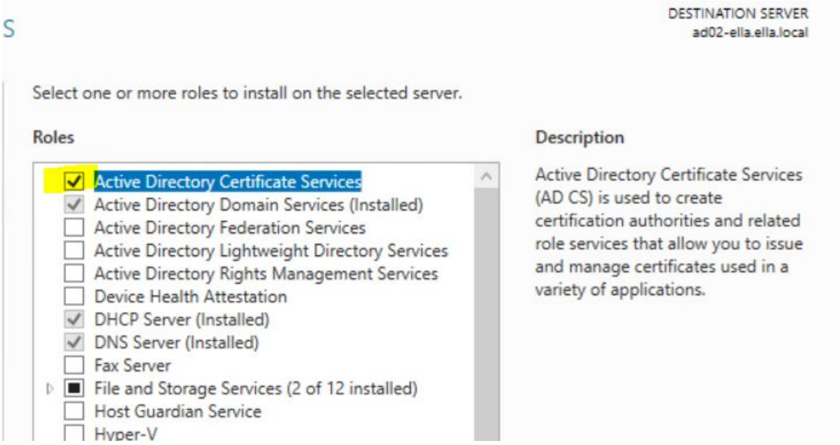
Windows Server Active Directory Certificate Services Installation and Implementation

Build Documentation

💡 This requires that you already have Windows Server 2016 setup with AD DS and a basic apache web server running on the same network.

Installing AD CS on AD02

Go to the server manager dashboard and click on install roles and features, and select your AD machine, then under roles click on Active Directory Certificate Services.



S

DESTINATION SERVER
ad02-ella.ella.local

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

Roles

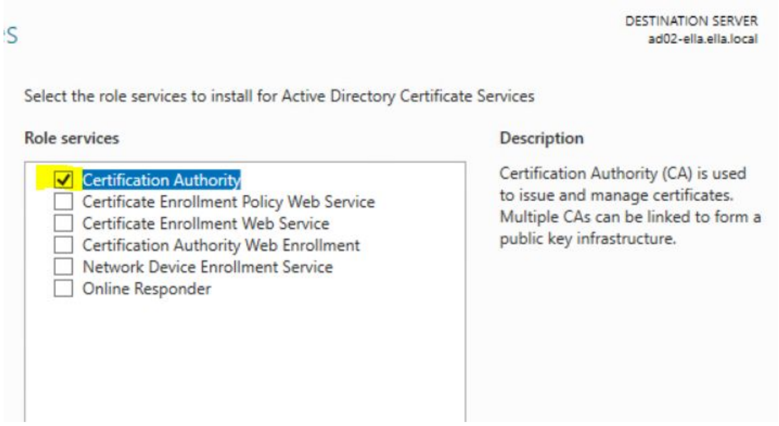
☑ Active Directory Certificate Services
☑ Active Directory Domain Services (Installed)
□ Active Directory Federation Services
□ Active Directory Lightweight Directory Services
□ Active Directory Rights Management Services
□ Device Health Attestation
☑ DHCP Server (Installed)
☑ DNS Server (Installed)
□ Fax Server
■ File and Storage Services (2 of 12 installed)
□ Host Guardian Service
□ Hyper-V

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

💡 Make sure that you are also installing the necessary management tools. This checkbox will appear in the pop-up when you select the box to install AD CS

We will only be installing the Certificate Authority, so that's all you need to have selected.



