



TelePresence

Creating a Cisco TelePresence Video Communication Server (VCS) Certificate

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at <http://www.cisco.com/go/trademarks>. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Creating a Cisco TelePresence Video Communication Server (VCS) Certificate
September 2012 Edition
© 2012 Cisco Systems, Inc. All rights reserved.

Table of Contents

1	INTRODUCTION	4
1.1	Release Notes	4
2	CREATING A VCS CERTIFICATE	4
2.1	Installing OpenSSL on Windows 7 64bit.....	4
2.2	Using OpenSSL Already Present on the VCS	12
2.3	Creating a self-signed certificate.....	20

List of Tables

Table 1 - Release Notes	4
-------------------------------	---

List of Figures

Figure 1 - Windows\system32\cmd.exe - openssl	5
Figure 2 - OpenSSL.....	8
Figure 3 - Microsoft Active Directory Certificate Services	8
Figure 4 - Request a Certificate	9
Figure 5 - Advanced Certificate Request.....	9
Figure 6 - Submit a Certificate Request or Renewal Request	9
Figure 7 - Submit a Certificate Request or Renewal Request	10
Figure 8 - Certificate Issued	11
Figure 9 - Main Certificate Authority Page	11
Figure 10 - Download a CA Certificate, Certificate Chain, or CRL	11
Figure 11 - Openssl already present on the VCS.....	15
Figure 12 - Microsoft Active Directory Certificate Services	15
Figure 13 - Request a Certificate	16
Figure 14 - Advanced Certificate Request.....	16
Figure 15 - Submit a Certificate Request or Renewal Request	16
Figure 16 - Submit a Certificate Request or Renewal Request	17
Figure 17 - Certificate Issued	18
Figure 18 - Main Certificate Authority Page	18
Figure 19 - Download a CA Certificate, Certificate Chain, or CRL	18
Figure 20 - WinSCP	19
Figure 21 - Main Certificate Authority Page	20
Figure 22 - Download a CA Certificate, Certificate Chain, or CRL	20
Figure 23 - Login Screen on VCS	21
Figure 24 - Security certificate.....	25
Figure 25 - WinSCP	26
Figure 26 - Server certificate date	27

1 Introduction

This document provides three options and instructions for creating a **Cisco TelePresence Video Communication Server (VCS)** certificate

1.1 Release Notes

Table 1 - Release Notes

Technical Change	Title(s) of Affected Section(s)	Changes Made By	Date
Initial Release		Charles Brown	6/29/2012
Revised format and title			8/9/2012
Elaboration of Installing OpenSSL		Matt Limbrick	9/26/2012

2 Creating a VCS Certificate

The three options for creating a VCS certificate are:

- Create a certificate request by downloading and installing **OpenSSL** or whatever application is used to generate certificate requests by the enterprise and requesting certificate from your **Certificate Authority (CA)**.
- Create a certificate request using the **OpenSSL** that is already present on the VCS (with caveats) to use with your CA.
- Create a self-signed certificate if certificate authority not required.

2.1 Installing OpenSSL on Windows 7 64bit

Note: This section is for Windows 7 64bit, but you can install OpenSSL and the correct Visual C++ Redistributions for your particular version of Windows from the following link:

<http://slproweb.com/products/Win32OpenSSL.html>

1. Download and install the Microsoft Visual C++ 2010 Redistributable Package needed to support OpenSSL Light. This file should be vcredist_x64.exe.

<http://www.microsoft.com/en-us/download/details.aspx?id=14632>

2. Download OpenSSL ([Win64 OpenSSL v1.0.1c Light](#)) and install the .exe file.

<http://slproweb.com/products/Win32OpenSSL.html>

- Once all is installed, open a Windows command prompt and Type: `cd\openssl-win64\bin`

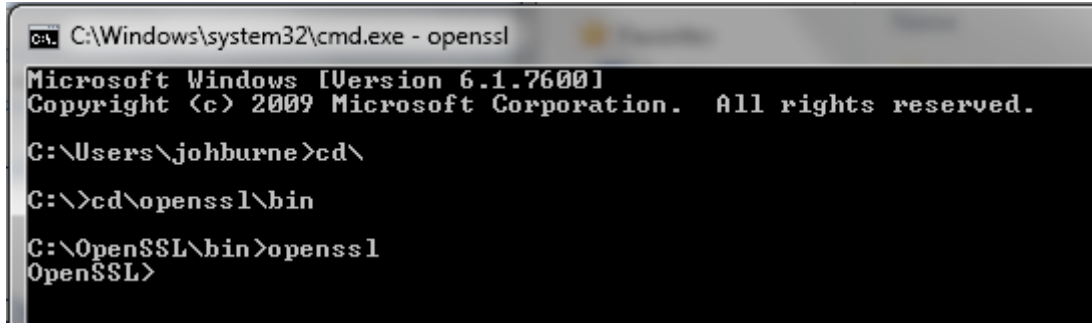
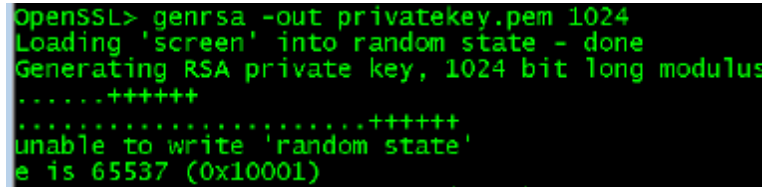


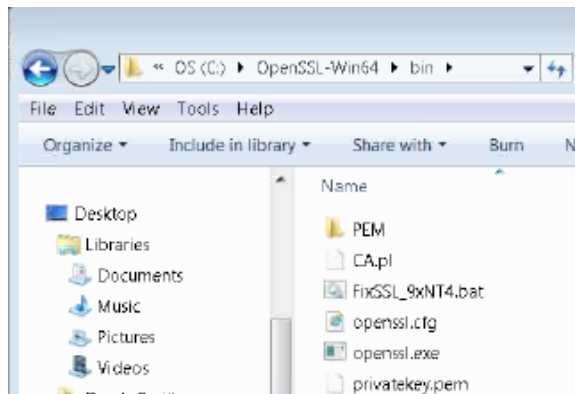
Figure 1 - Windows\system32\cmd.exe - openssl

- Next, type: `openssl` to initiate the program and obtain an "OpenSSL>" prompt.
- Type: `genrsa -out privatekey.pem 1024` You should get the output below:

```
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....+++++
.....+++++
unable to write 'random state'
e is 65537 (0x10001)
OpenSSL>
```



NOTE: The name **privatekey.pem** is the name of the private key you are generating. This could be **cocolaprivkey.pem** for example. You can verify the file `privatekey.pem` was created in the `C:\openssl-win64\bin` folder



- Type: `req -new -key privatekey.pem -out certcsr.pem`. You should get the following output below. (**certcsr.pem** is the certificate request submitted to your CA.)

```
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
```

Into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value.

If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:

```
OpenSSL> req -new -key privatekey.pem -out certcsr.pem
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
what you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value.
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
```

If instead you get the error "**Unable to load config file from /usr/local/ssl/openssl.cnf error in req**", you will need to exit the OpenSSL> prompt by typing "exit" and then use the following command:

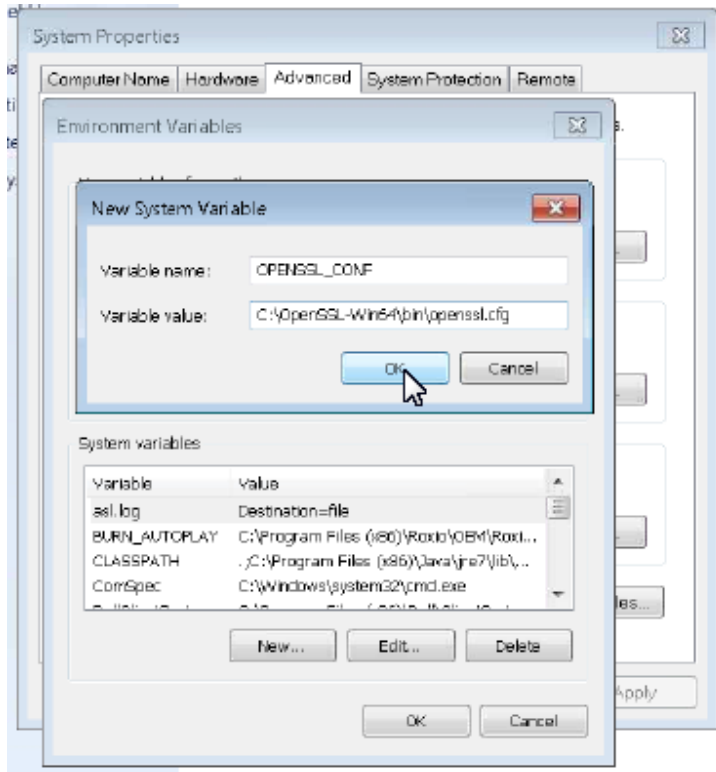
```
OpenSSL> req -new -key privatekey.pem -out certcsr.pem
Unable to load config info from /usr/local/ssl/openssl.cnf
error in req
OpenSSL>
```

c:\OpenSSL-Win64\bin>SET OPENSSL_CONF=C:\OpenSSL-Win64\bin\openssl.cfg

or you can right-click "Computer"/ Properties/ Advances System settings/ Environment Variable/ New (Under System Variable).

