# 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.

© 2012 Dell Inc. All rights reserved. Dell and its affiliates cannot be responsible for errors or omissions in typography or photography. Dell, the Dell Iogo, and PowerEdge are trademarks of Dell Inc. Intel and Xeon are registered trademarks of Intel Corporation in the U.S. and other countries. Microsoft, Windows, and Windows Server are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims proprietary interest in the marks and names of others.

January 2013 | Rev 1.0

# Contents

Introduction	4
Audience and scope	4
Prerequisites	4
Why use an SSL certificate?	4
Why use a custom certificate?	4
Custom certificate attributes	5
Generating a CSR using the Administration Console	5
Certificate signing using Microsoft Windows CA	8
Uploading a certificate to the virtual appliance 1	2

## 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 infrastructureboth 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 (<u>http://en.wikipedia.org/wiki/X.509</u>).

# Generating a CSR using the Administration Console

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

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

	ATION CONSOLE	Logout						
VCENTER REGISTRATION	Appliance Management							
APPLIANCE MANAGEMENT	APPLIANCE SETTINGS	Ξ						
ALERT MANAGEMENT	HTTP PROXY SETTINGS	Ŧ						
BACKUP AND RESTORE	NTP SETTINGS							
	HTTPS CERTIFICATES							
	Tasks: 💭 Generate Certificate Signing Request 💭 Upload Certificate 🖓 Restore Default Certificate	_						
	Issued To : Dell   Issued By : null   Validity 15 Oct 2012 15:23:26 GMT - 15 Oct 2013 15:33:26 GMT	-						

Figure 1. Using the Administration Console.

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

1nformation	Fill in the Generate Certifica	details below and click to create a new te Signing Request (CSR).
Common Name		Not configured
Organizational Name		Not configured
Organizational Unit		Not configured
locality		Not configured
state Name		Not configured
Country		SELECT COUNTRY -
Email		Not configured

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.
(C) (A https://10.255.4.33/misc/customerCSR.txt
<u>F</u> ile <u>E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp
👍 🖪 Artifactory - Users - Gradl 🧃 Anaqua User Sign On 🧃 Index of -nexus-content-g 🧃 vSp
BEGIN CERTIFICATE BEOUEST
MIIC1TCCAb0CAOAwgY8xHjAcBgNVBAMTFWxyY2FsaG9zdC5sb2NhbGRybWFpbjEN
MAsGA1UEChMERGVsbDELMAkGA1UEBhMCVVMxDjAMBqNVBAqTBVR1eGFzMRMwEQYD
VQQHEwpSb3VuZCBSb2NrMRAwDgYDVQQLEwdTcGVjdHJ1MRowGAYJKoZIhvcNAQkB
FgthbnlAYW55LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ7s
ZBuGx2VPjmdf0w0EyZY1b0e2VH5V+qU0PcZzWKq8+v/6XswfT5+dT8NsmIJYDp10
mEuIFcxEihu2Jy1aS6Hy1VxuIPE9celeYzONHIAPbbs5S4dSjiwGZit8O8X/r7nV
oU7BVN5+9+QCE/Dfac/hBudJBHfNEo79/qRt07s9j4iLPZJGtKv1IUiNzOUwsyE3
Pfr1dyjNtZv+/eIAQ7o4GYtUKtpRDYEwKr26HEak6/iu2Lv3aspS4971e3GaozEN
LfH++1FVxR9P25u8RJSi9J9/yyFYBnwij3q60eYrDoPMfn/k8T+Ua6NPihJTr4Zq
K0Y9v40SpwuKUVGGm8cCAwEAAaAAMA0GCSqGSIb3DQEBBQUAA4IBAQB/+gLWwe3D
f/ebZ7fwAdK2voCFQLeWExfL1gCtNfg2UR0k93J5wKguQGqIJbiJ1Kb5fZyp4bL1
5BW0ED71y0DFjsHfHLDRETG7q+8NohzT9Js18C2zQxpW1/hCUnzShc5B+hunxiWU
H+SLIEI/UKNH6ZOKO/YMJE/O+LXESTA/SLYTQ9UKp2UVZOI8KUSCZ3MYUS9IIVFA
21/Caw2+MkVn40/n1m1qv0t6QMx3pvK4nAx2KqabQ59k6y+Jperb5/SgrCNb9/He
221D0KY0NF5FM2CT0JHDXd5CKDw04X/11LFKAX/piwa/wnq591qg0K00HHWMHQ01
FND_CERTIFICATE_REQUEST
LAD CERTITIONED REXCEPT