'S

DESTINATION SERVER
ad02-ella.ella.local

Select the role services to install for Active Directory Certificate Services

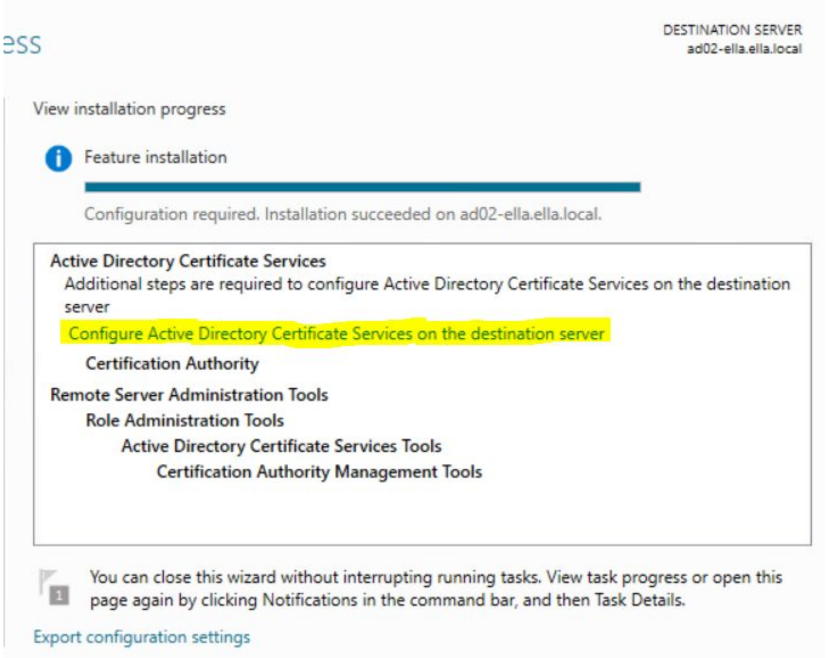
Role services

☑ 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.

Install the certificate authority, no restart is required. After installation is complete, open the notifications flag to configure services, or click the highlighted link below



ess

DESTINATION SERVER
ad02-ella.ella.local

View installation progress

Feature installation

Configuration required. Installation succeeded on ad02-ella.ella.local.

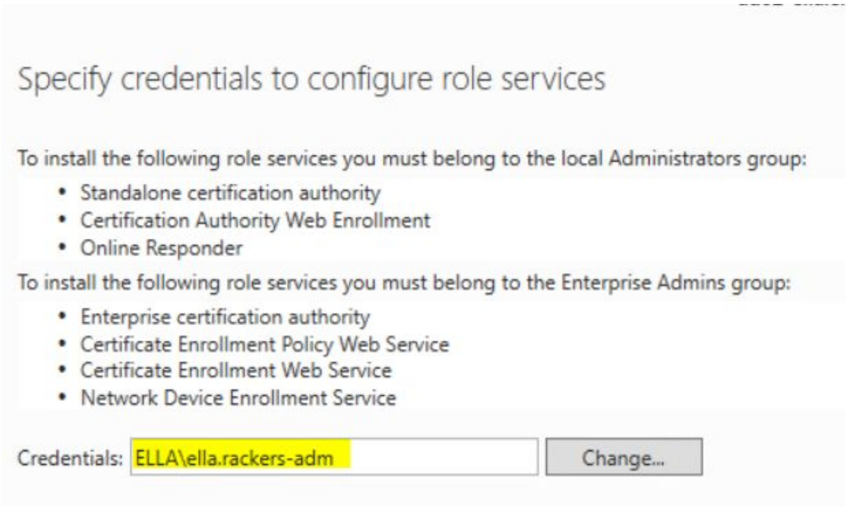
Active Directory Certificate Services
Additional steps are required to configure Active Directory Certificate Services on the destination server
Configure Active Directory Certificate Services on the destination server
Certification Authority
Remote Server Administration Tools
Role Administration Tools
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

You must choose an account to control the certificate, you should use an account that belongs to the enterprise admins group, like the admin account you created before.

💣 You have to use an admin account to manage these services. Unprivileged users will not be able to configure the services after you've installed them.



