



# CHAPTER 5

## Configuring Certificates on Cisco VCS Expressway

---

Revised: April 2014

### Introduction

This chapter describes the best practices for configuring certificates on Cisco VCS Expressway.

There are three parts to the configuration:

- Generating a certificate signing request (CSR)
- Installing the SSL Server Certificate on the VCS Expressway
- Configuring the Trusted CA List on the VCS Expressway

Both VCS Expressway X7.2.2 and X8.1 are supported. There are important differences in how each are configured, which are noted in the procedures that follow.



Caution

---

Customers using Static NAT on VCS Expressway X7.2.2 are highly recommended to not upgrade to X8.1. If you are using Static NAT with X8.1, refer to the recommended workarounds in [VCS Expressway X8.1 Encryption Issue and Workarounds](#).

---

### VCS Expressway X8.1 Encryption Issue and Workarounds

There is an issue with the Encrypt on Behalf feature in VCS Expressway X8.1 when using Static NAT. Because VCS Expressway X8.1 uses the Ethernet 2 IP address for the media part in SDP, the media part of calls will fail. (Caveat ID: CSCum90139). Customers using Static NAT on their VCS Expressways running X7.2.2 are urged not to upgrade to X8.1 until a maintenance release fixes this issue.

If you are using Static NAT on VCS Expressway X8.1, Cisco recommends one of the following workarounds:

- Downgrade VCS Expressway to X7.2.2.
- Reconfigure VCS Expressway X8.1 to not use Static NAT.
- Use VCS Control to Encrypt on Behalf instead of VCS Expressway.

To use VCS Control to encrypt on behalf, do the following:

- 
- Step 1** On MCU, turn Encryption **OFF** for all conferences.
- Step 2** On VCS Control, change the dedicated WebEx Traversal zone to **Force Encrypted**.
- Step 3** On VCS Expressway, change the dedicated WebEx DNS zone to **Encryption Auto**.
- 

## Videos Available

The entire configuration process for VCS Expressway 7.2.2 is also described and demonstrated in the following video series:

[Configuring Certificates on Cisco VCS Expressway for WebEx Enabled TelePresence](#)

## Supported Certificates

Make sure you submit your certificate signing request to a public certificate authority that issues a certificate that WebEx supports.



### Note

---

Self-signed certificates are NOT supported.

---

WebEx supports certificates that are issued by specific Root Certificate Authorities. Certificate providers may have multiple Root Certificate Authorities and not all may be supported by WebEx. Your certificate must be issued by one of the following Root Certificate Authorities (or one of their Intermediate Certificate Authorities) or the call from your VCS Expressway will not be authorized by WebEx:

- entrust\_ev\_ca
- digicert\_global\_root\_ca
- verisign\_class\_2\_public\_primary\_ca\_-\_g3
- godaddy\_class\_2\_ca\_root\_certificate
- Go Daddy Root Certification Authority - G2
- verisign\_class\_3\_public\_primary\_ca\_-\_g5
- verisign\_class\_3\_public\_primary\_ca\_-\_g3
- dst\_root\_ca\_x3
- verisign\_class\_3\_public\_primary\_ca\_-\_g2
- equifax\_secure\_ca
- entrust\_2048\_ca\*
- verisign\_class\_1\_public\_primary\_ca\_-\_g3
- ca\_cert\_signing\_authority
- geotrust\_global\_ca
- globalsign\_root\_ca
- thawte\_primary\_root\_ca
- geotrust\_primary\_ca

- addtrust\_external\_ca\_root



---

**Note** This list may change over time. For the most current information, contact WebEx.

---

\*To use a certificate generated by entrust\_2048\_ca with Cisco VCS Expressway, you must replace the Entrust Root CA certificate in the trusted CA list on the Cisco VCS Expressway with the newest version available from Entrust.

You can download the newer entrust\_2048\_ca.cer file from the Root Certificates list on the Entrust web site at the following URL:

[https://www.entrust.net/downloads/root\\_index.cfm](https://www.entrust.net/downloads/root_index.cfm)



**Caution**

---

Wildcard certificates are not supported on VCS Expressway.


---

## Generating a Certificate Signing Request (CSR)

To generate a certificate signing request, do the following:

- 
- Step 1** In VCS Expressway:
- X7.2.2, go to **Maintenance > Certificate management > Server certificate**.
  - X8.1, go to **Maintenance > Security certificates > Server certificate**.
- Step 2** Click **Generate CSR**.

## ■ Generating a Certificate Signing Request (CSR)

 Cisco TelePresence Video Communication Server Expressway

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

**Server certificate** You are here: [Maintenance](#) > [Certificate management](#) > Server certificate

**Server certificate data**

Server certificate	PEM File <a href="#">Show server certificate</a>
Currently loaded certificate expires on	Dec 12 2014

[Reset to default server certificate](#)

**Certificate signing request (CSR)**

Certificate request	There is no certificate signing request in progress
---------------------	---

[Generate CSR](#)

**Upload new certificate**

Select the server private key file	<input type="text"/>	<a href="#">Browse...</a>	<a href="#">i</a>
Select the server certificate file	<input type="text"/>	<a href="#">Browse...</a>	<a href="#">i</a>

[Upload server certificate data](#)

**Generate CSR** You are here: [Maintenance](#) > [Certif](#)

**Generate Certificate Signing Request**

Common name	<input type="text" value="FQDN of VCS"/>
Common name as it will appear	<input type="text" value="xyz-vcse-1.example.com"/>
Subject alternative names	<input type="text" value="None"/>
Additional alternative names (comma separated)	<input type="text"/>
Alternative name as it will appear	<input type="text" value="xyz-vcse-1.example.com"/>
Key length (in bits)	<input type="text" value="2048"/>
Country	<input type="text" value="* US"/>
State or province	<input type="text" value="* California"/>
Locality (town name)	<input type="text" value="* San Jose"/>
Organization (company name)	<input type="text" value="* Example"/>
Organizational unit	<input type="text" value="* XYZ"/>

**Generate CSR**

- Step 3** Enter the required information for the CSR and click **Generate CSR**.  
After clicking the Generate CSR button, the Server Certificate page is displayed and a message indicating that CSR creation was successful.



**Note**

The private key is automatically generated as part of the CSR creation process. **DO NOT** click the option to Discard CSR, this will force you to regenerate the CSR and the auto-generated private key will not appear on the Server Certificate page.

## Generating a Certificate Signing Request (CSR)

**Server certificate** You are here: [Maintenance](#) > [Certificate management](#) > Server certificate

**CSR creation successful:** Certificate Signing Request saved to /tandberg/persistent/certs/csr.pem.

**Server certificate data**

Server certificate	PEM File	<a href="#">Show server certificate</a>
Currently loaded certificate expires on	Dec 12 2014	

[Reset to default server certificate](#)

**Certificate signing request (CSR)**

Certificate request	PEM File	<a href="#">View</a>	<a href="#">Download</a>
Generated on	Apr 26 2013		

[Discard CSR](#)

**Upload new certificate**

Select the server private key file System will use the private key file generated at the same time as the CSR.


Select the server certificate file  [Browse...](#) [i](#)

[Upload server certificate data](#)

**Step 4** In order to complete the CSR process and receive a signed certificate from a supported public certificate authority (CA), you must download the CSR by clicking **Download**.

Most certificate authorities will require the CSR to be provided in a PKCS#10 request format (Shown below).

**Server certificate** You are here: [Maintenance](#) > [Certificate](#)

 **CSR creation successful:** Certificate Signing Request saved to /tandberg/persistent/certs/csr.pem.

**Server certificate data**

Server certificate PEM File [Show server certificate](#)

Currently loaded certificate expires on

[Reset to default server certificate](#)

**Certificate signing request (CSR)**

Certificate request

Generated on

[Discard CSR](#)

