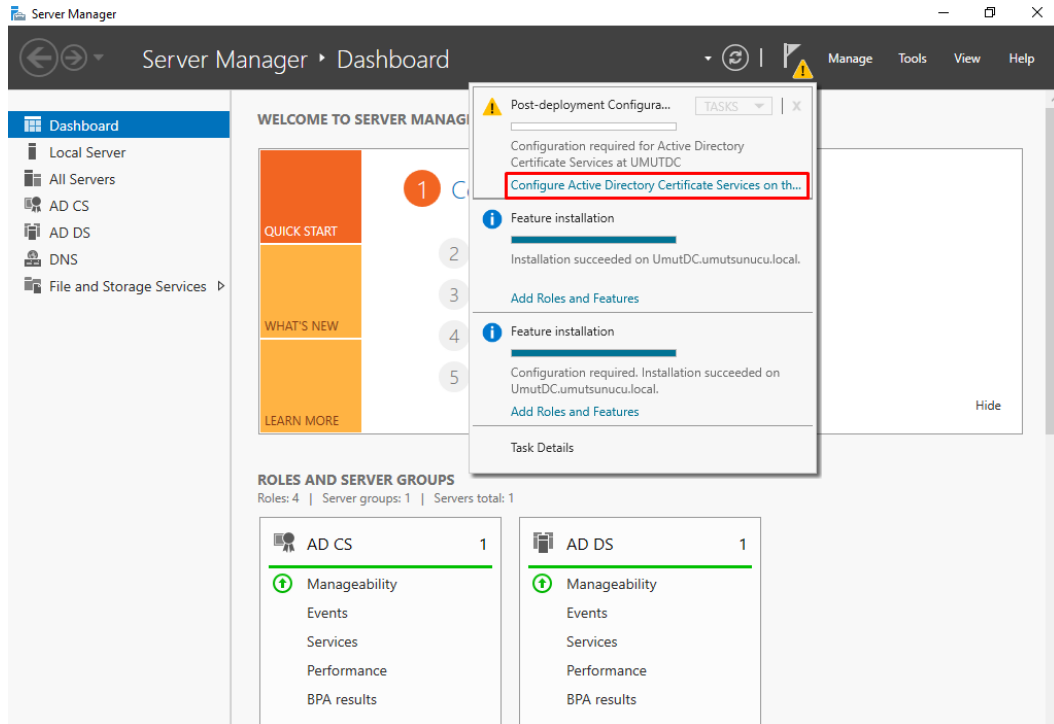
## 2) Eklemeler ve Enterprise CA Kurulumu



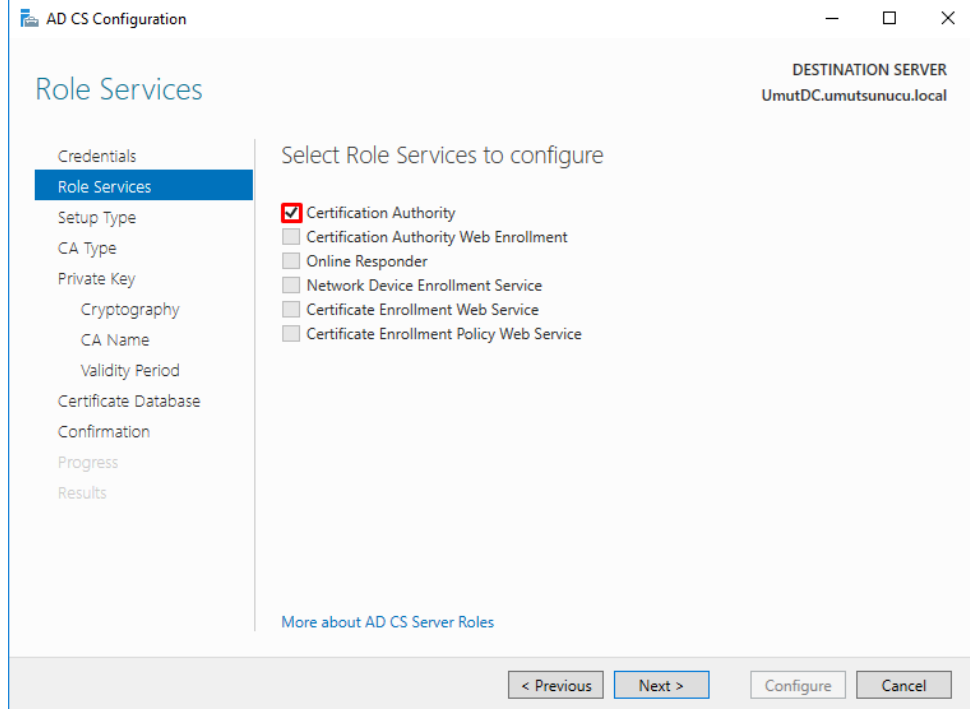
Services rolümüz halihazırda ekliyd. Buna ek olarak, sunucumuza Certificate Services rolünü de ekleriz.



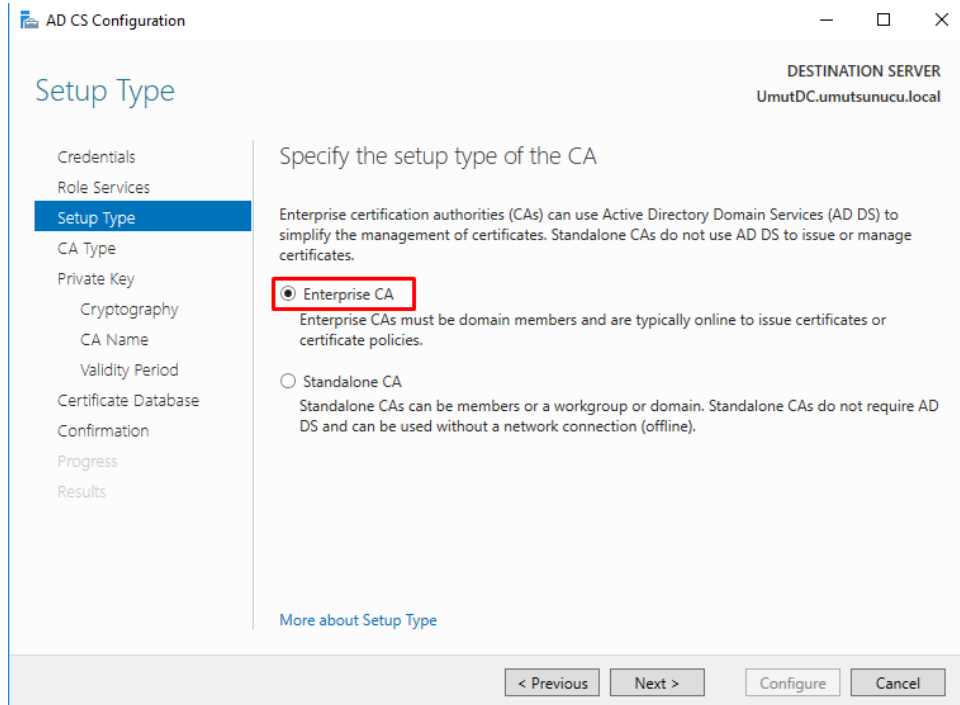
AD CS altında Role Services sekmesinden Certification Authority yüklenir.



Yükleme tamamlandıktan sonra Configure AD CS bağlantısı tıklanır.



Bu sekmede iki önceki adımda yüklemiş olduğumuz CA özelliğini kurarız.



CA ( Certification Authority) 'nin kurulum şeklini seçeriz. Ben Enterprise CA seçtim.