Specify credentials to configure role services

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

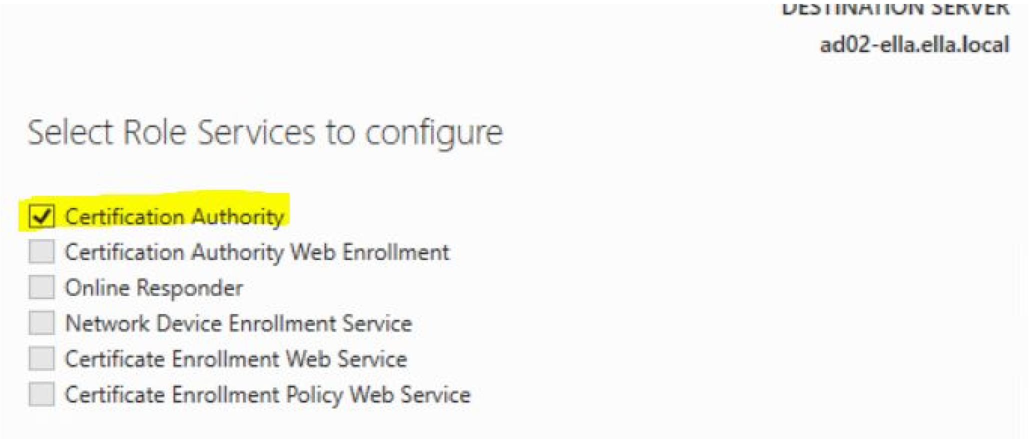
- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

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: ELLA\ella.rackers-adm

Select the Certification Authority option, as that’s what we installed and need to configure.

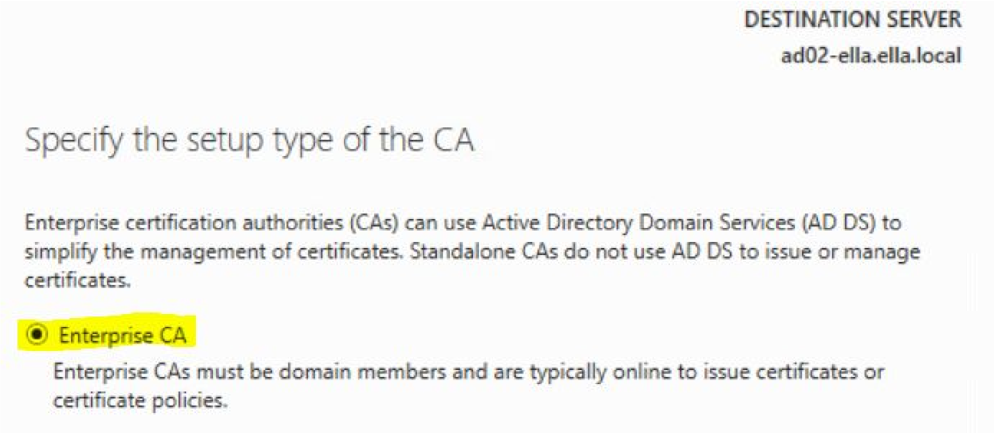


DESTINATION SERVER
ad02-ella.ella.local

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

Choose an enterprise CA. These CAs have to be online to distribute and sign certificates or update certificate policies.