**Upload new certificate**

Select the server private key file System will use the private key file generated at the same time as the CSR.

```

-----BEGIN CERTIFICATE REQUEST-----
MIIDLDCCAhQCAQAwEjEhMB8GA1UEAwYY3RnLWVmdC12Y3NlLlTEuY2lzy28uY29t
MQswCQYDVQQGEwJWUzETMBEGA1UECAwKQ2FsaWZvcn5yTERMA8GA1UEBwwIU2Fu
IEpvc2UxZjAMBGNVBAoMBUNpc2NvMRAwDgYDVQQLEAdVcG9uRUZUMiBIjANBgkq
hkIG9w0BAQEFAA0CAQ8AMIIBCgKCAQEAuqf35MXVBYnZyXbsKDbY+ZEXPDH4fqt4
fULpqtBEbD/z148dib7/i+UmMIS0RN9deXatSttkZ7vh3VghvRfGzy63t2wu6FHy
bmkMxBu82UhnfmPHC3WtpFZKoG95hWiojR66yWE43ZqkeYBUkn9Ij7hKD+YyTbMA
3JnzF8cEGh8KEK5RjfbBbRqVwep1wXTon92Y8tm3hitnHGzFEvXk7qZNeEAIx9Dv
e69PqjdiB0RvSNk7GrLQRg5uORvUgPjHBLug9HDY1MMQeK6xvrgEfLACgn/i55rT
Sy6eEbiZfmrNHNf+/zIr7utphlzhliYZAV5zaxXBCbbmOvs0RNYB0wIDAQABoG0w
awYJKoZIhvcNAQkOMV4wXDAJBGNVHRMEAjAAMAsGA1UdDwQEAwIF4DAdBgNVHSUE
FjAUBgggrBgEFBQcDAQYIKwYBBQUHwIwIwYDVR0RBwwGoIYY3RnLWVmdC12Y3Nl
LlTEuY2lzy28uY29tMA0GCsq5Ib3DQEBAUAA4IBAQBmquN74IDxgb5PvYPT3oYM
hYwiUxYso+900kqyJbzM5i5g+GKMQRcy70rb5EEQt3RyD2Qyzt4jsAu6rpSrqLJ
mc1J/jJspIEL1EXtgo69T47aGhYxoG0xd7neMUT3p5qG5w7cWaxiMEzRfBj16MBH
RaBgPNDsIkzbaQt2Md0W13no0ux0ZCV//KsKOMKdwm1kYkp+Noqw05hYToKEAGgf
ijgEemDeHw5HxwL8XmpfvsTJ3Z86DiRzbvLHpNnuXVQuzF48DsD+rIjkcM90YRJ
R4W4e12+vuYQ/oDRHKK1UQm3v4IfociI04dMjrdI3m6NPKsmKvh5fKxgtz26Hf4g
-----END CERTIFICATE REQUEST-----

```

**Step 5** Submit the CSR to your public CA.



**Note** Important: Make sure your public CA provides you with an SSL server certificate that includes both Server and Client Auth keys.

Once you've received the SSL server certificate from your public CA, you are ready to install it on the VCS Expressway.

## Installing the SSL Server Certificate on the VCS Expressway



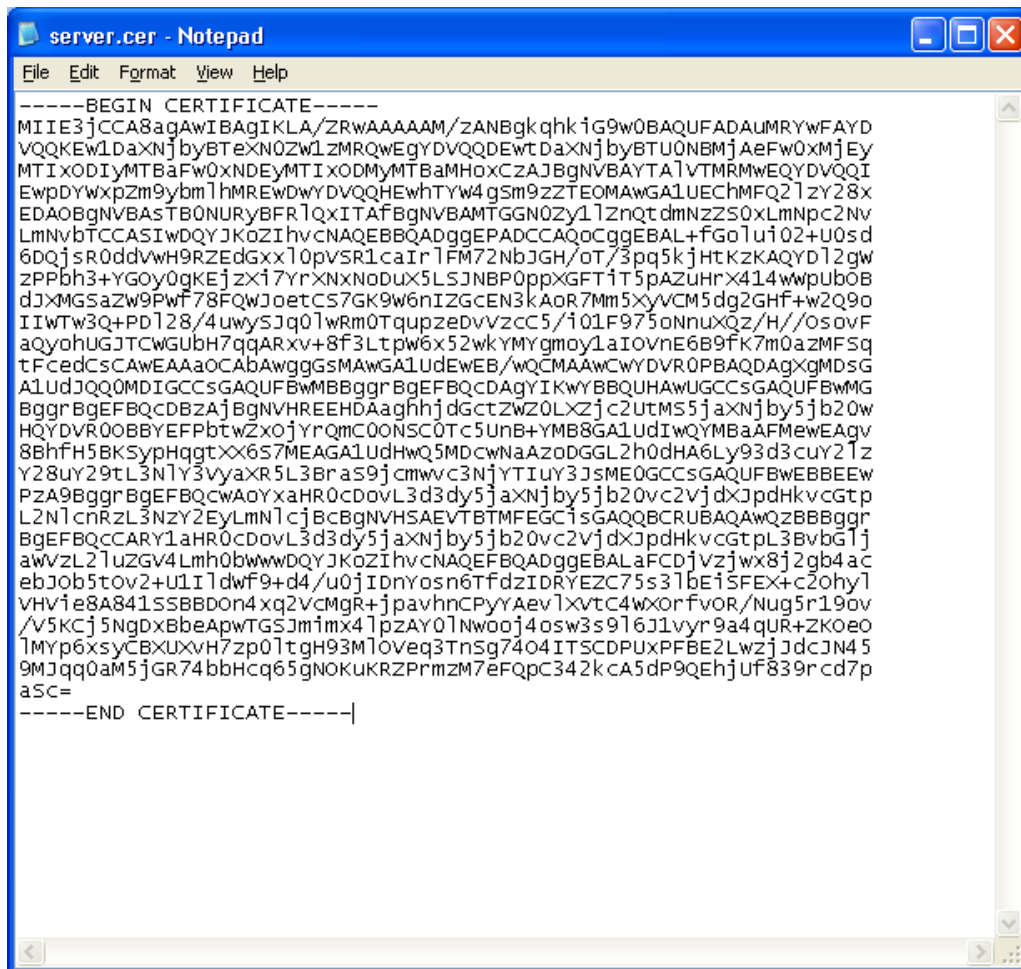
**Note** Before installing the server certificate on the VCS Expressway, make sure it is in the .PEM format. If the certificate you received is in a .CER format, you can convert it to a .PEM file by simply changing the file extension to .PEM.



**Caution** The server certificate must not be stacked along with the root or intermediate CA Certificates.

To install the SSL server certificate on the VCS Expressway, do the following:

- Step 1 (Recommended) Open the server certificate in a text editing application such as Notepad and verify that you see a single certificate (Noted by Begin and End Certificate brackets).