AD CS Configuration

DESTINATION SERVER  
UmutDC.umutsunucu.local

CA Type

Credentials  
Role Services  
Setup Type  
CA Type  
Private Key  
Cryptography  
CA Name  
Validity Period  
Certificate Database  
Confirmation  
Progress  
Results

Specify the type of the CA

When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

☒ Root CA  
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

☐ Subordinate CA  
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

[More about CA Type](#)

< Previous Next > Configure Cancel

PKI hiyerarşisinde Root CA'ler en önde gelir.

AD CS Configuration

DESTINATION SERVER  
UmutDC.umutsunucu.local

Private Key

Credentials  
Role Services  
Setup Type  
CA Type  
Private Key  
Cryptography  
CA Name  
Validity Period  
Certificate Database  
Confirmation  
Progress  
Results

Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

☒ Create a new private key  
Use this option if you do not have a private key or want to create a new private key.

☐ Use existing private key  
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

☐ Select a certificate and use its associated private key  
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

☐ Select an existing private key on this computer  
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

[More about Private Key](#)

< Previous Next > Configure Cancel

Hiç private key'imiz olmadığı için create a new private key deriz.

AD CS Configuration

DESTINATION SERVER  
UmutDC.umutsunucu.local

### Cryptography for CA

Credentials  
Role Services  
Setup Type  
CA Type  
Private Key  
**Cryptography**  
CA Name  
Validity Period  
Certificate Database  
Confirmation  
Progress  
Results

Specify the cryptographic options

Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider

Key length: 2048

Select the hash algorithm for signing certificates issued by this CA:

SHA256  
SHA384  
SHA512  
SHA1  
MD5

☐ Allow administrator interaction when the private key is accessed by the CA.

[More about Cryptography](#)

< Previous Next > Configure Cancel

Key'imizin kriptolanma algoritmasını ve uzunluğunu belirleriz.

AD CS Configuration

DESTINATION SERVER  
UmutDC.umutsunucu.local

### CA Name

Credentials  
Role Services  
Setup Type  
CA Type  
Private Key  
Cryptography  
**CA Name**  
Validity Period  
Certificate Database  
Confirmation  
Progress  
Results

Specify the name of the CA

Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA: umutsunucuşertifika-UMUTDC-CA

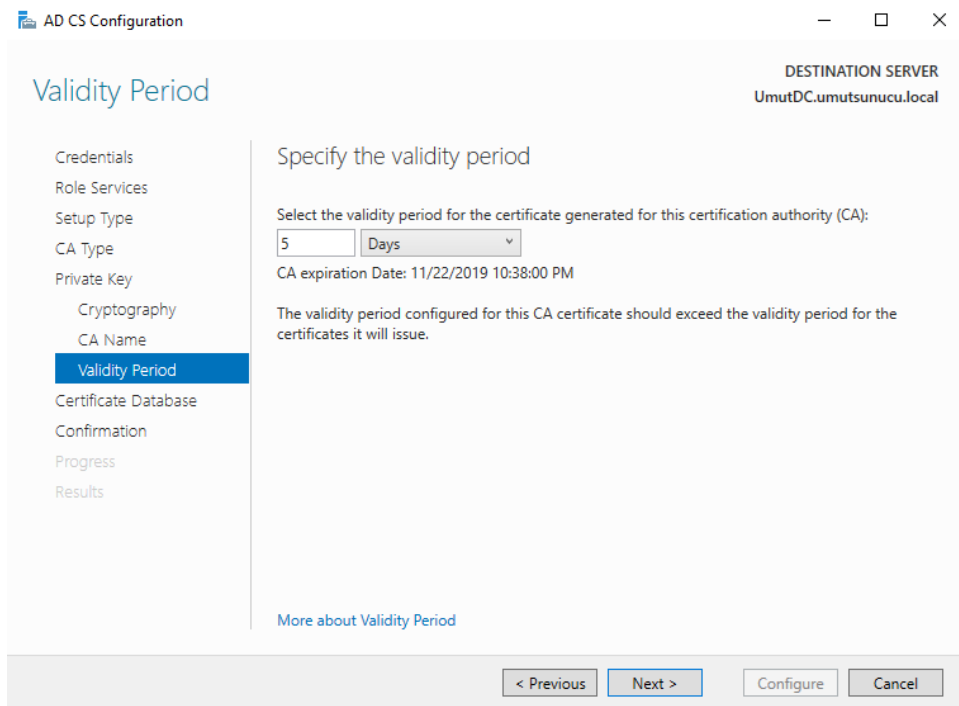
Distinguished name suffix: DC=umutsunucu,DC=local

Preview of distinguished name: CN=umutsunucusertifika-UMUTDC-CA,DC=umutsunucu,DC=local

[More about CA Name](#)

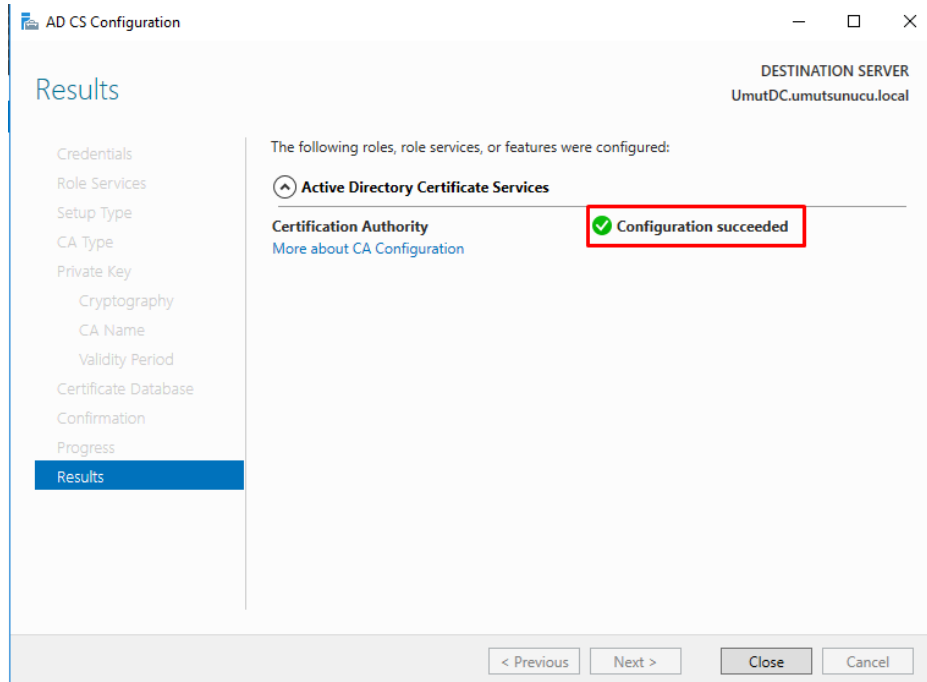
< Previous Next > Configure Cancel

CA ve CA'dan alınan sertifikanın uzantısı için isim belirlenir.



