

# Setup LDAPS on Windows server

## How to configure LDAP over SSL (LDAPS) on Windows server?

**Overview:** This article explains how to set up **LDAP over SSL (LDAPS)** to create a secure, encrypted connection between the LDAP server and Ezeelogin.

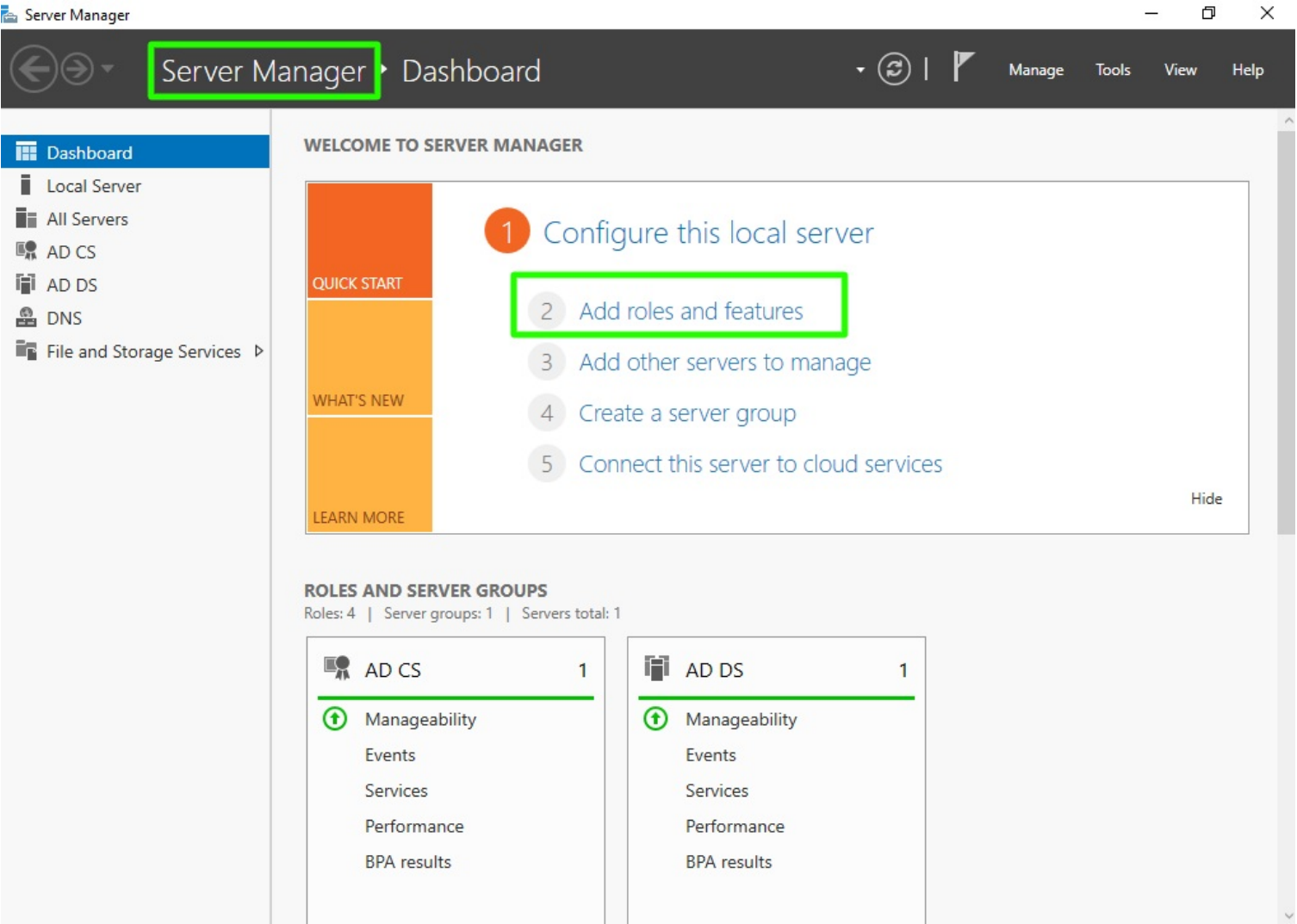
### Steps to secure Active Directory / Configure LDAPS

1. Install Active Directory Certificate Services (AD CS)
2. Create certificate template
3. Issue certificate template
4. Request new certificate for created certificate template
5. Export the created certificate
6. Configure LDAPS on the gateway server

### Detailed Step-by-Step instructions

#### 1 Install Active Directory Certificate Services (AD CS)

**Step 1(A):** On the Windows Server Machine, click on **Start -> Server Manager -> Add Roles and Features**.



**Step 1(B):** After selecting Add Roles and Features and Click on **Next**.

## Before you begin

### Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:  
[Start the Remove Roles and Features Wizard](#)

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

☐ Skip this page by default

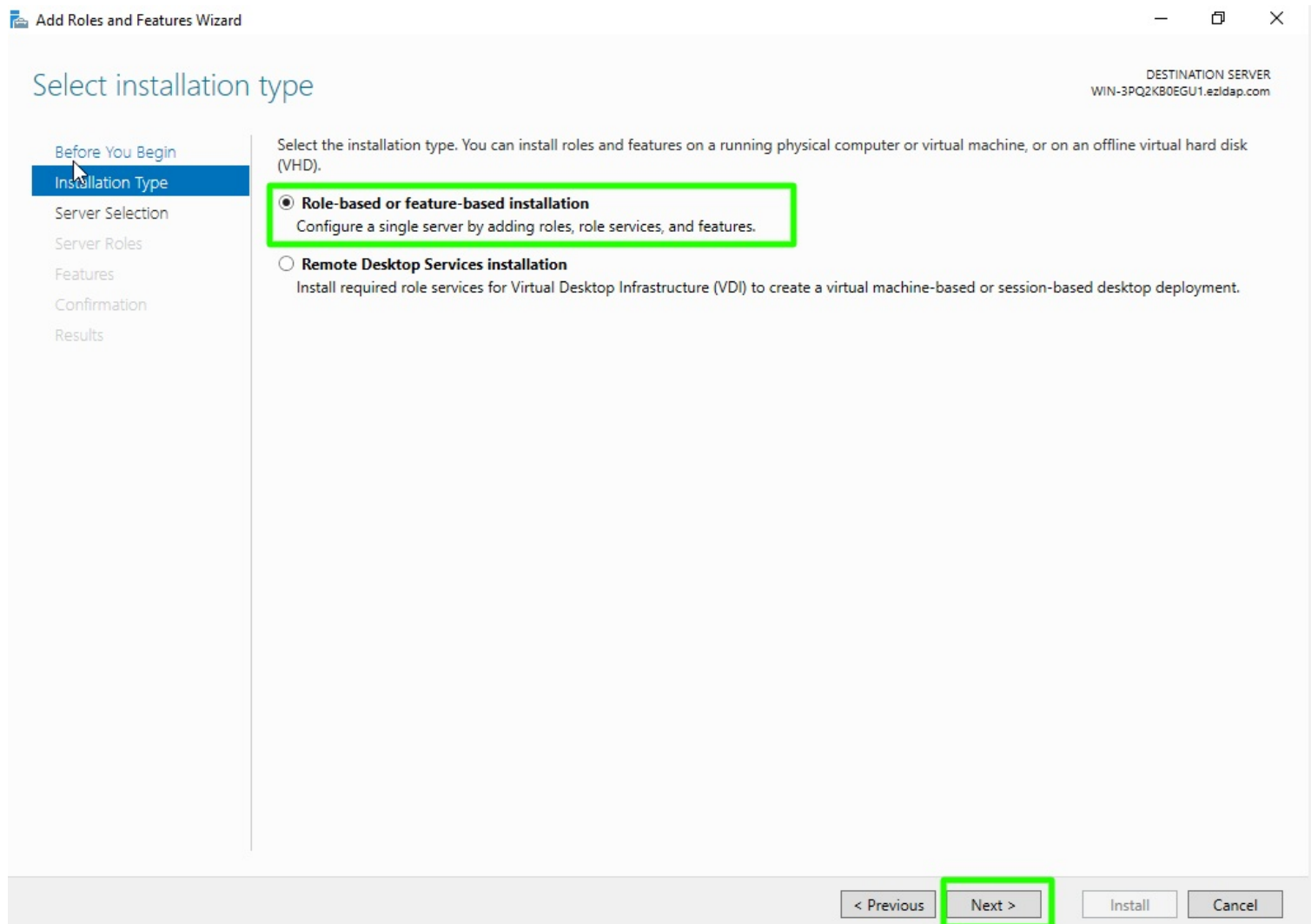
< Previous

Next >

Install

Cancel

**Step 1(C):** Choose "**Role-based or feature-based installation**" option and Click on Next button.



**Step 1(D):** Choose "**Select a server from the server pool**" option & select the **Idap server** from the server pool and click on Next button.

Add Roles and Features Wizard

DESTINATION SERVER  
WIN-3PQ2KB0EGU1.ezldap.com

## Select destination server

Before You Begin

Installation Type

**Server Selection**

Server Roles

Features

Confirmation

Results

Select a server or a virtual hard disk on which to install roles and features.

☒ Select a server from the server pool

☐ Select a virtual hard disk

Server Pool

Filter:

| Name                    | IP Address        | Operating System                                  |
|-------------------------|-------------------|---------------------------------------------------|
| WIN-3PQ2KB0EGU1.ezld... | 169.254.197.23... | Microsoft Windows Server 2022 Standard Evaluation |

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

< Previous

**Next >**

Install

Cancel

**Step 1(E):** Select "**Active Directory Certificate Services**" from the list of roles, then in the next window, click "**Add Features**" and proceed by clicking Next.

## Select server roles

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select one or more roles to install on the selected server.

## Roles

- ☐ Active Directory Certificate Services
- ☒ Active Directory Domain Services (installed)
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation
- ☐ DHCP Server
- ☒ DNS Server (installed)
- ☐ Fax Server
- ☐ File and Storage Services (2 of 12 installed)
- ☐ Host Guardian Service
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services
- ☐ Windows Server Update Services

## Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services. AD CS is used in

**Add Roles and Features Wizard**

**Add features that are required for Active Directory Certificate Services?**

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Remote Server Administration Tools
  - Role Administration Tools
    - Active Directory Certificate Services Tools
      - [Tools] Certification Authority Management Tools

☒ Include management tools (if applicable)

 **Add Features** **Cancel**

&lt; Previous

Next &gt;

Install

Cancel

**Step 1(F):** Choose nothing from the list of features and click on Next button.

## Select features

DESTINATION SERVER  
WIN-3PQ2KB0EGU1.ezldap.com

Before You Begin

Installation Type

Server Selection

Server Roles

**Features**

AD CS

Role Services

Confirmation

Results

Select one or more features to install on the selected server.

## Features

- ▷ ☐ .NET Framework 3.5 Features
- ▷ ☒ .NET Framework 4.8 Features (2 of 7 installed)
- ▷ ☐ Background Intelligent Transfer Service (BITS)
- ☐ BitLocker Drive Encryption
- ☐ BitLocker Network Unlock
- ☐ BranchCache
- ☐ Client for NFS
- ☐ Containers
- ☐ Data Center Bridging
- ☐ Direct Play
- ☐ Enhanced Storage
- ☐ Failover Clustering
- ☒ Group Policy Management (Installed)
- ☐ Host Guardian Hyper-V Support
- ☐ I/O Quality of Service
- ☐ IIS Hostable Web Core
- ☐ Internet Printing Client
- ☐ IP Address Management (IPAM) Server
- ☐ LPR Port Monitor
- ☐ Management OData IIS Extension
- ☐ Media Foundation
- ▷ ☐ Message Queuing
- ☒ Microsoft Defender Antivirus (Installed)
- ☐ Multipath I/O
- ▷ ☐ MultiPoint Connector
- ☐ Network Load Balancing
- ☐ Network Virtualization
- ☐ Peer Name Resolution Protocol
- ☐ Quality Windows Audio Video Experience
- ☐ RAS Connection Manager Administration Kit (CMAK)
- ☐ Remote Assistance

## Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

&lt; Previous

**Next >**

Install

Cancel

**Step 1(G):** In **Active Directory Certificate Services** (AD CS) choose nothing and click on Next button.

# Active Directory Certificate Services

DESTINATION SERVER  
WIN-3PQ2KB0EGU1.ezldap.com

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD CS

Role Services

Confirmation

Results

Active Directory Certificate Services (AD CS) provides the certificate infrastructure to enable scenarios such as secure wireless networks, virtual private networks, Internet Protocol Security (IPSec), Network Access Protection (NAP), encrypting file system (EFS) and smart card log on.

Things to note:

- The name and domain settings of this computer cannot be changed after a certification authority (CA) has been installed. If you want to change the computer name, join a domain, or promote this server to a domain controller, complete these changes before installing the CA. For more information, see certification authority naming.

&lt; Previous

Next &gt;

Install

Cancel

**Step 1(H):** Enable "**Certification Authority**" from the list of roles and click on Next button.



## Select role services

DESTINATION SERVER  
WIN-3PQ2KB0EGU1.ezldap.com

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD CS

Role Services

Confirmation

Results

Select the role services to install for Active Directory Certificate Services

## Role services

- ☒ Certification Authority
- ☐ Certificate Enrollment Policy Web Service
- ☐ Certificate Enrollment Web Service
- ☐ Certification Authority Web Enrollment
- ☐ Network Device Enrollment Service
- ☐ Online Responder

## Description

Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.

&lt; Previous

Next &gt;

Install

Cancel

**Step 1(I):** Click on **install** button to confirm installation.



## Confirm installation selections

DESTINATION SERVER  
WIN-3PQ2KB0EGU1.ezldap.com

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD CS

Role Services

Confirmation

Results

To install the following roles, role services, or features on selected server, click Install.

