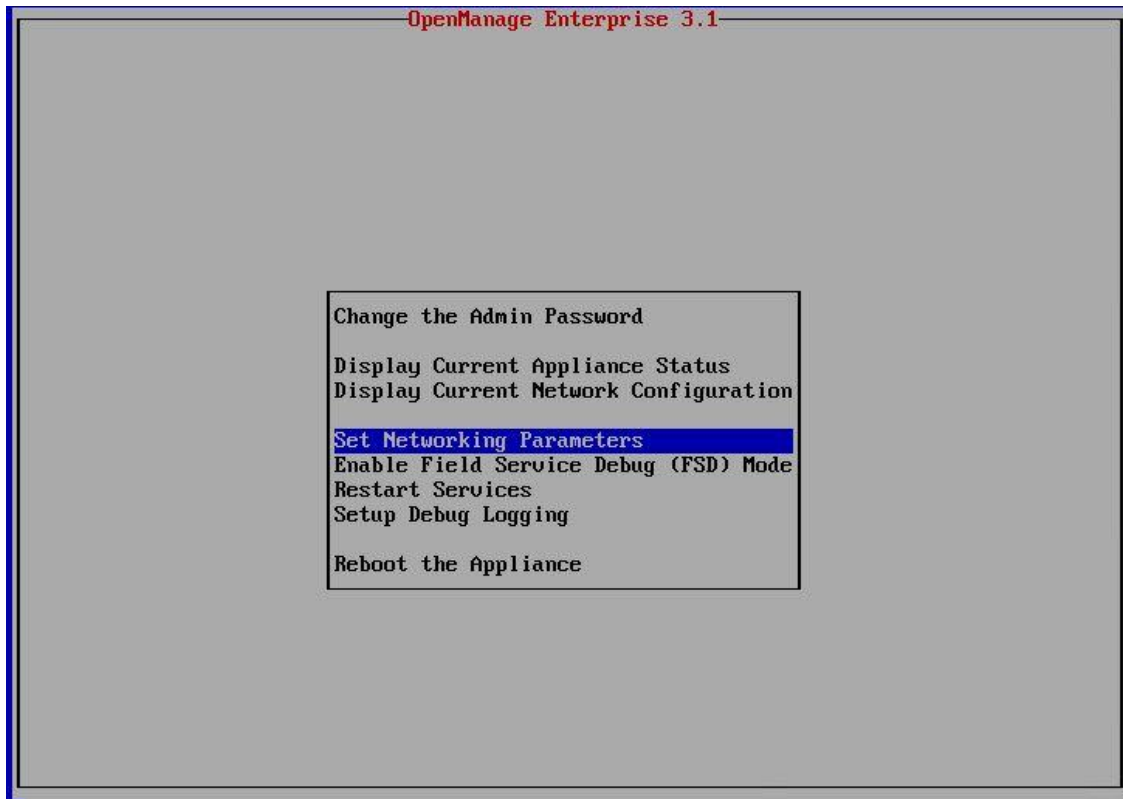
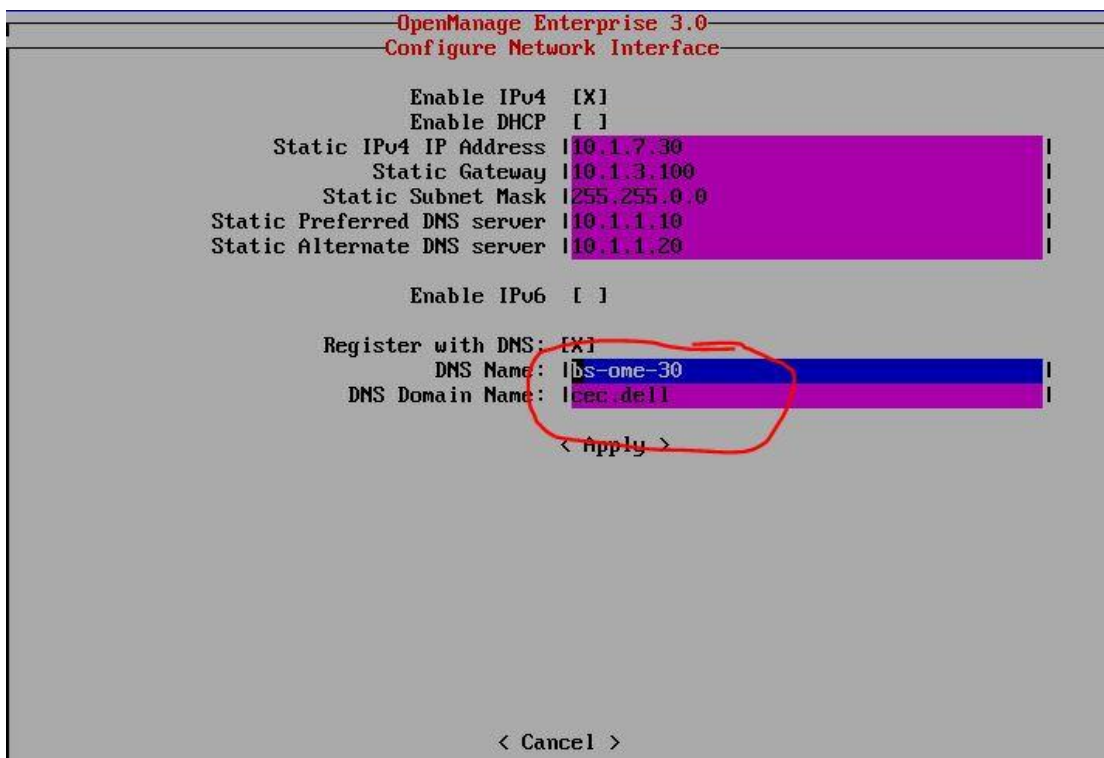