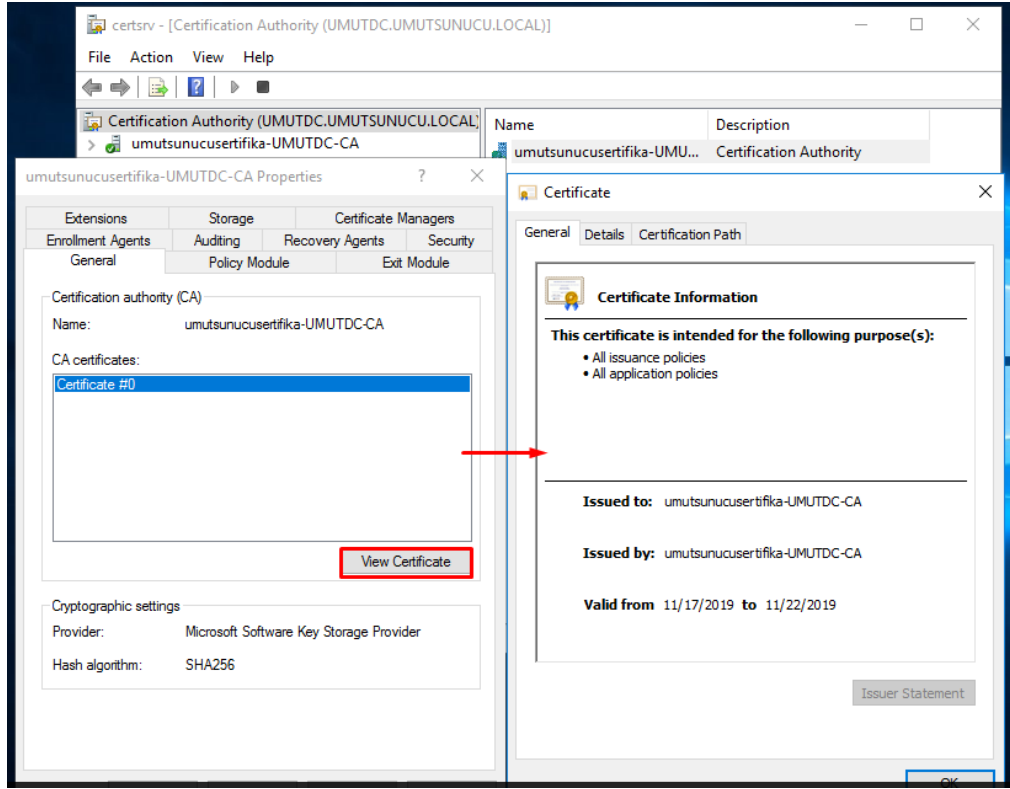
The screenshot shows the 'Validity Period' step in the AD CS Configuration wizard. The left sidebar lists the steps: Credentials, Role Services, Setup Type, CA Type, Private Key, Cryptography, CA Name, **Validity Period**, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Specify the validity period'. It contains a text box with '5' and a dropdown menu set to 'Days'. Below this, it says 'CA expiration Date: 11/22/2019 10:38:00 PM'. A note states: 'The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.' At the bottom, there are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'. The 'DESTINATION SERVER' is listed as 'UmutDC.umutsunucu.local'.

Sertifikanızın geçerlilik süresini belirleriz.



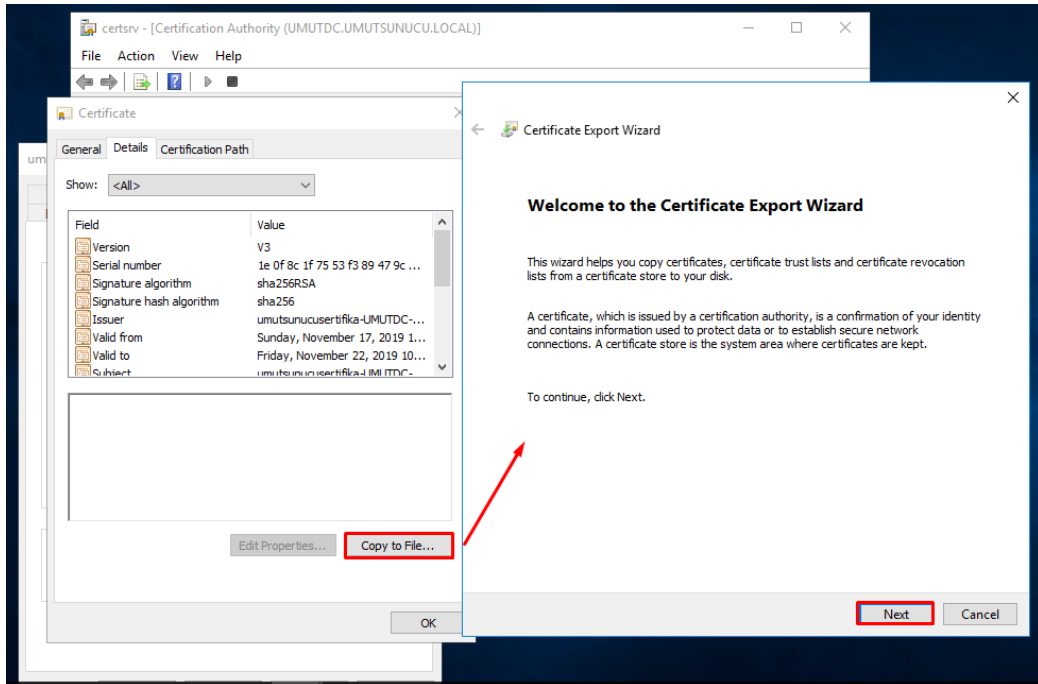
The screenshot shows the 'Results' step in the AD CS Configuration wizard. The left sidebar lists the steps: Credentials, Role Services, Setup Type, CA Type, Private Key, Cryptography, CA Name, Validity Period, Certificate Database, Confirmation, Progress, **Results**, and Results. The main area is titled 'Results'. It contains a section 'The following roles, role services, or features were configured:' with a sub-section 'Active Directory Certificate Services'. Under this, it says 'Certification Authority' with a link 'More about CA Configuration'. To the right of this, there is a green checkmark icon and the text 'Configuration succeeded', which is highlighted with a red rectangle. At the bottom, there are buttons for '< Previous', 'Next >', 'Close', and 'Cancel'. The 'DESTINATION SERVER' is listed as 'UmutDC.umutsunucu.local'.

Kurulumumuzun başarıyla sonlandığı görülür.



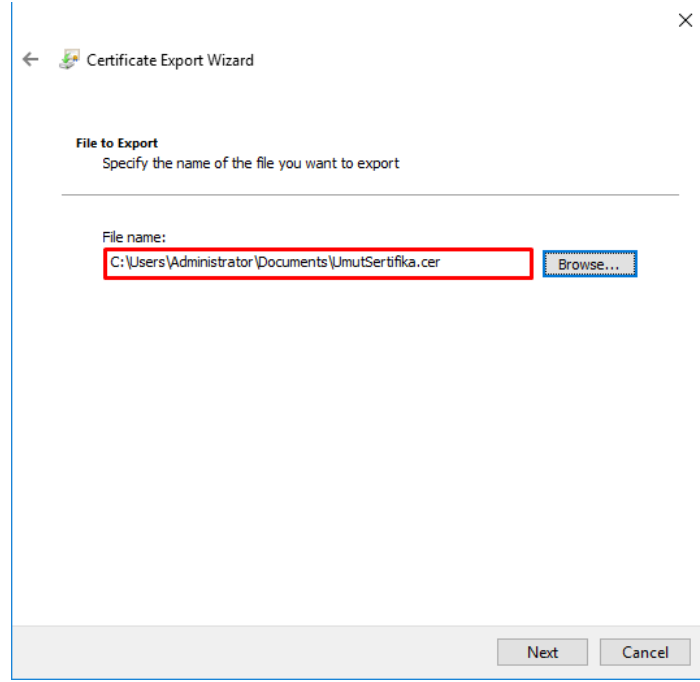
Server Manager > Tools > Certification Authorities seçeriz.

CA üzerine sağ tık > General sekmesi > View Certificate tıklarız.

