VCS Certificate Creation

VCS Certificate Creation
<Month> 2011 Edition

Table of Contents

List of Tables

List of Figures

1 Introduction

This document provides three options and instructions for creating a VCS certificate

1.1 Release Notes

Table 1 - Release Notes

Technical Change	Title(s) of Affected Section(s)	Changes Made By	Date

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 cert from your 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 Downloading and installing application

To create a certificate by downloading and installing either openssl or whatever application is used to generate certificate requests, complete the following steps:

1. Download **OpenSSL**, browse to the command line, and open the application.

http://www.openssl.org/ (Link to download OpenSSL)

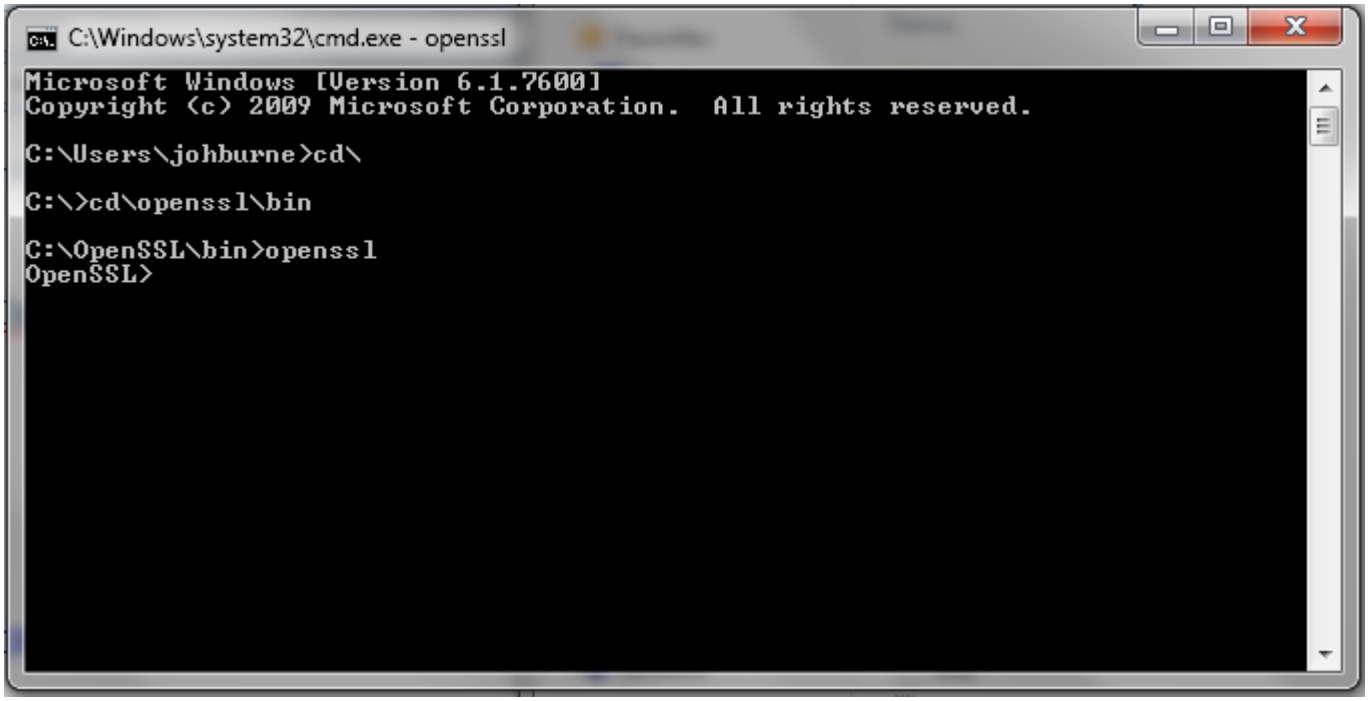


Figure 1 - Windows\system32\cmd.exe - openssl

2. At the **OpenSSL** prompt, type:

   `genrsa -out privatekey.pem 1024`

NOTE: The name **privatekey.pem** is the name of the privatekey you are generating. This could be **cocacolaprivkey.pem** for example.

3. If you've installed **openssl** on your windows pc, the **privatekey.pem** file will be stored in the bin directory
4. At the **OpenSSL** prompt type:

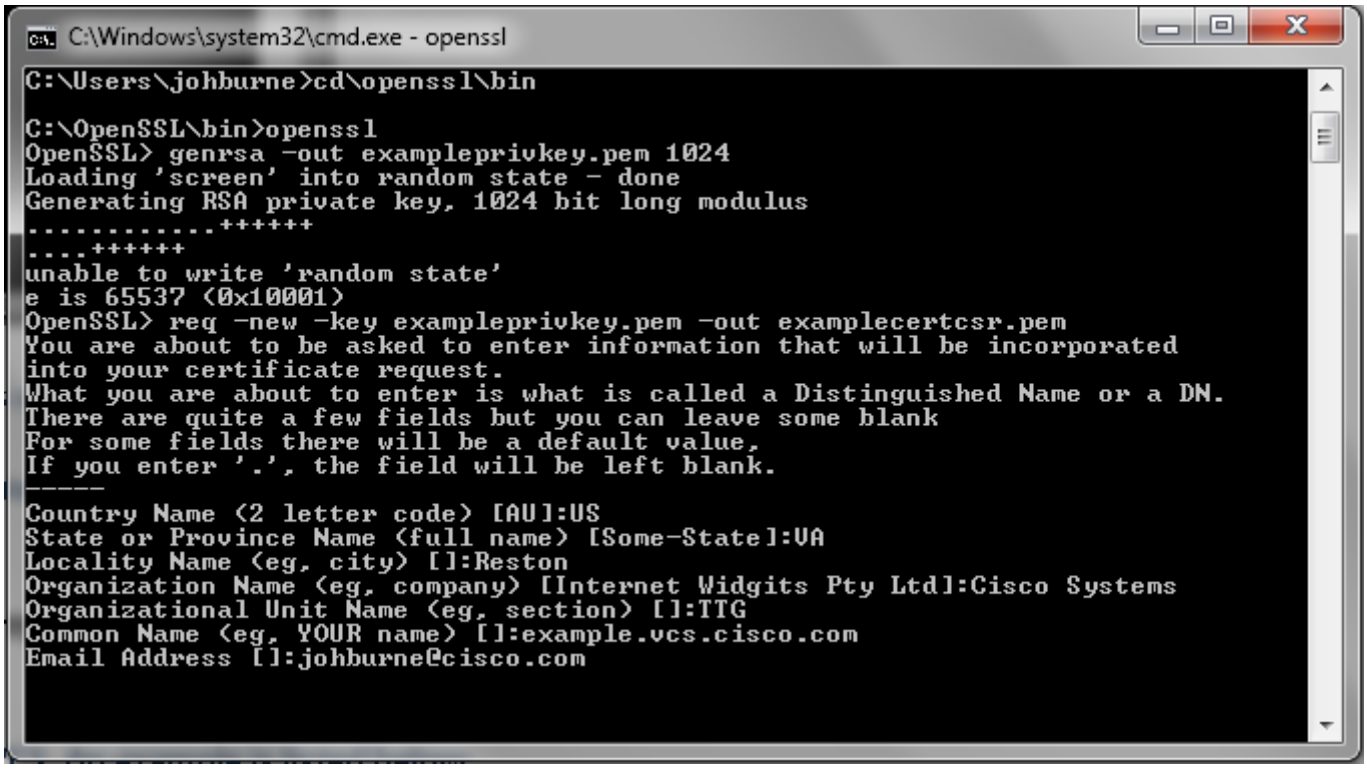
   `req -new -key privatekey.pem -out certcsr.pem`

   certcsr.pem is the certificate request submitted to your certificate authority (CA).

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

5. 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.



6. Go to the bin directory and find the **certcsr.pem** file that you generated. This is your certificate request.
7. Open the file with notepad or wordpad or notepad ++

8. 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.

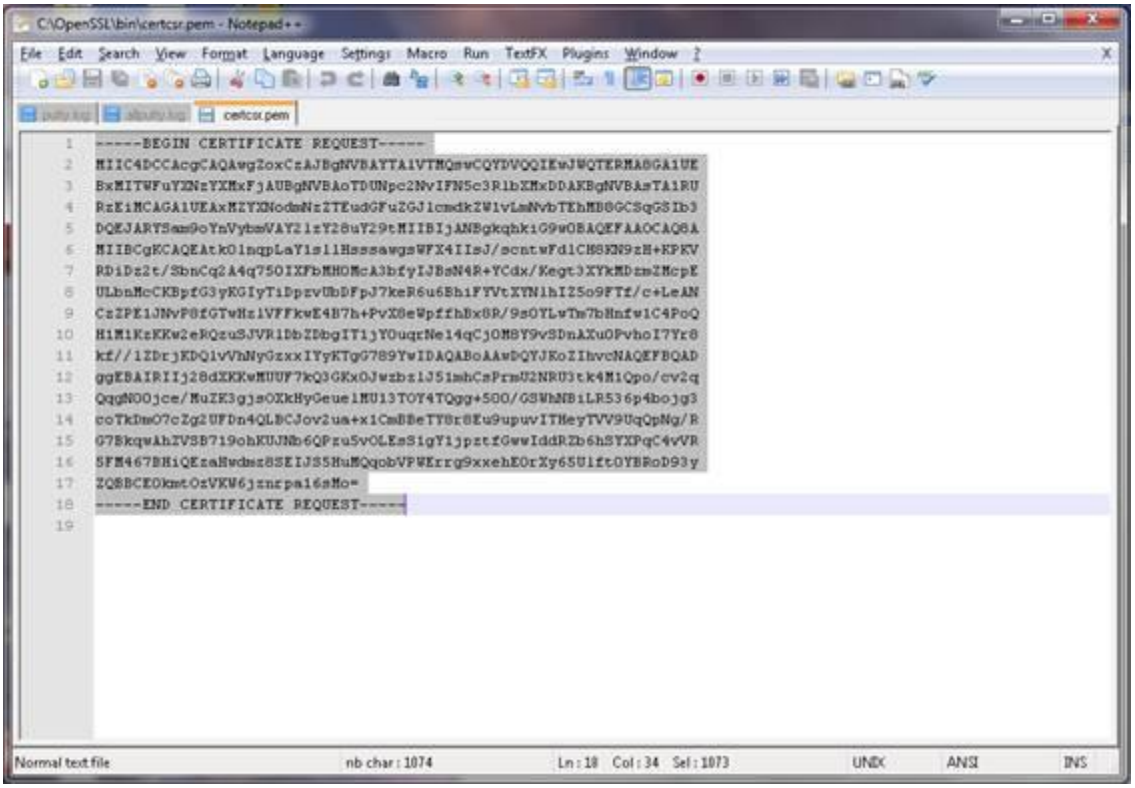


Figure 2 - OpenSSL

9. 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
10. 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 **Wecome** page, select **Request a Certificate**.