# Assigning a Openmanage Enterprise Webserver Certificate with Microsoft Certificate Server

Open the OM Enterprise Console and go "Set Networking Parameters



Verify / change DNS Name and DNS Domain Name and apply



Open the Web Gui, and go to application Settings -> Security -> Certificates

! Note your distinguished name is filled with you FQDN

Now choose generate Certificate Signing Request

The screenshot shows the OpenManage Enterprise web interface. The breadcrumb navigation is 'Application Settings' > 'Security' > 'Certificates'. The 'Issued To' section is highlighted with a yellow circle, showing the distinguished name 'bs-ome-30.cec.dell'. The 'Generate Certificate Signing Request' button is highlighted with a yellow box and a red 'L' mark.

Issued To	
Distinguished Name	bs-ome-30.cec.dell
Business Name	Dell Inc.
Department Name	Server Solutions
Locality	Round Rock
State	TX
Country	US
Email	support@dell.com

Issued By	
Distinguished Name	bs-ome-30.cec.dell
Business Name	Dell Inc.
Department Name	Server Solutions
Locality	Round Rock
State	TX
Country	US
Email	support@dell.com

Valid	
From	Jan 17, 2019 2:52:12 PM
To	Jan 14, 2029 2:52:12 PM

Fill in the Fields. ! Use the proper FQDN

The screenshot shows the 'Generate Certificate Signing Request' form. The form fields are filled with the following values:

Distinguished Name (hostName.domainName.com)	bs-ome-30.cec.dell
Business Name	Dell CSC
Department Name	OSE
Locality (Town/City)	Frankfurt
State (Providence/Region)	Hessen
Country Code	DE
Email	administrator@cec.dell