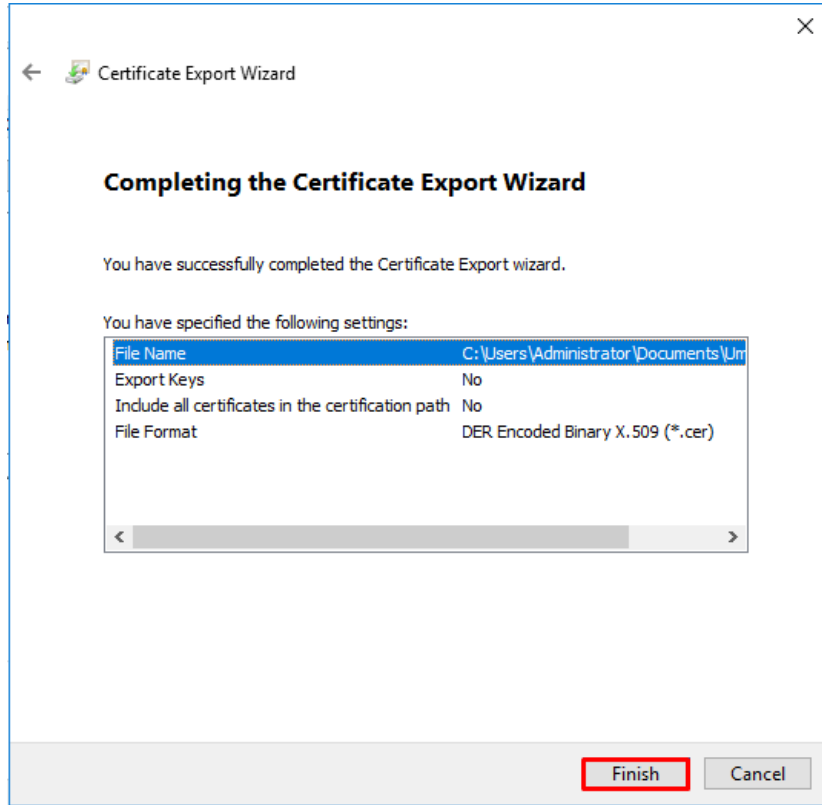




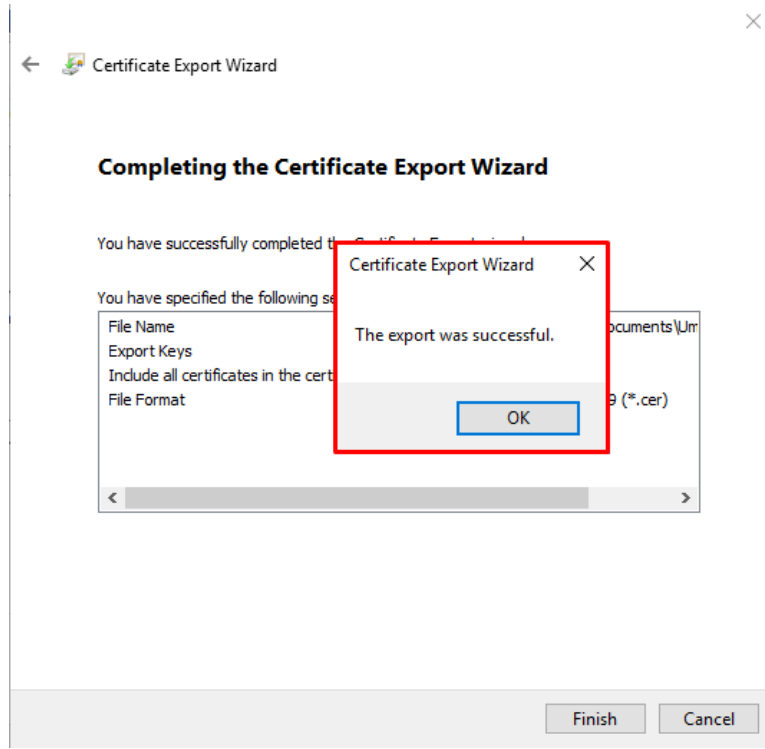
Açılan sekmede Details > Copy to File... > Next tıklanır.



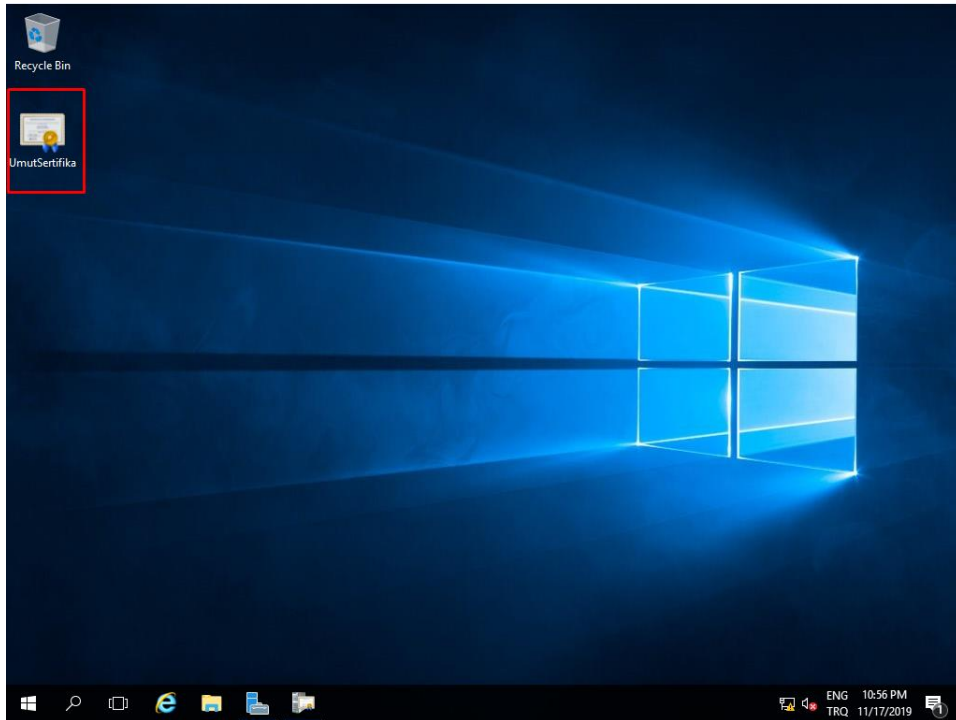
Sertifikayı yerleştireceğimiz klasörü belirleriz.



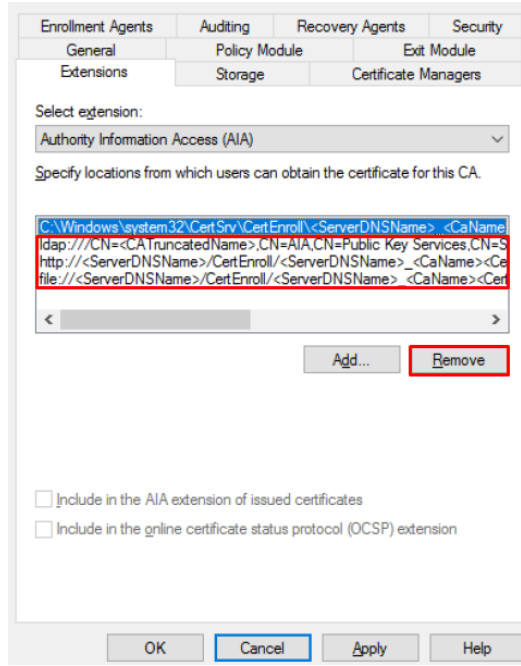
Sertifikayı istediğimiz klasöre yükleriz ve bu işlem tamamlanır.



Export işleminin başarıyla tamamlandığı görülür.

