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)

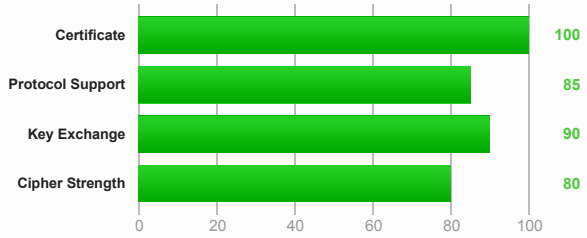
Assessed on: Sat Oct 05 19:30:20 UTC 2013 | Clear cache

Scan Another »

Summary

Overall Rating

A



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

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	No

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

Handshake Simulation

Chrome 30 / Win 7	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS	128
Firefox 10.0.12 ESR / Win 7	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS	128
Firefox 17.0.7 ESR / Win 7	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS	128
Firefox 21 / Fedora 19	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS	128
Firefox 24 / Win 7	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS	128
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_RC4_128_SHA (0x5)	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_RC4_128_SHA (0x5)	No FS	128
IE 11 / Win 8.1				Fail**
Java 6u45	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4)	No FS	128
Java 7u25	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS	128
OpenSSL 0.9.8y	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS	128
OpenSSL 1.0.1e	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS	128
Opera 12.15 / Win 7	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS	128
Opera 16 / Win 7	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS	128
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS	128
Safari 6 / iOS 6.0.1	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS	128
Safari 6.0.4 / OS X 10.8.4	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS	128
Safari 7 / OS X 10.9	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS	128

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

** Only first connection attempt simulated. Browsers are likely to retry with a lower protocol version or other tweaks.

Protocol Details

Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initated Renegotiation	No

Protocol Details

BEAST attack	
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	Sat Oct 05 19:29:46 UTC 2013
Test duration	34.110 seconds
HTTP status code	400
HTTP server signature	Apache/2.2.24 (Unix)
Server hostname	d2d-ceworx-ns1.helweb.co.uk
PCI compliant	Yes
FIPS-ready	No

SSL Report v1.6.7