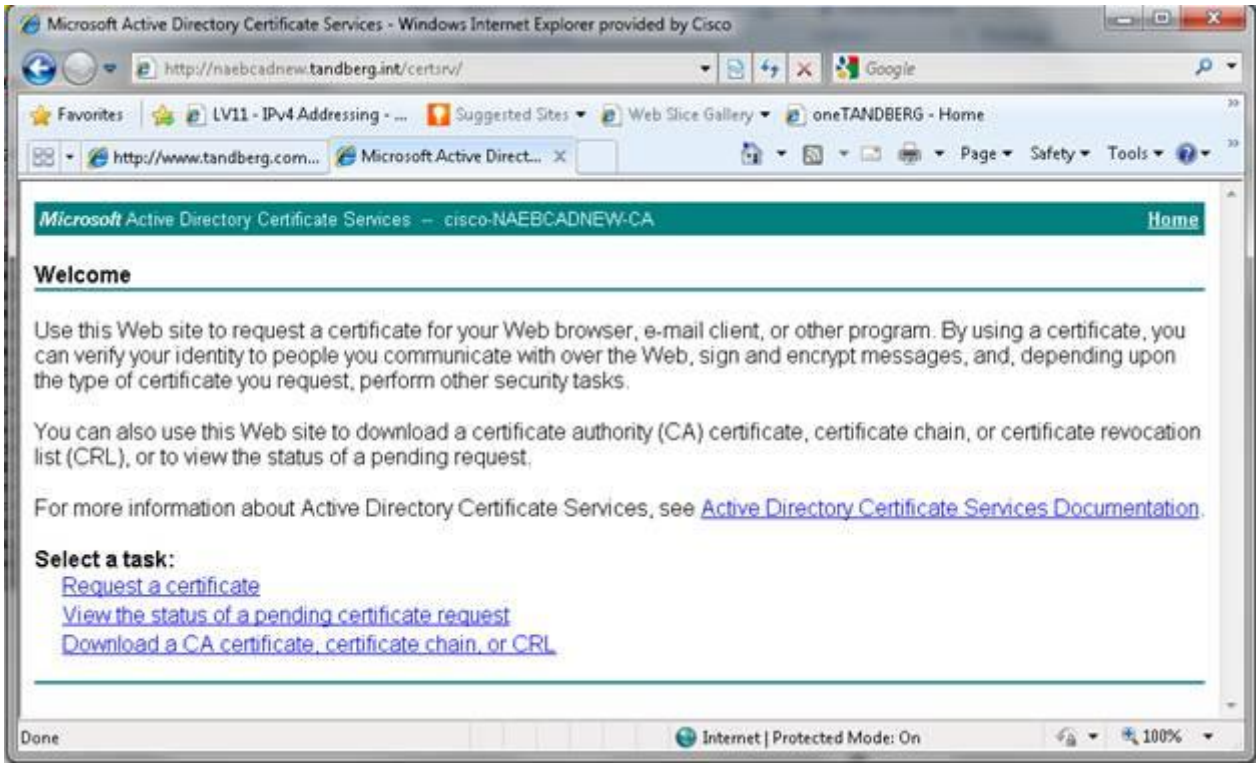


Figure 3 - Microsoft Active Directory Certificate Services

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

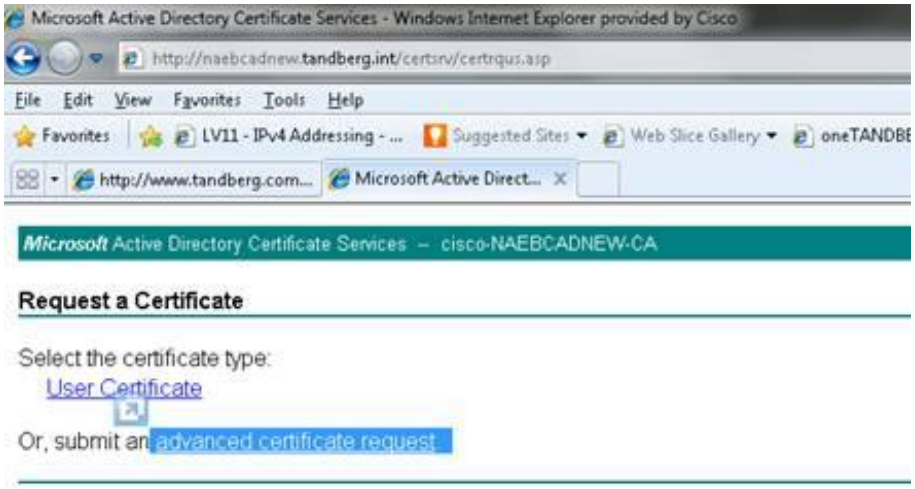


Figure 4 - Request a Certificate

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

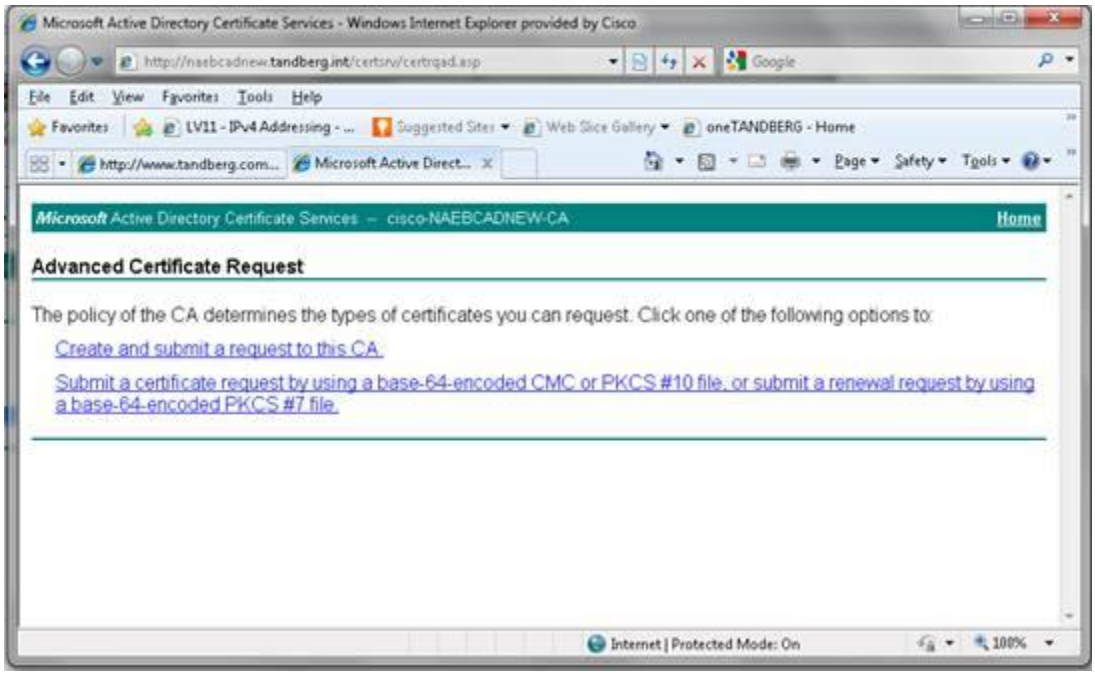


Figure 5 - Advanced Certificate Request

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

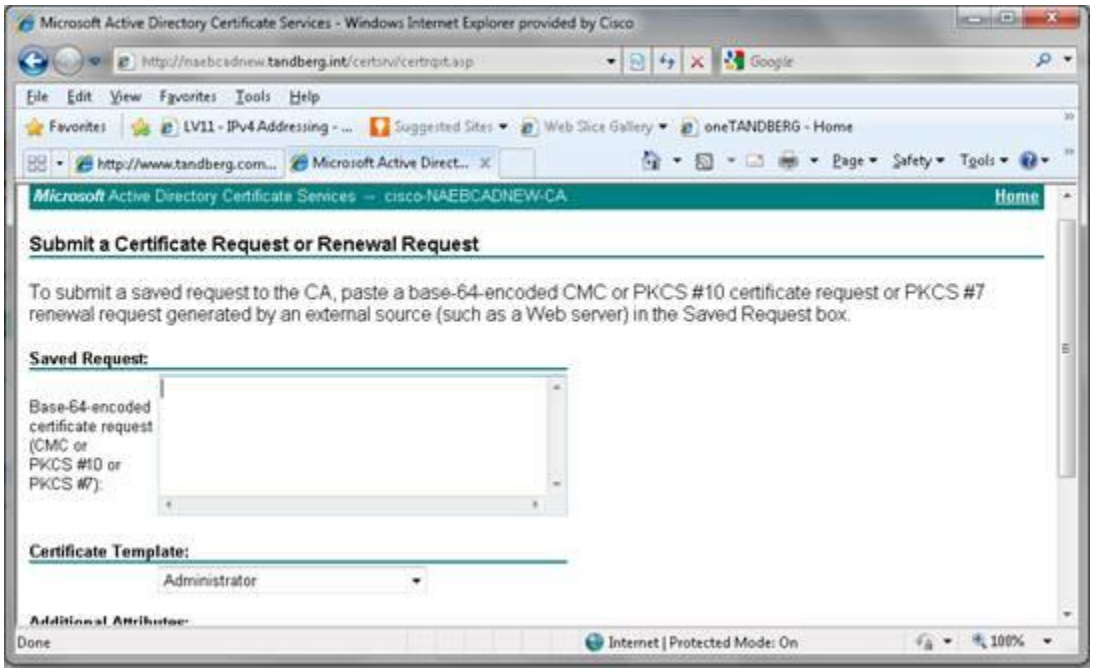
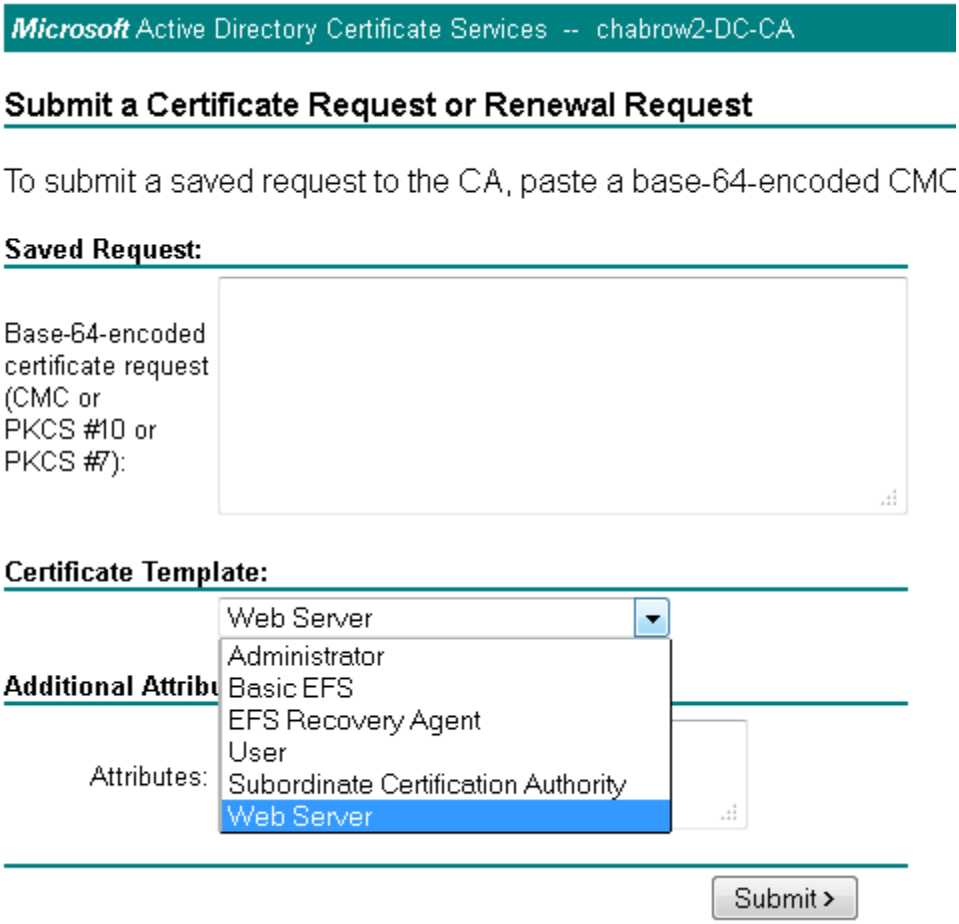