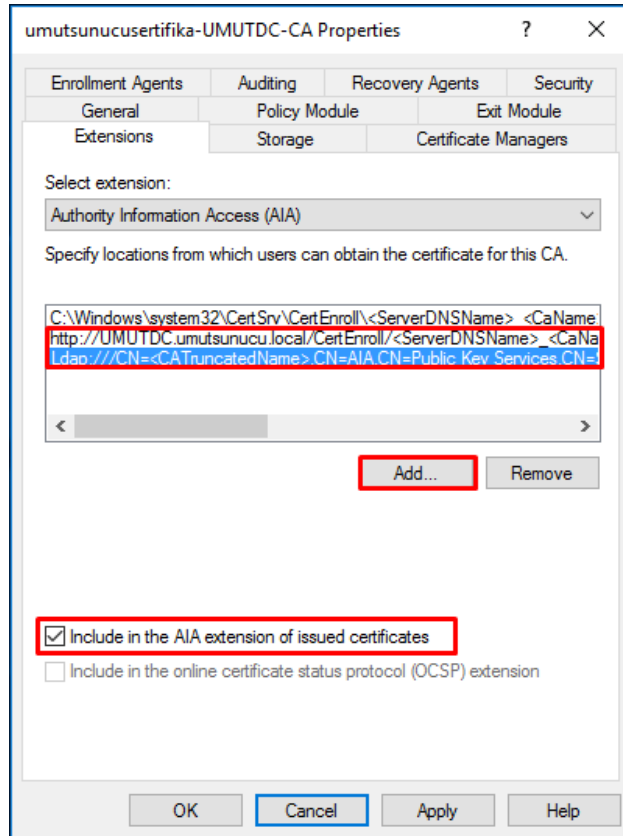


.cer uzantılı sertifikamız masaüstünde görülür.

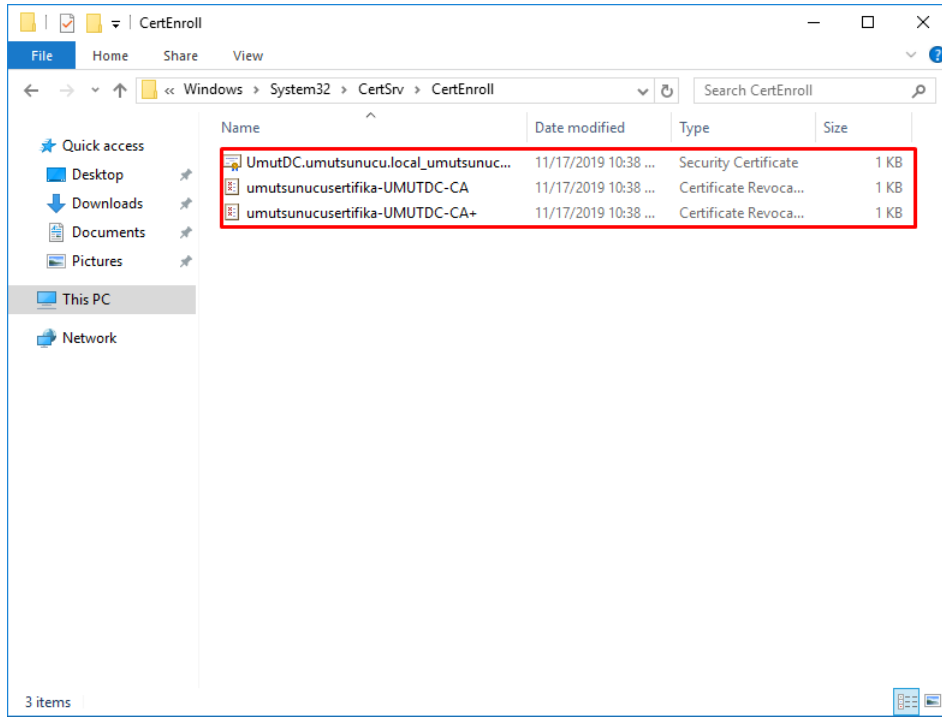


Tekrar Server Manager > Tools > Certification Authorities seçeriz.

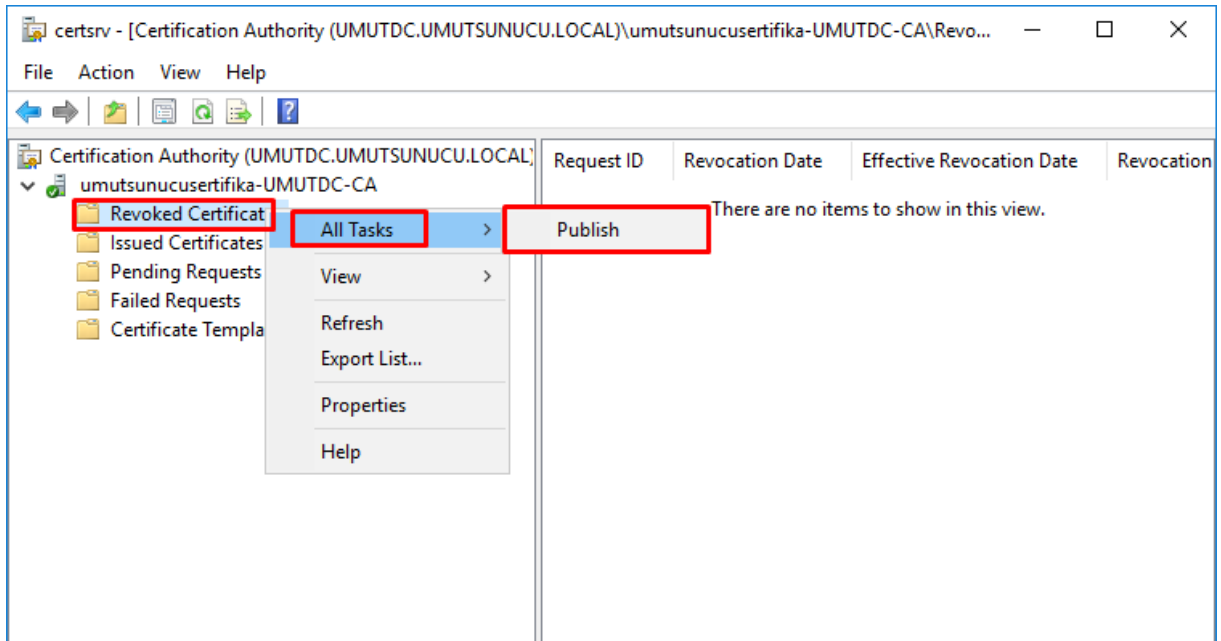
CA üzerine sağ tık > Extension sekmesini seçeriz. Kutu içinde olanları kaldırırız.



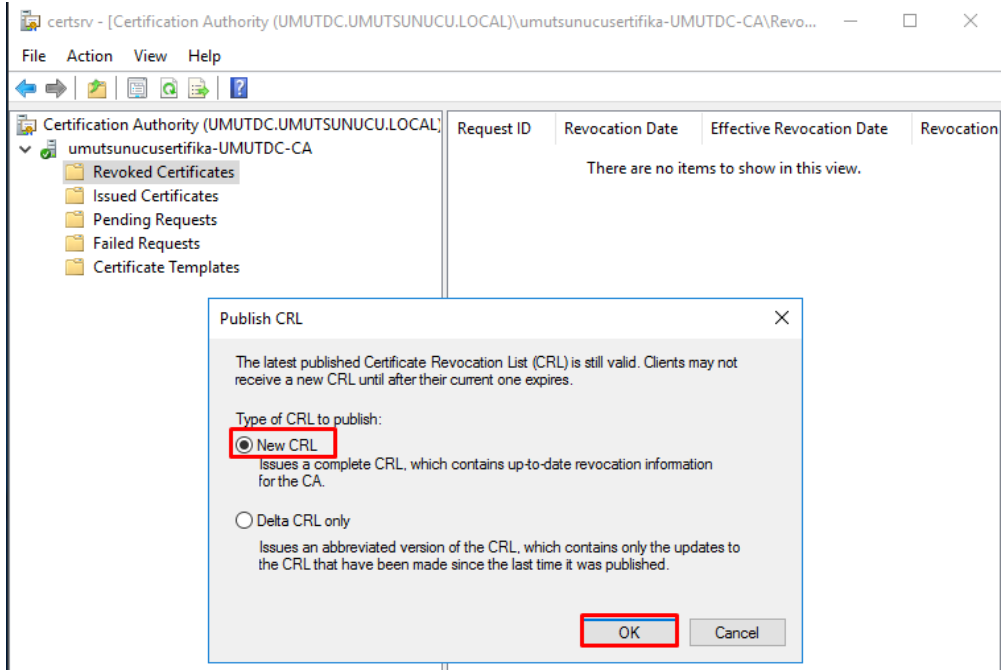
Kaldırdığımız AIA extension'ları yerine, kutu içindeki 2 extension'ı ekleriz.



