

MSM Custom SSL Cert Using Microsoft Certificate Authority

Revisions

Date	Description
Jan 2019	Initial release

Acknowledgements

This paper was produced by the following members of the Dell EMC storage engineering team:

Author: Santosh

Table of contents

Revisions.....	2
Acknowledgements.....	2
Audience and scope	4
Prerequisites	4
Why use an SSL certificate?	4
Why use a custom certificate?	4
Custom certificate attributes	4
Generating a Certificate Signing Request (CSR)	4
Certificate signing using Microsoft Windows CA	7
Uploading cert to OpenManage Enterprise Modular	12

Audience and scope

The scope of the document is to provide a detailed procedure towards setting up a custom SSL/HTTPS certificate for Dell EMC OpenManage Enterprise Modular using Microsoft Windows Certification Authority. This white paper is intended for sale engineers, field application engineers, test engineers, architects or IT administrators who are involved in the decision-making process for the planning, configuration, and operation of a dynamic datacenter.

Prerequisites

You are expected to have working knowledge of networking, SSL, HTTP and digital certificates. This illustrates the usage of Microsoft Windows Certification Authority for the generation of custom certificate. You are expected to know the steps for accessing and logging into the Dell EMC OpenManage Enterprise Modular web console. You can find more information about how to access and login to the console using the console's user guide.

Why use an SSL certificate?

For secure HTTPS communication, the web server requires the SSL certificate on the Dell EMC OpenManage Enterprise Modular chassis. It secures data between the server and user's browser for safety.

Why use a custom certificate?

By default the console comes with a self-signed SSL/HTTPS certificate generated on the chassis. It serves the purpose of securing the communication but it shows an untrusted certificate exception in the browser.

Uploading a custom SSL certificate, signed by a trusted CA, establishes a trusted/secure client and server communication within the organization. This custom certificate fixes the untrusted certificate exception in the web browser.

Custom certificate attributes

The chassis supports a X.509 certificate with RSA 4096-bit key encryption standard and requires a web server certificate in DER Base64 encoded format.

Generating a Certificate Signing Request (CSR)

Open the OpenManage Enterprise Modular web console using <https://chassis-ip-or-fqdn> and then navigate to Application Settings -> Security -> Certificates tab.

Generating a Certificate Signing Request (CSR)

Application Settings

Network Users Security Alerts

Settings

Certificates

SSL Certificates

Issued To

Distinguished Name	localhost
Business Name	Dell Inc.
Department Name	Server Solutions
Locality	Round Rock
State	TX
Country	US
Email	support@dell.com

Issued By

Distinguished Name	localhost
Business Name	Dell Inc.
Department Name	Server Solutions
Locality	Round Rock
State	TX
Country	US
Email	support@dell.com

Valid

From	Jul 19, 2018 2:19:03 PM
To	Jul 16, 2028 2:19:03 PM

Upload

[Generate Certificate Signing Request](#)

Click [Generate Certificate Signing Request](#), provide the required information, and make sure that the Distinguished Name field contains the chassis FQDN/Hostname or localhost.localdomain if FQDN/Hostname is not set.

Generating a Certificate Signing Request (CSR)

Generate Certificate Signing Request



Enter the details and click Generate. This information will be used to generate a Certificate Signing Request.

Distinguished Name (hostName.domainName.com)	CDEV123.dell.com
Business Name	DellEMC
Department Name	ISG
Locality (Town/City)	Round Rock
State (Providence/Region)	TX
Country Code	US
Email	support@dell.com

Step 1 of 2

Generate

Cancel

Click generate, and then click Download Certificate Signing Request or Copy and/or save the text from the newly opened browser tab or window.

Certificate signing using Microsoft Windows CA

Certificate Signing Request

Copy the text below and submit it to a certificate authority to receive a valid SSL certificate.