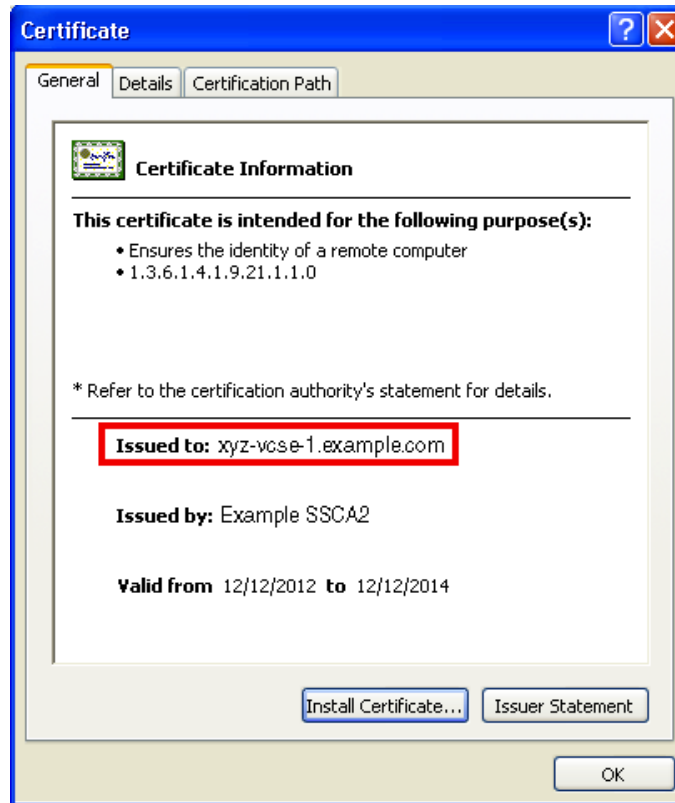
```

-----BEGIN CERTIFICATE-----
MIIIE3jCCA8agAwIBAgIKLA/ZRwAAAAAM/zANBgkqhkiG9w0BAQUFADAUMRYWFAyD
VQQKEw1DaXNjbyBTenN0ZW1zMRQWEgyDVQQDEwtDaXNjbyBTU0NBMTAeFw0xMjE5
MTIxODIyMTBhZmF0xNDEyMTIxODMyMTBhMHoXCzAJBgNVBAYTA1VTMRMWEQYDVQQI
EwppYXp0Ym9ybmhmREwDyDVQQHEWhTYW4gSm9zZTEOMAwGA1UEChMFQ2l2Y28x
EDA0BgNVBAsTB0NURyBFRlQxITAFBgNVBAMTGGN0Zy1lZnqt dmnZZ50xLmNpc2Nv
LmNvbTCCASIwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAL+FGoluiQ2+U0sd
6DQjSR0ddvW9RZEdGxxlQpVSR1caIr lFM72NbJGH/ot/3pg5kjHtKzKAQYDl2gw
ZPPbh3+YGOy0gKEjzx17yrXNxn0dux5LSJNBP0ppXGFTi5pazuhrx414wpub0B
dJXMGsaZw9Pwf78FQWJoetCS7GK9w6nIZGcEN3kAOR7Mm5xyVCM5dg2GHf+w2Q9o
IIWtW3Q+PDl28/4uwysJq0lwRm0TqupzeDvVzcc5/i01F975qNnuxQz/H//Os0vF
aqyohUGJTCwGubh7qqARxv+8f3Ltpw6x52wkYMYgmoy1aIOVnE6B9fK7m0azMFSq
tFcedCsCAwEAAaOCAbAwggGSMawGA1UdEwEB/wQCMAAwCwYDVR0PBAQDAgXgMDSG
A1UdJQQ0MDIGCCSGAQUBwMBBgggrBgEFBQcDAgYIKwYBBQUHAwUGCCSGAQUBwMG
BggrBgEFBQcDBzAjBgNVHREEHDAaghhjdGctZWZ0LXZjc2UtMS5jaXNjby5jb20w
HQYDVR0OBBYEFpbTwxoYjYRqmc0ONSC0Tc5UnB+YMB8GA1UdIwQYMBaAFMewEAqv
8BhfH5BKsyphqgtXX6S7MEAGA1UdHwQ5MDcwNaAzodGGL2h0dHA6Ly93d3cuY2l2
Y28uY29tL3NlY3VyYXR5L3Bras9jcmwvc3NjYTIuY3JSMEOGCCSGAQUBwEBBEEW
PZA9BggrBgEFBQcCwAqYxaHR0cdovL3d3dy5jaXNjby5jb20vc2VjdXJpdHkvcGtp
L2NlcnRzL3NzY2EyLmNlclJcBGNVHSAEVTBMTFEGC1sGAQQBRCRUBAQAwQZBBBggr
BgEFBQcCARY1aHR0cdovL3d3dy5jaXNjby5jb20vc2VjdXJpdHkvcGtpL3BvbG1j
awVzL2luZGV4Lmhh0bwwdQYJKoZIhvcNAQEFBQADggEBALaFCDjVzjwx8j2gb4ac
ebJ0b5tov2+u1I1ldwf9+d4/u0jIDnyosn6TfdzIDRYEzC75s3lbe1sFEX+c2ohy1
VHVie8A841SSBBDOn4xq2VcmGr+jpavhncPyAevlXvtC4wxorfvor/Nug5r19ov
/V5Kcj5NgDxBbeApwTGSJm1mx4lpzAY0lNw00j4osw3s9l6J1vyr9a4qUR+ZKoeO
lMyP6xSyCBXUXvH7zp0ltgh93Ml0veq3Tnsq7404ITSCDPuxPFBE2LwzjJdcJN45
9MJqq0am5jGR74bbHcq65gnOKuKRZPrmzm7eFQpc342kca5dP9QEHjuf839rcd7p
aSC=
-----END CERTIFICATE-----

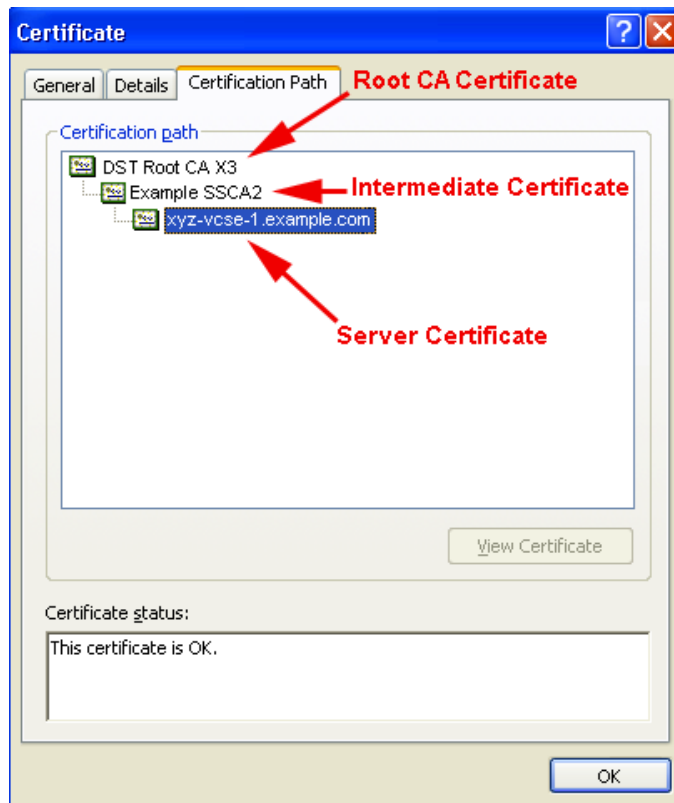
```

You may also want to verify that the validity of the server certificate by opening it as a .CER file. Here you should observe that the **Issued to** field is that of the VCS Expressway server.



**Tip**

It is worth noting whether the CA that issued the certificate uses an intermediate CA or issues/signs certificates from a root CA. If an intermediate CA is involved then you'll need to "stack" or add the Intermediate CA Certificate to the Trusted CA Certificate.



**Step 2** In VCS Expressway:

- X7.2.2, Go to **Maintenance > Certificate management > Server certificate**.
- X8.1, Go to **Maintenance > Security certificates > Server certificate**.

**Step 3** Click **Browse** and select the server certificate that you received from the public CA and click **Open**.





---

**Note** The server certificate must be loaded on to the Expressway in the .PEM certificate format.

---

**Step 4** Click **Upload server certificate data**.


**Server certificate**You are here: [Maintenance](#) > [Certificate management](#) > Server certificate **CSR creation successful:** Certificate Signing Request saved to /tandberg/persistent/certs/csr.pem.**Server certificate data**

Server certificate	PEM File	<a href="#">Show server certificate</a>
Currently loaded certificate expires on	Dec 12 2014	

[Reset to default server certificate](#)**Certificate signing request (CSR)**

Certificate request	PEM File	<a href="#">View</a>	<a href="#">Download</a>
Generated on	Apr 26 2013		

[Discard CSR](#)**Upload new certificate**

Select the server private key file	System will use the private key file generated at the same time as the CSR.	
Select the server certificate file	<input type="text"/>	<a href="#">Browse...</a> 

[Upload server certificate data](#)

After uploading the server certificate, you'll see a message at the top of the page indicating that files were uploaded.

**Server certificate** You are here: [Maintenance](#) > [Certificate management](#) > Server certificate

**Files uploaded**

**Certificate info:** This certificate expires on Dec 12 2014.

**Server certificate data**

Server certificate	PEM File	<a href="#">Show server certificate</a>
Currently loaded certificate expires on	Dec 12 2014	

[Reset to default server certificate](#)

**Certificate signing request (CSR)**

Certificate request There is no certificate signing request in progress

[Generate CSR](#)

**Upload new certificate**

Select the server private key file  [Browse...](#) ⓘ

Select the server certificate file  [Browse...](#) ⓘ

[Upload server certificate data](#)

## Configuring the Trusted CA Certificate List on the VCS Expressway

The version of VCS Expressway you are using will determine how you configure the trusted CA certificate list.

### VCS Expressway X7.2.2

The default trusted CA certificate list for VCS Expressway X7.2.2 contains 140 certificates. It is very likely the public root CA that issued your server certificate is already part of the default trusted CA certificate list.

For details on how to configure the trusted CA certificate list on VCS Expressway X7.2.2, go to [Configuring the Trusted CA Certificate List on VCS Expressway X7.2.2](#).

### VCS Expressway Upgraded from X7.2.2 to X8.1

If you upgraded your VCS Expressway from X7.2.2 to X8.1, the trusted CA certificate list from X7.2.2 will be retained.

For details on how to configure the trusted CA certificate list on VCS Expressway upgraded from X7.2.2 to X8.1, go to [Configuring the Trusted CA Certificate List on VCS Expressway Upgraded from X7.2.2 to X8.1](#).

### VCS Expressway X8.1

If you are using a freshly installed VCS Expressway X8.1, you will need to load your own list of trusted CA certificates, because it does not (by default) contain any certificates in its default trusted CA certificate list.

In addition, you will need to add the root certificate used by the WebEx cloud to the default trusted CA certificate list on your VCS Expressway, which is DST Root CA X3.

For details on how to configure the trusted CA certificate list on a freshly installed VCS Expressway X8.1, go to [Configuring the Trusted CA Certificate List on VCS Expressway X8.1](#).

## Configuring the Trusted CA Certificate List on VCS Expressway X7.2.2

If the default trusted CA certificate list is not currently in use, it is recommended that you reset it back to the default CA Certificate. This will simplify the process of ensuring the required certificates are in place.

### Resetting the Trusted CA Certificate List on VCS Expressway X7.2.2

To reset the trusted CA certificate list on VCS Expressway X7.2.2, do the following:

- Step 1** Go to **Maintenance > Certificate management > Trusted CA certificate** and click **Reset to default CA certificate**.



#### Note

Your VCS Expressway must trust the certificate issuer of the server certificate that's passed by the server during the client/server SSL Handshake, in this case the server will be the SIP Proxy in the WebEx Cloud.

The default trusted CA certificate list on the VCS Expressway already contains the public root CA Certificate for the server certificate that the cloud will present. The root CA for the WebEx cloud is DST Root CA X3 with an intermediate CA of Cisco SSCA2.

If the server certificate was issued by the root CA (rather than an intermediate CA), it is likely that the root certificate is part of the default trusted CA list.

