

Qualys[®] SSL Labs

[Home](#)[Projects](#)[Qualys Free Trial](#)[Contact](#)

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

SSL Report: ssloffload.cntestwebsite.com (3.109.113.40)

Assessed on: Fri, 25 Feb 2022 08:55:03 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating

T

If trust issues are ignored: C

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's certificate is not trusted, see [below](#) for details.

This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. [MORE INFO »](#)


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 »](#)

This server's certificate chain is incomplete. Grade capped to B.

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

Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1

Subject	*.citrixns.com Fingerprint SHA256: a5d338e8b3e1ec203ce53aa69327f8b6aa42588e244600ab51dbddd160551a48 Pin SHA256: j2W6MqiN65r4KFU0NJimr3ErZqFIR30PfiNrcCe5iys=
Common names	*.citrixns.com
Alternative names	*.citrixns.com MISMATCH
Serial Number	0dbf9caff78937de0bc44d74bcc4e7c2
Valid from	Mon, 13 Sep 2021 00:00:00 UTC
Valid until	Tue, 13 Sep 2022 23:59:59 UTC (expires in 6 months and 19 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	DigiCert TLS RSA SHA256 2020 CA1 AIA: http://cacerts.digicert.com/DigiCertTLRSASHA2562020CA1-1.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl3.digicert.com/DigiCertTLRSASHA2562020CA1-3.crl OCSP: http://ocsp.digicert.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	No NOT TRUSTED (Why?) Mozilla Apple Android Java Windows

https://www.ssllabs.com/ssltest/analyze.html?d=ssloffload.cntestwebsite.com

1/5



Additional Certificates (if supplied)

Certificates provided	1 (1731 bytes)
Chain issues	Incomplete



Certification Paths

Mozilla Apple Android Java Windows

Path #1: Not trusted (invalid certificate [Fingerprint SHA256: a5d338e8b3e1ec203ce53aa69327f8b6aa42588e244600ab51dbddd160551a48])

1	Sent by server	*.citrixns.com Fingerprint SHA256: a5d338e8b3e1ec203ce53aa69327f8b6aa42588e244600ab51dbddd160551a48 Pin SHA256: j2W6MqiN65r4KFU0NJimr3ErZqFIR30PfiNrcCe5iys= RSA 2048 bits (e 65537) / SHA256withRSA
2	Extra download	DigiCert TLS RSA SHA256 2020 CA1 Fingerprint SHA256: 52274c57ce4dee3b49db7a7ff708c040f771898b3be88725a86fb4430182fe14 Pin SHA256: RQeZkB42znUfsDIIFWIRIYEckI7nHwNFwWCmMMJbVc= RSA 2048 bits (e 65537) / SHA256withRSA
3	In trust store	DigiCert Global Root CA Self-signed Fingerprint SHA256: 4348a0e9444c78cb265e058d5e8944b4d84f9662bd26db257f8934a443c70161 Pin SHA256: r/mlkG3eEpVdm+u/ko/cwxzOMo1bk4TyHIIByibiA5E= 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	Yes
TLS 1.0	Yes
SSL 3 INSECURE	Yes
SSL 2	No



Cipher Suites

# TLS 1.2 (suites in server-preferred order)			
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	WEAK		256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	WEAK		128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	WEAK		256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	WEAK		128
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_CBC_SHA (0xc014)	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_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA) FS	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
# TLS 1.1 (suites in server-preferred order)			
# TLS 1.0 (suites in server-preferred order)			
# SSL 3 (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
---------------	---------------------	-------------------	---------	------------------------------	-------

Handshake Simulation

Android 4.0.4	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 4.1.1	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 4.2.2	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 4.3	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 6.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 8.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 8.1	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 9.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Baidu Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Chrome 69 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Chrome 70 / Win 10	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Chrome 80 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Firefox 62 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Firefox 73 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Googlebot Feb 2018	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
IE 6 / XP No FS ¹ No SNI ²	Server sent fatal alert: handshake_failure		
IE 7 / Vista	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No 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_RSA_WITH_AES_256_CBC_SHA No FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
IE 10 / Win Phone 8.0	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_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_256_CBC_SHA No FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Edge 16 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Edge 18 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No 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_RSA_WITH_AES_128_CBC_SHA No FS
Java 8u161	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Java 11.0.3	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Java 12.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
OpenSSL 0.9.8y	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
OpenSSL 1.0.1l R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
OpenSSL 1.0.2s R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
OpenSSL 1.1.0k R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
OpenSSL 1.1.1c R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 5.1.9 / OS X 10.6.8	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 6.0.4 / OS X 10.8.4 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 8 / OS X 10.10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS

Handshake Simulation

Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA 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_CBC_SHA 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_CBC_SHA No FS
Apple ATS 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS

- (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

	No, server keys and hostname not seen elsewhere with SSLv2	
DROWN	(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	Not mitigated server-side (more info) SSL 3: 0x35, TLS 1.0: 0x35	
POODLE (SSLv3)	Vulnerable INSECURE (more info) SSL 3: 0x35	
POODLE (TLS)	No (more info)	
Zombie POODLE	No (more info) TLS 1.2: 0x0035	
GOLDENDOODLE	No (more info) TLS 1.2: 0x0035	
OpenSSL 0-Length	No (more info) TLS 1.2: 0x0035	
Sleeping POODLE	No (more info) TLS 1.2: 0x0035	
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 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)	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	TLS 1.152 TLS 2.152	
Incorrect SNI alerts	No	
Uses common DH primes	No, DHE suites not supported	

Protocol Details

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	Yes



HTTP Requests



1 https://sslload.cntestwebsite.com/ (HTTP/1.1 200 OK)



Miscellaneous

Test date	Fri, 25 Feb 2022 08:51:34 UTC
Test duration	208.713 seconds
HTTP status code	200
HTTP server signature	Apache/2.4.41 (Ubuntu)
Server hostname	ec2-3-109-113-40.ap-south-1.compute.amazonaws.com

Why is my certificate not trusted?

There are many reasons why a certificate may not be trusted. The exact problem is indicated on the report card in bright red. The problems fall into three categories:

- 1. Invalid certificate
- 2. Invalid configuration
- 3. Unknown Certificate Authority

1. Invalid certificate

A certificate is invalid if:

- It is used before its activation date
- It is used after its expiry date
- Certificate hostnames don't match the site hostname
- It has been revoked
- It has insecure signature
- It has been blacklisted

2. Invalid configuration

In some cases, the certificate chain does not contain all the necessary certificates to connect the web server certificate to one of the root certificates in our trust store. Less commonly, one of the certificates in the chain (other than the web server certificate) will have expired, and that invalidates the entire chain.

3. Unknown Certificate Authority

In order for trust to be established, we must have the root certificate of the signing Certificate Authority in our trust store. SSL Labs does not maintain its own trust store; instead we use the store maintained by Mozilla.

If we mark a web site as not trusted, that means that the average web user's browser will not trust it either. For certain special groups of users, such web sites can still be secure. For example, if you can securely verify that a self-signed web site is operated by a person you trust, then you can trust that self-signed web site too. Or, if you work for an organisation that manages its own trust, and you have their own root certificate already embedded in your browser. Such special cases do not work for the general public, however, and this is what we indicate on our report card.

4. Interoperability issues

In some rare cases trust cannot be established because of interoperability issues between our code and the code or configuration running on the server. We manually review such cases, but if you encounter such an issue please feel free to contact us. Such problems are very difficult to troubleshoot and you may be able to provide us with information that might help us determine the root cause.

SSL Report v2.1.10