☐ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Active Directory Certificate Services

Certification Authority

Remote Server Administration Tools

Role Administration Tools

Active Directory Certificate Services Tools

Certification Authority Management Tools

[Export configuration settings](#)  
[Specify an alternate source path](#)

&lt; Previous

Next &gt;

Install

Cancel

**Step 1(J):** Wait for the process to complete, then in the next window, click "**Configure Active Directory Certificate Services on Destination Server**", and finally, click Close.

Add Roles and Features Wizard

DESTINATION SERVER

WIN-3PQ2KB0EGU1.ezldap.com

Installation progress

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD CS

Role Services

Confirmation

Results

View installation progress

Feature installation

Configuration required. Installation succeeded on WIN-3PQ2KB0EGU1.ezldap.com.

Active Directory Certificate Services

Additional steps are required to configure Active Directory Certificate Services on the destination server

Configure Active Directory Certificate Services on the destination server

Certification Authority

Remote Server Administration Tools

Role Administration Tools

Active Directory Certificate Services Tools

Certification Authority Management Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

[Export configuration settings](#)

< Previous

Next >

Close

Cancel

**Step 1(K):** Use the currently logged on user to configure role services and then click on Next button.

## Credentials

DESTINATION SERVER  
WIN-3PQ2KB0EGU1.ezldap.com

## Credentials

Role Services

Confirmation

Progress

Results

## Specify credentials to configure role services

To install the following role services you must belong to the local Administrators group:

- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

To install the following role services you must belong to the Enterprise Admins group:

- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials: EZLDAP\Administrator

Change...

[More about AD CS Server Roles](#)

&lt; Previous

Next &gt;

Configure

Cancel

**Step 1(L):** Enable "**Certification Authority**" from the list of roles and Click on Next button.

## Role Services

DESTINATION SERVER  
WIN-3PQ2KB0EGU1.ezldap.com

Credentials

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Confirmation

Progress

Results

## Select Role Services to configure

- ☒ Certification Authority
- ☐ Certification Authority Web Enrollment
- ☐ Online Responder
- ☐ Network Device Enrollment Service
- ☐ Certificate Enrollment Web Service
- ☐ Certificate Enrollment Policy Web Service

[More about AD CS Server Roles](#)

&lt; Previous

Next &gt;

Configure

Cancel

**Step 1(M):** Choose "**Enterprise CA**" option and click on Next.

## Setup Type

DESTINATION SERVER  
WIN-3PQ2KB0EGU1.ezldap.com

Credentials

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Confirmation

Progress

Results

## Specify the setup type of the CA

Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

☒ Enterprise CA

Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

☐ Standalone CA

Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

[More about Setup Type](#)

&lt; Previous

Next &gt;

Configure

Cancel

**Step 1(N):** Choose "Root CA" option and click on Next button.

## CA Type

DESTINATION SERVER  
WIN-3PQ2KB0EGU1.ezldap.com

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](#)

&lt; Previous

Next &gt;

Configure

Cancel

**Step 1(O):** Choose "Create a new private key" option and click on Next button.

## Private Key

DESTINATION SERVER  
WIN-3PQ2KB0EGU1.ezldap.com

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](#)

&lt; Previous

Next &gt;

Configure

Cancel

**Step 1(P):** Choose "SHA256" as the hash algorithm and click on Next. Recommended to select the most recent hashing algorithm.



## Cryptography for CA

DESTINATION SERVER  
WIN-3PQ2KB0EGU1.ezldap.com

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

MD4

MD2

☐ Allow administrator interaction when the private key is accessed by the CA.[More about Cryptography](#)

&lt; Previous

Next &gt;

Configure

Cancel

**Step 1(Q):** Click on Next button.

## CA Name

DESTINATION SERVER  
WIN-3PQ2KB0EGU1.ezldap.com

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:

ezldap-WIN-3PQ2KB0EGU1-CA-1

Distinguished name suffix:

DC=ezldap,DC=com

Preview of distinguished name:

CN=ezldap-WIN-3PQ2KB0EGU1-CA-1,DC=ezldap,DC=com

[More about CA Name](#)

&lt; Previous

Next &gt;

Configure

Cancel

**Step 1(R):** Set the certificate validity period to the default value of 5 years, then click Next.

## Validity Period

DESTINATION SERVER  
WIN-3PQ2KB0EGU1.ezldap.com

Credentials

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Confirmation

Progress

Results

## Specify the validity period

Select the validity period for the certificate generated for this certification authority (CA):

 Years

CA expiration Date: 9/24/2030 4:04:00 PM

The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.

[More about Validity Period](#)

&lt; Previous

Next &gt;

Configure

Cancel

**Step 1(S):** Select the **default database location** and click on Next.

## CA Database

DESTINATION SERVER  
WIN-3PQ2KB0EGU1.ezldap.com

Credentials

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Confirmation

Progress

Results

## Specify the database locations

Certificate database location:

C:\Windows\system32\CertLog

Certificate database log location:

C:\Windows\system32\CertLog

[More about CA Database](#)

&lt; Previous

Next &gt;

Configure

Cancel

**Step 1(T):** Click on **Configure** button to confirm.

## Confirmation

DESTINATION SERVER  
WIN-3PQ2KB0EGU1.ezldap.com

Credentials

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Confirmation

Progress

Results

To configure the following roles, role services, or features, click Configure.

## ^ Active Directory Certificate Services

## Certification Authority

|                                    |                                                 |
|------------------------------------|-------------------------------------------------|
| CA Type:                           | Enterprise Root                                 |
| Cryptographic provider:            | RSA#Microsoft Software Key Storage Provider     |
| Hash Algorithm:                    | SHA256                                          |
| Key Length:                        | 2048                                            |
| Allow Administrator Interaction:   | Disabled                                        |
| Certificate Validity Period:       | 9/25/2030 10:01:00 AM                           |
| Distinguished Name:                | CN=ezldap-WIN-3PQ2KB0EGU1-CA-1,DC=ezldap,DC=com |
| Certificate Database Location:     | C:\Windows\system32\CertLog                     |
| Certificate Database Log Location: | C:\Windows\system32\CertLog                     |

&lt; Previous

Next &gt;

Configure

Cancel

**Step 1(U):** Once the configuration succeeded and click on Close button.

## Results

DESTINATION SERVER  
WIN-3PQ2KB0EGU1.ezldap.com

Credentials

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Confirmation

Progress

Results

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

## ^ Active Directory Certificate Services

## Certification Authority

[More about CA Configuration](#)

✓ Configuration succeeded

&lt; Previous

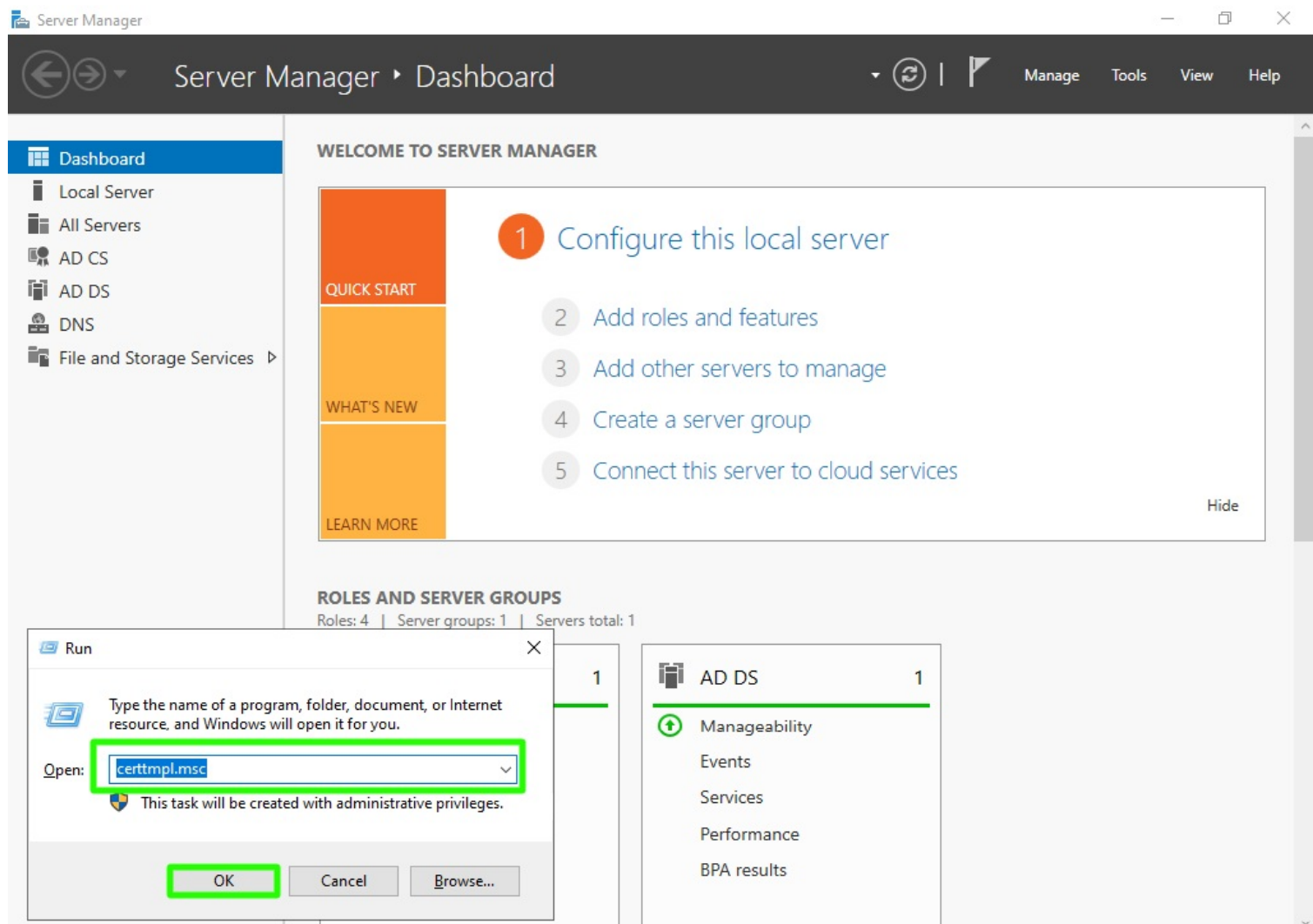
Next &gt;