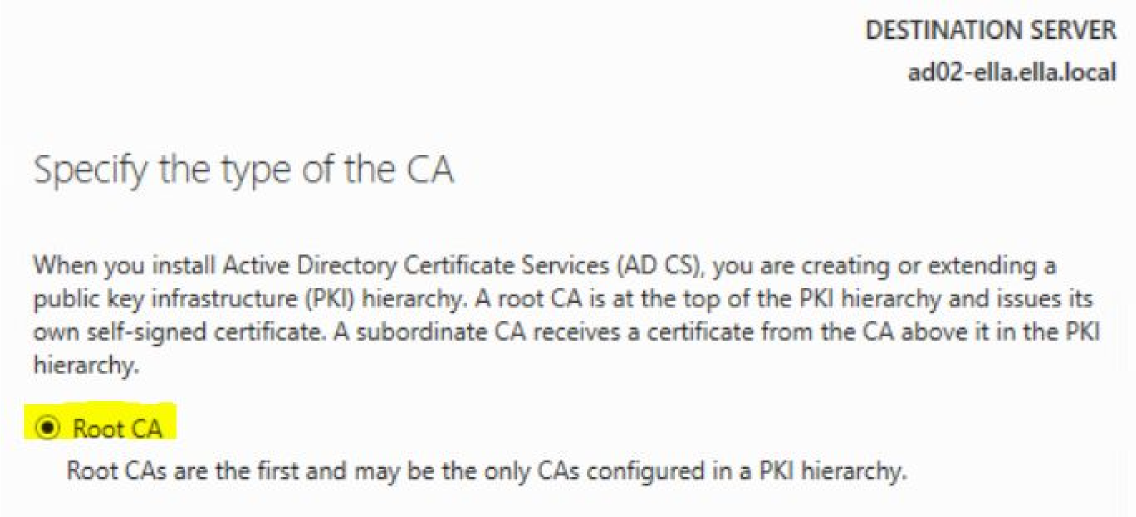
DESTINATION SERVER
ad02-ella.ella.local

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.

We will choose a root CA because this is the first CA we are configuring. Standalone CAs can be installed in addition to the root CA only after the root CA is installed and configured.



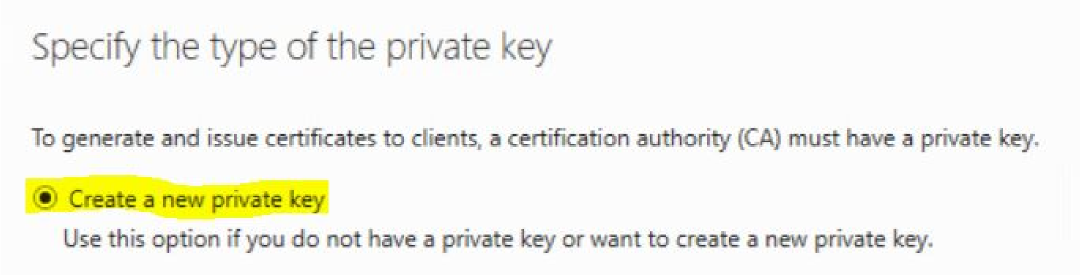
DESTINATION SERVER
ad02-ella.ella.local

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.

We will create a new key because we haven’t made one yet.



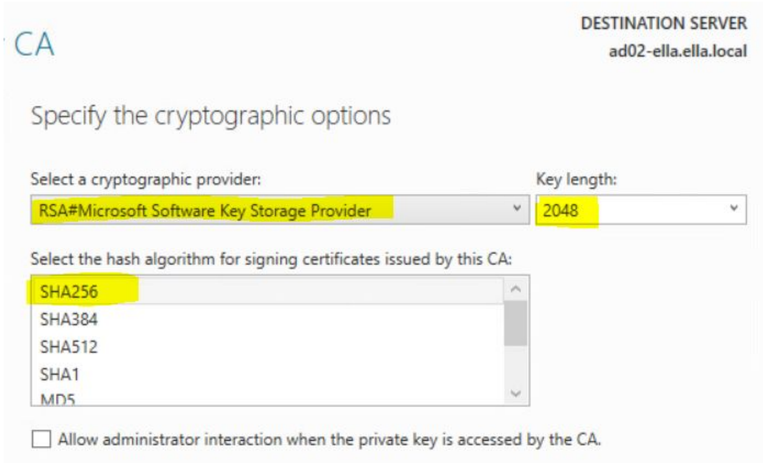
Specify the type of the private key

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.

We will choose an RSA key with a length of 2048, using a SHA256 hash for signing.



CA

DESTINATION SERVER
ad02-ella.ella.local

Specify the cryptographic options

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

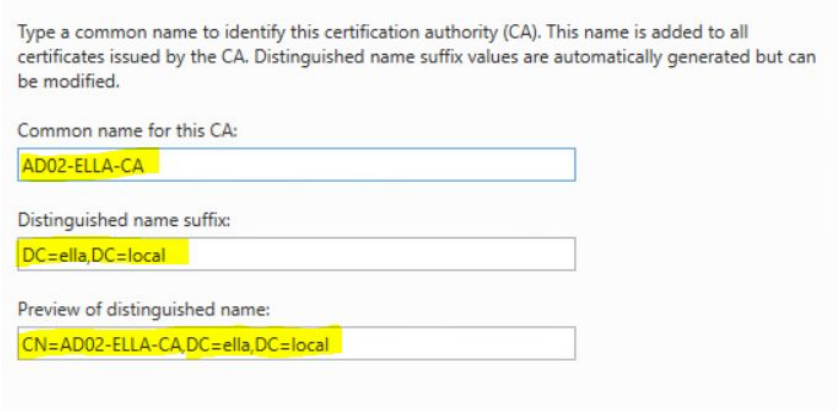
Key length: 2048

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.