.crt uzantılı dosyalarımızın oluştuğu görülür.

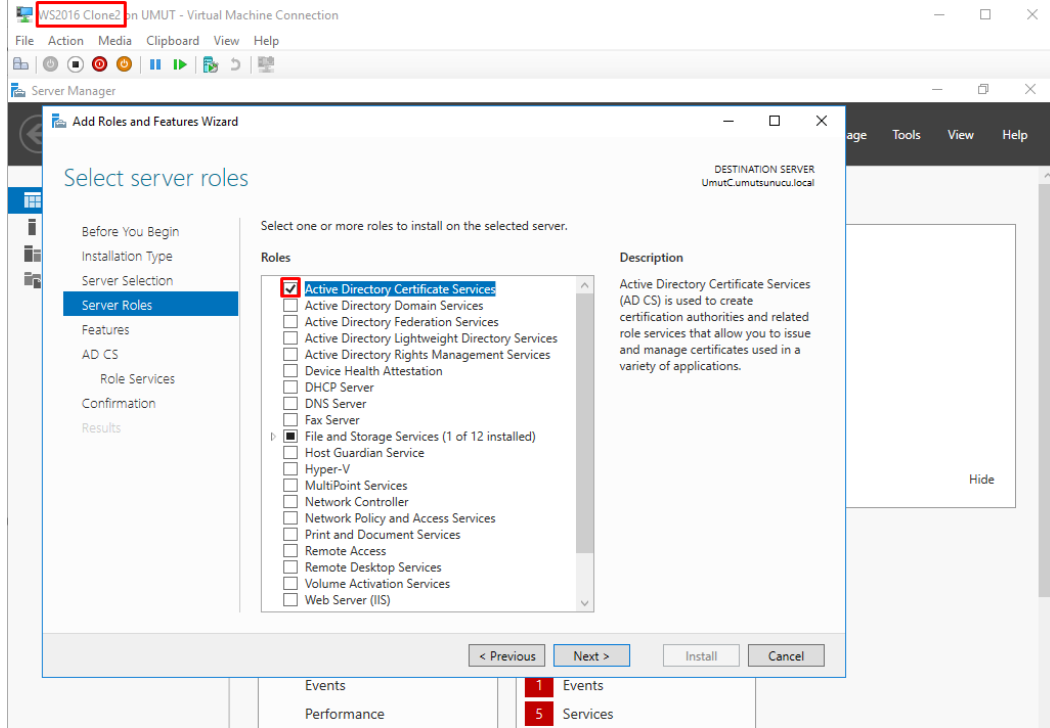


CA'nın alt başlığı olan Revoked Certificate'a sağ tıklarız. > All Tasks > Publish seçilir.

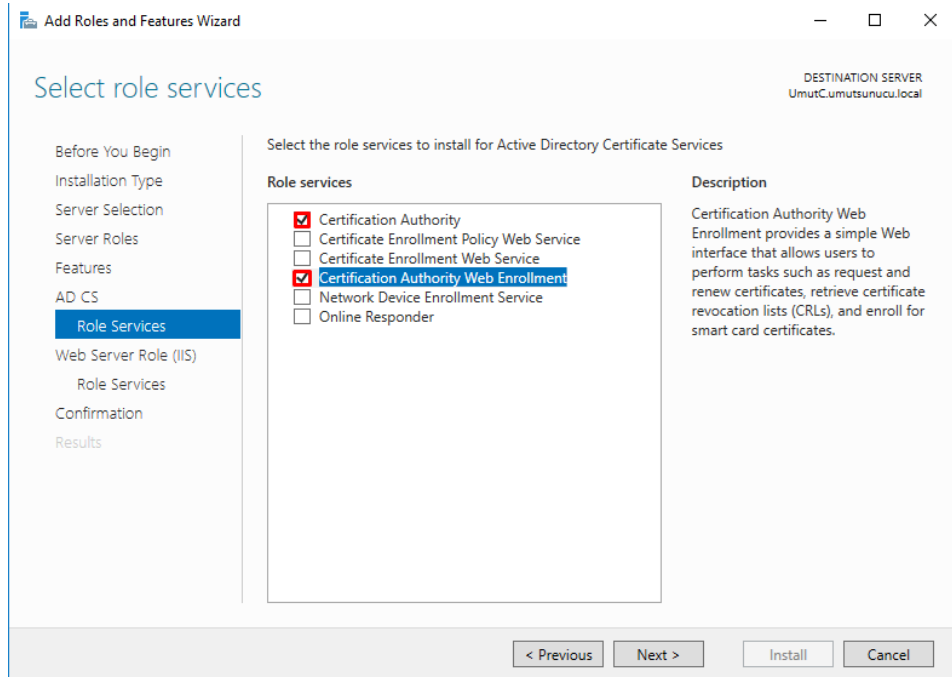


Yeni bir CRL oluşturmak için görseldeki seçeneği tıklarız.

