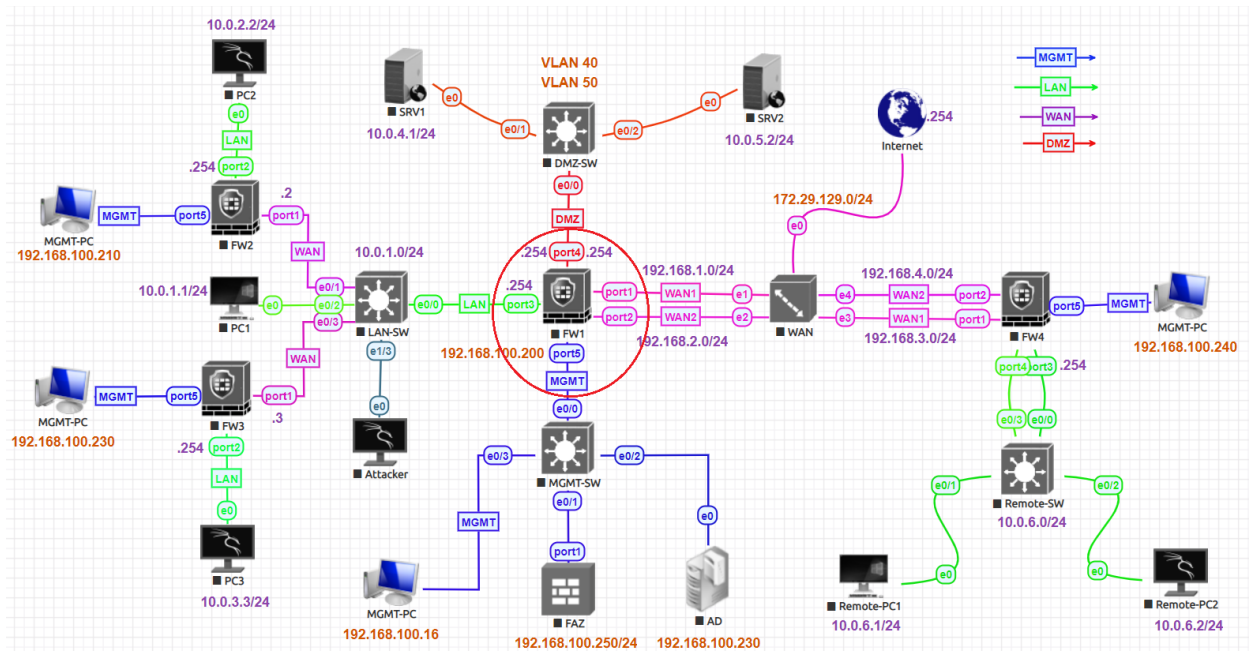


SSL Inspection Lab:



Go to **System -> Certificates>Create/Import** and select **Generate CSR**. Create CSRs, Which will be used to issue Subordinate Certification Authority certificate.

The screenshot shows the FortiGate GUI with the 'System' menu open and 'Certificates' selected. The 'Generate CSR' option is highlighted in red. Below the menu, a table of local certificates is displayed:

Local Certificate	Subject
Fortigate-CSR	C = SA, ST = Riyadh, L = Riyadh, O = Test, OU = IT, CN = ...
Fortinet_Factory	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...
Fortinet_Factory_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...
Fortinet_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...
Fortinet_SSL_DSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...

Provide Certificate Name, ID Type, Optional Information and Click **OK**.