Variable Name: **OPENSSL_CONF**

Variable Value: **C:\OpenSSL-Win64\bin\openssl.cfg**



Note: When adding these variable via the command prompt, they remain set only during that instance. When adding these variables via System Properties, you will need to reboot your PC after in order for the changes to implement permanently. When finished adding the variable through, return to step 6.

7. Answer the questions in the certificate request. The common name must be the FQDN of the VCS. See the following example.

Do not enter a challenge password. Leave this blank.

```

C:\Windows\system32\cmd.exe - openssl

C:\Users\johburne>cd\openssl\bin

C:\OpenSSL\bin>openssl
OpenSSL> genrsa -out exampleprivkey.pem 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....+++++
.....+++++
unable to write 'random state'
e is 65537 (0x10001)
OpenSSL> req -new -key exampleprivkey.pem -out examplecertcsr.
You are about to be asked to enter information that will be in
into your certificate request.
What you are about to enter is what is called a Distinguished
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:UA
Locality Name (eg, city) []:Reston
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cis
Organizational Unit Name (eg, section) []:ITG
Common Name (eg, YOUR name) []:example.vcs.cisco.com
Email Address []:johburne@cisco.com
    
```

8. Go to the bin directory and find the **certcsr.pem** file that you generated. This is your certificate request.

NOTE: Note: For clarity purposes, the name could be **cocacolacertcsr.pem**

9. Open the file with notepad or WordPad or notepad ++
10. As shown in the following example, copy the entire certificate, including the beginning and ending certificate lines to paste into the certificate request page of your CA.

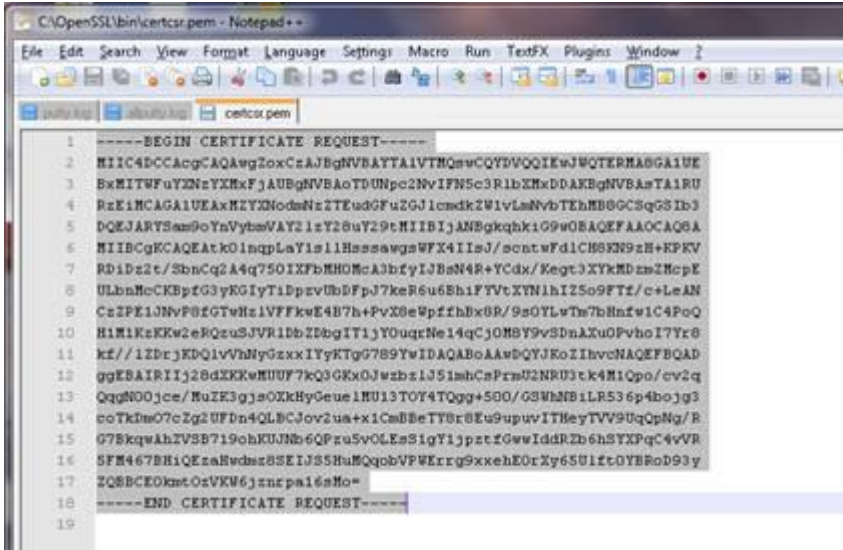


Figure 2 - OpenSSL

11. If your CA is Microsoft, you need to have an admin login to take you to this page. If your CA is another company, have them take you to the certificate request page.
12. To paste the request you copied into the certificate request page, complete the following steps:
 - a. Go to the **Certificate Services** page of your CA.
 - b. On the **Welcome** page, select **Request a Certificate**.

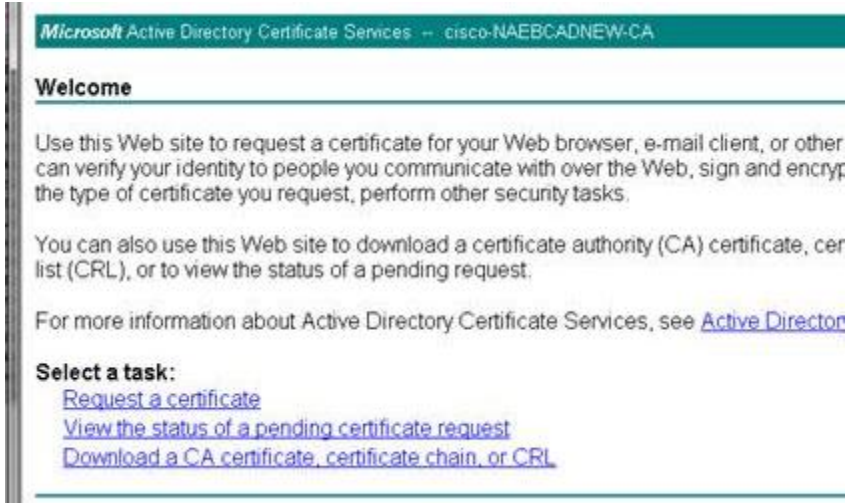


Figure 3 - Microsoft Active Directory Certificate Services

- c. On the **Request a Certificate** page, select submit an **advanced certificate request**.



Figure 4 - Request a Certificate

- d. On the **Advanced Certificate Request** page, select **Create and submit a request to this CA**.

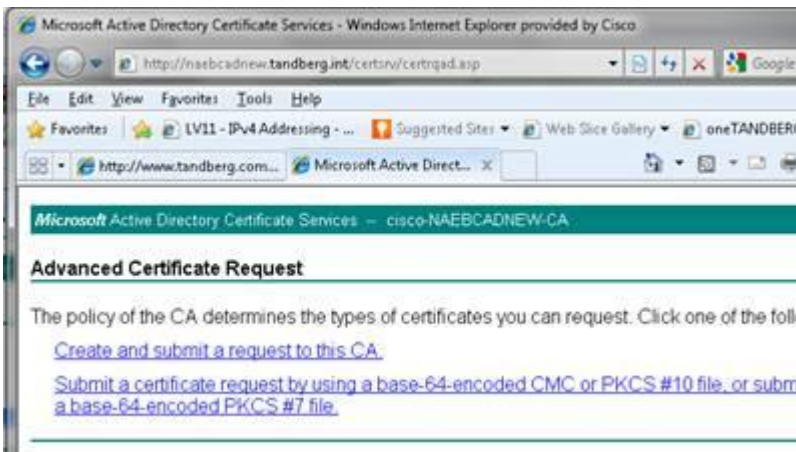


Figure 5 - Advanced Certificate Request

- e. On the **Submit a Certificate Request or Renewal Request** page, paste the request you copied into the **Saved Request** space.

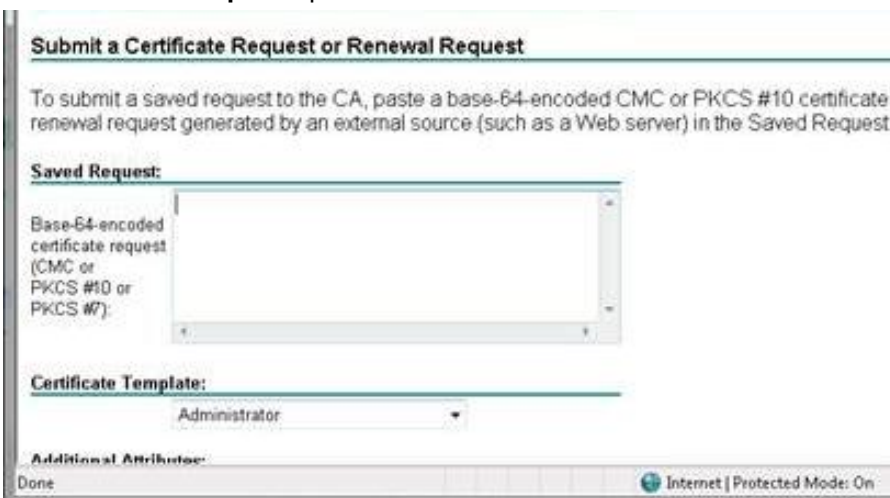


Figure 6 - Submit a Certificate Request or Renewal Request

- f. Under **Certificate Template**, select the dropdown menu and select **Web Server**.

