Entrust®

A Step-by-Step Migration Guide to SHA-2 SSL Certificates

Avoiding pitfalls, meeting critical deadlines and eliminating service disruptions during SHA-1 certificate deprecation

+1-888-690-2424
entrust.com

switchtosha2.com
#SwitchToSHA2

Table of contents

Entrust®

Table of contents

continued …

Entrust®

Executive summary

"Failure to migrate to SHA-2 in a timely manner will result in browsers not displaying content properly and end-users receiving security warnings."

Many organizations urgently need to upgrade to SHA-2 (also known as SHA-256) SSL certificates in conjunction with updated federal and PCI compliance standards currently in place, as well as to meet Microsoft's and Google's SHA-1 deprecation policies set to begin in November 2014.

SHA-1 has been in use among commercial certification authorities (CAs) since the late 1990s, and today accounts for the overwhelming majority of digital certificates in use. As of June 2014, SHA-1 SSL certificates accounted for over 98 percent of certificates issued worldwide.[1]

Recent advances in cryptographic attacks upon SHA-1 have led to the decision that the industry must move to prohibit continued issuance of SHA-1, but also transition to SHA-2 certificates, which are exponentially more secure.

With SHA-2 certificates now available and widely supported by browsers and servers, and the technical deadline for replacement fast approaching, organizations need to establish a migration path and process to ensure that there are no service disruptions or compromises of their security posture.

Failure to migrate to SHA-2 in a timely manner will result in browsers not displaying content properly and end-users receiving security warnings. This often causes users to abandon a site or transaction or call support services such as helpdesks or customer service. System outages, if certificates are inappropriately replaced, are also a possibility.

The plan for replacement and issuance of new certificates will require the coordination of people, process and technology across an organization.

This paper will describe the technical and business impact of SHA-1 migration as it pertains to SSL certificates only. It will outline a recommended migration path to minimize the cost and operational impact of replacing affected SSL certificates.

1 In total, more than 98 percent of all SSL certificates in use on the Web are still using SHA-1 signatures. Netcraft's June 2014 SSL Survey found more than 256,000 of these certificates would otherwise be valid beyond the start of 2017 and, due to the planned deprecation of SHA-1, will need to be replaced before their natural expiry dates.

What is SHA?

The SHA family of hashing algorithms was developed by the U.S. National Institute of Standards and Technology (NIST) and are used by CAs when digitally signing certificates that are subsequently issued to end-entities.

Secure Hash Algorithm (SHA) is a type of cryptographic hash function that ensures data has not been modified. SHA accomplishes this by computing a cryptographic hash value for a given piece of data that is unique to that data. Different pieces of data yield unique hash values, and any change to a given piece of data will result in a different hash value. As a result, differing hash values are key to determining if data has been altered.

Hash values help ensure the integrity of a given piece of data because they are virtually guaranteed to be unique, infeasible to predict and yet easy to compute.

Why is there a Problem with SHA-1?
Over time, security standards usually become less effective for two reasons. Research finds weaknesses in them, and the plummeting cost of computing power makes computationally difficult attacks more practical.

For example, SHA-1's predecessor, MD5, was in use well beyond the point that attacks on it were cheap and easy.

There are no practical attacks on SHA-1 yet, but it's just a matter of years before they appear. Security researchers have discovered an attack strategy that requires only 261 computations. This would make the time required to perform an attack below current standards.

In fact, in 2012 noted security researcher **Bruce Schneier reported the calculations of Intel researcher Jesse Walker**, who found that the estimated cost of performing a SHA-1 collision attack will be within the range of organized crime by 2018 and for a university project by 2021.

How can SHA-1 be Attacked?
Simply put, SHA-1 can be exploited by attackers to generate and install a fake certificate. For those interested in a more in-depth technical explanation of hash attacks, they are outlined below, in increasing order of difficulty for an attacker.

Collision Attacks

A collision attack occurs when it is possible to find two different messages that hash to the same value. A collision attack against a CA happens at the time of certificate issuance.

In a past attack against MD5, the attacker was able to produce a pair of colliding messages, one of which represented the contents of a benign end-entity certificate, and the other of which formed the contents of a malicious CA certificate.

