Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > wikipedia.org > 208.80.154.224

SSL Report: wikipedia.org (208.80.154.224)

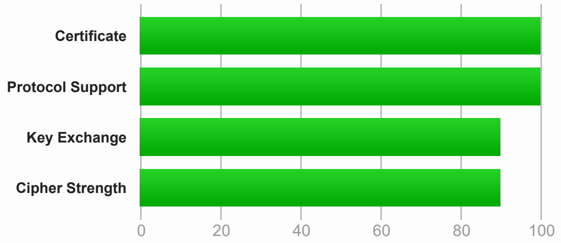
Assessed on: Fri, 22 Oct 2021 19:16:39 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

A+



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.3.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

DNS Certification Authority Authorization (CAA) Policy found for this domain. MORE INFO »

Certificate #1: EC 256 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	*.wikipedia.org Fingerprint SHA256: b0b211022d1ac8c98d126cb1a44b7f1dd36d849d2ef7769376625d07eb1fba94 Pin SHA256: UA/9EtY5W1/0r+Yc/JFoD96uUqegHXsEKUaWfhGIGBM=
Common names	*.wikipedia.org
Alternative names	*.m.mediawiki.org *.m.wikibooks.org *.m.wikidata.org *.m.wikimedia.org *.m.wikinews.org *.m.wikipedia.org *.m.wikiquote.org *.m.wikisource.org *.m.wikiversity.org *.m.wikivoyage.org *.m.wiktionary.org *.mediawiki.org *.planet.wikimedia.org *.wikibooks.org *.wikidata.org *.wikimedia.org *.wikimediafoundation.org *.wikinews.org *.wikipedia.org *.wikiquote.org *.wikisource.org *.wikiversity.org *.wikivoyage.org *.wiktionary.org *.wmfusercontent.org mediawiki.org w.wiki wikibooks.org wikidata.org wikimedia.org wikimediafoundation.org wikinews.org wikipedia.org wikiquote.org wikisource.org wikiversity.org wikivoyage.org wiktionary.org wmfusercontent.org
Serial Number	03952f4669dee4d219357ff0276afafe09cb
Valid from	Mon, 13 Sep 2021 08:02:37 UTC
Valid until	Sun, 12 Dec 2021 08:02:36 UTC (expires in 1 month and 19 days)
Key	EC 256 bits
Weak key (Debian)	No
Issuer	R3 AIA: http://r3.i.lencr.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	**Yes (certificate)**
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://r3.o.lencr.org
Revocation status	Good (not revoked)

Server Key and Certificate #1

DNS CAA	**Yes** policy host: wikipedia.org issue: globalsign.com flags:0 issue: digicert.com flags:0 issue: letsencrypt.org flags:0 iodef: mailto:dns-admin@wikimedia.org flags:0
Trusted	**Yes** **Mozilla Apple Android Java Windows**

Additional Certificates (if supplied)

Certificates provided	3 (4490 bytes)
Chain issues	None

#2

Subject	R3 Fingerprint SHA256: 67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd Pin SHA256: jQJTbIh0grw0/1TkHSumWb+Fs0Ggogr621gT3PvPKG0=
Valid until	Mon, 15 Sep 2025 16:00:00 UTC (expires in 3 years and 10 months)
Key	RSA 2048 bits (e 65537)
Issuer	ISRG Root X1
Signature algorithm	SHA256withRSA

#3

Subject	ISRG Root X1 Fingerprint SHA256: 6d99fb265eb1c5b3744765fcbc648f3cd8e1bffafdc4c2f99b9d47cf7ff1c24f Pin SHA256: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M=
Valid until	Mon, 30 Sep 2024 18:14:03 UTC (expires in 2 years and 11 months)
Key	RSA 4096 bits (e 65537)
Issuer	DST Root CA X3
Signature algorithm	SHA256withRSA