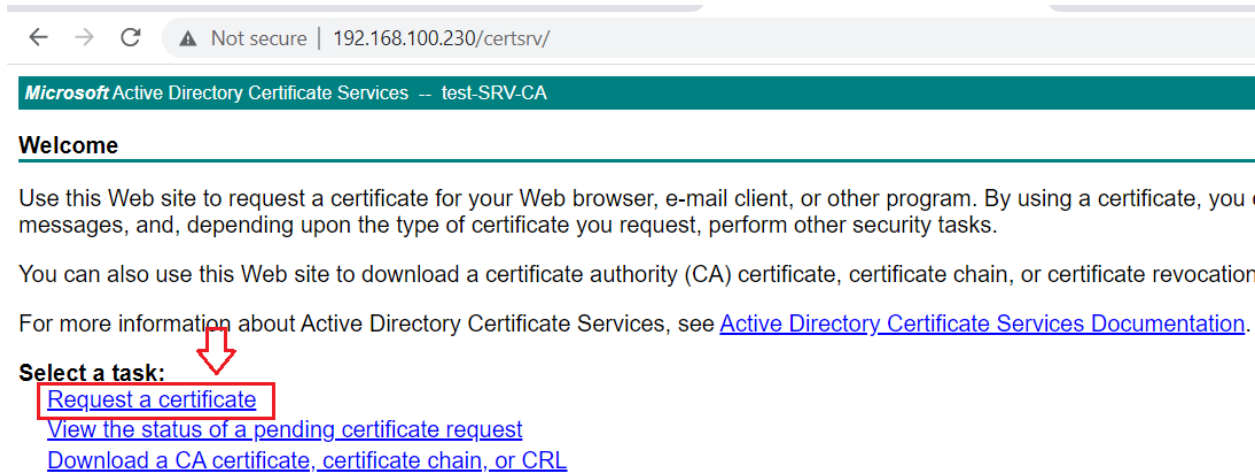
After creating CSRs, it will be visible in the Certificates view. Select the CSRs created in previous step and select **Download**.

Name	Subject	Comments
Local CA Certificate 2		
Fortinet_CA_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...	This is the default CA certificate the
Fortinet_CA_Untrusted	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...	This is the default CA certificate the
Local Certificate 15		
Fortigate-CSR		
Fortinet_Factory	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...	This certificate is embedded in the f
Fortinet_Factory_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...	This certificate is embedded in the f
Fortinet_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...	This certificate is embedded in the f
Fortinet_SSL_DSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...	This certificate is embedded in the f
Fortinet_SSL_DSA2048	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...	This certificate is embedded in the f
Fortinet_SSL_ECDSA256	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...	This certificate is embedded in the f
Fortinet_SSL_ECDSA384	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...	This certificate is embedded in the f
Fortinet_SSL_ECDSA521	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...	This certificate is embedded in the f
Fortinet_SSL_ED448	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...	This certificate is embedded in the f
Fortinet_SSL_ED25519	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...	This certificate is embedded in the f
Fortinet SSL RSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...	This certificate is embedded in the f

