SSL Report: ofxs.ameritrade.com (198.200.171.142)

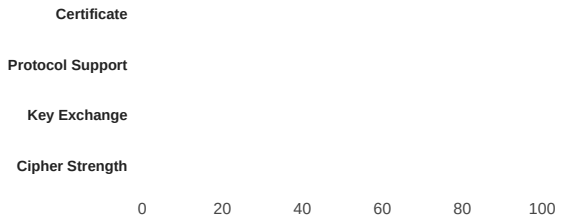
Assessed on: Thu, 14 Apr 2022 20:02:17 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

B



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

There is no support for secure renegotiation. MORE INFO »

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

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

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	*.ameritrade.com Fingerprint SHA256: d80d2a6be5a44f67851bb8f6f4499998e9dc206f0e249aea8dee4f5f9aaf66a6 Pin SHA256: 8ODlLtnsZnAvpmi6x7IGyHsIqzb02CRbVHQhWjARQ4A=
Common names	*.ameritrade.com
Alternative names	*.ameritrade.com ameritrade.com
Serial Number	038ec0b6f1785a3cb5402028d82181be
Valid from	Tue, 29 Mar 2022 00:00:00 UTC
Valid until	Tue, 25 Apr 2023 23:59:59 UTC (expires in 1 year)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	DigiCert TLS RSA SHA256 2020 CA1 AIA: http://cacerts.digicert.com/DigiCertTLSRSASHA2562020CA1-1.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl3.digicert.com/DigiCertTLSRSASHA2562020CA1-4.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 (2999 bytes)
Chain issues	None

#2

Subject	DigiCert TLS RSA SHA256 2020 CA1 Fingerprint SHA256: 25768713d3b459f9382d2a594f85f34709fd2a8930731542a4146ffb246bec69 Pin SHA256: RQeZkB42znUfsDIIFWIRiYEcKl7nHwNFwWCrnMMJbVc=
Valid until	Mon, 23 Sep 2030 23:59:59 UTC (expires in 8 years and 5 months)
Key	RSA 2048 bits (e 65537)
Issuer	DigiCert Global Root CA
Signature algorithm	SHA256withRSA

Certification Paths

Mozilla Apple Android Java Windows

Path #1: Trusted

1	Sent by server	*.ameritrade.com Fingerprint SHA256: d80d2a6be5a44f67851bb8f6f4499998e9dc206f0e249aea8dee4f5f9aaf66a6 Pin SHA256: 8ODlLtnsZnAvpmi6x7IGyHsIqzb02CRbVHQhWjARQ4A= RSA 2048 bits (e 65537) / SHA256withRSA
2	Sent by server	DigiCert TLS RSA SHA256 2020 CA1 Fingerprint SHA256: 25768713d3b459f9382d2a594f85f34709fd2a8930731542a4146ffb246bec69 Pin SHA256: RQeZkB42znUfsDIIFWIRiYEcKl7nHwNFwWCrnMMJbVc= RSA 2048 bits (e 65537) / SHA256withRSA
3	In trust store	DigiCert Global Root CA Self-signed Fingerprint SHA256: 4348a0e9444c78cb265e058d5e8944b4d84f9662bd26db257f8934a443c70161 Pin SHA256: r/mIkG3eEpVdm+u/ko/cwxzOMo1bk4TyHIlByibiA5E= RSA 2048 bits (e 65537) / SHA1withRSA Weak or insecure signature, but no impact on root certificate

Configuration

Protocols

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

Cipher Suites

TLS 1.2 (suites in server-preferred order)

TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) **WEAK**		256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) **WEAK**		128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	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

Handshake Simulation

Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384 No FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS