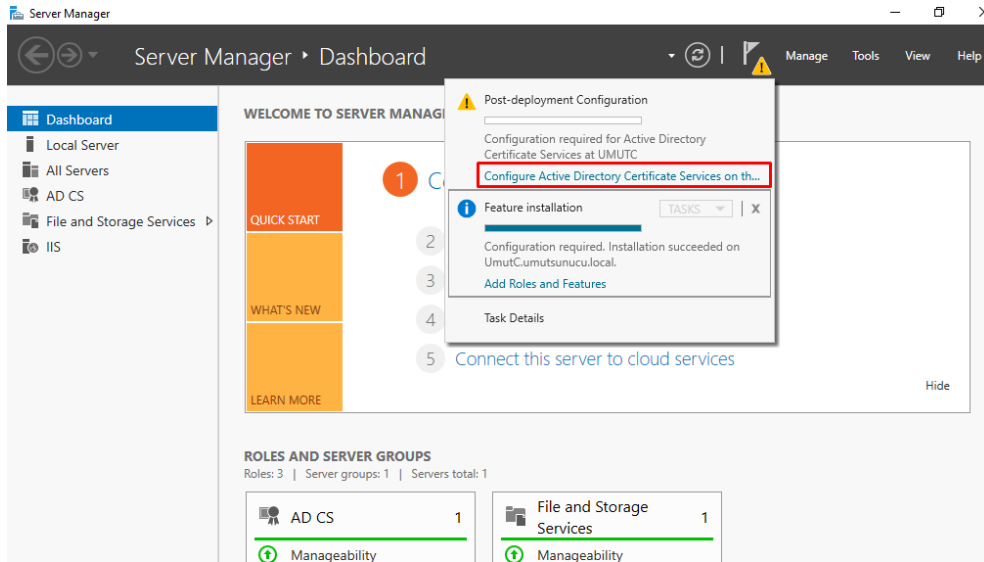
### 3) User Kısımındaki Kurulumlar



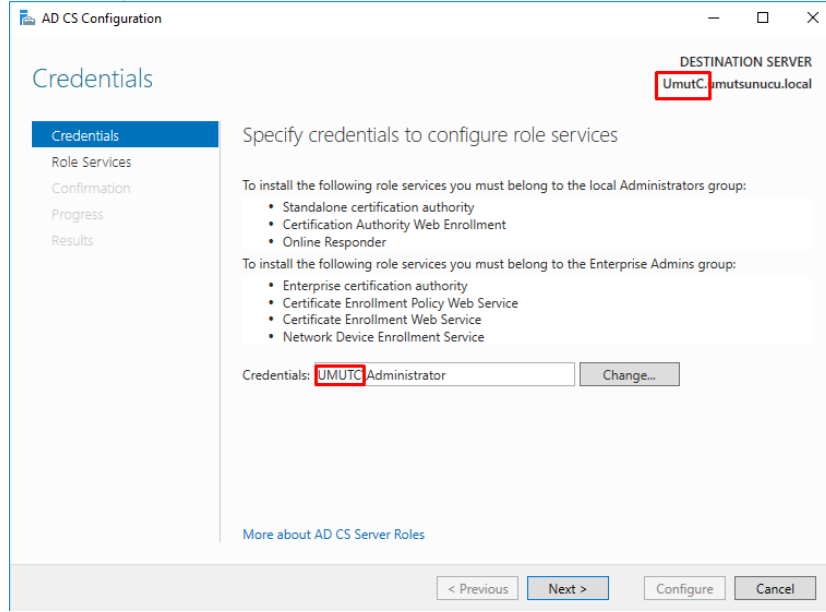
Domain'imizde oluşturduğumuz user'lardan birinden giriş yaparız. Ona da AD Certificate Services yükleriz.



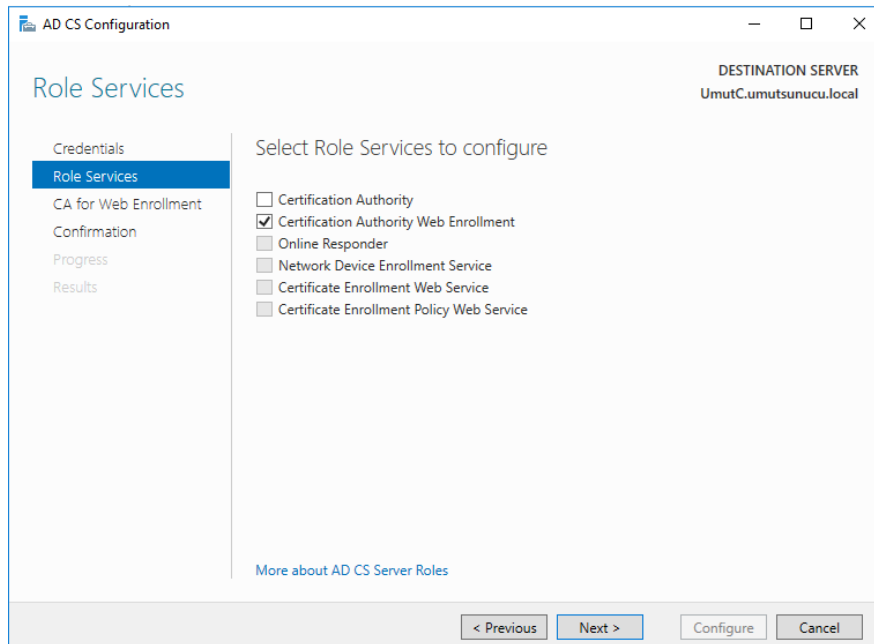
User'ımıza CA ve CA Web Enrollment rol servisleri eklenir.



User tarafında da AD Certification Services konfigür edilir.



Rol servislerinin ekleneceği kullanıcı adı ve uzantısı belirlenir.



Kullanıcıma CA Web Enrollment rol servisi yüklemiştik. Onu konfigüre edeceğiz.



AD CS Configuration

DESTINATION SERVER  
UmutC.umutsunucu.local

## CA for Web Enrollment

Credentials  
Role Services  
**CA for Web Enrollment**  
Confirmation  
Progress  
Results

### Specify CA for Certification Authority Web Enrollment

To select the certification authority (CA) that you want to use for issuing certificates, browse for the name of the CA or the name of the computer that hosts the CA.

Select:  
☐ CA name  
☒ Computer name

Target CA:

[More about CA for Web Enrollment](#)

< Previous   Next >     

CA'yı ismiyle de bulabiliriz; CA'yı içinde bulunduran bilgisayar ismiyle de.

AD CS Configuration

DESTINATION SERVER  
UmutC.umutsunucu.local

## Results

Credentials  
Role Services  
CA for Web Enrollment  
Confirmation  
Progress  
**Results**

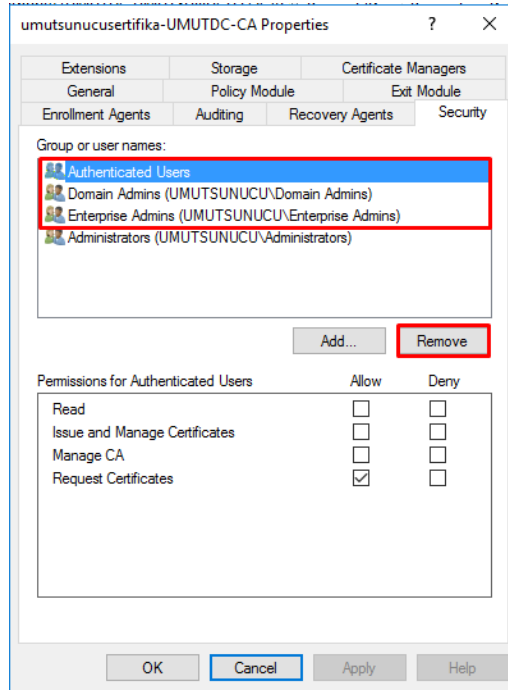
The following roles, role services, or features were configured:

^ **Active Directory Certificate Services**

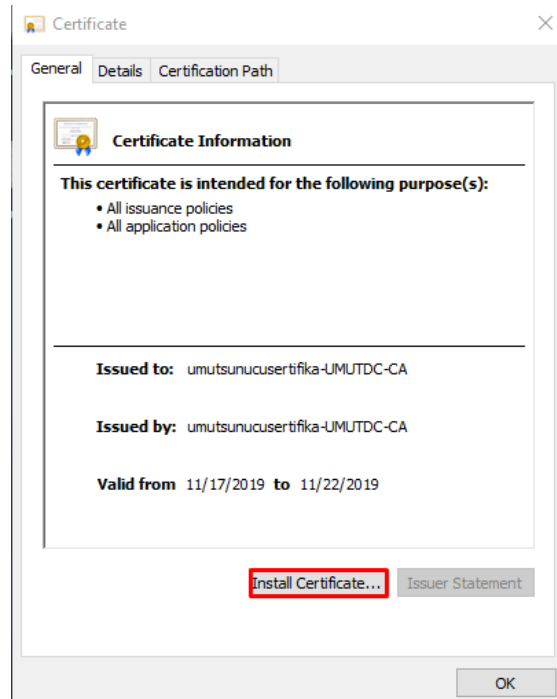
**Certification Authority Web Enrollment** ☒ Configuration succeeded  
[More about Web Enrollment Configuration](#)

< Previous   Next >     

Konfigürasyon tamamlanır.



Admin hariç tüm kullanıcıların giriş izinleri kaldırılır.



Sertifika bu kullanıcıya yüklenir.