Once the end-entity certificate was signed by the CA, the attacker reused the digital signature to produce a fraudulent CA certificate. The attacker then used their CA certificate to issue fraudulent end-entity certificates for any domain.

Collision attacks may be mitigated by putting entropy into the certificate, which makes it difficult for the attacker to guess the exact content of the certificate that will be signed by the CA. Entropy is typically found in the certificate serial number or in the validity periods. SHA-1 is known to have weaknesses in collision resistance.

Second Preimage Attacks

In a second preimage attack, a second message can be found that hashes to the same value as a given message. This allows the attacker to create fraudulent certificates at any time, not just at the time of certificate issuance. SHA-1 is currently resistant to second preimage attacks.

Preimage Attacks

A preimage attack is against the one-way property of a hash function. In a preimage attack, a message can be determined that hashes to a given value. This could allow a password attack, where the attacker can determine a password based on the hash of the password found in a database. SHA-1 is currently resistant to preimage attacks.

SHA-2 & beyond

At this point, we have time to move beyond SHA-1 before problems hit the real world. The next standard, SHA-2, is a series of hash functions with several hash sizes: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256. There is also a SHA-3, but it is a very young standard with no commercial implementations.

Certificates can be used for SSL, code-signing, document-signing, email encryption, and other identification and encryption purposes. Each of these usages ensure the integrity and security of embedded messages.

Using a weak hashing algorithm puts the security of messages at risk, which is why the security industry is moving to SHA-2, and why everyone should seriously consider switching to SHA-2. By using SHA-2, you can protect signed items from hash attacks — now and in the future.

SHA-1 deprecation policy specifics & impact

Important dates

NOVEMBER 2014

November 2014

SHA-1 SSL certificates expiring any time in 2017 will show a warning (via a change in the domain name display) in Google Chrome.

DECEMBER 2014

December 2014

SHA-1 SSL certificates expiring after June 1, 2016 will show a warning (via a change in the domain name display) in Google Chrome indicated by a yellow triangle.

JANUARY 2015

January 2015

SHA-1 SSL certificates expiring any time in 2016 will show a warning in Google Chrome.

JANUARY 2016

January 1, 2016

CAs must stop issuing new SHA-1 SSL and code-signing certificates. Microsoft will stop trusting SHA-1 code-signing certificates without time stamps.

JANUARY 2017

January 1, 2017

Microsoft will stop trusting SHA-1 SSL certificates.

A number of factors are driving the elimination of SHA-1, ranging from compliance with U.S. NIST and PCI standards, to the technical rejection of certificates in Microsoft's operating systems and Google's popular Chrome browser.

Important Considerations

It is important to understand that the failure to comply with NIST and PCI requirements that are currently in effect could result in significant financial penalties, but it will not have any operational effect.

At the same time, it should be strongly noted that the deprecation policies of Microsoft and Google could result in significant negative impact to IT operations and end-user experience.

NIST Guidance

U.S. NIST Guidance counseled that SHA-1 should not be trusted past January 2014 for the higher level of assurance communications over the U.S. Federal Bridge PKI. Agencies have been phasing out the use of SHA-1 certificates across the government. Most government contractors are also required to meet these requirements with varying deadlines.

PCI Compliance

PCI compliance scanners currently require their clients to use SHA-2-compatible SSL certificates. In order to validate PCI DSS compliance, you must ensure that Web server(s) in the PCI environment are configured to disallow SSL (Secure Sockets Layer) Version 2, as well as weak ciphers and hashes. PCI network scanners finding SHA-1 certificates will fail a compliance audit.

Industry Policy

Microsoft and Google have each announced new policies for CAs to deprecate the use of the SHA-1 algorithm in digital certificates in favor of SHA-2.

As it relates to SSL certificates, the Microsoft policy affects CAs that are members of the Windows Root Certificate Program that issue publicly trusted certificates.

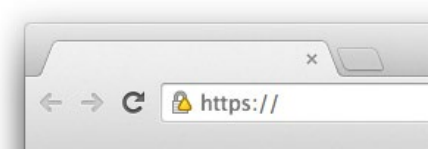
The Google policy affects any users of Chrome browser 39 and beyond. Microsoft will allow CAs to continue to issue SHA-1-signed SSL and code-signing certificates until January 1, 2016, and thereafter issue SHA-2 certificates only.

