



List of Operating Systems, Browsers, and Servers Which Support SHA-256 Hashes in SSL Certificates

Revised as of: September 8, 2014

The CA Security Council (CASC) has compiled the following lists of operating systems (OS), browsers, and servers which we believe support SHA-256 hashing in SSL certificates, as well as a partial list of servers which apparently do not. We are providing these lists as a starting point to help enterprises check their systems for SHA-256 compliance.

These lists were compiled from various sources as listed below. CASC has not 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, CASC recommends you independently research your own operating systems, browsers, and servers and obtain confirmation from your vendors before proceeding.

OS, Browsers, and Servers which 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 10.5

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+

Servers – support SHA-256

Adobe Acrobat/Reader 7
Blackberry 5+
Chrome 26+
Chrome under Linux
Chrome under Mac from Mac OS X 10.5
Chrome under Windows Vista and higher
Firefox 1.5+
Citrix Receiver models – see URL*
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+

Servers which reportedly DO NOT support SHA-256 in their entirety

Servers

Juniper SBR
IBM Domino
Citrix Receiver models – see URL*
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 URL (see table):

http://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-receiver-feature-matrix.pdf?accessmode=direct

Sources:

<https://www.tbs-certificates.co.uk/FAQ/en/477.html>

<https://www.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>

<https://support.globalsign.com/customer/portal/articles/1499561-sha-256-compatibility>

<http://www.entrust.com/should-you-use-sha-2/>

<http://www.p2vme.com/2014/02/sha2-certificates-and-citrix-receiver.html>

<http://h10025.www1.hp.com/ewfrf/wc/document?cc=us&lc=en&dlc=en&docname=c02671280>

<http://blogs.technet.com/b/pki/archive/2010/09/30/sha2-and-windows.aspx>

<http://www.entrust.net/knowledge-base/technote.cfm?tn=8526>