Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > facebook.com > 157.240.18.35

SSL Report: facebook.com (157.240.18.35)

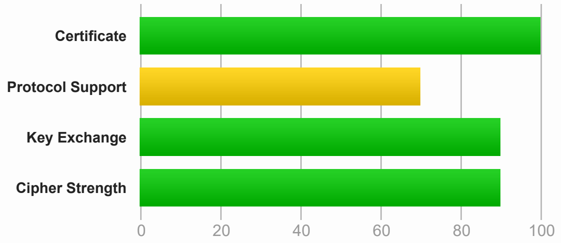
Assessed on: Fri, 22 Oct 2021 18:55:22 UTC | **HIDDEN** | Clear cache

Scan Another »

Summary

Overall Rating

B



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

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »

This server supports TLS 1.3.

Static Public Key Pinning observed for this server.

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

Certificate #1: EC 256 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	*.facebook.com Fingerprint SHA256: c414efebd7cc6d4b56b5426bb965137b5daa7bc8bb883c8e8d0896cf0ae9a296 Pin SHA256: Zg5PZHJ1Uzf4Fyu83RUQgRZTDqjEMZPND2AkFr7gJAM=
Common names	*.facebook.com
Alternative names	*.facebook.com *.facebook.net *.fbcdn.net *.fbsbx.com *.m.facebook.com *.messenger.com *.xx.fbcdn.net *.xy.fbcdn.net *.xz.fbcdn.net facebook.com messenger.com
Serial Number	0a1918a1c0b48d5990713dc42e32121a
Valid from	Sat, 31 Jul 2021 00:00:00 UTC
Valid until	Fri, 29 Oct 2021 23:59:59 UTC (expires in 7 days, 4 hours)
Key	EC 256 bits
Weak key (Debian)	No
Issuer	DigiCert SHA2 High Assurance Server CA AIA: http://cacerts.digicert.com/DigiCertSHA2HighAssuranceServerCA.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	**Yes (certificate)**
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl3.digicert.com/sha2-ha-server-g6.crl OCSP: http://ocsp.digicert.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)

Server Key and Certificate #1

Trusted	Yes Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	2 (2891 bytes)
Chain issues	None

#2

Subject	DigiCert SHA2 High Assurance Server CA Fingerprint SHA256: 19400be5b7a31fb733917700789d2f0a2471c0c9d506c0e504c06c16d7cb17c0 Pin SHA256: k2v657xBsOVe1PQRwOsHsw3bsGT2VzIqz5K+59sNQws=
Valid until	Sun, 22 Oct 2028 12:00:00 UTC (expires in 6 years and 11 months)
Key	RSA 2048 bits (e 65537)
Issuer	DigiCert High Assurance EV Root CA
Signature algorithm	SHA256withRSA

Certification Paths

Click here to expand

Certificate #2: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	*.facebook.com Fingerprint SHA256: 580e20be56a312e4157146bd4e9f85722470ea622463c64fafb3f37eda02a1ca Pin SHA256: 6vu4Ri38qsvDAylBi5+x72NPNmYJ9F2cTfAt4DdbFig=
Common names	*.facebook.com
Alternative names	*.facebook.com *.facebook.net *.fbcdn.net *.fbsbx.com *.m.facebook.com *.messenger.com *.xx.fbcdn.net *.xy.fbcdn.net *.xz.fbcdn.net facebook.com messenger.com
Serial Number	0f2b21f84c512c3f8f10e887eea7f573
Valid from	Sat, 31 Jul 2021 00:00:00 UTC
Valid until	Fri, 29 Oct 2021 23:59:59 UTC (expires in 7 days, 4 hours)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	DigiCert SHA2 High Assurance Server CA AIA: http://cacerts.digicert.com/DigiCertSHA2HighAssuranceServerCA.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl3.digicert.com/sha2-ha-server-g6.crl OCSP: 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	2 (3096 bytes)
Chain issues	None

#2

Additional Certificates (if supplied)

Subject	DigiCert SHA2 High Assurance Server CA Fingerprint SHA256: 19400be5b7a31fb733917700789d2f0a2471c0c9d506c0e504c06c16d7cb17c0 Pin SHA256: k2v657xBsOVe1PQRwOsHsw3bsGT2VzIqz5K+59sNQws=
Valid until	Sun, 22 Oct 2028 12:00:00 UTC (expires in 6 years and 11 months)
Key	RSA 2048 bits (e 65537)
Issuer	DigiCert High Assurance EV Root CA
Signature algorithm	SHA256withRSA

