QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > lb02.dualinventive.com

SSL Report: lb02.dualinventive.com (87.233.176.102)

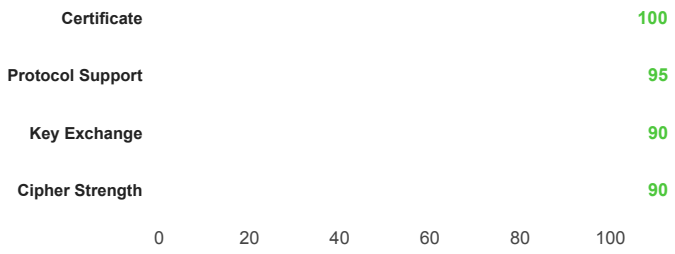
Assessed on: Fri, 14 Aug 2015 19:35:30 UTC | HIDDEN | Clear cache

Scan Another »

Summary

Overall Rating

A+



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_FALLBACK_SCSV to prevent protocol downgrade attacks.

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

Authentication

Server Key and Certificate #1

Common names	*.dualinventive.com
Alternative names	*.dualinventive.com dualinventive.com
Prefix handling	Not required for subdomains
Valid from	Thu, 23 Oct 2014 00:00:00 UTC
Valid until	Tue, 22 Oct 2019 23:59:59 UTC (expires in 4 years and 2 months)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	COMODO RSA Domain Validation Secure Server CA
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	Yes

Additional Certificates (if supplied)

Certificates provided	4 (5410 bytes)
Chain issues	**Contains anchor**

#2

Subject	AddTrust External CA Root In trust store Fingerprint: 02faf3e291435468607857694df5e45b68851868
Valid until	Sat, 30 May 2020 10:48:38 UTC (expires in 4 years and 9 months)
Key	RSA 2048 bits (e 65537)
Issuer	AddTrust External CA Root Self-signed
Signature algorithm	SHA1withRSA Weak, but no impact on root certificate

#3

Subject	COMODO RSA Certification Authority Fingerprint: f5ad0bcc1ad56cd150725b1c866c30ad92ef21b0
Valid until	Sat, 30 May 2020 10:48:38 UTC (expires in 4 years and 9 months)
Key	RSA 4096 bits (e 65537)
Issuer	AddTrust External CA Root
Signature algorithm	SHA384withRSA

#4

Subject	COMODO RSA Domain Validation Secure Server CA Fingerprint: 339cdd57cfd5b141169b615ff31428782d1da639
Valid until	Sun, 11 Feb 2029 23:59:59 UTC (expires in 13 years and 5 months)
Key	RSA 2048 bits (e 65537)
Issuer	COMODO RSA Certification Authority
Signature algorithm	SHA384withRSA

Certification Paths

Path #1: Trusted

1	Sent by server	*.dualinventive.com Fingerprint: 70394ebc32e39f1fab0c8befc7958543d6f73c6a RSA 2048 bits (e 65537) / SHA256withRSA
2	Sent by server	COMODO RSA Domain Validation Secure Server CA Fingerprint: 339cdd57cfd5b141169b615ff31428782d1da639 RSA 2048 bits (e 65537) / SHA384withRSA
3	In trust store	COMODO RSA Certification Authority Self-signed Fingerprint: afe5d244a8d1194230ff479fe2f897bbcd7a8cb4 RSA 4096 bits (e 65537) / SHA384withRSA

Path #2: Trusted

1	Sent by server	*.dualinventive.com Fingerprint: 70394ebc32e39f1fab0c8befc7958543d6f73c6a RSA 2048 bits (e 65537) / SHA256withRSA
2	Sent by server	COMODO RSA Domain Validation Secure Server CA Fingerprint: 339cdd57cfd5b141169b615ff31428782d1da639 RSA 2048 bits (e 65537) / SHA384withRSA
3	Sent by server	COMODO RSA Certification Authority Fingerprint: f5ad0bcc1ad56cd150725b1c866c30ad92ef21b0 RSA 4096 bits (e 65537) / SHA384withRSA
4	Sent by server In trust store	AddTrust External CA Root Self-signed Fingerprint: 02faf3e291435468607857694df5e45b68851868 RSA 2048 bits (e 65537) / SHA1withRSA Weak or insecure signature, but no impact on root certificate

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; deprecated and SSL 2 suites at the end)

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH 256 bits (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits (p: 256, g: 1, Ys: 256) FS	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 2048 bits (p: 256, g: 1, Ys: 256) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH 256 bits (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH 256 bits (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 2048 bits (p: 256, g: 1, Ys: 256) FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 2048 bits (p: 256, g: 1, Ys: 256) FS	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 2048 bits (p: 256, g: 1, Ys: 256) FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 2048 bits (p: 256, g: 1, Ys: 256) FS	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256

Handshake Simulation

Android 2.3.7 No SNI [2]	Incorrect certificate because this client doesn't support SNI		Fail[2]
Android 4.0.4	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Android 4.1.1	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Android 4.2.2	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Android 4.3	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Android 4.4.2	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Android 5.0.0	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Baidu Jan 2015	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
BingPreview Jan 2015	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Chrome 43 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Firefox 31.3.0 ESR / Win 7	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Firefox 39 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Googlebot Feb 2015	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
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_128_CBC_SHA (0xc013) FS	128
IE 8 / XP No FS [1] No SNI [2]	Protocol or cipher suite mismatch		Fail[3]
IE 8-10 / Win 7 R	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
IE 11 / Win 7 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) FS	128

IE 11 / Win 8.1 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) FS	128
IE 10 / Win Phone 8.0	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
IE 11 / Win Phone 8.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) FS	128
IE 11 / Win Phone 8.1 Update R	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) FS	128
Edge 12 / Win 10 (Build 10130) R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Java 6u45 No SNI [2]	Client does not support DH parameters > 1024 bits		Fail[3]
Java 7u25	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Java 8u31	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
OpenSSL 0.9.8y	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
OpenSSL 1.0.1l R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
OpenSSL 1.0.2 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Safari 6 / iOS 6.0.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) FS	128
Safari 6.0.4 / OS X 10.8.4 R	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Safari 7 / iOS 7.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) FS	128
Safari 7 / OS X 10.9 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) FS	128
Safari 8 / iOS 8.4 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) FS	128
Safari 8 / OS X 10.10 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) FS	128
Yahoo Slurp Jan 2015	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
YandexBot Jan 2015	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128

(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: 0xc013
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	**Yes, TLS_FALLBACK_SCSV supported** (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
Forward Secrecy	**Yes (with most browsers) ROBUST** (more info)
Next Protocol Negotiation (NPN)	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	**Yes** max-age=31536000
Public Key Pinning (HPKP)	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
SSL 2 handshake compatibility	Yes

Miscellaneous

Test date	Fri, 14 Aug 2015 19:33:22 UTC
Test duration	127.956 seconds
HTTP status code	200
HTTP server signature	nginx
Server hostname	-

SSL Report v1.19.33