Both of these SHA-1 deprecation plans also impact SHA-1 intermediate certificates; SHA-2 end-entity certificates must be chained to SHA-2 intermediate certificates to avoid the adverse browser behaviors described above. SHA-1 root certificates are not impacted.

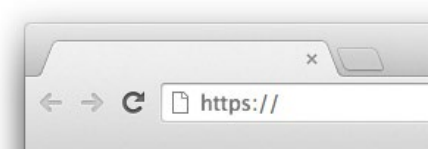
The CA/Browser Forum, an industry vendor consortium that comprises both CAs and Web browser vendors, came to an agreement to take advantage of the deprecation of SHA-1 by accelerating the forum's planned move to shorter maximum certificate lifetimes. The deprecation alone will mean that some five-year certificates that are valid today will not be usable for their entire lifetime.

What this Policy Means for Google Chrome Users
If a website currently uses a SHA-1 SSL certificate that **expires later than December 31, 2015, you need to take action** to future-proof SSL security. Google is making changes to the user interface in Google Chrome 39 to advise browser users of the use of SHA-1 certificates.

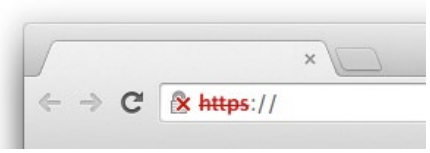
The changes will happen in stages and start with Chrome 39, which is due to be available in **November 2014**. Initially, the warnings will be limited to a "Secure, but minor errors" icon, in the form of a lock with a yellow triangle, but in later versions will become a red crossed-out lock.



Secure, but minor errors



Lock not displayed



Affirmatively insecure, major errors

Note: The provided chart is for planning only. Google has yet to officially announce upcoming Chrome release dates. All timelines are approximations based on past releases and should not be considered final.

Chrome Version	Earliest Release Date	SHA-1 Expires Jan.- May 2016	SHA-1 Expires June - Dec. 2016	SHA-1 Expires After 2016
39	3 Nov. 2014	No Change	No Change	Yellow Triangle Over Lock
40	15 Dec. 2014	No Change	Yellow Triangle Over Lock	No Lock
41	26 Jan. 2015	Yellow Triangle Over Lock (sub resources will also trigger icon)	Yellow Triangle Over Lock (sub resources will also trigger icon)	Red X Over Lock (sub resources trigger yellow icon)

Know the dates.
To prevent a downgraded user experience, it is essential for all SHA-1 certificates that expire after December 31, 2015, be upgraded prior to November 2014.

Special note

Microsoft has not set any dates for blocking other types of certificates (e.g., S/MIME) except for SSL and code-signing CAs. However, SHA-1 certificates issued after January 1, 2017, may stop working at any time.

What this Policy Means for Windows Users

In publishing its policy, Microsoft stated, "Microsoft has examined the SHA-1 issue, and consulted with affected CAs. We are committed to this SHA-1 deprecation policy and its timeline. We believe that this provides the best assurance of security for Windows customers and the broader PKI-based ecosystem of users.

"The quicker we can make such a transition, the fewer SHA-1 certificates there will be when collisions attacks occur and the sooner we can disable SHA-1 certificates."

SHA-2 capabilities are native to Microsoft® Windows Vista®, Windows 7® and Windows Server 2008® (R2), so these users do not need to do anything in response to this new technical requirement. Windows® XP Service Pack 3 supports SHA-2 SSL certificates, and Windows® Server 2003 Service Pack 2 or later add SHA-2 functionality to SSL certificate by application of hotfixes (**KB968730** and **KB938397**). However, there are potential issues related to applications (see section on **Adoption Difficulties**).

Website operators must request new certificates to replace SHA-1 SSL and code-signing certificates that expire on or after January 1, 2017. CAs will be integral to this transition as they begin to promote SHA-2 certificates as replacements.

