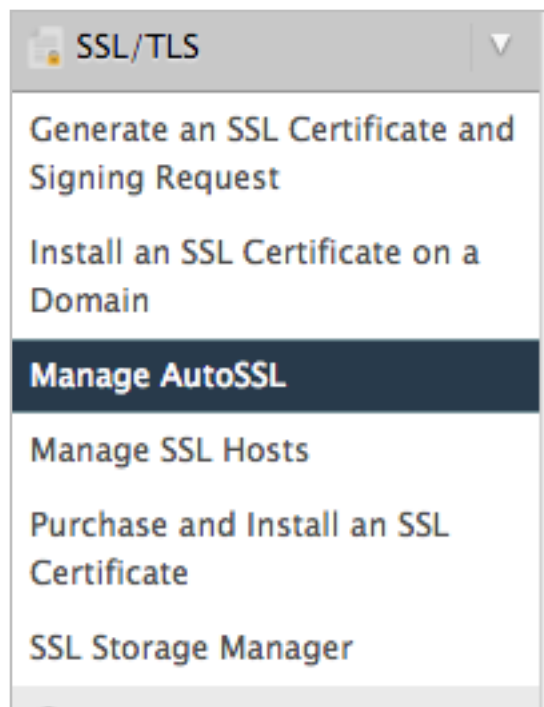


HTTP to HTTPS for BizzyWeb

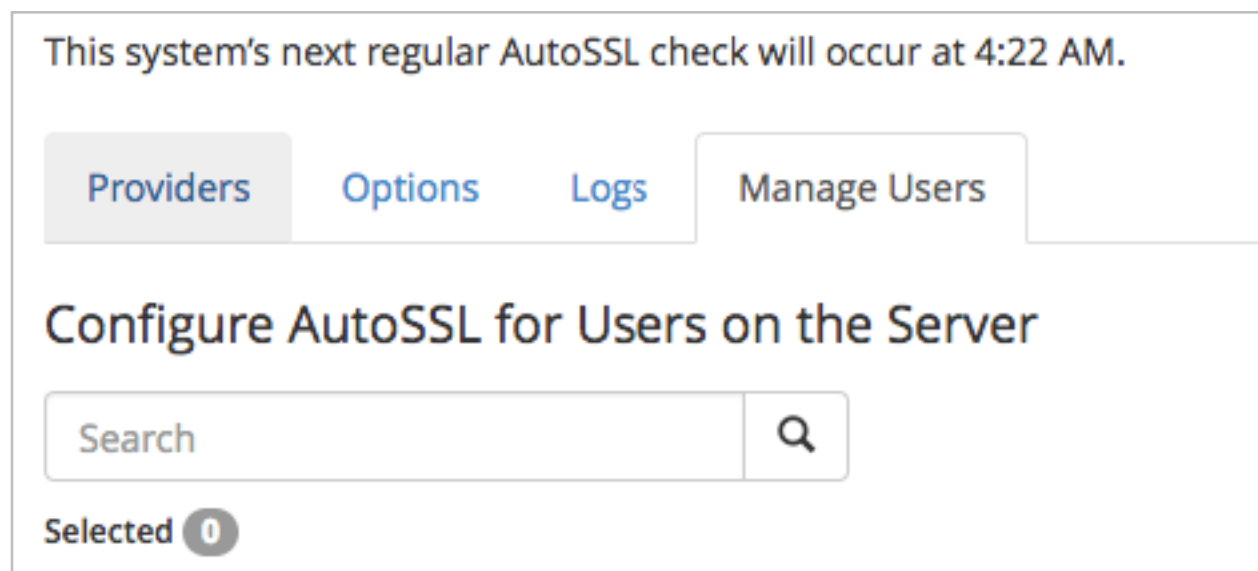
22 August 2017

WHM

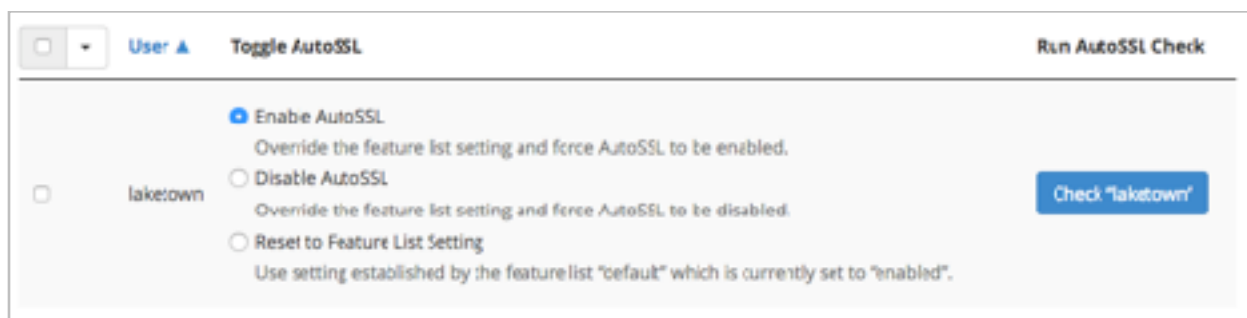
In WHM Admin go to SSL/TLS > Manage Auto SSL



Make sure that “Let’s Encrypt” is the selected provider. Then go to the Manage User Tab and search for the