

SSL Cert CSR Creation and Installation for Cobalt RaQ4/XTR

How to generate a CSR in Cobalt RaQ4-XTR Web Server

Enable SSL on a Virtual Site

1. Browse to the Server Management area
2. Click the Green Wrench (RaQ4) or Pencil (XTR) button next to the virtual site which you want to enable SSL
3. This will bring up the Site Management UI
4. On the left side Click Site Settings (if in XTR select General)
5. Select the Checkbox to Enable SSL
6. Click Save Changes

Create a Self Signed SSL Certificate:

After you have enabled SSL, you will generate a Self Signed SSL Certificate.

1. Proceed to the Server Management screen
2. Again as above - Click the Green Wrench (RaQ4) or Pencil (XTR) button next to the virtual site which you want to enable SSL
3. On the left side Click Site Settings
4. This will open the Certificate Subject Information table
Enter the following details:

Country (two-letter Country Code)
State (full name of State or County)
Locality Enter (name of City or Locality)
Organization (Legal Organization/Company or Personal Name)
Organizational Unit (this can be any name such as a department)
5. Click Generate Self-Signed Certificate from the bottom menu
6. Select - Save Changes
7. RaQ4/XTR generates the screen with your new Self-Signed Certificate in the Certificate Request & Certificate fields

Site Management - digicert.com

User Management

List Management

Site Settings

FTP Settings

SSL Settings

Site Usage

Backup

Restore

Server Management

Certificate Subject Information	
Country	US
State	Utah
Locality	Lindon
Organization	DigiCert, Inc.
Organizational Unit	Security

Certificate Request

-----BEGIN CERTIFICATE REQUEST-----

```

MIIB7jCCAveCAQAwaOxCzAJBgNVBAYTA1VLMRhwEQYDVQIEwpxZ2XNOIF1vcmtz
MREvDwYDVQQHEwhCcmFkZm9yZDEQA4GA1UEChMHQ1REIEx0ZDEUMBIGA1UECxML
RGV2ZWxvcG1lbnQxIDAeBgNVBANTF2R1dmVzLnN1Y3V5ZS5jb21vZG8ubmVOMSw
KgYJKoZIhvcNAQkBFhh1ZG1pbkpkBkZkZ1bC5zZW51cmUyZ9tb2RvLm5ldDCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAtdBZ+xxwYQW9Jy9A82U3herwO/BikOh+S
09F72h19/ESALKs43mj6n8yZG0x3I5Hq2PIMaiJBUQJd9uao3vdep+/Zd8Nd5yag
ku2GDCCXCD3VDxnsV1+C8ZG5yBCGyUYRVZJtUzqSLAJqI3Jr8qPKwXyrS1vfhdt5
a/31VsHI738CAvEAaAAMAOGCSqGSIb3DQEBAUAA4GBAJKinrn/jj9OhFRHOW3T
31DgGz4CuXgcAkIONd1KHSuy79h5WymSFRFR31+zx12tGOEGm24VQM8B/d09m
t98Umkyt3XM3qHS0g459ww6pEKNRnn46zAhCC3aEdy6vtg+J2aQX1Oar6eiuxbbf
SwwE8Fm/AmJNZCYsuX9DdSgk
-----END CERTIFICATE REQUEST-----

```

Certificate

```

-----BEGIN CERTIFICATE-----
mRjsdyOR6tjyDGoIQVECKfBmqN73Xqfv2XfDXecmoJLthgw1wg91Q827FdfgvGRu
cgQhs1GEVUSbVM6kiwCaiNya/KjwysF8q+Zb34XbeWv95VbByO9/AgMBAAEwDQYJ
KoZIhvcNAQEEBQADgYEAfM08DHqNkq/vheNnLyRHKTzTNRlgN7Zffyo+MabZIrN
rWz+Kr/KYdyoQnva9tRsOX6RRFVSTCZYcaaLalv5h5t13oEESyVHvtoGyPvYZuI9
47poU8HbqQJNBycK6sqHygB432x90J2dExkn9KQucr1BiarWaz2YOTBOfaymiA=

```

RSA SECURED

Use manually entered certificate

Save Changes

Paste CSR

Copy the all contents of the Certificate Request and save it to text file and [submit to us](#) for our process.

Example of code copied:

```

-----BEGIN CERTIFICATE REQUEST-----
text ...
-----END CERTIFICATE REQUEST-----

```

SSL Digital Certificate Installation on Cobalt

1) Installing your Primary Server Certificate (your_domain_name.crt):

1. In the Server Management screen, click on the Green icon (RaQ4 is a Wrench icon and XTR is a Pencil icon) for the site you are securing.
2. Choose SSL settings.

- Copy your Primary Server Certificate (your_domain_name.crt) into the form. Make sure you copy the entire contents. Example:
 -----BEGIN CERTIFICATE-----
 text ...
 -----END CERTIFICATE-----
- Select 'Use manually entered certificate' from the drop-down menu, and click 'Save Changes'.



2) Installing the Intermediate Certificate:

- With Apache you will install the Intermediate SSL Certificate. Copy the file you received.
- Edit your httpd.conf file by adding the following line to the SSL section.
 SSLCACertificateFile /your_directory_path/IntermediateCA.crt

This should make your config file look something like this (directories may vary on your server):

```
<VirtualHost 192.168.0.1:443>
DocumentRoot /var/www/html2
ServerName www.yourdomain.com
SSLEngine on
SSLCertificateFile /etc/ssl/crt/your_domain_name.crt
SSLCertificateKeyFile /etc/ssl/crt/your_private.key
SSLCACertificateFile /etc/ssl/crt/IntermediateCA.crt
</VirtualHost>
```

3) Save your config file, and restart Apache.