Microsoft Active Directory Certificate Services -- chabrow2-DC-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC

Saved Request:

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

Certificate Template:

Additional Attributes:

Attributes:

Web Server

Administrator

Basic EFS

EFS Recovery Agent

User

Subordinate Certification Authority

Web Server

- g. The following example shows the *Certificate Request or Renewal Request* with the beginning and ending lines pasted into it.

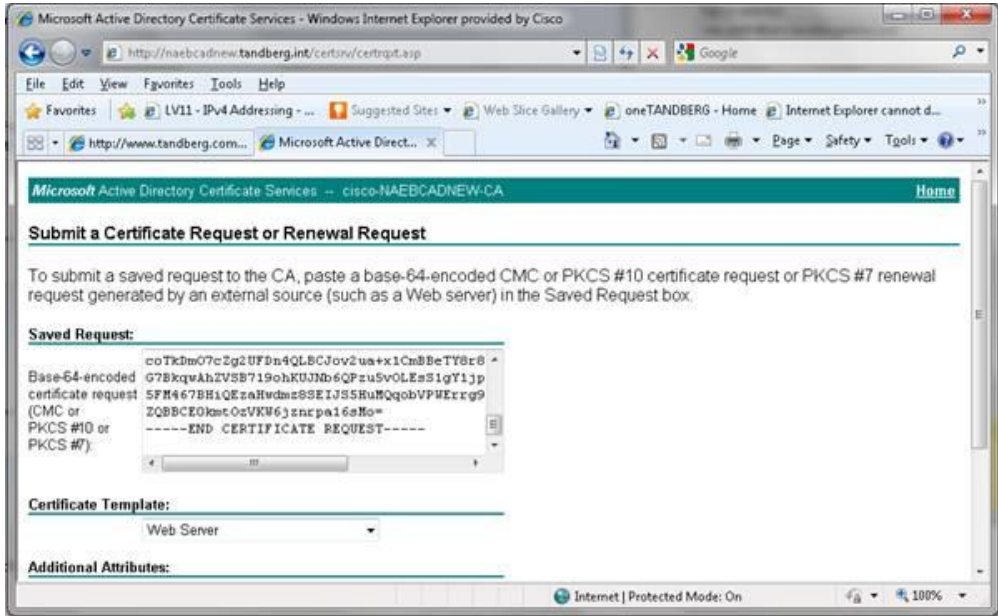


Figure 7 - Submit a Certificate Request or Renewal Request

13. On the Certificate Issued page, select **Base 64**, then **Download certificate**.



Figure 8 - Certificate Issued

The certificate is issued in **.cer** format, which is fine for the VCS. You can change this to **.pem** format.

14. After you have both the private key and the certificate for the VCS, you need the CA certificate.
 - a. Go back to the main CA webpage and select **Download a CA certificate, certificate chain, or CRL**.

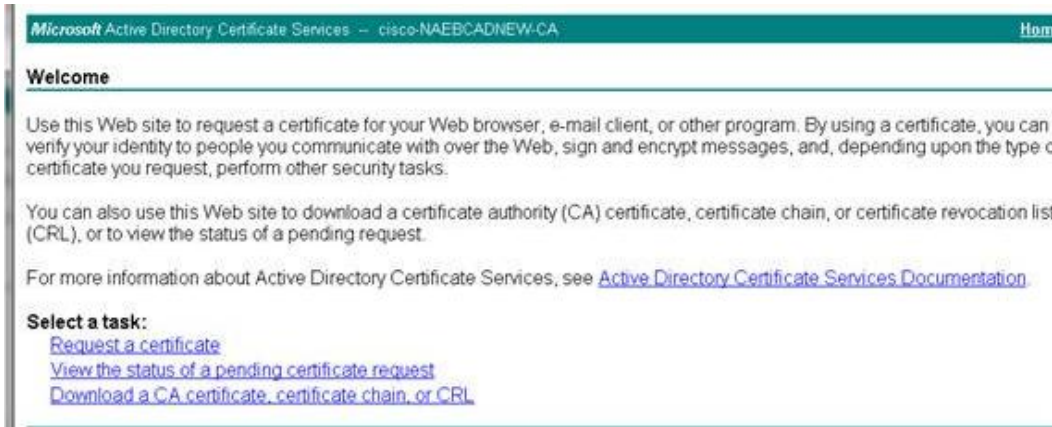


Figure 9 - Main Certificate Authority Page

- b. On the **Download a CA Certificate, Certificate Chain, or CRL**, select **Base 64**.



Figure 10 - Download a CA Certificate, Certificate Chain, or CRL

15. You can load the CA certificate to the VCS in **.cer** format or convert to **.pem**. Either works.

2.2 Using OpenSSL Already Present on the VCS

(First the caveat: You can use **openssl** on the VCS to generate a certificate request for a CA, but cluster names cannot be used because the application lacks the ability to add an alternate subject name to the certificate request. So the local **openssl** on the VCS cannot be used if the certificate produced is to set up connectivity via TLS over a sip trunk that involves more than one name, i.e. Lync interop using OCS relay)

As shown in the following example:

1. Log into the VCS as `root`.
2. Move to the application prompt and type `openssl`

```

10.1.7.59 - PuTTY
login as: root
Using keyboard-interactive authentication.
Password:
WARNING: Security alert: the TMS Agent database has the default password set
WARNING: Security alert: The admin user has the default password set
WARNING: Configuration warning: expected default link between the Default Zone and the Default Zone is missing
WARNING: Security alert: The root user has the default password set
WARNING: Security alert: the TMS Agent database has the default replication password set.
WARNING: Configuration warning: expected default link between the Default Zone and the Traversal Subzone is missing
WARNING: Configuration warning: expected default link between the Default Zone and the Cluster Subzone is missing
WARNING: Configuration warning: expected default link between the Traversal Subzone and the Default Zone is missing
~ # openssl
OpenSSL>
    
```

After you are in the application, as shown in the following example, instead of the file names that I used starting with **chabrow2**, you can name these files whatever you want, just leave the extension the same.

The following “ls” command where used is not required but shows that the relevant files were created and are present in the current directory.

GENERATING THE PRIVATE KEY=

```

OpenSSL> genrsa -out chabrow2.pem 1024
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
    
```

```

OpenSSL> exit
~ #
~ #
~ #
~ # ls -lart
total 2596
drwxr-xr-x 3 root root 4096 2010-11-17 10:12 app
drwxr-xr-x 5 root root 4096 2011-03-04 10:07 proxy-registration
drwxr-xr-x 2 root root 4096 2011-10-17 04:50 web
drwxr-xr-x 2 root root 4096 2011-10-17 04:50 lib
drwxr-xr-x 2 root root 4096 2011-10-17 05:00 certs
drwxr-xr-x 2 root root 4096 2011-12-16 11:57 images
drwxr-xr-x 4 root root 4096 2011-12-16 11:57 tbl
drwx----- 2 root root 16384 2012-02-23 16:00 lost+found
    
```

```
drwxr-xr-x 23 root root 4096 2012-02-23 16:00 ..
drwxr-xr-x 2 root root 4096 2012-02-23 16:03 ivy
drwxr-xr-x 2 root root 4096 2012-02-23 16:03 bramble
drwxr-xr-x 4 root root 4096 2012-02-23 16:03 management
drwxr-xr-x 6 root root 4096 2012-02-23 16:03 upgrade
drwxr-xr-x 4 root root 4096 2012-02-23 16:04 log
drwxrwxrwx 5 root root 4096 2012-02-23 16:05 crash
drwxr-xr-x 10 root root 4096 2012-02-23 16:19 provisioning
-rw-r--r-- 1 root root 1007478 2012-03-21 10:27 xlite-test.pcap
-rw-r--r-- 1 root root 1536670 2012-03-21 10:40 xlite-test.pcap2
drwxr-xr-x 8 root root 4096 2012-04-03 13:40 etc
-rw----- 1 root root 635 2012-04-03 14:21 .bash_history
drwxr-xr-x 15 root root 4096 2012-04-10 09:07 persistent
-rw----- 1 root root 1024 2012-04-10 09:35 .rnd
-rw-r--r-- 1 root root 887 2012-04-10 09:35 chabrow2.pem
drwxr-xr-x 19 root root 4096 2012-04-10 09:35 .
```

THE FOLLOWING COMMAND USES THE ABOVE CREATED KEY TO PRODUCE THE CERTIFICATE REQUEST.

```
OpenSSL> req -new -key chabrow2.pem -out chabrow2certcsr.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
```

What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

```
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:NC
Locality Name (eg, city) []:RTP
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco
Organizational Unit Name (eg, section) []:TAC
Common Name (eg, YOUR name) []:vcs1.chabrow2.local ← (PLEASE NOTE NEEDS TO FULLY
RESOLVABLE FQDN HERE)
Email Address []:chabrow2@cisco.com
```

