

TeleDynamic | *we get it*  
COMMUNICATIONS



---

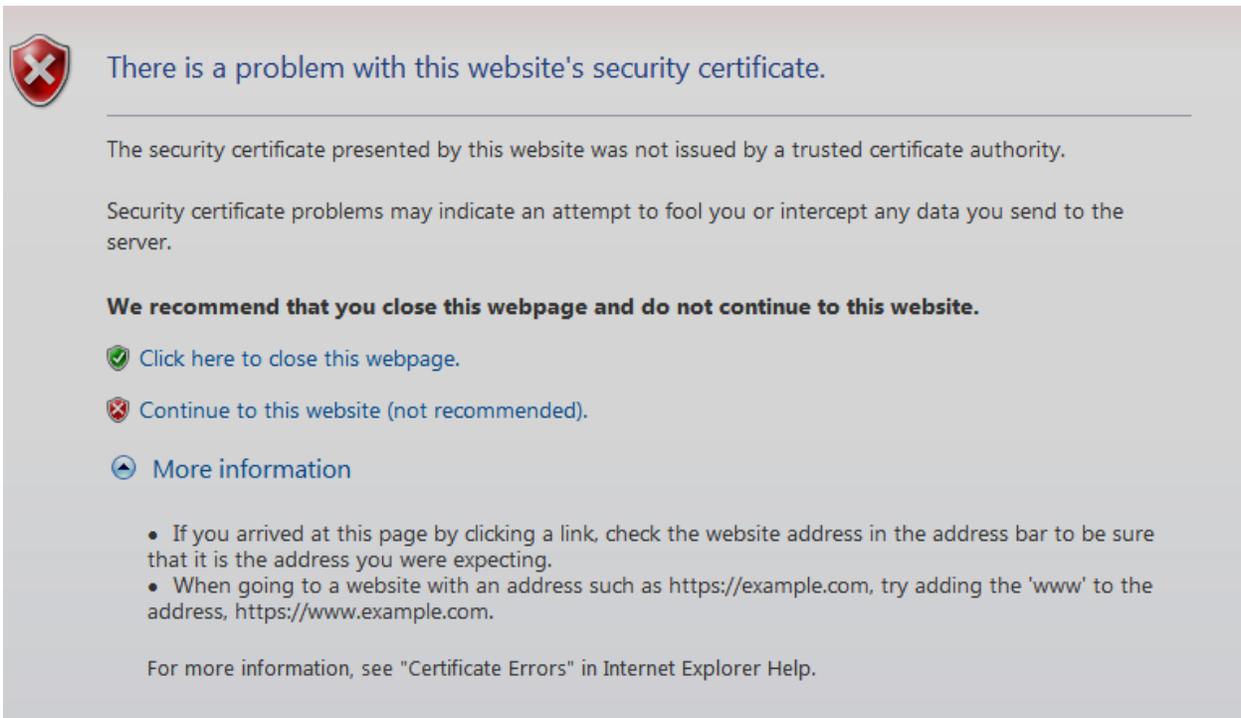
# SSL Certificate Creation

---

## SWITCHBOARD SECURITY

The Switchvox Switchboard uses https which is more secure than http. https requires a security certificate to be installed or for each user to allow a security exception. Teledynamic recommends using an SSL certificate, but ultimately, it is your decision on whether you allow end users to make the exceptions or provide a SSL certificate. We outline three options here.

**Option 1: (not recommended):** Have users override the warning message. Below is an example from IE8. Depending on the browser you will be asked if you wish to proceed, please select to do so. Some browsers can be set to remember this choice, but others will require your permission each time.



The screenshot shows a security warning dialog box with a red shield icon containing a white 'X'. The text reads: "There is a problem with this website's security certificate." Below this, it states: "The security certificate presented by this website was not issued by a trusted certificate authority." It further explains: "Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server." A bold recommendation follows: "We recommend that you close this webpage and do not continue to this website." There are three options with icons: a green checkmark for "Click here to close this webpage.", a red 'X' for "Continue to this website (not recommended).", and a blue shield with a white 'X' for "More information". Below these are two bullet points: "If you arrived at this page by clicking a link, check the website address in the address bar to be sure that it is the address you were expecting." and "When going to a website with an address such as https://example.com, try adding the 'www' to the address, https://www.example.com." At the bottom, it says: "For more information, see 'Certificate Errors' in Internet Explorer Help."