- Step 2** It is best practice to verify that the proper root certificate is present. You may do this by clicking **Show CA certificate**.

This will open in a new window displaying the default Trusted CA list that is currently loaded on the VCS Expressway.

- Step 3** Search for the root CA that issued the server certificate.

```

https://ctg-eft-vcse-1.cisco.com/download?file=CA_CERTIFICATE - Internet Explorer, optimized for Bing and MSN
dHBsdXMxGzAZBqNVBAMTEKRNsYXNzIDIGUHJpbWFyeSBdQTCCASiWdQYJKoZlIhvcNAQEBBQADggEP
ADCCAQoCggEBANxQ1tAS+DXSCHh6t1Jw/W/uz7kRy1134ezpfgSN1sxvc0NXyKwzCkTtA18cgCSR
5aiRVhKC9+Ar9NuuYS6JEI1rbLqzAr3VNsvINyPi8Fo3UjMXEuLRYE2+L0ER4/YXJQyLkcAbmXuZ
Vg2v7tK8R1fjeU17NIknJITesezpwE7+Tt9avkGtrAjFGA7v01PubNCdEgETjdyAYveVqUSISnFO
YFWe2yMZeVYHDD9jC1yw4r5+FfyUM1hBOHTE4Y+L3yasH7WLO7dDWwWuJK2tkIvEcupdM5i3y95e
e++U8Rs+yskhwcWYAqq19lt3m/V+11U0HGdpwPFC40es/CgcZ1UCAwEAAaOBjDCBiTAPBgNVHRME
CDAGAQH/AgEKMAsgA1UdDwQEAwIBBjAdBgNVHQ4EFgQU43Mt38sOKAze3bOkynm4jrvoMIkwEQYJ
YIZIAyb4QgEBBAQDAgEMDcGA1UdHwQwMC4wLKAqoC1GUmh0dHA6Ly93d3cuY2VydHBEdXMuY29t
LONSTC9jbgGFzc2IuY3JMa0GCSqGSIb3DQEBBQUAA4IBAQCnVM+IRBnL39R/AN9WM2K191EBkOvD
P9GIROkXe/nFLOgt5o8AP5tn9uQ3Nf0YtaLcF3n5QRIqWh8yfFC82x/xXp8HVG7
TtMTZGnkLuPT55sJmabq1ZvOgtD/vjzOUrMRfCpFF80Du5w1Fbqidon8BvEY0JN1
7UCmnYR0ObncHoUW21kbh1MAybuJfM6A1B4vFLQDJKgybW0aRywwv1bGp0ICcBvc
//1IMwrh3KWBk7tN3X3n57LNXMhqlf1i19o3EXXgIvnsG1knPGT2QIy4I5p4FTUcY
17+ijrRU
-----END CERTIFICATE-----

DST Root CA X3
=====
-----BEGIN CERTIFICATE-----
MIIDSjCCAjKqAwIBAgIQRK+wgNajJ7qJMDmGLvhAazANBgkqhkiG9w0BAQUFADA/
ExtEaWdpdGFsIFNpZ25hdHVyZSBUcnVzdCBDbY4xFzAVBgNVBAMTDkRlRVCSb290IENBI FgzMB4X
DTAwMDkzMDIwMTIxOVoXDTIxMDkzMDU0MDExNVowPzEkMCIgA1UEChMhRGlNaXRhbCBTaWduYXR1
cmUgVHJ1c3QgQ28uMRcwFQYDVOQDEw5EU1QgUm9vdCBDQSBYmZCCASiWdQYJKoZlIhvcNAQEBBQAD
ggEPADCCAQoCggEBAN+v6ZdGCINXtMxi2faQguzH0yxrMMpb7NnDfcdAwRgUi+DoM3ZJKuM/IUmT
rE4Orz5Iy2Xu/NMhD2XSktkyj4z193ewEnu1lcCJo6m67XMuegwGMoOifooUMMORoOEQOL15CjH9
UL2A2d+3UWODyOKIYepLYYHsUmu5ouJLG1ifSKOeDNoJjj4XLh7dIN9bxiqKqy69cK3FCxolkHry
xXtqzqTWMIn/5WgTe1QLyNau7FqcKh49ZLOMxt+/yUFw7B2y1SbsOFU5Q9D8/RhcQPGX69Wam40d
utolucbY38EVAjqr2m7xPi71XAicPNaDaeQQmxkqtl1X4+U9m5/wA10CAwEAAaNCMEAwDwYDVR0T
AQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFMSnsaR7LHH62+FLkHX/xBvghYkQ
MA0GCSqGSIb3DQEBBQUAA4IBAQCjG1ybFwBcqR7uKGY3Or+Dxz9Lwmmg1SBd4912RNI+DT69i kug
dB/OEIKcdBodfpga3csTS7MgROSr6cz8faXbauX+5v3gTt23ADq1cEmv8uXrAvHRAos2y5Q6XkjE
GB5YGV8eAlrwdPGxranwYaLbumR9YbK+r1mM6pZW87ipxZzR8srzJmWNojP41ZL9c8PDHIyh8bw
RLtTcm1D9S2ImlUnt1ir/md2cXjbDaJWFbM5JDGFoqgCWjBH4d1QB7wCC2AA62RjYJswvIjJEubS
fZGL+I0yJWW06XyxV3bqxbYoOb8VZRzI9neWagqNdwwYkQsEjgfbKbYK7p2CNTUQ
-----END CERTIFICATE-----

DST ACES CA X6
=====

```

If the server certificate is issued by the top-level root CA and NOT by an intermediate CA and the valid root CA certificate is present in the default trusted CA certificate list, then certificate configuration on your VCS Expressway is complete.

If the server certificate is issued by an intermediate CA, go to the next section.

#### Note

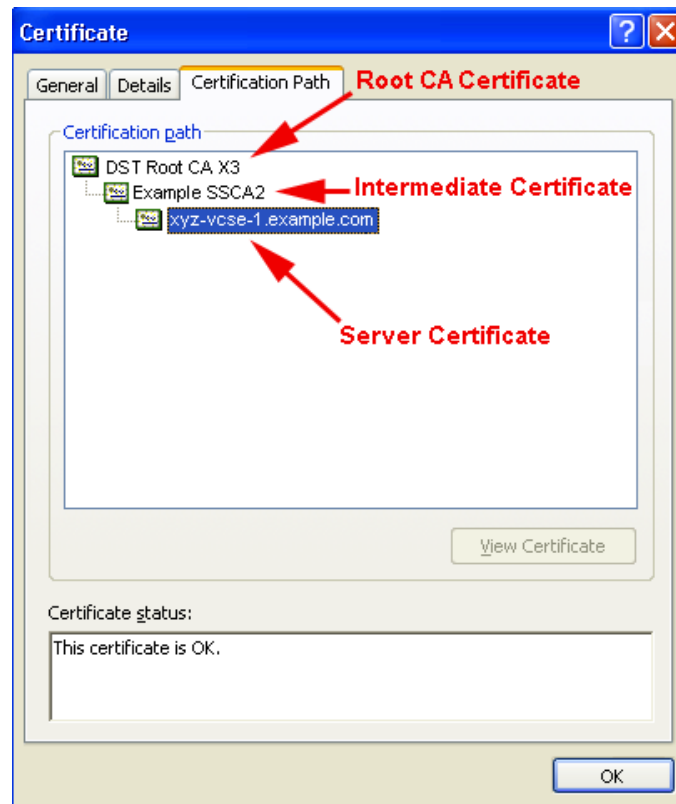
If the certificate for the top-level root CA that issued your server certificate is not part of the default trusted CA certificate list, you must add it using the same procedure that is described for stacking the intermediate CA certificate, detailed in the next section.

## Stacking the Intermediate CA Certificate in the Trusted CA Certificate List on VCS Expressway X7.2.2

In some cases, root CAs will use an intermediate CA to issue certificates.

