

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [amazon.com](#) > 205.251.242.103

SSL Report: [amazon.com](#) (205.251.242.103)

Assessed on: Fri, 16 Aug 2024 17:00:19 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating

B

Certificate

Protocol Support

Key Exchange

Cipher Strength

020406080100

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. [MORE INFO »](#)

This server supports TLS 1.3.

Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1

| | |
|--------------------------|---|
| Subject | *.peg.a2z.com Fingerprint SHA256: bb638b53bbde53dff9e8f707b9be32751e84fd865910636281902b204b062a50 Pin SHA256: Ed2cQ7afGimEu1/mbjgo+6D7bLWOGn14R83JptnHogk= |
| Common names | *.peg.a2z.com amazon.co.uk uedata.amazon.co.uk www.amazon.co.uk origin-www.amazon.co.uk *.peg.a2z.com amazon.-com amzn.com uedata.amazon.com us.amazon.com www.amazon.com www.amzn.com corporate.amazon.-com buybox.amazon.com iphone.amazon.com yp.amazon.com home.amazon.com origin-www.amazon.com origin2-www.amazon.com buckeye-retail-website.amazon.com huddles.amazon.com amazon.de www.amazon.de origin-www.amazon.de amazon.co.jp amazon.jp www.amazon.jp www.amazon.co.jp origin-www.amazon.co.jp *.aa.peg.a2z.com *.ab.peg.a2z.com *.ac.peg.a2z.com origin-www.amazon.com.au www.amazon.-com.au *.bz.peg.a2z.com amazon.com.au origin2-www.amazon.co.jp edgeflow.aero.4d5ad1d2b-frontier.amazon.co.jp edgeflow.aero.04f01a85e-frontier.amazon.com.au edgeflow.aero.47cf2c8c9-frontier.amazon.com edgeflow.aero.abe2c2f23-frontier.amazon.de edgeflow.aero.bfbdc3ca1-frontier.amazon.co.uk edgeflow-dp.aero.4d5ad1d2b-frontier.amazon.co.jp edgeflow-dp.aero.04f01a85e-frontier.amazon.com.au edgeflow-dp.aero.47cf2c8c9-frontier.amazon.com |
| Alternative names | |
| Serial Number | 0edb97391cb586451865e838f9f52971 |
| Valid from | Fri, 02 Feb 2024 00:00:00 UTC |
| Valid until | Tue, 07 Jan 2025 23:59:59 UTC (expires in 4 months and 22 days) |
| Key | RSA 2048 bits (e 65537) |
| Weak key (Debian) | No |
| Issuer | DigiCert Global CA G2 AIA: http://cacerts.digicert.com/DigiCertGlobalCAG2.crt |
| Signature algorithm | SHA256withRSA |
| Extended Validation | No |
| Certificate Transparency | Yes (certificate) |
| OCSP Must Staple | No |
| Revocation information | CRL, OCSP CRL: http://crl3.digicert.com/DigiCertGlobalCAG2.crl |

| | |
|-------------------------------|---|
| Server Key and Certificate #1 | |
| | OCSF: http://ocsp.digicert.com |
| Revocation status | Good (not revoked) |
| DNS CAA | No (more info) |
| Trusted | Yes Mozilla Apple Android Java Windows |

| | |
|---------------------------------------|---|
| Additional Certificates (if supplied) | |
| Certificates provided | 3 (5043 bytes) |
| Chain issues | None |
| #2 | |
| Subject | DigiCert Global CA G2 Fingerprint SHA256: 8fac576439c9fd3ef153b51f9edd0d381b5df7b87559cebeca04297dd44a639b Pin SHA256: njN4rRG+22dNXAi+yb8e3UMypgzPUPHlV4+foULw1g= |
| Valid until | Tue, 01 Aug 2028 12:00:00 UTC (expires in 3 years and 11 months) |
| Key | RSA 2048 bits (e 65537) |
| Issuer | DigiCert Global Root G2 |
| Signature algorithm | SHA256withRSA |
| #3 | |
| Subject | DigiCert Global Root G2 Fingerprint SHA256: aadadd5a879d2eb8c41a89597291292709d42052f5b6399541c694c3b7353cd1 Pin SHA256: i7WTqTvh0OiolrulfFR4kMPnBqrS2rdiVPI/s2uC/CY= |
| Valid until | Sun, 02 Apr 2028 23:59:59 UTC (expires in 3 years and 7 months) |
| Key | RSA 2048 bits (e 65537) |
| Issuer | VeriSign Class 3 Public Primary Certification Authority - G5 |
| Signature algorithm | SHA256withRSA |

| | |
|---------------------------------|--|
| Certification Paths | |
| <div>Click here to expand</div> | |

