SSL/TLS certificates in Lightsail

Note
Lightsail uses SSL/TLS certificates to handle encrypted web traffic (HTTPS requests). You can create certificates, verify domain ownership, and then attach the validated certificates to your Lightsail load balancer.

Last updated: November 29, 2017

When you create a Lightsail load balancer, port 80 is open for handling regular (unencrypted) web traffic by default. You must create a Transport Layer Security (TLS) certificate to enable HTTPS (encrypted) traffic. TLS is just an updated, more secure version of Secure Socket Layer (SSL). Throughout the documentation and the Lightsail console, you'll see us refer to it as **SSL/TLS**.

You can create up to two SSL/TLS certificates per Lightsail load balancer. Only one certificate can be active at a time. If you delete a valid, in-use certificate from your load balancer, you will no longer be able to handle encrypted (HTTPS) traffic with your load balancer until you attach another valid certificate.

Why use HTTPS?

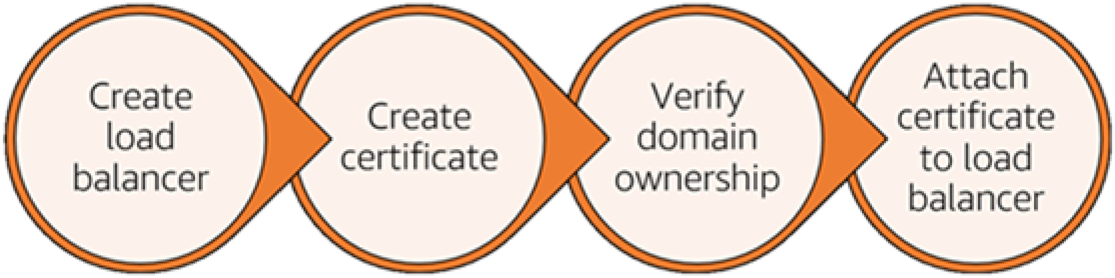
First and foremost is security. HTTPS offers an extra layer of security because it uses TLS to move data. HTTPS encryption is confidential between the web server and the client's browser, because they are the only two entities who can decrypt the traffic. HTTPS connections are also more secure because the data a client exchanges with the server can't be modified by another party.

Aside from security benefits mentioned above, there are other reasons to use HTTPS in addition to HTTP. For example, in 2014 Google began ranking secure websites higher in search results. In other words, a site that uses HTTPS ranks closer to the top of search results compared to a site that only uses HTTP (all other things being equal).

Learn more about HTTPS as a ranking signal

Get started

To enable HTTPS, you must follow these steps in order.



You can get started with HTTPS by following these links.

- Create a Lightsail load balancer and attach instances to it
- Create an SSL/TLS certificate
- Verify domain ownership
- Attach your validated certificate to enable HTTPS