QUALYS® SSL LABS

Home Qualys.com Projects Contact

You are here: Home > Projects > SSL Server Test > sentmail.co.uk

SSL Report: sentmail.co.uk (84.234.26.239)

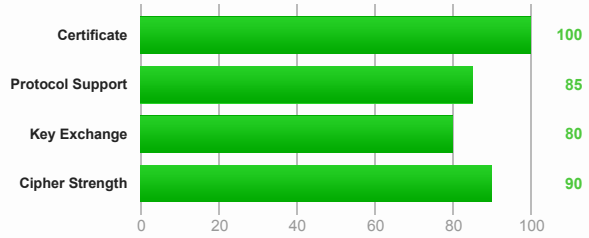
Assessed on: Fri Sep 27 19:24:09 UTC 2013 | Clear cache

Scan Another »

Summary

Overall Rating

A



Documentation: SSL/TLS Deployment Best Practices and SSL Server Rating Guide.

This site supports only older protocol versions, but not the most recent and more secure TLS 1.2.

Authentication

Server Key and Certificate #1

Common names	sentmail.co.uk
Alternative names	sentmail.co.uk www.sentmail.co.uk
Prefix handling	Both (with and without WWW)
Valid from	Thu Aug 15 18:23:31 UTC 2013
Valid until	Sat Aug 15 18:23:31 UTC 2015 (expires in 1 year and 10 months)
Key	RSA 2048 bits
Weak key (Debian)	No
Issuer	Go Daddy Secure Certification Authority
Signature algorithm	SHA1withRSA
Extended Validation	Yes
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	Yes

Additional Certificates (if supplied)

Certificates provided	2 (2726 bytes)
Chain issues	None

#2

Subject	Go Daddy Secure Certification Authority SHA1: 7c4656c3061f7f4c0d67b319a855f60ebc11fc44
Valid until	Mon Nov 16 01:54:37 UTC 2026 (expires in 13 years and 1 month)
Key	RSA 2048 bits
Issuer	The Go Daddy Group / Go Daddy Class 2 Certification Authority
Signature algorithm	SHA1withRSA

Certification Paths

Certification Paths

Path #1: Trusted

1	Sent by server	sentmail.co.uk SHA1: 959bb010077763b510bcb7c39e653181dd1cf68d RSA 2048 bits / SHA1withRSA
2	Sent by server	Go Daddy Secure Certification Authority SHA1: 7c4656c3061f7f4c0d67b319a855f60ebc11fc44 RSA 2048 bits / SHA1withRSA
3	In trust store	The Go Daddy Group / Go Daddy Class 2 Certification Authority SHA1: 2796bae63f1801e277261ba0d77770028f20eee4 RSA 2048 bits / SHA1withRSA

Configuration

Protocols

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

(*) N next to protocol version means the protocol has no cipher suites enabled

Cipher Suites (sorted by strength; the server has no preference)

TLS_RSA_WITH_RC4_128_MD5 (0x4)	128
TLS_RSA_WITH_RC4_128_SHA (0x5)	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	128
TLS_RSA_WITH_SEED_CBC_SHA (0x96)	128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	168
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	168
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	256

Handshake Simulation

Chrome 29 / Win 7	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Firefox 10.0.12 ESR / Win 7	TLS 1.0	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) FS	256
Firefox 17.0.7 ESR / Win 7	TLS 1.0	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) FS	256
Firefox 21 / Fedora 19	TLS 1.0	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) FS	256
Firefox 22 / Win 7	TLS 1.0	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) FS	256
IE 6 / XP No FS *	SSL 3	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS	128
IE 7 / Vista	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
IE 8 / XP No FS *	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS	128
IE 8-10 / Win 7	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
IE 11 / Win 8.1	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Java 6u45	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS	128
Java 7u25	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
OpenSSL 0.9.8y	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
OpenSSL 1.0.1e	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256

Handshake Simulation

Opera 12.15 / Win 7	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Opera 15 / Win 7	TLS 1.0	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) FS	256
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Safari 6 / iOS 6.0.1	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Safari 6.0.4 / OS X 10.8.4	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Safari 7 / OS X 10.9	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128

* Browsers that do not support Forward Secrecy are excluded when determining support for it.

Protocol Details

Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	**Not mitigated server-side** (more info) SSL 3: 0x2f, TLS 1.0: 0x2f
TLS compression	No
RC4	**Yes NOT DESIRABLE** (more info)
Forward Secrecy	**No NOT DESIRABLE** (more info)
Next Protocol Negotiation	No
Session resumption	Yes
Session tickets	Yes
OCSP stapling	No
Strict Transport Security	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	TLS 2.98
SSL 2 handshake compatibility	Yes

Miscellaneous

Test date	Fri Sep 27 19:23:34 UTC 2013
Test duration	35.37 seconds
HTTP status code	200
HTTP server signature	Apache/2.2.24 (Unix)
Server hostname	d2d-ceworx-ns1.helweb.co.uk
PCI compliant	No
FIPS-ready	No

SSL Report v1.6.0