

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [dashboard.outcomes.com](#) > 52.1.221.21

## SSL Report: [dashboard.outcomes.com](#) (52.1.221.21)

### 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](#).

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

<b>Subject</b>	*.outcomes.com Fingerprint SHA1: 3e0b2cecd60e7d49cf5a985561a6f045b3ddbcaf Pin SHA256: faMyAeJmL2r12hAvTIFxZGJNtcZbwocRCVeAFhJeGVk=
<b>Common names</b>	*.outcomes.com
<b>Alternative names</b>	*.outcomes.com outcomes.com
<b>Valid from</b>	Wed, 01 Jul 2015 01:24:09 UTC
<b>Valid until</b>	Sun, 01 Jul 2018 01:24:09 UTC (expires in 1 year and 3 months)
<b>Key</b>	RSA 2048 bits (e 65537)
<b>Weak key (Debian)</b>	No
<b>Issuer</b>	AlphaSSL CA - SHA256 - G2 AIA: http://secure2.alphassl.com/cacert/gsalphasha2g2r1.crt
<b>Signature algorithm</b>	SHA256withRSA
<b>Extended Validation</b>	No
<b>Certificate Transparency</b>	No
<b>OCSP Must Staple</b>	No
<b>Revocation information</b>	CRL, OCSP CRL: http://crl2.alphassl.com/gsalphasha2g2.crl OCSP: http://ocsp2.globalsign.com/gsalphasha2g2
<b>Revocation status</b>	Good (not revoked)
<b>DNS CAA</b>	No
<b>Trusted</b>	Yes



#### Additional Certificates (if supplied)

<b>Certificates provided</b>	3 (3234 bytes)
<b>Chain issues</b>	Contains anchor
<b>#2</b>	

**Additional Certificates (if supplied)**

<b>Subject</b>	AlphaSSL CA - SHA256 - G2 Fingerprint SHA1: 4c27431717565a3a07f3e6d0032c4258949cf9ec Pin SHA256: amMeV6gb9QNx0ZF7FtJ19Wart2B7KpCF/1n2Js3UuSU=
<b>Valid until</b>	Tue, 20 Feb 2024 10:00:00 UTC (expires in 6 years and 11 months)
<b>Key</b>	RSA 2048 bits (e 65537)
<b>Issuer</b>	GlobalSign Root CA
<b>Signature algorithm</b>	SHA256withRSA

#3

<b>Subject</b>	GlobalSign Root CA <a href="#">In trust store</a> Fingerprint SHA1: b1bc968bd4f49d622aa89a81f2150152a41d829c Pin SHA256: K87oWBWM9UZfydvdvDfoxL+8lpNyoUB2ptGtn0fv6G2Q=
<b>Valid until</b>	Fri, 28 Jan 2028 12:00:00 UTC (expires in 10 years and 10 months)
<b>Key</b>	RSA 2048 bits (e 65537)
<b>Issuer</b>	GlobalSign Root CA Self-signed
<b>Signature algorithm</b>	SHA1withRSA Weak, but no impact on root certificate



**Certification Paths**



[Click here to expand](#)

## Configuration



**Protocols**

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



**Cipher Suites**

# TLS 1.2 (suites in server-preferred order)



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_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)	ECDH secp256r1 (eq. 3072 bits RSA) FS	112
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)		112
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)	DH 2048 bits FS	112

