



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

SSL Report: mawidaqa.com (23.21.205.96)

Assessed on: Tue Jul 09 18:38:45 UTC 2013 | [Clear cache](#)

[Scan Another >>](#)

Summary

Overall Rating

A

Certificate	100
Protocol Support	85
Key Exchange	80
Cipher Strength	90

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	*.mawidaqa.com
Alternative names	*.mawidaqa.com mawidaqa.com
Prefix handling	Both (with and without WWW)
Valid from	Fri Feb 15 00:00:00 UTC 2013
Valid until	Sun Mar 02 23:59:59 UTC 2014 (expires in 7 months and 26 days)
Key	RSA 2048 bits
Weak key (Debian)	No
Issuer	EssentialSSL CA
Signature algorithm	SHA1withRSA
Extended Validation	No
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	Yes



Additional Certificates (if supplied)

Certificates provided	4 (4989 bytes)
Chain issues	None

#2

Subject	EssentialSSL CA SHA1: 73820a20f8f47a457cd0b54cc4e4e31cefa5c1e7
Valid until	Tue Dec 31 23:59:59 UTC 2019 (expires in 6 years and 5 months)
Key	RSA 2048 bits
Issuer	COMODO Certification Authority

Issuer	COMODO Certification Authority
Signature algorithm	SHA1withRSA
#3	
Subject	COMODO Certification Authority SHA1: 4e154acb683efd5578001432b92afe896812b85e
Valid until	Sat May 30 10:48:38 UTC 2020 (expires in 6 years and 10 months)
Key	RSA 2048 bits
Issuer	UTN - DATACorp SGC
Signature algorithm	SHA1withRSA

#4

Subject	UTN - DATACorp SGC SHA1: 9e99817d12280c9677674430492eda1dce2e4c63
Valid until	Sat May 30 10:48:38 UTC 2020 (expires in 6 years and 10 months)
Key	RSA 2048 bits
Issuer	AddTrust External CA Root
Signature algorithm	SHA1withRSA



Certification Paths

Path #1: Trusted

1	Sent by server	*.mawidaqa.com SHA1: aacfa8b7bbfa7c3fb7bfd6cb326a7845dd45485 RSA 2048 bits / SHA1withRSA
2	Sent by server	EssentialSSL CA SHA1: 73820a20f8f47a457cd0b54cc4e4e31cefa5c1e7 RSA 2048 bits / SHA1withRSA
3	In trust store	COMODO Certification Authority SHA1: 6631bf9ef74f9eb6c9d5a60cba6abed1f7bdef7b RSA 2048 bits / SHA1withRSA

Path #2: Trusted

1	Sent by server	*.mawidaqa.com SHA1: aacfa8b7bbfa7c3fb7bfd6cb326a7845dd45485 RSA 2048 bits / SHA1withRSA
2	Sent by server	EssentialSSL CA SHA1: 73820a20f8f47a457cd0b54cc4e4e31cefa5c1e7 RSA 2048 bits / SHA1withRSA
3	Sent by server	COMODO Certification Authority SHA1: 4e154acb683efd5578001432b92afe896812b85e RSA 2048 bits / SHA1withRSA
4	In trust store	UTN - DATACorp SGC SHA1: 58119f0e128287ea50fdd987456f4f78dcfad6d4 RSA 2048 bits / SHA1withRSA

Path #3: Trusted

1	Sent by server	*.mawidaqa.com SHA1: aacfa8b7bbfa7c3fb7bfd6cb326a7845dd45485 RSA 2048 bits / SHA1withRSA
2	Sent by server	EssentialSSL CA SHA1: 73820a20f8f47a457cd0b54cc4e4e31cefa5c1e7 RSA 2048 bits / SHA1withRSA
3	Sent by server	COMODO Certification Authority SHA1: 4e154acb683efd5578001432b92afe896812b85e RSA 2048 bits / SHA1withRSA
4	Sent by server	UTN - DATACorp SGC SHA1: 9e99817d12280c9677674430492eda1dce2e4c63 RSA 2048 bits / SHA1withRSA
		AddTrust External CA Root

5

In trust store

SHA1: 02faf3e291435468607857694df5e45b68851868
RSA 2048 bits / SHA1withRSA

Configuration



Protocols

TLS 1.2	No
TLS 1.1	No
TLS 1.0	Yes
SSL 3.0	Yes
SSL 2.0	No



Cipher Suites (SSLv3+ suites in server-preferred order, then SSLv2 suites where used)

TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) ECDH 256 bits (eq. 3072 bits RSA) Forward Secrecy	128
SSL_RSA_WITH_RC4_128_SHA (0x5)	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH 256 bits (eq. 3072 bits RSA) Forward Secrecy	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 1024 bits (p: 128, g: 1, Ys: 128) Forward Secrecy	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) DH 1024 bits (p: 128, g: 1, Ys: 128) Forward Secrecy	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)	256
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH 256 bits (eq. 3072 bits RSA) Forward Secrecy	168
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits (p: 128, g: 1, Ys: 128) Forward Secrecy	168
SSL_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	168
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH 256 bits (eq. 3072 bits RSA) Forward Secrecy	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits (p: 128, g: 1, Ys: 128) Forward Secrecy	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 1024 bits (p: 128, g: 1, Ys: 128) Forward Secrecy	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)	128



Handshake Simulation (Experimental)

Chrome 27	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) Forward Secrecy	128
Firefox 21	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) Forward Secrecy	128
Internet Explorer 10	TLS 1.0	SSL_RSA_WITH_RC4_128_SHA (0x5)	128
Safari iOS 6.0.1	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) Forward Secrecy	128
Safari 5.1.9	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) Forward Secrecy	128



Protocol Details

Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not vulnerable
Compression	No
RC4	Yes PROBLEMATIC (more info)
Forward Secrecy	No (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
SSLv2 handshake compatibility	Yes



Miscellaneous

Test date	Tue Jul 09 18:38:06 UTC 2013
Test duration	39.633 seconds
HTTP status code	200
HTTP server signature	nginx/1.2.6 + Phusion Passenger 3.0.19
Server hostname	ec2-23-21-205-96.compute-1.amazonaws.com
PCI compliant	Yes
FIPS-ready	No

SSL Report v1.2.79