CA Certificate with Certificate authority from Windows Server 2022

From WTI Unit

1. Access WTI via web GUI to create a certificate by navigate to Configuration >> Network Configuration >> IPv4 >> Eth0 >> Web >> SSL Certificate and fill in all the requirement.

2. Click Display CSR and copy the Begin to End Certificate Request.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDAzCCAesCAQAwgYkxGTAXBgNVBAMMEHRlc3Qud3RpLWxhYi5jb20xCzAJBgNV
BAgMAkNBMQ8wDQYDVQQHDAZJcnZpbmUxCzAJBgNVBAYTAlVTMSIwIAYJKoZIhvcN
AQkBFhNlbmtub3duQHd0aS1sYWIuY29tMRAwDgYDVQQKDAd3dGktbGFiMQswCQYD
VQQLDAJJVDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMlUU79GxQdV
YW4nnNy4NnN5zAqmrEC1Sgvx5xXXuUjK7uL1BJwRJ/5MpJbW8ud9NpD7isxrEktC
vlozERxiXu+fm0iV6PyvHVbroG1fZLFweW1sMPuTDC82NpI2yeLTNM8mnYXdySFW
Sva7Hb45lzdrAzj6SdlST85ErcNDEJKI6wpLT2KA86rYDdY7JC/TSSqgkd1BT59j
mxjeDI8lt8GEjvgv3Cns6jcwe2DojJ3XFsq6mqSh4gHVCv8KDbal1QL2IuloyQQq
0oUtCBPpoaOzxqodYDBxC4sIdvBvOw4xeoKDHNa+uKT1REauyxDOrbe3a5tvxwDY
rCnPdN2Uc9UCAwEAAaA0MDIGCSqGSIb3DQEJDjElMCMwIQYDVR0RBBowGIIQdGVz
dC53dGktbGFiLmNvbYcErBAALDANBgkqhkiG9w0BAQsFAAOCAQEAj+iZKwnGXc3J
YXhkPl7jDvjiTQGDWHeEhEwDoB/8mDQH8XU7owv4tHjpkdNUMqQOb9Hxe459i1rN
6SuraOg3KsY86bEyttIWlbqmVBb+KN9DaKzdJPIaDYs9YThtWCaRYHYGUwvJYKfA
lEbMvCRlFMKnjYD8ycUfKpDZznATJ9dTm31ADX8IcNmf5QnRza6rH/NfnJ+Rfyw/
gM+/ZcAtOncl5ph6oBAg0co5HDB8RwrfW36PwZ1v7iTxlfQPNfskzClSL6ch0awi
ZC5WE4BUvvMjE+6AvDrmGIKZkItDEAE9MJK9V4LYbZXgX0ZLHFSjRy5HaQZxEGQc
q7sBL3TeIA==
-----END CERTIFICATE REQUEST-----
```

Certificate Request Created - Tue Mar 19 16:48:16 2024 UTC time

subject=CN = test.wti-lab.com, ST = CA, L = Irvine, C = US, emailAddress = unknown@wti-lab.com, O = wti-lab, OU = IT

[SSL Certificate Home]

3. Go to the browser where you host your Certificate Authority for example we host it here http://dcwin2022/certsrv/
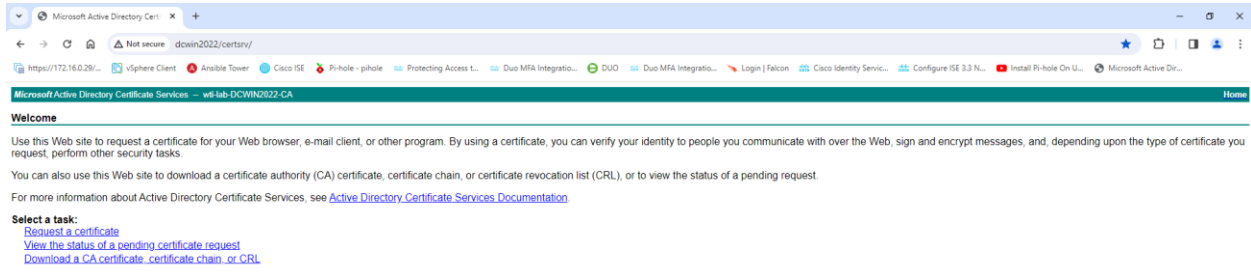
4. Under Select a task. Choose Request a certificate link >> Advanced certificate request. Paste the CSR from step 2 to the first box and select web Server under the certificate template and click submit button.