Certification Paths

⊞

Click here to expand

Certificate #2: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	*.wikipedia.org Fingerprint SHA256: 5a9e52ce90bec2a8c768284bfd3e354efb290c5f8e31c4b57d66721a515dd053 Pin SHA256: Yc1/66RpyWrBzwe/JqswCvEJQcm39j479Uxip19OIHM=
Common names	*.wikipedia.org
Alternative names	*.m.mediawiki.org *.m.wikibooks.org *.m.wikidata.org *.m.wikimedia.org *.m.wikinews.org *.m.wikipedia.org *.m.wikiquote.org *.m.wikisource.org *.m.wikiversity.org *.m.wikivoyage.org *.m.wiktionary.org *.mediawiki.org *.planet.wikimedia.org *.wikibooks.org *.wikidata.org *.wikimedia.org *.wikimediafoundation.org *.wikinews.org *.wikipedia.org *.wikiquote.org *.wikisource.org *.wikiversity.org *.wikivoyage.org *.wiktionary.org *.wmfusercontent.org mediawiki.org w.wiki wikibooks.org wikidata.org wikimedia.org wikimediafoundation.org wikinews.org wikipedia.org wikiquote.org wikisource.org wikiversity.org wikivoyage.org wiktionary.org wmfusercontent.org
Serial Number	0375c008dee3e6e49918735340afe6d8601a
Valid from	Mon, 13 Sep 2021 08:03:25 UTC
Valid until	Sun, 12 Dec 2021 08:03:24 UTC (expires in 1 month and 19 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	R3 AIA: http://r3.i.lencr.org/

Server Key and Certificate #1

Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	**Yes (certificate)**
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://r3.o.lencr.org
Revocation status	Good (not revoked)
DNS CAA	**Yes** policy host: wikipedia.org issue: globalsign.com flags:0 issue: digicert.com flags:0 issue: letsencrypt.org flags:0 iodef: mailto:dns-admin@wikimedia.org flags:0
Trusted	**Yes** **Mozilla Apple Android Java Windows**

Additional Certificates (if supplied)

Certificates provided	3 (4692 bytes)
Chain issues	None

#2

Subject	R3 Fingerprint SHA256: 67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd Pin SHA256: jQJTbIh0grw0/1TkHSumWb+Fs0Ggogr621gT3PvPKG0=
Valid until	Mon, 15 Sep 2025 16:00:00 UTC (expires in 3 years and 10 months)
Key	RSA 2048 bits (e 65537)
Issuer	ISRG Root X1
Signature algorithm	SHA256withRSA

#3

Subject	ISRG Root X1 Fingerprint SHA256: 6d99fb265eb1c5b3744765fcbc648f3cd8e1bffafdc4c2f99b9d47cf7ff1c24f Pin SHA256: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M=
Valid until	Mon, 30 Sep 2024 18:14:03 UTC (expires in 2 years and 11 months)
Key	RSA 4096 bits (e 65537)
Issuer	DST Root CA X3
Signature algorithm	SHA256withRSA

Certification Paths

Click here to expand

Configuration

Protocols

TLS 1.3	Yes
TLS 1.2	Yes
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

Cipher Suites

Cipher Suites

# TLS 1.3 (suites in server-preferred order)

TLS_AES_256_GCM_SHA384 (0x1302)	ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303)	ECDH x25519 (eq. 3072 bits RSA) FS	256P
TLS_AES_128_GCM_SHA256 (0x1301)	ECDH x25519 (eq. 3072 bits RSA) FS	128

# TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)	ECDH x25519 (eq. 3072 bits RSA) FS	256P
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)	ECDH x25519 (eq. 3072 bits RSA) FS	256P
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH x25519 (eq. 3072 bits RSA) FS	128

(P) This server prefers ChaCha20 suites with clients that don't have AES-NI (e.g., Android devices)

