MSM Custom SSL Cert Using Microsoft Certificate Authority

Dell EMC Technical White Paper

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

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.

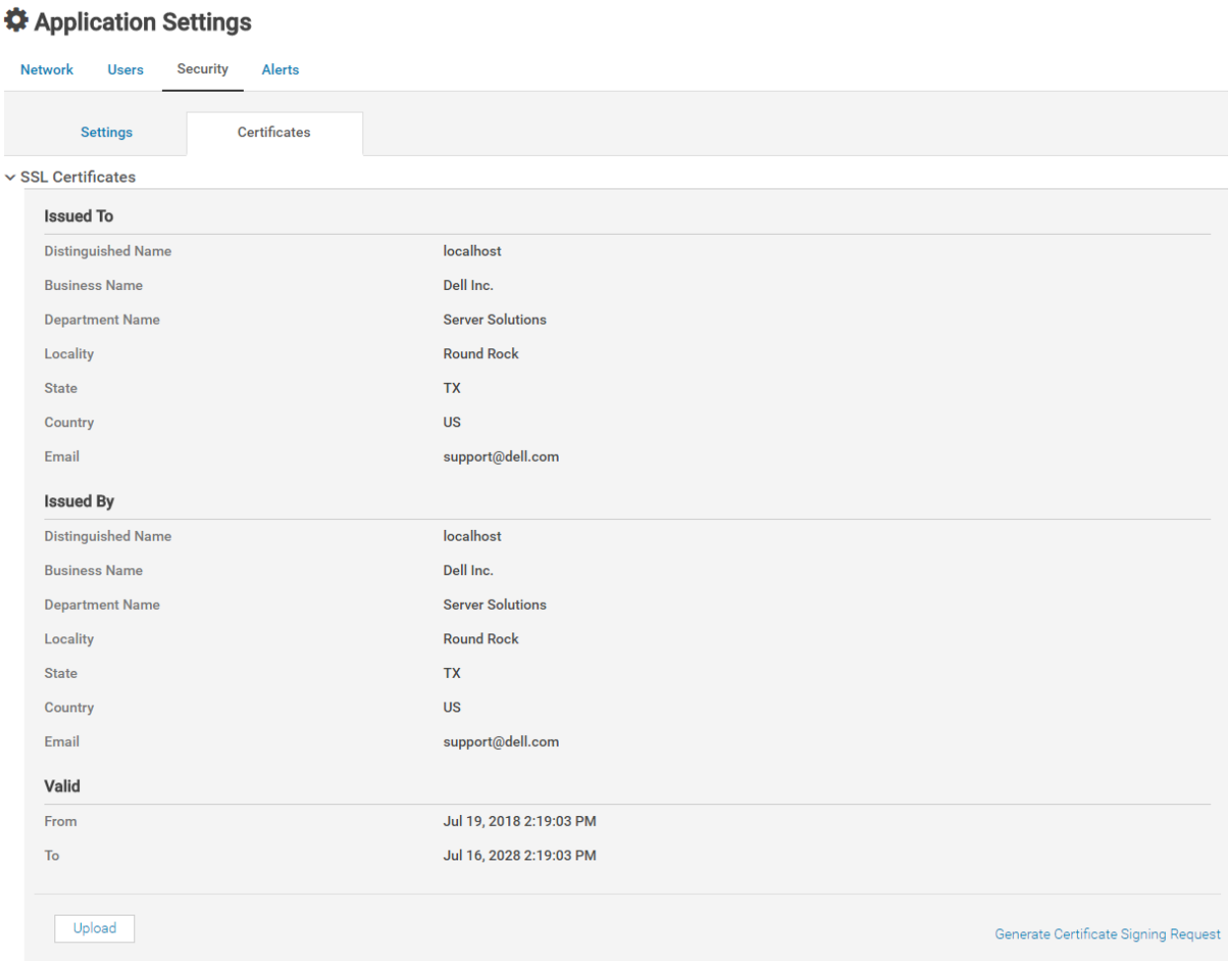
Uploading a custom SSL certificate, signed by a trusted CA, establishes a trusted/secure client and server communication within the organization. This custom certificate fixes the untrusted certificate exception in the web browser.