Figure 6 - Submit a Certificate Request or Renewal Request

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



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

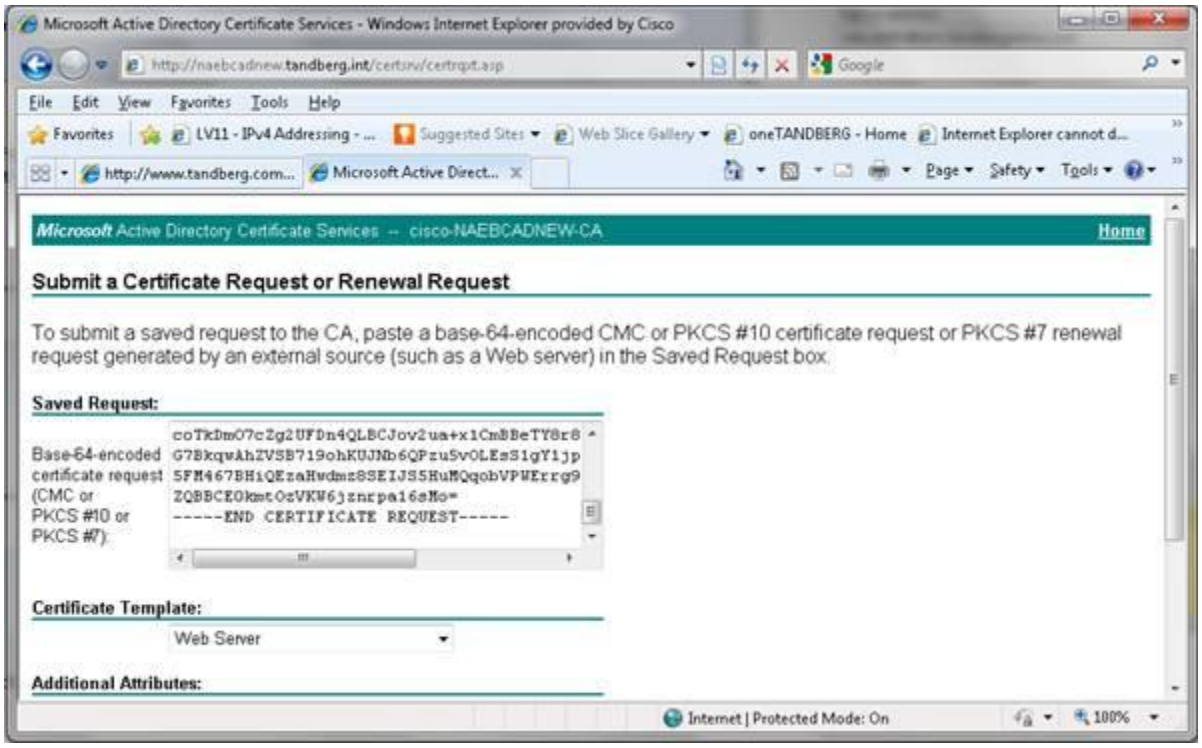


Figure 7 - Submit a Certificate Request or Renewal Request

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

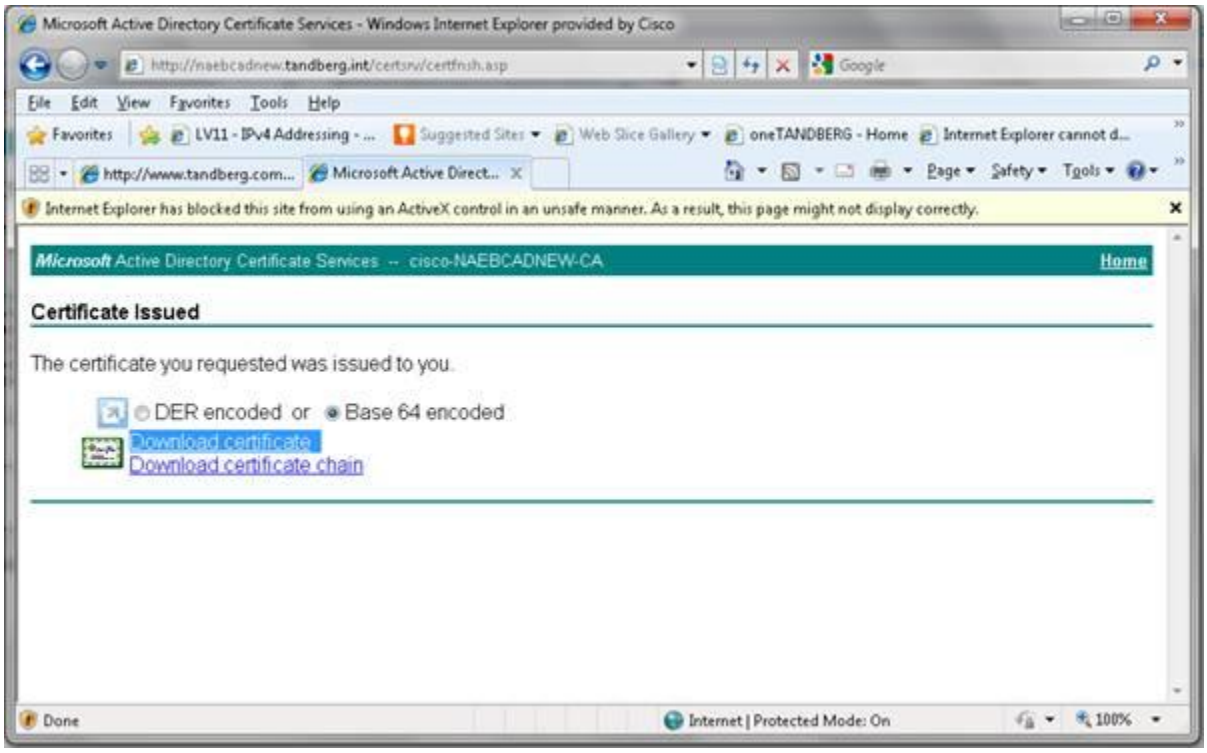


Figure 8 - Certificate Issued

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

12. 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, certficate chain, or CRL**.

