Dell Management Plug-in for VMware vCenter: Custom SSL/HTTPS Certificate using Microsoft Windows Certification Authority

This Dell Technical white paper describes the necessary steps to generate and consume a custom SSL/HTTPS certificate for the Dell Management Plug-in using Microsoft Windows Certification Authority.

Irfan Azam

Yousaf Sajjad

This document is for informational purposes only and may contain typographical errors and technical inaccuracies. The content is provided as is, without express or implied warranties of any kind.

January 2013| Rev 1.0

Contents

Introduction

The Dell Management Plug-in is a virtual appliance used to reduce tools and tasks associated with the management and deployment of Dell servers in your virtual environment. It reduces complexity by natively integrating the key management capabilities into the vCenter console. It minimizes risk with hardware alarms, streamlined firmware updates and deep visibility into inventory and provides health and warranty details.

The Dell Management Plug-in for VMware vCenter is designed to streamline the management processes in your data center environment. It lets you use VMware vCenter to manage your entire infrastructure-both physical and virtual. From firmware updates to bare metal deployment, the Dell Management Plug-In for VMware vCenter expands and enriches your data center management experience with Dell PowerEdge servers.

This white paper provides all necessary information to generate and consume custom SSL/HTTPS certificate for the Dell Management Plug-in using Microsoft Windows Certification Authority.

Audience and scope

The scope of the document is to provide a detailed procedure towards setting up a custom SSL/HTTPS certificate for Dell Management Plug-in appliance 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. This document is intended to assist you in using the Dell Management Plug-in for managing vSphere hosts, which are Dell servers in a vCenter.

Prerequisites

You are expected to have working knowledge of networking, SSL, HTTP and digital certificates. This document also requires the Microsoft Windows Certification Authority services running on a server within the same/trusted network where the Dell Management Plug-in is running.

You are expected to know the steps for installing Dell Management Plug-in for VMware vCenter and registering it to a vCenter. You can find more information on installing and registering the Dell Management Plug-in to a vCenter in *Dell Management Plug-in for VMware vCenter User's Guide.*

Why use an SSL certificate?

For secure HTTPS communication, the web server requires the SSL certificate on the Dell Management Plug-in.

Why use a custom certificate?

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 trusted certificate exception in the web browser. In addition, it fixes the problem of accepting the virtual appliance certificate while connecting to the vSphere client or browsing the virtual appliance content within vSphere client.

Custom certificate attributes

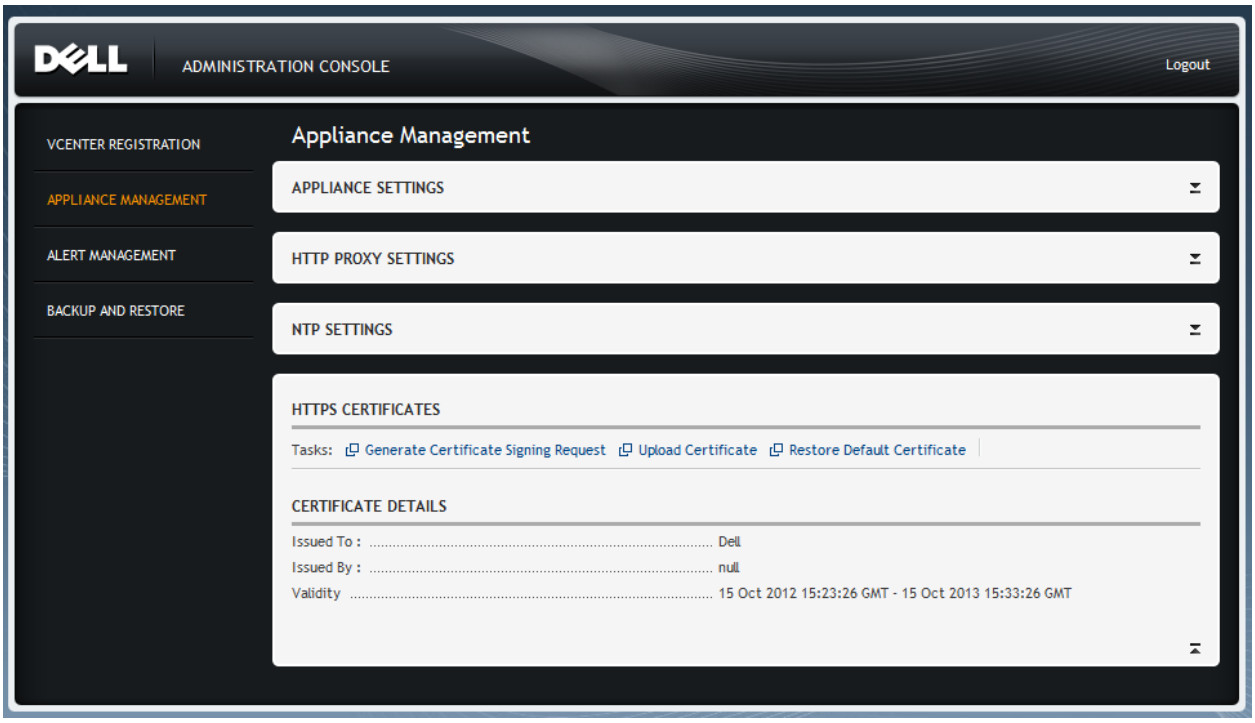
The virtual appliance supports a X.509 certificate with RSA 2048-bit key encryption standard and requires the certificate to be in the PEM format (http://en.wikipedia.org/wiki/X.509).