Step 1 of 2

Generate Cancel

## Download or copy the content including --- Begin -> xx <- --- End

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-----
MIIFDT0CAvUQAQAwZcxOZAJBgNVBAYTAkRFMQ8wDQYDVQQIDAZlZXNzZW4xZjEQAQ
BgNVBAcMCMUyZyY5W5rZnVydDERMA8GA1UECgwIRGVsbCBDU0MxDDAKBgNVBAsMA09T
RTebMBkGA1UEAwwSYnMtb21lTmwlMnNlYy5kZWxsMSUwLWlwYjkoZlhcNAQkBFhZh
ZG1pbmRzdHJhdG9yQGNNYy5kZWxsMII0IjANBgkqhkiG9w0BAQEFAAOCBg8AMIIC
GgKCAQEAshPRRvPvNkd7IMD9xUdGuz3uP2tomWlIRFjk4Fv9QTfQCNg+7ebf86x
eDFcdUWIR2nnsz5NwPvqAG9qxFVs/TEBv8XFISA0UMZtBFDJicforWjgsr19Q/a
Jsd9t476andMrtFq/1anPrMCsIOvplOdJe5y0Pk20C1zMwQvtpS8GksGxa4aT
72pXAE6RhGmf1T+PkuOZGr5K1Z4q2NRpxDKEBRfBUJ82dl7qWS9hTV7dW+gKfl.
uCNzUUVzKnuffRz1ps10KQdy5Eo8n6A+C579Kel6t7v/OvYrzPSuP089Xfw4Jk1
SDPVOQZAS8EYtQpoOp2B5XD5NzaaeLdvpMPC40mU1Sw2W9mflw72LcPL0eL5FbJEr
9LaO7sZBz3oPplLlvcagK68G19A7XNApc0uoCbtTsdCuoj59rEbyYVCJ34bmAK7
tUlu9uHI/FeZJMYxu8wP9yh5wKajpBhx9UxvctGXNzS3FAGN2JTQ9W3FIF1NnA
2YqOzQ9iyUzyinMNM8pjm8Cy3DE9zo+HFwfpccQ4PlkqbrLFusLBS0NhnLmeGB
eeq8AUJ4TEVewR/SUae5GGjHXKAibMQ4itGkkX+7cLTKGaphv74b60jQ5uTbx86
nns7FNIG0ooeclogQqazsSibCntCkME8+g6ZYwSW9ER4aOcx5ECAwEAAAwMC4G
CSqGSIb3DQEJDIjEhMB8wHQYDVR0RBBywFIIISYnMtb21lTmwlMnNlYy5kZWxsMAQG
CSqGSIb3DQEBChUA4ICAQA52v2PGkE/ADsqcuK0YwpoK6s1P3p/vfaaXowQk6qQ
4PNzIhgXRbZHZKcByeGEaWEX/pdNvO5Ur3rb2eHIL3cSBOPsX8YM+Ot8/veyfv
Tul5wPbzJnZ9vM+OpOy6HlhtBSI83qXyarnZjh6rxs9u75uJXx6ZsH0lrWsAjrxM
AsL1ALiSZk11tdv9+u/9PwpOsc1ouomhdnffKKGQu0WKQ0q9fofY19ywlJ8V1Qak
u1XwzDHtjUjG8zBlhDkAM8YARZoNXkhvXQsqf8fWuD2hLpcqmqHBLINGJYR16G
qnDnE+VelI9VJfAEZQoQEsj4YmTOtJr6YOnzUvRrdDHC7mqK1Ap6wLgEOTA2DA/zw
8pg8kZLh07+VRzhHRALNOr2cGuT5SABmbq2uAAvK6lqAPGv0nc8xWYT6/jbvmAU
lWn8nGnyHLSO3J2+M3GHoaWR//6rNYyqmvrmrL+zo8nf01Ttwi8l9778HFcSqJeE
jTK7vDX3iu0Tx9oc+cGu7LFVizgBzD4dc7LLB3hlnTAVSVa9aFlavJSBOHFEjppj
lWmQ59rb9xbS5qQvoOap0b+Wbo3LqmrIprnGmyQ5QksrZXOy3VQqVvdi0jOO+Y
2Y/c2/BNls/ToVEbtCrw1qoR2B2r9tSetED/c6JHDoj3SrzyFY7N0lHnofYQaTI
Ug==
-----END CERTIFICATE REQUEST-----
```

Step 2 of 2

Previous

Finish

## Open a Web session to you Certification Server (https://x.x.x.x/certsrv) Request a Certificate

Microsoft Active Directory Certificate Services - cec-M520-W2012-DC1-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 Web, sign and encrypt messages, and, depending upon the type of certificate you 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

## Choose "advanced cert..."

Microsoft Active Directory Certificate Services – cec-M520-W2012-DC1-CA

### Request a Certificate

Select the certificate type:  
[User Certificate](#)

Or, submit an **advanced certificate request**.

## Submit a cert .....

Microsoft Active Directory Certificate Services – cec-M520-W2012-DC1-CA

### 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.**

## Past the content from the file or buffer in the filed

## Don't miss to change to "Weber Server" and submit

Microsoft Active Directory Certificate Services – cec-M520-W2012-DC1-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 PKCS #7 Web server) in the Saved Request box.

**Saved Request:**

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