Download Certificate Signing Request

```
-----BEGIN CERTIFICATE REQUEST-----
MIIE/zCCAucCAQAwYsxCzAJBgNVBAYTAiVTMQswCQYDVQQIDAJUWDETMBEGA1UE
BwwKUm91bmQgUm9jazEQMA4GA1UECgwHRGVsbEVNqzEMMAoGA1UECwwDSVNHMRkw
FwYDVQQDDDBDEREVWMTizLmRlbGwuY29tMR8wHQYJKoZIhvcNAQkBFhBzdXBwb3J0
QGRlbgwY29tMIIiCljANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAWGPq6RQ0
QouGmhkKHcgDL7ea75l+cmRm+MaDnK/IRtZwnlZHEliE3eFRV5eldcv74uw/PpeM
uw0bbv2Dy68Fpg//bM5yLQyLx++s54gXsNn7oL4aG3IK7+BtH1Lt2xuudSmNARDB
ZuYVwZ8ttWizvFGWKMMqZWjdUbjCAWaoJOy4LA/4g3vTxv18WT3jnZ+XOUF8STkJ
VYd0c5Pj/7B9z3g2uM1knh7d1Zu2BBjnx8f4fKDXstMtbHyDI0oLwkuJBX4frpQ
bujicPg3mFDubJCK5ihp4UeUofhKWP/kUPQ4GtKk4hZph/UHkjBMgDsJui7WetRl
eivhO9zX5JzflVFpyvz/99bBX718m3qkmzrQ+ORU6UboPNPvVa9ZJY2eFWnjUKAM
5PMiKDQ6ZV7ptXsBgal/7pV09WpC8N0+YFISw5GFmRqdQOLB9EXhSI4WHHvZ62mj
yibXEm9qt4hvBSdmhHMCGmmaGteYU2UujqAqHBQRGnfwiZ4kzE1QfONAVHGNQ8Cy
vJim6A1vnyHyxJT9nY+zyWmcyjAczYqu3XqUwt8KNIHUELmQw7eamR/LvTFXd63M
kTkbyOhONERRJCheerImAALgWvjCMrgSguNOMNwWnXWA1uPULmY3RXKt1PgAjEYS
YCi4UFF+ccqfG0vkfTA7oFQ3P9u7vQh+mghMCAwEAaAuMCwGCSqGSIb3DQEJJDJf
MB0wGwYDVR0RBQQwEoIQ0RfVjEyMy5kZWxsLmNvbTANBgkqhkiG9w0BAQsFAAOC
AgEAe7vdApj6iK+CxWNDg/rfzL/pwFZms2V0cFnJnPKl2549jY+aFhvRiz08jKwx
x/UhBT/fk3xcwDTkzrJGQz6/zGKfHLNhwU9eVPOQ8135tRjt4jrwWzJ520iTFst
ddkKFTBhlcQaSyhWDqu4n9NHpt5VQmCdIW+ihjYgHzHkprHcqCAAsniHsfrVp09xO
rJ8FRZXWsoeW6NTD0o3hjHBBYUmpEpdHb8k41jVsKtka6o9JZpmoxlFQlyyEkCoE
w3cCBx660VNbcjufKEw7+m3qgof2h+F9msy9OM+QrifYb/4wdyp3vNHrvzECU9gs
J29OP9cjc/xs/3zOzfJoaKK/aDJ0fEE/NG309ePdtjBuMPmwoZUOWqzhirqFNGx2
jbdHxtjtqGv0ieNxlZwblDhy4o6GSfxqW5mUnJha5QJuC6pBdntYaKsAIQijlj+
jZZ6wK1xe0HbaUdXE0eljWLLhAef646r8NOTeX7sGtKFYsn14NHRsAK+67ysR6Ct
42fb1TCpsD96Cd3XlJh4k7GgFM3VjV2yfyCLinpJQxuvCqnxfk+F8sdrkRkNm2Nh
2y7EcTc9JZvAtahmino7mM9vEf/6lRyoP6Vbor4M7wjAtZollB4jUMFEOWTryzW
EqONT9G3k8cLG/cTWsICYYArXA2BLoAT/fjbKqWhITH4yUI=
-----END CERTIFICATE REQUEST-----
```