Custom certificate attributes

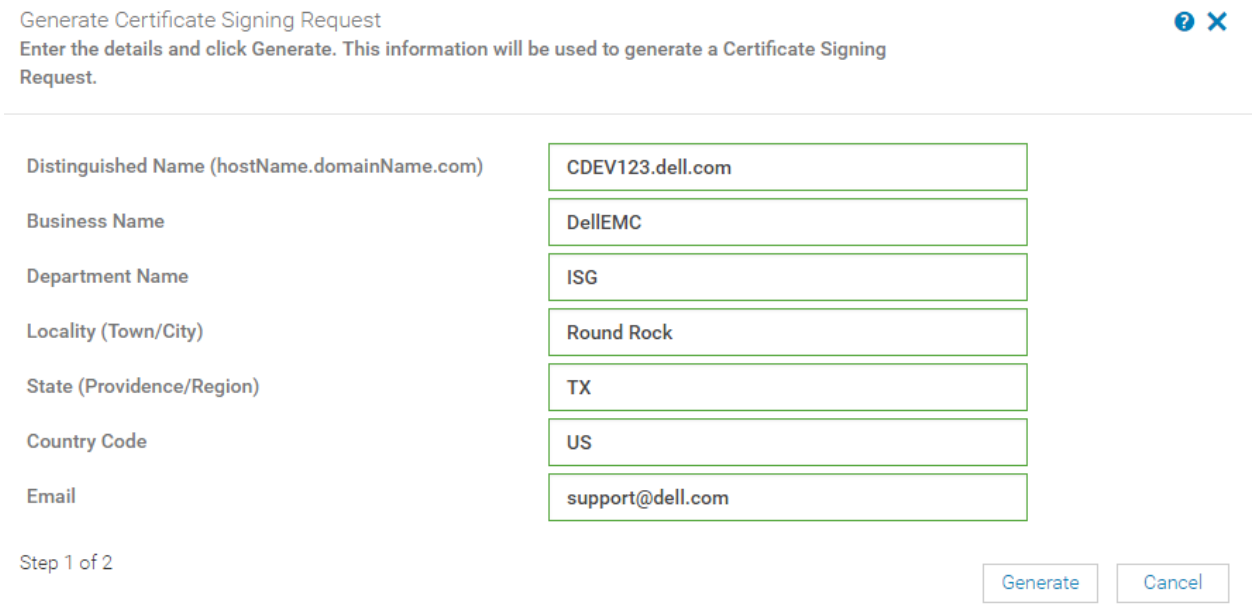
The chassis supports a X.509 certificate with RSA 4096-bit key encryption standard and requires a web server certificate in DER Base64 encoded format.

Generating a Certificate Signing Request (CSR)