Handshake Simulation

Android 4.4.2	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Android 5.0.0	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Android 6.0	EC 256 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Android 7.0	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	ECDH x25519	FS
Android 8.0	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	ECDH x25519	FS
Android 8.1	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH x25519	FS
Android 9.0	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH x25519	FS
BingPreview Jan 2015	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDH secp256r1	FS
Chrome 69 / Win 7 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH x25519	FS
Chrome 70 / Win 10	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519	FS
Chrome 80 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519	FS
Firefox 31.3.0 ESR / Win 7	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 47 / Win 7 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	ECDH secp256r1	FS
Firefox 49 / XP SP3	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Firefox 62 / Win 7 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH x25519	FS
Firefox 73 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519	FS
Googlebot Feb 2018	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH x25519	FS
IE 11 / Win 7 R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
IE 11 / Win 8.1 R	EC 256 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
IE 11 / Win Phone 8.1 R	EC 256 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
IE 11 / Win Phone 8.1 Update R	EC 256 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
IE 11 / Win 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Edge 15 / Win 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH x25519	FS
Edge 16 / Win 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH x25519	FS
Edge 18 / Win 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH x25519	FS
Edge 13 / Win Phone 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Java 8u161	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Java 11.0.3	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH secp256r1	FS
Java 12.0.1	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH secp256r1	FS
OpenSSL 1.0.1l R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
OpenSSL 1.0.2s R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
OpenSSL 1.1.0k R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH x25519	FS
OpenSSL 1.1.1c R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519	FS
Safari 6 / iOS 6.0.1	Server sent fatal alert: handshake_failure				
Safari 7 / iOS 7.1 R	Server sent fatal alert: handshake_failure				

Handshake Simulation

Safari 7 / OS X 10.9 R	Server sent fatal alert: handshake_failure			
Safari 8 / iOS 8.4 R	Server sent fatal alert: handshake_failure			
Safari 8 / OS X 10.10 R	Server sent fatal alert: handshake_failure			
Safari 9 / iOS 9 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Safari 10 / iOS 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Safari 10 / OS X 10.12 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Safari 12.1.2 / MacOS 10.14.6 Beta R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH x25519 FS
Safari 12.1.1 / iOS 12.3.1 R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH x25519 FS
Apple ATS 9 / iOS 9 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Yahoo Slurp Jan 2015	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
YandexBot Jan 2015	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS

# Not simulated clients (Protocol mismatch)

⊞

Click here to expand

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

(3) Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.

(R) Denotes a reference browser or client, with which we expect better effective security.

(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).

(All) Certificate trust is not checked in handshake simulation, we only perform TLS handshake.

Protocol Details

DROWN	No, server keys and hostname not seen elsewhere with SSLv2 **(1) For a better understanding of this test, please read this longer explanation** (2) Key usage data kindly provided by the Censys network search engine; original DROWN website here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Mitigated server-side (more info)
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info)
GOLDENDOODLE	No (more info)
OpenSSL 0-Length	No (more info)
Sleeping POODLE	No (more info)
Downgrade attack prevention	**Yes, TLS_FALLBACK_SCSV supported** (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
ROBOT (vulnerability)	No (more info)
Forward Secrecy	**Yes (with most browsers)** **ROBUST** (more info)
ALPN	Yes h2 http/1.1
NPN	Yes h2 http/1.1 http/1.0
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	**Yes**

Protocol Details

Strict Transport Security (HSTS)	**Yes** max-age=106384710; includeSubDomains; preload
HSTS Preloading	**Chrome Edge Firefox IE**
Public Key Pinning (HPKP)	No (more info)
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No (more info)
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
ECDH public server param reuse	No
Supported Named Groups	x25519, secp256r1 (server preferred order)
SSL 2 handshake compatibility	No
0-RTT enabled	No

HTTP Requests

1 **https://wikipedia.org/** (HTTP/1.1 301 Moved Permanently)

Miscellaneous

Test date	Fri, 22 Oct 2021 19:14:40 UTC
Test duration	59.519 seconds
HTTP status code	301
HTTP forwarding	https://www.wikipedia.org
HTTP server signature	mw1430.eqiad.wmnet
Server hostname	text-lb.eqiad.wikimedia.org

SSL Report v2.1.8

Copyright © 2009-2021 Qualys, Inc. All Rights Reserved.

Terms and Conditions

Try Qualys for free! Experience the award-winning Qualys Cloud Platform and the entire collection of Qualys Cloud Apps, including certificate security solutions.