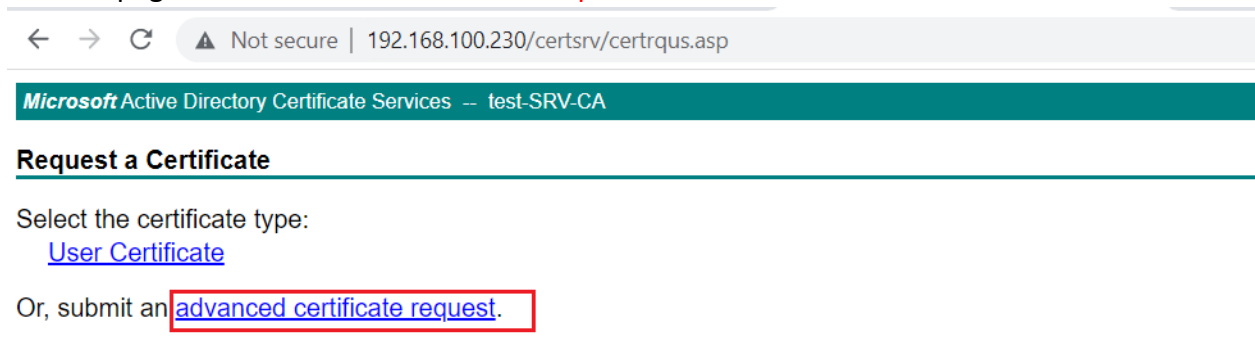
Open CSR request with **notepad** or **notepad++** select all text The copied text must include the header and footer line as well.

```
Fortigate-CSR.csr x
1 -----BEGIN CERTIFICATE REQUEST-----
2 MIIC9DCCAdwCAQAwYUxCzAJBgNVBAYTA1NBMQ8wDQYDVQQIEwZSaXlhZGgxZDZAN
3 BgNVBACtB1JpeWFkaDENMAsgAlUEChMEVGVzdDELMAkGAlUECxmCSVQxGDAWBgNV
4 BAMTDzE5Mi4xNjguMTAwLjIwMDEeMBwGCSqGSIB3DQEJARYPdGVzdEB0ZXN0LmXv
5 Y2FsMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAx4POKSRdwVxvvoAS
6 ztpRWsIfc/igGQf71gyiv+JT0RcNL02+Nj2yG0Vr2714NkP+mOjDUNwHAzgJh4eG
7 5KDPqSIAwPT5ImDml0M3lqX/eG3G3vEPUTumyt6egDw6j34mU95IKQDoMebgCBN5
8 0dOJfANGtd5gC+BS8tN7b/r1/PPS0+svq7bzLNJ9oUvSc2dUowkwBfeKeZI82evf
9 67MdzyaXs2kpmEoEwMO3wwbwrNumdmWlungXt6U9xMsbPSM/zYDDI712dY6XlHZw
10 v0TRFDanduX4YhZGhVOIZh442KsC4NHIPoMGOUvdBUwMOKs+UImGEL67x1P1v8e
11 8ME+/QIDAQABoCkwJwYJKoZIHvcNAQkOMRowGDAJBGNVHRMEAjAAMAsGAlUdDwQE
12 AwIFoDANBgkqhkiG9w0BAQsFAAOCAQEAN8Ig8uz9jN0EUYVOA2pgB2NaA4cyfrlt
13 3fDOBD6rvag7wMK+uE/W/eYza+C59lAzanXkANimEWonIqrtoXthtwJlMht8Mqr
14 6ek8ADTRcGSsrN1EidgElladh7F8QUxldbhfzr3Wgz9TgtpgwNZkbE5RepmPwQHO
15 agegGn3Z/6+Ejp/AvJmbJgbTVLkLxKXqQ/VRr7NjCzfvSQ1WLXBwTYoJclsdJ1aL
16 u92UZeXpcwG3FJZC3j/88UYC/Q6XKRSSJsti5HJg/Can3YAo4p7ViTkIei2EbVF5
17 dHiIKs1bZzZ3S1XHubMRm6oxweSqx0R6cXajN1KVA5spteVKCPf8XQ==
18 -----END CERTIFICATE REQUEST-----
```

Go to Microsoft Certification Authority server on the link <http://192.168.100.230/certsrv> and sign in with administrative account. Select **Request a Certificate**



On next page select **advanced certificate request**.



Paste the copied CSR request, select **Subordinate Certification Authority** in Certificate Template: field and select **Submit**.