Step 2 of 2

Previous

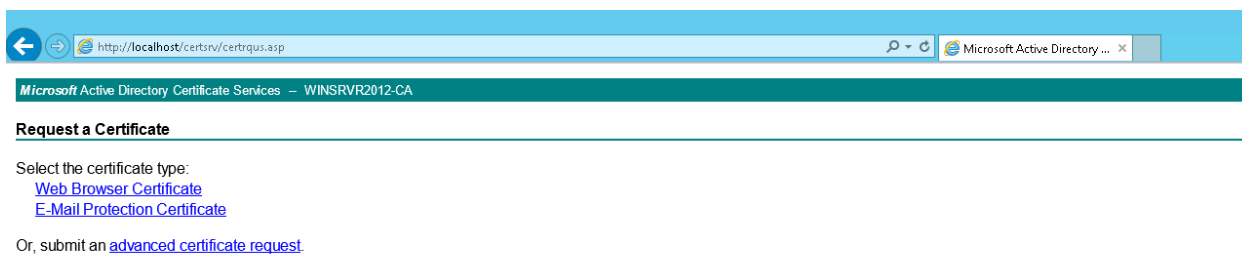
Finish

Certificate signing using Microsoft Windows CA

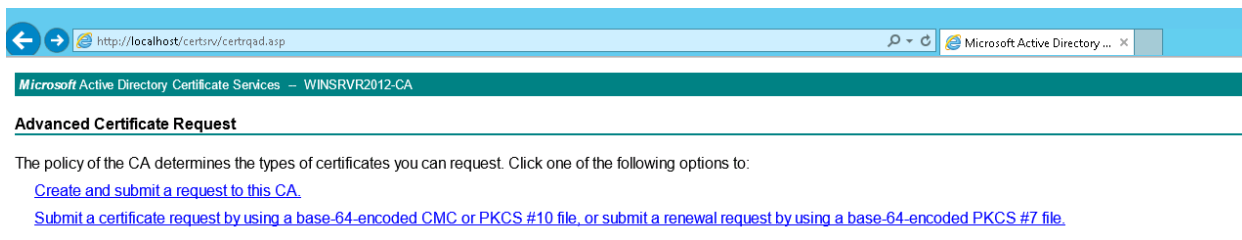
This section shows you how to digitally sign a CSR generated using Microsoft Windows Certification Authority. This section assumes that the certification authority server has already been configured.

Open the certification authority portal page in the web browser by using <http://certificateauthority-ad/certsrv>. Click certificate request and then advanced certificate request.

Certificate signing using Microsoft Windows CA



Then click the Submit a certificate request by using a base-64-encoded CMC or PKCS#10 file.



Copy and paste the contents of the CSR either by opening the downloaded CSR file or paste the already copied text into the Saved Request text area. Make sure that the BEGIN and END certificate REQUEST tags are present in the text and there are not trailing spaces in the text.

Certificate signing using Microsoft Windows CA

The screenshot shows a web browser window with the address bar containing `http://localhost/certsrv/certreq.asp`. The page title is "Microsoft Active Directory Certificate Services - WINSRV2012-CA". The main heading is "Submit a Certificate Request or Renewal Request". Below this, a paragraph explains that users can submit a saved request to the CA by pasting a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request. A section titled "Saved Request:" contains a text area with the following content:

```
jbdHxtjtq9v0ie2Nx1Zwb1dhy4o6GSFxdW5mUnJh  
jZ26wK1xe0HbaUdXE0e1jWLLhAef646r8NOIeX7s  
42fb1TCpeD96Cd3X1Jh4k7GgFM3VjV2yFyCLInpJ  
2y7EcTc9JzvAtahmino7mM9vEf/6lRyoP6Vbor4  
EqONT963k0LG/cIW8ICYArXA2BL0AT/fjbKqWh  
-----END CERTIFICATE REQUEST-----
```