Close

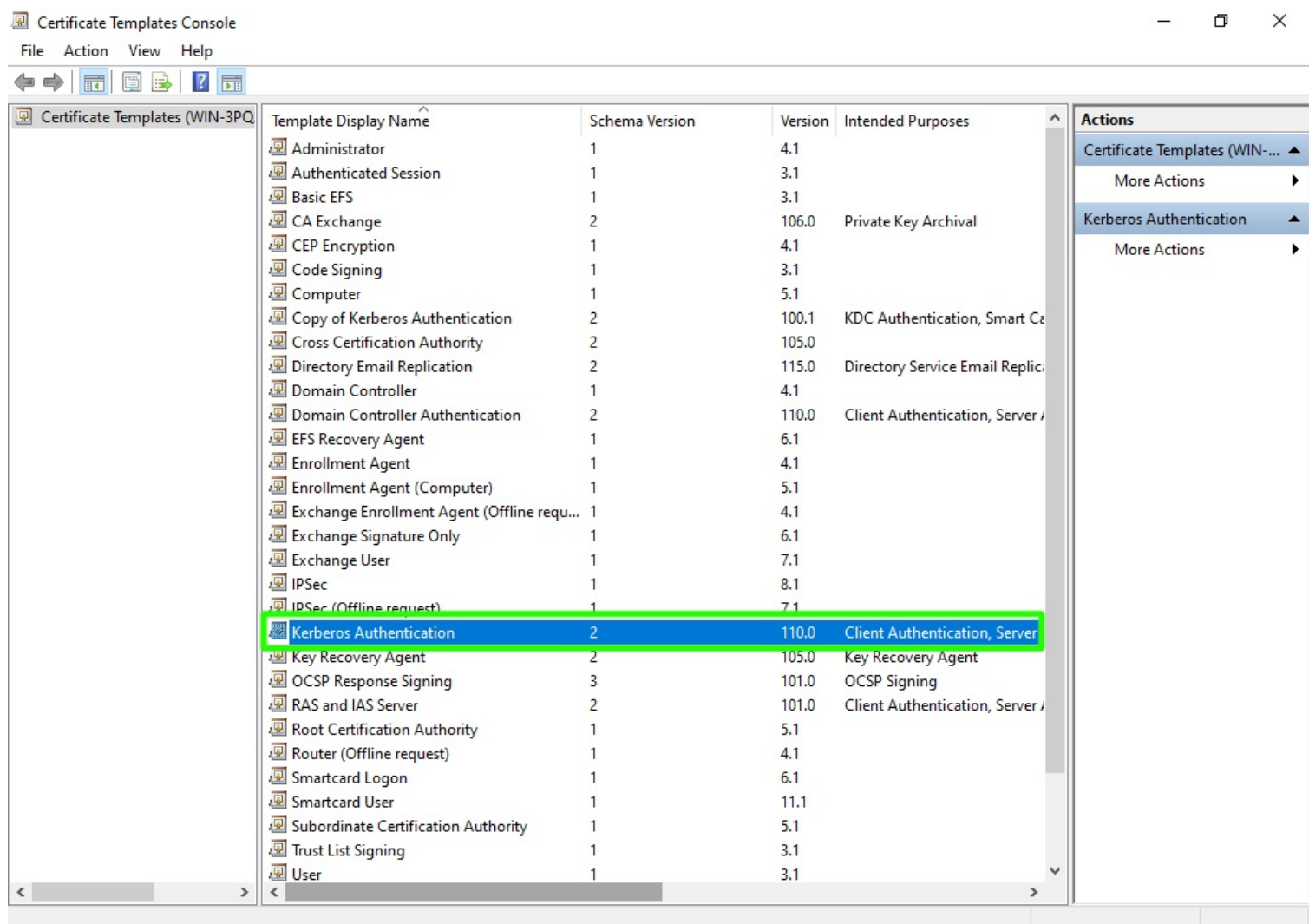
Cancel

## 2. Create certificate template

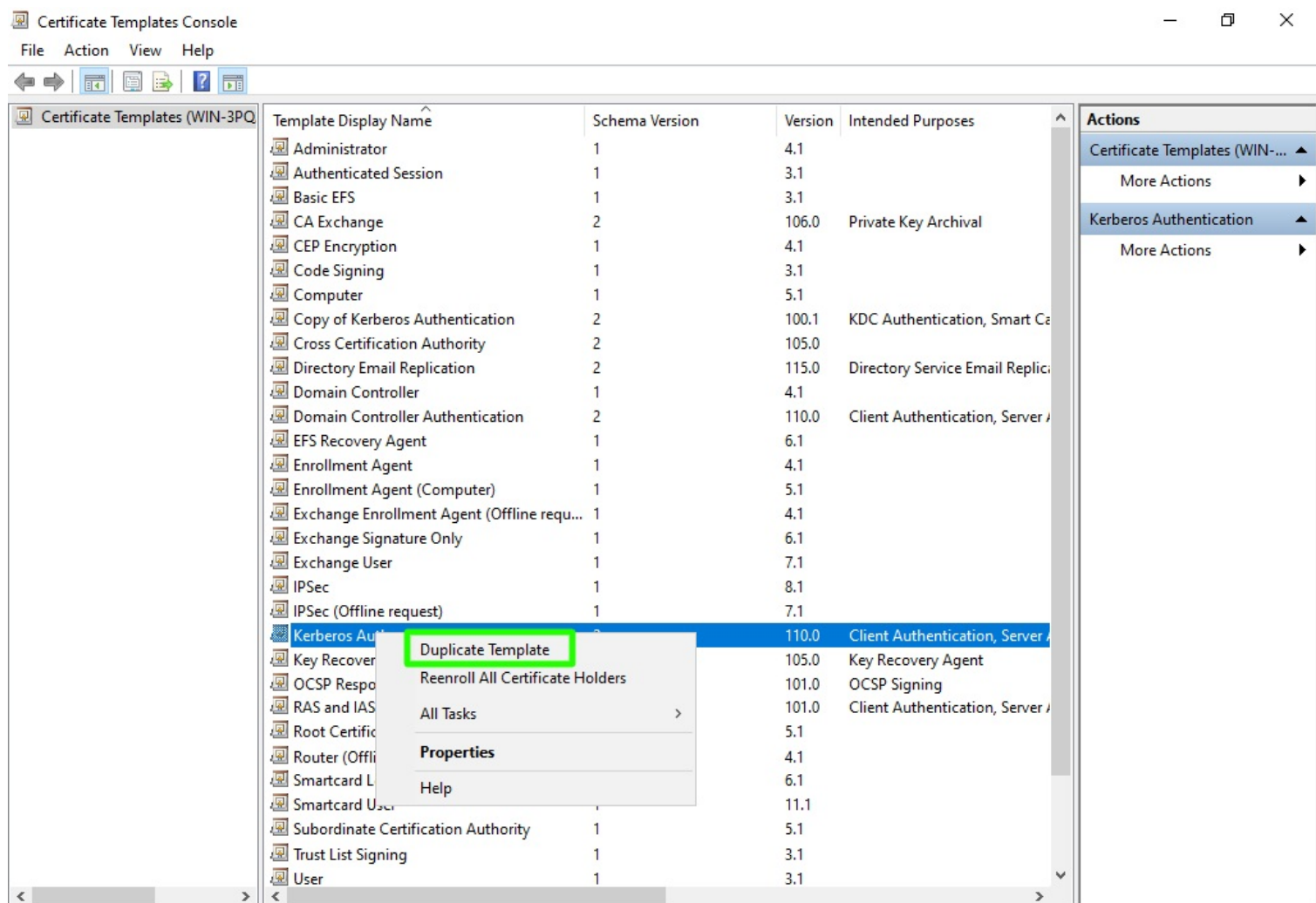
**Step 2(A):** Press **Windows Key+R**, and type **certtmpl.msc**, and press Enter.



