eTrigue Corporation
6399 San Ignacio Avenue
San Jose, CA 95119

www.etrigue.com

800.858.8500 toll-free
408.490.2901 fax

eTrigue® DemandCenter®

Adding HTTPS / SSL Support to eTrigue Landing Pages

Introduction - Why do I need to enable HTTPS on my subdomain?

We're often asked why it's essential to make landing pages "secure". Secure means that pages are served as HTTPS instead of HTTP. The short answer is that HTTPS has become the standard, it's expected and in some case required for serving web pages.

Hypertext Transfer Protocol Secure (HTTPS) adds a layer of security on the data in transit from a web page to a browser through a secure socket layer (SSL) or transport layer security (TLS) protocol connection.

In brief, here are a few important reasons:

- HTTPS is becoming a requirement. Browsers have begun to flag HTTP sites as insecure. That doesn't create the best impression to your users.
- HTTPS protects your user's privacy by preventing intruders from passively listening to communications between your websites and users.
- HTTPS prevents others from injecting information (scripts, images, or ad content) into your web pages and into the user's browser. Folks with malicious intent could even include inject malware over insecure sites.

To implement HTTPS support for your eTrigue landing pages, refer to the table below to determine the scenario that is applicable to your organization's situation.

Your organization…	Follow the instructions under…
Does not have a SSL certificate. Purchases a new SSL certificate for your subdomain	Scenario 1
Has an existing wildcard certificate that could include the subdomain	Scenario 2

Scenario 1 – Purchase a new SSL certificate

Your organization purchases a SSL certificate from a 3rd Party Certificate Authority, such as GoDaddy, Verisign, Digicert, GeoTrust, etc. This SSL certificate will then be applied to your landing page subdomain to support HTTPS.

1. Send an email to the eTrigue Success Team at success@etrigue.com and provide the following information to generate a Certificate Signing Request (CSR). The CSR is required to start the SSL certificate purchase process:

   a. **Country Name** (Standard 2 Letter Country Code; example: **US** for United States):
   b. **State or Province Name** (Full Name; example: **California**):
   c. **Locality Name** (Full Name; example: **San Jose**):
   d. **Organization Name** (Full Name; example: **Company Inc**.):
   e. **Organization Unit** (Department Name; example: **IT Department**):
   f. **Common Name** (Base URL to reference: example: **ww2.mydomain.com**):
   g. **Email Address** (Email address, example: **IT_department@company.com**):
   h. **Desired Years for Valid Certificate Status before Renewal**
   (Must match what is submitted to the Certificate Authority. Common choices are **1, 2, 3 or 5 years**):

2. After we have received the information above, we will return a CSR to your organization via email.

3. Choose a Certificate Authority (CA) of your choice and use the **CSR** to purchase a SSL certificate. If your CA prompts you to specify a server type, choose **Apache (+ModSSL)**.

4. Send the purchased certificate to success@etrigue.com.

   IMPORTANT: It is strongly recommended that users provide the certificates within a zip attachment (.zip).

   Users should password protect the zip file before sending it to success@etrigue.com and call the Customer Success Team at 408-490-2903 to provide their password over the phone.

5. We will apply your certificate to your landing page subdomain to support HTTPS.

   Please allow for 2-3 business days to complete. A confirmation email will be sent to let you know when the work is completed.

Scenario 2 – Your organization owns a wildcard SSL certificate

If your organization maintains a wildcard SSL certificate for your main domain, the same SSL certificate can be used to secure your subdomain if the root domain is the same.

1. Provide the following to success@etrigue.com:
   a. the wild card SSL certificate
   b. any Intermediate certificates
   c. the Private Key used to generate the SSL certificate (your CA Authority should have provided this key)

   IMPORTANT: It is strongly recommended that users provide the certificates within a zip attachment (.zip).

   Users should password protect the zip file before sending it to success@etrigue.com and call the Customer Success Team at (408) 490-2903 to provide their password over the phone.

2. After all items have been received, we will apply your certificate to your landing page subdomain to support HTTPS.

   Please allow for 2-3 business days to complete. A confirmation email will be sent to let you know when the work is completed.