CAs must also work with website operators to replace already-issued SHA-1 code-signing certificates before January 1, 2016. This deadline applies to code-signing certificates intended for use on Microsoft® Windows® only. CAs may continue to issue SHA-1 certificates for non-Windows platforms.

SHA-2 adoption difficulties

The widespread adoption of SHA-1 by systems requiring hashing functions will contribute to the difficulty of SHA-2 adoption.

The widespread adoption of SHA-1 by systems requiring hashing functions will contribute to the difficulty of SHA-2 adoption. The wide spectrum of possible crypto devices, applications and systems demand a variety of management and upgrade paths. The most difficult aspect? Not everything that uses SHA-1 is compatible with SHA-2.

Upgrading an entire PKI from SHA-1 to SHA-2 will not only require the installation of CAs that are capable of issuing SHA-2 certificates, but ensuring all subscribers, relying parties, applications and devices can actually use the resulting SHA-2-based certificates is challenging.

For Microsoft systems, SHA-2 capabilities are native to Microsoft Windows Vista, Windows 7 and Windows Server 2008 (R2). However, Microsoft Windows XP Service Pack 3 and Windows Server 2003 SP2 clients with **KB968730** have only limited support for SHA-2. Support for SHA-2 on these platforms is limited to SSL/TLS capabilities.

Applications that use certificates, even on supported platforms, will also have to be evaluated to determine their compatibility with SHA-2. For example, Microsoft Outlook 2003 cannot validate a SHA-2 S/MIME certificate.

Platforms such as mobile devices, mainframes, mid-range computers, WAP devices, radius servers and VPN concentrators will also need to be evaluated to ensure compatibility with SHA-2. In many cases, an upgrade of some sort is required.

In short, because SHA-1 is embedded in so many different platforms, it can be a challenge to determine the full impact of migrating to SHA-2. Even newer systems include support for SHA-1 for compatibility with legacy CAs.

Many older clients don't support SHA-256. But which of those are relevant? The answer will vary depending on the site.

On the desktop, Microsoft Windows XP introduced SHA-256 in Service Pack 3. Users running SP2 should be able to upgrade to SP3. Depending on a site's profile, a significant portion of the user base might be running Microsoft Windows XP. This operating system is still very popular in China and there is also strong anecdotal evidence that it remains widely used in some large organizations.

And don't forget about mobile and embedded browsers. Among the mobile platforms, Google Android (Version 2.3+), Apple iOS (3.0+) and BlackBerry (5.0+) include SHA-256 support. Earlier versions — still used in large numbers — only support SHA-1.

Want the latest?

For detailed information on SHA-2 migration strategies, visit Entrust's resource center. Get the latest news, updates and information that will help you navigate through the sun-setting of the SHA-1 standard.

Visit Resource Center Now

Migration: people, process & technology

The migration of certificates is not trivial and has the potential to cause major problems, particularly if the process is not carefully planned and all affected parties are not considered.

The migration of certificates is not trivial and has the potential to cause major problems, particularly if the process is not carefully planned and all affected parties are not considered. This is not simply a patch that can be released as a global update, but rather requires strategic coordination between responsible IT and security management teams.

This involves establishing a process to ensure nothing is overlooked; all technological implications are considered; technology is implemented properly; and people know what to do in the event issues arise.

People First

People are always the weakest link in the security chain, so ensure everyone in the organization who manages or deploys applications, platforms or IT infrastructure is aware of the migration plan. This also includes help desks, customer service and support, and business application owners.

Organizations should consider this a time-sensitive initiative and appoint a project leader to drive the migration effort. The goal is to replace all certificates in a timely manner and ensure certificates currently in use (as well as applications and platforms scheduled to be deployed) are using SHA-2.

Everyone involved needs to be aware of the need for SHA-2 certificates, as well as the procedure for removing old certificates and procuring new ones. Each person who has knowledge of certificates — in use or planned for the future — should provide this information to the project lead to ensure that any and all certificates that require SHA-2 are accounted for in the migration plan.

At the same time, it's best to be prepared for the possibility that a certificate may not be replaced in time or that one is replaced on an incompatible system. It is not at all uncommon for a "rogue certificate" — one that has been purchased, deployed and is in use — to be completely unknown to an organization. This occurs when certificates are not centrally tracked or the person who purchased it has left the organization and no record remains.