Handshake Simulation

Android 6.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_GCM_SHA256	No FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
Android 8.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
Android 8.1	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
Android 9.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_GCM_SHA256	No FS
Chrome 69 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
Chrome 70 / Win 10	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
Chrome 80 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_GCM_SHA384	No 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_256_GCM_SHA384	ECDH secp256r1 FS
Firefox 62 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Firefox 73 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Googlebot Feb 2018	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
IE 11 / Win Phone 8.1 R	Server sent fatal alert: handshake_failure			
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
Edge 16 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
Edge 18 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
Java 8u161	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
Java 11.0.3	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
Java 12.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
OpenSSL 1.0.1l R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
OpenSSL 1.0.2s R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
OpenSSL 1.1.0k R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
OpenSSL 1.1.1c R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
Safari 6 / iOS 6.0.1	Server sent fatal alert: handshake_failure			
Safari 7 / iOS 7.1 R	Server sent fatal alert: handshake_failure			
Safari 7 / OS X 10.9 R	Server sent fatal alert: handshake_failure			
Safari 8 / iOS 8.4 R	Server sent fatal alert: handshake_failure			
Safari 8 / OS X 10.10 R	Server sent fatal alert: handshake_failure			
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
Safari 12.1.2 / MacOS 10.14.6 Beta R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
Safari 12.1.1 / iOS 12.3.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
Apple ATS 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS

Not simulated clients (Protocol mismatch)

Android 2.3.7 No SNI [2]	Protocol mismatch (not simulated)
Android 4.0.4	Protocol mismatch (not simulated)
Android 4.1.1	Protocol mismatch (not simulated)

Handshake Simulation

Android 4.2.2	Protocol mismatch (not simulated)
Android 4.3	Protocol mismatch (not simulated)
Baidu Jan 2015	Protocol mismatch (not simulated)
IE 6 / XP No FS [1] No SNI [2]	Protocol mismatch (not simulated)
IE 7 / Vista	Protocol mismatch (not simulated)
IE 8 / XP No FS [1] No SNI [2]	Protocol mismatch (not simulated)
IE 8-10 / Win 7 R	Protocol mismatch (not simulated)
IE 10 / Win Phone 8.0	Protocol mismatch (not simulated)
Java 6u45 No SNI [2]	Protocol mismatch (not simulated)
Java 7u25	Protocol mismatch (not simulated)
OpenSSL 0.9.8y	Protocol mismatch (not simulated)
Safari 5.1.9 / OS X 10.6.8	Protocol mismatch (not simulated)
Safari 6.0.4 / OS X 10.8.4 R	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	**Not supported ACTION NEEDED** (more info)
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)
GOLDENDOODLE	No (more info)
OpenSSL 0-Length	No (more info)
Sleeping POODLE	No (more info)
Downgrade attack prevention	Unknown (requires support for at least two protocols, excl. SSL2)
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 some browsers** (more info)
ALPN	Yes http/1.1
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	No
OCSP stapling	No
Strict Transport Security (HSTS)	**Yes** max-age=31536000
HSTS Preloading	**Not in: Chrome Edge Firefox IE**

Protocol Details

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	TLS 1.152 TLS 2.152
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, secp384r1, secp224r1, secp521r1 (server preferred order)
SSL 2 handshake compatibility	No

HTTP Requests

1 **https://ofxs.ameritrade.com/** (HTTP/1.1 404 Not Found)

1	**Date**	Thu, 14 Apr 2022 20:01:01 GMT
	Server	Apache
	Content-Length	317
	Keep-Alive	timeout=15
	Connection	Keep-Alive
	Content-Type	text/html; charset=iso-8859-1
	Set-Cookie	NSC_UY-DGF-pgyt.bnfsjusbef.dpn-443=30dfa3db0a40eef92dde9ac5a006fdc40689af2a2596a8434a51acbe2dc70e9f36a340b1;path=/;secure;httponly
	Strict-Transport-Security	max-age=31536000

Miscellaneous

Test date	Thu, 14 Apr 2022 20:00:50 UTC
Test duration	87.17 seconds
HTTP status code	404
HTTP server signature	Apache
Server hostname	ofxs-tx.ameritrade.com

SSL Report v2.1.10