# 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 <u>http://certificate-authority-address/certsrv</u>
- 2. Click Request a certificate.

Figure 5. Using Microsoft Active Directory Certificate Services.

Contraction of the local division of the loc	
	P → C ×
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp	
👍 👖 Artifactory - Users - GradI 🧧 Anaqua User Sign On 🖉 Index of -nexus-content-g 🧃 vSphere Documentation	🧉 Index of -nexus-content-g 🔞 Merlin Wiki - Home 🧉 Inside Dell Home 🧃 S <sub>l</sub>
Microsoft Active Directory Certificate Services WIN-N1CLRT9QHNG-CA	
Welcome	
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By u request, perform other security tasks.	sing a certificate, you can verify your identity to people you commun
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, c	or certificate revocation list (CRL), or to view the status of a pending
For more information about Active Directory Certificate Services, see Active Directory Certificate Services	ervices Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRI

Click Advanced certificate request.

	Figure 6.Requesting a certificate.					
Microsoft Active Directory Certificate Services WIN-N1CLRT9QHNG-CA						
Request a Certi	ficate					
Select the certific	ate type:					
Web Browser	<u>Certificate</u>					
E-Mail Protect	ion Certificate					
Or, submit an <u>adv</u>	anced certificate r	request.				

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

#### Figure 7. Advanced Certificate Request screen.

Microsoft Active Directory Certificate Services WIN-N1CLRT9QHNG-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.

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.
and the second s	
C 3 Attp://10.255.5.150:801/certsrv/certrqxt.asp	P → C × Ø Microsoft Active Directory ×
<u>Eile E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp	
🚖 N Artifactory - Users - Gradl 🤌 Anaqua User Sign On 🤌 Index of -nexus-	-content-g 🧉 vSphere Documentation 🧧 Index of -nexus-content-g 🛐 Merlin Wiki - Home 🧧 Inside Dell Home 🧧 S
Microsoft Active Directory Certificate Services WIN-N1CLRT9QHNG-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 renewal request generated by an external source (
Saved Request:	
Base-64-encoded MIIC1TCCAb0CAQAwgY8xHjAcBgNVBAMTFWxvY2Fs	
certificate request MAsGA1UEChMERGVsbDELMAkGA1UEBhMCVVMxDjAM	
CLINC or VQQHEWDSD3VU2CBSD2NTMRAWDGIDVQQLEWdLCGV] PKCS #10 or FgthbnlAYW55LmNvbTCCASIwDQYJKoZIhvcNAQEB	
PKCS #7): ZBuGx2VPjmdfOw0EyZY1b0e2VH5V+qU0PcZzWKq8 *	
< III P	
Additional Attributes:	
Attributes:	
Submit >	-

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

#### Figure 9. Opening the Certificate Authority snapshot.

🚋 certsrv - [Certification Authority	(Local)\WIN-I	1CLRT9QHNG-CA	\Pending Requests]					
Eile Action Yiew Help								
🗢 🔿 🙇 💁								
🙀 Certification Authority (Local)	Request ID	Binary Request	Request Status Code	Request Disposition Message	Request Submission Date	Requester Name	Request Country/Region	Request Organization
🖃 🚽 WIN-N1CLRT9QHNG-CA	<b>5</b> 10	BEGIN NE	The operation comple	Taken Under Submission	10/15/2012 4:57 PM	NT AUTHORITY\	US	Dell
Revoked Certificates								
Issued Certificates								
Pending Requests								
Failed Requests								
	1							

