How to use AutoSSL on your websites

We are pleased to make the following announcement in response to increased requests we have received lately about SSL. (SSL is an obsolete technical term but still everyone uses it in general sense. Technically now it is TLS).

Why do I need my site to use https:// protocol?

So two things are driving people to get TLS certificate thus moving their website to https: protocol.

1. Google includes TLS (i.e. https) as an SEO ranking signal among many others.
   Reference: https://webmasters.googleblog.com/2014/08/https-as-ranking-signal.html
2. Google is pushing, via their Chrome browser, for everyone to use TLS (i.e. https) instead of regular http so that the entire web is encrypted communication. They have announced they will start showing a warning icon if site is on http.
   Reference: http://www.zdnet.com/article/google-chrome-gets-ready-to-mark-all-http-sites-as-bad/

What is needed to have TLS on my web address?

The good news is that we have installed Auto-SSL on your Oceania account. cPanel now provides a 90 day free TLS certificate that can be renewed freely as well using their own signing authority for every website hosted on a cPanel server. As long as the site is hosted on cPanel, the certificate will be auto-renewed every 3 months.

These certificates are not meant for business (shopping carts, sensitive data, etc.) as they come with no end-user warranty in dollar value since anyone can just get them without any verification of domain or business ownership. The other type of 1-year TLS certificates (like RapidSSL) are still available and can also be installed on your account. However for the two things mentioned above regarding Google, websites can use free TLS and move to https. And the good news continues… TLS certificates do not require a unique IP on our latest cPanel / CentOS servers. What this means is that you can have free 3-month auto-renewed TLS (https or SSL whatever you want to call it) without changing IP.

And it is already available right now.

All websites that have their domains hosted and pointed to our shared servers and that do not have their own SSL Certificates now have free 90-day certificates automatically installed. No action is required by account holders.

What does it mean?

What it means is that the site(s) on your hosting account will be accessible using both http: and https: protocols.

It is totally up to you as the account holder whether you want to redirect all http traffic to https. This can be done easily with mod_rewrite rule like this in .htaccess file (the .htaccess file is be found in cpanel File Manager in the public_html directory or addon domain folder)

```
RewriteEngine On
RewriteCond %{SERVER_PORT} !^443$
RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI} [R=301,L]
```

Look for Green Lock in URL address

https green lock will only appear if the site does not contain any hard coded http links to images/css/js etc. files. If your website has hard coded http links you will need to get your web developers to fix if you wish to see lock and no warning.

How to Update Website to Apply AutoSSL

Because AutoSSL is installed, you can use HTTPS directly in any site hosted on your hosting account, no further extra steps needed. In certain cases the next thing to do is update website to use HTTPS.

At this point if you go to https://yoursite.com you should see it load! Congrats, you've successfully installed SSL and enabled the HTTPS protocol! But your visitors aren't protected just yet, you need to make sure they're accessing your site through HTTPS!

You can update all links to the target pages to use the HTTPS links.

How do I know the SSL is working?

It is very important for your visitors to know when they are on a secure area of your site. When the SSL is active on the page you are viewing, they can tell by checking the address bar at the top of the browser. There should be a **small green padlock icon** in the address bar area.

Why does my lock disappear?

It is a common reaction to blame the SSL or host for having the certificate installed improperly. This is usually not the case. The SSL lock will only appear or display properly if all items on the page are linking securely. If there is even one unsecure link on the page, the SSL will appear as broken. This means it may not display at all, or it may display differently. Again, this will vary depending on the browser you are using.

Almost exclusively, the cause for this is the use of absolute links for images and text links within the page code instead of relative links. If even ONE link on the page is using the absolute format it will 'break' an otherwise secure page. Below are descriptions of **absolute** and **relative addresss** linking.

> ***Absolute addresses***
>
> *Absolute adddressing for images and links include the entire domain name and the protocol, which is typically http://. For example, if you were linking cool_image.jpg and your domain name was example.com, the link would be code as <imgsrc="http://example.com/cool_image.jpg">*
>
> ***Relative addresses***
>
> *Relative addresses differ from absolute in that they include neither the protocol nor the domain name. Using the same image.jpg file as before, the link code to that file in would simply be <img src="/support/image.jpg">.*

It's a coding issue? How do I correct it?

The solution is 'relatively' easy, pun intended. You will need to go through the code for your site and change all absolute links to relative ones. With hand-coded sites this can be a simple, but tedious process. If your site is coded with a Content Management System such as WordPresss or Drupal, they should already follow this rule on the core level, so you will want to check any links that have been included in the content addition areas such as the editors within the program where you create pages and posts. Once you or your developer has completed this process, you should be able to refresh your site and the lock should display in the correct format.

Notes

1. Understand that HTTPS doesn't mean information on your server is magically secure. It simply protects the TRANSFER of data from your visitor's computer to yours, and the other way too. Once the sensitive data is on your server it's up to you to keep that data safe (encrypt in database, etc).
2. Some people just look for a lock on the page, not on the browser. After you've installed SSL you might want to try adding a lock icon on your pages just to let them know it's secure if they don't look in the url bar.

P O Box 321 Brunswick Heads NSW 2483 Australia
ABN 37 175 432 807
Phone: 1300 301 990 / **Fax:** (02) 9475-0070
Email: support@oceaniawebhosting.com.au

Oceania
Business Solutions