sslstore™ ()

SSL Brands ▼
Only the most trusted
(/brands.aspx)

SSL Products ▼
What type do you need?
(/products/ssl.aspx)

Partner Programs ▼
Reseller, Affiliate & Enterprise
(/partner/partner-program.aspx)

Norton SECURED
powered by Symantec

https://www.
SSL+ROI= ♡

SHA-1 Sunsetting, Google, and Your Next Steps.

SHA-1 Sunsetting, Google, and Your Next Steps.

What is happening, and what was happening?

The SSL Industry and the CA/B Forum have planned for the "sunsetting" (depreciation) of the SHA-1 signing algorithm for quite some time. However, their plan was mainly formed around Microsoft's desires to phase it out in 2017, alongside the end-of-life for Windows XP. This was widely understood to be the approved plan for CAs to follow, and the preparation for moving from SHA-1 to its successor, SHA-2, wouldn't be necessary for many months from now.

However, Google recently made an announcement, in stark contrast to Microsoft's plan, that they are implementing their own SHA-1 sunsetting timeline, which will begin on September 26th 2014.

This timeline has three distinct stages, which will result in degraded visual indicators in Google Chrome (padlock, green-bar) for SHA-1 signed certificates meeting specific criteria (this is discussed in the section "What certificates are affected?" below).

This means it is now necessary to educate and assist our partners and customers on how to make the transition away from SHA-1.

Why?

First, let's understand what SHA-1 does. Both SHA-1 and its successor, SHA-2, are specific types of signing algorithms. Signing algorithms are used as part of the identity validation role that SSL certificates perform. They are mathematical functions (referred to as a "hash") which, when performed, should calculate a persistent and unique value for each file. So, for instance, the Word doc this text is stored in has a unique SHA-1 hash value. If I change a single part of this file – add an extra period somewhere, change a letter, etc. – it will produce a different SHA-1 hash value.

When a certificate is downloaded from a server to the client's browser, a hash is taken of it. The type of hash taken (SHA-1, SHA-2, MD5, etc.) depends on how the certificate is signed. The hash calculated by the browser is compared to the hash value provided by the server, which has been verified by the Certificate Authority (CA) at the time of issuance. If they match, the identity of the certificate and server are verified.

+ Read More

When is this happening?

Google's policy involves three distinct steps, the first beginning on September 26th. On this date, only customers with SHA-1 signed certificates expiring in 2017 are affected. However, the amount of affected certificates will expand in November, and again in Q1 2015. The full details on what certificates are affected is in the below section, "The Nitty Gritty."

What certificates are affected?

Certificates are affected if they meet the any of the following criteria:

✔ All certificates from the RapidSSL or QuickSSL family issued before September 15th, 2014 and expiring after January 31st, 2016 (They are
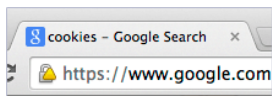
signed by a SHA-1 Intermediate).

✓ If they are signed with SHA-1 and expire after January 1st, 2016.

✓ They have an Intermediate Certificate Chain that are SHA-1 signed certificates.

To understand the exact certificates affected, please see the below section which gives explicit detail.
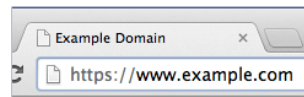
The Nitty Gritty[1]

On September 26th, 2014:

SHA-1 signed certificates expiring on or after January 1st, 2017 will be treated as "secure, but with minor errors" and will receive the yellow triangle padlock.

On November 7th, 2014:

SHA-1 signed certificates expiring on or after June 1st, 2016 to December 31st, 2016 are treated as above. Certificates expiring after January 1st, 2017 are treated as "neutral, lacking security." These certificates will receive a blank page icon, as seen with HTTP sessions.

---

1 The majority of this section comes from Google's official announcement:
http://googleonlinesecurity.blogspot.com/2014/09/gradually-sunsetting-sha-1.html (http://googleonlinesecurity.blogspot.com/2014/09/gradually-sunsetting-sha-1.html)

In Q1 2015:
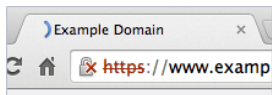
SHA-1 signed certificates expiring on or after January 1st, 2016 to December 31st, 2016 will continue to be treated as "secure, but with minor errors."

SHA-1 signed certificates that expire on or after January 1st, 2017 are treated as "affirmatively insecure." This will be identified by the red "X".

How is the problem solved?

Affected certificates can be fixed by reissuing (There are no situations where anything other than a reissue is needed). Our partner CAs have sped up their implementation of SHA-2 compatible infrastructure due to Google's new policy.