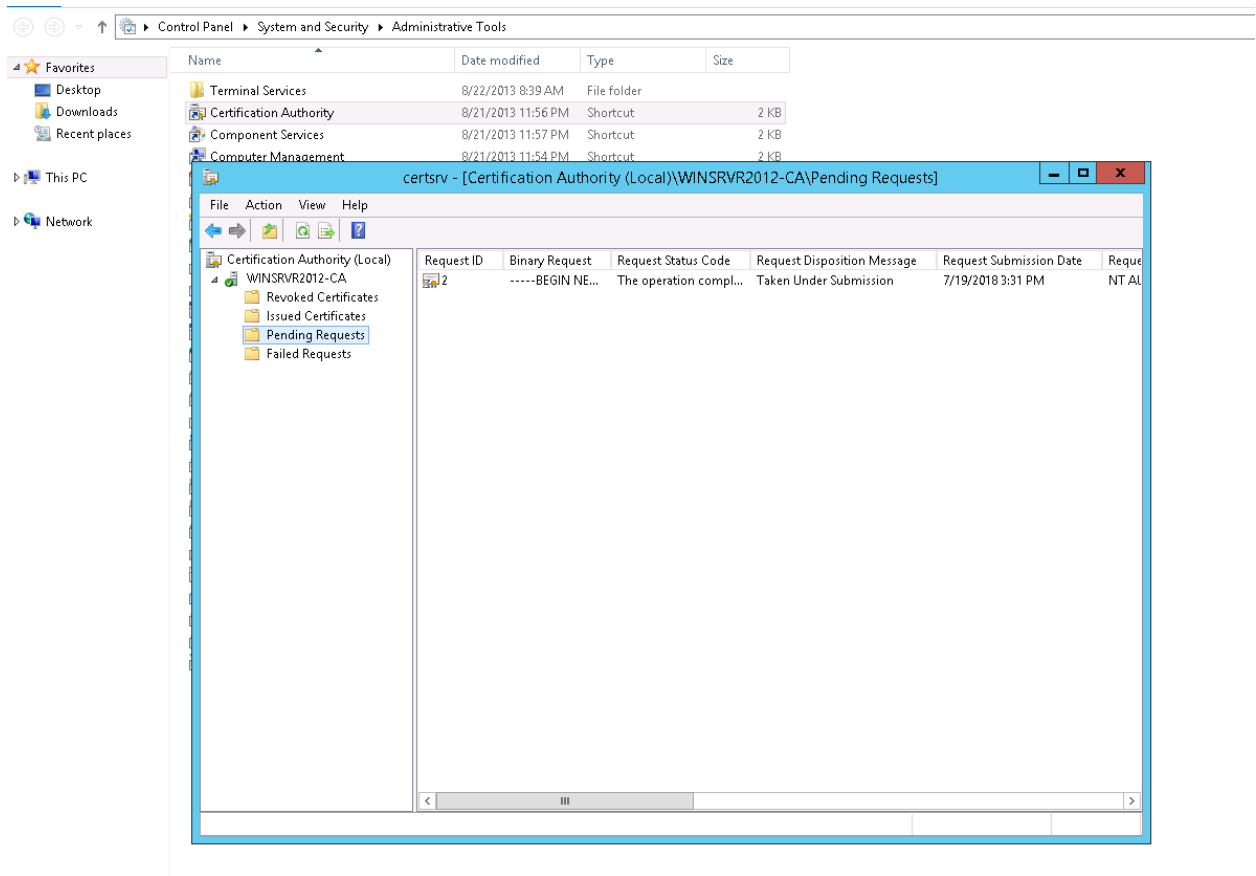
Below the text area is an "Additional Attributes:" section with a label "Attributes:" and a text input field. At the bottom right of the form is a "Submit >" button.