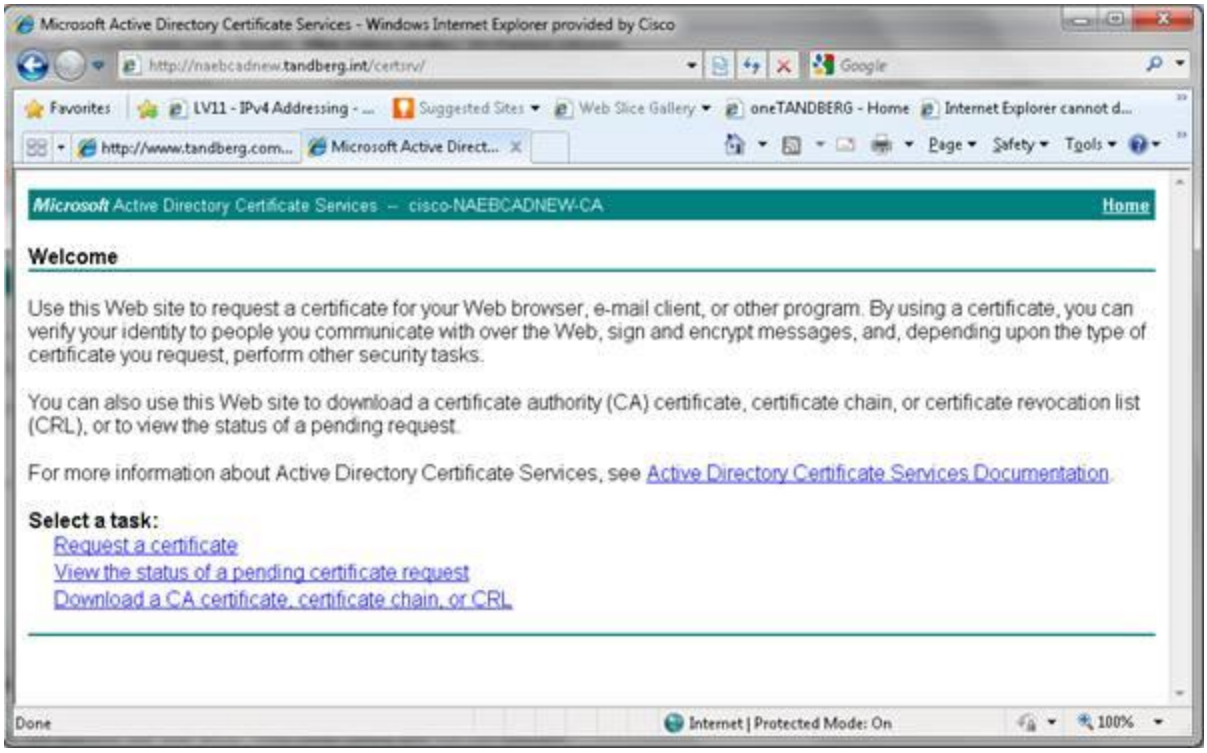


Figure 9 - Main Certificate Authority Page

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

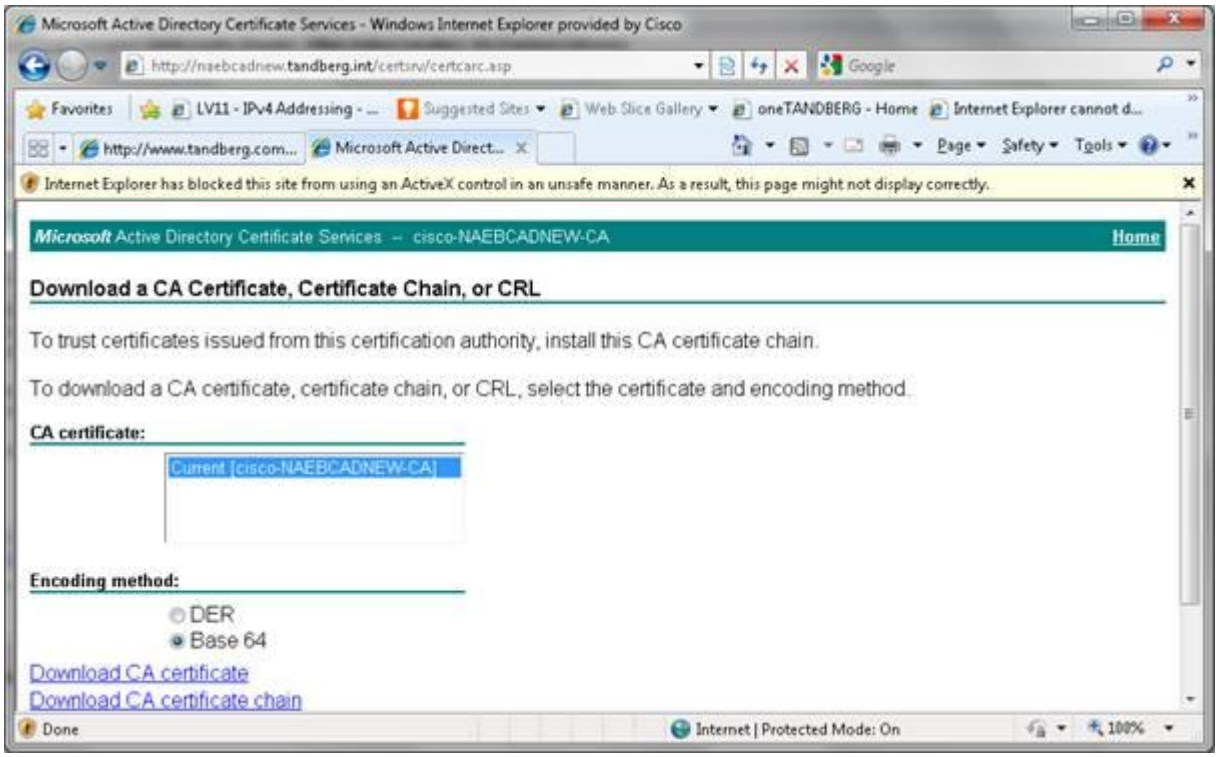


Figure 10 - Download a CA Certificate, Certificate Chain, or CRL

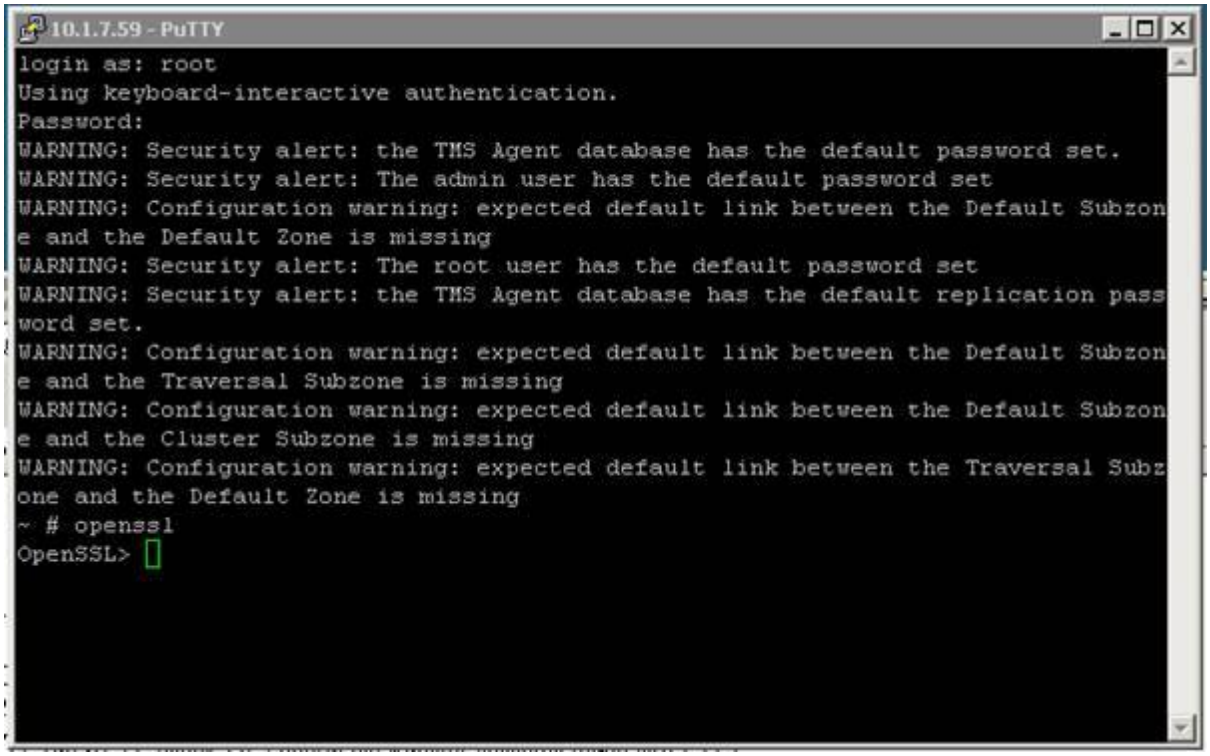
13. You can load the CA certificate to the VCS in .**cer** format or convert to .**pem**. Either works.

2.2 Use 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`



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-----
MIIByDCCATECAQAwgYcxCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJOQzEMMAoGA1UE
BwwDUlRQMQ4wDAYDVQQKDAVDaXNjbzEMMAoGA1UECwwDVEFDMRwwGgYDVQQDDBN2
Y3MxLmNoYWJyb3cyLmxvY2FsMSEwHwYJKoZIhvcNAQkBFhJjaGFicm93MkBjaXNj
by5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANphU8KVa3iPHoOAY+SF
8XVhA+CyY82XHqGbx6H28/ID+f77UVIFV8Yfe+9KfumjFLBwCKgPZVXPPdNsIau4
8gZdn6LDZb+M2qTWWJZB33+3kWFqL7rMElyYLhLarJZy7maAGSkFT2QHSZhlIcpR
wbzV95wYd/7yhk7RvLbl+qSLAgMBAAGgADANBgkqhkiG9w0BAQUFAAOBgQA/H+Xi
aBPGoOr3j942UcoNwMiO1OpJ/SWUusprlEEOpR+Excii3kRgyOASjW0I5JwFtCvP
rYkudlw2Iz69t1c9iIPMWBMXUuiauLC6clnxruCPp+l83xCIt0fgyUHlYPpf5l73
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.

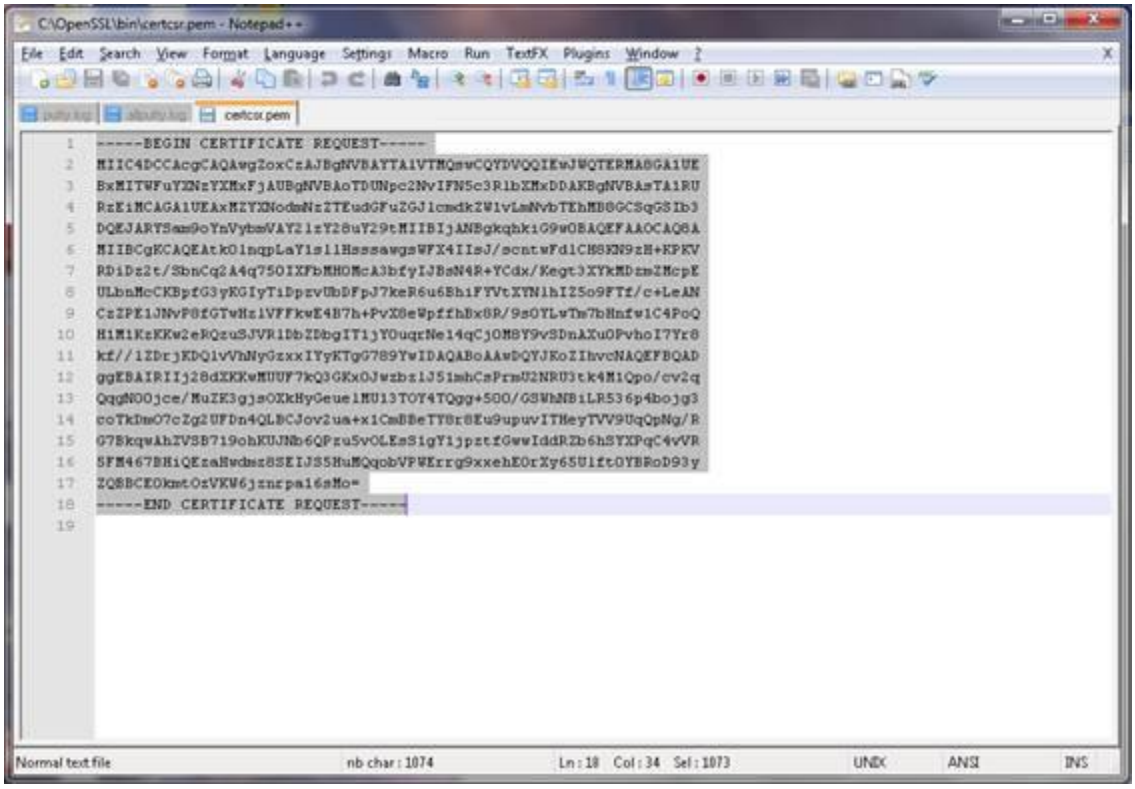


Figure 11 - Openssl already present on the VCS

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 **Wecome** page, select **Request a Certificate**.

