Migrating To Always-On SSL

Now that Google has added a rank boost for Always-On SSL (AOSSL), it makes sense to enable HTTPS across your entire Website. But where do you start? DigiCert created this guide to give you an in-depth look on how AOSSL can help you and to get you started with implementing AOSSL on your own Website.

Get Your Company On Top With AOSSL

We know you're always looking for new ways to make your company stick out—whether that's in search engine rankings or in your customer's minds. And with Google's recent announcement that HTTPS everywhere is a factor in their ranking algorithm, SSL can be part of your solution.

Unlike many of the ranking factors in Google's search algorithm that are vague or difficult to measure, having HTTPS everywhere is a guaranteed way to get your site ranked above your competitors. And though it's starting out as a lightweight signal, Google has promised that the weight of SSL as a ranking factor will increase once webmasters have time to migrate their sites.

Having SSL site-wide also helps your marketing and user engagement. SSL Certificates are the top method for online encryption and authentication today and users immediately recognize them to mean security. By ranking higher in Google, you will be driving more traffic; and with the added security benefits of SSL your new users will feel confident on your site, positively affecting conversion rates.

How AOSSL Benefits You

The HTTPS everywhere ranking signal is standalone and is independent from any of Google's other ranking signals or algorithms. As soon as a new HTTPS page is indexed by Google, you get a boost in your search ranking just because of the HTTPS URL. While this doesn't mean that your page will automatically jump up a few ranks in search results, it does mean that you will get a boost in your overall rank.

As is the case with every other SEO ranking factor, the first wave of Websites who follow Google's recommendation and migrate to HTTPS everywhere should receive the best long-term results. By implementing AOSSL now, your pages will rank higher than your competitors who haven't implemented SSL yet. By incorporating SSL into your SEO strategy, you prepare your company for the future of SEO and show your visitors that you take their data security seriously.

Because users trust SSL Certificates, they are proven to increase conversion rates, improve engagement metrics, and elevate brand reputation. According to a study by Tech-Ed, 100% of participants would prefer doing business with a company that has an EV SSL Certificate.

Currently, SSL Certificates are mainly used on pages that handle sensitive data, like on login or checkout pages. This causes users to bounce back and forth between HTTP and HTTPS sessions. By having SSL on all of your pages, users' sessions are secured the entire time they are on your site—protecting any and all data that they transfer.

Migrating To AOSSL

Moving your site to HTTPS involves more than just going out and purchasing an SSL Certificate. DigiCert recommends reading the following sections thoroughly and working closely with your IT administration team to make the transition.

1. Figure Out What Certificates You Already Have

If your site deals with sensitive user information, you may already have an SSL Certificate on a portion of your Website. Before you go buy an SSL Certificate, it's best to know what you already have. In most organizations, the IT administrators handle purchasing and installing the SSL Certificates. Work with your IT team to find out what certificate(s) you already have, if any, and what pages of your Website they secure.

We recommend using DigiCert's Certificate Inspector tool to find all of the certificate resources in your environment. This tool will scan your domain or a range of IPs to find certificates. You can also use Certificate Inspector to scan your internal network for SSL Certificates.

2. Decide What Kind of Certificate You Need

Once you understand your current certificate landscape, you will better know what kind of certificate you need. Even if you already have an SSL Certificate, you may need to purchase an additional certificate to secure your entire site.

For example, if you handle sensitive data you may already have an SSL Certificate that secures the login or checkout page on your site. However, this singlename SSL Certificate may not be able to secure the rest of your company's resources if you have multiple subdomains or even multiple domains.

You may want to switch to a UC (SAN) or Wildcard certificate if you need to secure multiple subdomains or domains. You may also want to transition to an EV SSL Certificate for the added user trust and visual cues like the green address bar.

DigiCert has many types of SSL Certificates designed to meet a variety of needs. For a more detailed description of each certificate type and more information on what type of SSL Certificate is right for your situation, read this article.

3. Create a CSR

Once you figure out what kind of certificate you need, you must create a CSR. A CSR is a file that you (or your IT admin) generate on the server where you will install the certificate. Work with your IT admin to determine what server this is and to generate the CSR file.

You can find step by step instructions on creating a CSR for a variety of platforms in the support section of DigiCert's Website. Or, if you have a Windows server, you can download the DigiCert Certificate Utility for Windows to automatically generate and upload your CSR.

4. Purchase the Certificate

Now that you know what kind of certificate you need and you have a CSR, you are ready to buy your certificate. There are a few factors you should take into account when deciding who to purchase your certificate from:

Issuance Time: Some CAs take days or even weeks to issue a certificate. DigiCert has the fastest issuance times out of any CA, we can even issue an EV certificate in a matter of hours!