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

```
OpenSSL> exit
~ #
~ #
~ # ls -lart
total 2600
drwxr-xr-x 3 root root 4096 2010-11-17 10:12 app
drwxr-xr-x 5 root root 4096 2011-03-04 10:07 proxy-registration
drwxr-xr-x 2 root root 4096 2011-10-17 04:50 web
drwxr-xr-x 2 root root 4096 2011-10-17 04:50 lib
drwxr-xr-x 2 root root 4096 2011-10-17 05:00 certs
drwxr-xr-x 2 root root 4096 2011-12-16 11:57 images
drwxr-xr-x 4 root root 4096 2011-12-16 11:57 tbl
drwx----- 2 root root 16384 2012-02-23 16:00 lost+found
drwxr-xr-x 23 root root 4096 2012-02-23 16:00 ..
```

```
drwxr-xr-x 2 root root 4096 2012-02-23 16:03 ivy
drwxr-xr-x 2 root root 4096 2012-02-23 16:03 bramble
drwxr-xr-x 4 root root 4096 2012-02-23 16:03 management
drwxr-xr-x 6 root root 4096 2012-02-23 16:03 upgrade
drwxr-xr-x 4 root root 4096 2012-02-23 16:04 log
drwxrwxrwx 5 root root 4096 2012-02-23 16:05 crash
drwxr-xr-x 10 root root 4096 2012-02-23 16:19 provisioning
-rw-r--r-- 1 root root 1007478 2012-03-21 10:27 xlite-test.pcap
-rw-r--r-- 1 root root 1536670 2012-03-21 10:40 xlite-test.pcap2
drwxr-xr-x 8 root root 4096 2012-04-03 13:40 etc
-rw----- 1 root root 635 2012-04-03 14:21 .bash_history
drwxr-xr-x 15 root root 4096 2012-04-10 09:07 persistent
-rw----- 1 root root 1024 2012-04-10 09:35 .rnd
-rw-r--r-- 1 root root 887 2012-04-10 09:35 chabrow2.pem
-rw-r--r-- 1 root root 696 2012-04-10 09:41 chabrow2certcsr.pem
drwxr-xr-x 19 root root 4096 2012-04-10 09:41 .
```

THE FOLLOWING COMMAND DISPLAYS CONTENTS OF CERTIFICATE REQUEST—

```
~ # more chabrow2certcsr.pem
-----BEGIN CERTIFICATE REQUEST-----
MIIBYDCCATECAQAwwYcxZAJBgNVBAYTAIVTMQswCQYDVQQIDAJQzEMMAoGA1UE
BwwDUIRQM4wDAYDVQQKDAVDaXNjbzEMMAoGA1UECwwDVEFDMRwwGgYDVQQDBN2
Y3MxLmNoYWJyb3cyLmxvY2FsMSEwHwYJKoZIhvcNAQkBFhJjaGFicm93MkBJaXNj
by5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANphU8KVa3iPHoOAY+SF
8XVhA+CyY82XHqGbx6H28/ID+f77UVIFV8Yfe+9KfumjFLBwCKgPZVXPPdNslau4
8gZdn6LDZb+M2qTWWJZB33+3kWFqL7rMElyYLhLarJZy7maAGSkFT2QHSZhlcpR
wbzV95wYd/7yhk7RvLbi+qSLAgMBAAGgADANBgkqhkiG9w0BAQUFAAOBgQA/H+Xi
aBPGoOr3j942UcoNwMiO1OpJ/SWUusprEEOpR+Excii3kRgyOASjW015JwFtCvP
rYkudlw2lz69t1c9ilPMWBMXUuiaulc6clnxruCpP+l83xClt0fgyUHIYPpf5I73
5YQBv0OE1S2mQ6C/ITOTsQG/ao3Kt/aWYIcGgQ==
-----END CERTIFICATE REQUEST-----
~ #
~ #
~ #
```

3. As shown in the following example, copy the entire certificate, including the beginning and ending certificate lines to paste into the certificate request page of your CA.

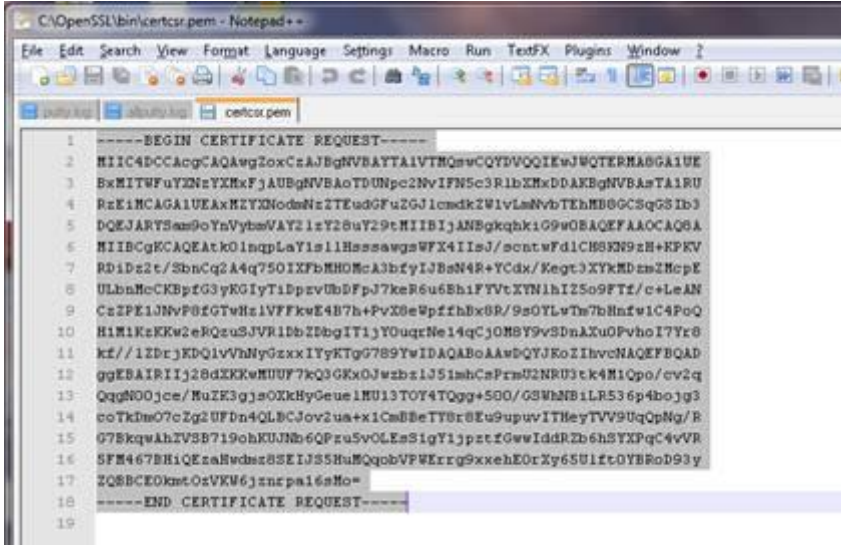


Figure 11 - Openssl already present on the VCS

4. If your CA is Microsoft, you need to have an admin login to take you to this page. If your CA is another company, have them take you to the certificate request page
5. To paste the request you copied into the certificate request page, complete the following steps:
 - c. Go to the **Certificate Services** page of your CA.
 - d. On the **Welcome** page, select **Request a Certificate**.

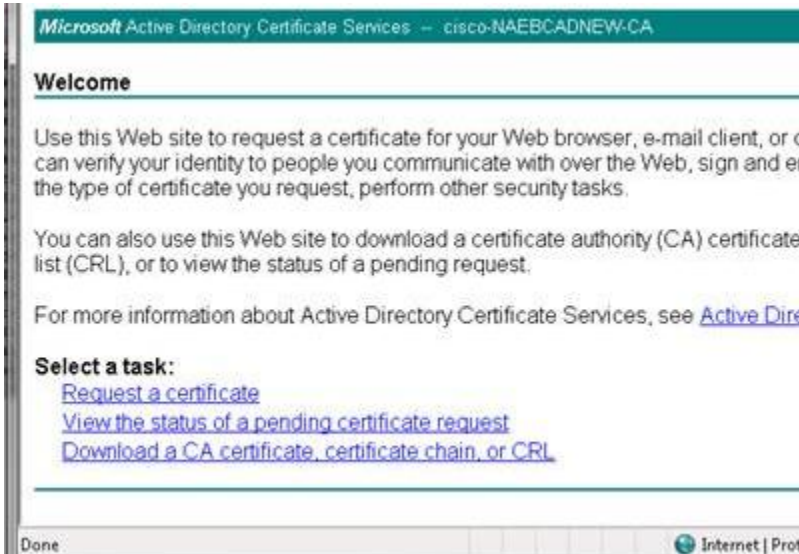


Figure 12 - Microsoft Active Directory Certificate Services

- e. On the **Request a Certificate** page, select submit an **advanced certificate request**.