**Step 2(B):** Then, select the "**Kerberos Authentication**" template.

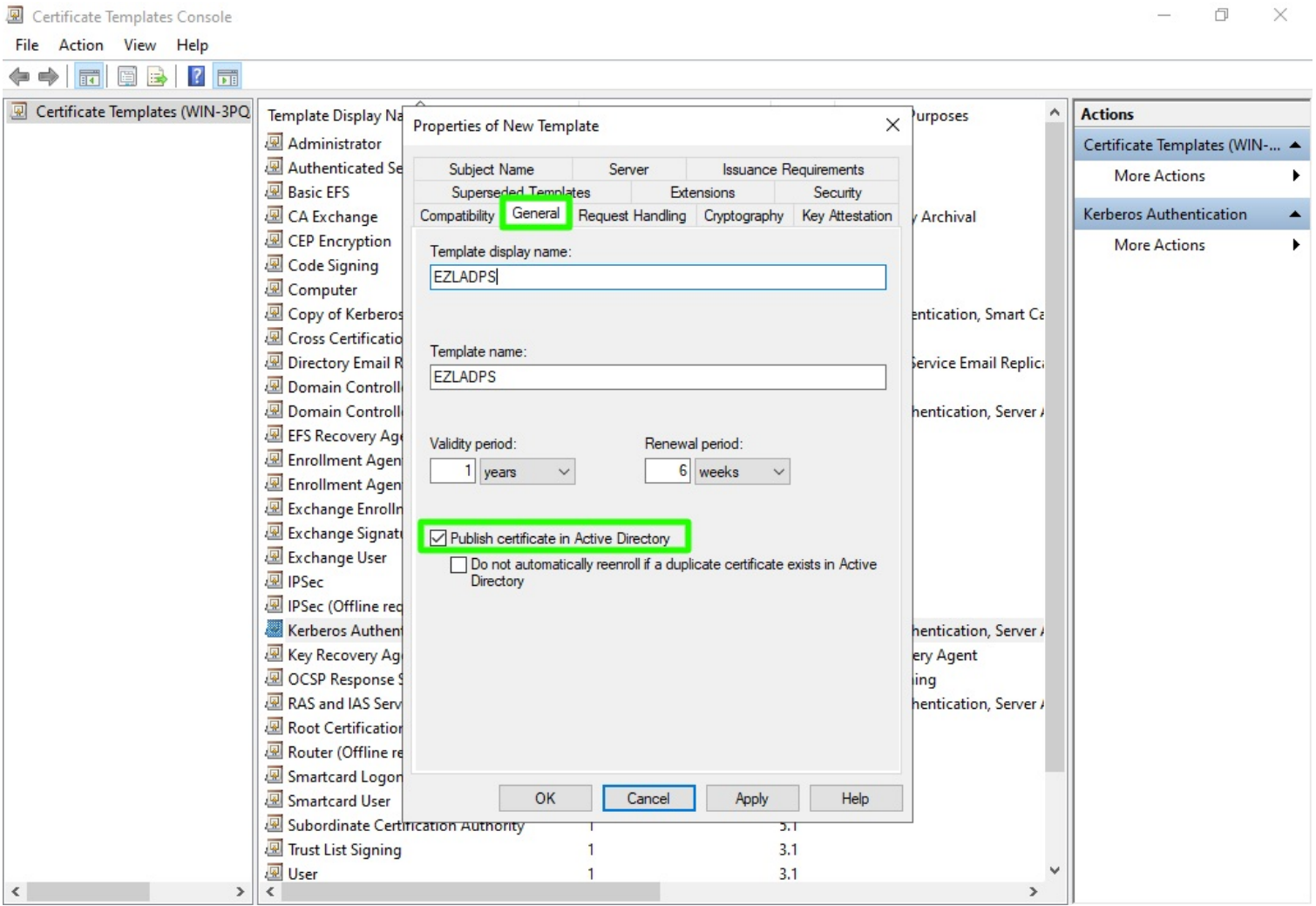


**Step 2(C):** Right-click on Kerberos Authentication and then select "Duplicate Template".

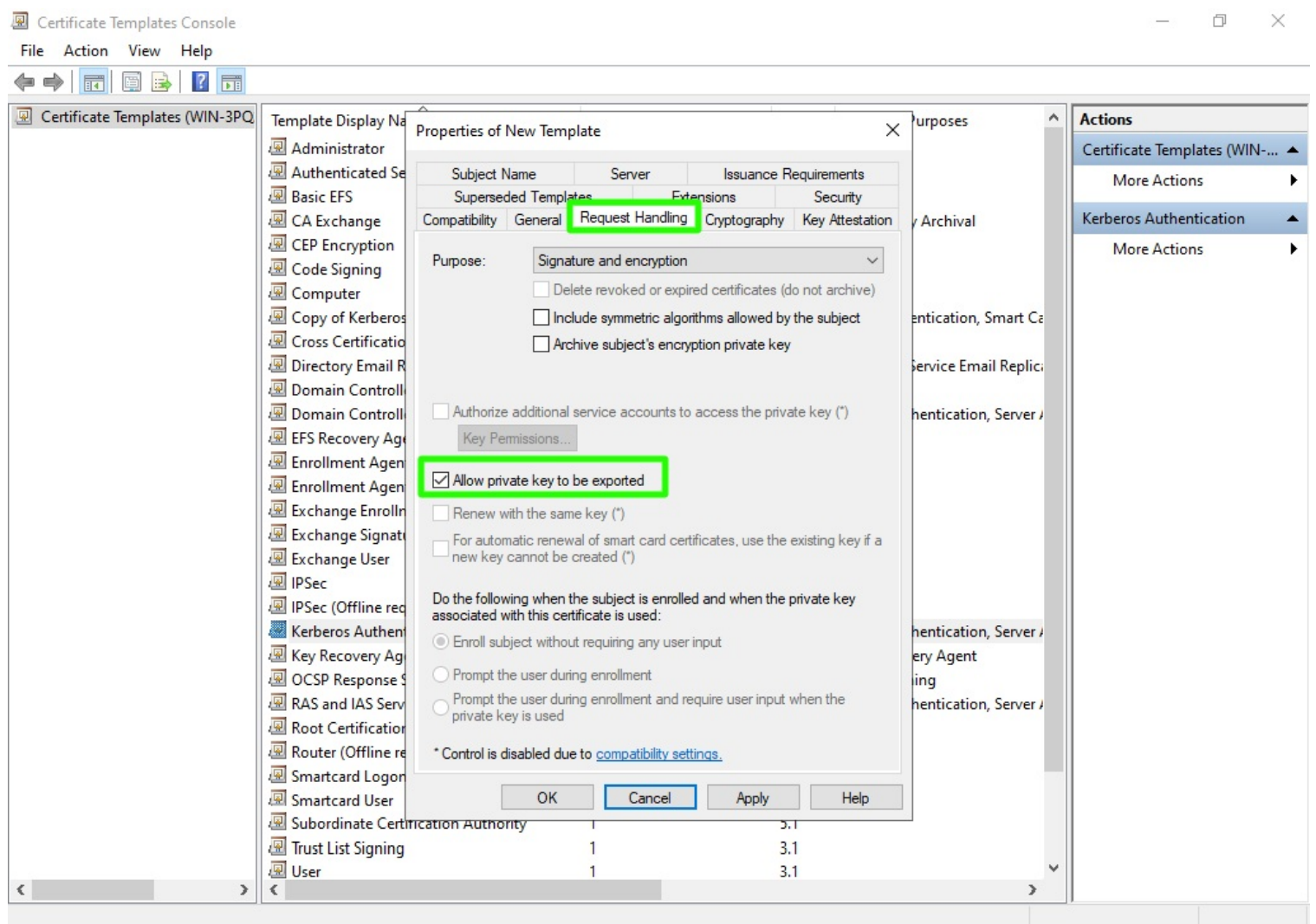




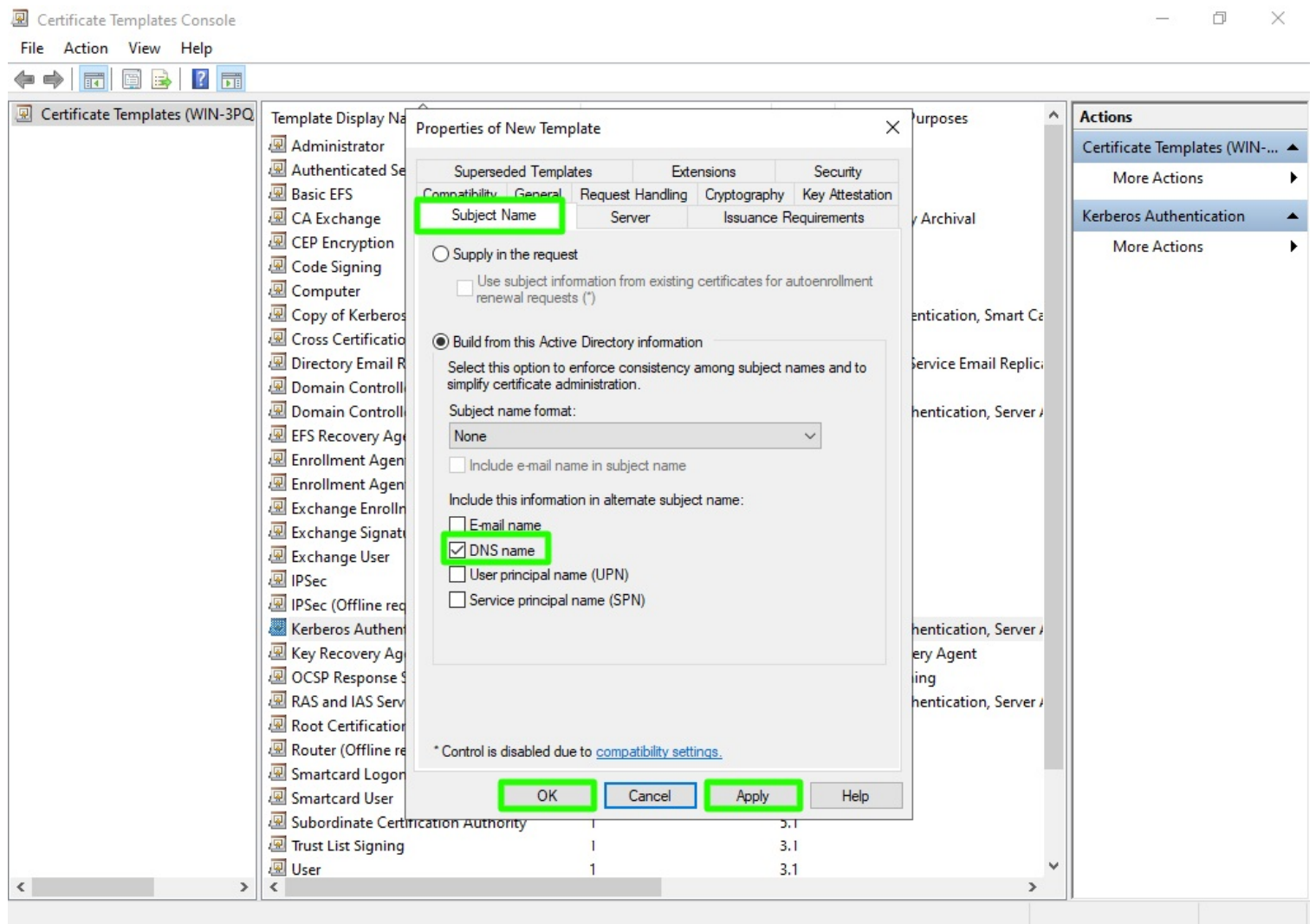
**Step 2(D):** The Properties of new template will appear. Configure the setting according to your requirements. Navigate to the "**General**" tab and enable "**publish certificate**" in Active Directory option.



**Step 2(E):** Go to the "**Request Handling**" tab and enable "**Allow private key to be exported**" option.

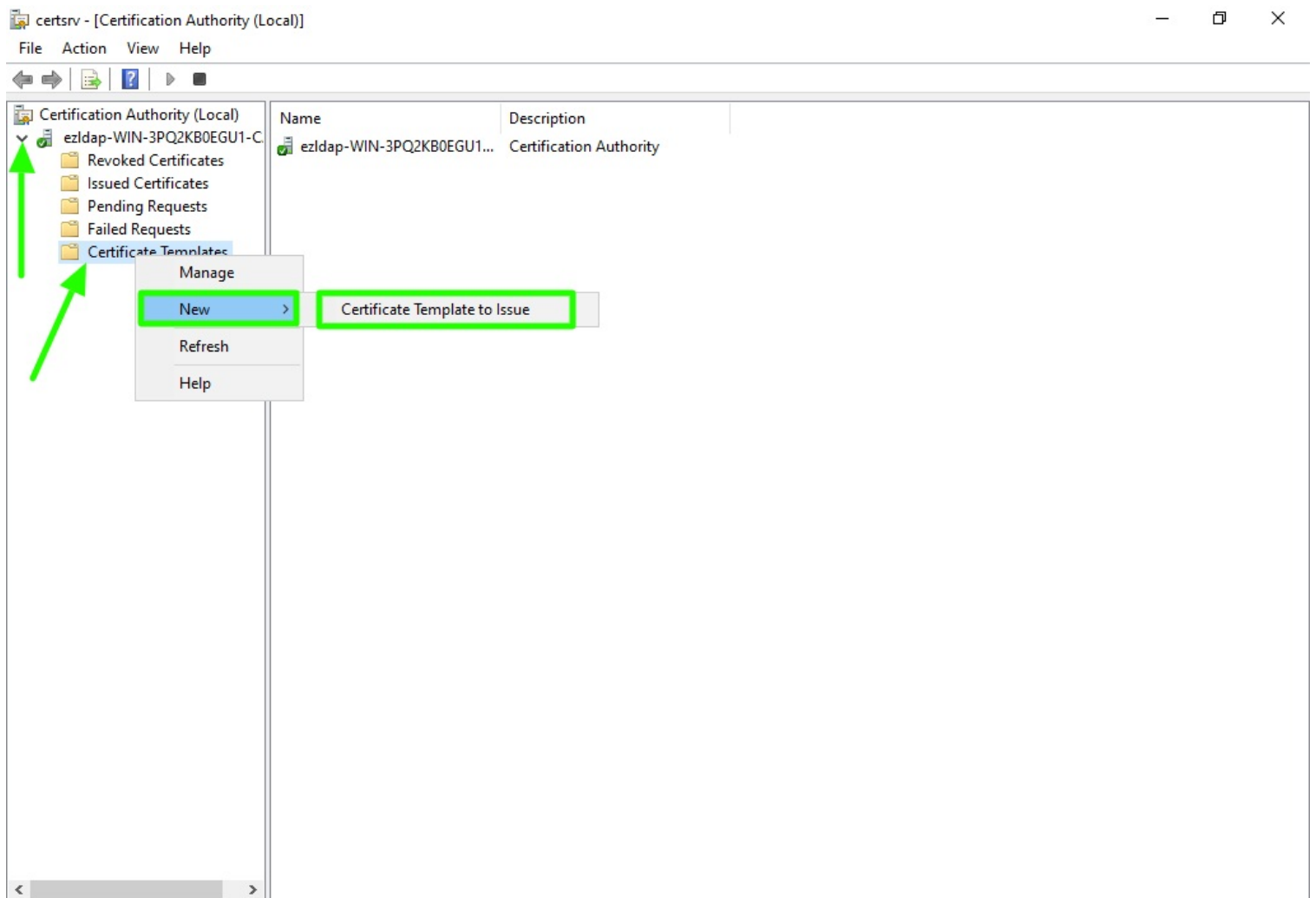


**Step 2(F):** Navigate to the **"Subject Name"** tab and enable subject name format a **"DNS"** Name and click on Apply & OK button.

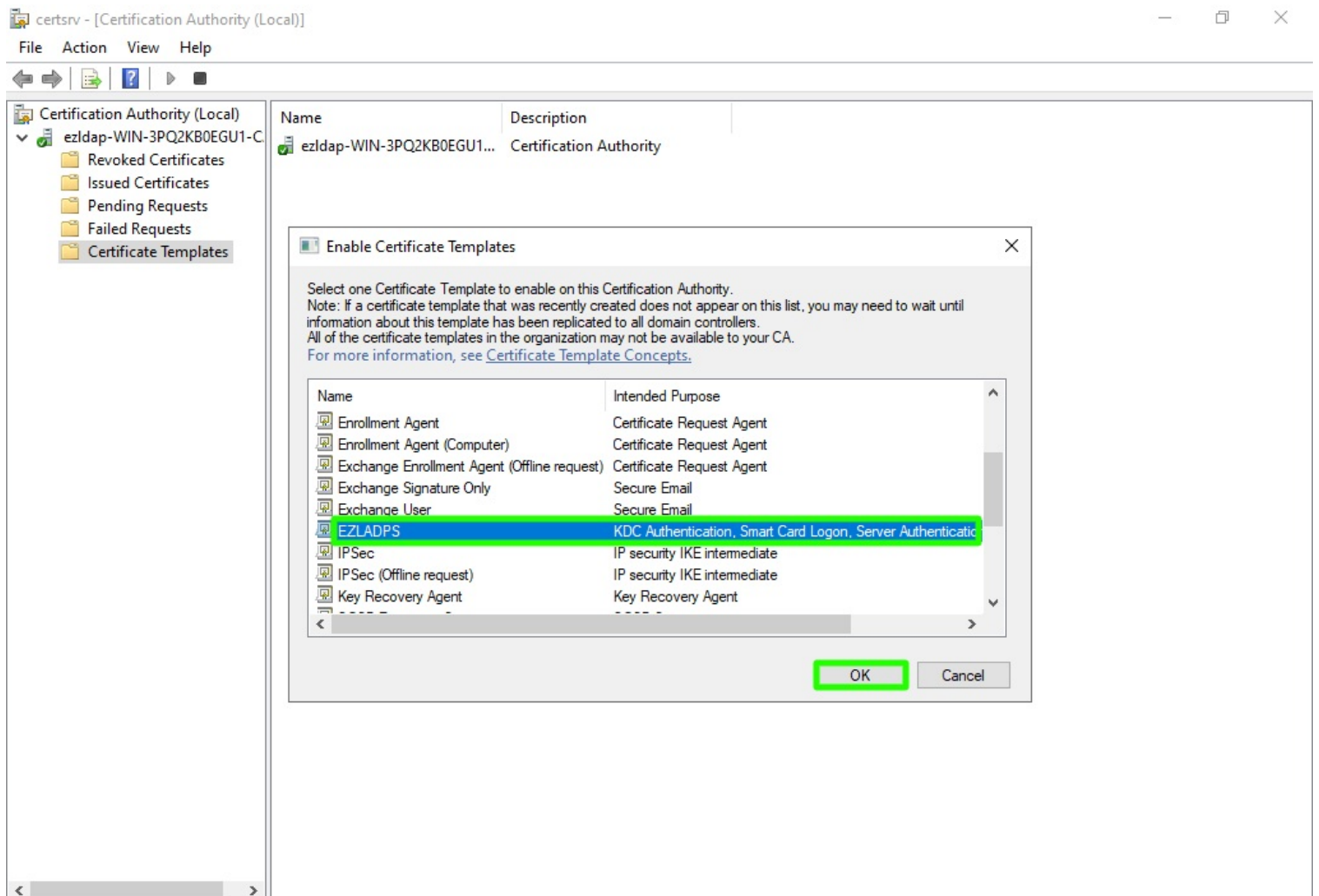


### 3. Issue certificate template

**Step 3(A):** From the start menu, search for and open "**Certification Authority**". In the console, expand your server, right-click on "**Certificate Templates**", then go to "**New**" and select "**Certificate Template to Issue**".