Submit the certificate signing request using the Submit button. The Certificate Authority portal will show a pending certificate id on the next page.

The screenshot shows a web browser window with the address bar containing `http://localhost/certsrv/certifnsh.asp`. The page title is "Microsoft Active Directory Certificate Services - WINSRV2012-CA". The main heading is "Certificate Pending". Below this, a paragraph states: "Your certificate request has been received. However, you must wait for an administrator to issue the certificate you requested." Another paragraph says: "Your Request Id is 2." A third paragraph says: "Please return to this web site in a day or two to retrieve your certificate." A "Note:" section at the bottom states: "You must return with this web browser within 10 days to retrieve your certificate".

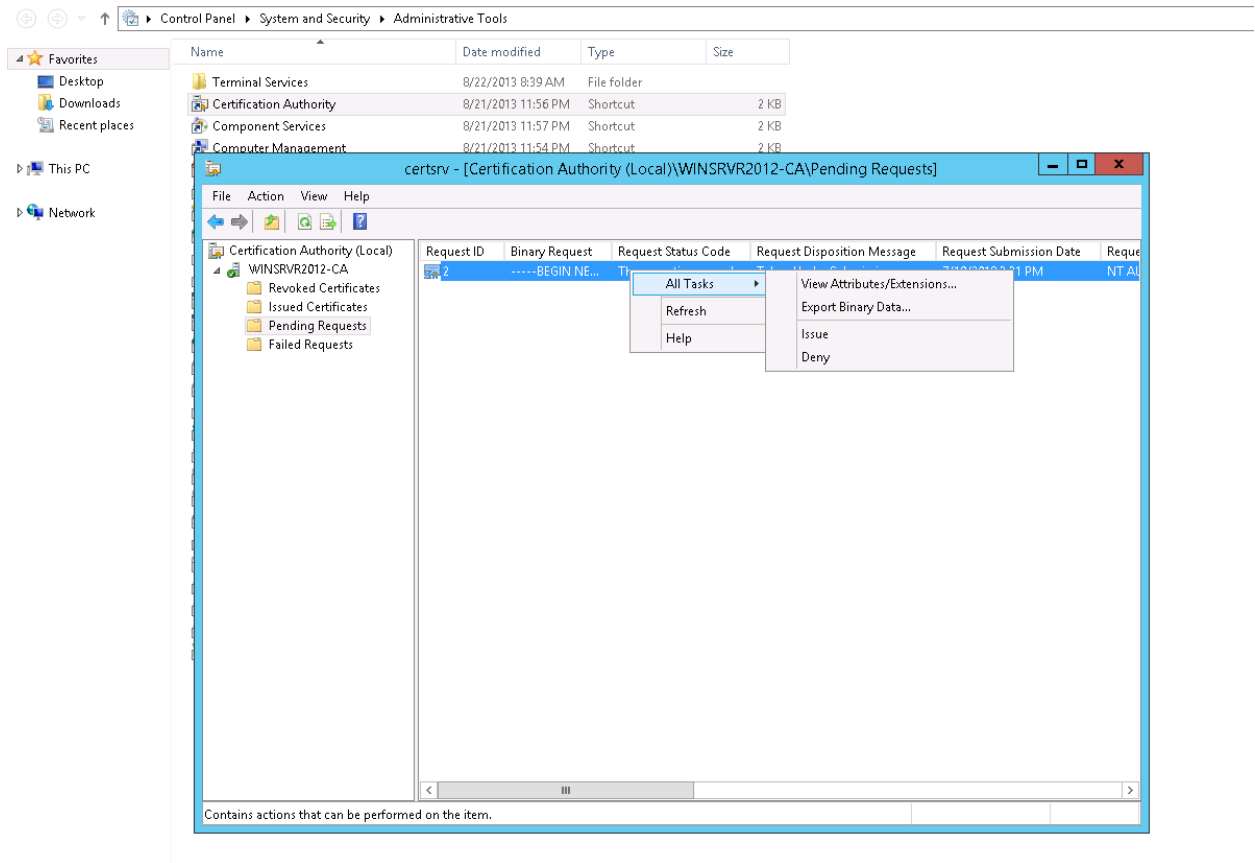
On the Certification Authority server, open the Certification Authority snapshot from Administrative Tools and go to pending requests.

