




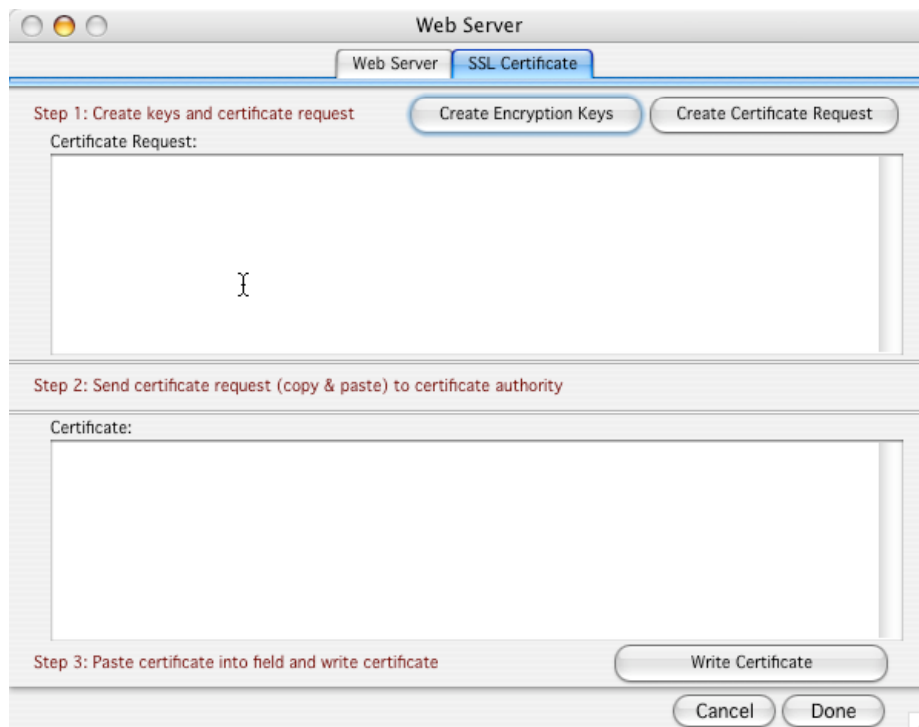
## Generating an SSL Certificate for use with Med-Center

### Introduction

This technical note discusses generating Secure Socket Layer (SSL) certificates to allow secure communications to Med-Center using a web browser. Two methods of generating the certificate are covered. The first method involves generating a certificate request and sending it to a certification agency. The second method involves generating a self-signed certificate using the standard Macintosh utilities available within UNIX.

### Method 1 “Generating Certificate Request using a Certificate Authority”

1. Start by opening Med-Center and choosing the ‘Administrator’ module.
2. Next, open the ‘Web Server’ dialog by pressing the web server icon. 
3. Next, select the ‘SSL Certificate’ tab
4. The SSL Certificate screen (Figure 1) should be shown.