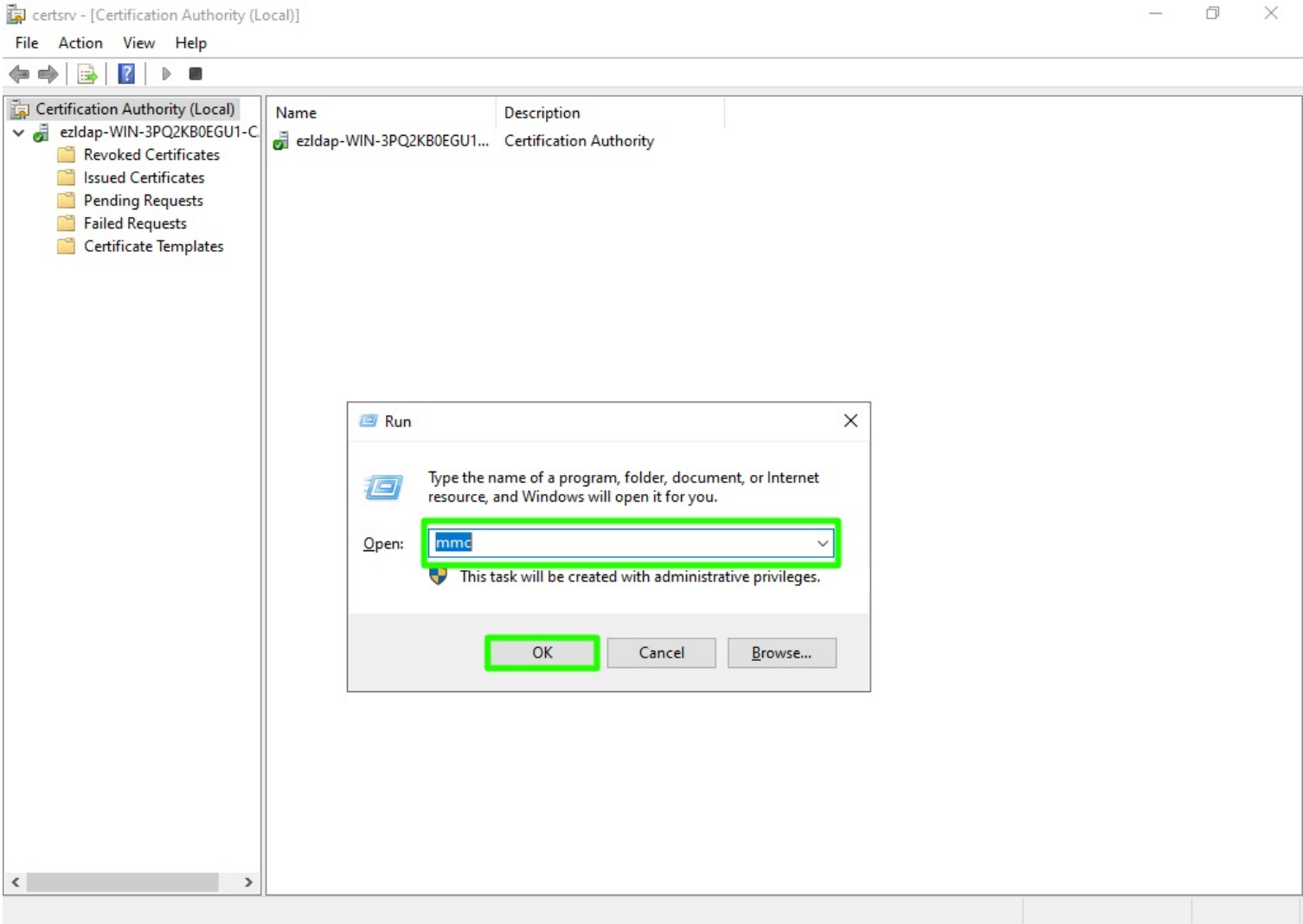


**Step 3(B):** Now, select your **recently** created **Certificate Template** and click on ok button.



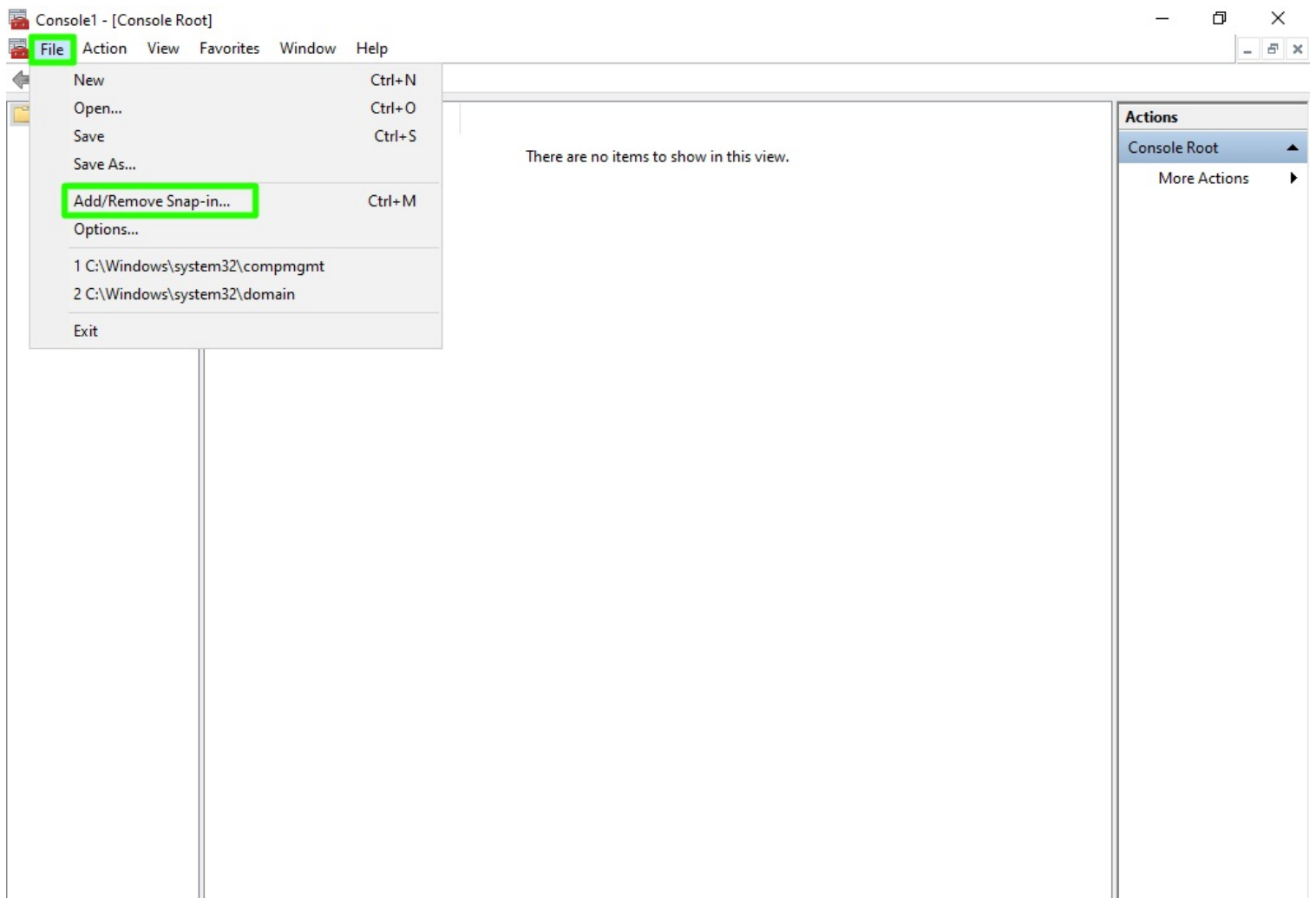
4. Request new certificate for created certificate template

Step 4(A): Navigate to **Windows Key+R** and type "**mmc**" and press enter

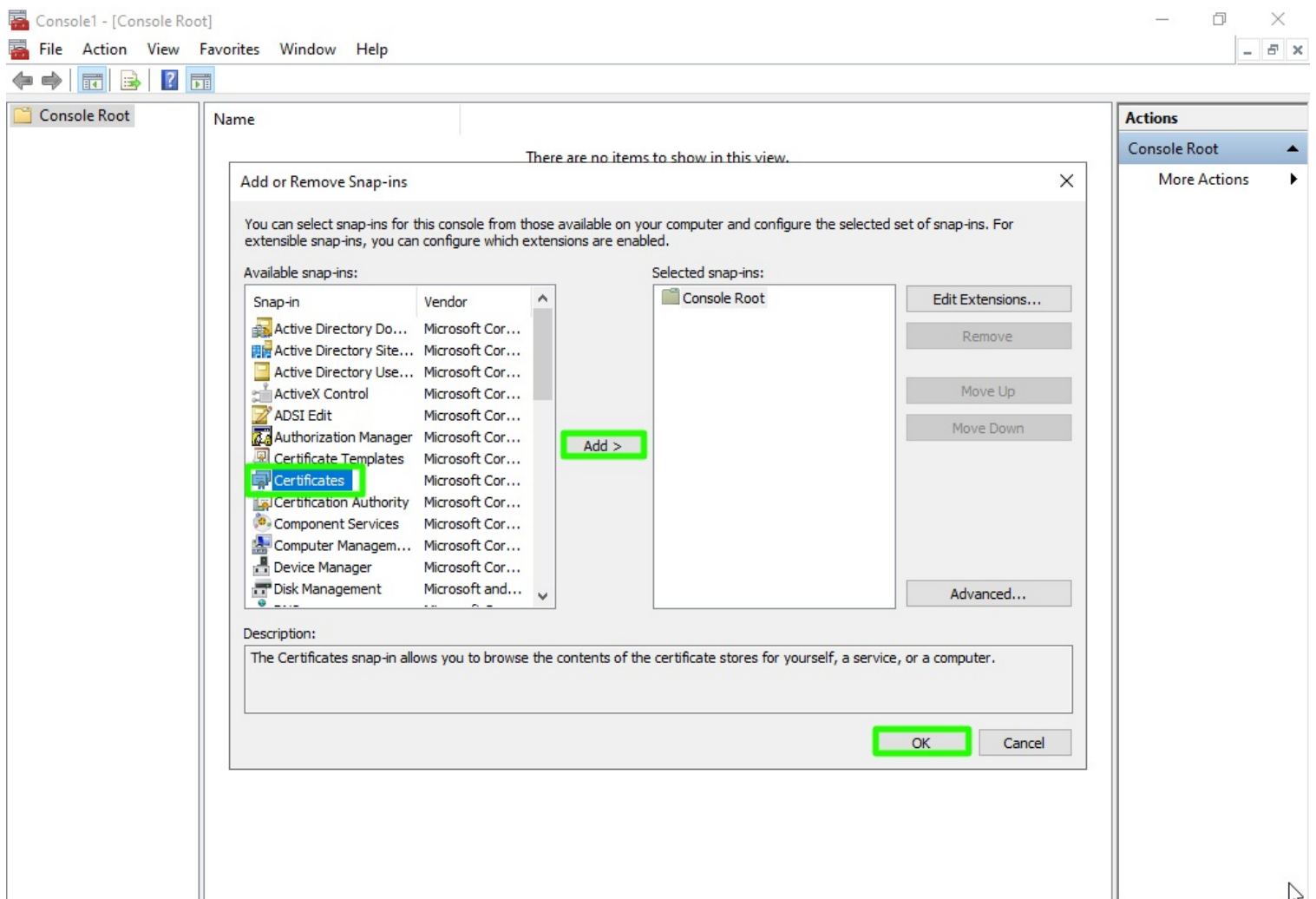


Step 4(B): Navigate to **File** and click on "**Add/Remove snap-in**".