## 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

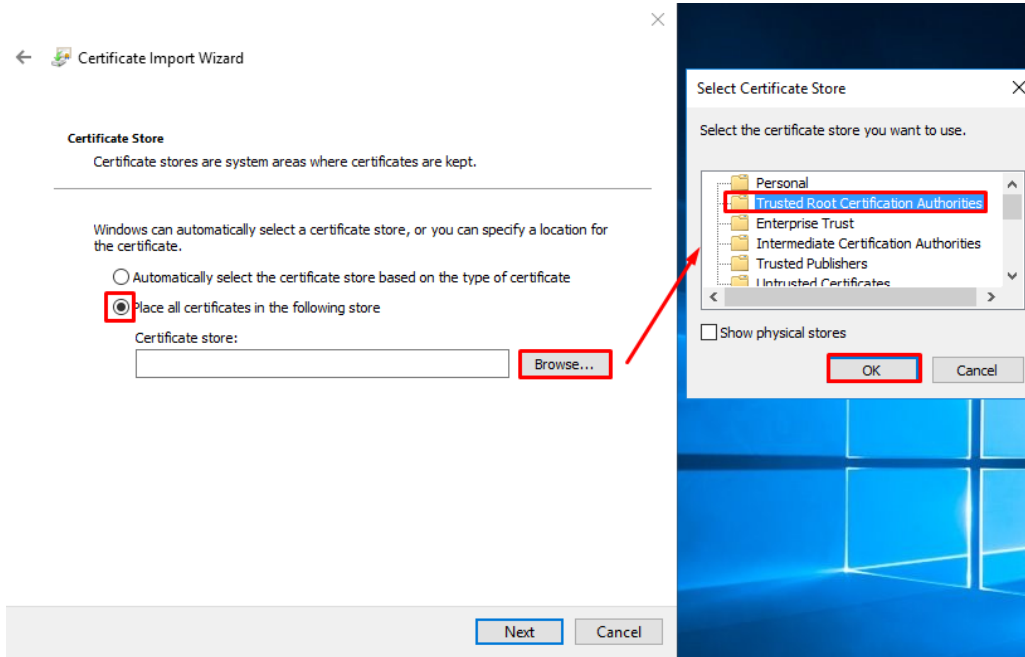
- ☐ Current User  
☒ Local Machine

To continue, click Next.

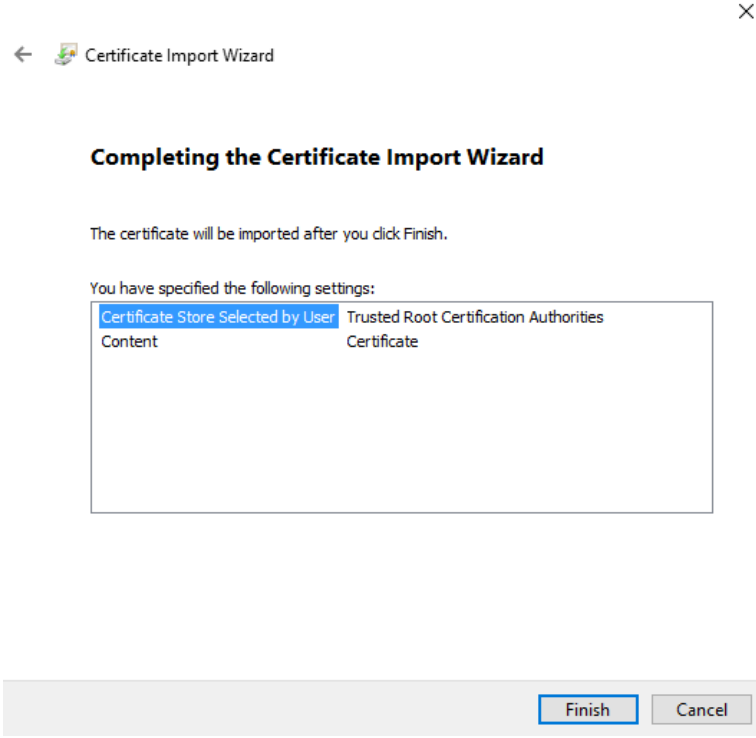
Next

Cancel

Sertifikanın saklanacağı lokasyon seçilir.

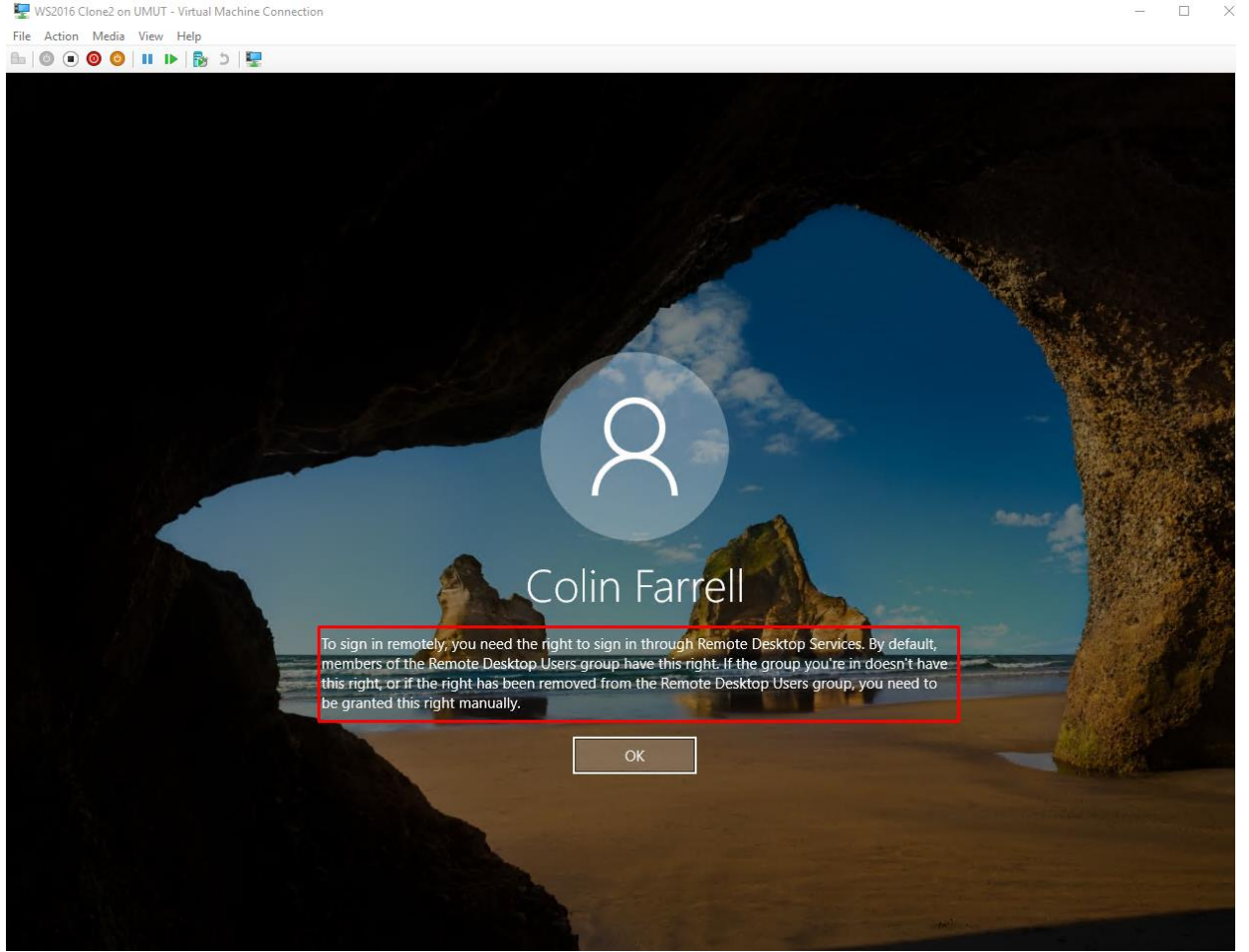


Sertifikanın saklanacağı klasör seçilir.



Sertifika import işlemi tamamlanır.

#### 4) Sonuç



Sertifikası olmayan kullanıcımızın giriş yapamadığı gözlemlendi.