Generating a CSR using the Administration Console

Use the Administration Console to generate the certificate signing request (CSR).

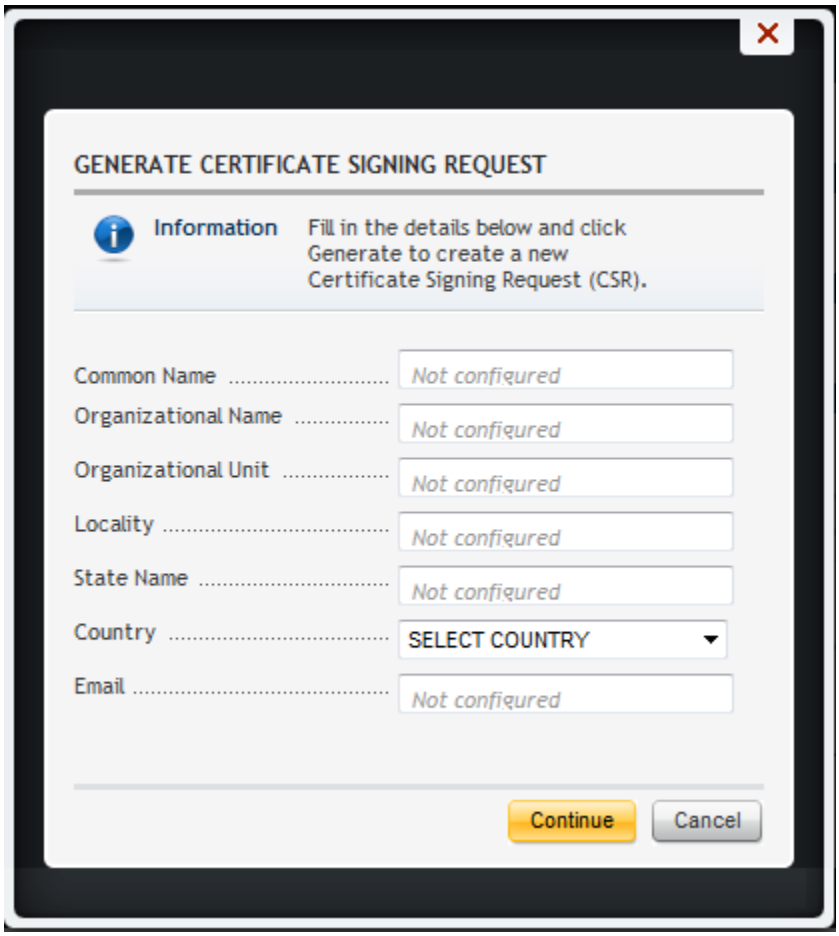
1. Open the Administration Portal using https://appliance-ip-or-fqdn and on the left side of the Administration Console, click **Appliance Management**.