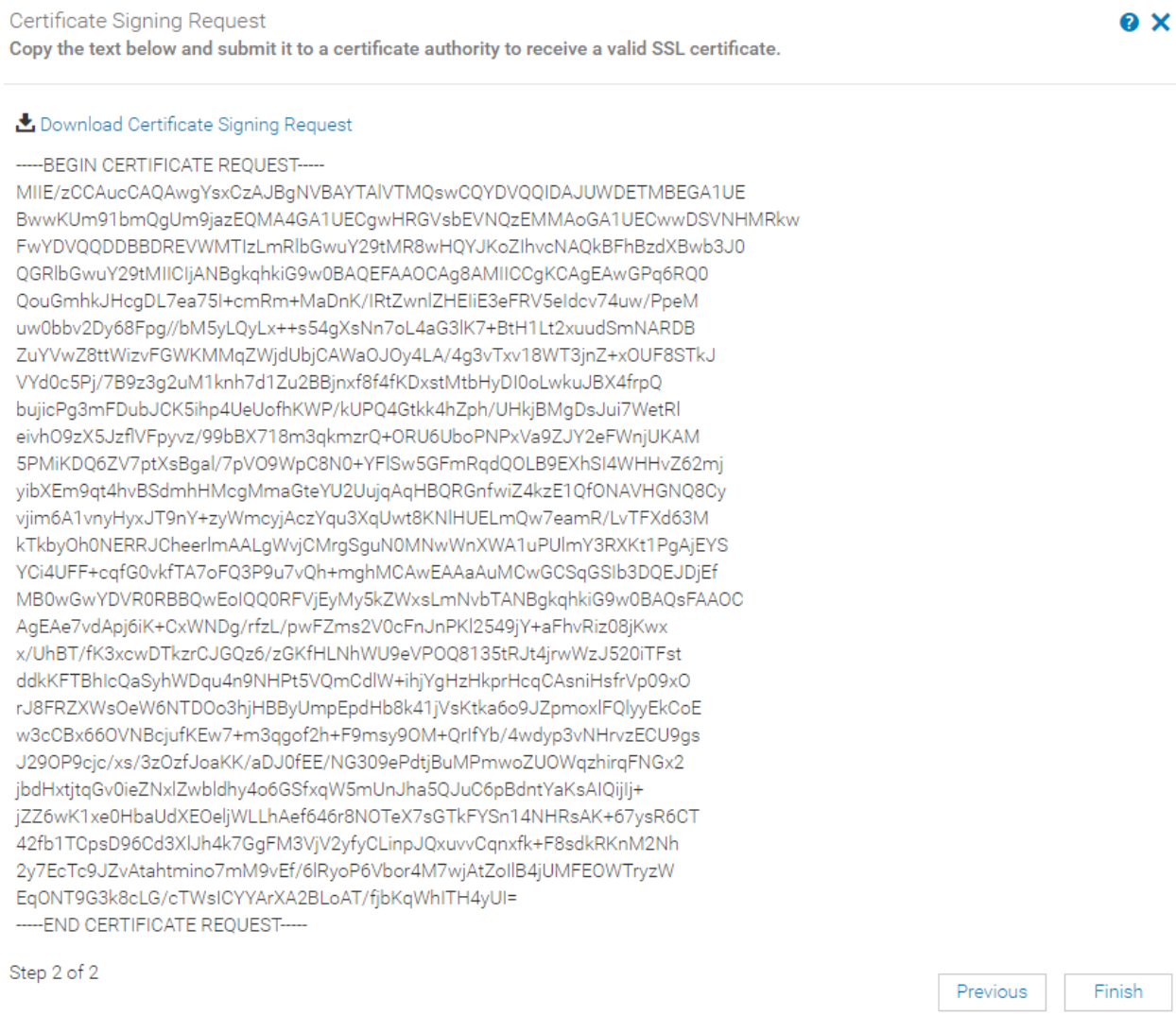
Open the OpenManage Enterprise Modular web console using https://chassis-ip-or-fqdn and then navigate to Application Settings -> Security -> Certificates tab.



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.



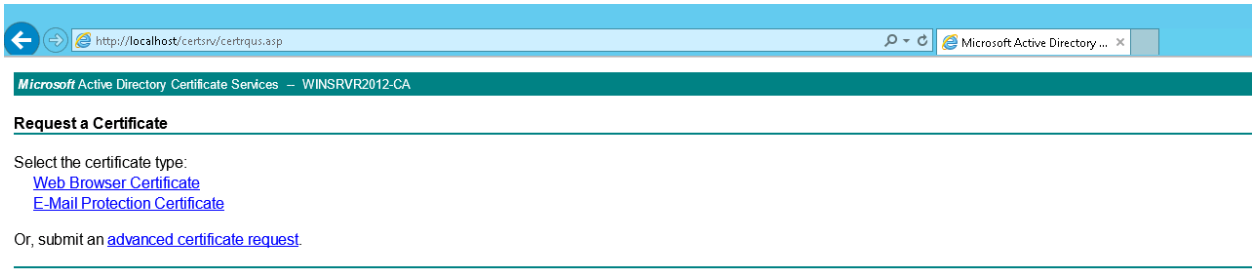
Click generate, and then click Download Certificate Signing Request or Copy and/or save the text from the newly opened browser tab or window.



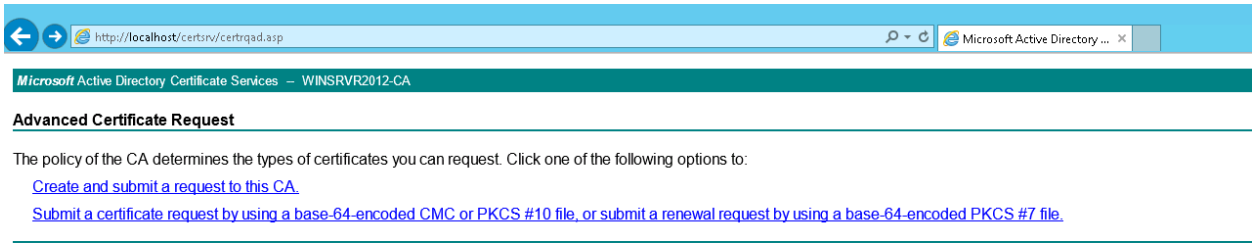
Certificate signing using Microsoft Windows CA

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.