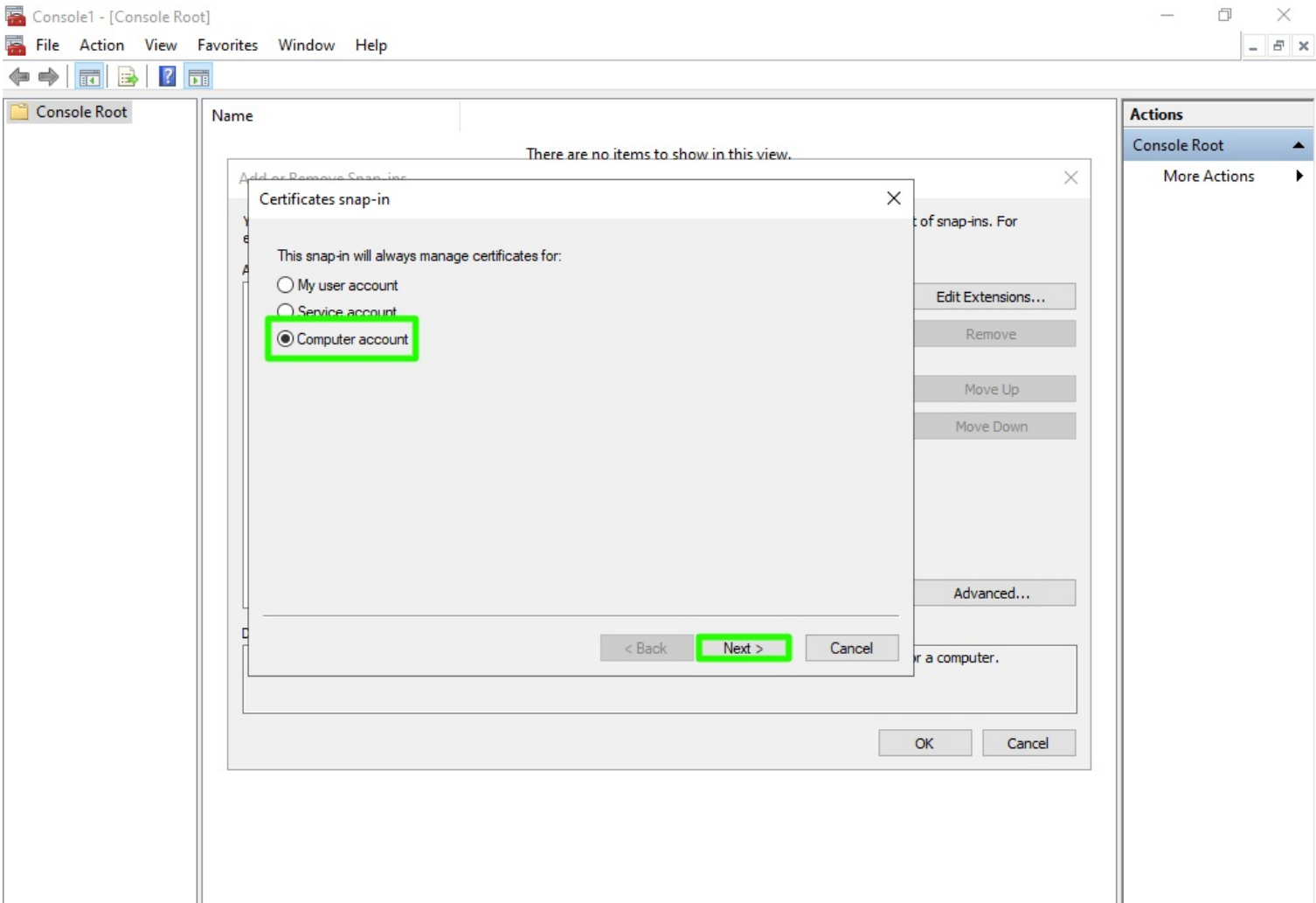




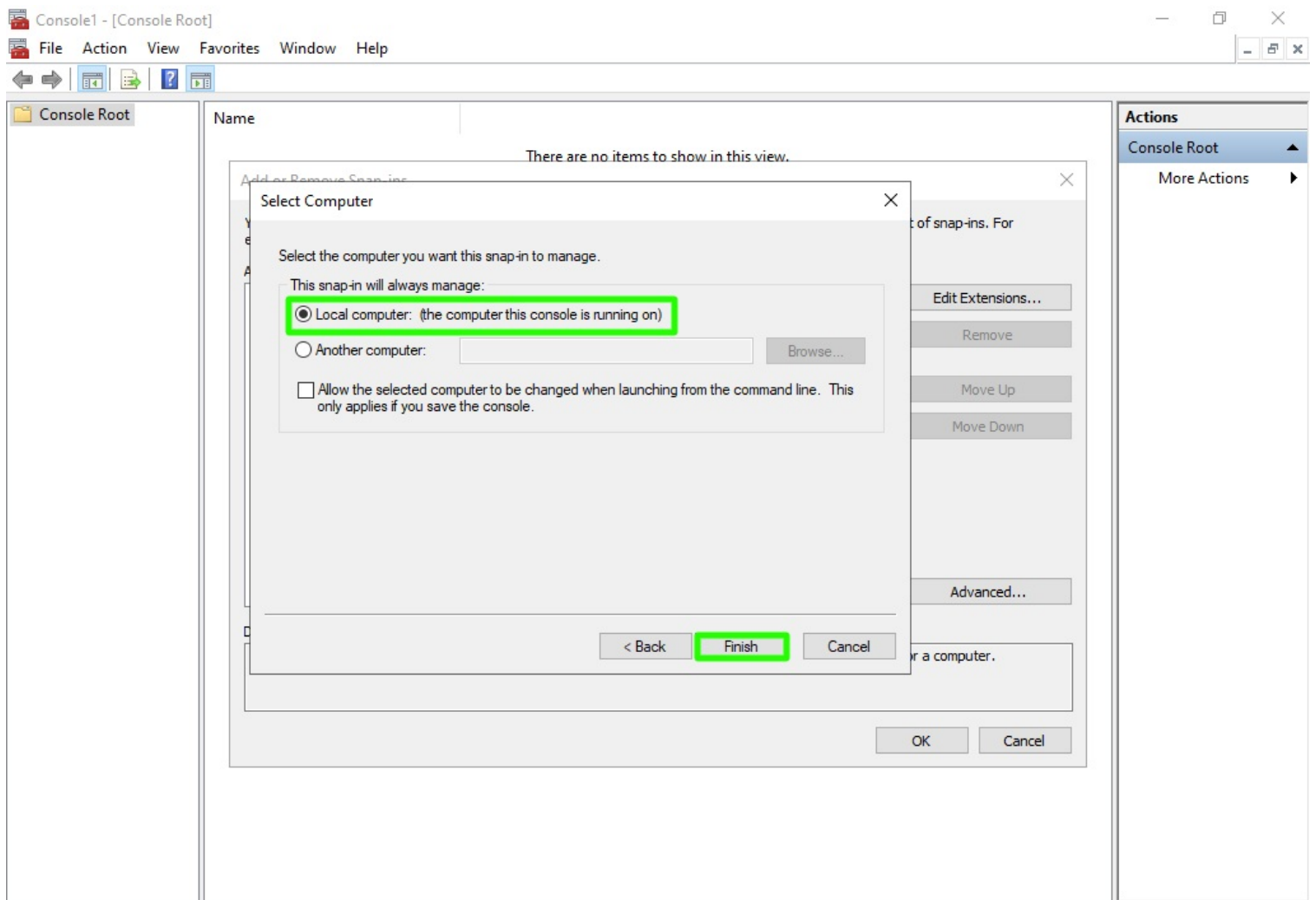
**Step 4(C):** Select "**Certificates**", and click on Add button.



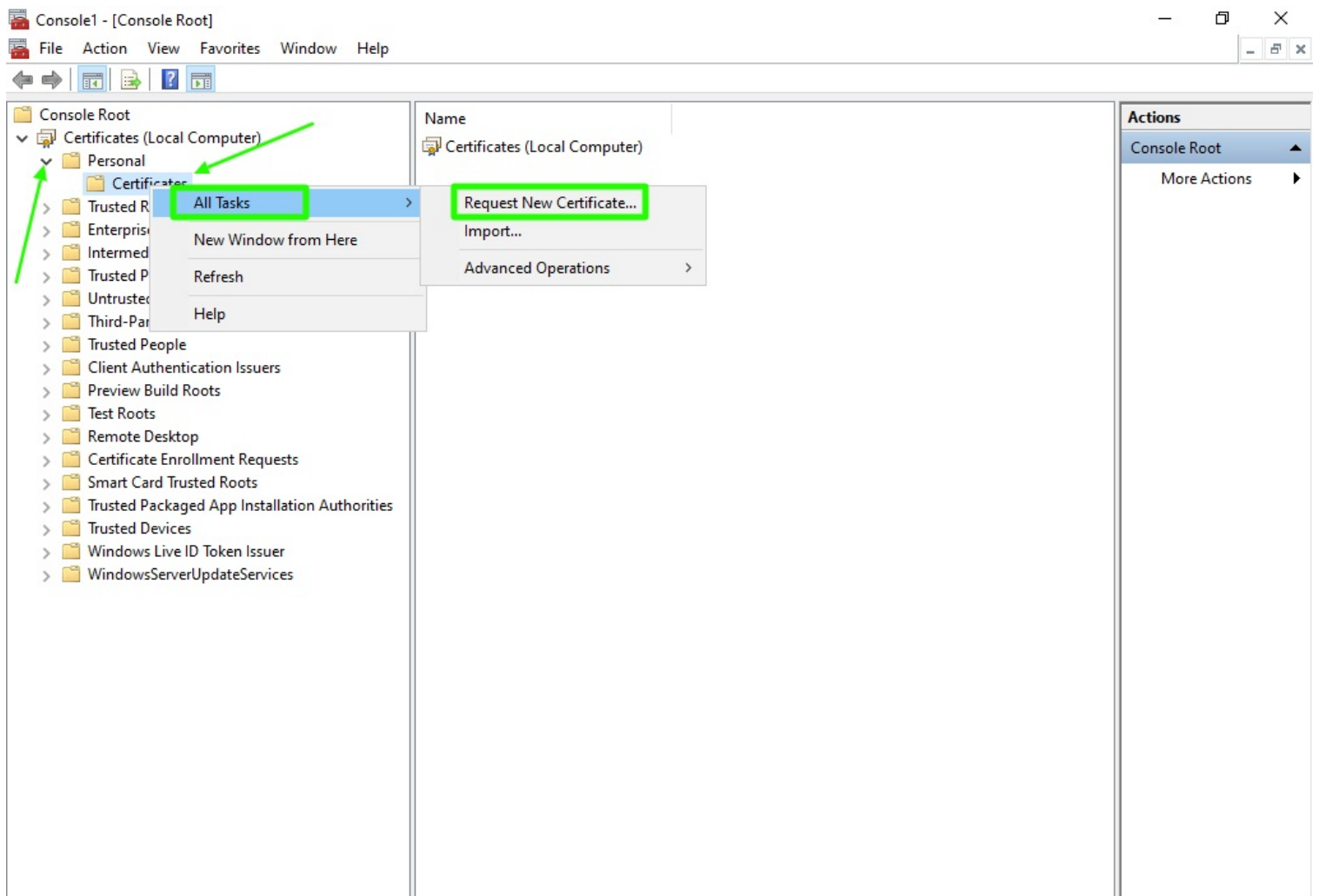
**Step 4(D):** Select "**Computer account**" option and click on Next button.



**Step 4(E):** Select "**Local computer**" option and click on Finish button and then click on OK button.

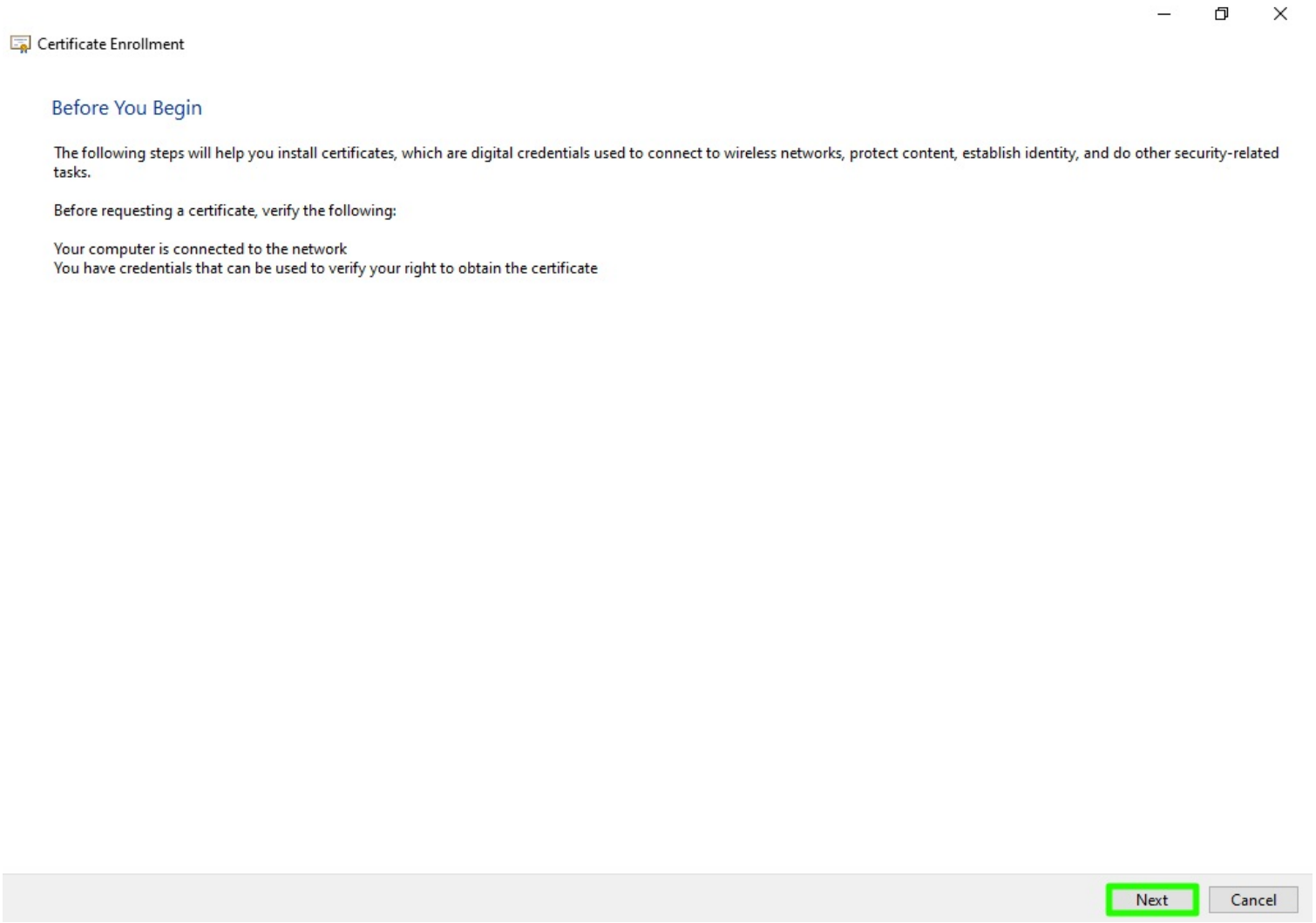


**Step 4(F):** Expand Personal, then **right-click** on **Certificates**, go to "**All Tasks**", and select "**Request New Certificate**".





**Step 4(G):** Click on Next button.



**Step 4(H):** On the next window click on Next button.

## Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

### Configured by your administrator

Active Directory Enrollment Policy



### Configured by you

[Add New](#)

Next

Cancel

**Step 4(I):** Select your certificate and click on "**Enroll**" button.

## Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

| Active Directory Enrollment Policy                        |                                                                                                     |           |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------|-----------|
| <input type="checkbox"/> Directory Email Replication      |  STATUS: Available | Details ▾ |
| <input type="checkbox"/> Domain Controller                |  STATUS: Available | Details ▾ |
| <input type="checkbox"/> Domain Controller Authentication |  STATUS: Available | Details ▾ |
| <input checked="" type="checkbox"/> EZLADPS               |  STATUS: Available | Details ▾ |
| <input type="checkbox"/> Kerberos Authentication          |  STATUS: Available | Details ▾ |

☐ Show all templates

**Enroll**

Cancel

**Step 4(J):** Click on Finish button.

## Certificate Installation Results

The following certificates have been enrolled and installed on this computer.