Organizations can consume vast resources responding to and troubleshooting outages or security warnings caused by a rogue certificate. If help desks and application owners are notified about this scenario, then remediation will take place more rapidly.

The process: migration & support

Introducing a process will allow for a systematic migration where priority is placed on the most mission-critical applications and help prevent the use of incompatible certificates, which could impact operations. This approach should include this five-step process.

1

Identify all SHA-1 Certificates

Catalog all certificates currently in use or are planned on being deployed in the near future, including the certificate type, where they are deployed, and the applications and platforms they support.

Many organizations manually maintain this catalog in spreadsheets, so it's important to make sure all people are brought into the process. If you are using a certificate management service, the process will be easier but may not include "rogue certificates" deployed outside the service.

To address both these scenarios, use a certificate discovery tool to decrease the time and effort of cataloging and ensure a more accurate inventory. If you have servers and/or certificates hosted and managed outside your data centers (e.g., AWS, Rackspace, GoDaddy, etc.), make sure these are considered in your migration plan.

2

Prioritize Certificate Replacement

Start with certificates used on your most important sites, as well as those that expire after 2016. These certificates will be the most affected by the proposed changes and might stop working in 2017.

Next, work your way back to replace the remaining certificates. This step is time-consuming, but shouldn't involve further direct costs because most CAs will reissue certificates for free.

Replace SHA-1 certificates expiring on or before Jan. 1, 2017	○ With SHA-2 by Chrome version 39, November 3, 2014
Replace SHA-1 certificates expiring between Jan. 1, 2016, and Dec. 31, 2016	○ With SHA-2 by Chrome version 40, December 15, 2014
Replace SHA-1 certificates expiring between Jan. 1, 2016, and May 31, 2016	○ With SHA-2 by Chrome version 41, January 26, 2015 ○ **NOTE:** SHA-1 certificates expiring on or before December 31, 2015, should be renewed with SHA-2 by December 31, 2015
Other Considerations	○ Is the certificate used for server-to-server security? With server-to-server security, there is no end-user to see a trust dialogue or an error indication. ○ Are the users external? You have to assume that 50 percent of external users have Chrome and more than 50 percent are using Microsoft Windows. As such, most external users will be impacted. ○ Are the users internal? If internal users don't use Chrome, then they won't receive the security warnings.

3 Determine SHA-2 Support

This step is especially important as it relates to server platforms and older clients. Older server platforms might not be able to support SHA-256 certificates.

For example, Windows Server 2003 doesn't support SHA-256. Thus, upgrading to a SHA-256 certificate might require an upgrade or patching of the underlying platform.

Do you have significant use of older clients that don't support SHA-256? Most general-purpose sites can upgrade to SHA-256 and expect the users to upgrade, too, but large sites with diverse user bases might want to preserve SHA-1 compatibility for as long as possible. In some cases, this will be possible with dual-certificate deployment, described below.

4 Evaluate Use of Multi-Domain Certificates

If you use multiple SANs, Unified Communications or Wildcard certificates, consider splitting the certificate into multiple certificates. This will allow you to upgrade to SHA-2 for most uses and, if required, use SHA-1 for supporting legacy applications. This ONLY applies to the connections between servers and legacy applications.

5 Publish Policy on Certificate Issuance & Monitoring

This final step helps ensure that the proper certificates are deployed. Deploy a centralized certificate management, monitoring and notification system, along with an escalation notification process, to avoid one person being the single point of failure.

Technology considerations & implementation

If your new certificates are not guaranteed to be SHA-256, then all your other efforts will be futile.

There are a variety of technology-related factors to be taken into account, and system improvements to be considered, for more efficient ongoing operations.

Ensure New Certificates & Chains use SHA-256
This is critical. If your new certificates are not guaranteed to be SHA-256, then all your other efforts will be futile. At the end of a successful migration, all SHA-1 certificates that expire by the end of 2015 will be guaranteed to be ready for 2016 without further effort.