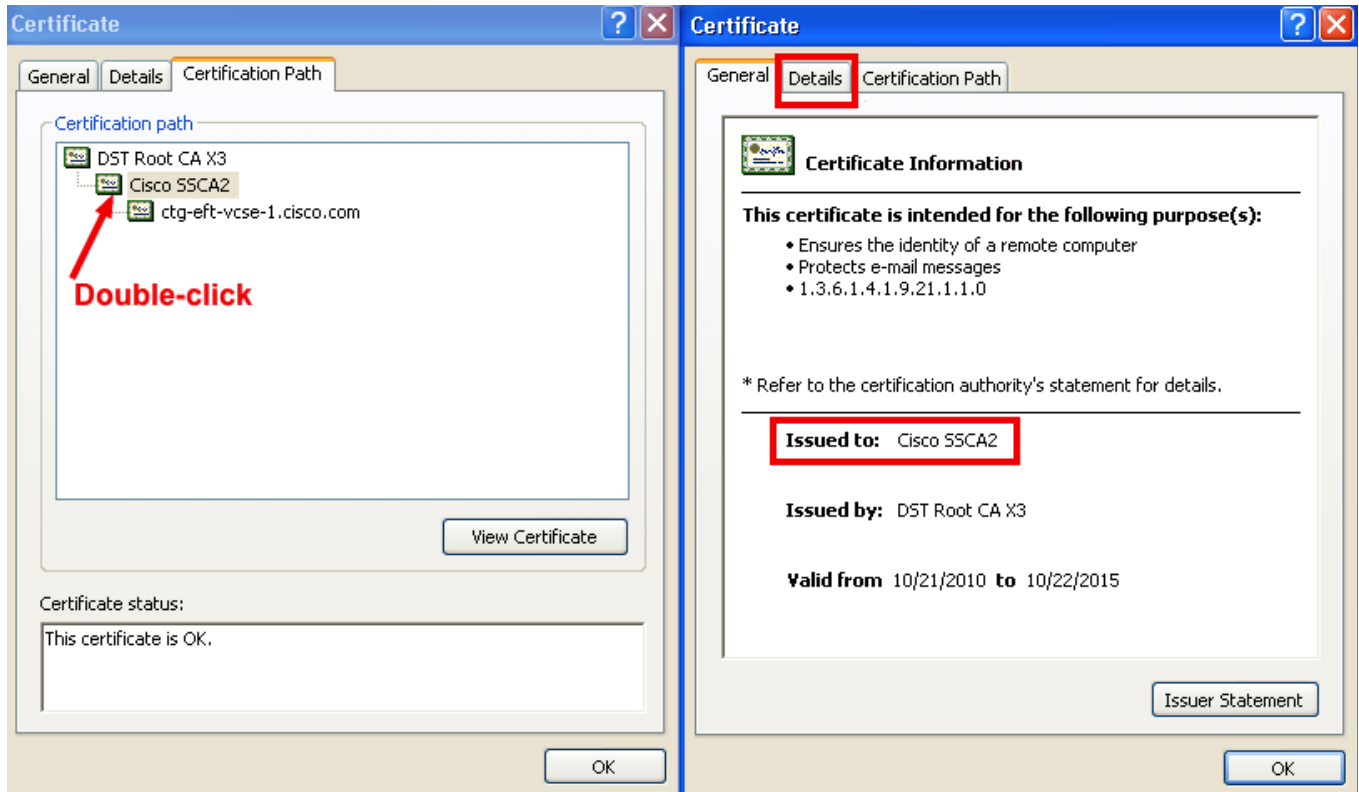
If the server certificate is issued by an intermediate CA, then you'll need to add the intermediate CA certificate to the default Trusted CA list.

Figure 5-1 Server Certificate in .CER File Format



Unless the public CA provided you the exact intermediate and root certificates that must be loaded, you can retrieve them from the server certificate. In some cases this is a better approach to ensure you're that you're stacking the correct intermediate CA certificate.

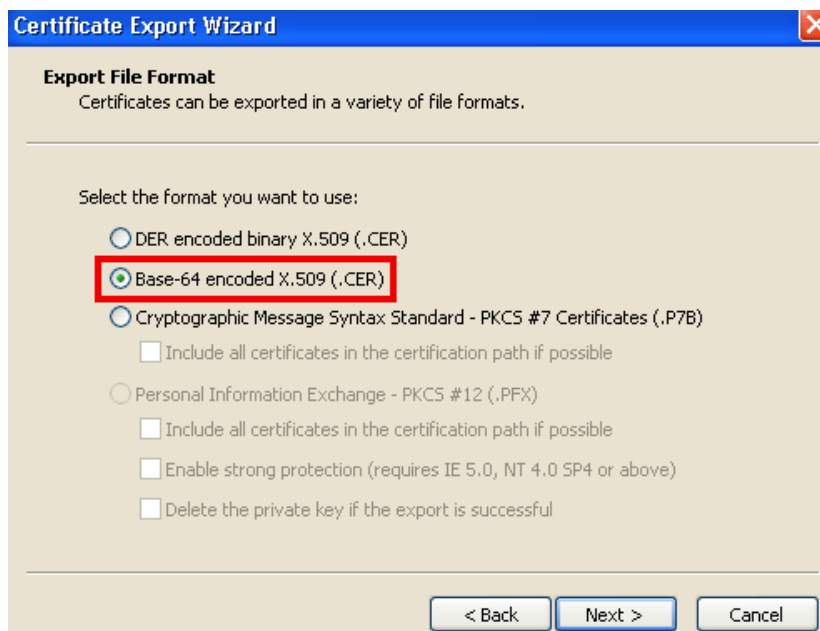
- 
- Step 1** Open the server certificate as a .CER file (see [Figure 5-1](#))
  - Step 2** Click the **Certification Path** tab, double-click the **Intermediate Certificate**.  
This will open the intermediate CA certificate in a separate certificate viewer.
  - Step 3** Make sure the 'Issued to' field displays the name of the Intermediate CA.
  - Step 4** Click the **Details** tab followed by **Copy to File...**



The 'Welcome to the Certificate Export Wizard' appears.

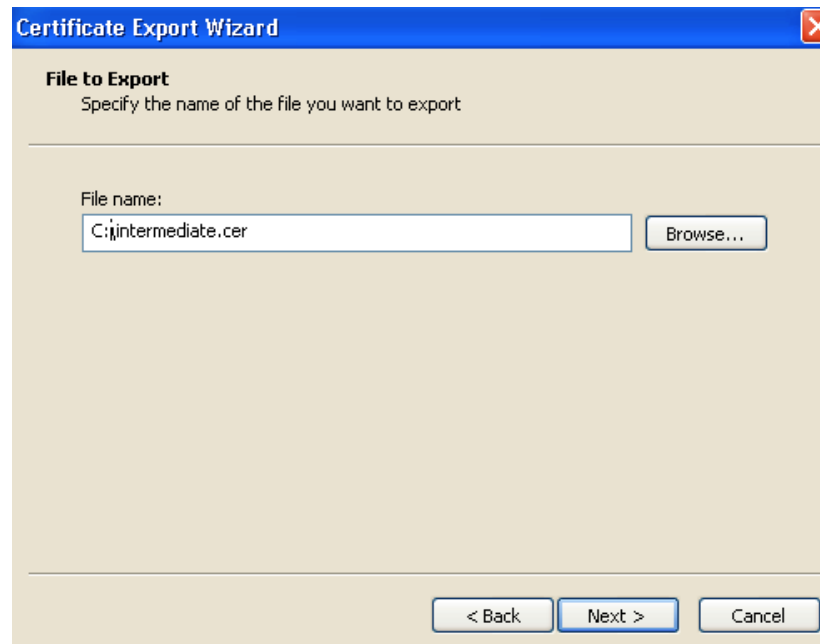
**Step 5** Click **Next**.

**Step 6** Choose **Base-64 encoded X.509 (.CER)** as the Export File Format and click **Next**.



**Step 7** Name the file, click **Next**, and **Finish**.





- Step 8** Copy the default Trusted CA list from the VCS Expressway by going to **Maintenance > Certificate management > Trusted CA certificate** and clicking **Show CA Certificate**. In the window that opens, select all contents.
- Step 9** Paste the contents into a text editing application such as Notepad.
- Step 10** Open the intermediate.cer file within a new window of your text editing application and copy the contents to your clipboard.
- Step 11** Do a search for the existing root CA certificate within the text file that contains the contents of the default Trusted CA list.
- Step 12** Paste the intermediate CA certificate above the root certificate.
- Step 13** Save the text file as .PEM file (Example: *NewDefaultCA.pem*)

Configuring the Trusted CA Certificate List on the VCS Expressway



**Note** If the root CA is not part of the default trusted CA list. Follow same procedure of stacking the intermediate CA certificate.

**Step 14** Click **Browse**, find your newly created/stacked Trusted CA list and click **Open**.

**Step 15** Click **Upload CA certificate**.

**Trusted CA certificate** You are here: [Maintenance](#) > [Certificate management](#) > Trusted CA certificate

**File uploaded:** CA certificate file uploaded. File contents - Certificates: 141, CRLS: 0. **Result**

**Upload**

Select the file containing trusted CA certificates   ⓘ

CA certificate

Certificate configuration on your VCS Expressway X7.2.2 is complete.

For additional details on how to configure client/server certificates, including information about security terminology and definitions, refer to the “Cisco VCS Certificate Creation and Use Deployment Guide (X7.2)” at the following location:

[https://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config\\_guide/Cisco\\_VCS\\_Certificate\\_Creation\\_and\\_Use\\_Deployment\\_Guide\\_X7-2.pdf](https://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/Cisco_VCS_Certificate_Creation_and_Use_Deployment_Guide_X7-2.pdf)

## Configuring the Trusted CA Certificate List on VCS Expressway Upgraded from X7.2.2 to X8.1

If the default trusted CA certificate list is not currently in use, it is recommended that you reset it back to the default CA Certificate. This will simplify the process of ensuring the required certificates are in place.

