QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > mailbox.org

SSL Report: mailbox.org (80.241.60.194)

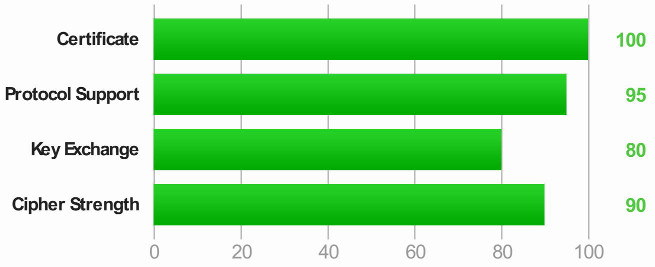
Assessed on: Mon Jun 23 09:42:25 UTC 2014 | Clear cache

Scan Another »

Summary

Overall Rating

A+



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

This server supports HTTP Strict Transport Security with long duration. Grade set to A+. MORE INFO »

This server is not vulnerable to the Heartbleed attack.

Experimental: This server is not vulnerable to the OpenSSL CCS vulnerability (CVE-2014-0224).

Authentication

Server Key and Certificate #1

Common names	*.mailbox.org
Alternative names	*.mailbox.org mailbox.org
Prefix handling	Both (with and without WWW)
Valid from	Wed May 14 14:52:09 UTC 2014
Valid until	Tue May 14 14:52:09 UTC 2019 (expires in 4 years and 10 months)
Key	RSA 4096 bits
Weak key (Debian)	No
Issuer	SwissSign Server Silver CA 2008 - G2
Signature algorithm	SHA1withRSA
Extended Validation	No
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	Yes

Additional Certificates (if supplied)

Certificates provided	3 (4896 bytes)
Chain issues	Contains anchor

#2

Subject	SwissSign Server Silver CA 2008 - G2 SHA1: 95eef9f8bb003d337c47b0f9a947ffafe02725c3
Valid until	Fri Jul 07 17:07:16 UTC 2023 (expires in 9 years)

Key	RSA 2048 bits
Issuer	SwissSign Silver CA - G2
Signature algorithm	SHA1withRSA

#3

Subject	SwissSign Silver CA - G2 In trust store SHA1: 9baae59f56ee21cb435abe2593dfa7f040d11dcb
Valid until	Sat Oct 25 08:32:46 UTC 2036 (expires in 22 years and 4 months)
Key	RSA 4096 bits
Issuer	SwissSign Silver CA - G2 Self-signed
Signature algorithm	SHA1withRSA

Certification Paths

Path #1: Trusted

1	Sent by server	*.mailbox.org SHA1: 0c6479b4e783dbb3f2162c5d0d2570011fa2dab3 RSA 4096 bits / SHA1withRSA
2	Sent by server	SwissSign Server Silver CA 2008 - G2 SHA1: 95eef9f8bb003d337c47b0f9a947ffafe02725c3 RSA 2048 bits / SHA1withRSA
3	Sent by server In trust store	SwissSign Silver CA - G2 SHA1: 9baae59f56ee21cb435abe2593dfa7f040d11dcb RSA 4096 bits / SHA1withRSA

Configuration

Protocols

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

Cipher Suites (SSL 3+ suites in server-preferred order, then SSL 2 suites where used)

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH 256 bits (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH 256 bits (eq. 3072 bits RSA) FS	128
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	112
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH 256 bits (eq. 3072 bits RSA) FS	112
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH 256 bits (eq. 3072 bits RSA) FS	128
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256

TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)	128

Handshake Simulation

Android 2.3.7 No SNI [2]	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) FS	112
Android 4.0.4	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) FS	112
Android 4.1.1	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) FS	112
Android 4.2.2	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) FS	112
Android 4.3	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) FS	112
Android 4.4.2	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) FS	256
BingBot Dec 2013 No SNI [2]	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
BingPreview Dec 2013	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) FS	112
Chrome 34 / OS X R	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) FS	128
Firefox 24.2.0 ESR / Win 7	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) FS	112
Firefox 29 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Googlebot Oct 2013	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) FS	112
IE 6 / XP No FS [1] No SNI [2]	Protocol or cipher suite mismatch		Fail[3]
IE 7 / Vista	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
IE 8 / XP No FS [1] No SNI [2]	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS	112
IE 8-10 / Win 7 R	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
IE 11 / Win 7 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) FS	128
IE 11 / Win 8.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) FS	128
IE Mobile 10 / Win Phone 8.0	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
IE Mobile 11 / Win Phone 8.1	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) FS	128
Java 6u45 No SNI [2]	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) FS	112
Java 7u25	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) FS	112
Java 8b132	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) FS	128
OpenSSL 0.9.8y	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) FS	112
OpenSSL 1.0.1e	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) FS	256
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) FS	112
Safari 6 / iOS 6.0.1 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) FS	256
Safari 7 / iOS 7.1 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) FS	256
Safari 6.0.4 / OS X 10.8.4 R	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) FS	112
Safari 7 / OS X 10.9 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) FS	256
Yahoo Slurp Oct 2013	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) FS	112
YandexBot May 2014	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) FS	112

(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 tend to 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

Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0x16
TLS compression	No
RC4	No
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	No (more info)

OpenSSL CCS vuln. (CVE-2014-0224)	No
Forward Secrecy	Yes (with most browsers) ROBUST (more info)
Next Protocol Negotiation	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	Yes max-age=15768000
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	TLS 2.98
SSL 2 handshake compatibility	Yes

Miscellaneous

Test date	Mon Jun 23 09:40:54 UTC 2014
Test duration	91.421 seconds
HTTP status code	200
HTTP server signature	Apache
Server hostname	www.mailbox.org
PCI compliant	Yes
FIPS-ready	No

SSL Report v1.10.11

Terms and Conditions