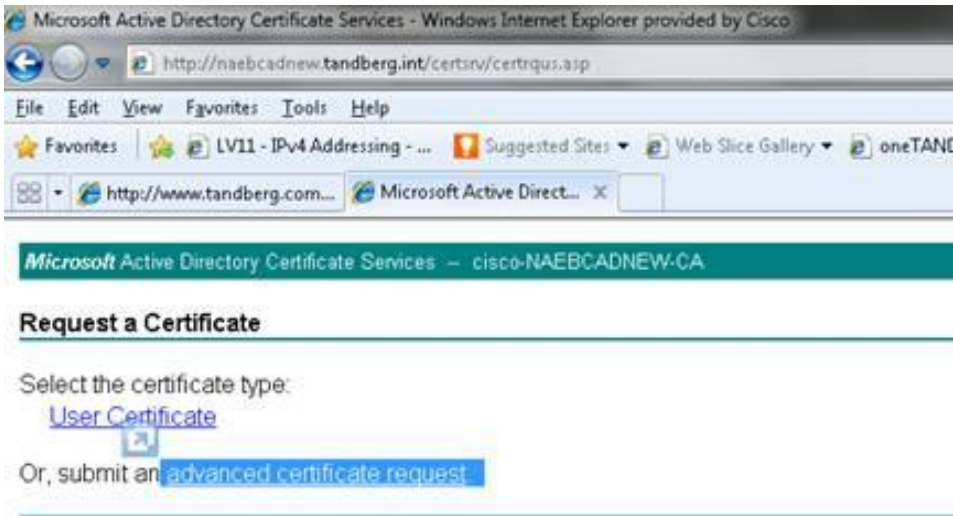


Figure 13 - Request a Certificate

- f. On the **Advanced Certificate Request** page, select **Create and submit a request to this CA.**

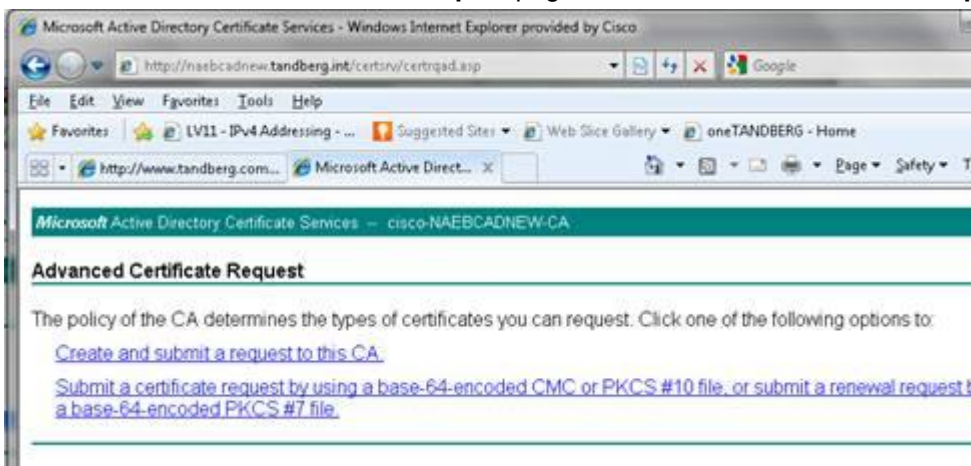


Figure 14 - Advanced Certificate Request

- g. On the **Submit a Certificate Request or Renewal Request** page, paste the request you copied into the **Saved Request** space.



Figure 15 - Submit a Certificate Request or Renewal Request

- h. Under **Certificate Template**, select the dropdown menu and select **Web Server**.

Microsoft Active Directory Certificate Services -- chabrow2-DC-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC

Saved Request:

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

Certificate Template:

Additional Attributes:

Attributes:

Web Server

Administrator

Basic EFS

EFS Recovery Agent

User

Subordinate Certification Authority

Web Server

Submit >

- i. The following example shows the *Certificate Request or Renewal Request*.with the beginning and ending lines pasted into it.

Microsoft Active Directory Certificate Services -- cisco-NAEBCADNEW-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 request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

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

```

coTxDm07cZg2UFdn4QLBcJov2ua+x1Cn8BeTY8r8
G7BkquAhZVSB719ohKUJNb6QPzuSvOLEaSlgY1jp
5FM467BH1QEzaHvdmz8SEIJS5HuMqobVPWErg9
ZQBBCE0kacOzVKW6jzncpa16aMo=
-----END CERTIFICATE REQUEST-----
    
```

Certificate Template:

Web Server

Additional Attributes:

Internet | Protected Mode: On

Figure 16 - Submit a Certificate Request or Renewal Request

6. On the Certificate Issued page, select **Base 64**, then **Download certificate**.



Figure 17 - Certificate Issued

The certificate is issued in **.cer** format, which is fine for the VCS. You can change this to **.pem** format.

7. After you have both the private key and the certificate for the VCS, you need the CA certificate.
 - a. Go back to the main CA webpage and select **Download a CA certificate, certificate chain, or CRL**.



Figure 18 - Main Certificate Authority Page

- b. On the **Download a CA Certificate, Certificate Chain, or CRL**, select **Base 64**.



Figure 19 - Download a CA Certificate, Certificate Chain, or CRL

8. You can load the CA certificate to the VCS in **.cer** format or convert to **.pem**. Either works.

An easy way to accomplish this is to use winscp to connect to the VCS using root as shown in the following example and move the private key file from the VCS to your local pc

Winscp can be downloaded for free at below link --

<http://winscp.net/download/winscp438setup.exe>

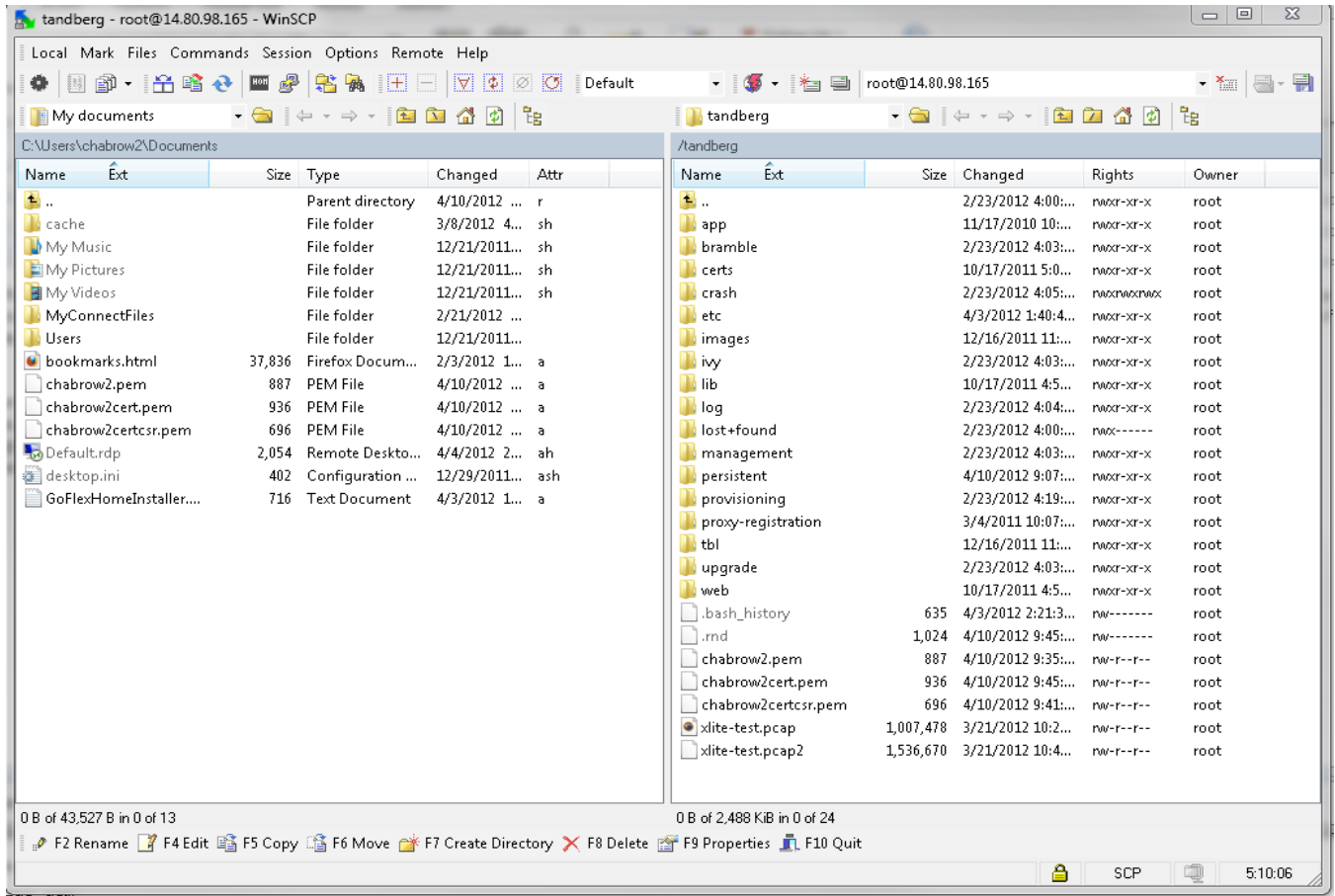


Figure 20 - WinSCP

9. After you have both the private key and the certificate for the VCS, you need the CA certificate.
 - a. Go back to the main CA webpage and select **Download a CA certificate, certificate chain, or CRL**.