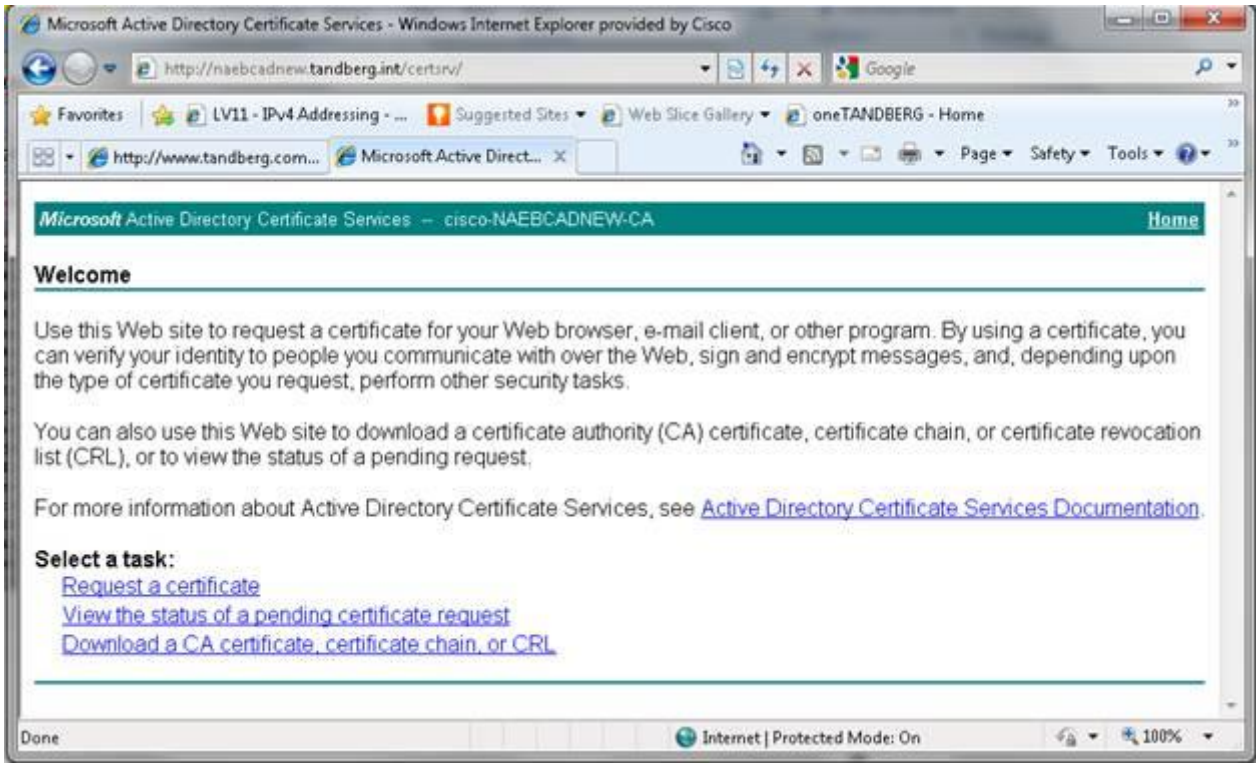


Figure 12 - Microsoft Active Directory Certificate Services

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

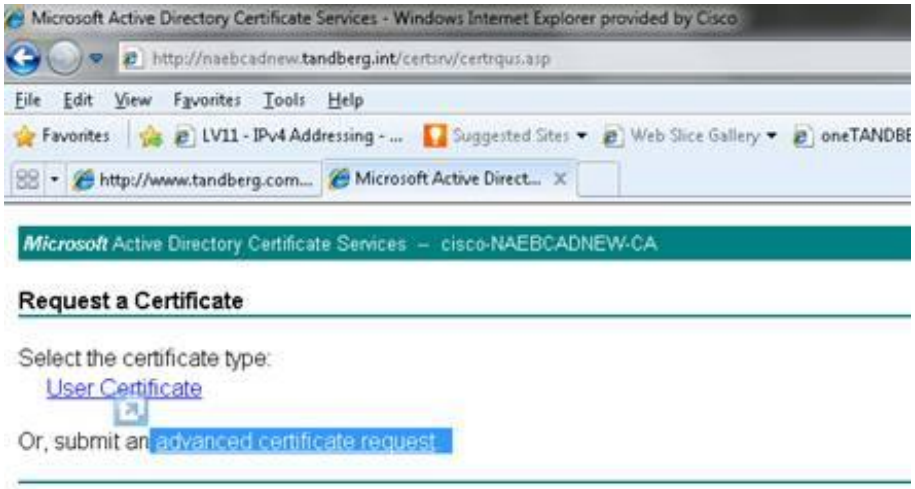


Figure 13 - Request a Certificate

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

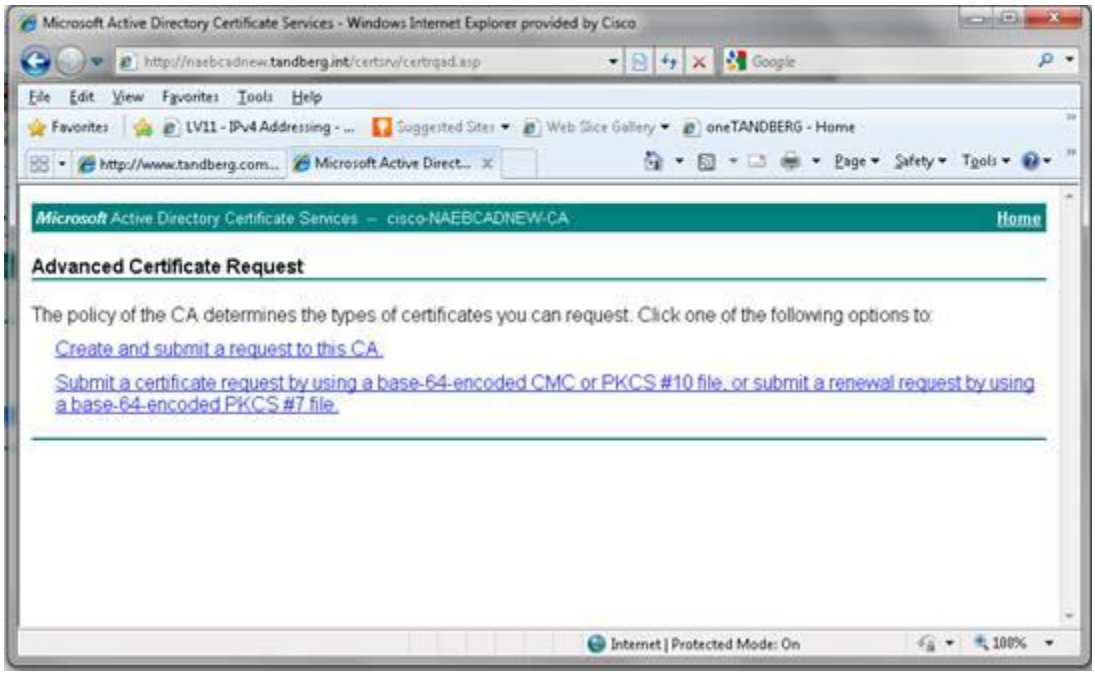


Figure 14 - Advanced Certificate Request

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

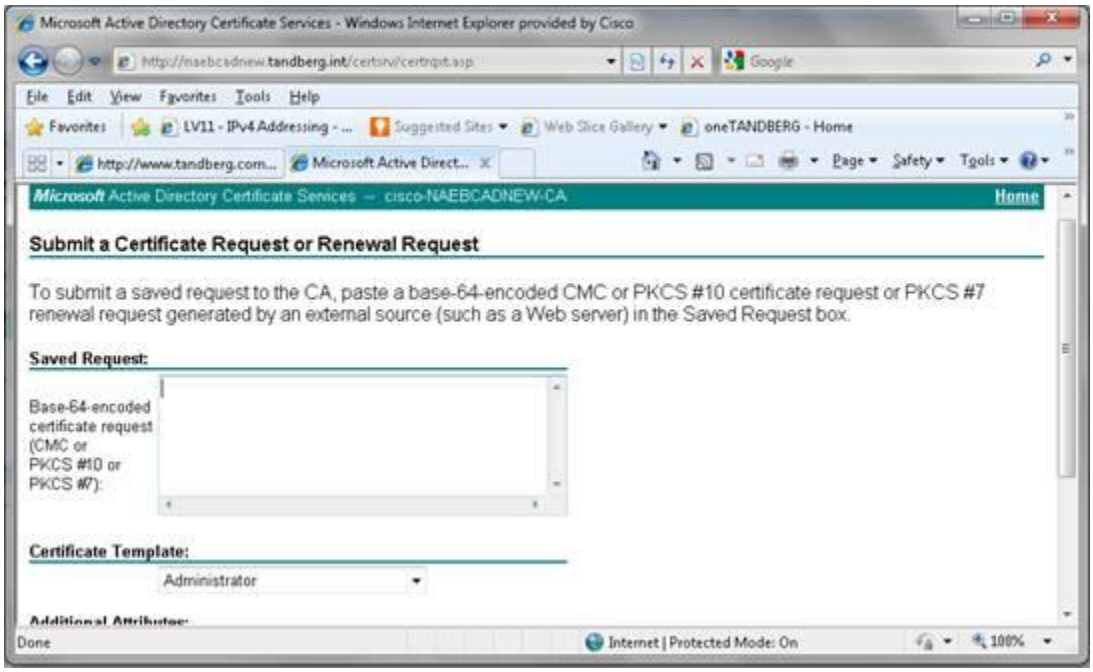
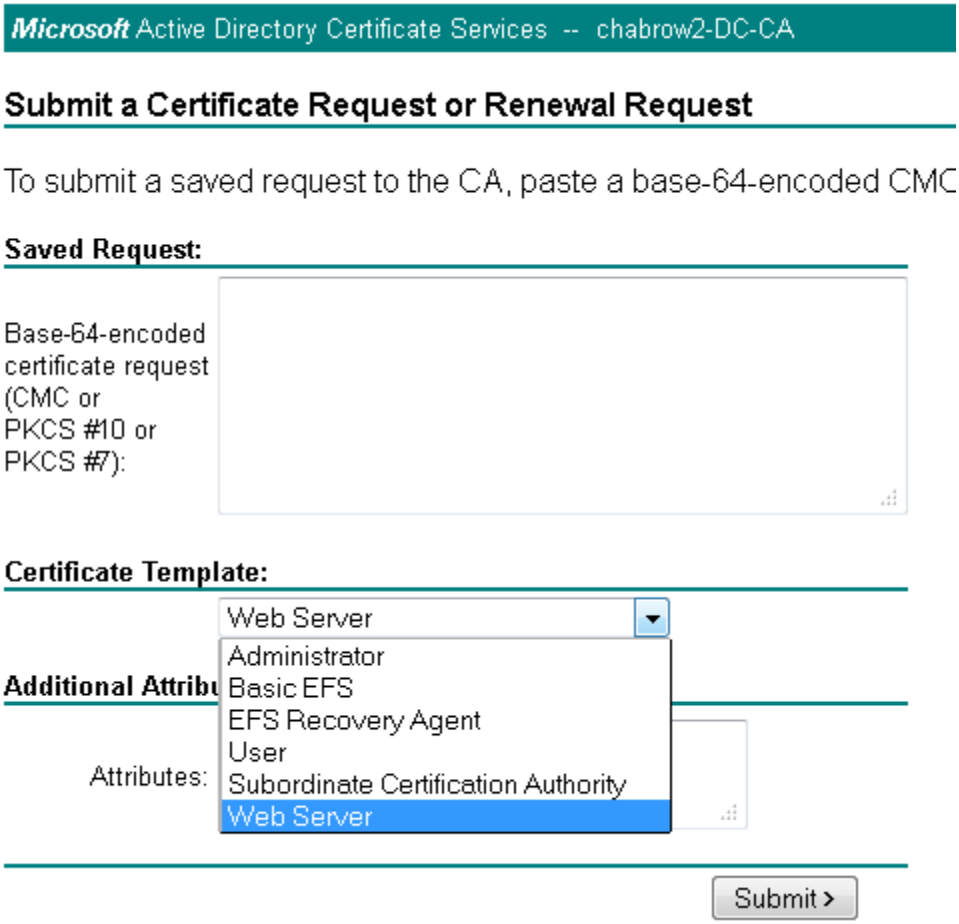