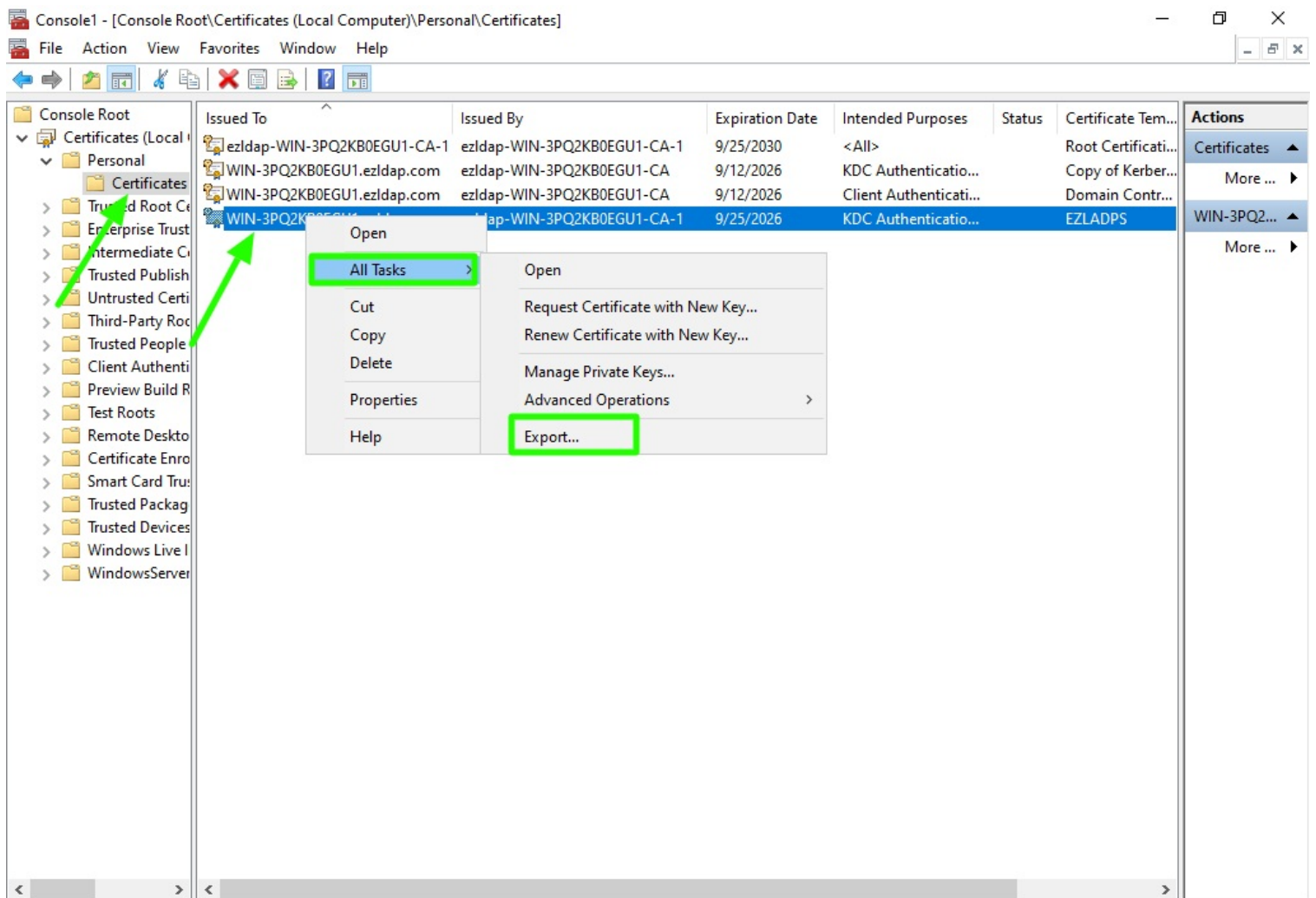
### Active Directory Enrollment Policy

☒ EZLADPS

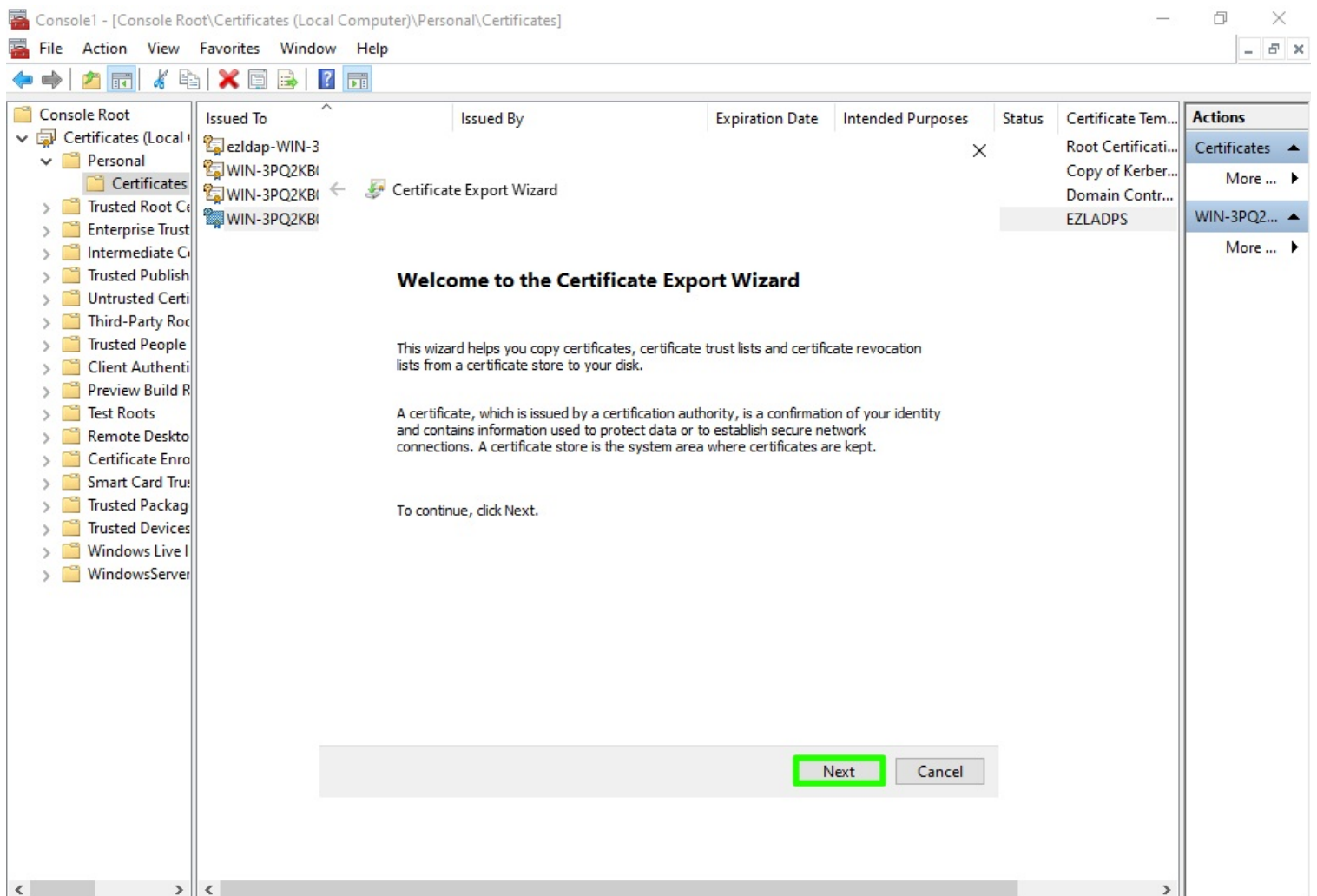
✓ **STATUS:** Succeeded

Details ▾

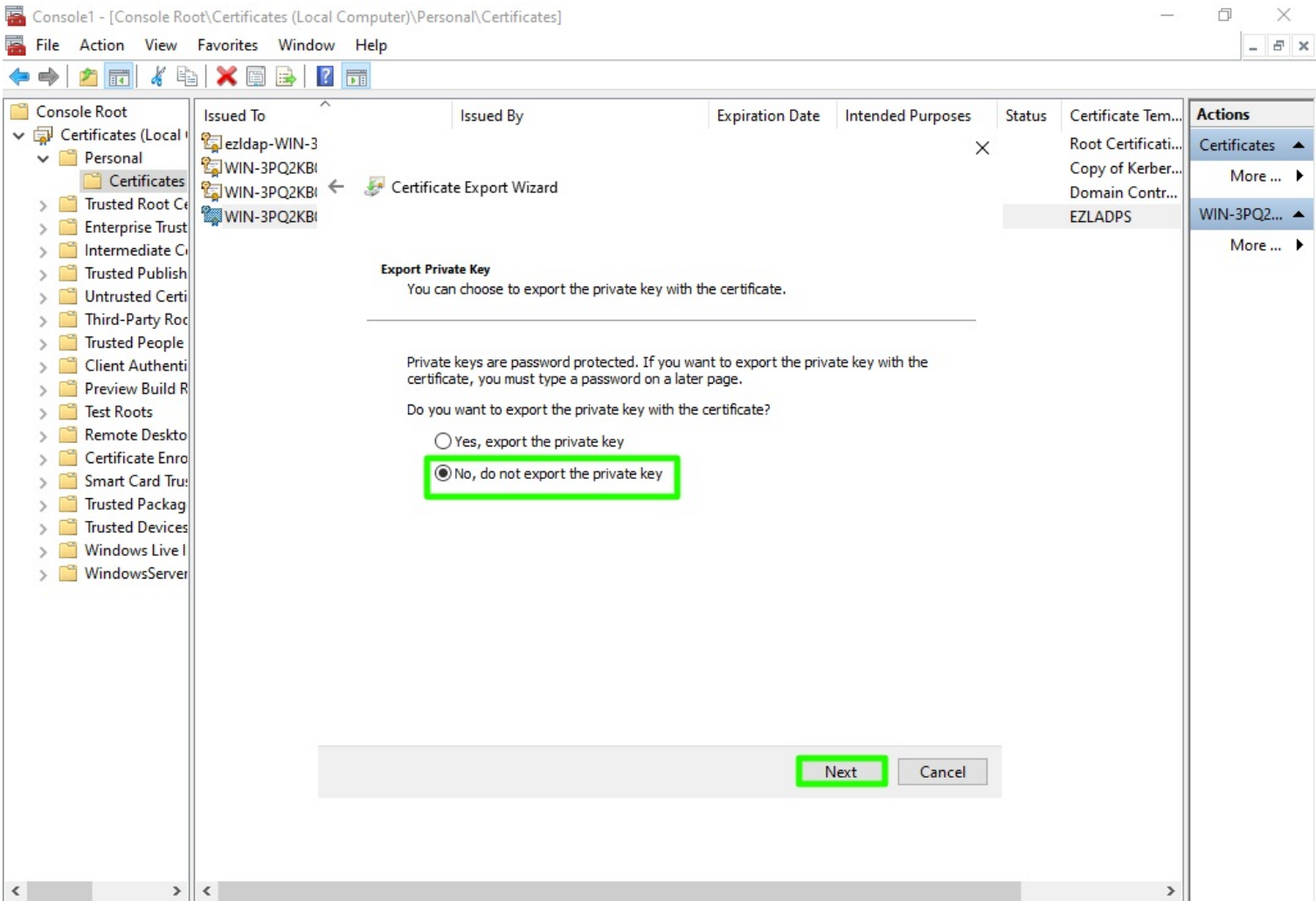
Finish



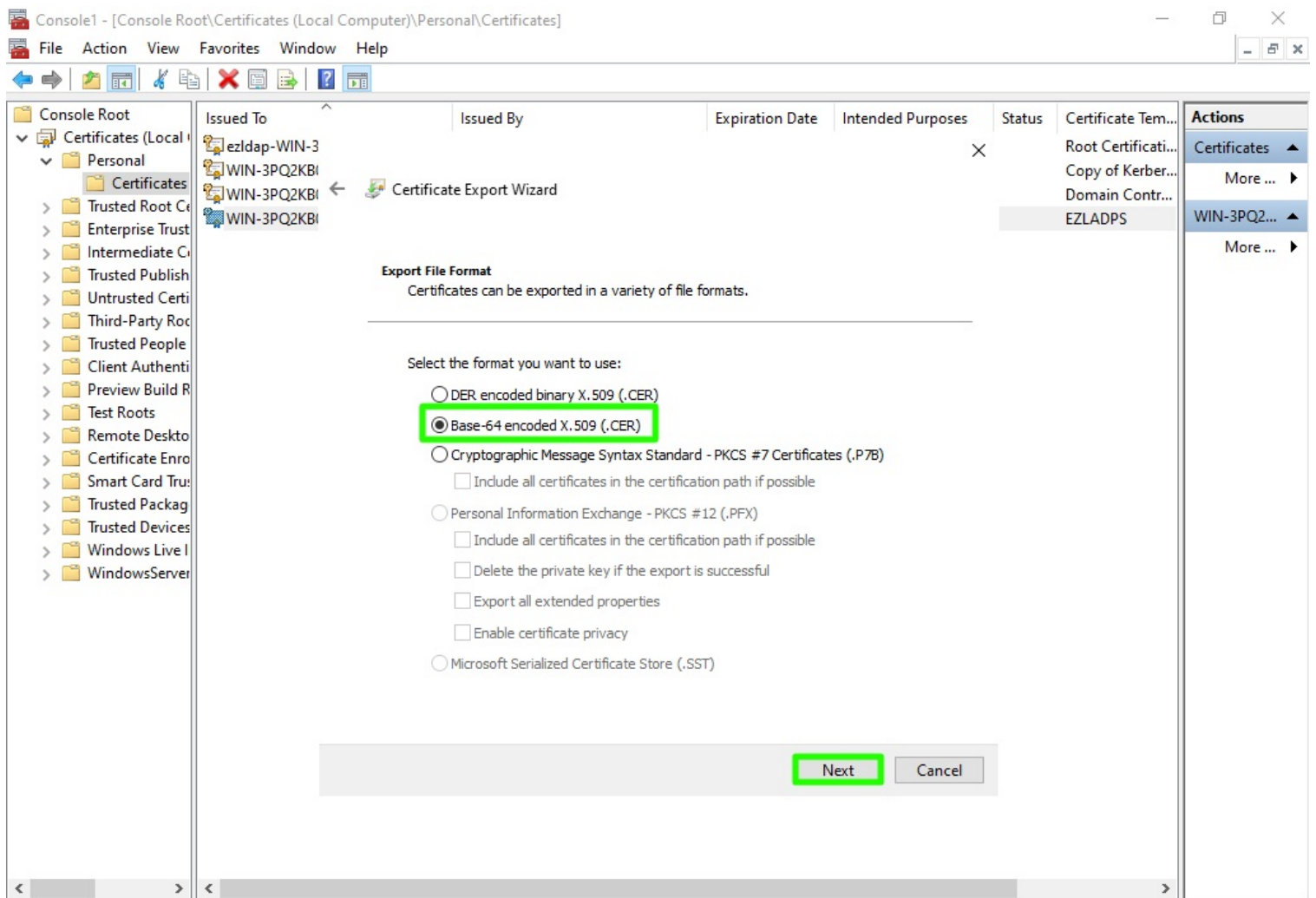
**Step 5(B):** Click on Next button.



