Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > www.tocupboard.rf.gd

SSL Report: www.tocupboard.rf.gd (185.27.134.34)

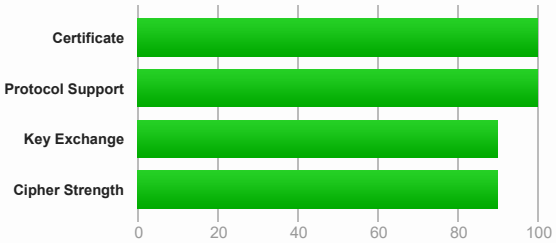
Assessed on: Thu, 05 Sep 2024 02:44:27 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

B



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

This server's certificate chain is incomplete. Grade capped to B.

This server's certificate is not trusted by Java trust store (see below for details).

This site works only in browsers with SNI support.

This server supports TLS 1.3.

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	tocupboard.rf.gd Fingerprint SHA256: 414f0a10ed4bcf7a4434471e16a180e9f643cfe5580ef79f33c29314fdc322a5 Pin SHA256: fRaQ40SXwsSPUWixwNJeES01U5O1i21SIwdky3/mxrQ=
Common names	tocupboard.rf.gd
Alternative names	tocupboard.rf.gd *.tocupboard.rf.gd
Serial Number	00b6df8cea9379bf590d5e44cf0cd45d5b
Valid from	Sun, 01 Sep 2024 21:58:25 UTC
Valid until	Sat, 30 Nov 2024 21:58:24 UTC (expires in 2 months and 25 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	WR1 AIA: http://i.pki.goog/wr1.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://c.pki.goog/wr1/-4CjnBIfzTs.crl OCSP: http://o.pki.goog/s/wr1/tt8
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	1 (1347 bytes)
Chain issues	Incomplete

Certification Paths

Mozilla Apple Android Java Windows

Path #1: Trusted

1	Sent by server	tocupboard.rf.gd Fingerprint SHA256: 414f0a10ed4bcf7a4434471e16a180e9f643cfe5580ef79f33c29314fdc322a5 Pin SHA256: fRaQ40SXwsSPUWixwNJeES01U5O1i21SIwdky3/mxrQ= RSA 2048 bits (e 65537) / SHA256withRSA
2	Extra download	WR1 Fingerprint SHA256: b10b6f00e609509e8700f6d34687a2bfce38ea05a8fdf1cdc40c3a2a0d0d0e45 Pin SHA256: yDu9og255NN5GEf+Bwa9rTrqFQ0EydZ0r1FCh9TdAW4= RSA 2048 bits (e 65537) / SHA256withRSA
3	In trust store	GTS Root R1 Self-signed Fingerprint SHA256: 2a575471e31340bc21581cbd2cf13e158463203ece94bcf9d3cc196bf09a5472 Pin SHA256: hxqRlPTu1bMS/0DITB1SSu0vd4u/8l8TjPgfaAp63Gc= RSA 4096 bits (e 65537) / SHA384withRSA

Path #2: Not trusted (path does not chain to a trusted anchor)

1	Sent by server	tocupboard.rf.gd Fingerprint SHA256: 414f0a10ed4bcf7a4434471e16a180e9f643cfe5580ef79f33c29314fdc322a5 Pin SHA256: fRaQ40SXwsSPUWixwNJeES01U5O1i21SIwdky3/mxrQ= RSA 2048 bits (e 65537) / SHA256withRSA
2	Extra download	WR1 Fingerprint SHA256: b10b6f00e609509e8700f6d34687a2bfce38ea05a8fdf1cdc40c3a2a0d0d0e45 Pin SHA256: yDu9og255NN5GEf+Bwa9rTrqFQ0EydZ0r1FCh9TdAW4= RSA 2048 bits (e 65537) / SHA256withRSA
3	Extra download Not in trust store	GTS Root R1 Self-signed Fingerprint SHA256: d947432abde7b7fa90fc2e6b59101b1280e0e1c7e4e40fa3c6887fff57a7f4cf Pin SHA256: hxqRlPTu1bMS/0DITB1SSu0vd4u/8l8TjPgfaAp63Gc= RSA 4096 bits (e 65537) / SHA384withRSA

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

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	256
TLS_AES_128_GCM_SHA256 (0x1301) ECDH x25519 (eq. 3072 bits RSA) FS	128

TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) 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_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 2048 bits FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	256

Cipher Suites

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 2048 bits FS **WEAK**	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 2048 bits FS **WEAK**	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 2048 bits FS **WEAK**	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 2048 bits FS **WEAK**	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) **WEAK**	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) **WEAK**	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) **WEAK**	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) **WEAK**	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) **WEAK**	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK**	256
TLS_DHE_RSA_WITH_AES_256_CCM_8 (0xc0a3) DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CCM (0xc09f) DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_128_CCM_8 (0xc0a2) DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_128_CCM (0xc09e) DH 2048 bits FS	128
TLS_RSA_WITH_AES_256_CCM_8 (0xc0a1) **WEAK**	256
TLS_RSA_WITH_AES_256_CCM (0xc09d) **WEAK**	256
TLS_RSA_WITH_AES_128_CCM_8 (0xc0a0) **WEAK**	128
TLS_RSA_WITH_AES_128_CCM (0xc09c) **WEAK**	128
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 (0xc077) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256 (0xc4) DH 2048 bits FS **WEAK**	256
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xc076) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xbe) DH 2048 bits FS **WEAK**	128
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) DH 2048 bits FS **WEAK**	256
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 2048 bits FS **WEAK**	128
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 (0xc0) **WEAK**	256
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xba) **WEAK**	128
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) **WEAK**	256
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) **WEAK**	128

Handshake Simulation

Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 6.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Android 8.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Android 8.1	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS
Android 9.0	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 69 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 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	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 62 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Firefox 73 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS
Googlebot Feb 2018	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 DH 2048 FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 DH 2048 FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 DH 2048 FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS

Handshake Simulation

Edge 16 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Edge 18 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Java 8u161	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	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	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
OpenSSL 1.0.2s R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
OpenSSL 1.1.0k R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	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	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
Safari 8 / OS X 10.10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Safari 12.1.2 / MacOS 10.14.6 Beta R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Safari 12.1.1 / iOS 12.3.1 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Apple ATS 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	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

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) TLS 1.2 : `0xc027`
GOLDENDOODLE	No (more info) TLS 1.2 : `0xc027`
OpenSSL 0-Length	No (more info) TLS 1.2 : `0xc027`
Sleeping POODLE	No (more info) TLS 1.2 : `0xc027`
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)

Protocol Details

Forward Secrecy	**Yes (with most browsers) ROBUST** (more info)
ALPN	Yes http/1.1
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: 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
DH public server param (Ys) reuse	No
ECDH public server param reuse	No
Supported Named Groups	x25519, secp256r1, x448, secp521r1, secp384r1 (server preferred order)
SSL 2 handshake compatibility	No
0-RTT enabled	No

HTTP Requests

1 **https://www.tocupboard.rf.gd/** (HTTP/1.1 200 OK)

Miscellaneous

Test date	Thu, 05 Sep 2024 02:42:05 UTC
Test duration	141.675 seconds
HTTP status code	200
HTTP server signature	nginx
Server hostname	-

SSL Report v2.3.0