Figure 1. Using the Administration Console.



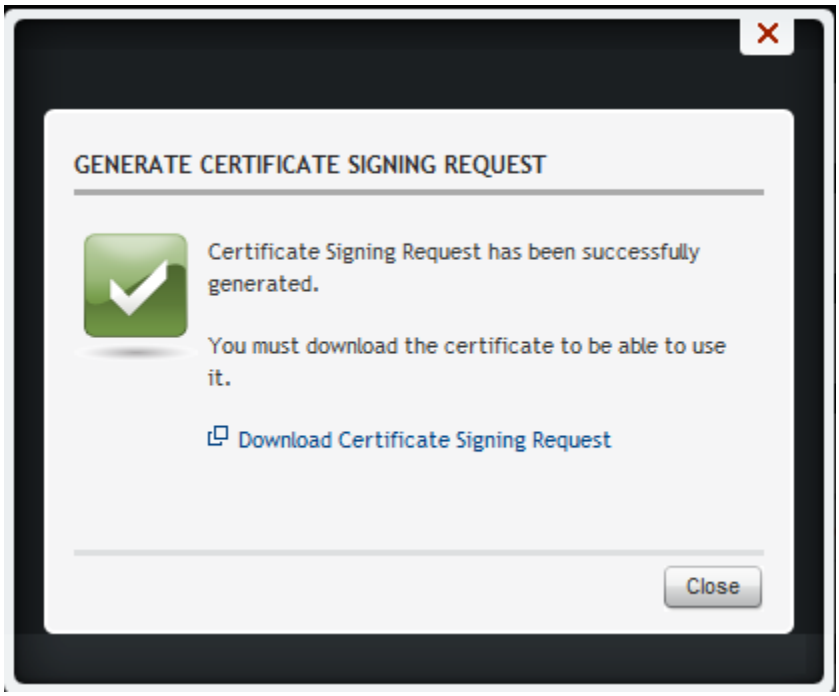
2. Under HTTPS Certificates, click **Generate Certificate Signing Request**.

Figure 2. Generating the certificate signing request.



