Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

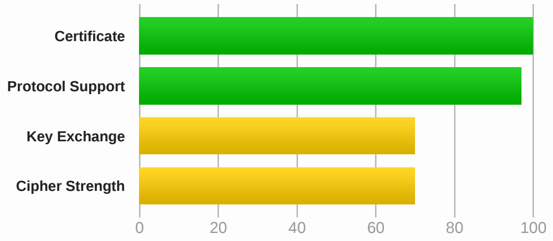
You are here: Home > Projects > SSL Server Test > www.fedex.com > 2600:1406:1a:386:0:0:0:2070

SSL Report: www.fedex.com (2600:1406:1a:386:0:0:0:2070)

Summary

Overall Rating

B



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

This server accepts RC4 cipher, but only with older protocols. Grade capped to B. MORE INFO »

This server does not support Forward Secrecy with the reference browsers. Grade capped to B. MORE INFO »

This server does not support Authenticated encryption (AEAD) cipher suites. Grade capped to B. MORE INFO »

Renegotiation test has been disabled temporarily due to an Apache httpd 2.4.37 bug. MORE INFO »

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	www.fedex.com Fingerprint SHA256: 3aaccdae3b6276c42a14c9481768abaad23e5439c6e1ab223f49109151656987 Pin SHA256: LuJl4DLEfXcyqmgBQdkBX1bY02KKCnEdeLPDc18dFNU=
Common names	www.fedex.com
Alternative names	www.fedex.com fedex.com brandtest.fedex.com api.fedex.com wwwtest.fedex.com m.fedex.com images.fedex.com
Serial Number	078795e6669c2fedcddc2d1a2c1d7dcf
Valid from	Tue, 07 Aug 2018 00:00:00 UTC
Valid until	Wed, 06 Nov 2019 12:00:00 UTC (expires in 8 months and 13 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	GeoTrust RSA CA 2018 AIA: http://cacerts.geotrust.com/GeoTrustRSACA2018.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	**Yes (certificate)**
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://cdp.geotrust.com/GeoTrustRSACA2018.crl OCSP: http://status.geotrust.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 (2816 bytes)
Chain issues	None

#2

Subject	GeoTrust RSA CA 2018 Fingerprint SHA256: 8cc34e11c167045824ade61c4907a6440edb2c4398e99c112a859d661f8e2bc7 Pin SHA256: zUIraRNo+4JoAYA7ROeWjARtIoN4rIEbCpfCRQT6N6A=
Valid until	Sat, 06 Nov 2027 12:23:45 UTC (expires in 8 years and 8 months)
Key	RSA 2048 bits (e 65537)
Issuer	DigiCert Global Root CA
Signature algorithm	SHA256withRSA

Certification Paths

Click here to expand

Configuration

Protocols

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

For TLS 1.3 tests, we only support RFC 8446.

Cipher Suites

# TLS 1.2 (suites in server-preferred order)

TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) **WEAK**	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK**	256
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) **WEAK**	112
TLS_RSA_WITH_RC4_128_MD5 (0x4) **INSECURE**	128
TLS_RSA_WITH_RC4_128_SHA (0x5) **INSECURE**	128

# TLS 1.1 (suites in server-preferred order)

Handshake Simulation

Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Android 6.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA No FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Chrome 69 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Chrome 70 / Win 10	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA No FS

Firefox 62 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Googlebot Feb 2018	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Java 8u161	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
OpenSSL 1.0.1l R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
OpenSSL 1.0.2e R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Safari 8 / OS X 10.10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Apple ATS 9 / iOS 9 R	Server sent fatal alert: handshake_failure			
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No 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
BEAST attack	Mitigated server-side (more info)
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	**Yes, TLS_FALLBACK_SCSV supported** (more info)
SSL/TLS compression	No
RC4	**Yes INSECURE** (more info)
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	**No WEAK** (more info)
ALPN	Yes http/1.1
NPN	Yes http/1.1 http/1.0
Session resumption (caching)	Yes

Session resumption (tickets)	Yes
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, ECDHE suites not supported
Supported Named Groups	-
SSL 2 handshake compatibility	Yes

HTTP Requests

1 **https://www.fedex.com/** (HTTP/1.1 301 Moved Permanently)

2 **https://www.fedex.com/global/choose-location.html** (HTTP/1.1 200 OK)

Miscellaneous

Test date	Sat, 23 Feb 2019 21:56:44 UTC
Test duration	67.245 seconds
HTTP status code	200
HTTP server signature	Apache/2.2
Server hostname	g2600-1406-001a-0386-0000-0000-0000-2070.deploy.static.akamaitechnologies.com

SSL Report v1.32.16