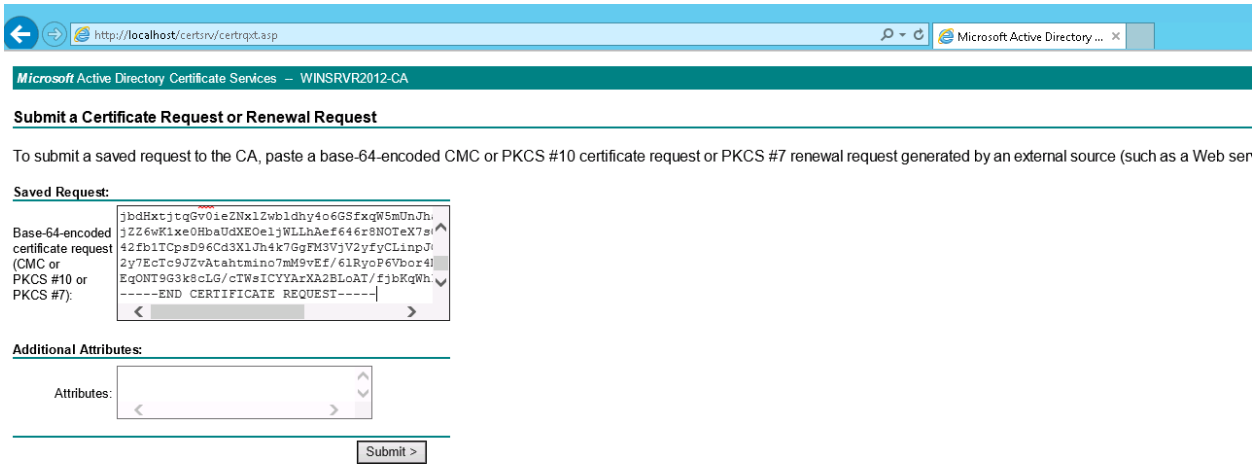
Open the certification authority portal page in the web browser by using http://certificateauthority-ad/certsrv. Click certificate request and then advanced certificate request.



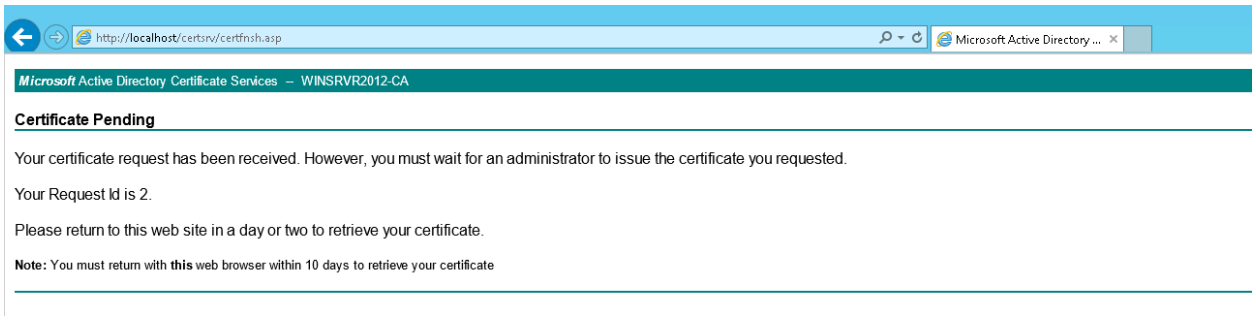
Then click the Submit a certificate request by using a base-64-encoded CMC or PKCS#10 file.