# TLS 1.1 (suites in server-preferred order)



## Cipher Suites

# TLS 1.0 (suites in server-preferred order)



## Handshake Simulation

<a href="#">Android 2.3.7</a> No SNI <sup>2</sup>	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA	No FS
<a href="#">Android 4.0.4</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
<a href="#">Android 4.1.1</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
<a href="#">Android 4.2.2</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
<a href="#">Android 4.3</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
<a href="#">Android 4.4.2</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	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 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
<a href="#">Baidu Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
<a href="#">BingPreview Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
<a href="#">Chrome 49 / XP SP3</a>	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Chrome 51 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 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 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Firefox 49 / XP SP3</a>	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
<a href="#">Firefox 49 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
<a href="#">Googlebot Feb 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">IE 6 / XP</a> No FS <sup>1</sup> No SNI <sup>2</sup>	Server closed connection			
<a href="#">IE 7 / Vista</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
<a href="#">IE 8 / XP</a> No FS <sup>1</sup> No SNI <sup>2</sup>	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA	
<a href="#">IE 8-10 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
<a href="#">IE 11 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
<a href="#">IE 11 / Win 8.1</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
<a href="#">IE 10 / Win Phone 8.0</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
<a href="#">IE 11 / Win Phone 8.1</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
<a href="#">IE 11 / Win Phone 8.1 Update</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
<a href="#">IE 11 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
<a href="#">Edge 13 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
<a href="#">Edge 13 / Win Phone 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
<a href="#">Java 6u45</a> No SNI <sup>2</sup>	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA	No FS
<a href="#">Java 7u25</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 FS
<a href="#">Java 8u31</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">OpenSSL 0.9.8y</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA	No FS
<a href="#">OpenSSL 1.0.1l</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
<a href="#">OpenSSL 1.0.2e</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
<a href="#">Safari 5.1.9 / OS X 10.6.8</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
<a href="#">Safari 6 / iOS 6.0.1</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
<a href="#">Safari 6.0.4 / OS X 10.8.4</a> R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
<a href="#">Safari 7 / iOS 7.1</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
<a href="#">Safari 7 / OS X 10.9</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
<a href="#">Safari 8 / iOS 8.4</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
<a href="#">Safari 8 / OS X 10.10</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
<a href="#">Safari 9 / iOS 9</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
<a href="#">Safari 9 / OS X 10.11</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
<a href="#">Safari 10 / iOS 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
<a href="#">Safari 10 / OS X 10.12</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS

**Handshake Simulation**

<a href="#">Apple ATS 9 / iOS 9</a> <small>R</small>	RSA 2048 (SHA256)	<b>TLS 1.2 &gt; http/1.1</b>	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	<b>FS</b>
<a href="#">Yahoo Slurp Jan 2015</a>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	<b>FS</b>
<a href="#">YandexBot Jan 2015</a>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	<b>FS</b>

- (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).



**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 test [here](#)  
 (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete

<b>Secure Renegotiation</b>	<b>Supported</b>
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side ( <a href="#">more info</a> ) TLS 1.0: 0xc014
POODLE (SSLv3)	No, SSL 3 not supported ( <a href="#">more info</a> )
POODLE (TLS)	No ( <a href="#">more info</a> )
<b>Downgrade attack prevention</b>	<b>Yes, TLS_FALLBACK_SCSV supported</b> ( <a href="#">more info</a> )
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	Yes
Heartbleed (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> )
Forward Secrecy	With modern browsers ( <a href="#">more info</a> )
ALPN	Yes
NPN	Yes http/1.1
<b>Session resumption (caching)</b>	<b>No (IDs assigned but not accepted)</b>
Session resumption (tickets)	Yes
OCSP stapling	No
<b>Strict Transport Security (HSTS)</b>	<b>Yes</b> max-age=31536000
HSTS Preloading	<b>Not in: Chrome Edge Firefox IE</b>
Public Key Pinning (HPKP)	No
Public Key Pinning Report-Only	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No
DH public server param (Ys) reuse	No
ECDH public server param reuse	No
Supported EC Named Curves	secp256r1
SSL 2 handshake compatibility	Yes



**HTTP Requests**

1 <https://dashboard.outcomes.com/> (HTTP/1.1 200 OK)

**Miscellaneous**



<b>Test date</b>	Thu, 02 Mar 2017 18:36:24 UTC
<b>Test duration</b>	82.907 seconds
<b>HTTP status code</b>	200
<b>HTTP server signature</b>	nginx
<b>Server hostname</b>	ec2-52-1-221-21.compute-1.amazonaws.com

SSL Report v1.27.3