**Figure 1 “SSL Certificate Setup Screen”**

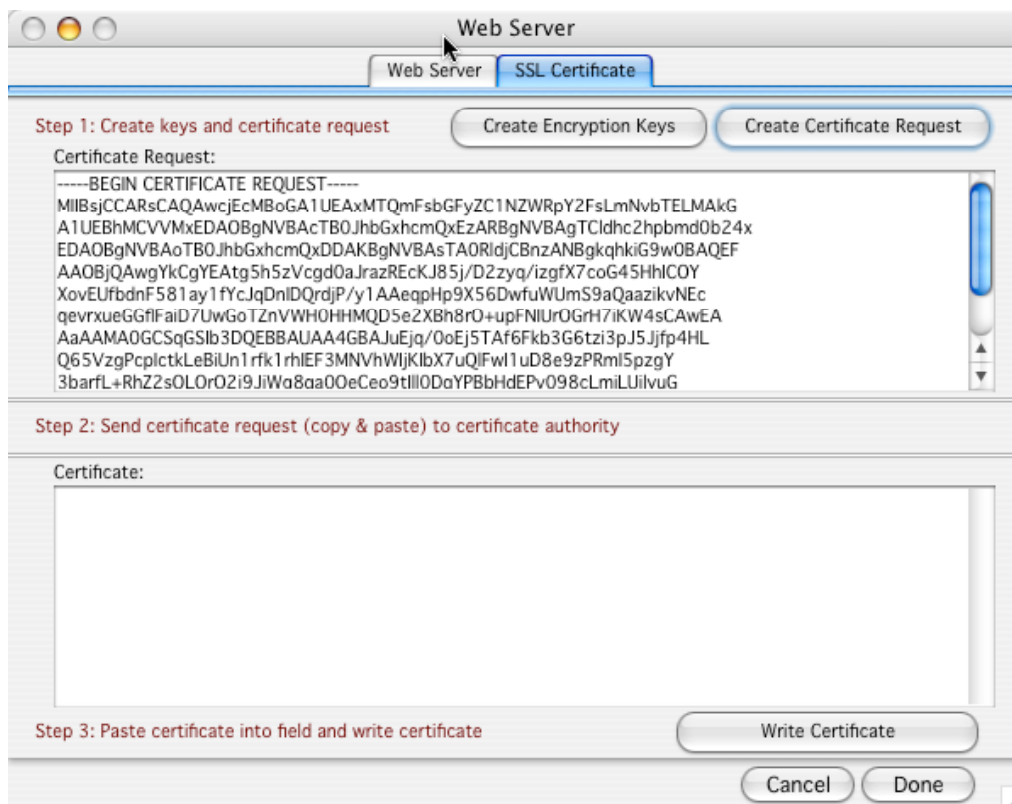
5. The next few steps will create the encryption keys and the certificate request that can then be sent to the certificate authority.
6. Create the encryption keys: Press the ‘Create Encryption keys’ button.
7. Create the certificate request: Press the ‘Create Certificate Request’ button and enter the appropriate information when requested. The dialog will look similar to the following screen shot. It is important that the site name have a valid domain name format.



The image shows a 'Certificate Information' dialog box. It contains several text input fields: 'Site Name' (with 'Ballard-Medical.com' entered), 'Country' (with 'US'), 'State' (with 'Washington'), 'City' (with 'Ballard'), 'Org Name', and 'Org Unit'. There are 'Cancel' and 'Continue' buttons at the bottom. A note below the Site Name field states: 'Note: Must be valid domain name'.

**Figure 2 “Certificate Request Information”**

8. The certificate request will look like what is shown in Figure 3. The certificate text is what should be copied and pasted into the form or document that is sent to the certificate authority.



The image shows a 'Web Server' dialog box with two tabs: 'Web Server' and 'SSL Certificate'. The 'SSL Certificate' tab is active. It has two buttons: 'Create Encryption Keys' and 'Create Certificate Request'. Below these is a text area labeled 'Certificate Request:' containing a long string of base64-encoded text. Below that is a section labeled 'Step 2: Send certificate request (copy & paste) to certificate authority' with a large empty text area labeled 'Certificate:'. At the bottom, there are buttons for 'Write Certificate', 'Cancel', and 'Done'.

**Figure 3 “Certificate Request Generated”**

9. Each certificate authority has their own process for submitting a certificate request and then delivering a processed certificate. The most common submittal technique uses the web and usually results in a certificate within minutes of the submittal. Common certificate authorities include Verisign (<http://www.verisign.com>) and Thawte (<http://www.thawte.com>).

## Technical Note – SSL Certificates

10. Finally, once your certificate has arrived, copy and paste it into the certificate area of the SSL Certificate screen. Press 'Write Certificate' to place the certificate correctly for Med-Center to use. The screen shot will look similar to Figure 4.