### Resetting the Trusted CA Certificate List on VCS Expressway Upgraded from X7.2.2. to X8.1

To reset the trusted CA certificate list on VCS Expressway X8.1, do the following:

- Step 1** Go to **Maintenance > Security certificates > Trusted CA certificate** and click **Reset to default CA certificate**.
- Note** Your VCS Expressway must trust the certificate issuer of the server certificate that’s passed by the server during the client/server SSL Handshake, in this case the server will be the SIP Proxy in the WebEx Cloud.
- The default trusted CA certificate list on the VCS Expressway already contains the public root CA Certificate for the server certificate that the cloud will present. The root CA for the WebEx cloud is DST Root CA X3 with an intermediate CA of Cisco SSCA2.
- If the server certificate was issued by the root CA (rather than an intermediate CA), it is likely that the root certificate is part of the default trusted CA list.
- Step 2** It is best practice to verify that the proper root certificate is present. You may do this by clicking **Show all (PEM file)**.

This will open in a new window displaying the default Trusted CA list that is currently loaded on the VCS Expressway.

- Step 3** Search for the root CA that issued the server certificate.

```

https://ctg-eft-vcse-1.cisco.com/download?file=CA_CERTIFICATE - Internet Explorer, optimized for Bing and MSN
-----BEGIN CERTIFICATE-----
MIIDISjCCAjKqAwIBAgIQRkK+wqNajJ7qJMDmGLvhAazANBgkqhkiG9w0BAQUFADA/
ExtEaWdpdGfIFNpZ25hdHVyZSBUcnVzdCBDbY4xZAVBgnVBAMTDkRTVCBSb290IENBIFgzMB4X
DTAwMDkzMDIxMTIxOVoXDTIxMDkzMDU0MDExNjVwPzEkMCIGA1UEChMhRGlnaXRhbCBTaWduYXR1
cmUgVHJ1c3QgQ28uMRcwFQYDVQDEw5EU1QgUm9vdCBDbQSBYmZCCAS1wDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAN+v6ZdQcINXtMxiZfaQguzH0yxrMpb7NndfcdAwRgUi+DoM3ZJKuM/IUmT
rE4Orz5Iy2Xu/NmHd2XSktkyj4z193ewEnu1lcCJo6m67XMuegWGMoOifooUMMORoOEQOL15CjH9
UL2AZd+3UWODyOKIYepLYYHsUmu5ouJLGi1fSKOeDNoJj4XLh7dIN9bxiQKqy69cK3FCxolkHRY
xXtqqzTWMIn/5WgTelQlyNau7Fqckh49ZLOMxt+/yUFw7B2y1SbsOFU5Q9D8/RhcQPGX69Wam40d
utolucbY38EVAjqr2m7xPi171XAicPNADaeQQmxkqt1lX4+U9m5/wA10CAwEAANCMEAwDwYDVR0T
AQH/BAUwAwEB/zAOBgnVHQ8BAf8EBAMCAQYwHQYDVRO0BbYEFMSnsaR7LHH62+FLKHX/xBVghYkQ
MA0GCSqGSIb3DQEBBQUAA4IBAQCjG1yFwBcqR7uKGY3Or+Dxz9Lwmg1SBd491ZRNI+DT69ikug
dB/OEIKcdBodfpga3csTS7MgROSR6cz8faXbauX+5v3gTt23ADq1cEmv8uXrAvHRAos2y5Q6XkjE
GB5YGV8eAlrWDPGxrancWYaLbumR9YbK+r1mM6pZW87ipxZzR8erzJmwN0jP41ZL9c8PDHIyh8bw
RLtTcm1D9S2ImlJnt1ir/md2cXjbDaJWFbM5JDGFoqgCWjBH4d1QB7wCCZAA62RjYJswVijJEubS
fZGL+T0yJWW06XyxV3bqxbYoOb8VZRzI9neWagqNdwYkQsEjgfbKbYK7p2CNTUQ
-----END CERTIFICATE-----

DST Root CA X3
=====

-----BEGIN CERTIFICATE-----
MIIDISjCCAjKqAwIBAgIQRkK+wqNajJ7qJMDmGLvhAazANBgkqhkiG9w0BAQUFADA/
ExtEaWdpdGfIFNpZ25hdHVyZSBUcnVzdCBDbY4xZAVBgnVBAMTDkRTVCBSb290IENBIFgzMB4X
DTAwMDkzMDIxMTIxOVoXDTIxMDkzMDU0MDExNjVwPzEkMCIGA1UEChMhRGlnaXRhbCBTaWduYXR1
cmUgVHJ1c3QgQ28uMRcwFQYDVQDEw5EU1QgUm9vdCBDbQSBYmZCCAS1wDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAN+v6ZdQcINXtMxiZfaQguzH0yxrMpb7NndfcdAwRgUi+DoM3ZJKuM/IUmT
rE4Orz5Iy2Xu/NmHd2XSktkyj4z193ewEnu1lcCJo6m67XMuegWGMoOifooUMMORoOEQOL15CjH9
UL2AZd+3UWODyOKIYepLYYHsUmu5ouJLGi1fSKOeDNoJj4XLh7dIN9bxiQKqy69cK3FCxolkHRY
xXtqqzTWMIn/5WgTelQlyNau7Fqckh49ZLOMxt+/yUFw7B2y1SbsOFU5Q9D8/RhcQPGX69Wam40d
utolucbY38EVAjqr2m7xPi171XAicPNADaeQQmxkqt1lX4+U9m5/wA10CAwEAANCMEAwDwYDVR0T
AQH/BAUwAwEB/zAOBgnVHQ8BAf8EBAMCAQYwHQYDVRO0BbYEFMSnsaR7LHH62+FLKHX/xBVghYkQ
MA0GCSqGSIb3DQEBBQUAA4IBAQCjG1yFwBcqR7uKGY3Or+Dxz9Lwmg1SBd491ZRNI+DT69ikug
dB/OEIKcdBodfpga3csTS7MgROSR6cz8faXbauX+5v3gTt23ADq1cEmv8uXrAvHRAos2y5Q6XkjE
GB5YGV8eAlrWDPGxrancWYaLbumR9YbK+r1mM6pZW87ipxZzR8erzJmwN0jP41ZL9c8PDHIyh8bw
RLtTcm1D9S2ImlJnt1ir/md2cXjbDaJWFbM5JDGFoqgCWjBH4d1QB7wCCZAA62RjYJswVijJEubS
fZGL+T0yJWW06XyxV3bqxbYoOb8VZRzI9neWagqNdwYkQsEjgfbKbYK7p2CNTUQ
-----END CERTIFICATE-----

DST ACES CA X6
=====

```

If the server certificate is issued by the top-level root CA and NOT by an intermediate CA and the valid root CA certificate is present in the default trusted CA certificate list, then certificate configuration on your VCS Expressway is complete.

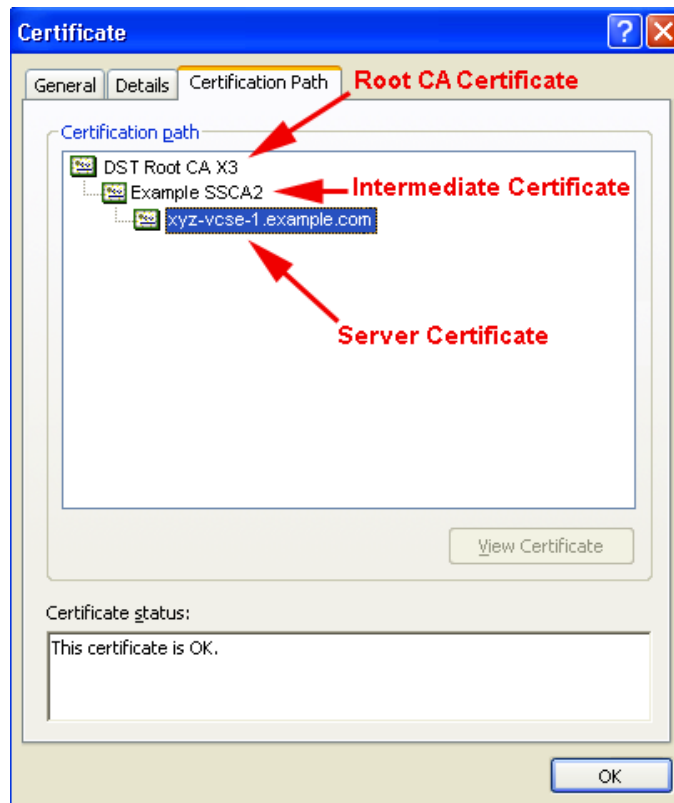
If the server certificate is issued by an intermediate CA or if the certificate for the top-level root CA that issued your server certificate is not part of the trusted CA certificate list, you must add it to the trusted CA certificate list, as detailed in the next section.

## Adding the Intermediate CA Certificate to VCS Expressway X8.1

In some cases, root CAs will use an intermediate CA to issue certificates.

