

Steps to request internal Microsoft CA signed certificate for WSA HTTPS proxy Certificate Signing Request (CSR) Option

1. Download the CSR from the WSA
2. Open the CSR using Wordpad or another text editor and copy the Certificate Request section (only the section --BEGIN CERTIFICATE REQUEST-- xxxxx --END CERTIFICATE REQUEST--)
3. Navigate to the MS CA server: <https://server/certsrv>
4. Select "Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file"
5. Click Certificate Template and choose Subordinate Certification Authority
6. Paste in your copied CSR
7. Download your CA signed certificate
8. Upload the signed certificate (make sure you use the Signed certificate upload section and not the top section).

Note: We need to Submit > Commit the changes on every step changed on WSA.

Reference:

Video KB: Steps to enable HTTPS proxy on WSA & Certificate Signing Request (CSR) option.

<https://supportforums.cisco.com/video/11933356/steps-enable-https-proxy-wsa-certificate-signing-request-csr-option>

Internal KB: Create Subordinate CA Certificate Microsoft CA Server

<https://techzone.cisco.com/t5/Web-Security-Appliance-WSA/Create-Subordinate-CA-Certificate-Microsoft-CA-Server/ta-p/272772>

1. Download the CSR from the WSA

HTTPS Proxy Settings

Enable HTTPS Proxy

HTTPS Ports to Proxy:

Root Certificate for Signing:

Use Uploaded Certificate and Key [Upload Files](#)

Certificate: [Browse...](#)

Key: [Browse...](#)

Key is Encrypted

No certificate has been uploaded.

Use Generated Certificate and Key [Generate New Certificate and Key](#)

Common name: Demo Cert
Organization: Test
Organizational Unit: Lab
Country: US
Expiration Date: Apr 11 00:47:11 2016 GMT
Basic Constraints: Not Critical

[Download Certificate...](#) | [Download Certificate Signing Request...](#)

Signed Certificate:

To use a signed certificate, first download a certificate signing request using the link above. Submit the request to a certificate authority, and when you receive the signed certificate, upload it using the field below.

Certificate: [Browse...](#) [Upload File](#)

2. Open the CSR using Wordpad or another text editor and copy the Certificate Request section (only the section --BEGIN CERTIFICATE REQUEST-- xxxxx --END CERTIFICATE REQUEST--)

```
Certificate Request:
  Data:
    Version: 0 (0x0)
    Subject: C=US, O=Test, OU=Lab, CN=Demo Cert
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
        Modulus (1024 bit):
          00:a2:33:04:bc:93:27:3d:12:7e:fa:ce:51:00:65:
          62:59:08:26:f2:5b:73:c0:65:28:e4:31:c4:a4:5a:
          57:a5:93:12:c0:c4:49:9a:f6:84:39:a8:36:c1:32:
          6c:95:00:7e:51:ff:2b:6b:e0:0c:5e:82:e3:e5:d9:
          fc:7c:2a:d4:46:ac:97:40:0b:77:eb:c6:99:58:e9:
          28:21:6e:b7:eb:57:d0:88:5d:e3:80:4b:32:37:ab:
          3a:a4:40:01:d5:ca:84:44:90:96:2f:b8:0a:c2:27:
          54:a5:75:4e:31:47:b5:16:24:98:31:9e:cb:59:ea:
          b0:bd:9b:c6:3c:8b:1e:af:81
        Exponent: 65537 (0x10001)
    Attributes:
      a0:00
  Signature Algorithm: sha1WithRSAEncryption
    3b:a7:a7:11:27:88:bd:92:01:c2:3a:c1:50:a7:ee:2b:e1:35:
    03:b2:d5:e9:1a:d7:93:18:cc:fa:59:69:7e:1c:83:17:33:12:
    38:a9:20:c9:f7:64:3d:c3:62:ee:d3:2e:7f:f3:76:6b:61:cd:
    1e:cf:bd:34:79:79:26:cf:e5:51:53:89:3c:7e:6b:35:20:6a:
    b1:00:45:85:a9:f0:01:6d:6c:a3:45:93:60:4f:87:59:a6:fe:
    66:8e:75:8a:87:49:8f:46:a8:ab:61:2f:4e:c9:13:68:be:1b:
    d4:da:42:2a:59:b3:98:81:b3:78:f9:a0:e8:88:a7:50:08:b7:
    a6:5c
```

