Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

**You are here:** Home > Projects > SSL Server Test > wp.98-89-111-197.sslip.io

# SSL Report: wp.98-89-111-197.sslip.io (98.89.111.197)

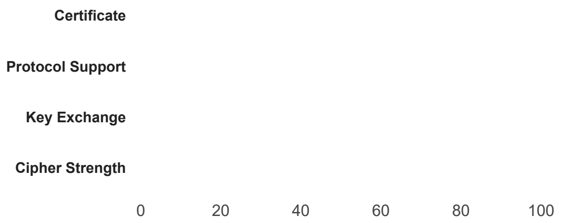
**Assessed on:** Wed, 19 Nov 2025 22:34:56 UTC | Hide | Clear cache

**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.** MORE INFO »

## Certificate #1: EC 256 bits (SHA384withECDSA)

### Server Key and Certificate #1

| | |
|---|---|
| **Subject** | wp.98-89-111-197.sslip.io<br>Fingerprint SHA256: 6f1a13e11a1cc923302d7e5581d23830e1632d00d968761c6ce95ae76ce17ec9<br>Pin SHA256: 694vMN4O4OyUWr57il88TzfcALjoKFH0jjFBP4s7xo0= |
| **Common names** | wp.98-89-111-197.sslip.io |
| **Alternative names** | wp.98-89-111-197.sslip.io |
| **Serial Number** | 05a43e1612b58bf2b7bb1a985fc82f9617d7 |
| **Valid from** | Wed, 19 Nov 2025 19:19:21 UTC |
| **Valid until** | Tue, 17 Feb 2026 19:19:20 UTC (expires in 2 months and 28 days) |
| **Key** | EC 256 bits |
| **Weak key (Debian)** | No |
| **Issuer** | E7<br>AIA: http://e7.i.lencr.org/ |
| **Signature algorithm** | SHA384withECDSA |
| **Extended Validation** | No |
| **Certificate Transparency** | **Yes (certificate)** |
| **OCSP Must Staple** | No |
| **Revocation information** | CRL<br>CRL: http://e7.c.lencr.org/88.crl |
| **Revocation status** | **Validation error**<br>**CRL ERROR: IOException occurred** |
| **DNS CAA** | No (more info) |
| **Trusted** | **Yes**<br>**Mozilla Apple Android Java Windows** |

### Additional Certificates (if supplied)

| | |
|---|---|
| **Certificates provided** | 2 (2045 bytes) |
| **Chain issues** | None |

### Additional Certificates (if supplied)

#### #2

| | |
|---|---|
| **Subject** | E7<br>Fingerprint SHA256: aeb1fd7410e83bc96f5da3c6a7c2c1bb836d1fa5cb86e708515890e428a8770b<br>Pin SHA256: y7xVm0TVJNahMr2sZydE2jQH8SquXV9yLF9seROHHHU= |
| **Valid until** | Fri, 12 Mar 2027 23:59:59 UTC (expires in 1 year and 3 months) |
| **Key** | EC 384 bits |
| **Issuer** | ISRG Root X1 |
| **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

#### # 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_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) | ECDH x25519 (eq. 3072 bits RSA) FS | 256 |
| TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) | ECDH x25519 (eq. 3072 bits RSA) FS | 128 |
| TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) | ECDH x25519 (eq. 3072 bits RSA) FS **WEAK** | 256 |
| TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384 (0xc073) | ECDH x25519 (eq. 3072 bits RSA) FS **WEAK** | 256 |
| TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) | ECDH x25519 (eq. 3072 bits RSA) FS **WEAK** | 128 |
| TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256 (0xc072) | ECDH x25519 (eq. 3072 bits RSA) FS **WEAK** | 128 |
| TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9) | ECDH x25519 (eq. 3072 bits RSA) FS | 256 |
| TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8 (0xc0af) | ECDH x25519 (eq. 3072 bits RSA) FS | 256 |
| TLS_ECDHE_ECDSA_WITH_AES_256_CCM (0xc0ad) | ECDH x25519 (eq. 3072 bits RSA) FS | 256 |
| TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384 (0xc05d) | ECDH x25519 (eq. 3072 bits RSA) FS | 256 |
| TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 (0xc0ae) | ECDH x25519 (eq. 3072 bits RSA) FS | 128 |
| TLS_ECDHE_ECDSA_WITH_AES_128_CCM (0xc0ac) | ECDH x25519 (eq. 3072 bits RSA) FS | 128 |
| TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256 (0xc05c) | ECDH x25519 (eq. 3072 bits RSA) FS | 128 |
| TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) | ECDH x25519 (eq. 3072 bits RSA) FS **WEAK** | 256 |
| TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) | ECDH x25519 (eq. 3072 bits RSA) FS **WEAK** | 128 |