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

🧱 certsry - [Certification Authority	(Local)\WIN-N	N1CLRT9QHNG-C4	\\Pending Requests]					
Eile Action View Help								
🗢 🔿 🙋 🙆 👔								
🙀 Certification Authority (Local)	Request ID	Binary Request	Request Status Code	Request Disposition Message	Request Submission Date	Requester Name	Request Country/Region	Request Organization
🖃 🚽 WIN-N1CLRT9QHNG-CA	10	BEGIN NE	The operation comple	Taken Under Submission		NT AUTHORITY	. US	Dell
Revoked Certificates				All	Tasks View Attributes/E	xtensions		
Issued Certificates				Re	resh Export Binary Dat	:a		
Pending Requests					Tssue			
Failed Requests				He	P Depy			
					Dony			
1								

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.



- 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:
  - <u>https://www.sslshopper.com/ssl-converter.html</u>
  - <u>http://www.bo.infn.it/alice/introgrd/certmgr/node2.html</u>

Figure 12. Converting SLL formats.

#### **SSL Converter**

Use this **SSL Converter to convert SSL certificates** to and from different formats such as **pem, der, p7b, and pfx.** Different platforms and devices require SSL certificates to be converted to different formats. For example, a Windows server exports and imports .pfx files while an Apache server uses individual PEM (.crt, .cer) files. To use the SSL Converter, just select your certificate file and its current type (it will try to detect the type from the file extension) and then select what type you want to convert the certificate to and click **Convert Certificate**. For more information about the different <u>SSL certificate</u> types and how you can convert certificates on your computer using OpenSSL, see below.

Certificate File to Convert:	C:\Users\irfan_azam\Downloads\certnew.cer Browse_
Type of Current Certificate:	DER/Binary - Detected type from file extension
Type To Convert To:	Standard PEM 🔸
	Convert Certificate

#### **PEM Format**

The PEM format is the most common format that <u>Certificate Authorities</u> issue certificates in. PEM certificates usually have extentions such as **.pem**, **.crt**, **.cer**, **and .key**. They are Base64 encoded ASCII files and contain "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" statements. Server certificates, intermediate certificates, and private keys can all be put into the PEM format.

**Apache and other similar servers** use PEM format certificates. Several PEM certificates, and even the private key, can be included in one file, one below the other, but most platforms, such as Apache, expect the certificates and private key to be in separate files.

# 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.

Choose File to Upload		_	-	_
🕥 🗸 🚺 🕨 Azam, Irf	an 🕨 Downloads 🕨			
Organize 👻 New fold	er			
🔆 Favorites	Name	Date modified	Туре	Size
📃 Desktop	퉬 apache-ant-1.8.4-bin	7/18/2012 10:45 AM	File folder	
🗼 Downloads	퉬 apache-cxf-2.6.2	9/7/2012 10:54 AM	File folder	
📃 Recent Places	퉬 axiom-1.2.13-bin	8/23/2012 6:08 PM	File folder	
	퉬 axis2-1.6.2-bin	8/23/2012 6:01 PM	File folder	
🥃 Libraries	퉬 cschneider-Karaf-Tutorial-ce569af	9/7/2012 10:38 AM	File folder	
Documents	퉬 DVCPLog	9/19/2012 4:24 PM	File folder	
👌 Music	퉬 eclipse-jee-indigo-SR2-win32-x86_64	8/6/2012 2:28 PM	File folder	
Pictures	🌗 ProcessExplorer	9/12/2012 11:58 AM	File folder	
😸 Videos	📮 certnew.crt	10/15/2012 10:56	Security Certificate	2 KB

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.