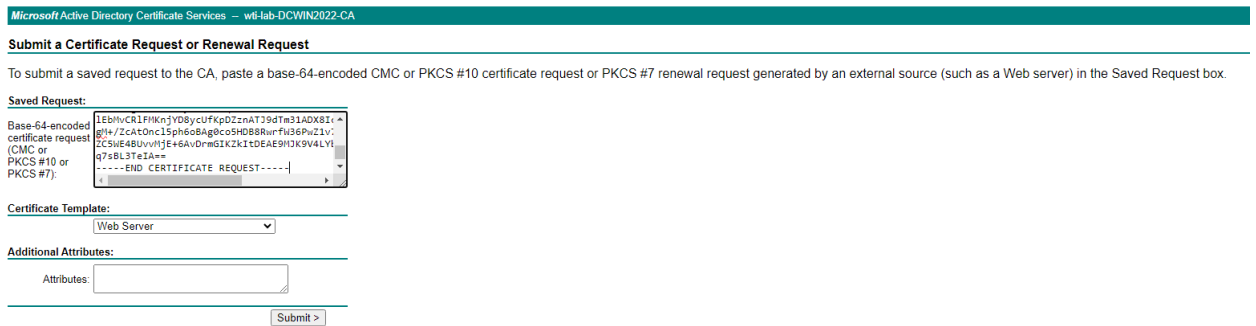
5. Select Base 64 encoded and click download certificate link.
6. Open the certificate that you just download it in notepad and copy the begin to end certificate and paste it to WTI unit under SSL certificate Signed Certificate box section and click import CRT button.

SSL Certificates [eth0]

⊘ Common Name:	test.wti-lab.com
⊘ State or Province:	CA
⊘ Locality:	Irvine
⊘ Country Code:	US
⊘ Email Address:	unknown@wti-lab.com
⊘ Organization (O):	wti-lab
⊘ Organizational Unit (OU):	IT
⊘ SAN Options:	☐ (Show SAN)
SAN 1:	DNS ⌄ test.wti-lab.com
SAN 2:	IP ⌄ 172.16.0.44

Cancel CSR

Display CSR

⊘ Signed Certificate

```
-----BEGIN CERTIFICATE-----
MIIGtTCCBJ2gAwIBAgITKgAAAAeRaju5J0A1YQAAAAABzANBgkqhkiG9w0BAQsF
ADBNMRMwEQYKCZImiZPyLGQBGRYDY29tMRcwFQYKCZImiZPyLGQBGRYHd3RpLWxh
YjEdMBsGA1UEAxMUd3RpLWxhYi1EQ1dJTjIwMjItQ0EwHhcNMjQwMzE5MTY0NjA0
```

⊘ ☐ Show Intermediate CA Certificate

Import CRT

7. After the import completed the screen will look like the below.

Site ID: (undefined)

SSL Certificates [eth0]

② Common Name:	test.wti-lab.com
② State or Province:	CA
② Locality:	Irvine
② Country Code:	US
② Email Address:	unknown@wti-lab.com
② Organization (O):	wti-lab
② Organizational Unit (OU):	IT
② SAN Options:	☐ (Show SAN)
SAN 1:	DNS ∨ test.wti-lab.com
SAN 2:	IP ∨ 172.16.0.44
	Remove CRT

Display CRT File

Current Certificate

subject=C = US, ST = CA, L = Irvine, O = wti-lab, OU = IT, CN = test.wti-lab.com, emailAddress = unknown@wti-lab.com

② ☐ Show Intermediate Certificate

8. You will need to install or import the Server CA Certificate to your machine where you will access the WTI unit by going to step 3 and choose Down load a CA Certificate, certificate chain or CRL link.