Figure 15 - Submit a Certificate Request or Renewal Request

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



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

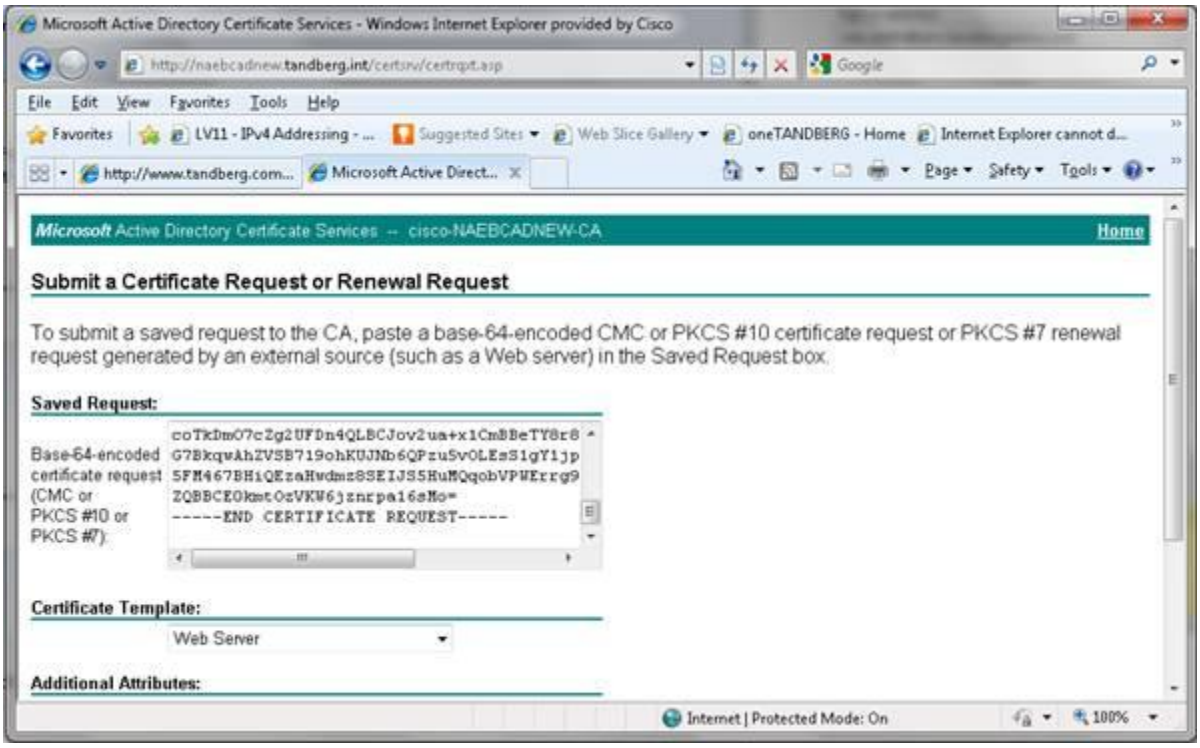


Figure 16 - Submit a Certificate Request or Renewal Request

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

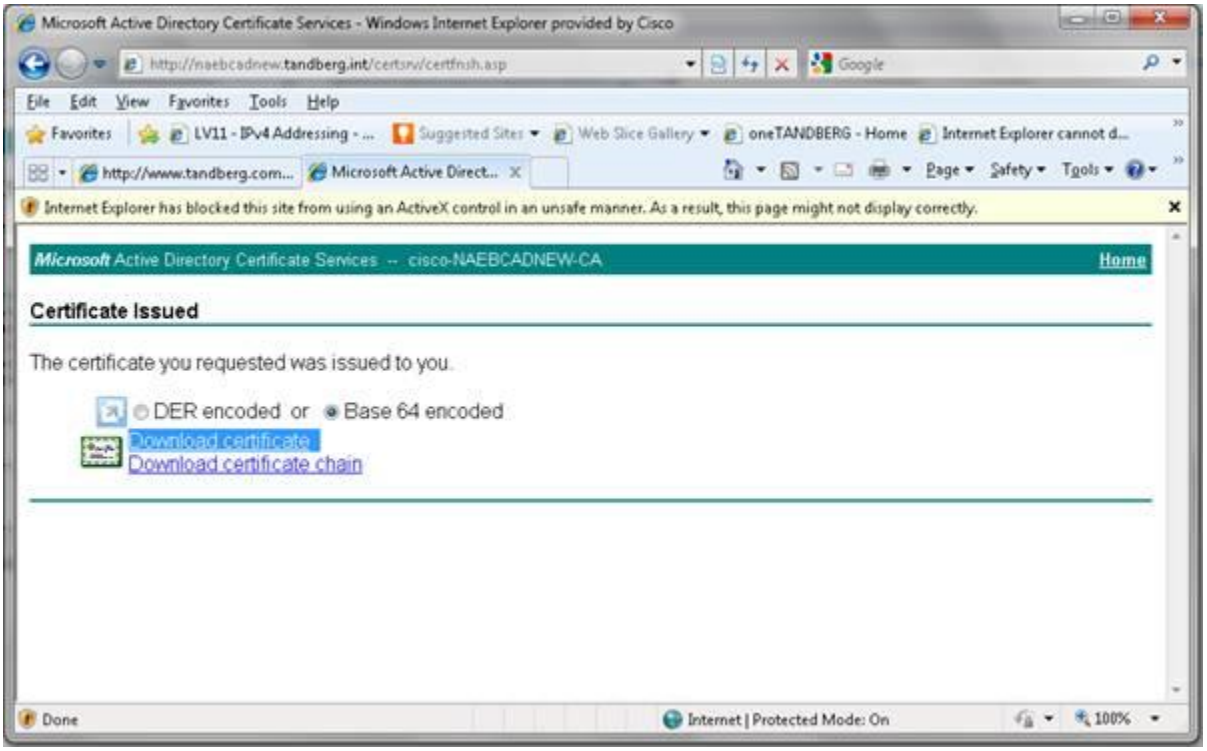


Figure 17 - Certificate Issued

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, certficate chain, or CRL**.