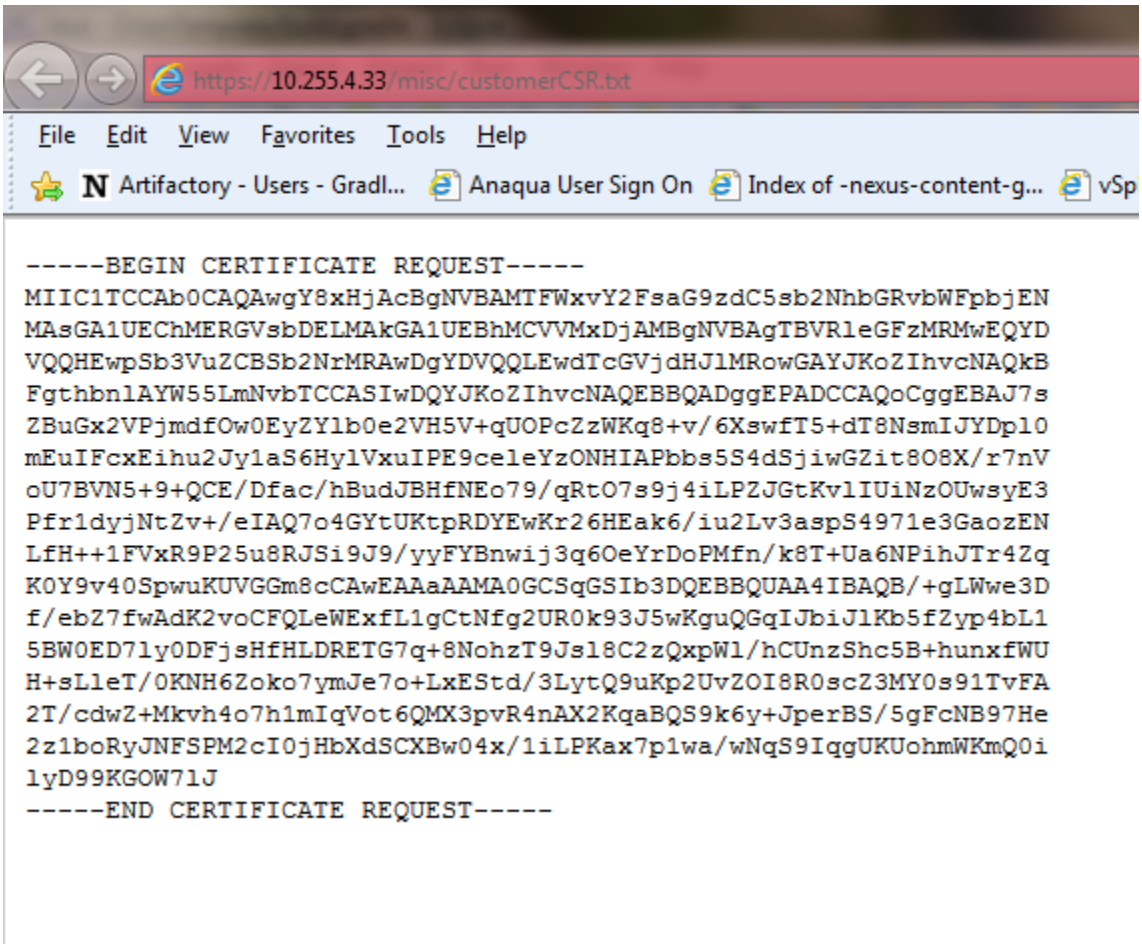
3. Provide the required information and make sure that the Common Name field contains the appliance's FQDN/Hostname or localhost.localdomain if FQDN/Hostname is not set.

Figure 3. Success dialog box.



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

Figure 4. Copy the BEGIN and END of the Certificate Request.



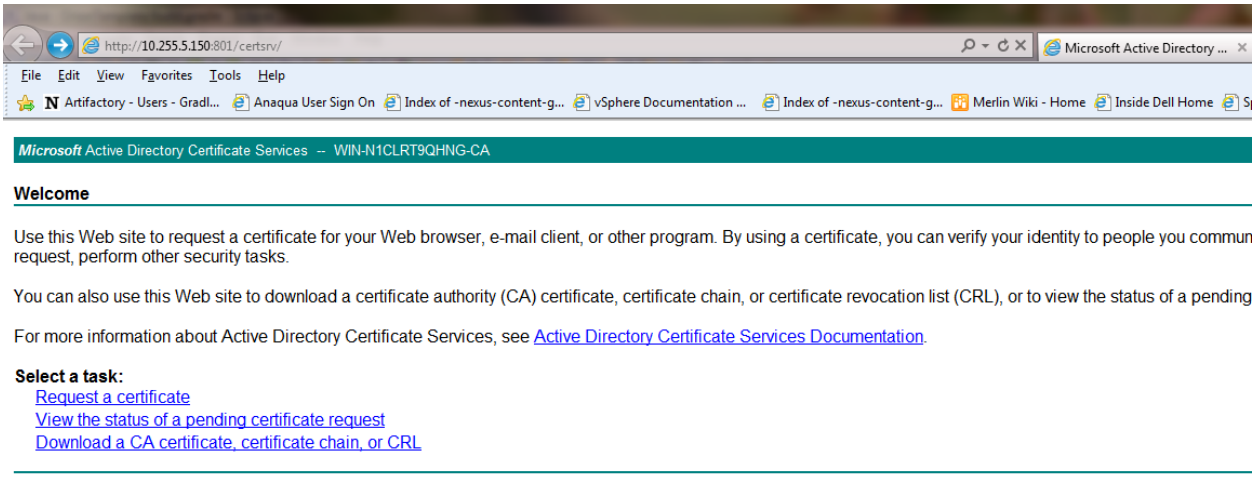
Certificate signing using Microsoft Windows CA

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

1. Open the certification authority portal page in the web browser by using http://certificate-authority-address/certsrv

2. Click **Request a certificate**.

Figure 5. Using Microsoft Active Directory Certificate Services.