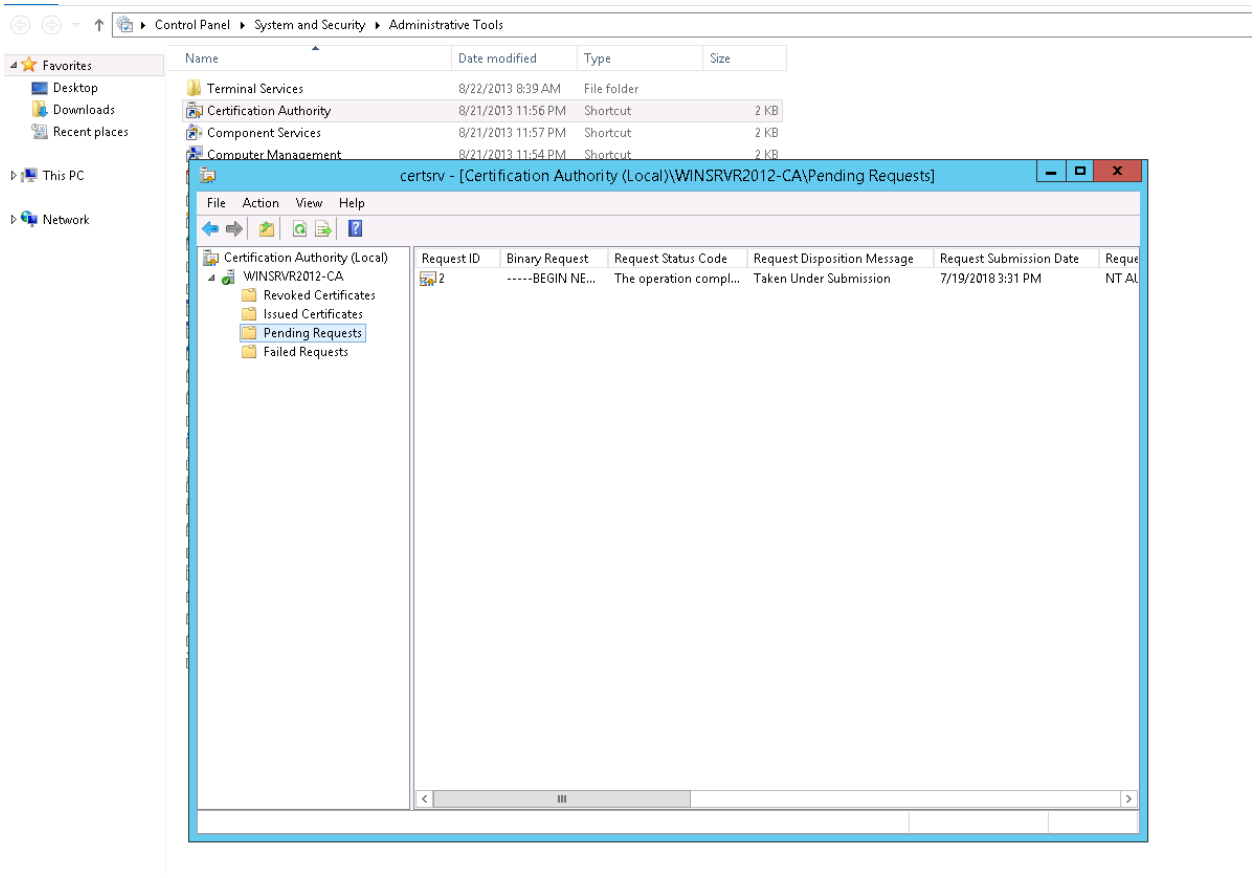
Copy and paste the contents of the CSR either by opening the downloaded CSR file or paste the already copied text into the Saved Request text area. Make sure that the BEGIN and END certificate REQUEST tags are present in the text and there are not trailing spaces in the text.



