

Contents

1	Introduction	1
2	Prerequisites	1
3	Installing/Configuring Active Directory Certificate Services	4
3.1	Confirming the CA works	6

1 Introduction

This explains how to

2 Prerequisites

1. You should have joined the CA to the Domain.
2. You should be logged in as a **domain** administrator in the Cert Publishers group

To add the Cert Publishers permission, RDP into one of the Domain Controllers. Then add a user (probably the administrator) to the Cert Publishers group.

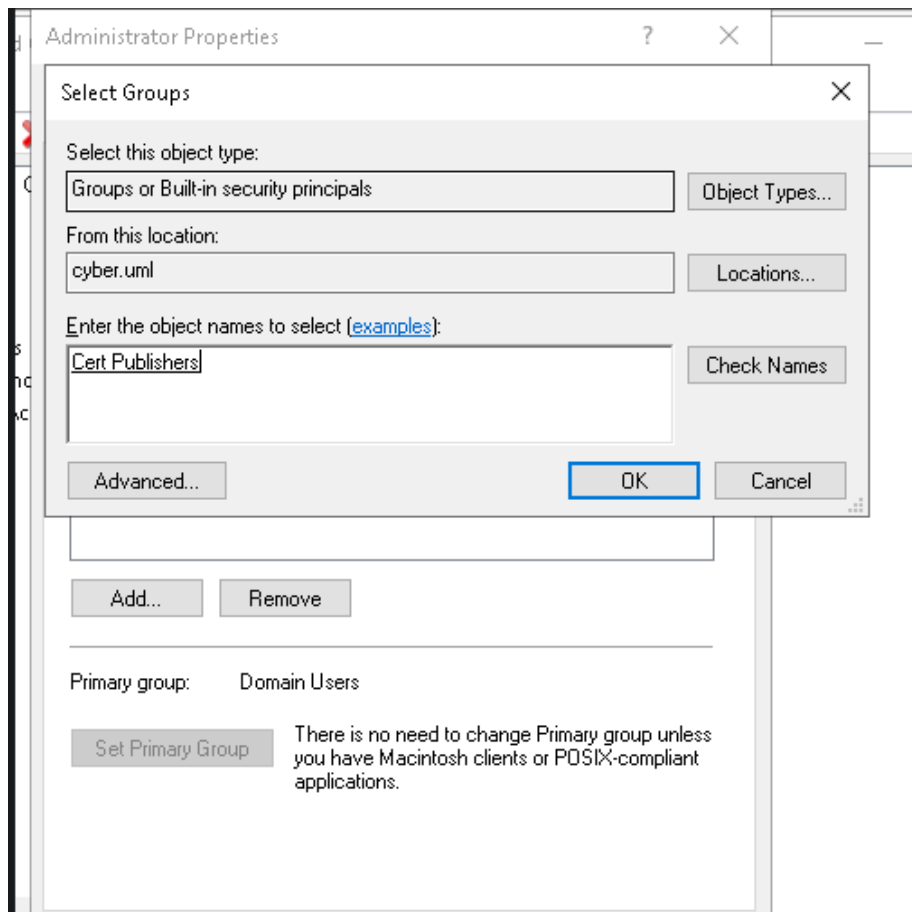


Figure 1: Adding administrator to the Cert Publishers group

To install an Enterprise CA, you must be logged in as a member of both the Enterprise Admins group and the root domain's Domain Admins group. These groups have the necessary permissions to install and configure AD CS on a domain-joined computer. You do not need to give the computer itself any additional permissions in Active Directory.