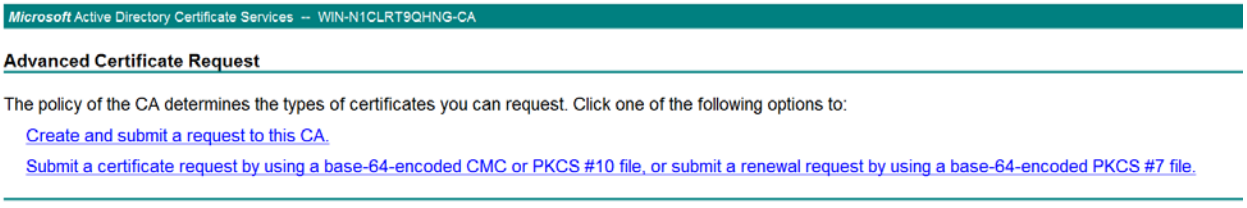


Click **Advanced certificate request**.

Figure 6. Requesting a certificate.

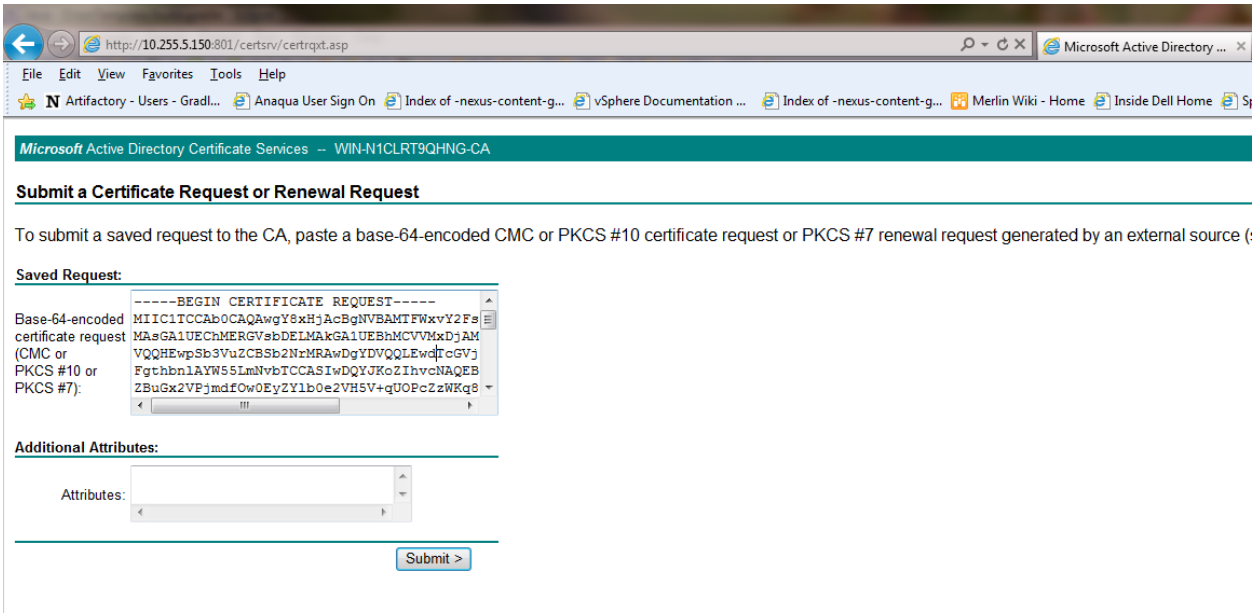
3. Click **Submit a certificate request by using base-64-encoded CMC or PKCS #10 file**… .