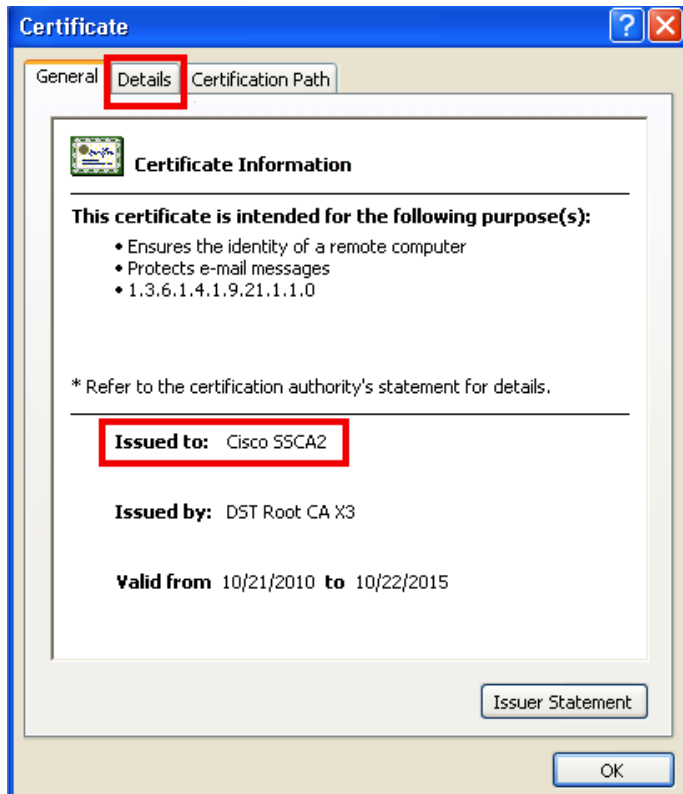
If the server certificate is issued by an intermediate CA, then you'll need to add the intermediate CA certificate to the default trusted CA certificate list.

Figure 5-2 Server Certificate in .CER File Format



Unless the public CA provided you the exact intermediate and root certificates that must be loaded, you can retrieve them from the server certificate. In some cases this is a better approach to ensure you're that you're stacking the correct intermediate CA certificate.

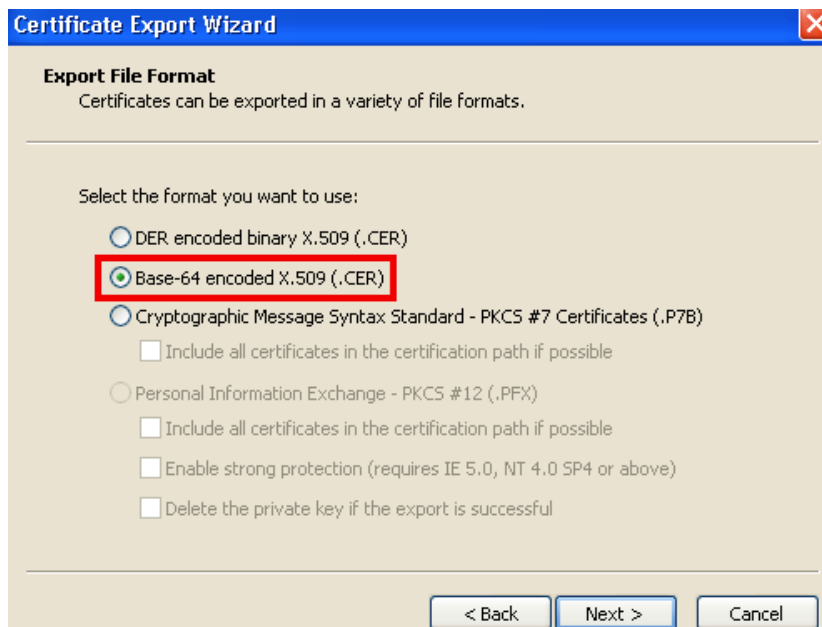
- 
- Step 1** Open the server certificate as a .CER file (see [Figure 5-2](#))
  - Step 2** Click the **Certification Path** tab.
  - Step 3** Double-click the **Intermediate Certificate**.  
This will open the intermediate CA certificate in a separate certificate viewer.
  - Step 4** Make sure the 'Issued to' field displays the name of the Intermediate CA.
  - Step 5** Click the **Details** tab followed by **Copy to File...**



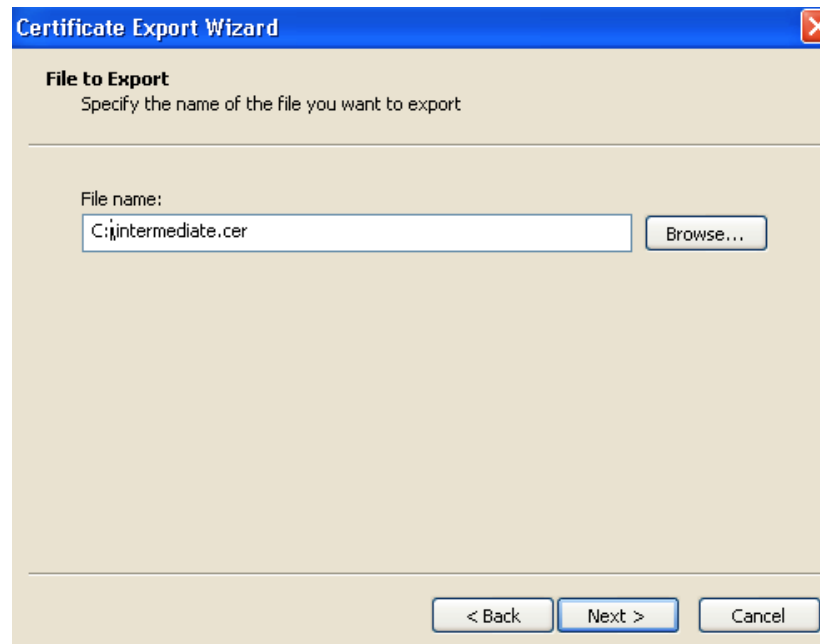
The 'Welcome to the Certificate Export Wizard' appears.

**Step 6** Click **Next**.

**Step 7** Choose **Base-64 encoded X.509 (.CER)** as the Export File Format and click **Next**.



**Step 8** Name the file, click **Next**, and **Finish**.



**Step 9** Change the extension of your intermediate CA certificate from .cer to .pem.

For example: **intermediate.pem**

**Step 10** In VCS Expressway X8.1, go to **Maintenance > Security certificates > Trusted CA certificate**.

**Step 11** Click **Browse**, find your intermediate CA certificate and click **Open**.

**Step 12** Click **Append CA certificate**.

Certificate configuration on your VCS Expressway X8.1 is complete.

---

For additional details on how to configure client/server certificates, including information about security terminology and definitions, refer to the “Cisco VCS Certificate Creation and Use Deployment Guide (X8.1)” at the following location:

[http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config\\_guide/X8-1/Cisco-VCS-Certificate-Creation-and-Use-Deployment-Guide-X8-1.pdf](http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/X8-1/Cisco-VCS-Certificate-Creation-and-Use-Deployment-Guide-X8-1.pdf)

## Configuring the Trusted CA Certificate List on VCS Expressway X8.1

Because a freshly installed VCS Expressway X8.1, does not have certificates in its trusted CA certificates list, you must add the following two certificates:

- The DST Root CA certificate (the root CA for the WebEx cloud)
- The CA certificate of the CA that issued your server certificate

## Adding the DST Root Certificate to VCS Expressway X8.1

Your VCS Expressway must trust the certificate issuer of the server certificate that's passed by the server during the client/server SSL Handshake, in this case the server will be the SIP Proxy in the WebEx Cloud, which is DST Root CA.

To add the DST Root certificate to the trusted CA certificate list on VCS Expressway X8.1, do the following:

- 
- Step 1** Go to: [http://www.identrust.com/doc/SSLTrustIDCAA5\\_DSTCAX3.p7b](http://www.identrust.com/doc/SSLTrustIDCAA5_DSTCAX3.p7b)  
A page with the DST Root certificate contents appears with “-----Begin Certificate-----” at the top.
  - Step 2** Select and copy the entire contents of the page.
  - Step 3** Open a text editor, such as Notepad, on your computer and paste the contents of the DST Root certificate.
  - Step 4** Save the text file with an extension of .PEM. For example: **dst\_root\_ca.pem**.
  - Step 5** In VCS Expressway X8.1, go to **Maintenance > Security certificates > Trusted CA certificate**.
  - Step 6** Click **Browse**, select the DST Root certificate you saved in step 4 and click **Open**.
  - Step 7** Click **Append CA certificate**.
- 

## Adding the Root or Intermediate CA Certificate to VCS Expressway X8.1

For the WebEx cloud to trust your VCS Expressway's server certificate, you must add the root or intermediate CA certificate for the CA that issued your server certificate.

