

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.vendasta.com](#) > 151.101.129.91

SSL Report: [www.vendasta.com](#) (151.101.129.91)

Assessed on: Sun, 07 Jul 2024 10:18:23 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating

A

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 site works only in browsers with SNI support.

This server supports TLS 1.3.

Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1

Subject	
www.vendasta.com	
Fingerprint SHA256: 9cd94cd1ab246522d977d46c81b05387d4d8ee88e13f1f3d072173251d35a49d	
Pin SHA256: ywJIPLVbCzTz8qEnobflUOuFJRan+beNeYsWIA7oxIA=	
Common names	
www.vendasta.com	
Alternative names	
www.vendasta.com	
Serial Number	
76a07a734d39c5b8fba7a175e0866c62cab3	
Valid from	
Sat, 29 Jun 2024 16:15:15 UTC	
Valid until	
Mon, 29 Jul 2024 16:15:14 UTC (expires in 22 days, 5 hours)	
Key	
RSA 2048 bits (e 65537)	
Weak key (Debian)	
No	
Issuer	
Certainly Intermediate R1	
AIA: http://int-r1.certainly.com	
Signature algorithm	
SHA256withRSA	
Extended Validation	
No	
Certificate Transparency	
Yes (certificate)	
OCSP Must Staple	
No	
Revocation information	
OCSP	
OCSP: http://ocsp.int-r1.certainly.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 (2488 bytes)
-----------------------	----------------

Additional Certificates (if supplied)

Chain issues	None
#2	
Subject	Certainly Intermediate R1 Fingerprint SHA256: fec41e32ca75c295a6240fa639d3abe3bfb5cb131d6690e2331a176bed2e5bd2 Pin SHA256: oW7smChMJRcnzTObF7K+HzInReAPTxB/L1h6eZTmw9Q=
Valid until	Mon, 21 Jun 2032 23:59:59 UTC (expires in 7 years and 11 months)
Key	RSA 2048 bits (e 65537)
Issuer	Starfield Root Certificate Authority - G2
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	Yes
TLS 1.2	Yes*
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

(\*) Experimental: Server negotiated using No-SNI

 [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_AES_256_GCM_SHA384 (0x1302)	ECDH x25519 (eq. 3072 bits RSA) FS		256
TLS_CHACHA20_POLY1305_SHA256 (0x1303)	ECDH x25519 (eq. 3072 bits RSA) FS		256 <sup>P</sup>
# TLS 1.2 (suites in server-preferred order)			
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc030)	ECDH x25519 (eq. 3072 bits RSA) FS		256
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

(P) This server prefers ChaCha20 suites with clients that don't have AES-NI (e.g., Android devices)

 [Handshake Simulation](#)

<a href="#">Android 4.4.2</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Android 5.0.0</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Android 6.0</a>	RSA 2048 (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 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDH x25519 FS

## Handshake Simulation

<a href="#">Android 8.0</a>	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDH x25519	FS
<a href="#">Android 8.1</a>	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519	FS
<a href="#">Android 9.0</a>	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519	FS
<a href="#">BingPreview Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Chrome 49 / XP SP3</a>	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Chrome 69 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519	FS
<a href="#">Chrome 70 / Win 10</a>	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519	FS
<a href="#">Chrome 80 / Win 10</a> R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519	FS
<a href="#">Firefox 31.3.0 ESR / Win 7</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Firefox 47 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Firefox 49 / XP SP3</a>	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Firefox 62 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519	FS
<a href="#">Firefox 73 / Win 10</a> R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519	FS
<a href="#">Googlebot Feb 2018</a>	RSA 2048 (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 2048 (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 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519	FS
<a href="#">Edge 16 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519	FS
<a href="#">Edge 18 / Win 10</a> R	RSA 2048 (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 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Java 8u161</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Java 11.0.3</a>	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Java 12.0.1</a>	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">OpenSSL 1.0.1l</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">OpenSSL 1.0.2s</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">OpenSSL 1.1.0k</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDH x25519	FS
<a href="#">OpenSSL 1.1.1c</a> R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519	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 2048 (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 2048 (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 2048 (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 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Safari 12.1.2 / MacOS 10.14.6 Beta</a> R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH x25519	FS
<a href="#">Safari 12.1.1 / iOS 12.3.1</a> R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH x25519	FS
<a href="#">Apple ATS 9 / iOS 9</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Yahoo Slurp Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">YandexBot Jan 2015</a>	RSA 2048 (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.

Handshake Simulation

(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	
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> )
Zombie POODLE	No ( <a href="#">more info</a> )
GOLDENDOODLE	No ( <a href="#">more info</a> )
OpenSSL 0-Length	No ( <a href="#">more info</a> )
Sleeping POODLE	No ( <a href="#">more info</a> )
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported ( <a href="#">more info</a> )
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
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> )
Forward Secrecy	Yes (with most browsers) ROBUST ( <a href="#">more info</a> )
ALPN	Yes h2 http/1.1
NPN	No
Session resumption (caching)	No (IDs assigned but not accepted)
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 ( <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 (server preferred order)
SSL 2 handshake compatibility	No
0-RTT enabled	Yes



HTTP Requests	
1	<a href="https://www.vendasta.com/">https://www.vendasta.com/</a> (HTTP/1.1 200 OK)



Miscellaneous	
Test date	Sun, 07 Jul 2024 10:12:16 UTC

Miscellaneous

Test duration	90.443 seconds
HTTP status code	200
HTTP server signature	website-pro/8.8.0
Server hostname	-

SSL Report v2.3.0