All of this information should be auto-filled. You should not change the distinguished name suffix, but the common name can be changed, just make sure you remember it for later.



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: AD02-ELLA-CA

Distinguished name suffix: DC=ella,DC=local

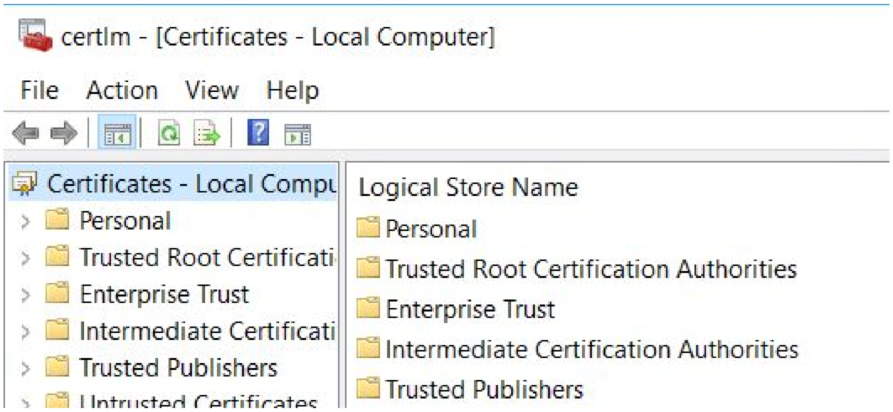
Preview of distinguished name: CN=AD02-ELLA-CA,DC=ella,DC=local

You can keep the rest of the options as defaults, then click configure to complete the process.

Now you should see you have AD CS installed on your windows server.

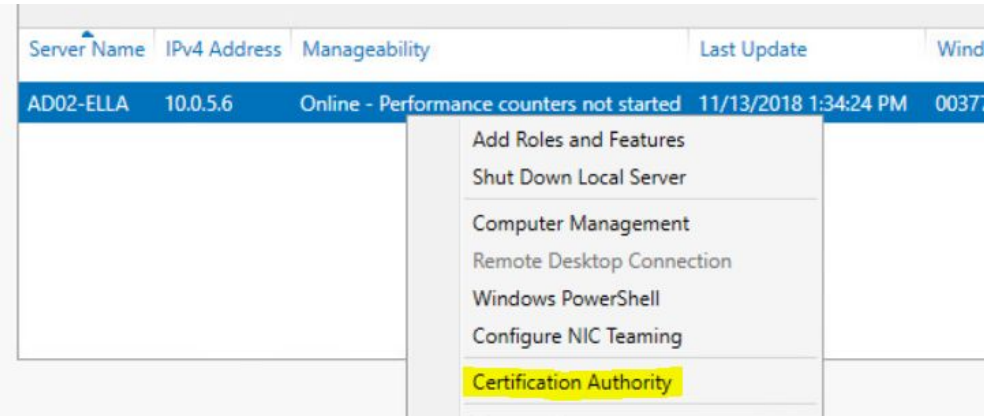
Creating a certificate template for your certificate authority