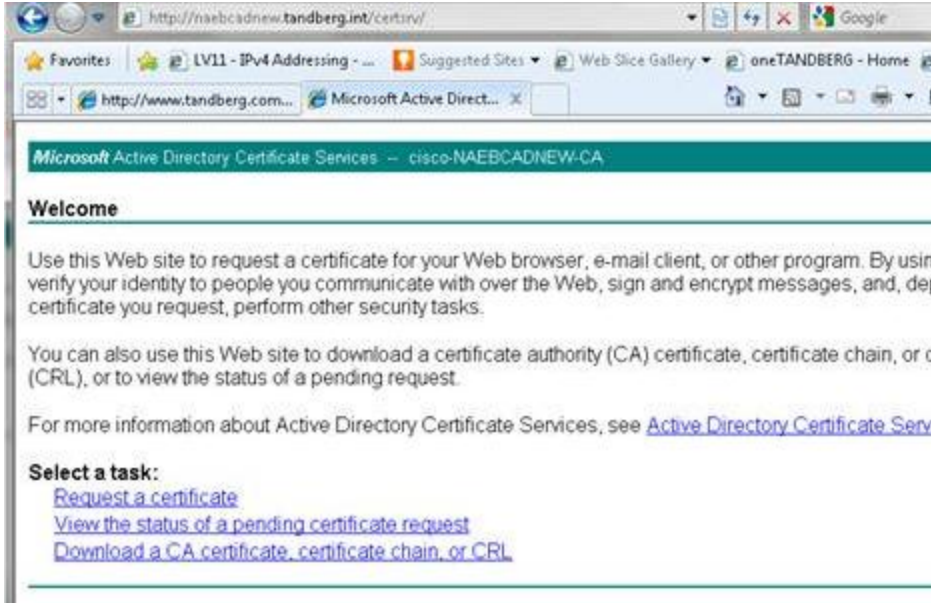


Figure 21 - Main Certificate Authority Page

- b. On the **Download a CA Certificate, Certificate Chain, or CRL**, select **Base 64**.



Figure 22 - Download a CA Certificate, Certificate Chain, or CRL

10. You can load the CA certificate to the VCS in **.cer** format or convert to **.pem**. Either works. You can also load the private key and VCS Certificate provided via the VCS web interface.

2.3 Creating a self-signed certificate

On the **OpenSSL** interface on the VCS, you need to login as root.

If you want to create a self-signed certificate, you follow the same steps with one exception. Instead of sending the **certcsr.pem** file to a CA, you process the file yourself, and you can use the **openssl** right there on the VCS if you so choose.

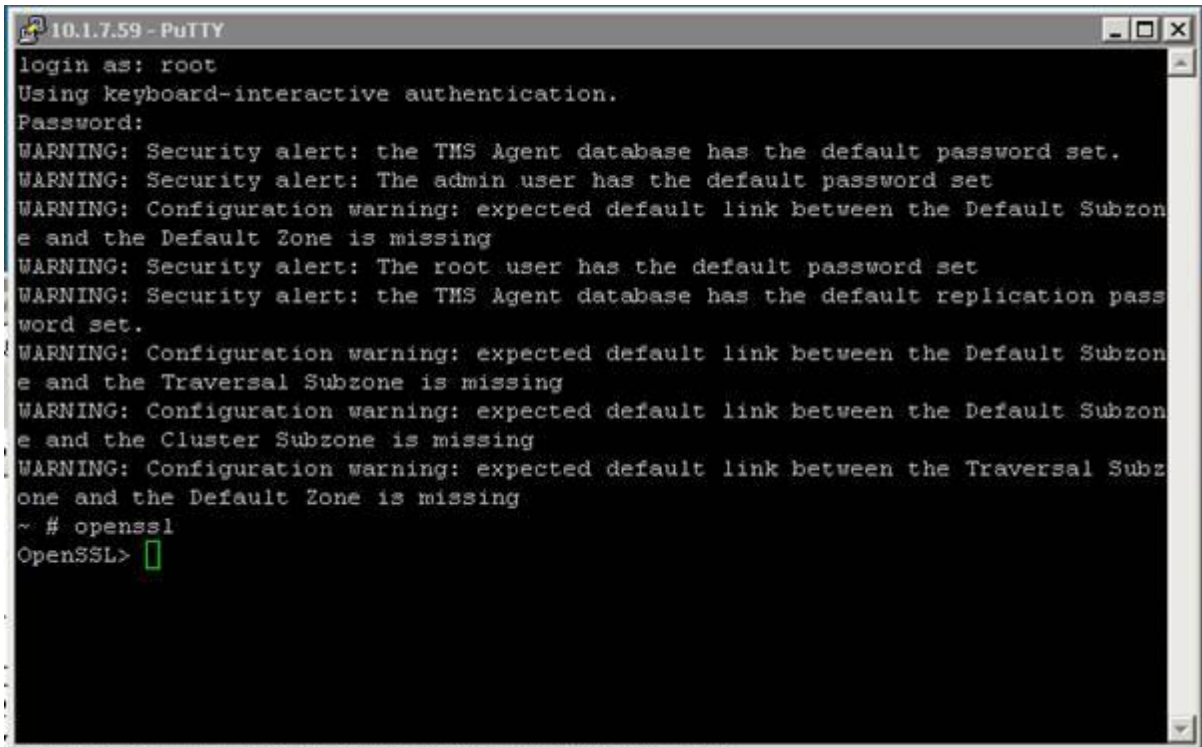


Figure 23 - Login Screen on VCS

NOTE: Once logged in as **root** (you cannot be logged in as admin), instead of the file names shown in the following example--starting with **chabrow2**--name these files whatever you want. However, you must leave the extension the same.

The following "ls" command, where used, is also not required but done to show that the relevant files were created and are present in the current directory.

```

GENERATING THE PRIVATE KEY=
OpenSSL> genrsa -out chabrow2.pem 1024
Generating RSA private key, 1024 bit long modulus
....++++++
.....++++++
e is 65537 (0x10001)
    
```

```

OpenSSL> exit
~ #
~ #
~ #
~ # ls -lart
total 2596
drwxr-xr-x 3 root root 4096 2010-11-17 10:12 app
    
```

```
drwxr-xr-x 5 root root 4096 2011-03-04 10:07 proxy-registration
drwxr-xr-x 2 root root 4096 2011-10-17 04:50 web
drwxr-xr-x 2 root root 4096 2011-10-17 04:50 lib
drwxr-xr-x 2 root root 4096 2011-10-17 05:00 certs
drwxr-xr-x 2 root root 4096 2011-12-16 11:57 images
drwxr-xr-x 4 root root 4096 2011-12-16 11:57 tbl
drwx----- 2 root root 16384 2012-02-23 16:00 lost+found
drwxr-xr-x 23 root root 4096 2012-02-23 16:00 ..
drwxr-xr-x 2 root root 4096 2012-02-23 16:03 ivy
drwxr-xr-x 2 root root 4096 2012-02-23 16:03 bramble
drwxr-xr-x 4 root root 4096 2012-02-23 16:03 management
drwxr-xr-x 6 root root 4096 2012-02-23 16:03 upgrade
drwxr-xr-x 4 root root 4096 2012-02-23 16:04 log
drwxrwxrwx 5 root root 4096 2012-02-23 16:05 crash
drwxr-xr-x 10 root root 4096 2012-02-23 16:19 provisioning
-rw-r--r-- 1 root root 1007478 2012-03-21 10:27 xlite-test.pcap
-rw-r--r-- 1 root root 1536670 2012-03-21 10:40 xlite-test.pcap2
drwxr-xr-x 8 root root 4096 2012-04-03 13:40 etc
-rw----- 1 root root 635 2012-04-03 14:21 .bash_history
drwxr-xr-x 15 root root 4096 2012-04-10 09:07 persistent
-rw----- 1 root root 1024 2012-04-10 09:35 .rnd
-rw-r--r-- 1 root root 887 2012-04-10 09:35 chabrow2.pem
drwxr-xr-x 19 root root 4096 2012-04-10 09:35 .
```

THE BELOW COMMAND USES THE ABOVE CREATED KEY TO PRODUCE THE CERTIFICATE REQUEST.

```
OpenSSL> req -new -key chabrow2.pem -out chabrow2certcsr.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
```

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:US

State or Province Name (full name) [Some-State]:NC

Locality Name (eg, city) []:RTP

Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco

Organizational Unit Name (eg, section) []:TAC

Common Name (eg, YOUR name) []:vcs1.chabrow2.local ← (PLEASE NOTE NEEDS TO FULLY RESOLVABLE FQDN HERE)

Email Address []:chabrow2@cisco.com

Please enter the following 'extra' attributes
to be sent with your certificate request

A challenge password []:

An optional company name []:

```
OpenSSL> exit
```

```
~ #
```

```
~ #
```

```

~ # ls -lart
total 2600
drwxr-xr-x 3 root root 4096 2010-11-17 10:12 app
drwxr-xr-x 5 root root 4096 2011-03-04 10:07 proxy-registration
drwxr-xr-x 2 root root 4096 2011-10-17 04:50 web
drwxr-xr-x 2 root root 4096 2011-10-17 04:50 lib
drwxr-xr-x 2 root root 4096 2011-10-17 05:00 certs
drwxr-xr-x 2 root root 4096 2011-12-16 11:57 images
drwxr-xr-x 4 root root 4096 2011-12-16 11:57 tbl
drwx----- 2 root root 16384 2012-02-23 16:00 lost+found
drwxr-xr-x 23 root root 4096 2012-02-23 16:00 ..
drwxr-xr-x 2 root root 4096 2012-02-23 16:03 ivy
drwxr-xr-x 2 root root 4096 2012-02-23 16:03 bramble
drwxr-xr-x 4 root root 4096 2012-02-23 16:03 management
drwxr-xr-x 6 root root 4096 2012-02-23 16:03 upgrade
drwxr-xr-x 4 root root 4096 2012-02-23 16:04 log
drwxrwxrwx 5 root root 4096 2012-02-23 16:05 crash
drwxr-xr-x 10 root root 4096 2012-02-23 16:19 provisioning
-rw-r--r-- 1 root root 1007478 2012-03-21 10:27 xlite-test.pcap
-rw-r--r-- 1 root root 1536670 2012-03-21 10:40 xlite-test.pcap2
drwxr-xr-x 8 root root 4096 2012-04-03 13:40 etc
-rw----- 1 root root 635 2012-04-03 14:21 .bash_history
drwxr-xr-x 15 root root 4096 2012-04-10 09:07 persistent
-rw----- 1 root root 1024 2012-04-10 09:35 .rnd
-rw-r--r-- 1 root root 887 2012-04-10 09:35 chabrow2.pem
-rw-r--r-- 1 root root 696 2012-04-10 09:41 chabrow2certcsr.pem
drwxr-xr-x 19 root root 4096 2012-04-10 09:41 .

```

BELOW COMMAND SIMPLY DISPLAYS CONTENTS OF CERT REQUEST—

```

~ # more chabrow2certcsr.pem
-----BEGIN CERTIFICATE REQUEST-----
MIIBYDCCATECAQAwwGyYcXZAJBgNVBAYTAIVTMQswCQYDVQQIDAJQzEMMAoGA1UE
BwwDUIRQM4wDAYDVQQKDAVDaXNjbzEMMAoGA1UECwwDVEFDMRwwGgYDVQQDDBN2
Y3MxLmNoYWVJb3cyLmXvY2FsMSEwHwYJKoZIhvcNAQkBFhJjaGFicm93MkBJaXNj
by5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANphU8KVa3iPHoOAY+SF
8XVhA+CyY82XHqGbx6H28/ID+f77UVIFV8Yfe+9KfumjFLBwCKgPZVXPPdNslau4
8gZdn6LDZb+M2qTWWJZB33+3kWFqL7rMElyYLhLarJZy7maAGSkFT2QHSZhlcpR
wbzV95wYd/7yhk7RvLbi+qSLAgMBAAGgADANBgkqhkiG9w0BAQUFAAOBGA/H+Xi
aBPGOOr3j942UcoNwMiO1OpJ/SWUusprEEOpR+Excii3kRgyOASjW015JwFtCvP
rYkudlw2lz69t1c9ilPMWBMXUuiaulc6clnxruCpP+l83xClt0fgyUHIYPpf5I73
5YQBv0OE1S2mQ6C/ITOTSQG/ao3Kt/aWYIcGgQ==
-----END CERTIFICATE REQUEST-----
~ #
~ #
~ #

```

NOW YOU CAN RUN THE COMMAND TO USE THE KEY YOU GENERATED KEY ALONG WITH THE GENERATED CERT REQUEST TO CREATE A CERT. YOU DO NOT HAVE TO BE AT THE OPENSsl PROMPT TO RUN THIS COMMAND AS PER BELOW. THE DAYS VALUE BELOW CAN BE WHATEVER PERIOD THE CERT SHOULD BE GOOD FOR —

Creating a Cisco TelePresence Video Communication Server (VCS) Certificate

```
~ # openssl x509 -req -days 360 -in chabrow2certcsr.pem -signkey chabrow2.pem -out
chabrow2cert.pem
Signature ok
subject=/C=US/ST=NC/L=RTP/O=Cisco/OU=TAC/CN=vcs1.chabrow2.local/emailAddress=chabrow2@ci
sco.com
Getting Private key
~ #
~ #
~ # ls -lart
total 2604
drwxr-xr-x 3 root root 4096 2010-11-17 10:12 app
drwxr-xr-x 5 root root 4096 2011-03-04 10:07 proxy-registration
drwxr-xr-x 2 root root 4096 2011-10-17 04:50 web
drwxr-xr-x 2 root root 4096 2011-10-17 04:50 lib
drwxr-xr-x 2 root root 4096 2011-10-17 05:00 certs
drwxr-xr-x 2 root root 4096 2011-12-16 11:57 images
drwxr-xr-x 4 root root 4096 2011-12-16 11:57 tbl
drwx----- 2 root root 16384 2012-02-23 16:00 lost+found
drwxr-xr-x 23 root root 4096 2012-02-23 16:00 ..
drwxr-xr-x 2 root root 4096 2012-02-23 16:03 ivy
drwxr-xr-x 2 root root 4096 2012-02-23 16:03 bramble
drwxr-xr-x 4 root root 4096 2012-02-23 16:03 management
drwxr-xr-x 6 root root 4096 2012-02-23 16:03 upgrade
drwxr-xr-x 4 root root 4096 2012-02-23 16:04 log
drwxrwxrwx 5 root root 4096 2012-02-23 16:05 crash
drwxr-xr-x 10 root root 4096 2012-02-23 16:19 provisioning
-rw-r--r-- 1 root root 1007478 2012-03-21 10:27 xlite-test.pcap
-rw-r--r-- 1 root root 1536670 2012-03-21 10:40 xlite-test.pcap2
drwxr-xr-x 8 root root 4096 2012-04-03 13:40 etc
-rw----- 1 root root 635 2012-04-03 14:21 .bash_history
drwxr-xr-x 15 root root 4096 2012-04-10 09:07 persistent
-rw-r--r-- 1 root root 887 2012-04-10 09:35 chabrow2.pem
-rw-r--r-- 1 root root 696 2012-04-10 09:41 chabrow2certcsr.pem
drwxr-xr-x 19 root root 4096 2012-04-10 09:44 .
-rw----- 1 root root 1024 2012-04-10 09:45 .rnd
-rw-r--r-- 1 root root 936 2012-04-10 09:45 chabrow2cert.pem
```

BELOW COMMAND DISPLAYS CONTENTS OF THE CERT—

```
~ # more chabrow2cert.pem
-----BEGIN CERTIFICATE-----
MIICHzCCAfACCQDCAAb5WW4vsDANBbkqkhiG9w0BAQUFADCBhzELMAkGA1UEBhMC
VVMxCzAJBgNVBAGMAk5DMQwwCgYDVQQHDANSVFAXDjAMBgNVBAoMBUNpc2NvMQww
CgYDVQQLDANUQUUMxHDAaBgNVBAMME3ZjczEuY2hhYnJvdzlibG9jYWwxITAFBgkq
hkiG9w0BCQEWEmNoYWJyb3cyQGNpc2NvLmNvbTAeFw0xMjA0MTAxMzQ1MDhaFw0x
MzA0MDUxMzQ1MDhaMIGHMQswCQYDVQQGEwJVUzELMAkGA1UECAwCTMxMzQ1MDha
BAcMA1JUUDEOMAwGA1UECgwFQ2l2Y28xDDAKBgNVBAsMA1RBQzEcMBoGA1UEAwwT
dmNzMS5jaGFicm93Mi5sb2NhbnRDEhMB8GCSqGSIb3DQEJARYSY2hhYnJvdzJAY2l2
Y28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDaYVPCiWt4jx6DgGPK
hfF1YQPgsmPNlx6hm8eh9vPyA/n++1FSBVfGH3vvSn7poxSwcAioD2VVzz3TbCGr
uPIGXZ+iw2W/jNqk1liWQd9/t5Fhai+6zBJcmC4S2qyWcu5mgBkpBU9kB0mYZSHK
UcG81fecGHf+8oZO0by25fqkiwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAH3FulsS
Vd+FoBc4RTTCX0tTjWovRlJzetz1j4maMklicJFT46Lx+mjNnwWml/qn2SntnllH
ZfWabOKfcdFZ/L3AnjhoR3ZQWND5KXZht9PDrAaZOwLTx4MgHcMVwwfth3WP2e2
Rh3sNnMOOK9RZACGbXo66D69Wacz3DaJsxBy
-----END CERTIFICATE-----
```


Creating a Cisco TelePresence Video Communication Server (VCS) Certificate

~ #
~ #
~ #

PLEASE NOTE THAT ALTHOUGH PRODUCED ON THE VCS, THE VCS WILL NOT AUTOMATICALLY APPLY THE CERT. YOU NEED TO GO INTO THE VCS WEB INTERFACE AND POINT TO THE CREATED KEY FILE (DETAILS ON NEXT PAGE) AS WELL AS THE CREATED CERT FILE.