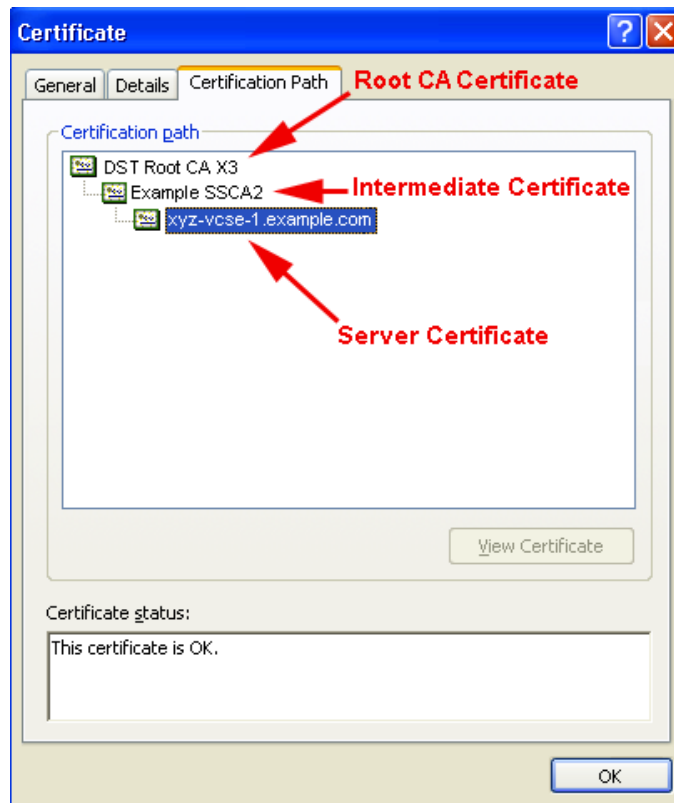
Unless the public CA provided you the exact intermediate or root certificates that must be loaded, you can retrieve them from the server certificate. In some cases this is a better approach to ensure you're that you're stacking the correct intermediate CA certificate.

To add the root or intermediate CA to VCS Expressway X8.1, do the following:

- 
- Step 1** Open the server certificate as a .CER file
  - Step 2** Click the **Certification Path** tab. (see [Figure 5-3](#))



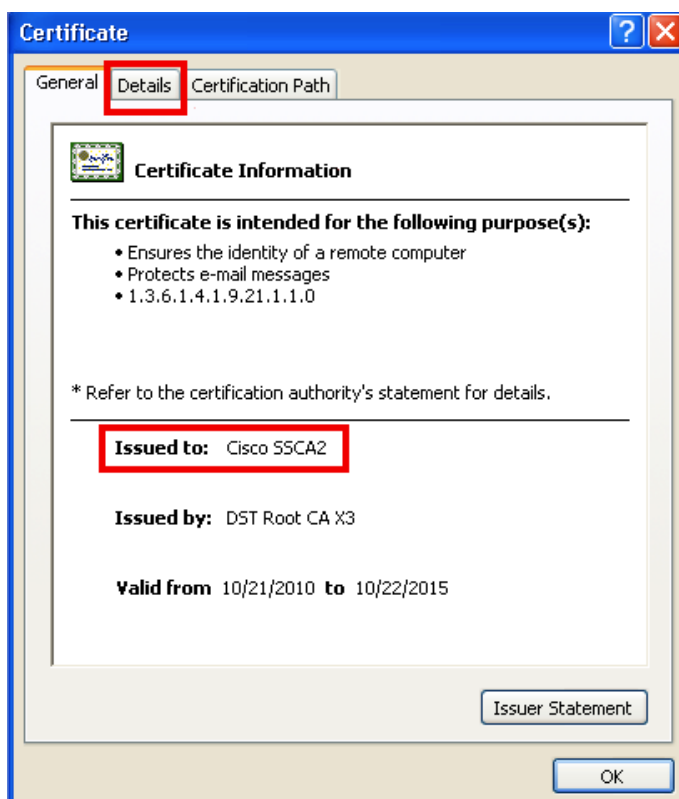
Figure 5-3 Server Certificate from Intermediate CA in .CER File Format



**Note**

The server certificate example shown here is one issued by an intermediate CA. If your certificate was issued by a root CA, you would only see 2 certificates (the root and server certificates).

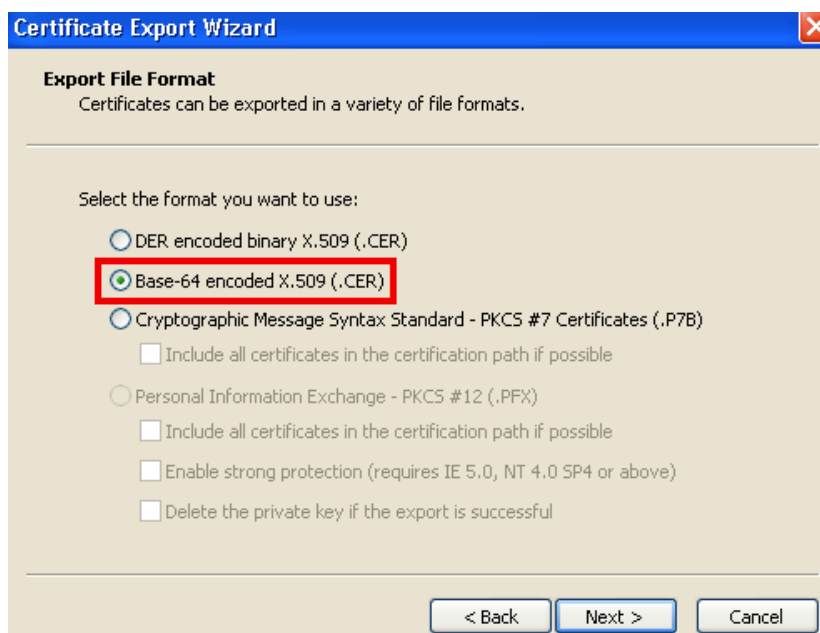
- Step 3** Open the CA certificate:
- If your certificate was issued by a root CA, double-click the **Root CA Certificate**.
  - If your certificate was issued by an intermediate CA, double-click the **Intermediate Certificate**.
- This will open the CA certificate in a separate certificate viewer.
- Step 4** Make sure the 'Issued to' field displays the name of the root or intermediate CA.
- Step 5** Click the **Details** tab followed by **Copy to File...**



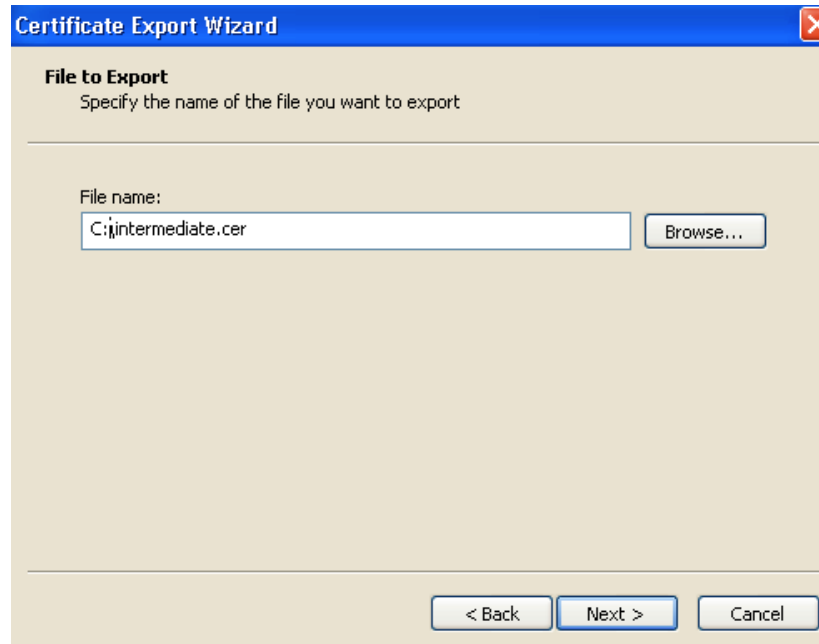
The 'Welcome to the Certificate Export Wizard' appears.

**Step 6** Click **Next**.

**Step 7** Choose **Base-64 encoded X.509 (.CER)** as the Export File Format and click **Next**.



**Step 8** Name the file, click **Next**, and **Finish**.



- Step 9** Change the extension of your root or intermediate CA certificate from .cer to .pem.  
For example: **root.pem** or **intermediate.pem**
- Step 10** In VCS Expressway X8.1, go to **Maintenance > Security certificates > Trusted CA certificate**.
- Step 11** Click **Browse**, find your root or intermediate CA certificate and click **Open**.
- Step 12** Click **Append CA certificate**.
- Certificate configuration on your VCS Expressway X8.1 is complete.
- 

For additional details on how to configure client/server certificates, including information about security terminology and definitions, refer to the “Cisco VCS Certificate Creation and Use Deployment Guide (X8.1)” at the following location:

[http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config\\_guide/X8-1/Cisco-VCS-Certificate-Creation-and-Use-Deployment-Guide-X8-1.pdf](http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/X8-1/Cisco-VCS-Certificate-Creation-and-Use-Deployment-Guide-X8-1.pdf)