Go to Control Panel > Administrative Tools > Certificate Authority



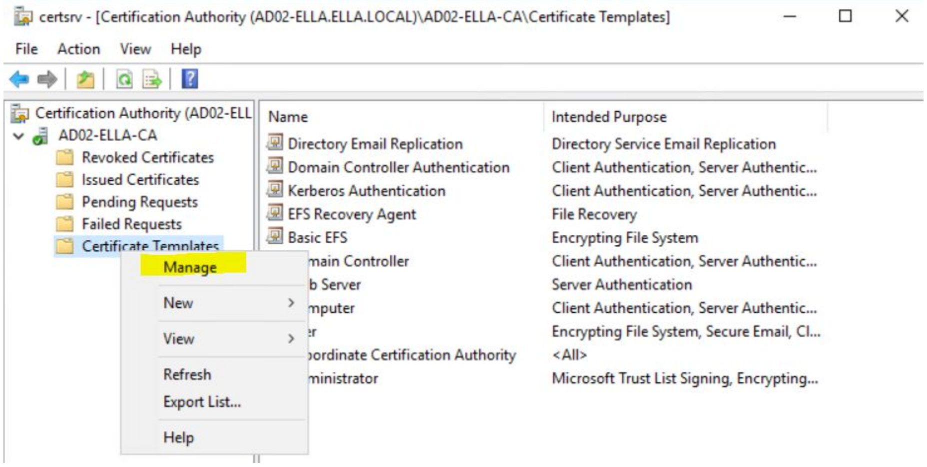
Logical Store Name
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers

To open the certificate authority settings, right-click on your server under the AD CS section and click on “Certification Authority”



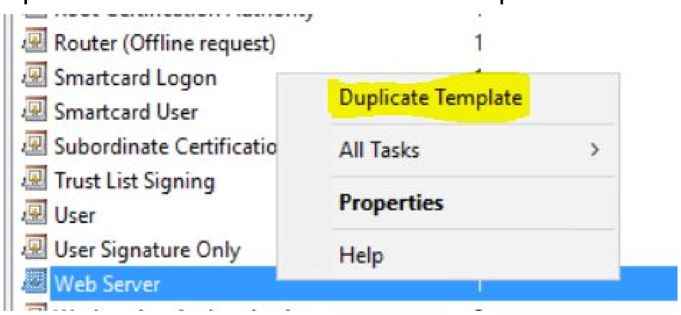
Server Name	IPv4 Address	Manageability	Last Update	Wind
AD02-ELLA	10.0.5.6	Online - Performance counters not started	11/13/2018 1:34:24 PM	00377

Navigate to manage certificate templates.

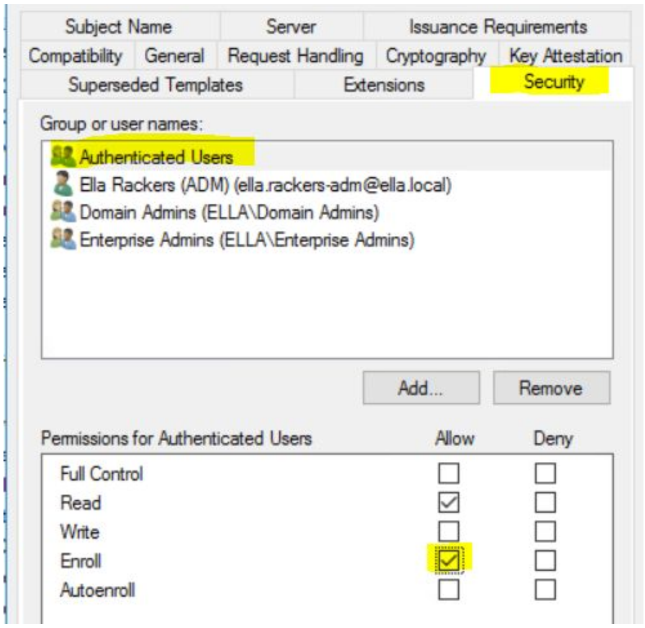


Name	Intended Purpose
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
main Controller	Client Authentication, Server Authentic...
b Server	Server Authentication
mputer	Client Authentication, Server Authentic...
er	Encrypting File System, Secure Email, Cl...
bordinate Certification Authority	<All>
ministrator	Microsoft Trust List Signing, Encrypting...