It's also necessary to check that the entire certificate chain is free of SHA-1. It's not common, but there are cases where the leaf uses SHA-256 but one of the intermediate certificates uses SHA-1. Don't worry if the root certificate uses SHA-1; signatures on roots are not verified (and the browsers won't warn about them).

Companies that use centralized certificate procurement should find this step straightforward. For others, this is a good opportunity to centralize certificate issuance.

Determine Older Client Support
Technically, it's possible to have the best of both worlds by providing SHA-256 certificates to modern clients and serve SHA-1 to those who can't migrate to the new standard. Indeed, there's nothing to say that a site can't use more than one certificate at the same time. This approach is ideal for transitions such as this one.

At this time, a site could use two certificates: ECDSA+SHA-256 for modern clients and RSA+SHA-1 for older clients. Unfortunately, this feature might not be available for your favorite platform.

At the time of publication, Apache is the only major server to support multiple certificates. If you are running Apache, consult their support documentation for dual-certificate deployment.

As for other platforms, CloudFlare and Yahoo have stated that they will add support to Nginx and Apache Traffic server, respectively.

Generate & Install New Certificates
When generating a new certificate, it is advisable to use a new private key. A new key is not a requirement to migrate from SHA-1 to SHA-2. Administrators should consider their own policy on whether they are required to use a new key pair. In some cases, new certificates may require a new CSR, so the key will change.

Consider how increased security may be achieved during this time; changing the key would be a good security practice and may help you mitigate another attack, such as Heartbleed.

Obtain installation instructions for your server to ensure that any changes required by SHA-2 are followed. Confirm proper installation using a configuration utility tool. And check to see if whether or not when installing the new SHA-2 certificates, you also need to install new intermediate and cross-certified certificate. This is often missed by in the process and is the source of many problems.

Deploy Management & Monitoring Systems
Implement a centralized and reliable tracking system. If you are manually tracking certificates, you will find cataloging all certificates to be inefficient unless you have only a few certificates and a single administrator.

Consider a certificate management service where all certificate activity is performed and monitored in a centralized account. This simplifies certificate inventory and helps your organization monitor certificate types and expiration dates.

Many services also offer renewal alerts, which provide a quick list of all your certificates that are approaching expiration. This helps you easily renew expiring certificates with the click of a button. Going forward, the default for all issued certificates should be SHA-2.

It's important to note, however, that many current certificate management systems may not be able to recognize if your organization deployed certificates on multiple servers. This is why certificate discovery tools are critical in today's certificate environment.

Theses advanced monitoring tools help you discover old certificates and prevent new ones from being deployed with SHA-1. An administrator should monitor the types of certificates being issued to ensure that SHA-1 or SHA-2 certificates are being deployed, as necessary.

A discovery system will allow organizations to monitor the deployment of rogue certificates and take quick action on non-compliant certificates. If you are not procuring and managing certificates via a central system, consider a management service to gain control of your complete certificate environment.

Looking forward

At this time, the plans for Apple Safari, Mozilla Firefox, Opera and other browsers are not known. As migrations being, more information will surface regarding incompatibility with a variety of servers, applications, platforms and devices. All will need to be addressed at some point.

Having the right processes and technology to manage these issues as they arise will serve organizations well. To stay up to date on SHA-2-related issues, visit Entrust's migration resource center for the latest news, tools and trends.

Visit SHA-2 Migration Center

Resource appendix

Important note

These lists were compiled from various sources as listed. As such, please note that Entrust nor the CA Security Council have independently tested the reported data and cannot guarantee that all entries on the lists are accurate.

In preparing your systems to be SHA-256-compliant, Entrust and the CASC recommends you independently research your own operating systems, browsers and servers and obtain confirmation from your vendors before proceeding.

Entrust is a member of the CA Security Council, which offers an up-to-date list of operating systems, browsers and servers that support SHA-2 SSL certificates. This version was accurate as of September 22, 2014.