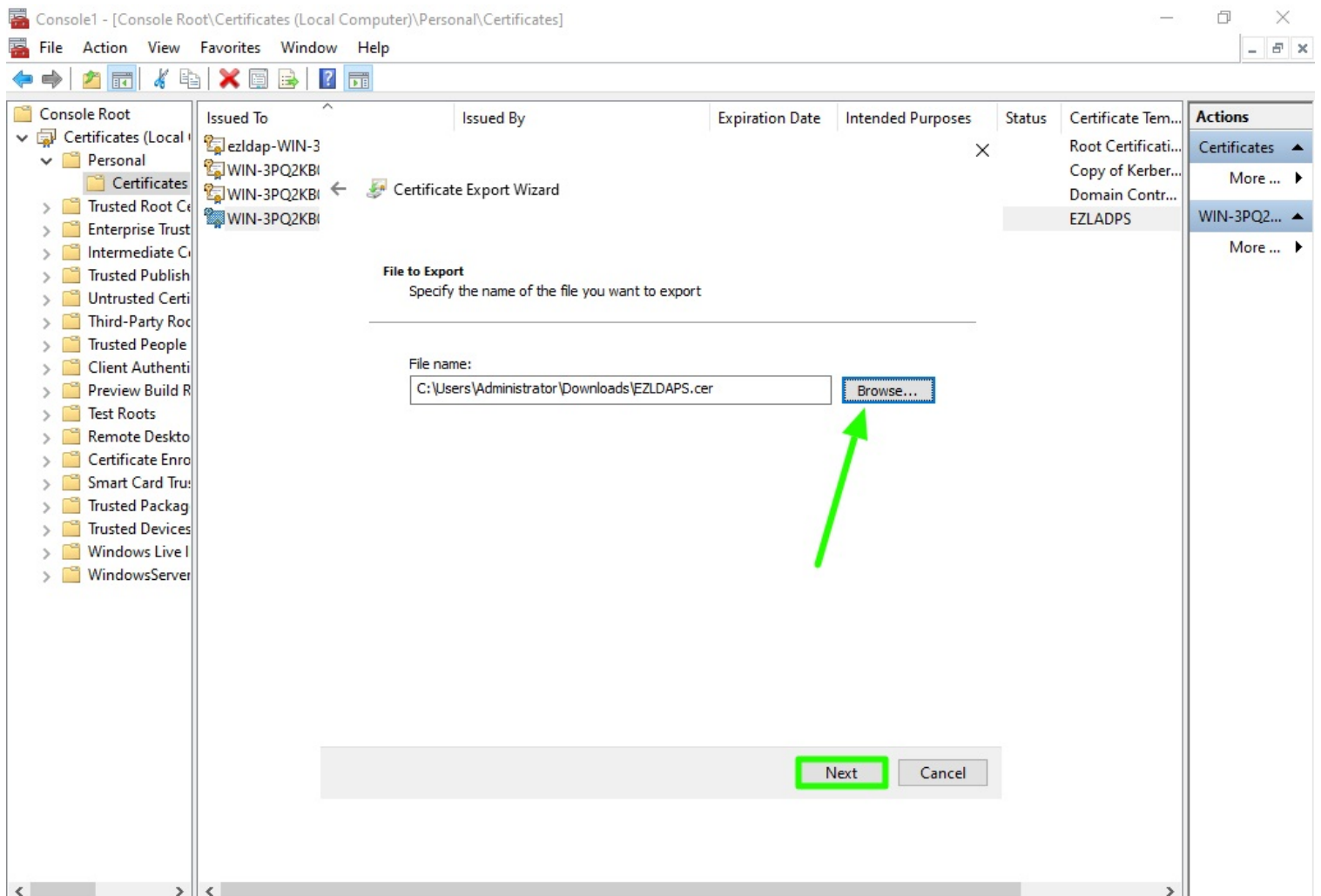
**Step 5(C):** Select **"Do not export the private key"** option and click on Next button.



**Step 5(D):** Choose **"Base-64 encoded X .509"** file format and click on Next.

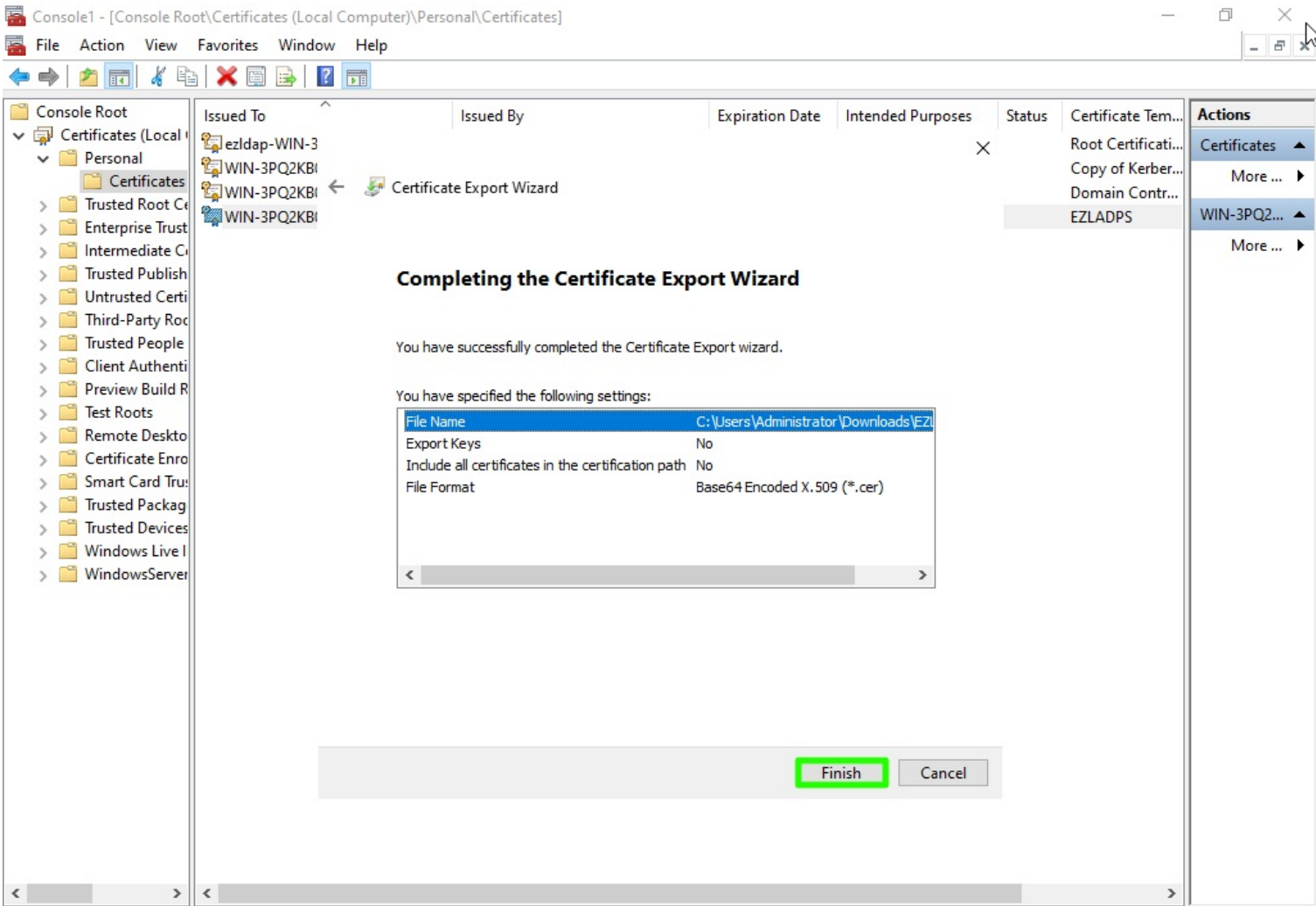


**Step 5(E):** Export the certificate to the desired location and click on Next.

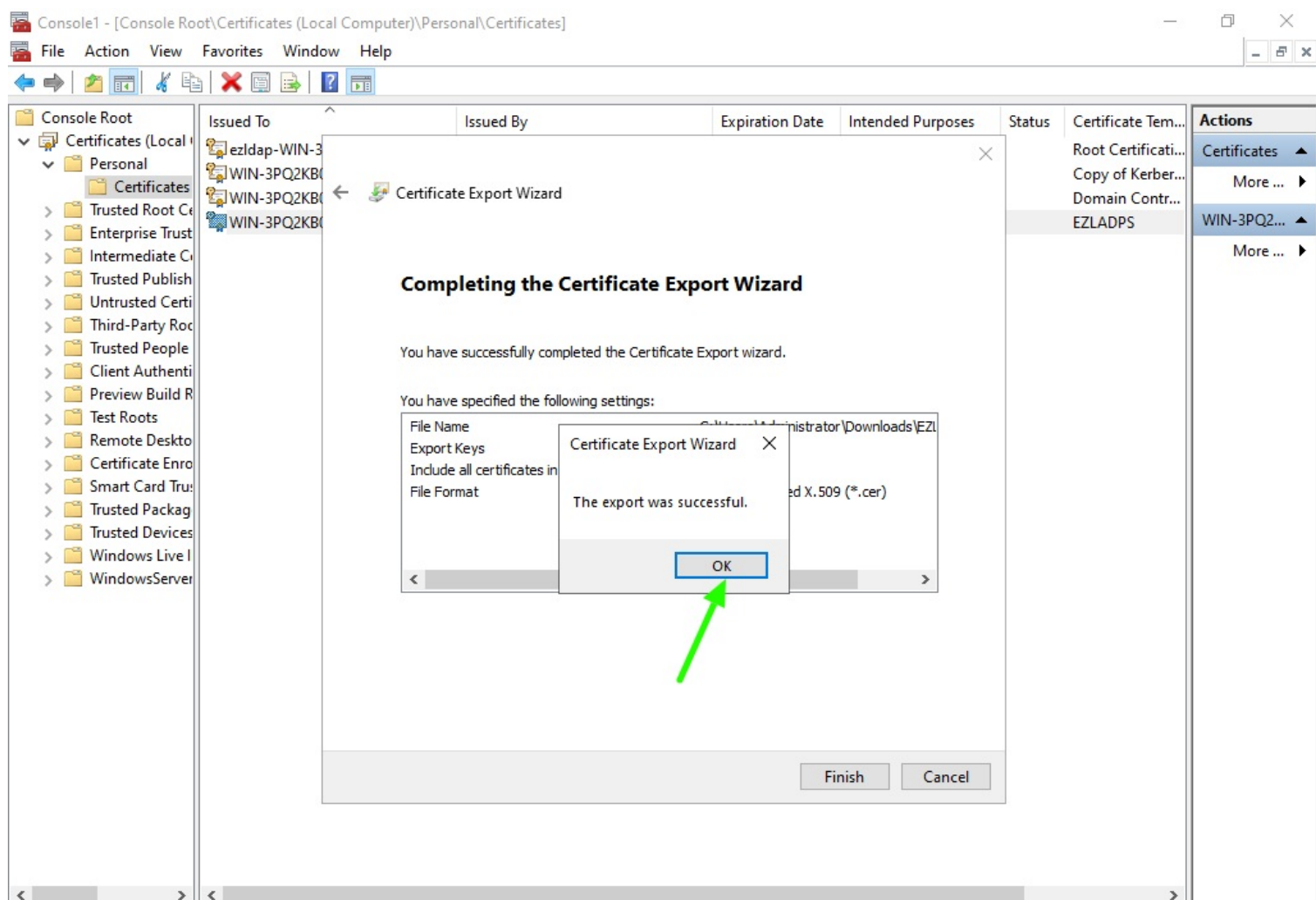




**Step 5(F):** Click on Finish button to complete the certificate export.



**Step 5(G):** On the next pop up window click on OK button.



## 6. Configure LDAPS on the gateway server

**Step 6(A):** Run the following command to install OpenSSL on the gateway server:

```
root@gateway:~# apt-get install openssl      #Ubuntu
root@gateway:~# yum install openssl          #RHEL/CentOS
```

**Step 6(B):** Copy the generated certificate in **step 5(E)** to the gateway server. Then, run the following command to convert it to a **.pem** format:

```
root@gateway:~# openssl x509 -in cert_name.cer -out cert_name.pem
```

**For example:**

```
root@gateway:~# openssl x509 -in EZLDAPS.cer -out EZLDAP.pem
```

**Step 6(C):** Move the converted **.pem** file to a secure location, such as **/etc/openssl/**

**Step 6(D):** Edit the ldap.conf file and add the following line to specify the path to your certificate:

```
root@gateway:~# vim /etc/ldap/ldap.conf
TLS_CACERT /etc/openssl/EZLDAPS.pem
```

**Step 6(E):** To test the LDAPS connection with a valid certificate, run the following command by replacing the values with the appropriate LDAP server details:

```
root@gateway:~# ldapsearch -H ldaps://<server-ip/domain.com>:636 -x -D "<bind-dn>" -W -b "<base-dn>"
```

**For Example:**

```
root@gateway:~# ldapsearch -H ldaps://192.168.56.108:636 -x -D  
"cn=Administrator,cn=Users,dc=ezeelogin,dc=com" -W -b "dc=ezeelogin,dc=com"
```

**Step 6(F):** Run ldapsearch from the terminal with "**LDAPTLS\_REQCERT=never**" if using a self-signed certificate.

```
root@gateway:~# LDAPTLS_REQCERT=never ldapsearch -H ldaps://<server-ip/domain.com>:636 -x -D "<bind-dn>" -W -b "<base-dn>"
```

**For Example:**

```
root@gateway:~# LDAPTLS_REQCERT=never ldapsearch -H ldaps://192.168.56.108:636 -x -D  
"cn=Administrator,cn=Users,dc=ezeelogin,dc=com" -W -b "dc=ezeelogin,dc=com"
```

**Step 6(G):** Run the following command to test the LDAP with StartTLS (on port 389). Use "**LDAPTLS\_REQCERT=never**" if the certificate is self-signed.

```
root@gateway:~# ldapsearch -H ldap://<server-ip/domain.com>:389 -ZZ -x -D "<bind-dn>" -W -b "<base-dn>"
```

**For Example:**

```
root@gateway:~# ldapsearch -H ldap://192.168.56.108:389 -ZZ -x -D  
"cn=Administrator,cn=Users,dc=ezeelogin,dc=com" -W -b "dc=ezeelogin,dc=com"
```

**Conclusion :**

Following these steps enables the configuration of Active Directory to use LDAP over SSL (LDAPS), establishing a secure, encrypted connection between the server and the gateway.

**Related Articles:**

[How to install and setup active directory?](#)

[Integrate OpenLDAP / Windows Active Directory authentication in Ezeelogin jump server](#)

Online URL: <https://www.ezeelogin.com/kb/article/setup-ldaps-on-windows-server-793.html>