Duplicate the web server certificate template



Under the security tab, make sure authenticated users can enroll

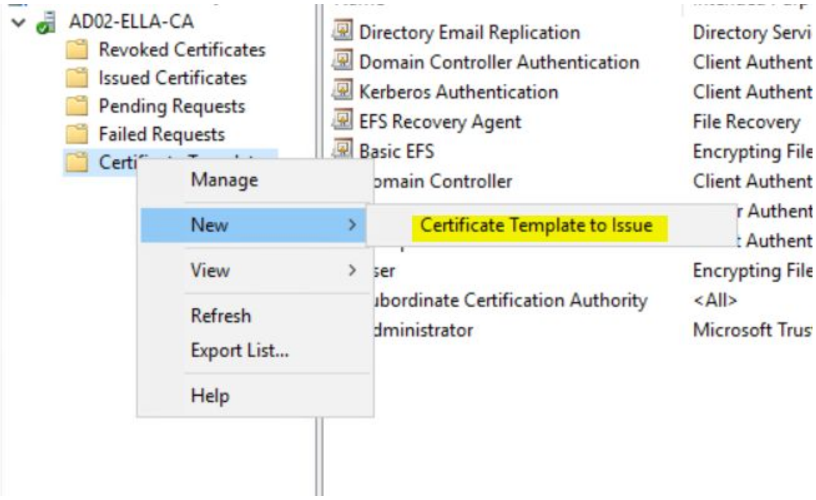


Group or user names:

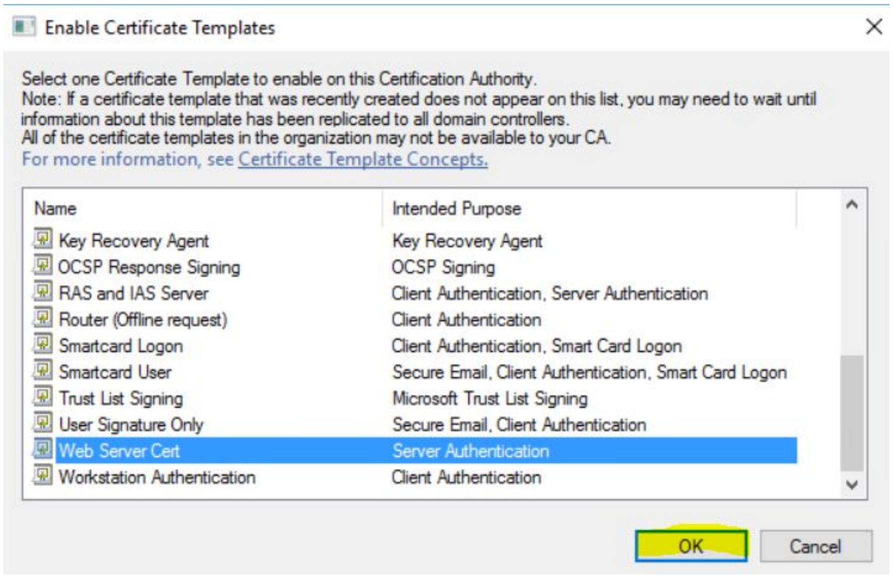
- Authenticated Users
- Ella Rackers (ADM) (ella.rackers-adm@ella.local)
- Domain Admins (ELLA\Domain Admins)
- Enterprise Admins (ELLA\Enterprise Admins)

Permissions for Authenticated Users	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	☑	□
Autoenroll	□	□

Change the name and apply the changes. Back in the certification authority settings, right click on certificate templates, and go to new > certificate template to issue.



Select your certificate and click OK



Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.

Name	Intended Purpose
Key Recovery Agent	Key Recovery Agent
OCSP Response Signing	OCSP Signing
RAS and IAS Server	Client Authentication, Server Authentication
Router (Offline request)	Client Authentication
Smartcard Logon	Client Authentication, Smart Card Logon
Smartcard User	Secure Email, Client Authentication, Smart Card Logon
Trust List Signing	Microsoft Trust List Signing
User Signature Only	Secure Email, Client Authentication
Web Server Cert	Server Authentication
Workstation Authentication	Client Authentication

Requesting the Certificate on CentOS box

To request a certificate, first we need to have a private key and a certificate request file. Enter in the following command:

- **`openssl req -newkey rsa:2048 -keyout webserver.key -out webserver.csr`**

It will ask you to enter in information about where you’re from. None of it really matters, but remember it for later because it all has to be the same besides the common name.