Figure 7. Advanced Certificate Request screen.



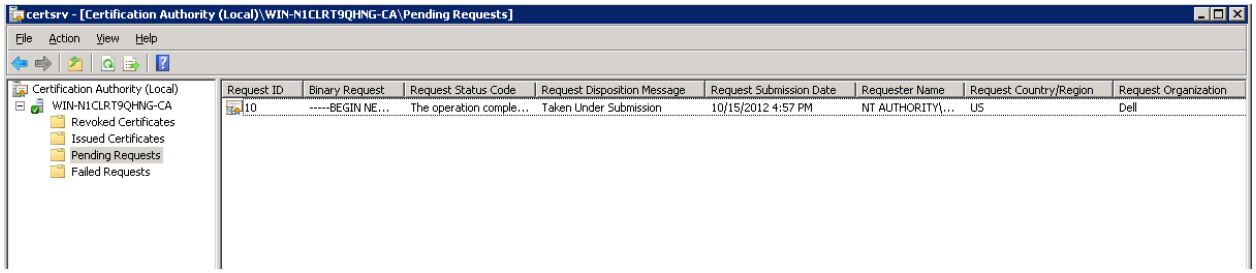
4. Paste the CSR text you copied in the previous procedure in the text area and submit the request. Make sure that the BEGIN and END certificate REQUEST tags are present in the text.

Figure 8. Pasting in the certificate request.



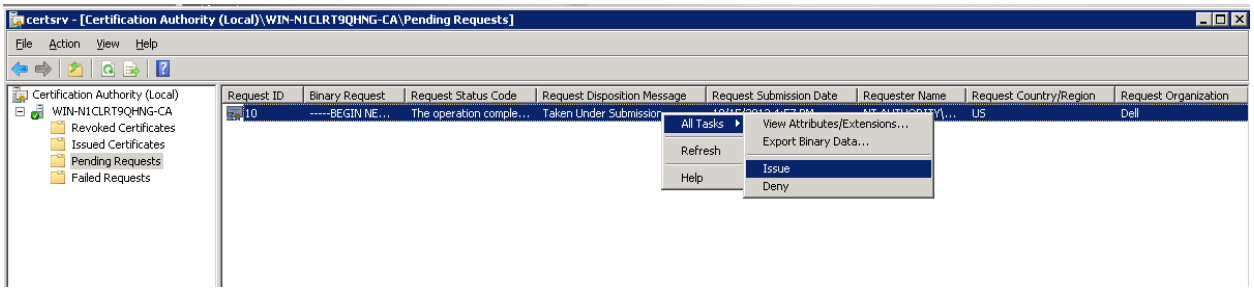
5. On the Certification Authority server, open the Certification Authority snapshot.

Figure 9. Opening the Certificate Authority snapshot.