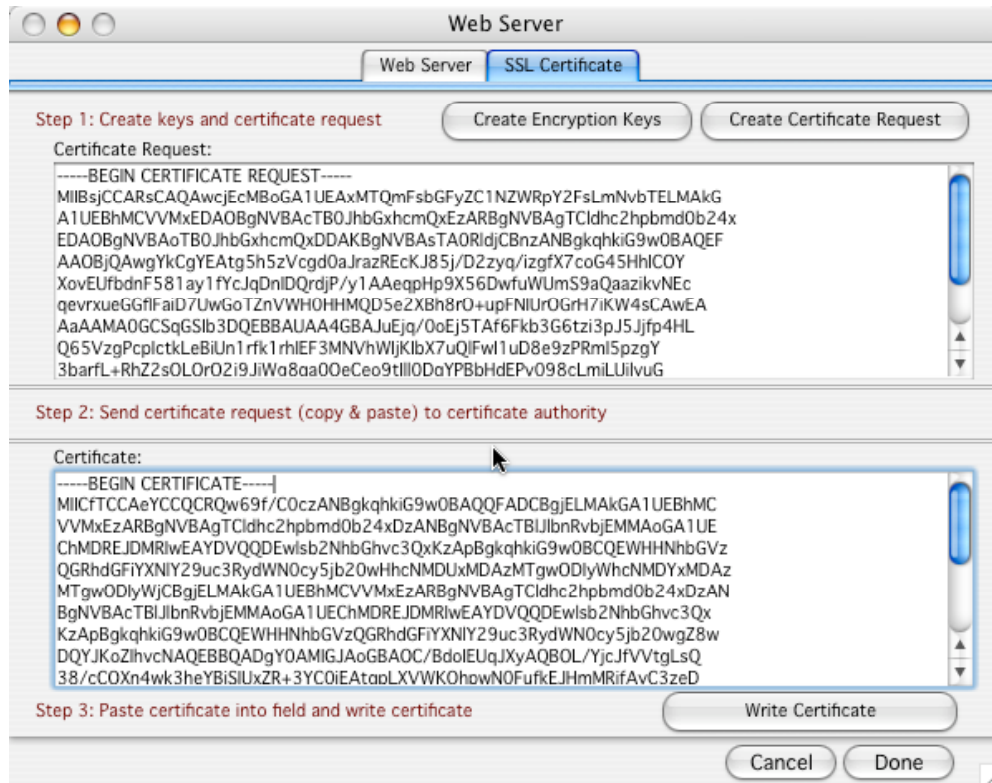


Figure 4 “SSL Certificate”

### Method 2 “Generating Self-Signed Certificates using Macintosh OSX”

1. Start by opening the Macintosh terminal program available in the utilities folder.
2. Generate the private key by entering the following command:

```
openssl genrsa -des3 -out server.key 1024
```

3. During the generation of the CSR, you will be prompted for several pieces of information. These are the X.509 attributes of the certificate. One of the prompts will be for "Common Name (e.g., Server name)". It is important that this field be filled in with the fully qualified domain name of the server to be protected by SSL. Generate the CSR (Certificate Signing Request) by entering the following command:

```
openssl req -new -key server.key -out server.csr
```

4. Remove the pass phrase by entering these commands:

```
cp server.key server.key.org  
openssl rsa -in server.key.org -out server.key
```

## Technical Note – SSL Certificates

---

5. Generate a self-sign certificate (in this case for 365 days) by entering the following command:

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

6. From the Finder, rename the private key file from “server.key” to “key.pem”. Also rename the certificate from “server.crt” to “cert.pem”.
7. Finally, Place both of these files into the Med-Center folder. The certificates will be effective the next time Med-Center is opened.

### Summary

SSL Certificates allow secure web connections to be made to Med-Center. This technical note covered the basics of generating a certificate request to send to a certificate authority or creating a self-signed certificate using the Macintosh OSX terminal utility.