**Option 2: Self-Signed Certificates** (process shown is for IE8 – the process for different browsers would vary):

1. Browse to the site whose certificate you want to trust.
2. When told "There is a problem with this website's security certificate.", choose "Continue to this website (not recommended)."
3. Select Tools->Internet Options.
4. Select Security->Trusted sites->Sites.
5. Confirm the URL matches, and click "Add" then "Close".
6. Close the "Internet Options" dialog box with either "OK" or "Cancel".
7. Refresh the current page.
8. When told "There is a problem with this website's security certificate.", choose "Continue to this website (not recommended)."
9. Click on "Certificate Error" at the right of the address bar and select "View certificates".
10. Click on "Install Certificate...", then in the wizard, click "Next".
11. On the next page select "Place all certificates in the following store".
12. Click "Browse", select "Trusted Root Certification Authorities", and click "OK".
13. Back in the wizard, click "Next", the "Finish".
14. If you get a "Security Warning" message box, click "Yes".
15. Dismiss the message box with "OK".
16. Select Tools->Internet Options.
17. Select Security->Trusted sites->Sites.
18. Select the URL you just added, click "Remove", then "Close".
19. Now shut down all running instances of IE, and start up IE again.
20. The site's certificate should now be trusted.

### Option 3: SSL Certificate (recommended):

Here's the process for using a customer SSL Certificate:

1. [Create a Certificate Service Request](#)
2. [Obtain an SSL Certificate](#)
3. [Install the Certificate](#)

#### Step #1. Create a Certificate Signing Request (CSR)

Use a utility to create a CSR, and a Key file. The CSR file will end in .csr and the Key will end in .key

On a machine such as a Mac with OS X, at the commandline you will use **openssl**:

1. openssl genrsa -out .key 2048
2. openssl req -new -key .key -out .csr

Answer the questions that openssl presents. To leave a field blank, use a period (.) For Wildcard SSL, you need to prepend the domain name with asterisk dot (\*). For example: **\*.domain.com**.

- Country Name (2 letter code) [AU]: **US**
- State or Province Name (full name) [Some-State]: **Arizona**
- Locality Name (eg, city) []: **Phoenix**
- Organization Name (eg, company) [Internet Widgits Pty Ltd]: **MyCompany Ltd**
- Organizational Unit Name (eg, section) []: **IT**
- Common Name (eg, YOUR name) []: **mysubdomain.mydomain.com** or **\*.mydomain.com**
- Email Address []: [email@mydomain.com](mailto:email@mydomain.com)

Please enter the following 'extra' attributes to be sent with your certificate request (no password necessary)

- A challenge password []: **IamN0tT3llinYou**
- An optional company name []:

The steps above will create a CSR file (.csr) and a Key file (.key).

As an alternative to openssl on the command line, you can try this URL:

[http://www.instantssl.com/ssl-certificate-support/csr\\_generation/ssl-cer...](http://www.instantssl.com/ssl-certificate-support/csr_generation/ssl-cer...)

## Step #2. Obtain a Certificate

1. Take the CSR to a Certificate Authority (CA) such as Godaddy.
2. Purchase a SSL Certificate (CRT).
3. Request or generate the CRT; you will need your CSR.  
Godaddy requires that you request the CRT and will prompt you for your CSR. Godaddy has a certificate manager page when you log in to your account on their website.
4. Download the CRT. You may receive some additional files, but the CRT is the one that you really need.
5. The files may be zipped. If so, expand the files.

Now you should have two files (note that your crt and key file names will be different that the examples below and they might not reflect your domain name):

- yourdomain.crt (your CA creates this using your CSR)
- yourdomain.key (you created this at the same time you created your CSR)

The contents of the files should look something like this:

---

-----BEGIN RSA PRIVATE KEY-----

MIIEo... followed by a large block of text...

-----END RSA PRIVATE KEY-----

---

### **Step #3. Install the Certificate in Switchvox**

- To install your certificate in Switchvox:
  1. Open these files in a plain text editor and copy the **WHOLE\*\*\*** contents of each file.
  2. Go to **Server > Networking > HTTPS & Proxy** in the Switchvox web suite.
  3. Open yourdomain.crt in a plain text editor and paste the entire contents into **X.509 Certificate in PEM Format**
  4. Open yourdomain.key in a plain text editor and paste the entire contents into **RSA Private Key in PEM Format**
  5. Leave **Intermediate CA Certificate** empty. This is created automatically.
  6. Click **Save HTTPS & Proxy**.

Now you should be able to use the Switchvox web suite without having to accept a private certificate.