### Handshake Simulation

| | | | |
|---|---|---|---|
| Android 4.4.2 | EC 256 (SHA384) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |

### Handshake Simulation

| | | | |
|---|---|---|---|
| Android 5.0.0 | EC 256 (SHA384) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Android 6.0 | EC 256 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Android 7.0 | EC 256 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS |
| Android 8.0 | EC 256 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 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 | EC 256 (SHA384) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| Chrome 49 / XP SP3 | Server sent fatal alert: handshake_failure | | |
| Chrome 69 / Win 7 R | EC 256 (SHA384) | TLS 1.2 > http/1.1 | 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 (SHA384) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Firefox 47 / Win 7 R | EC 256 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Firefox 49 / XP SP3 | EC 256 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| Firefox 62 / Win 7 R | EC 256 (SHA384) | TLS 1.2 > http/1.1 | 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 (SHA384) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS |
| IE 11 / Win 7 R | EC 256 (SHA384) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| IE 11 / Win 8.1 R | EC 256 (SHA384) | 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 (SHA384) | 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 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| IE 11 / Win 10 R | EC 256 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| Edge 15 / Win 10 R | EC 256 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS |
| Edge 16 / Win 10 R | EC 256 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS |
| Edge 18 / Win 10 R | EC 256 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS |
| Edge 13 / Win Phone 10 R | EC 256 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| Java 8u161 | EC 256 (SHA384) | 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 (SHA384) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| OpenSSL 1.0.2s R | EC 256 (SHA384) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| OpenSSL 1.1.0k R | EC 256 (SHA384) | 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 | EC 256 (SHA384) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS |
| Safari 7 / iOS 7.1 R | EC 256 (SHA384) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS |
| Safari 7 / OS X 10.9 R | EC 256 (SHA384) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS |
| Safari 8 / iOS 8.4 R | EC 256 (SHA384) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS |
| Safari 8 / OS X 10.10 R | EC 256 (SHA384) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS |
| Safari 9 / iOS 9 R | EC 256 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| Safari 9 / OS X 10.11 R | EC 256 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| Safari 10 / iOS 10 R | EC 256 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| Safari 10 / OS X 10.12 R | EC 256 (SHA384) | TLS 1.2 > http/1.1 | 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_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 | EC 256 (SHA384) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| Yahoo Slurp Jan 2015 | EC 256 (SHA384) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |
| YandexBot Jan 2015 | EC 256 (SHA384) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS |

**# Not simulated clients (Protocol mismatch)** ⊞

Click here to expand

### Handshake Simulation

(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 : `0xc023` |
| **GOLDENDOODLE** | No (more info) TLS 1.2 : `0xc023` |
| **OpenSSL 0-Length** | No (more info) TLS 1.2 : `0xc023` |
| **Sleeping POODLE** | No (more info) TLS 1.2 : `0xc023` |
| **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 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, 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://wp.98-89-111-197.sslip.io/** (HTTP/1.1 200 OK)

### Miscellaneous

| | |
|---|---|
| **Test date** | Wed, 19 Nov 2025 22:34:06 UTC |
| **Test duration** | 49.801 seconds |
| **HTTP status code** | 200 |
| **HTTP server signature** | Apache |
| **Server hostname** | ec2-98-89-111-197.compute-1.amazonaws.com |

SSL Report v2.4.1