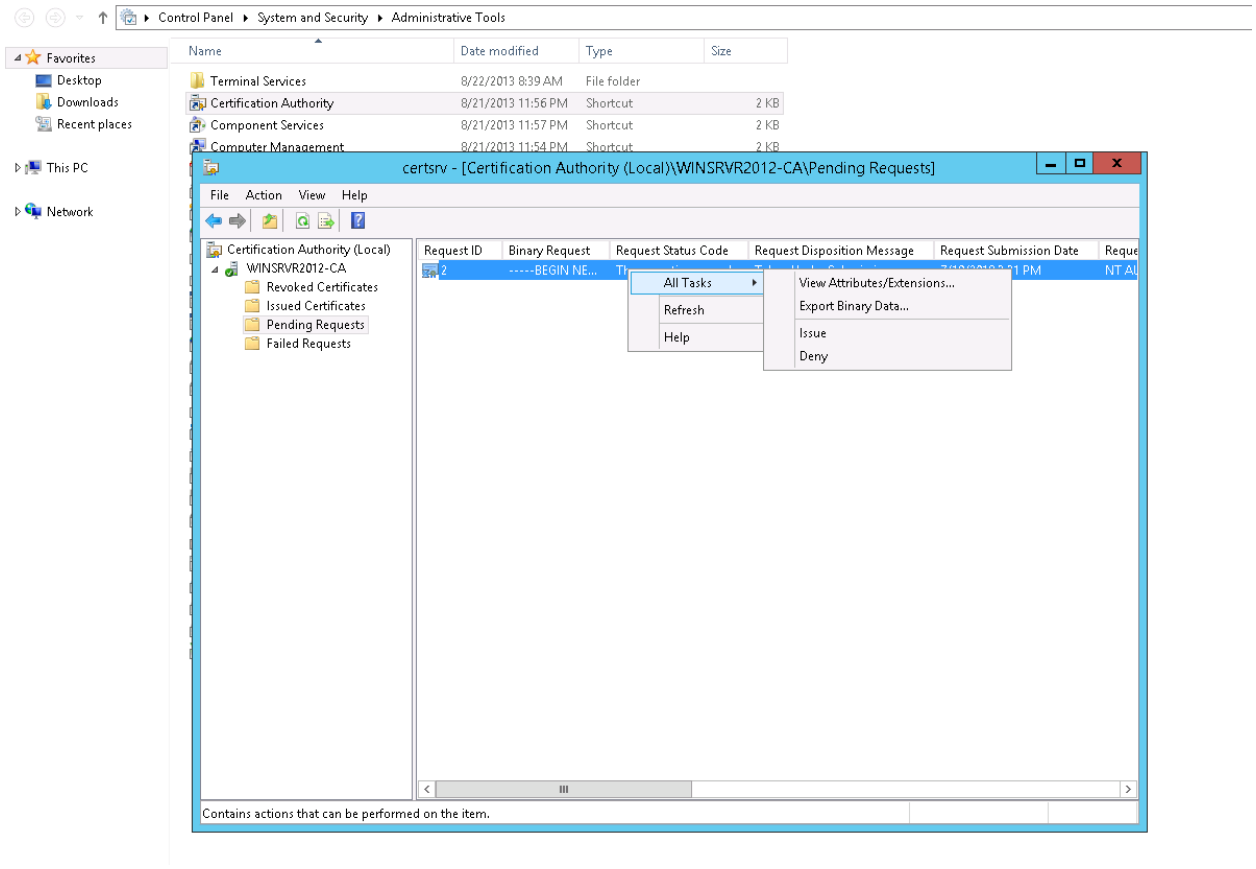
Submit the certificate signing request using the Submit button. The Certificate Authority portal will show a pending certificate id on the next page.



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

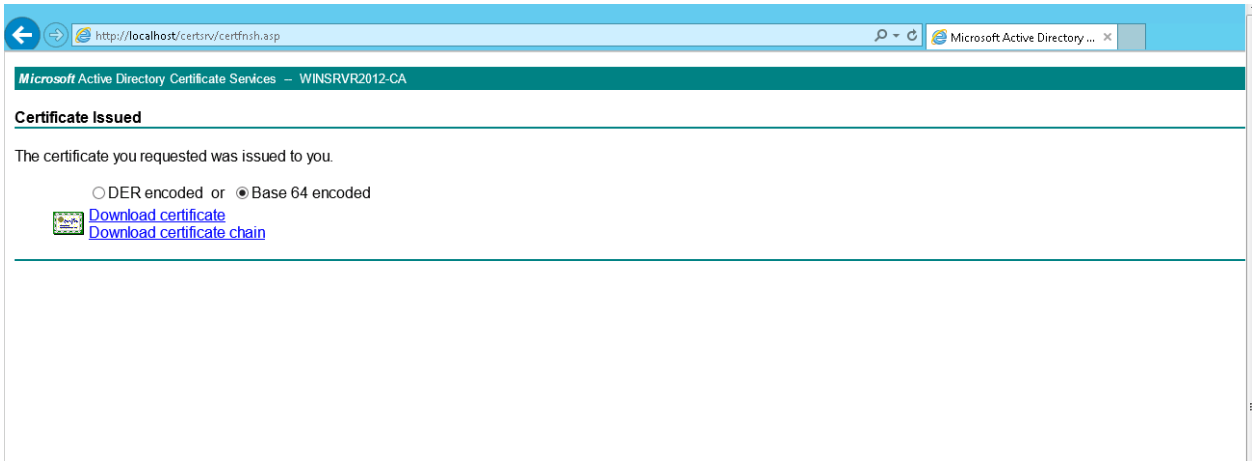


Right-click the pending certificate for the id generated before. On the context menu click All Tasks and Issue the certificate.