OS, Browsers and Servers that Reportedly Support SHA-256 in their Entirety

Operating Systems/Other – Support SHA-256

- Android 2.3+
- Apple iOS 3.0+
- Apple OS X 10.5+
- Blackberry 5.0+
- ChromeOS
- Windows 7
- Windows Outlook 2003+ running on Service Pack 3 (partial), complete on Windows
- Vista
- Windows Phone 7+
- Windows Server 2003 SP2 +Hotfixes (Partial)
- Windows Server 2003 with MS13-095 installed
- Windows Server 2008
- Windows Server 2008 R2
- Windows Vista
- Windows XP SP3+

Browsers – Support SHA-256

- Adobe Acrobat/Reader 7
- Blackberry 5+
- Chrome 26+
- Chrome under Linux
- Chrome under Mac from Mac OS X 10.52
- Chrome under Windows Vista and higher
- Firefox 1.5+
- Internet Explorer 7+ and higher
- Internet Explorer 7+ under Vista
- Internet Explorer 7+ under Windows XP SP3
- Java 1.4.2+ based products
- Konqueror 3.5.6+
- Mozilla 1.4+
- Mozilla products based on NSS 3.8+ (since April 2003)
- Netscape 7.1+
- Opera 9.0+
- Products based on OpenSSL 0.9.8o+
- Safari from Mac OS X 10.5+
- Windows Phone 7+

Need an updated list?

Visit Entrust's migration resource center for news, updates, compatibility lists and more.

Visit Now

Servers – Support SHA-256

- Apache server with OpenSSL 0.9.8o+
- Apache 2.x or higher, with OpenSSL 1.1.x or higher
- Cisco ACE module software version A4(1.0)
- Citrix Receiver models:
- Mac 11.8.2
- Windows 4.1 (std)
- Windows 3.4 (ent)
- Windows 8/RT (1.4)
- Windows Phone 8 (1.1)
- IBM HTTP Server 8.5 (bundled with Domino 9)
- Java based servers – Java 1.4.2+
- Mozilla NSS based servers - 3.8+
- OpenSSL based servers – OpenSSL 0.9.8o+
- Oracle WebLogic from the version 10.3.1+, see bug 8422724

Servers that Reportedly DO NOT Support SHA-256 in their Entirety

Servers

- Juniper SBR
- IBM Domino
- Citrix Receiver models*
- Linux 13.0
- IOS 5.8.3
- Android 3.4.13
- HTML 5 1.2
- Playbook 1.0
- Blackberry 2.2 / BlackBerry 1.0 Tech Preview
- Cisco ACE module software versions A2 and A3

* Citrix Receiver Models (See Table):
http://citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-receiver-feature-matrix.pdf?accessmode=direct

Sources
https://tbs-certificates.co.uk/FAQ/en/477.html
https://tbs-certificates.co.uk/FAQ/en/476.html
https://support.servertastic.com/sha2-sha256-compatibility/
http://kb.juniper.net/InfoCenter/index?page=content&id=KB23075
http://entrust.com/should-you-use-sha-2/
http://p2vme.com/2014/02/sha2-certificates-and-citrix-receiver.html
http://blogs.technet.com/b/pki/archive/2010/09/30/sha2-and-windows.aspx
http://entrust.net/knowledge-base/technote.cfm?tn=8526

Entrust and you

"More than ever, Entrust understands your organization's security pain points."

Entrust offers software authentication platforms that strengthen security in a wide range of identity and transaction ecosystems. Government agencies, financial institutions and other enterprises rely on Entrust solutions to strengthen trust and reduce complexity for consumers, citizens and employees.

Now, as part of Datacard Group, Entrust offers an expanded portfolio of solutions across more than 150 countries. Together, Datacard Group and Entrust issue more than 10 million secure identities every day, manage billions of secure transactions annually and issue a majority of the world's financial cards.

For more information about Entrust solutions, call **+1 888-690-2424**, email **entrust@entrust.com** or visit **www.entrust.com**.

Company Facts
Website: entrust.com
Employees: 359
Customers: 5,000
Offices: 10 globally

Headquarters
Three Lincoln Centre
5430 LBJ Freeway,
Suite 1250
Dallas, TX 75240 USA

Sales
North America:
+1-888-690-2424
EMEA: +44 (0) 118 953 3000
Email: entrust@entrust.com

Twitter Facebook Youtube LinkedIn Google+ RSS

Entrust®

30093/10-12