⌄ Microsoft Active Directory Cert ✕ +

← → C ⌂ ⚠ Not secure dcwin2022/certsrv/

📷 https://172.16.0.29/... 📷 vSphere Client Ⓐ Ansible Tower 🔵 Cisco ISE Pi-hole - pihole Protecting Access t... Duo MFA Integratio... ⊖ DUO Duo MFA Integratio... Login | Falcon Cisco Identity Se

Microsoft Active Directory Certificate Services — wti-lab-DCWIN2022-CA

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 the 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

9. In Encoded Method: select Base 64 and choose Download CA Certificate link.

Microsoft Active Directory Certificate Services — wti-lab-DCWIN2022-CA

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

    Current [wti-lab-DCWIN2022-CA]

Encoding method:

- ○ DER
- ● Base 64

Install CA certificate
Download CA certificate
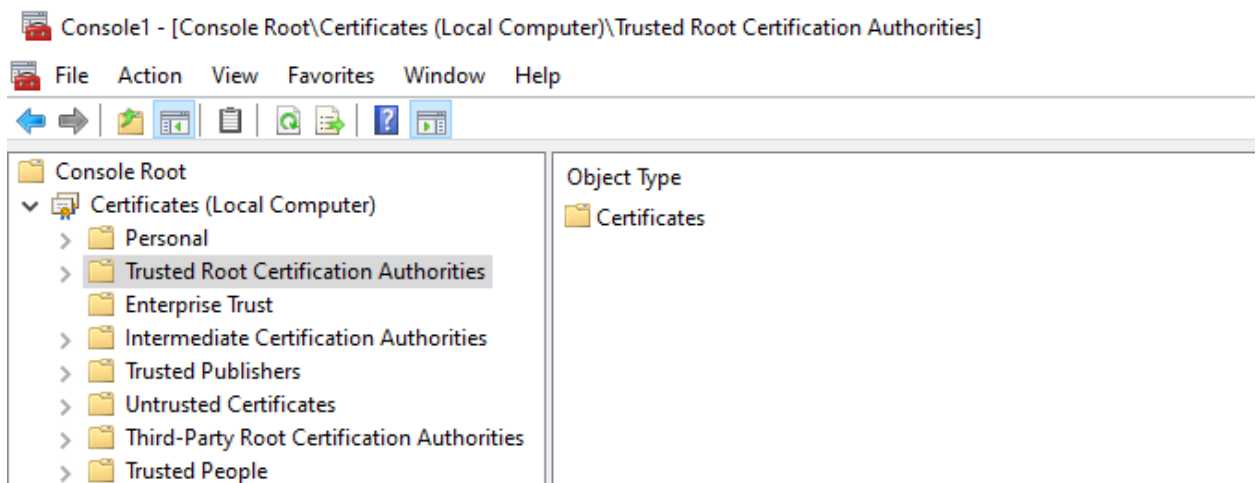Download CA certificate chain
Download latest base CRL
Download latest delta CRL

10. To import CA Certificate on Windows Machine, follow the steps below.
    - Type mmc in run windows >> File >> Add or Remove snap-ins >> certificate >> Add >> Computer Account >> Next >> Finish.

Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities]

File   Action   View   Favorites   Window   Help

Console Root
  ∨ Certificates (Local Computer)
      > Personal
      > Trusted Root Certification Authorities
        Enterprise Trust
      > Intermediate Certification Authorities
      > Trusted Publishers
      > Untrusted Certificates
      > Third-Party Root Certification Authorities
      > Trusted People

Object Type
  Certificates

11. Right-Click Trusted Root Certification Authorities >> All Task >> Import >> Next >> Browse the CA Certificate that you downloaded from step 9 >> Next >> Next >> Finish.

12. To Verify CA Certificate import successfully. Expand Trusted Root Certification Authorities >> Certificate and look for the certificate that you just imported.

13. Now access WTI from web GUI and see if the site secured.