```
JjGN0TfWk+yD9uxrrOcNttWfN11qShMeaL5hja9R:  
otPNUm6MsS7DQE1gD9NHCw9CSNGP0tDIHRR1C79K:  
ck6NfuqcsbqXrAZDvkOEmZtonxYC1X4SyP141Tqc-  
8LnMcuikYFsvATFwYH2kF9f8sW3etShXRvohcUmi  
IQ==  
-----END CERTIFICATE REQUEST-----
```

**Certificate Template:**

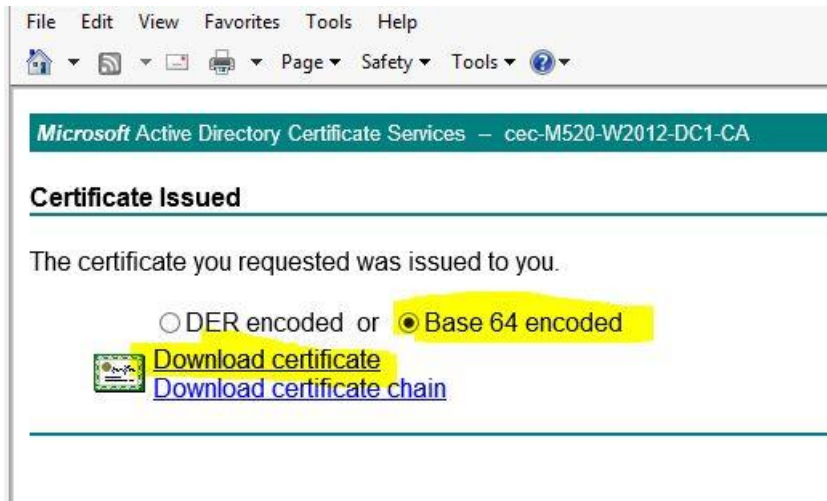
2 → **Web Server**

**Additional Attributes:**

Attributes:

3 → **Submit >**

## Select Base 64 Encoded and download certificate




File Edit View Favorites Tools Help

Microsoft Active Directory Certificate Services – cec-M520-W2012-DC1-CA

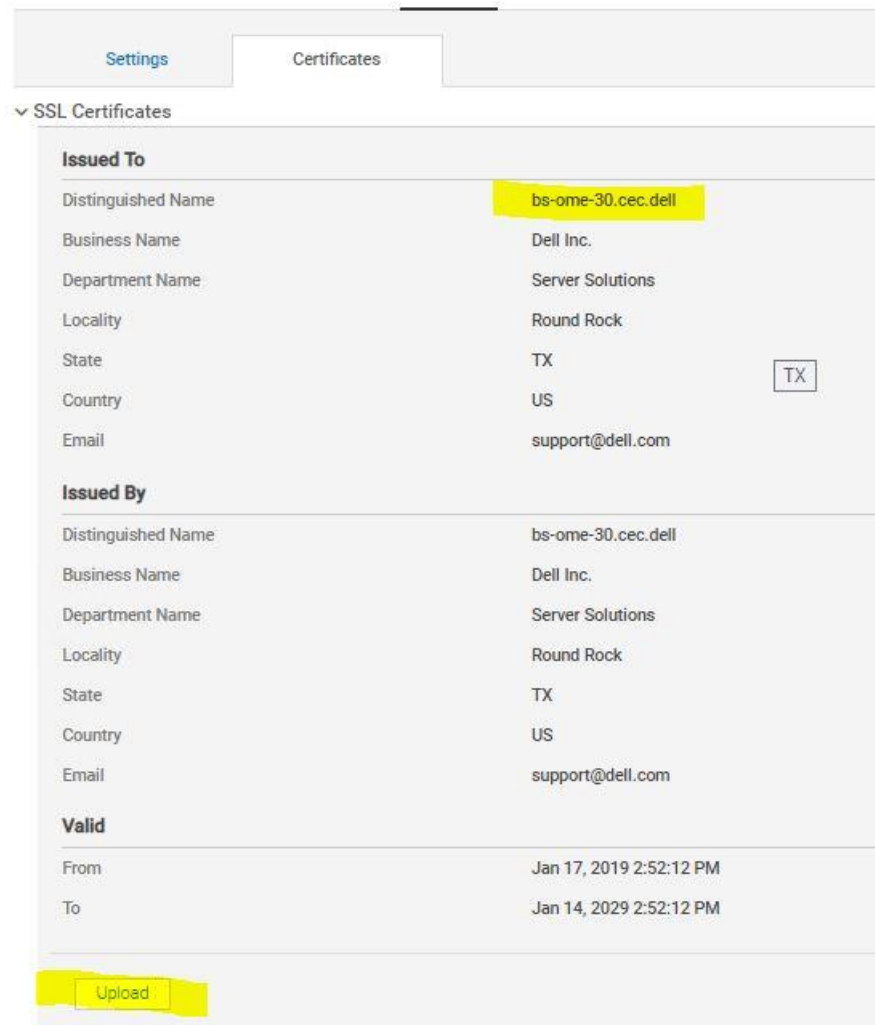
### Certificate Issued

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded

 [Download certificate](#)  
[Download certificate chain](#)

## Upload the certificate to your Openmanage Enterprise Web GUI



Settings Certificates

SSL Certificates

#### Issued To

Distinguished Name	bs-ome-30.cec.dell
Business Name	Dell Inc.
Department Name	Server Solutions
Locality	Round Rock
State	TX
Country	US
Email	support@dell.com

#### Issued By

Distinguished Name	bs-ome-30.cec.dell
Business Name	Dell Inc.
Department Name	Server Solutions
Locality	Round Rock
State	TX
Country	US
Email	support@dell.com

#### Valid

From	Jan 17, 2019 2:52:12 PM
To	Jan 14, 2029 2:52:12 PM

Upload

## Select your self-created certificate and open

The screenshot shows the OpenManage Enterprise console interface. The 'Certificates' tab is active, displaying a list of certificates under the 'Issued To' section. The certificate 'bs-ome-30.cer.dell' is highlighted with a red '1'. An 'Open' file explorer window is overlaid on the console, showing the file 'bs-ome-30.cer' selected in the 'Cert' folder, with a red '3' next to it. The 'File name' field in the explorer is set to 'bs-ome-30.cer', and the 'Open' button is highlighted with a red '4'. A red arrow points to the 'Upload' button at the bottom left of the console.

Name	Date modified	Type	Size
ad_cert_b64-chain.p7b	6/21/2018 2:42 PM	PKCS #7 Certificates	2 KB
ad_cert_b64-nochain.cer	6/21/2018 2:41 PM	Security Certificate	2 KB
ad_cert_der-chain.p7b	6/21/2018 2:41 PM	PKCS #7 Certificates	1 KB
ad_cert_der-nochain.cer	6/21/2018 2:41 PM	Security Certificate	1 KB
bs-ome-30.cer	1/17/2019 2:05 PM	Security Certificate	2 KB
bs-om-ent-2.cer	1/17/2019 1:32 PM	Security Certificate	3 KB
bs-om-ent-2-b64-web.cer	6/20/2018 11:06 AM	Security Certificate	3 KB
idrac-r740-csc-b64.cer	6/20/2018 11:41 AM	Security Certificate	3 KB

## Reopen your browser, open a link in "https://FQDN.YourDomain.ext" to your OMEnt

The screenshot shows a web browser window with the URL 'https://bs-ome-30.cer.dell:11111/console/console.htm'. The browser's address bar and tabs are highlighted with a green box. The page displays the OpenManage Enterprise logo and the text 'OpenManage Enterprise' in large white letters on a blue background. Below the logo, the copyright notice '© 2018 Dell Technologies. ALL RIGHTS RESERVED' and the 'DELL EMC' logo are visible. At the bottom of the page, there is a login form with fields for 'User Name' and 'Password', and a 'Login' button.