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

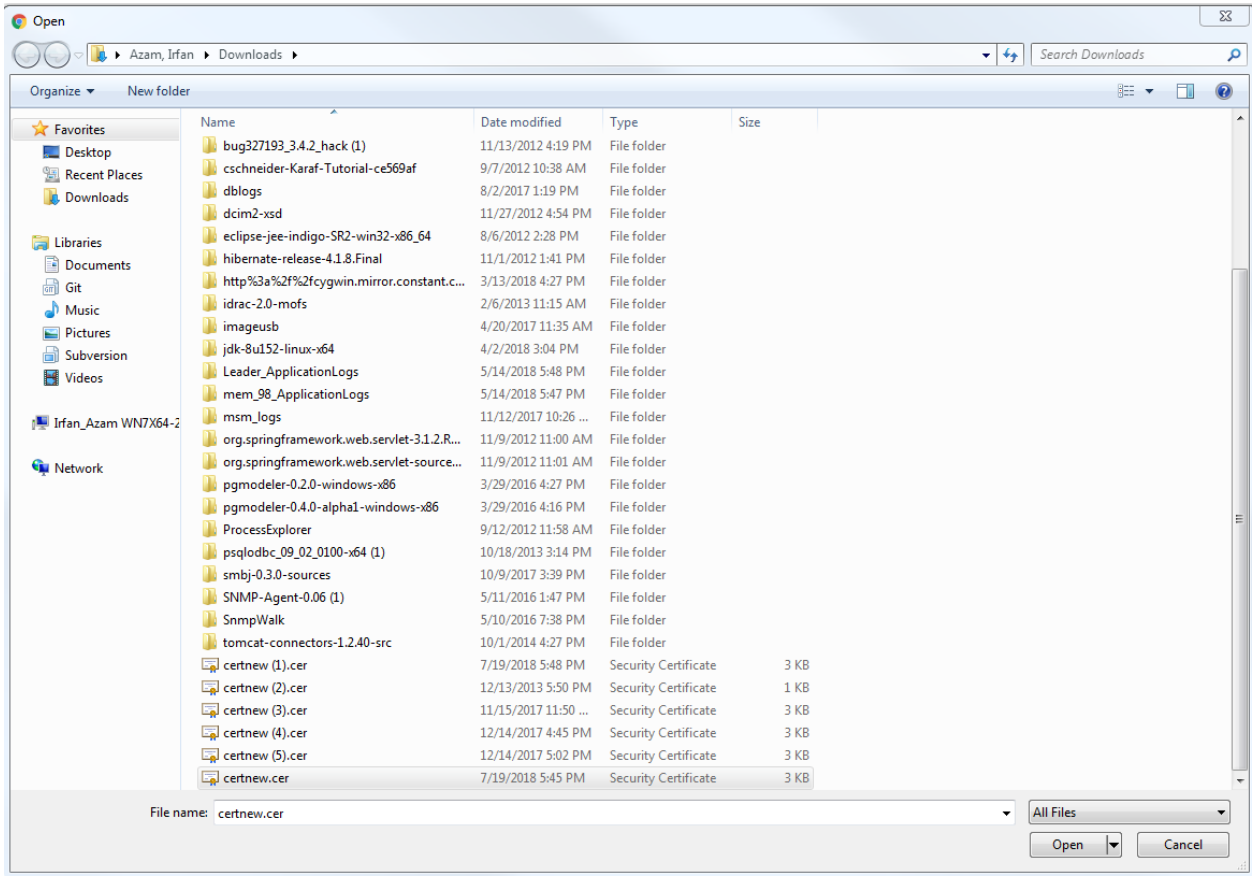
Click on the saved certificate request and download the certificate and Base 64 encoded file on the disk using the Download certificate link.



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.



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