

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > dashboard.stage.wholetale.org

# SSL Report: dashboard.stage.wholetale.org (149.165.168.151)

Assessed on: Tue, 19 Jun 2018 17:01:24 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

## Summary

Overall Rating

# A

Certificate

Protocol Support

Key Exchange

Cipher Strength

0 20 40 60 80 100

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This site works only in browsers with SNI support.

DNS Certification Authority Authorization (CAA) Policy found for this domain. [MORE INFO »](#)

## Certificate #1: RSA 4096 bits (SHA256withRSA)



### Server Key and Certificate #1

<b>Subject</b>	*.stage.wholetale.org Fingerprint SHA256: 6efdde14892c188bbf841c7a46ad8717f26dde1e72a265494c7b0d6f6a02b1e9 Pin SHA256: QerBlh9zi4NLNzIEQfGXdSchbhWhFuQhyfmewl1CHiA=
<b>Common names</b>	*.stage.wholetale.org
<b>Alternative names</b>	*.stage.wholetale.org
<b>Serial Number</b>	032d41b6833db6fd16332a92743ba3c16d15
<b>Valid from</b>	Fri, 08 Jun 2018 21:01:42 UTC
<b>Valid until</b>	Thu, 06 Sep 2018 21:01:42 UTC (expires in 2 months and 18 days)
<b>Key</b>	RSA 4096 bits (e 65537)
<b>Weak key (Debian)</b>	No
<b>Issuer</b>	Let's Encrypt Authority X3 AIA: <a href="http://cert.int-x3.letsencrypt.org/">http://cert.int-x3.letsencrypt.org/</a>
<b>Signature algorithm</b>	SHA256withRSA
<b>Extended Validation</b>	No
<b>Certificate Transparency</b>	Yes (certificate)
<b>OCSP Must Staple</b>	No
<b>Revocation information</b>	OCSP OCSP: <a href="http://ocsp.int-x3.letsencrypt.org">http://ocsp.int-x3.letsencrypt.org</a>
<b>Revocation status</b>	Good (not revoked)
<b>DNS CAA</b>	Yes policy host: wholetale.org issue: letsencrypt.org flags:0 issuewild: letsencrypt.org flags:0
<b>Trusted</b>	Yes Mozilla Apple Android Java Windows

**Additional Certificates (if supplied)**

Certificates provided	2 (2992 bytes)
Chain issues	None

## #2

Subject	Let's Encrypt Authority X3 Fingerprint SHA256: 25847d668eb4f04fdd40b12b6b0740c567da7d024308eb6c2c96fe41d9de218d Pin SHA256: YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg=
Valid until	Wed, 17 Mar 2021 16:40:46 UTC (expires in 2 years and 8 months)
Key	RSA 2048 bits (e 65537)
Issuer	DST Root CA X3
Signature algorithm	SHA256withRSA

**Certification Paths**[Click here to expand](#)**Certificate #2: RSA 2048 bits (SHA256withRSA) No SNI**[Click here to expand](#)**Configuration****Protocols**

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

For TLS 1.3 tests, we currently support draft version 23.

**Cipher Suites**

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



TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0ca8)	ECDH x25519 (eq. 3072 bits RSA) FS	256

**Handshake Simulation**

<a href="#">Android 4.4.2</a>	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Android 5.0.0</a>	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Android 6.0</a>	RSA 4096 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Android 7.0</a>	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519	FS
<a href="#">BingPreview Jan 2015</a>	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Chrome 49 / XP SP3</a>	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Chrome 65 / Win 7 R</a>	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519	FS

Handshake Simulation

<a href="#">Firefox 31.3.0 ESR / Win 7</a>	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Firefox 47 / Win 7</a> R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Firefox 49 / XP SP3</a>	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Firefox 59 / Win 7</a> R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519	FS
<a href="#">Googlebot Feb 2018</a>	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519	FS
<a href="#">IE 11 / Win 7</a> R	Server sent fatal alert: handshake_failure				
<a href="#">IE 11 / Win 8.1</a> R	Server sent fatal alert: handshake_failure				
<a href="#">IE 11 / Win Phone 8.1</a> R	Server sent fatal alert: handshake_failure				
<a href="#">IE 11 / Win Phone 8.1 Update</a> R	Server sent fatal alert: handshake_failure				
<a href="#">IE 11 / Win 10</a> R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Edge 15 / Win 10</a> R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519	FS
<a href="#">Edge 13 / Win Phone 10</a> R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Java 8u161</a>	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">OpenSSL 1.0.1l</a> R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">OpenSSL 1.0.2e</a> R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Safari 6 / iOS 6.0.1</a>	Server sent fatal alert: handshake_failure				
<a href="#">Safari 7 / iOS 7.1</a> R	Server sent fatal alert: handshake_failure				
<a href="#">Safari 7 / OS X 10.9</a> R	Server sent fatal alert: handshake_failure				
<a href="#">Safari 8 / iOS 8.4</a> R	Server sent fatal alert: handshake_failure				
<a href="#">Safari 8 / OS X 10.10</a> R	Server sent fatal alert: handshake_failure				
<a href="#">Safari 9 / iOS 9</a> R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Safari 9 / OS X 10.11</a> R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Safari 10 / iOS 10</a> R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Safari 10 / OS X 10.12</a> R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Apple ATS 9 / iOS 9</a> R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Yahoo Slurp Jan 2015</a>	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">YandexBot Jan 2015</a>	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	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 <a href="#">this longer explanation</a> (2) Key usage data kindly provided by the <a href="#">Censys</a> network search engine; original DROWN website <a href="#">here</a> (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	Mitigated server-side ( <a href="#">more info</a> )
POODLE (SSLv3)	No, SSL 3 not supported ( <a href="#">more info</a> )
POODLE (TLS)	No ( <a href="#">more info</a> )
Downgrade attack prevention	Unknown (requires support for at least two protocols, excl. SSL2)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No

### Protocol Details

Heartbleed (vulnerability)	No ( <a href="#">more info</a> )
Ticketbleed (vulnerability)	No ( <a href="#">more info</a> )
OpenSSL CCS vuln. (CVE-2014-0224)	No ( <a href="#">more info</a> )
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No ( <a href="#">more info</a> )
ROBOT (vulnerability)	No ( <a href="#">more info</a> )
<b>Forward Secrecy</b>	<b>Yes (with most browsers) ROBUST</b> ( <a href="#">more info</a> )
ALPN	Yes h2 http/1.1
NPN	Yes h2 http/1.1
<b>Session resumption (caching)</b>	<b>No (IDs empty)</b>
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	<b>Not in: Chrome Edge Firefox IE</b>
Public Key Pinning (HPKP)	No ( <a href="#">more info</a> )
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No ( <a href="#">more info</a> )
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, secp384r1, secp521r1 (server preferred order)
SSL 2 handshake compatibility	No



### HTTP Requests



1 <https://dashboard.stage.wholetale.org/> (HTTP/1.1 200 OK)



### Miscellaneous

Test date	Tue, 19 Jun 2018 17:00:50 UTC
Test duration	34.366 seconds
HTTP status code	200
HTTP server signature	nginx/1.14.0
Server hostname	js-168-151.jetstream-cloud.org

SSL Report v1.32.2

Copyright © 2009-2018 [Qualys, Inc.](#) All Rights Reserved.

[Terms and Conditions](#)

Qualys is the leading provider of integrated [infrastructure security](#), [cloud infrastructure security](#), [endpoint security](#), [devsecops](#), [compliance](#) and [web app security](#) solutions.