Configuration

| | |
|--|---|
| Protocols | |
| TLS 1.3 | Yes |
| TLS 1.2 | Yes |
| TLS 1.1 | Yes |
| TLS 1.0 | Yes |
| SSL 3 | No |
| SSL 2 | No |
| Cipher Suites | |
| # TLS 1.3 (suites in server-preferred order) | |
| TLS_AES_128_GCM_SHA256 (0x1301) | ECDH x25519 (eq. 3072 bits RSA) FS 128 |
| TLS_AES_256_GCM_SHA384 (0x1302) | ECDH x25519 (eq. 3072 bits RSA) FS 256 |
| # 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_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 |

Cipher Suites

| | |
|--|-------------------|
| TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK | 128 |
| TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK | 128 |
| TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK | 128 |
| # TLS 1.1 (suites in server-preferred order) | + |
| # TLS 1.0 (suites in server-preferred order) | + |



Handshake Simulation

| | | | |
|--|---|------------------------------|--|
| Android 2.3.7 No SNI ² | RSA 2048 (SHA256) | TLS 1.0 | TLS_RSA_WITH_AES_128_CBC_SHA No FS |
| Android 4.0.4 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS |
| Android 4.1.1 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS |
| Android 4.2.2 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS |
| Android 4.3 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS |
| 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_128_GCM_SHA256 ECDH x25519 FS |
| Android 9.0 | - | TLS 1.3 | TLS_AES_128_GCM_SHA256 ECDH x25519 FS |
| Baidu Jan 2015 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 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_128_GCM_SHA256 ECDH x25519 FS |
| Chrome 80 / Win 10 R | - | TLS 1.3 | TLS_AES_128_GCM_SHA256 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_128_GCM_SHA256 ECDH x25519 FS |
| Googlebot Feb 2018 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS |
| IE 7 / Vista | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS |
| IE 8 / XP No FS ¹ No SNI ² | Server sent fatal alert: handshake_failure | | |
| IE 8-10 / Win 7 R | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS |
| IE 11 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS |
| IE 11 / Win 8.1 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS |
| IE 10 / Win Phone 8.0 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 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_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 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 |
| 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 6u45 No SNI ² | RSA 2048 (SHA256) | TLS 1.0 | TLS_RSA_WITH_AES_128_CBC_SHA No FS |
| Java 7u25 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA 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_128_GCM_SHA256 ECDH secp256r1 FS |
| Java 12.0.1 | - | TLS 1.3 | TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS |


Handshake Simulation

| | | | | |
|--|-------------------|--------------------|---------------------------------------|-------------------|
| OpenSSL 0.9.8y | RSA 2048 (SHA256) | TLS 1.0 | TLS_RSA_WITH_AES_128_CBC_SHA | No 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_128_GCM_SHA256 | ECDH x25519 FS |
| Safari 5.1.9 / OS X 10.6.8 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | ECDH secp256r1 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 6.0.4 / OS X 10.8.4 R | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | 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_128_GCM_SHA256 | ECDH x25519 FS |
| Safari 12.1.1 / iOS 12.3.1 R | - | TLS 1.3 | TLS_AES_128_GCM_SHA256 | 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)

IE 6 / XP No FS ¹ No SNI ² Protocol mismatch (not simulated)

- (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 | Not mitigated server-side (more info) TLS 1.0: 0xc013 |
| 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 | With modern browsers (more info) |
| ALPN | Yes http/1.1 |
| NPN | Yes http/1.1 |
| Session resumption (caching) | Yes |
| Session resumption (tickets) | No |
| OCSP stapling | Yes |
| 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, 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, x448, secp521r1, secp384r1 (server preferred order) |
| SSL 2 handshake compatibility | Yes |
| 0-RTT enabled | No |



HTTP Requests



1 <https://amazon.com/> (HTTP/1.1 301 Moved Permanently)



Miscellaneous

| | |
|-----------------------|---|
| Test date | Fri, 16 Aug 2024 16:58:11 UTC |
| Test duration | 127.700 seconds |
| HTTP status code | 301 |
| HTTP forwarding | https://www.amazon.com |
| HTTP server signature | Server |
| Server hostname | s3-console-us-standard.console.aws.amazon.com |

SSL Report v2.3.0