Therefore, in this example case, the file names you are uploading to VCS are **chabrow2.pem**, which is the name of the key file and **chabrow2cert.pem** which is the file name of the certificate file. However, these will be whatever you named them when you created them.

PRIVATE KEY FILE = chabrow2.pem
SERVER CERTIFICATE FILE = chabrow2cert.pem

CISCO Cisco TelePresence Video Communication Server Control

Status System VCS configuration Applications **Maintenance** [Help](#) [Logout](#)

Security certificates You are here: [Maintenance](#) > [Certificate management](#) > [Security certificate](#)

Trusted CA certificate

Select the file containing trusted CA certificates

CA certificate PEM File

Server certificate data

Select the server private key file

Select the server certificate file

Server certificate PEM File

Currently loaded certificate expires on Aug 28 2029

Figure 24 - Security certificate

Creating a Cisco TelePresence Video Communication Server (VCS) Certificate

An easy way to accomplish this is to use winscp to connect to the VCS using root as shown in the following example

Winscp can be downloaded for free at below link --

<http://winscp.net/download/winscp438setup.exe>

Move the files from the VCS to your local PC, point to them using the above VCS interface, then select the “Upload server certificate data” button

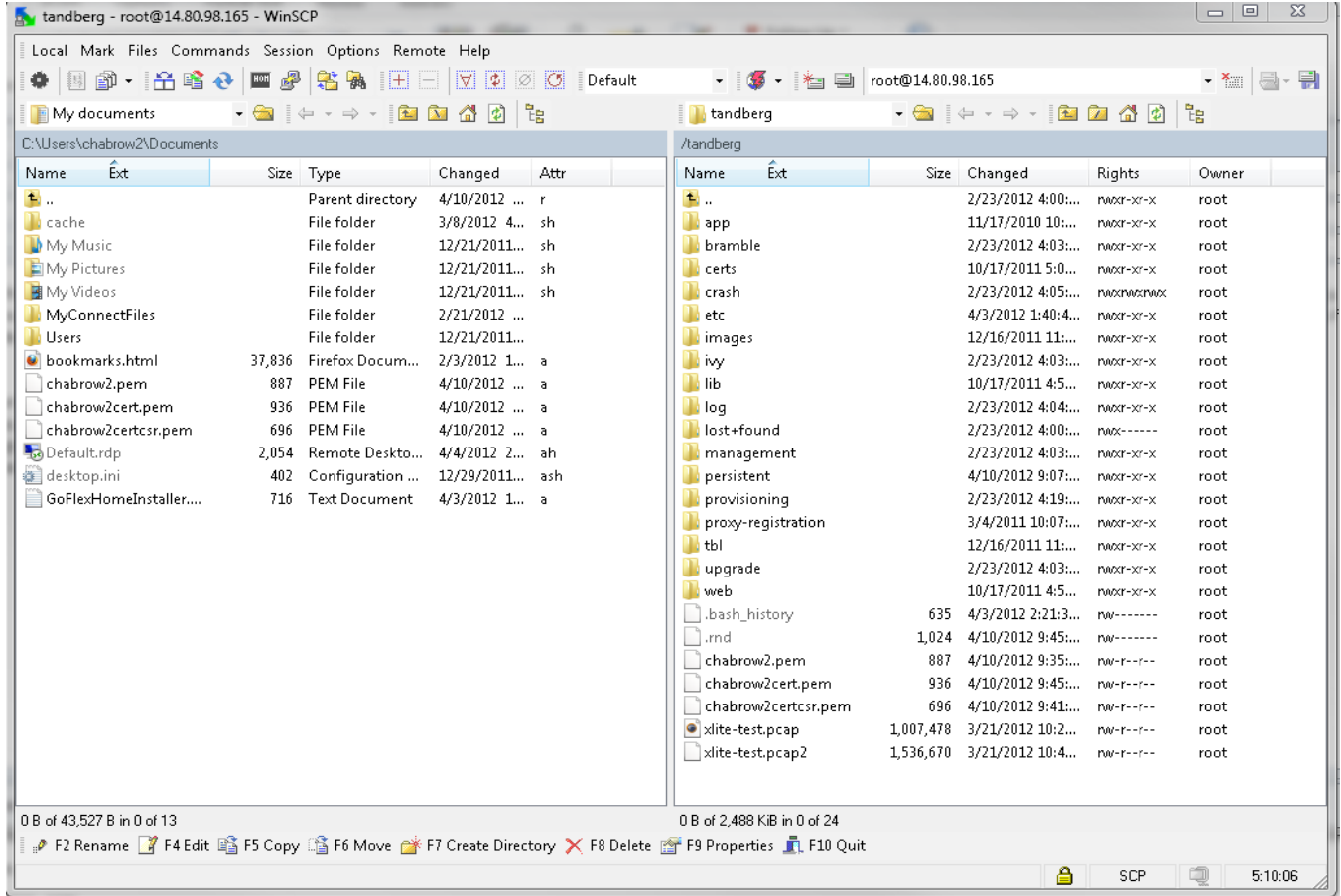


Figure 25 - WinSCP

Creating a Cisco TelePresence Video Communication Server (VCS) Certificate

To confirm that your created certificate is being used and not the default, look at the expiration date and confirm that it matches what was configured for the new cert.

The screenshot displays the Cisco TelePresence Video Communication Server Starter Pack Express configuration interface. The top navigation bar includes 'Status', 'System', 'VCS configuration', 'Applications', and 'Maintenance'. The 'Maintenance' section is active, and the breadcrumb trail shows 'You are here: Maintenance > Certificate management > Security certificates'. The 'Security certificates' section is divided into three main areas:

- Trusted CA certificate:** Includes a 'Browse...' button to select a file containing trusted CA certificates and a 'Show CA certificate' button. Below this are 'Upload CA certificate' and 'Reset to default CA certificate' buttons.
- Server certificate data:** This section is highlighted with a blue border. It contains:
 - 'Select the server private key file' with a 'Browse...' button.
 - 'Select the server certificate file' with a 'Browse...' button.
 - 'Server certificate' with a 'Show server certificate' button.
 - A field labeled 'Currently loaded certificate expires on' with the value 'Jun 13 2014', which is circled in red.Below this section are 'Upload server certificate data' and 'Reset to default server certificate' buttons.
- Related tasks:** Includes a link for 'Set up certificate revocation lists (CRLs)'.

Figure 26 - Server certificate date

APPENDIX -- LYNC/OCS INTEROP

If a certificate is needed for OCS/Lync interop as outlined in the following excerpt taken from the deployment guide:

“OCS/Lync gateway”: Generate and load private key, root certificate, and server certificate onto “OCS/Lync gateway” VCS Control (not needed if using a TCP connection)

Obtain and load Root CA certificate, server certificate and private key into the Cisco VCS.

Note: For mutual TLS authentication the server certificate must be capable of being used as a client certificate as well.

Either a single server certificate can be created to cover the “OCS/Lync gateway” cluster, or a server certificate can be created for each Cisco VCS. If the “OCS/Lync gateway” is a non-clustered VCS then use the section “Server certificate for each Cisco VCS”

Details on how to create certificates for VCS are documented in “Cisco VCS Deployment Guide – Certificate creation and use with Cisco VCS”.

Single server certificate that can be loaded into each cluster peer:

The certificate must specify:

- **Subject name:** the VCS cluster’s FQDN (DNS Local hostname concatenated with DNS Domain), e.g. *ocsvcs.ciscotp.com*
- **Subject Alternate Name:** a comma separated list of the VCS peers’ routable FQDNs e.g. *vcs01.ciscotp.com, vcs02.ciscotp.com*

Server certificate for each Cisco VCS:

A certificate must be created for each “OCS/Lync gateway” VCS; the certificate must specify:

- **Subject name:** the VCS peer’s FQDN e.g. *vcs01.ciscotp.com*

and if it is part of a cluster:

- **Subject Alternate Name:** the VCS cluster’s FQDN, e.g. *ocsvcs.ciscotp.com*

Load the certificates:

Load the certificates on the **Security certificates** page (**Maintenance > Certificate management > Security certificates**):

Please see the following guide for details on certificate creation

http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/Cisco_VCS_Certificate_Creation_and_Use_Deployment_Guide.pdf

In addition, as the VCS is treated by the Lync Server as a "Trusted Application Server" please reference below as well for Microsoft instructions on creating a certificate for "Trusted Application Servers".

<http://msdn.microsoft.com/en-us/library/hh347354.aspx>

End of Document