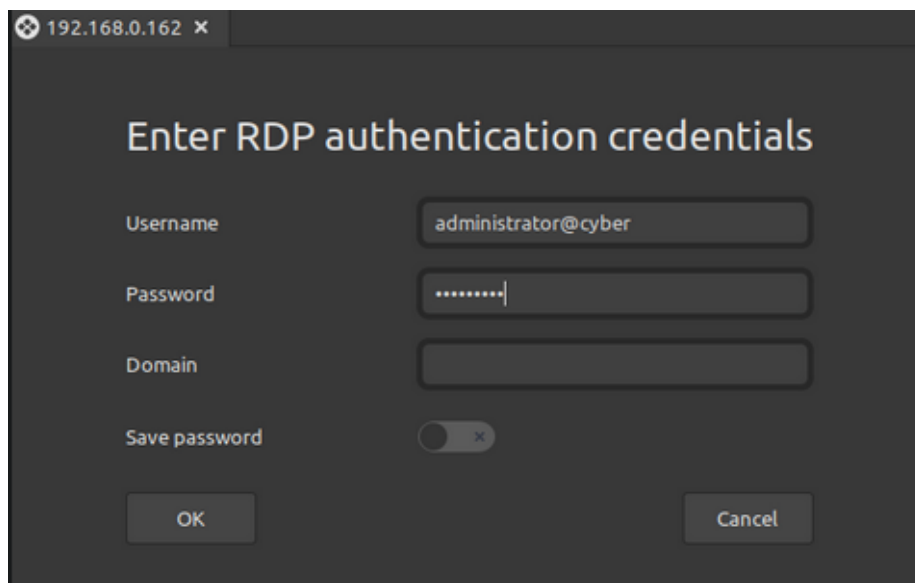
Figure 2: Bing on Permissions

After adding the permission, you will need to log in and out of the CA for it to take effect. Note that the domain administrator is possibly logged into differently than the local administrator.

Make sure to login with the administrator account, as seen in 4

If you have a domain user with the same name as your local user, you can log in with the domain user by specifying the domain name before the username. For example, if your domain is `mydomain.com` and your username is `myuser`, you can log in with the domain user by entering `mydomain\myuser` or `myuser@mydomain.com` as the username.

Figure 3: How to avoid possible naming conflicts



192.168.0.162 x

Enter RDP authentication credentials

Username: administrator@cyber

Password:

Domain:

Save password: ☐

OK Cancel

Figure 4: Example login, explicitly with the Domain Administrator (note the @cyber to show it the domain admin, not the local admin)

Your domain admin account should now have the necessary permissions to configure the CA.

3 Installing/Configuring Active Directory Certificate Services

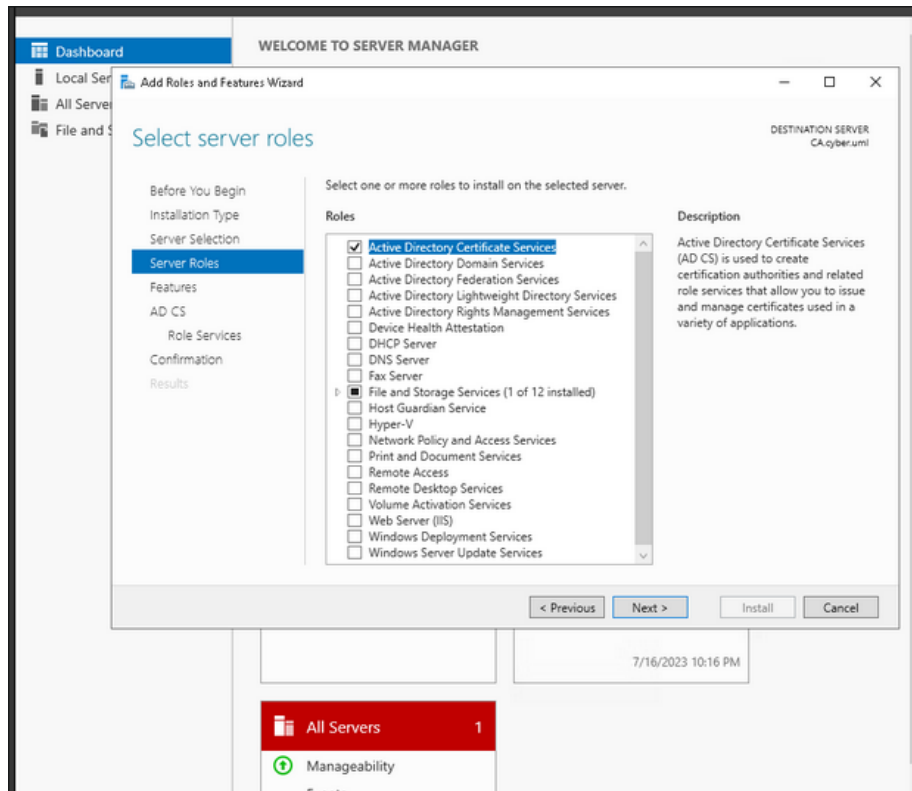


Figure 5: Clicking the ADCS button

Install Active Directory Certificate Services.