site you are going to add the ssl to. NOTE: This is the user you are looking for not necessarily the site url. (i.e. buildtheschool.org is user buildthe).

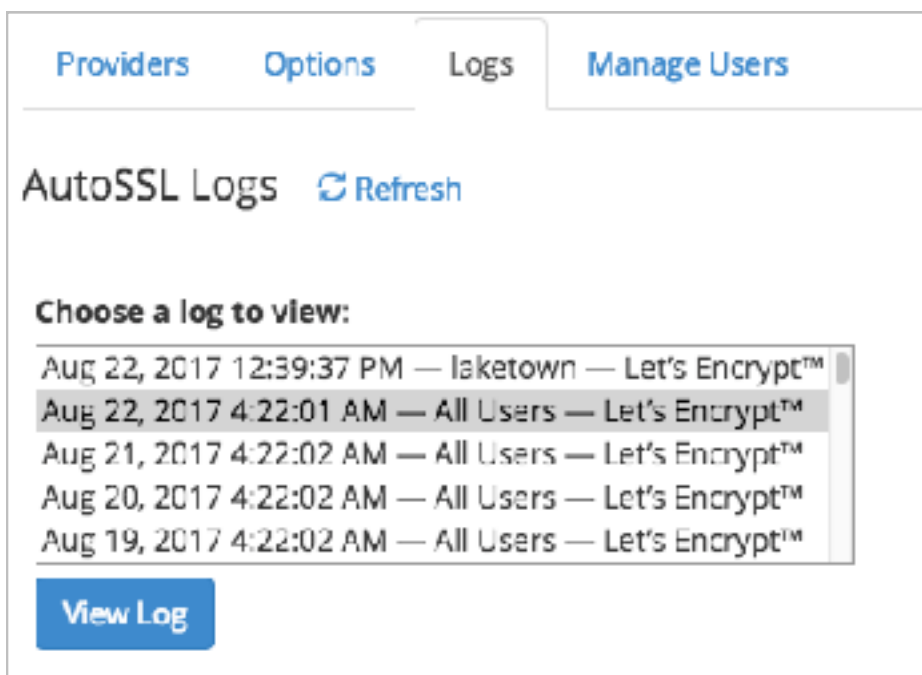


Once you have found your user click the “Enable AutoSSL” radio button and then the “Check “username”” button to verify the ssl.