Certificate signing using Microsoft Windows CA



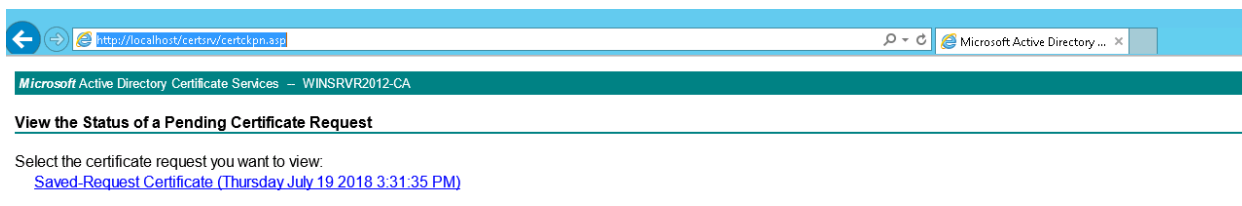
Right-click the pending certificate for the id generated before. On the context menu click All Tasks and Issue the certificate.

Certificate signing using Microsoft Windows CA

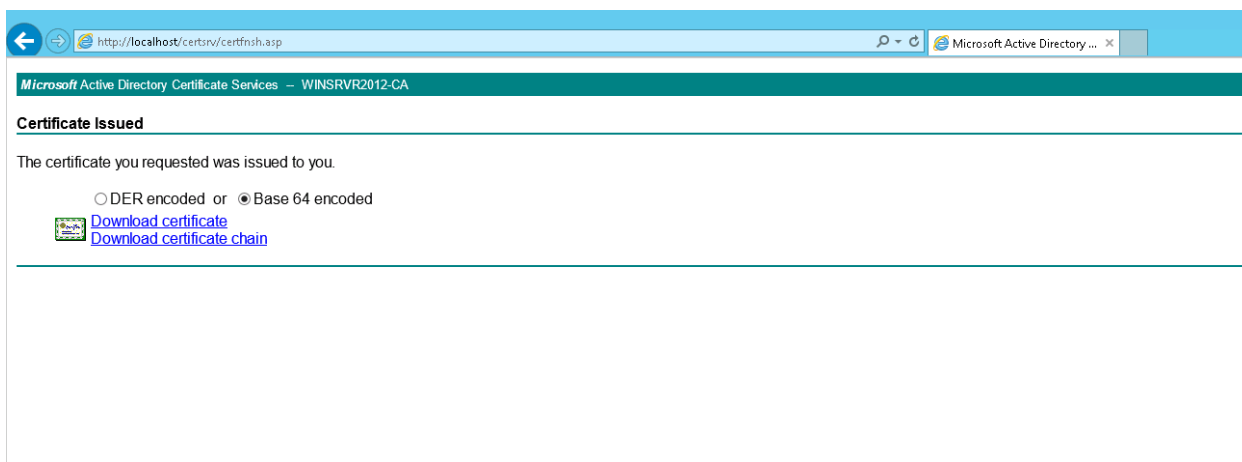


Open the Certification Authority portal page and go to View the status of a pending certificate request.

Uploading cert to OpenManage Enterprise Modular



Click on the saved certificate request and download the certificate and Base 64 encoded file on the disk using the Download certificate link.