← → ↻ ⚠ Not secure | 192.168.100.230/certsrv/certrqxt.asp

Microsoft Active Directory Certificate Services -- test-SRV-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or file into the text box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
0d0JfANGtd5gC+BS8tN7b/r1/PPS0+svq7bzLNJ9oUvSc2dUowkwBfeKeZIE
67MdzyaXs2kpmEoEwMO3wwbwrNumdmw1ungXt6U9xMsbPSM/zYDDI712dY6X
v0TRFDanduX4YhZGhVOIZh442KsC4NHiPoMGOUvdBUUnwMOKs+UImGEL67x1F
8ME+/QIDAQABoCkwJwYJKoZIHvcNAQkOMRowGDAJBGNVHRMEAjAAMAsGA1Uc
AwIFoDANBgkqhkiG9w0BAQsFAAOCAQEAN8I8uz9jn0EUYVOA2pgB2NaA4cy
3fDOBd6rvag7wMK+uE/W/eYza+C59lAzanXkANimEwonIiqrt0XthtwJlMht
6ek8ADTRcGSsrN1EidgE1ladh7F8QUx1dbhfzr3Wgz9TgtpgwNZkbE5RepMf
ageGn3Z/6+Ejp/AvJmbJgbTVLkLxKXqQ/VRr7NjCzfvSQ1WLXBwTYoJc1sc
u92UZeXpcwG3FJZC3j/88UYC/Q6XKR5SJsti5HJg/Can3YAo4p7ViTkIei2E
```

Certificate Template:

Subordinate Certification Authority

Additional Attributes:

Attributes:

Submit >

Select **Base64 encoded** and select **Download certificate**.


← → ↻ ⚠ Not secure | 192.168.100.230/certsrv/certifnsh.asp

Microsoft Active Directory Certificate Services -- test-SRV-CA

Certificate Issued

The certificate you requested was issued to you.

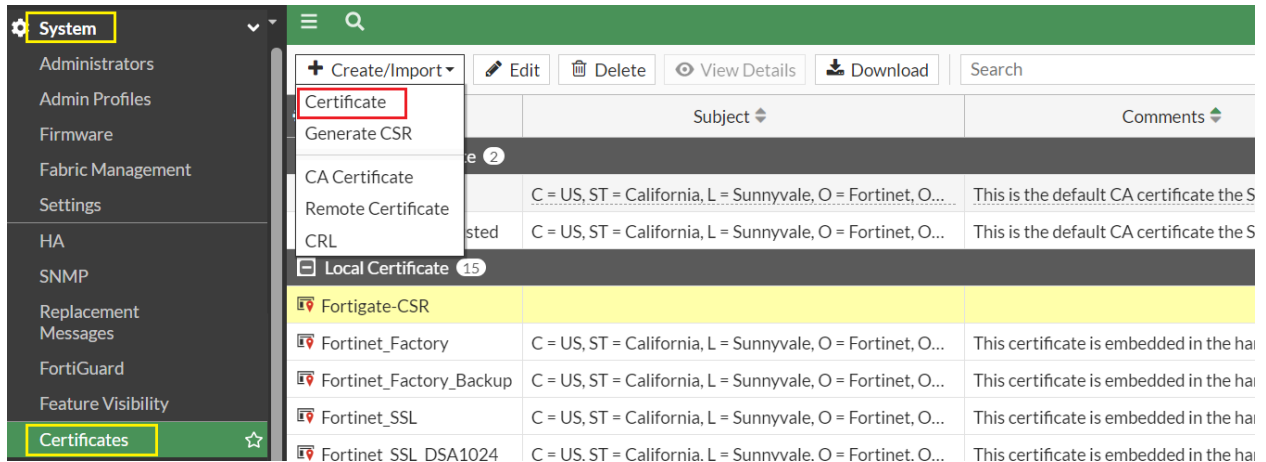
DER encoded or Base 64 encoded

 [Download certificate](#)

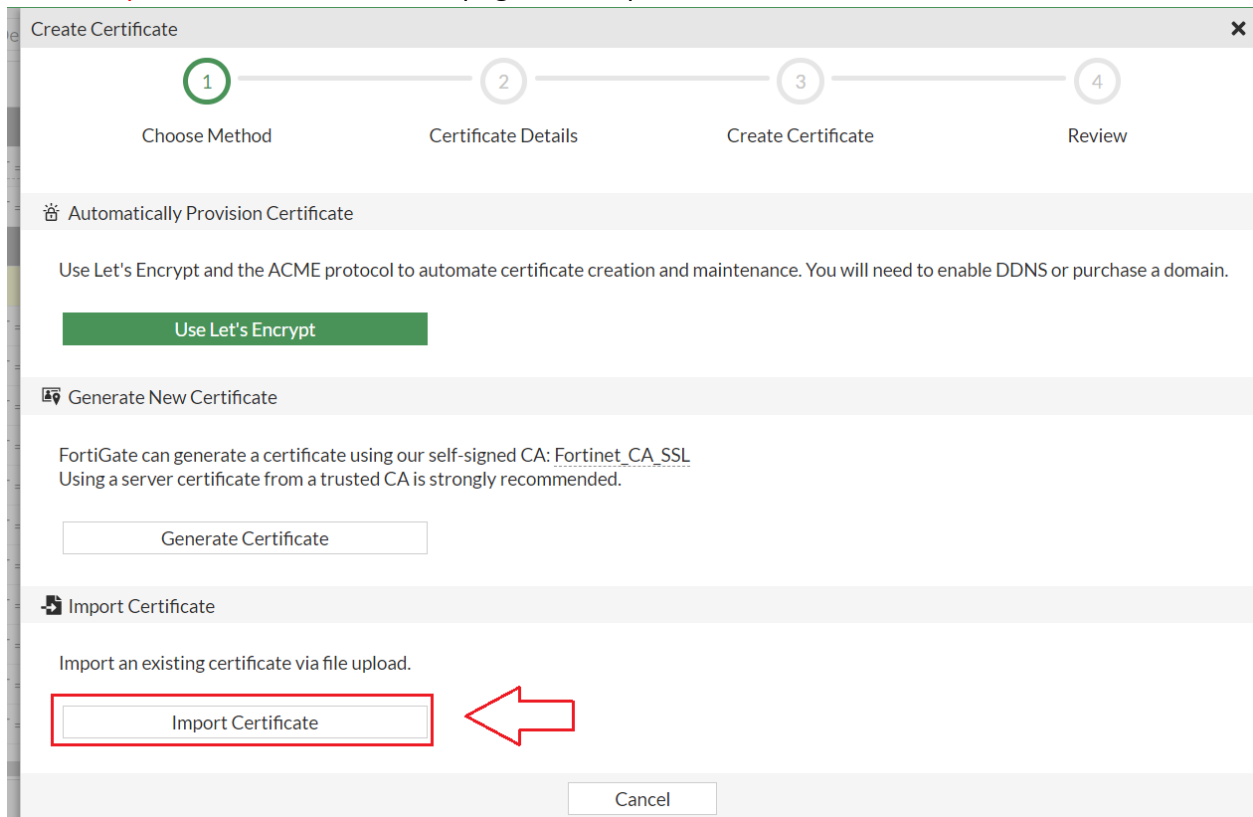
[Download certificate chain](#)



Now the CSR Request is read to import it to FortiGate Firewall in **System -> Certificates >Create/Import >Certificate**.



Select **Import Certificate** down the page it will open a new window.



Make sure **Local Certificate** is selected and select **Upload**. Browse to the folder where the certificates is downloaded, select the certificate and select **Open** and click Create to upload certificate to FortiGate.

Create Certificate

Choose Method Certificate Details Create Certificate Review

Import Certificate

Type Local Certificate PKCS #12 Certificate Certificate

Certificate file Fortigate-Win.cer

Create Back Cancel

To confirm the certificate has been imported and installed successfully visible below.

Name	Subject	Issuer	Expires	Status
Local CA Certificate 2				