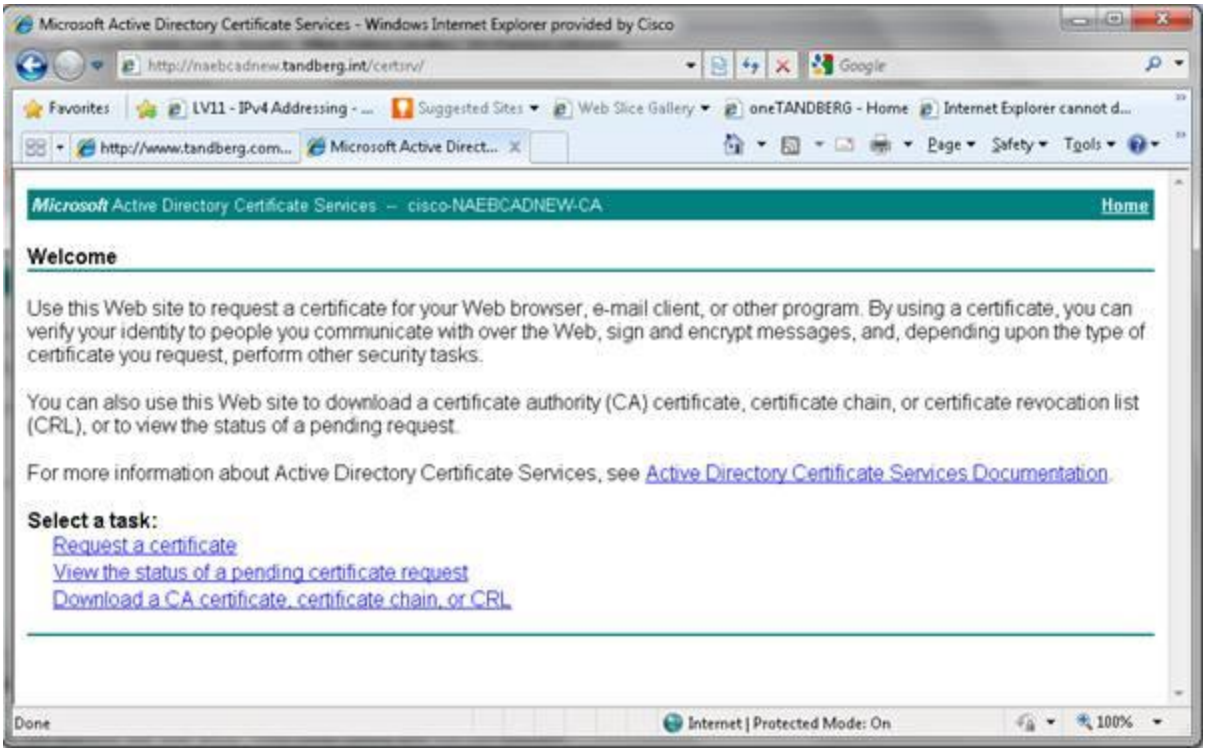


Figure 18 - Main Certificate Authority Page

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

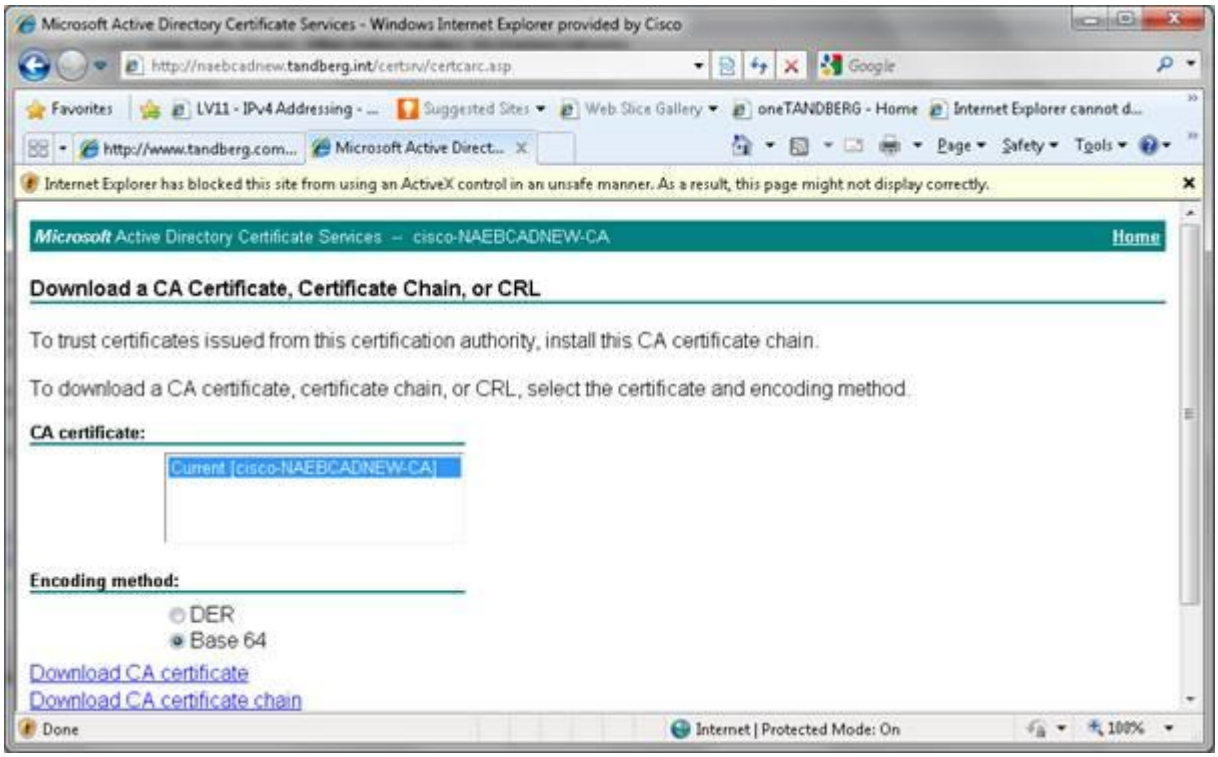


Figure 19 - Download a CA Certificate, Certificate Chain, or CRL

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

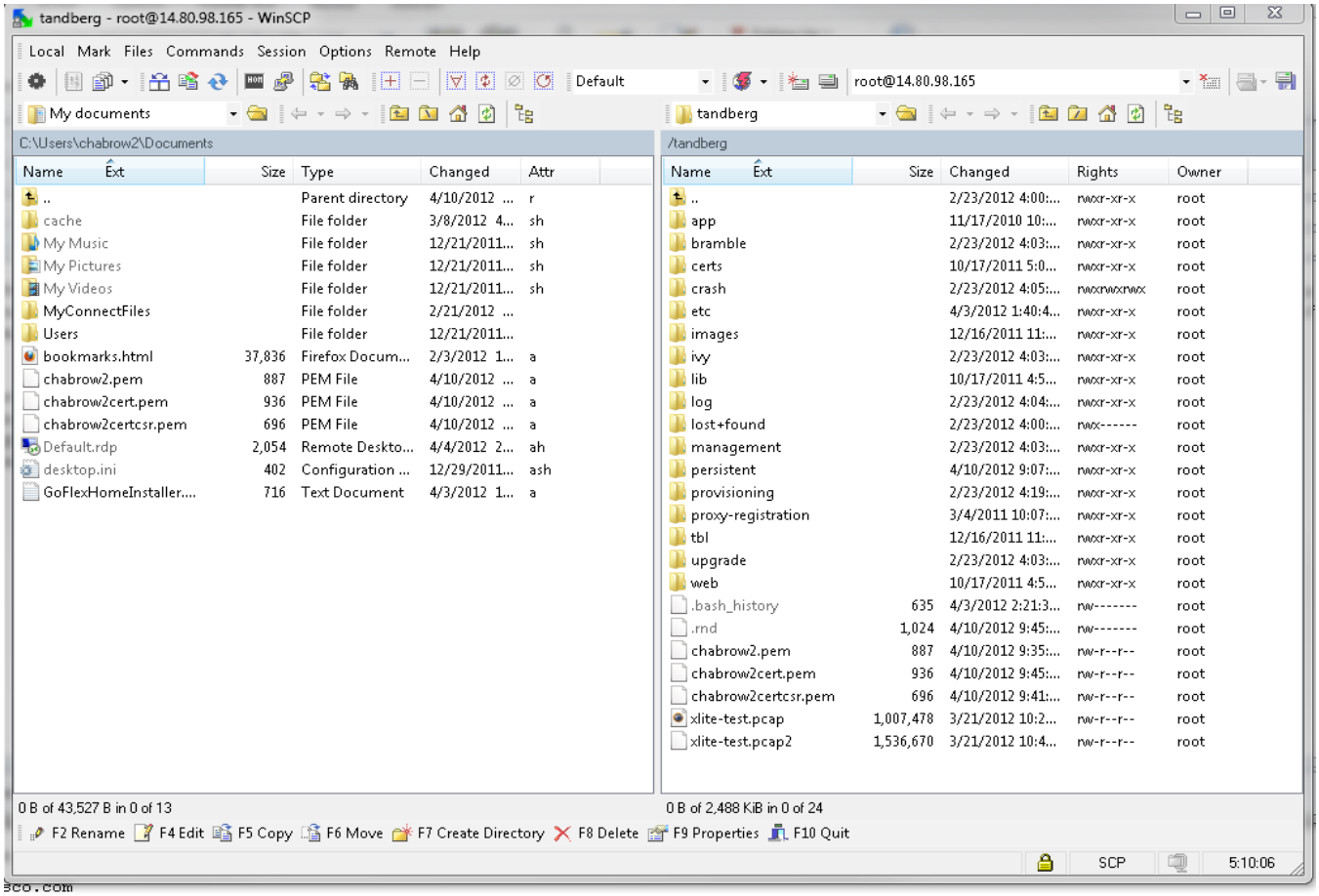


Figure 20 - WinSCP

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, certficate chain, or CRL**.

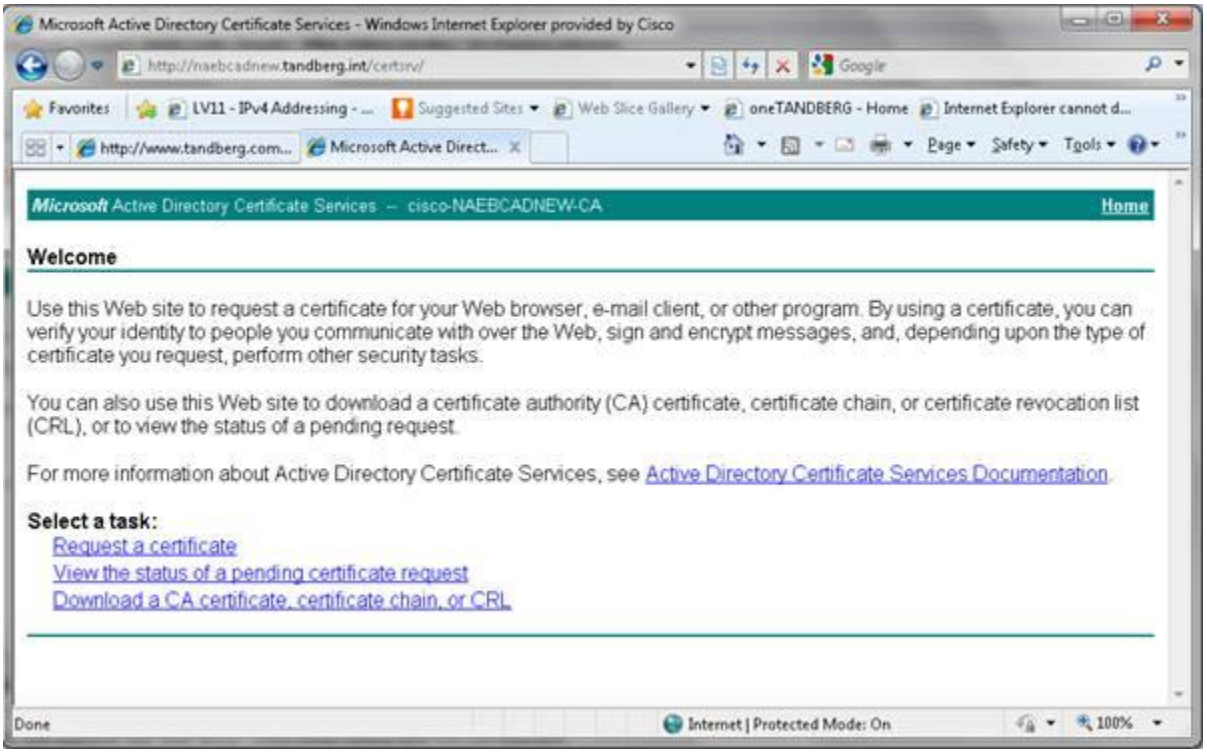


Figure 21 - Main Certificate Authority Page

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

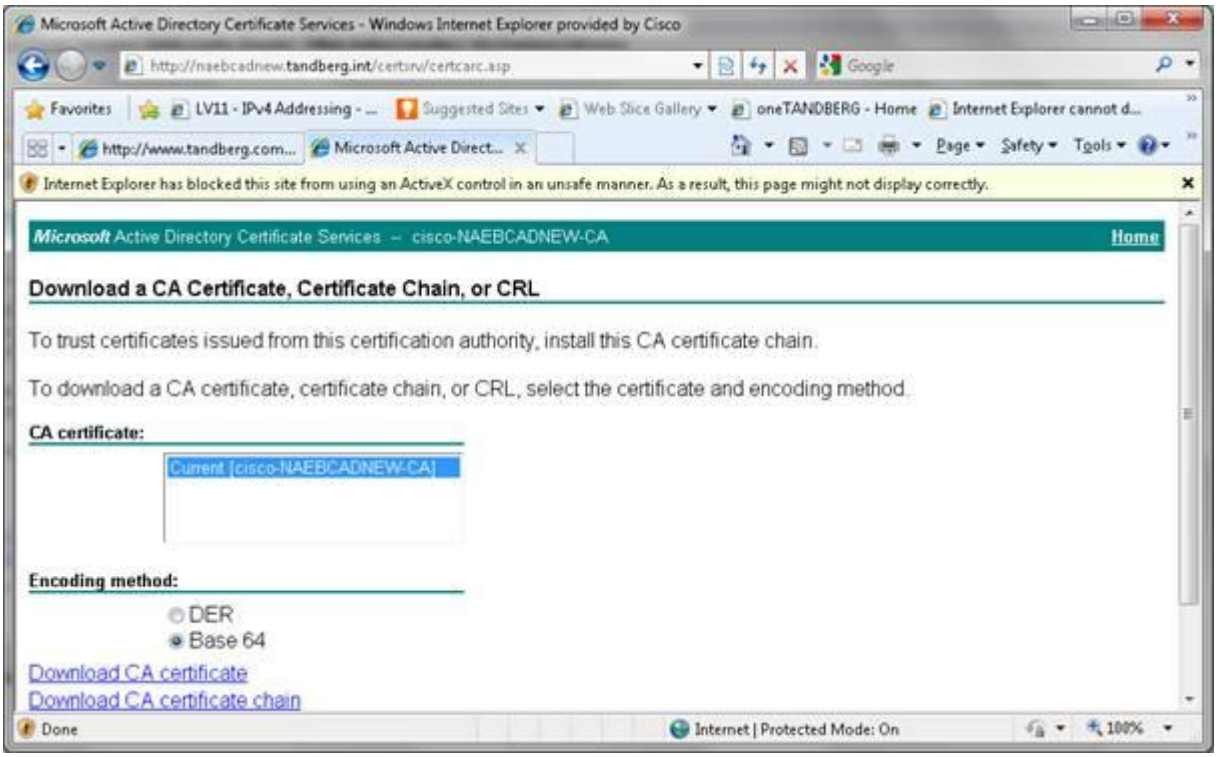


Figure 22 - Download a CA Certificate, Certificate Chain, or CRL

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.