Symantec has confirmed Officially That Their full product line will have a fully SHA -2 compatible chain" on September 15 , 2014. " 2 Comodo 's full product line is already ready for the SHA -2 transition and by default are now being 'issued as SHA -2 . Certum's product line is having fully SHA-2 compatible chain since November 2014.

What do I need to do?

If your certificate is SHA-1, you need to perform the following:
a) A reissue of your certificate to SHA-2

In addition to the step above, you probably also need to:
b) Install newly available SHA-2 Intermediate Certificates.

Please see below to determine what is necessary for your situation.

It will be necessary for you to perform a) if you have a SHA-1 certificate (as determined by your selection during the enrollment process). This can affect certificates from any of our providers, and is more likely to affect older certificates.

If your certificate was SHA-1, most likely it was also signed by a SHA-1 Intermediate. When you reissue the certificate it will be signed by the SHA-2 Intermediate, which must also be installed to your server. These will either be provided or linked to you when you receive your new certificate.

---

2 Symantec's full statement: "Google has announced that it plans to phase out SHA-1 support via degraded visual indicators. The plan is for that to happen in the upcoming Chrome 39 release on September 26, 2014. Google's plan is still subject to change. To help partners respond to this change, Symantec has accelerated its plan to offer SHA-2 end-entity certs chaining to SHA-2 intermediates. We expect these to be available for testing (by API-integrated partners) in our pre-production environment on September 12, 2014, and generally available on September 15, 2014."
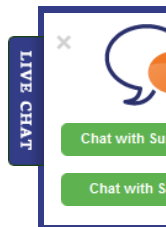
How can I tell if my certificates are effected?

You can use **this SHA checker tool to test if your certificates are affected (https://shachecker.com)**. You can also come to our 24/7 support to make sure, but please do use the checking tool first.

Q & A

[+] **What products have compatibility issues with this switch?**

[+] **What platforms have compatibility issues with this switch?**

[+] **What browsers have compatibility issues with this switch?**

[+] **What if I had a SHA-2 subscriber certificate issued before the SHA-2 roots were available (The certificate is signed with a SHA-1 Intermediate and has a "mixed-chain"?**

[+] **What if the customer has a SHA-1 subscriber certificate?**

[+] **Does the customer need to generate a new "SHA-2" CSR?**

[+] **Should I use something more secure than SHA-2?**

Platinum Partners of the World's Most Trusted SSL Brands

Buy SSL

Check out our unbeatable pricing. Browse over 80 of the most trusted certs in the industry.
Shop Now (/products/ssl.aspx)

SSL Assistance

Our SSL experts are available 24/7/365 via email, live chat, and telephone.
**Get Help
(https://www.thesslstore.com/support/)**

SSL Tools

FREE tools available to our customers and resellers to help with common SSL issues.
**Use Our Tools
(https://www.thesslstore.com/ssltools/)**

Buyer Zone

Extended Validation Cert (/extended-validation-ssl-certificates.aspx)

Domain Vetted Cert (/products/domain-vetted-certificates.aspx)

Organization Certificates (/products/organization-vetted-certificates.aspx)

Server SSL Certificates (/server-sslcertificates.aspx)

Free Tools (/ssltools/)

Compare SSL Certificates (/ssl-compare/compare-ssl-certificates-prices.aspx)

Request for Quotation (/partner/ssl-proposal.aspx)

Partner With Us

Reseller Program (/partner/reseller-program.aspx)

Affiliate Program (https://affiliate.thesslstore.com/)

Enterprise Program (/partner/enterprise-solutions.aspx)

Full Access API (/partner/api-integration.aspx)

Integrated Plug-ins (/partner/integration-tools.aspx)

Strategic Partnerships (/partner/strategicpartnerships.aspx)

Our Partners (/ssl-partner.aspx)

Custom Integration (/need-custom-integration.aspx)

About Us

About Us (/about-us.aspx)

Blog (https://www.thesslstore.com/blog/)

SSL Clients (/ssl-clients.aspx)

Case Studies (/casestudies/default.aspx)

Why Choose Us (/whychooseus.aspx)

Press Room (/press-room.aspx)

SSL Videos (/ssl-videos.aspx)

Announcements (/announcements.aspx)

24/7 Help Zone

SSL Support (/support/)

Manage Your Account (/quicklogin.aspx)

FAQ (/faq.aspx)

Help with EV (/helpwithev.aspx)

Request a Callback (/requestacallback.aspx)

Site Map (/sitemap.aspx)

Contact Us (/contact.aspx)

SSL Installation Service (/support/ssl-installation-service.aspx)

(http://www.shopperapproved.com/reviews/thesslstore.com/)

(https://www.facebook.com/thesslstoredotcom)

(https://twitter.com/thesslstore)

(https://plus.google.com/+TheSSLStore/)

(https://www.linkedin.com/company/the-ssl-store)