6. Right-click the pending certificates folder and issue the certificate.

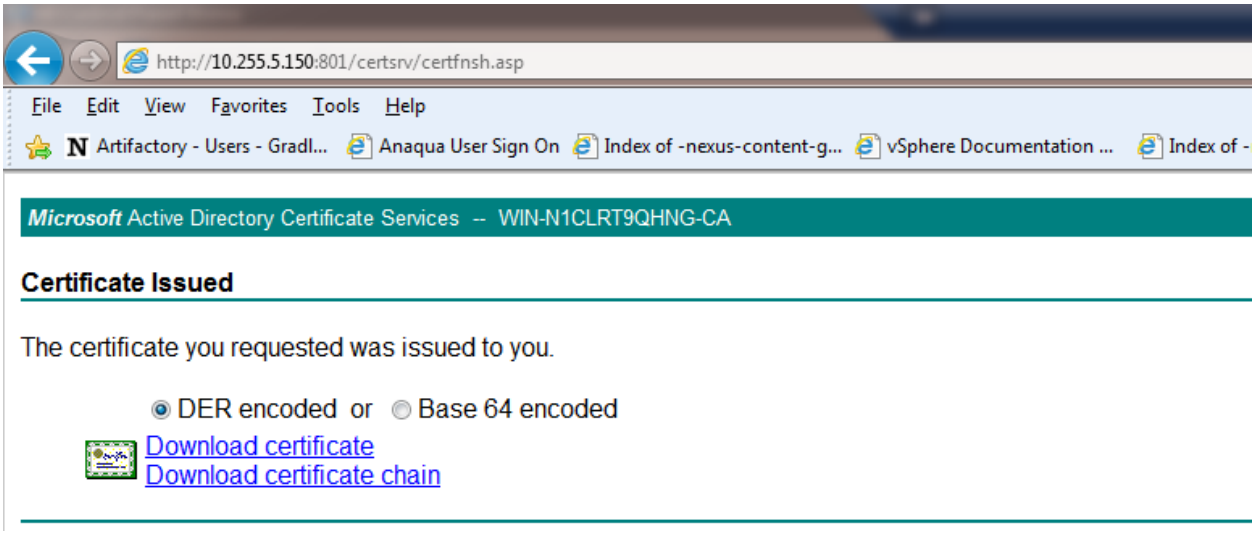
Figure 10. Issuing the certificate.



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

8. Download the *Saved-Request Certificate* to the local disk.

Figure 11. Downloading the certificate.



9. To Download DER encoded certificate, click **Download Certificate**.
10. Convert the certificate from cert/cer format to PEM format using openssl or using the directions from the following web sites:
    - https://www.sslshopper.com/ssl-converter.html
    - http://www.bo.infn.it/alice/introgrd/certmgr/node2.html

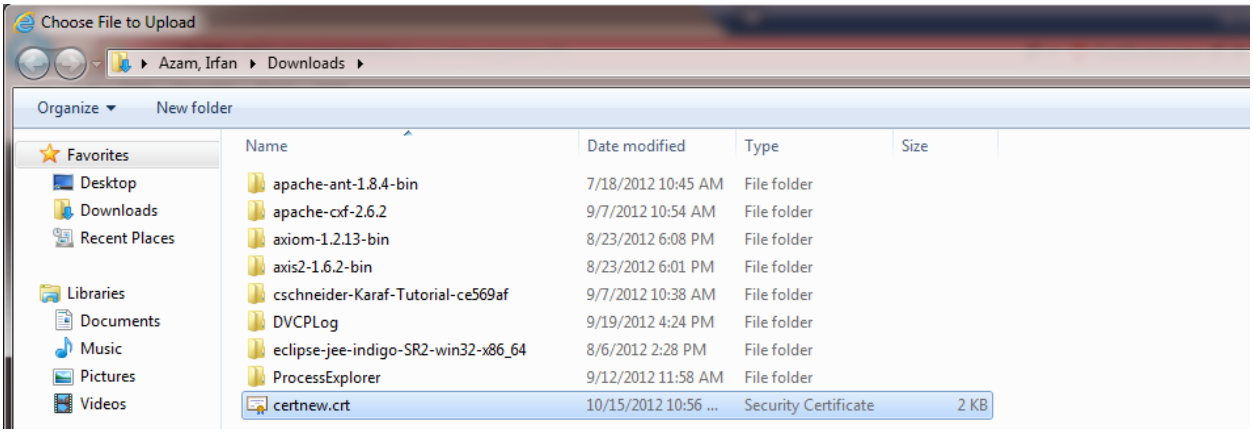
Figure 12. Converting SLL formats.

Uploading a certificate to the virtual appliance

This section provides information about how to upload the certificate, which you obtained following the instructions in the previous section, onto the virtual appliance using Administration Console.

1. Open the Administration Portal using https://appliance-ip-or-fqdn and on the left side of the Administration Console, click Appliance Management.
2. Click **Upload Certificate** and browse the *certificate.pem* or *certificate.crt* file.

Figure 13. Selecting the certificate to upload.



3. Click Upload certificate.
4. After upload is complete, log out from Administration Console, refresh the browser page and re-login to establish the HTTPS session using the new certificate.