Symantec Website Security

10 STEPS TO SWITCH FROM HTTP TO HTTPS

To work toward making the internet a safer place, Google Chrome and other browsers have started to mark all unencrypted HTTP websites as "Not Secure." This means that SSL/TLS encryption is no longer a luxury, but a necessity.

USE THESE STEPS TO HELP YOU PLAN AND FACILITATE YOUR WEBSITE MIGRATION.

STEP 1

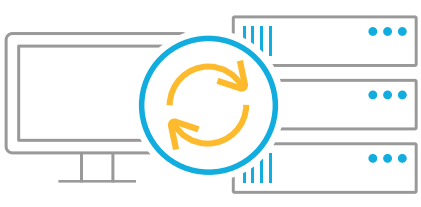
EVALUATE YOUR WEBSITE FOR SECURITY RISKS

Prepare a list of URLs, mapping them from the current HTTP structure to corresponding locations on the HTTPS website. Verify that all external scripts and images work with HTTPS.

STEP 2

PERFORM FULL WEBSITE BACKUP

Before making any changes to your site, complete a full backup. Consult with your hosting provider or system administrator on available backup options.



STEP 3

MAKE THE RIGHT CERTIFICATE CHOICE

Obtain an SSL/TLS certificate from a reputable certificate authority like Symantec, who can offer guidance and technical support as a part of enabling HTTPS for your website.

STEP 4

INSTALL AND TEST CERTIFICATES

Ensure your SSL certificates are properly installed. Symantec offers a free tool called CryptoReport that allows you to test your SSL/TLS certificates and view any browser warnings.

STEP 5

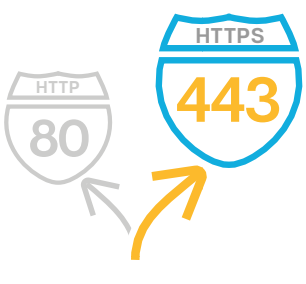
REMOVE MIXED CONTENT

Replace all HTTP references with HTTPS pointers. If you don't remove mixed content, some pages will not be displayed, "Not Secure" warnings may appear in browser windows and your entire site will be less secure.

STEP 6

MAINTAIN CERTIFICATE COMPLIANCE

Stay compliant by keeping your website updated with the latest security requirements and standards. Check the CA/Browser Forum and NIST for SSL/TLS standards, and PCI if your site accepts payments.



STEP 7

REDIRECT HTTP TRAFFIC TO HTTPS

Ensure that all instances of HTTP traffic are redirected to HTTPS. Set up 301 redirects to notify search engines of your new HTTPS address.

STEP 8

IMPLEMENT AN AUTOMATED SCANNING SYSTEM

Identify non-compliant elements and third-party content. Replace unsecured content with safer alternatives. Where possible, use verified and accountable third-party technology.

STEP 9

SECURE YOUR COOKIES

Use both the "HttpOnly" and "Secure" cookie settings to ensure that hackers can't break into your website.

STEP 10

IMPLEMENT HTTP STRICT TRANSPORT SECURITY

HTTP Strict Transport Security (HSTS) is a standard that protects your website visitors by ensuring they are connected over HTTPS. Make sure that all connections are only accessible via HTTPS and include HSTS in the HTTP response reader.

LEARN MORE:
HTTPS://GO.SYMANTEC.COM/BE-TRUSTED