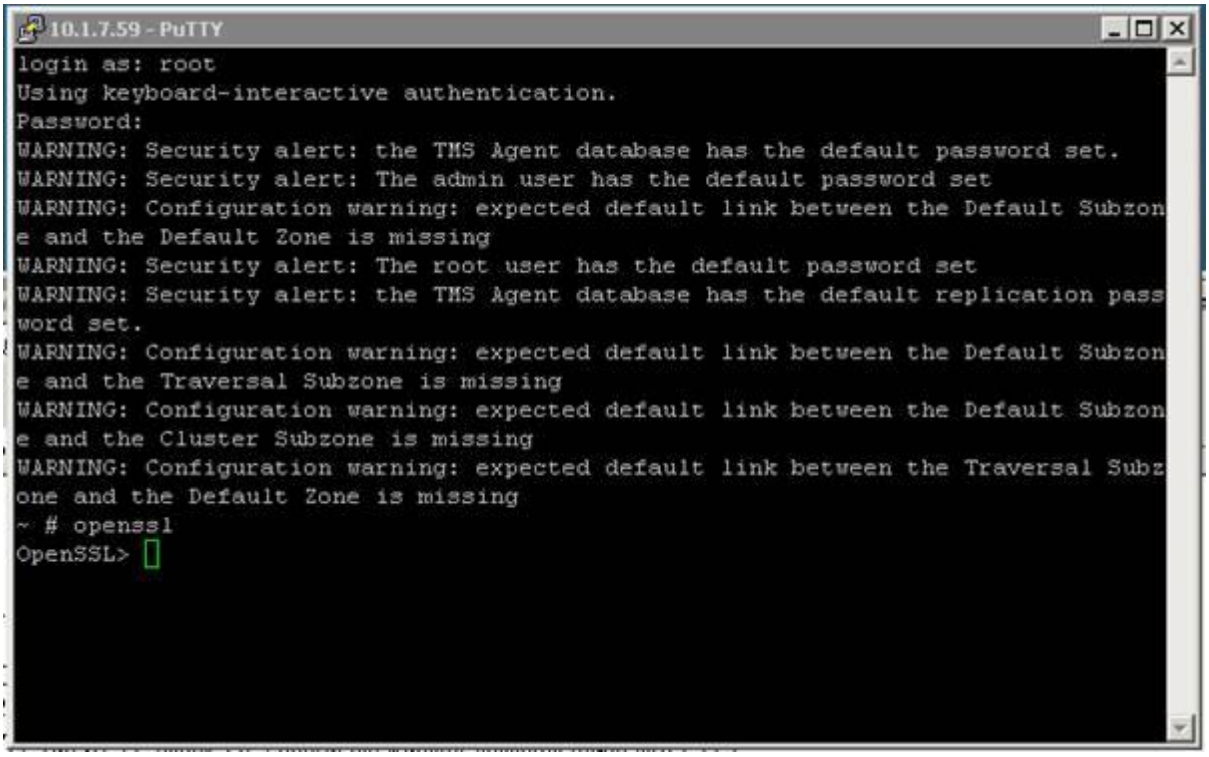


Figure 23 - Login Screen on VCS

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-----
MIIByDCCATECAQAwgYcxCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJOQzEMMAoGA1UE
BwwDUlRQMQ4wDAYDVQQKDAVDaXNjbzEMMAoGA1UECwwDVEFDMRwwGgYDVQQDDBN2
Y3MxLmNoYWJyb3cyLmxvY2FsMSEwHwYJKoZIhvcNAQkBFhJjaGFicm93MkBjaXNj
by5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANphU8KVa3iPHoOAY+SF
8XVhA+CyY82XHqGbx6H28/ID+f77UVIFV8Yfe+9KfumjFLBwCKgPZVXPPdNsIau4
8gZdn6LDZb+M2qTWWJZB33+3kWFqL7rMElyYLhLarJZy7maAGSkFT2QHSZhlIcpR
wbzV95wYd/7yhk7RvLbl+qSLAgMBAAGgADANBgkqhkiG9w0BAQUFAAOBgQA/H+Xi
aBPGoOr3j942UcoNwMiO1OpJ/SWUusprlEEOpR+Excii3kRgyOASjW0I5JwFtCvP
rYkudlw2Iz69t1c9iIPMWBMXUuiauLC6clnxruCPp+l83xCIt0fgyUHlYPpf5l73
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 —

```
~ # 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-----
MIIChzCCAfACCQDCAAb5WW4vsDANBgkqhkiG9w0BAQUFADCBhzELMAkGA1UEBhMC
VVMxCzAJBgNVBAgMAk5DMQwwCgYDVQQHDANSVFAxDjAMBgNVBAoMBUNpc2NvMQww
CgYDVQQLDANUQUMxHDAaBgNVBAMME3ZjczEuY2hhYnJvdzIubG9jYWwxITAfBgkq
hkiG9w0BCQEWEmNoYWJyb3cyQGNpc2NvLmNvbTAeFw0xMjA0MTAxMzQ1MDhaFw0x
MzA0MDUxMzQ1MDhaMIGHMQswCQYDVQQGEwJVUzELMAkGA1UECAwCTkMxDDAKBgNV
BAcMA1JUUDEOMAwGA1UECgwFQ2lzY28xDDAKBgNVBAsMA1RBQzEcMBoGA1UEAwwT
dmNzMS5jaGFicm93Mi5sb2NhbDEhMB8GCSqGSIb3DQEJARYSY2hhYnJvdzJAY2lz
Y28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDaYVPClWt4jx6DgGPk
hfF1YQPgsmPNlx6hm8eh9vPyA/n++1FSBVfGH3vvSn7poxSwcAioD2VVzz3TbCGr
uPIGXZ+iw2W/jNqk1liWQd9/t5Fhai+6zBJcmC4S2qyWcu5mgBkpBU9kB0mYZSHK
UcG81fecGHf+8oZO0by25fqkiwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAH3FuIsS
Vd+FoBc4RTTCX0tTwJovRlJzetz1j4maMkIicJFT46Lx+mjNnwWml/qn2SntnIlH
ZfWabOKfcnDFZ/L3AnjhoR3ZQWND5KXZHt9PDrAaZOwLTx4MgHcMVwwfth3WP2e2
Rh3sNnMOOK9RZACGbXo66D69Wacz3DaJsxBy
-----END 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

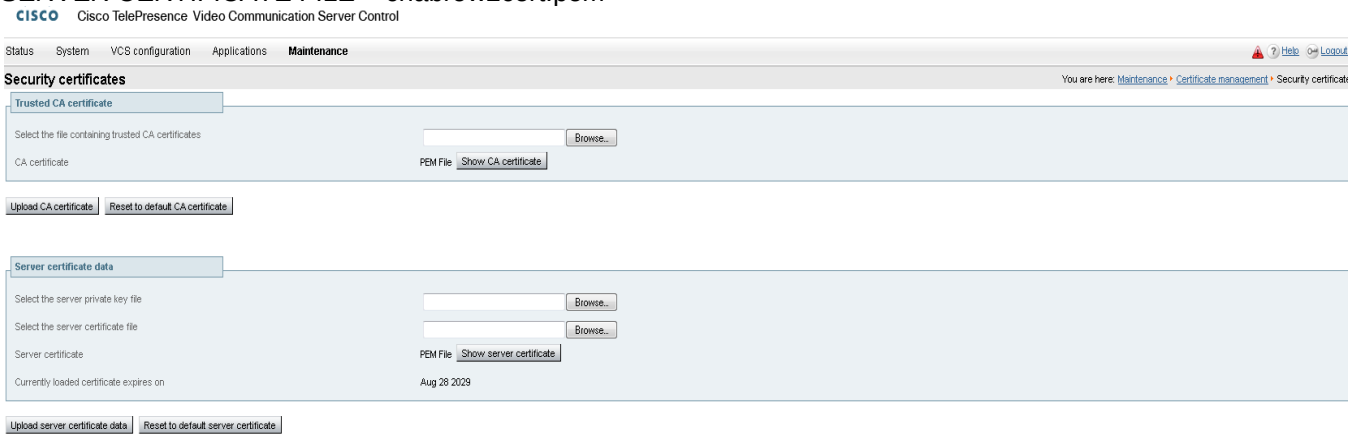


Figure 24 - Security certificate

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

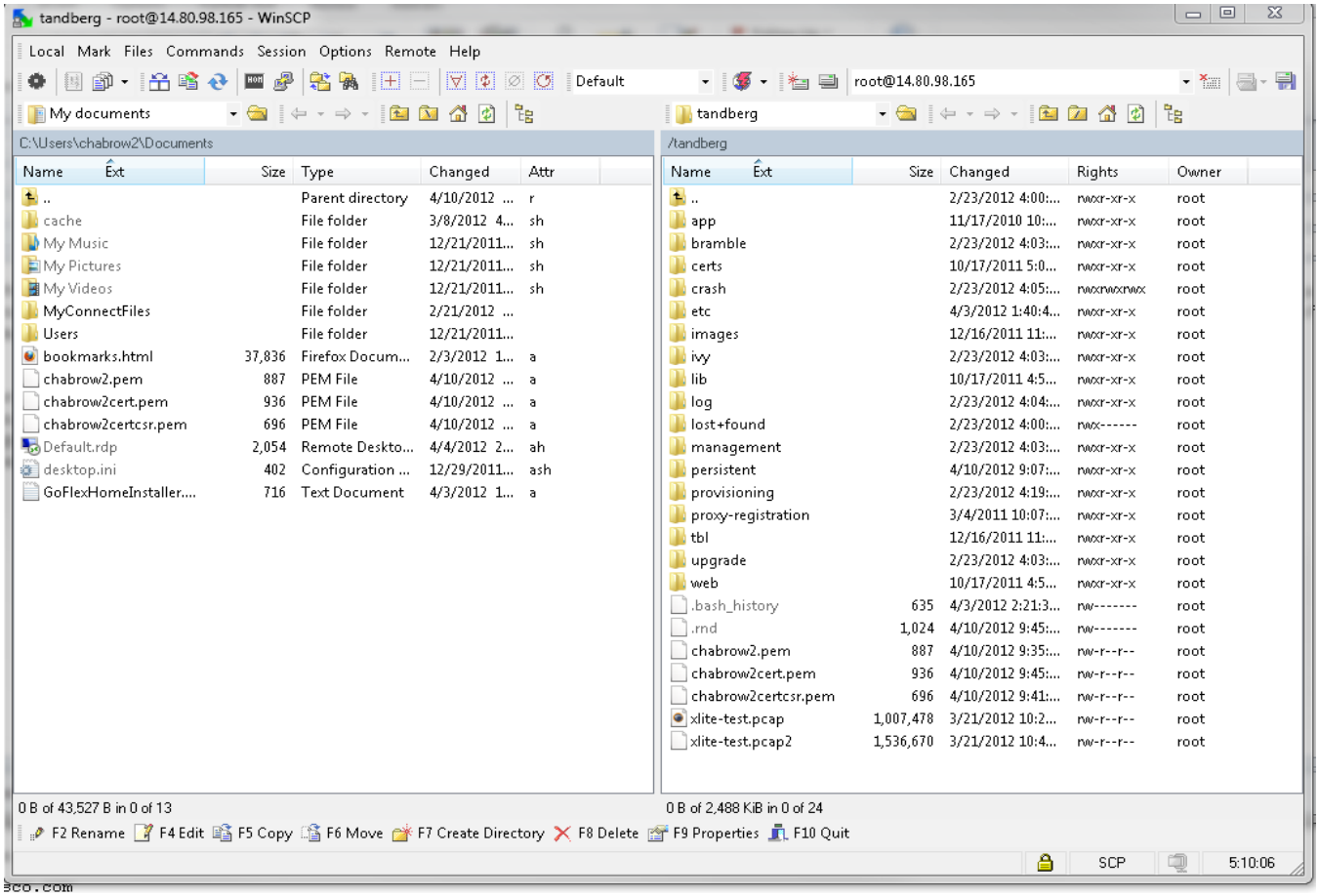


Figure 25 - WinSCP

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.

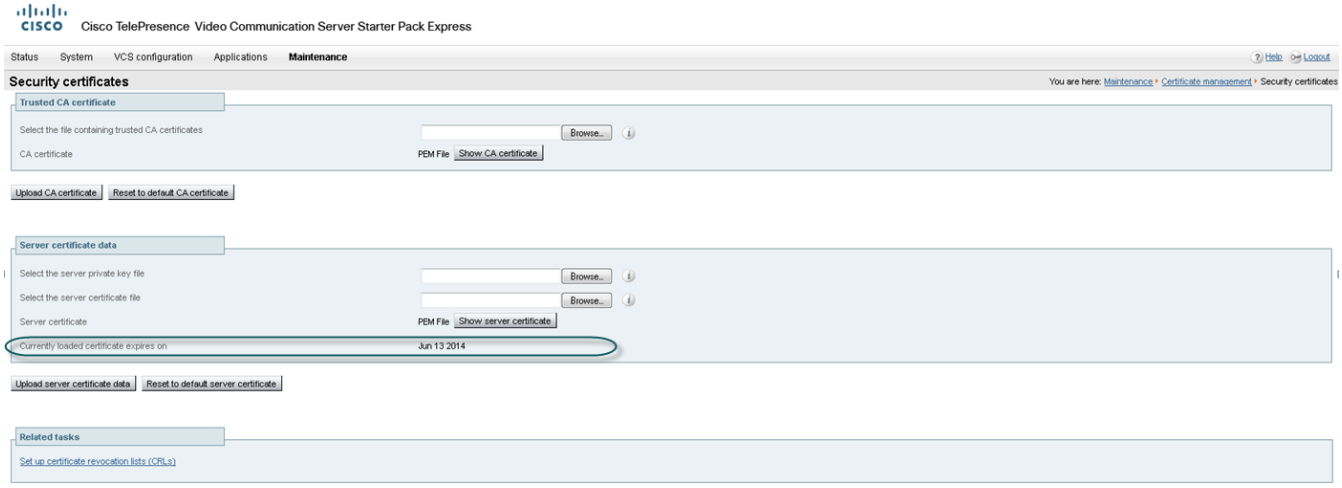


Figure 26 - Server certificate date

3 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 Micrsoft instructions on creating a certificate for "Trusted Application Servers".

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

End of Document

4 Glossary

Term

Definition of the word. Definition of the word.

Term 2

Definition of the word. Definition of the word.