Certification Paths ⊞

Click here to expand

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_CHACHA20_POLY1305_SHA256 (0x1303) ECDH x25519 (eq. 3072 bits RSA) FS	256^{P}
TLS_AES_256_GCM_SHA384 (0x1302) ECDH x25519 (eq. 3072 bits RSA) FS	256

# TLS 1.2 (suites in server-preferred order) ⊟

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) 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_SHA (0x2f) **WEAK**	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK**	256
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**	112
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**	112
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) **WEAK**	112

# 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	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 4.1.1	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 4.2.2	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 4.3	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 4.4.2	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 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_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 8.0	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 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
Baidu Jan 2015	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
BingPreview Jan 2015	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 69 / Win 7 R	Protocol or cipher suite mismatch 0x7f1c | TLS_AES_128_GCM_SHA256		
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	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_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 49 / XP SP3	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 62 / Win 7 R	Protocol or cipher suite mismatch 0x7f1c | TLS_AES_128_GCM_SHA256		
Firefox 73 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS
Googlebot Feb 2018	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
IE 7 / Vista	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
IE 8 / XP No FS [1] No SNI [2]	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA
IE 8-10 / Win 7 R	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
IE 11 / Win 7 R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
IE 11 / Win 8.1 R	EC 256 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
IE 10 / Win Phone 8.0	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
IE 11 / Win Phone 8.1 R	EC 256 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 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_128_GCM_SHA256 ECDH secp256r1 FS
IE 11 / Win 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 15 / Win 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 16 / Win 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 18 / Win 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 13 / Win Phone 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_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	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Java 8u161	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_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
OpenSSL 0.9.8y	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
OpenSSL 1.0.1l R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 1.0.2s R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 1.1.0k R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 1.1.1c R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Safari 5.1.9 / OS X 10.6.8	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS

Handshake Simulation

Safari 6 / iOS 6.0.1	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 6.0.4 / OS X 10.8.4 R	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 7 / iOS 7.1 R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 7 / OS X 10.9 R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 8 / iOS 8.4 R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 8 / OS X 10.10 R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 9 / iOS 9 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 10 / iOS 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 10 / OS X 10.12 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 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_128_GCM_SHA256 ECDH secp256r1 FS
Yahoo Slurp Jan 2015	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
YandexBot Jan 2015	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_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

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	Not mitigated server-side (more info) TLS 1.0: 0xc009
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info) TLS 1.2 : 0xc009
GOLDENDOODLE	No (more info) TLS 1.2 : 0xc009
OpenSSL 0-Length	No (more info) TLS 1.2 : 0xc009
Sleeping POODLE	No (more info) TLS 1.2 : 0xc009
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	With modern browsers (more info)
ALPN	Yes h2 h2-fb http/1.1
NPN	No

Protocol Details

Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	**Yes** max-age=15552000; includeSubDomains
HSTS Preloading	**Chrome Edge Firefox IE**
Public Key Pinning (HPKP)	No (more info)
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	**Yes** includeSubDomains: true pin-sha256: gMxWOrX4PMQesK9qFNbYBxjBfjUvlkn/vN1n+L9lE5E= pin-sha256: PZXN3lRAy+8tBKk2Ox6F7jIlnzr2Yzmwqc3JnyfXoCw= pin-sha256: WoiWRyIOVNa9ihaBciRSC7XHjliYS9VwUGOIud4PB18= pin-sha256: q4PO2G2cbkZhZ82+JgmRUyGMoAeozA+BSXVXQWB8XWQ=
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	secp256r1
SSL 2 handshake compatibility	Yes
0-RTT enabled	No

HTTP Requests

⊞

1 **https://facebook.com/** (HTTP/1.1 302 Found)

Miscellaneous

Test date	Fri, 22 Oct 2021 18:51:16 UTC
Test duration	123.912 seconds
HTTP status code	302
HTTP forwarding	https://m.facebook.com
HTTP server signature	-
Server hostname	edge-star-mini-shv-02-ort2.facebook.com

SSL Report v2.1.8

Terms and Conditions