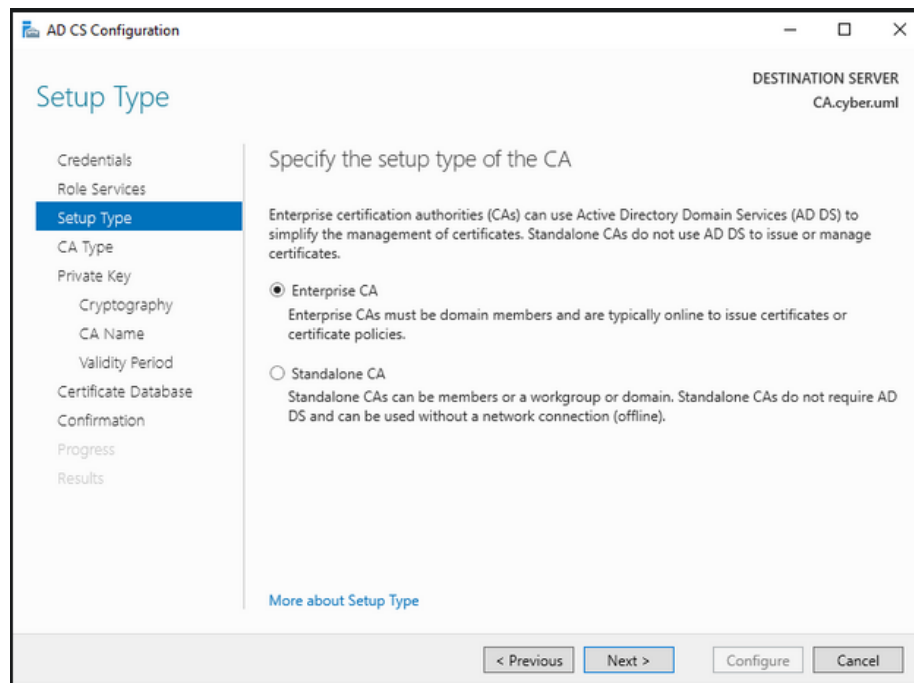


Figure 6: The only important button is the Enterprise CA button. Click it!

Make sure to select Enterprise CA.

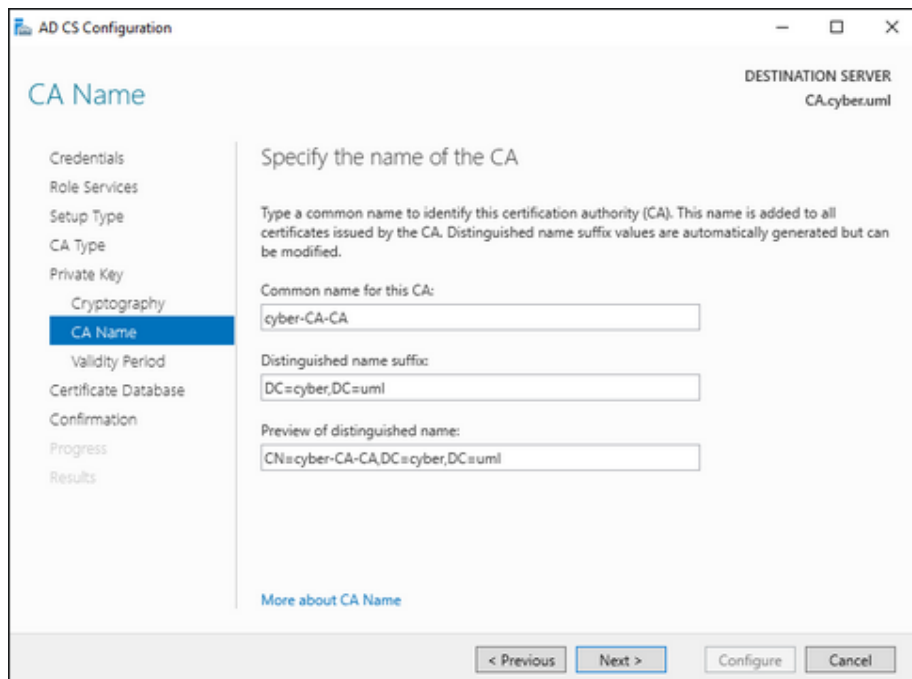


Figure 7: Selecting the CA name

As long as it is unique it should be fine, to be safe we can probably stick with the hostname of the CA machine.

3.1 Confirming the CA works

To check the CA we need to make a certificate signing request. Unless you have someone who needs a cert, you can make a request by putting this in a text file called "example.inf"

```
[Version]
Signature="$Windows NT$"

[NewRequest]
Subject = "CN=example.com"
KeySpec = 1
KeyLength = 2048
Exportable = TRUE
MachineKeySet = TRUE
SMIME = False
PrivateKeyArchive = FALSE
UserProtected = FALSE
```

```
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0

[RequestAttributes]
CertificateTemplate = WebServer

[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1 ; Server Authentication
```

```
PS C:\Users\Administrator.CYBER\Desktop> certreq -new example.inf example.csr
>>

CertReq: Request Created
PS C:\Users\Administrator.CYBER\Desktop> █
```

Figure 8: Making a test certificate request

Open a PowerShell prompt, navigate to the directory where you saved the example.inf file, and run the following command

```
certreq -new example.inf example.csr
```