User Trust: Though all SSL Certificates have the same encryption, the level of trust a certificate provides depends on the issuer. DigiCert has provided SSL Certificates for over a decade.

Customer Support: While migrating to Always-On SSL, you may have questions or run into a problem that you can't solve. At DigiCert, our expert support team is standing by 24/7 to help you.

Powerful Tools: Certificate management tools can save you and your IT team a lot of time. DigiCert's innovative dev team has created tools to help with every step of the cert management lifecycle.

5. Install the Certificate

Once you complete the validation process and receive your SSL Certificate, you or your IT administrator can install it on your server. You can find step by step instructions for installing an SSL Certificate on a variety of platforms in the support section of DigiCert's Website. Or, if you have a Windows server, you can download the DigiCert Certificate Utility for Windows to automatically install your certificate.

After your certificate is installed, we recommend that you check that everything is working correctly using our free Always-On SSL Site Checker.

If you have any questions, please contact our support team at 1.801.701.9600 or email support@digicert.com.

6. Migrate Your Site to HTTPS

Once your certificate is installed, you must migrate your site to HTTPS. By following some simple steps, you can make your transition to HTTPS easier and make sure you are getting the most out of the SEO benefit. We recommend that you provide the following tips to your IT administrator.

MAKING THE MOVE

Break up the transition to make it more manageable. Consider breaking up your transition into phases to make it more manageable. However, remember that the ranking boost only applies to pages that have HTTPS enabled so move pages with your target keywords first.

Track your site migration in Google Webmaster Tools. List the HTTP and HTTPS versions of your site separately in Webmaster Tools. Because all of your site traffic will move to the new HTTPS version of your site, you should track both sites in any analytics software and in Webmaster Tools to monitor site traffic.

CONFIGURING YOUR SERVER

Enforce 256-bit minimum session keys.

Test your Website for unsecured content. Manual testing can help you find pages where content is being accessed over HTTP. During testing, disable access via Port 80 (HTTP). While Port 80 is disabled, all content that was going through Port 80 will be broken and you can quickly find and fix it. Once elements that access Port 80 have been eliminated, re-open Port 80 and redirect it to Port 443 (HTTPS).

Use a server that supports HTTP Strict Transport Security (HSTS) and enable it. HSTS tells browsers to always load pages using HTTPS even when the user enters HTTP in the address bar or another site links to the HTTP version of a page. It also tells Google to serve HTTPS URLs in the search results.

Add a server-side 301 redirect. Set up a server-side 301 redirect to direct traffic from port 80 (HTTP) to port 443 (HTTPS). Google considers the HTTP and HTTPS versions of your Website to be different sites. Because of this, if you do not redirect traffic Google may see your sites as having duplicate content and penalize you.

MAKE SEARCH ENGINES SEE YOUR SITE AS SECURE

Use relative URLs for resources that are on the same secure domain. There are three types of URLs that you can use for resources on your domain:

- Absolute HTTP URL: <a href="http://www.domain.com/example/about.html">
- Absolute HTTPS URL: <a href="https://www.domain.com/example/about.html">
- Relative URL: <a href="/example/about.html">

While relative URLs are recommended, if you need to use absolute URLs you should make sure you are including HTTPS instead of HTTP. This will ensure that the user clicking the link will reach the HTTPS version of the resulting page or resource. This will also ensure that when Google is scanning your Website they will see HTTPS URLs.

Use protocol-relative URLs for all other domains. Use protocol-relative URLs or absolute HTTPS URLs for all other domains. Protocol-relative URLs for external sites can be formatted as follows: <a href="//domain.com/example/about.html">.

Don't block your HTTPS site from being crawled using robots.txt. Allow your pages to be indexed by search engines where possible and avoid the noindex robots meta tag.

Move all resources to HTTPS. To get the ranking benefit, your whole site (including all URLs, files, images, dynamic HTML, JavaScript, CSS, assets, and anything with a href attribute) must go through HTTPS. This means going through your entire Website and cleaning up the links, as well as making sure all of our resources are accessible through HTTPS to avoid mixed content.

About DigiCert

DigiCert is a premier provider of security solutions and certificate management tools. We have earned our reputation as the security industry leader by building innovative solutions for SSL Certificate management and emerging markets.

- OCSP 4x times faster than other CAs
- Secures 6 of top 10 biggest U.S. websites
- Solutions for IoT, WiFi, healthcare
- Secures over 2 trillion transactions a year
- Innovator in managed PKI
- 5-star customer support
- Clients in more than 180 countries
- Unlimited server license/free reissues

Trusted by Leading Enterprises

For more information, contact support at 1.801.701.9600 or email support@digicert.com.

digicert®