Fortinet_CA_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...	Fortinet	2032/05/24 16:58:18	Valid
Fortinet_CA_Untrusted	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...	Fortinet	2032/05/22 21:11:48	Valid
Local Certificate 15				
Fortigate-CSR	C = SA, ST = Riyadh, L = Riyadh, O = Test, OU = IT, CN = ...	test-SRV-CA	2024/05/27 15:55:44	Valid

Create SSL Inspection Profile:

Go to Security Profiles > SSL/SSH Inspection. Create a new profile, or clone the default profile. Configure the remaining setting as needed select CA certificate create previously Click OK.

The screenshot shows the 'Edit SSL/SSH Inspection Profile' configuration page. The left sidebar has 'Security Profiles' selected, with 'SSL/SSH Inspection' highlighted. The main panel shows the following settings:

- Name: WIN-Deep-Inspection
- Comments: Win CRT deep inspection profile. (32/255)
- SSL Inspection Options:
 - Enable SSL inspection of: Multiple Clients Connecting to Multiple Servers
 - Inspection method: Full SSL Inspection
 - CA certificate: Fortigate-CSR (highlighted with a red box and arrow)
 - Blocked certificates: Allow, Block, View Blocked Certificates
 - Untrusted SSL certificates: Allow, Block, Ignore, View Trusted CAs List
 - Server certificate SNI check: Enable, Strict, Disable
 - Enforce SSL cipher compliance: Off
 - Enforce SSL negotiation compliance: Off
 - RPC over HTTPS: Off

Go to Security Policy & Objects>Firewall Policy and select the newly created SSL Inspection Profile from the dropdown and click OK to apply the setting.

The screenshot shows the 'Security Profiles' configuration page. The left sidebar has 'Policy & Objects' selected, with 'Firewall Policy' highlighted. The main panel shows the following settings:

- AntiVirus: Off
- Web Filter: Off
- Video Filter: On (VF Youtube-Profile)
- DNS Filter: On (DNS Custom-DNS)
- Application Control: On (APP Custom-Apps)
- IPS: On (IPS Custom-IPS)
- File Filter: On (FF Custom-File)
- SSL Inspection: On (SSL WIN-Deep-Inspection, highlighted with a red box)

Internal Clients will still give Certificate error need to install root CA to work.