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBhTCB7wIBADBGMQswCOYDVQQGEwJBVTEZMBCGA1UEChMQQ29udGVudCBTZWN1
cm10eTEMMAoGA1UECxMDVEFDMQ4wDAYDVQQDEwUyMvdTQTCBnzANBgkqhkiG9w0B
AQEFAAOBjQAwgYkCgYEAojMEvJMnPRJ++s5RAGViWQgm81tzwGUo5DHEpFpXpZMS
wMRJmvaEOag2wTJslQB+Uf8ra+AMXoLj5dn8fCrURqyXQAt368aZWokoIW6361fQ
iF3jgEsyN6s6pEAB1cqERJCWL7gKwidUpXVOMUelFiSYM27LWeqwv2vGPIser4EC
AwEAAaAAMA0GCSqGSIb3DQEBBQUAA4GBAdunpxEniL28AcI6wVCn7ivhNQOy1eka
15MYzPpZax4cgxczEjipIMn3ZD3DYu7TLn/zdmthzR7PvTR5eSbP5VFTiTx+azUg
arEARYWp8AftbKNFk2BPhlmm/maOdYqHSY9GqKthL07JE2i+G9TaQipZs5iBs3j5
cOiIplAI6Zc
-----END CERTIFICATE REQUEST-----
```



3. Navigate to the MS CA server: <https://server/certsrv>

- a. Request a certificate
- b. advance certificate request

Microsoft Active Directory Certificate Services –

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

 [Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

Microsoft Active Directory Certificate Services –

[Home](#) 

Request a Certificate

Select the certificate type:

[User Certificate](#)

 Or, submit an [advanced certificate request](#).

4. Select "Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file"

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

[Create and submit a request to this CA.](#)

 [Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.](#)

5. Click Certificate Template and choose Subordinate Certification Authority

6. Paste in your copied CSR from step 2

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 PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

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

```
38:02:3b:c0:32:2e:eb:70:58:de:f3  
82:d6:36:c2:ee:b7:96:67:3d:54:60  
e6:02:7e:60:cc:3c:5c:a4:f5:73:1a  
35:84:cd:a2:3a:ba:20:94:a5:27:1e  
e8:a2:49:21:e0:68:13:ba:6f:d6:9b  
ef:91
```



Certificate Template:

Subordinate Certification Authority



Additional Attributes:

Attributes:

Submit

7. Download your CA signed certificate

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded 



[Download certificate](#)

[Download certificate chain](#)

8. Upload the signed certificate (make sure you use the Signed certificate upload section and not the top section).

HTTPS Proxy Settings

Enable HTTPS Proxy

HTTPS Ports to Proxy:

Root Certificate for Signing:

Use Uploaded Certificate and Key [Upload Files](#)

Certificate: [Browse...](#)

Key: [Browse...](#)

Key is Encrypted

No certificate has been uploaded.

Use Generated Certificate and Key [Generate New Certificate and Key](#)

Common name: Demo Cert
Organization: Test
Organizational Unit: Lab
Country: US
Expiration Date: Apr 11 00:47:11 2016 GMT
Basic Constraints: Not Critical

[Download Certificate...](#) | [Download Certificate Signing Request...](#)

Signed Certificate:

To use a signed certificate, first download a certificate signing request using the link above. Submit the request to a certificate authority, and when you receive the signed certificate, upload it using the field below.

Certificate: [Browse...](#) [Upload File](#)