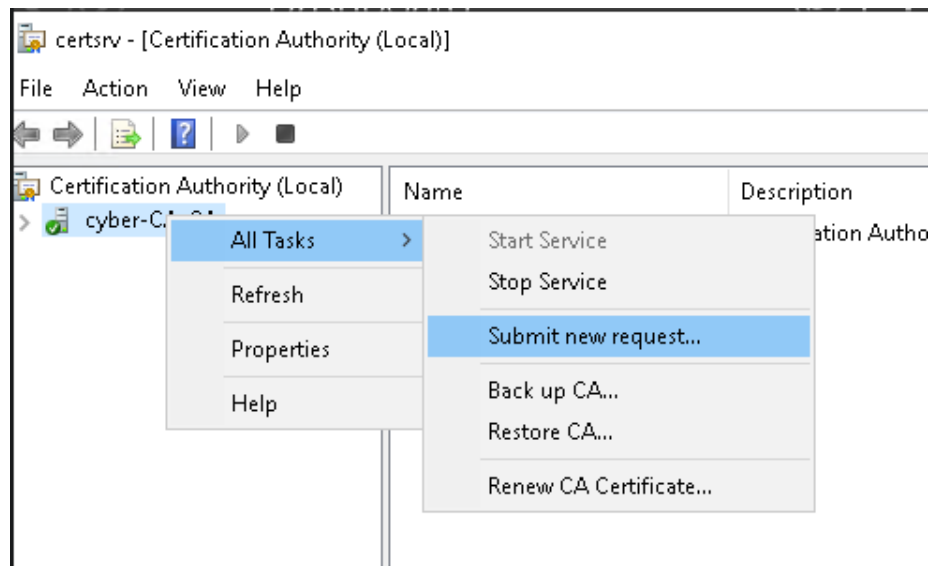


Figure 9: Submitting the request to the CA

Open up certsrv, either by searching for "Certificate Authority" on the machine, or by doing meta + r to run certsrv.msc. Right click on the CA's name (as in the screenshot), hover over "All Tasks", and click "Submit New Request." This prompts you to select the .csr file to submit.

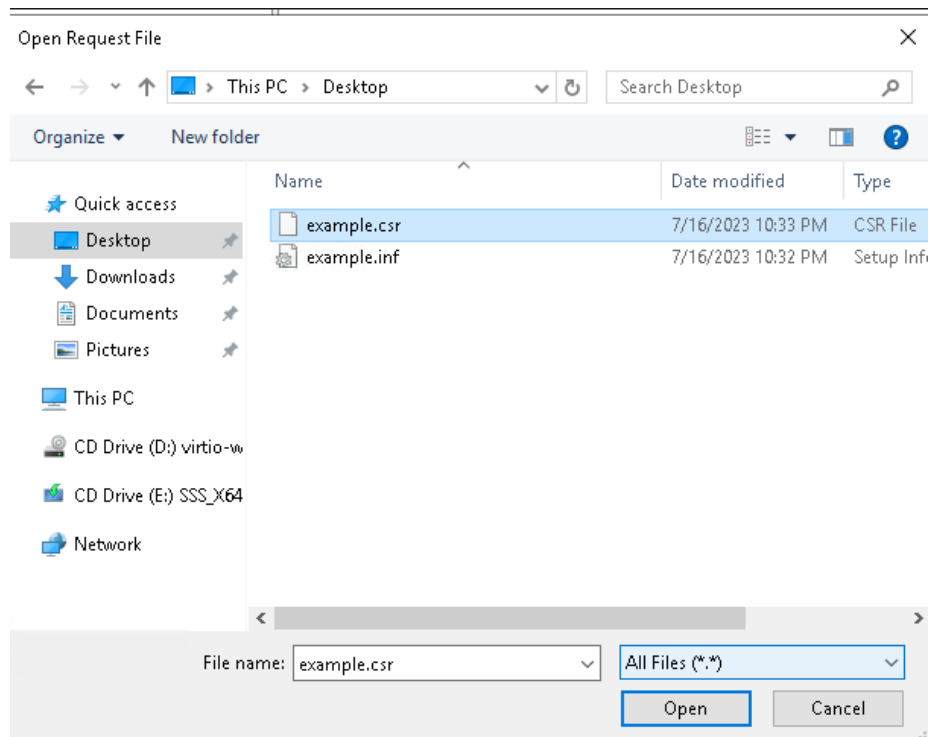


Figure 10: Select the .csr file. To find it, make sure to select "Show All Files" (on the bottom right)

To approve the request, expand the menu. Then click "Pending Requests." Then approve the request.