The screenshot shows a web interface for managing AutoSSL settings. At the top, there's a header with a dropdown menu, the text "User ▲", and a "Toggle AutoSSL" button. On the right, there's a "Run AutoSSL Check" button. Below the header, there are three radio button options: "Enable AutoSSL" (selected), "Disable AutoSSL", and "Reset to Feature List Setting". Each option has a description: "Override the feature list setting and force AutoSSL to be enabled.", "Override the feature list setting and force AutoSSL to be disabled.", and "Use setting established by the feature list 'default' which is currently set to 'enabled'." respectively. To the left of these options is a checkbox labeled "laketown". To the right of the options is a blue button labeled "Check 'laketown'".

Finally go into the Logs tab and refresh and view the log for the user you just enabled. If there are no errors you should be good to move on to the next step. We are primarily concerned with errors pertaining to the main domain, www. and mail. Additional errors may appear if DNS is improperly set up.



The screenshot shows a web interface for viewing AutoSSL logs. At the top, there are four tabs: "Providers", "Options", "Logs" (selected), and "Manage Users". Below the tabs, there's a heading "AutoSSL Logs" and a "Refresh" button. Underneath, there's a section titled "Choose a log to view:" with a list of log entries. The entries are: "Aug 22, 2017 12:39:37 PM — laketown — Let's Encrypt™", "Aug 22, 2017 4:22:01 AM — All Users — Let's Encrypt™" (highlighted), "Aug 21, 2017 4:22:02 AM — All Users — Let's Encrypt™", "Aug 20, 2017 4:22:02 AM — All Users — Let's Encrypt™", and "Aug 19, 2017 4:22:02 AM — All Users — Let's Encrypt™". At the bottom, there's a blue button labeled "View Log".

Wordpress Admin

In the Wordpress admin go to Settings » General and updating your WordPress and site URL address fields.



General Settings

Site Title

Tagline

In a few words, explain what this site is about.

WordPress Address (URL)

Site Address (URL)

Enter the address here if you want your site homepage to be different from the WordPress address

HTaccess

Now if you're adding SSL to your existing site, then you need to setup WordPress SSL redirect from HTTP to HTTPS.

You can do this by adding the following code in your **.htaccess** file:

```
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteCond %{SERVER_PORT} 80
RewriteRule ^(.*)$ https://www.yoursite.com/$1 [R,L]
</IfModule>
```

Don't forget to replace **yoursite.com** with your site URL.

WP-Config.php

If you want to add SSL and HTTPS on your WordPress multi-site admin area or login pages, then you need to configure SSL in **wp-config.php** file. Simply add the following code above the “That’s all, stop editing!” line in your **wp-config.php** file:

1

```
define('FORCE_SSL_ADMIN', true);
```

This wp-config.php SSL trick works for single sites as well as multi-sites.

Cloudflare

Optional depending upon DNS Setup

If the site is using Cloudflare for DNS you should go in and set up the ssl for cloudflare as well.

Once logged into Cloudflare go to Crypto and set the SSL to Strict.

Below is a definition of the different types of encryptions for CloudFlare’s ssl:

What SSL setting should I use?

This setting controls [how Cloudflare’s servers connect to your origin for HTTPS requests](#). We recommend enabling the Full SSL (Strict) setting if possible.

Common use cases for each are:

Off: No visitors will be able to view your site over HTTPS; they will be redirected to HTTP.

Flexible SSL: You cannot configure HTTPS support on your origin, even with a certificate that is not valid for your site. Visitors will be able to access your site over HTTPS, but connections to your origin will be made over HTTP. Note: You may [encounter a redirect loop with some origin configurations](#).

Full SSL: Your origin supports HTTPS, but the certificate installed does not match your domain or is self-signed. Cloudflare will connect to your origin over HTTPS, but will not validate the certificate.

Full SSL (strict): Your origin has a valid certificate (not expired and signed by a trusted CA or Cloudflare Origin CA) installed. Cloudflare will connect over HTTPS and verify the cert on each request.