On AD

> 💡 You will need to have pscp (putty) installed for this next step on your AD02 Machine.

In powershell, execute the following command (using your file path on your webserver). This will copy your certificate request onto your AD machine.

- **`pscp -scp [accounts]@[ip address]:/webserver.csr C:\Users\[admin account]\Downloads\`**
- **`certreq -submit -attrib “CertificateTemplate:Web Server Cert” Downloads\webserver.csr`**

Hit enter on all the following prompts, and when you’re prompted to save the certificate, remember the file path and name in which you save it. Finally, transfer the certificate back to your centos server with the following command:

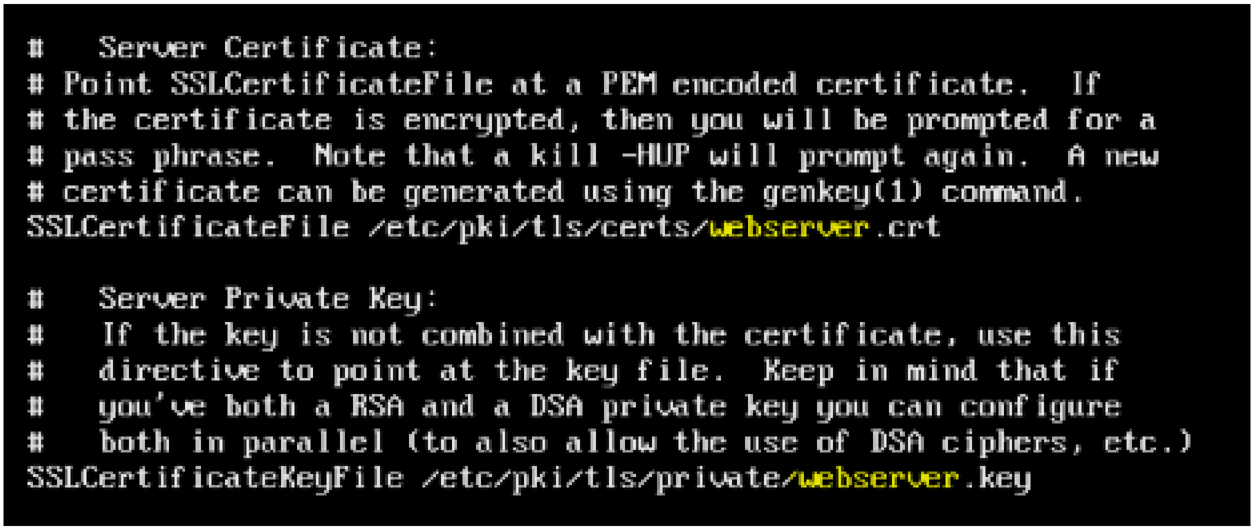
- **`pscp -scp Documents\webserver.cer [account]@[ip address]:/`**

On Web02

Run the following commands:

- **`cp webserver.cer webserver.crt`**
- **`cp webserver.crt /etc/pki/tls/certs`**
- **`cp webserver.key /etc/pki/tls/private`**
- **`yum install mod_ssl -y`**

In /etc/http/conf.d/ssl.conf, make sure to change the following file names to match your files.



```
#   Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate.  If
# the certificate is encrypted, then you will be prompted for a
# pass phrase.  Note that a kill -HUP will prompt again.  A new
# certificate can be generated using the genkey(1) command.
SSLCertificateFile /etc/pki/tls/certs/webserver.crt

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile /etc/pki/tls/private/webserver.key
```

Restart httpd. You will have to enter the password that you entered when creating your private key, and then it should be complete and your web service should be able to use http.