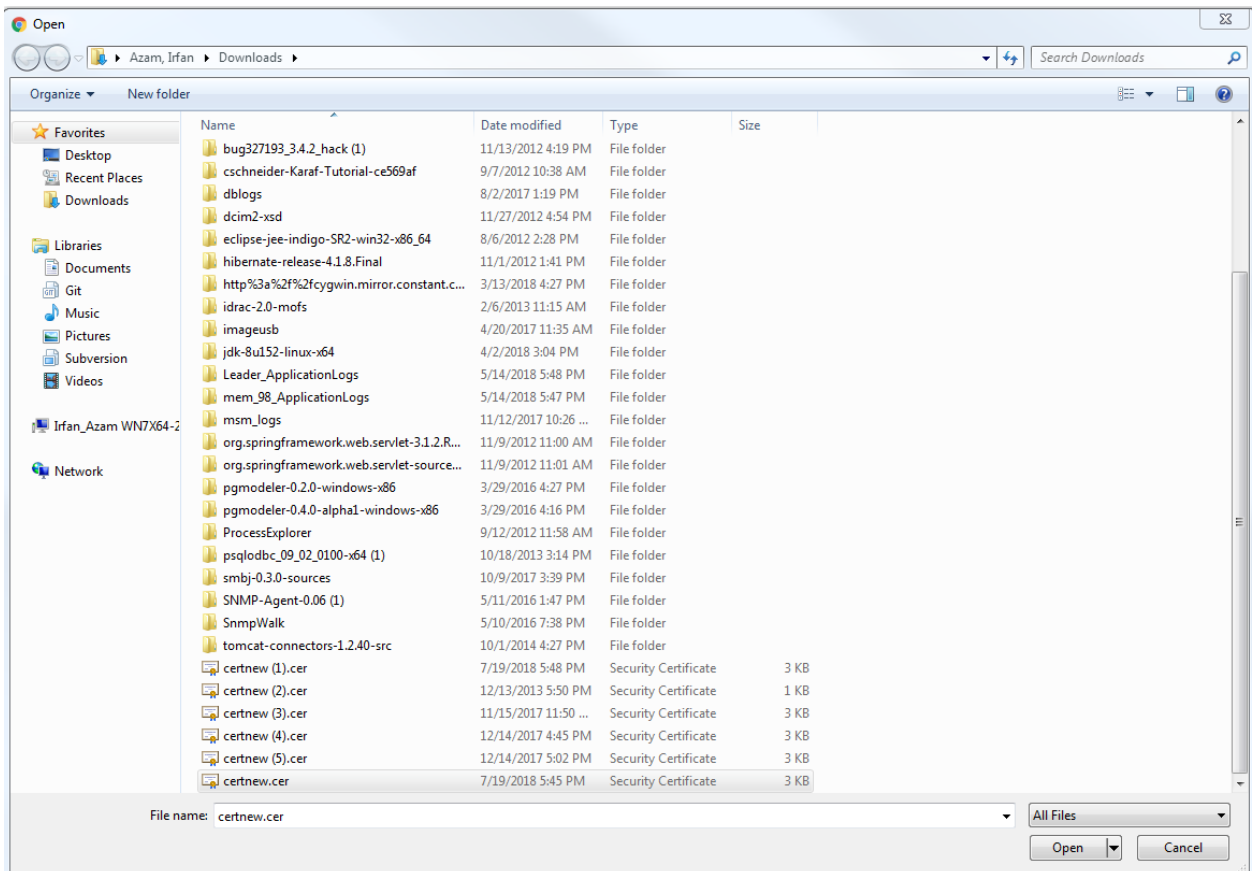


Uploading cert to OpenManage Enterprise Modular

Open the management console and go to Application Settings -> Security -> Certificates tab.

Click upload and browse the saved certificate to upload the certificate.

Uploading cert to OpenManage Enterprise Modular



MSM will logoff and show an info message about certificate upload success.