



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

SSL Report: www.isegurosdesaludadeslas.com (35.242.231.12)

Assessed on: Sun, 09 Nov 2025 08:30:31 UTC | HIDDEN | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating

A-

Certificate

Protocol Support

Key Exchange

Cipher Strength

0 20 40 60 80 100

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server does not support TLS 1.3. [MORE INFO »](#)

This site works only in browsers with SNI support.

Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1

Subject	isegurosdesaludadeslas.com Fingerprint SHA256: 44694ee4f6a026001777eaca8b86f5750bc88a30cd91b6695b6210b1df95700c Pin SHA256: 948N0p67my9JGBtqEj0PsR/hH4dqdUAh51sr89AEA64=
---------	--

Common names	isegurosdesaludadeslas.com
--------------	----------------------------

Alternative names	isegurosdesaludadeslas.com madrid.isegurosdesaludadeslas.com www.isegurosdesaludadeslas.com
-------------------	---

Serial Number	06fdadc38fe183666deccdac882537314ed6
---------------	--------------------------------------

Valid from	Fri, 07 Nov 2025 08:52:10 UTC
------------	-------------------------------

Valid until	Thu, 05 Feb 2026 08:52:09 UTC (expires in 2 months and 27 days)
-------------	---

Key	RSA 2048 bits (e 65537)
-----	-------------------------

Weak key (Debian)	No
-------------------	----

Issuer	R12 AIA: http://r12.i.lencr.org/
--------	-------------------------------------

Signature algorithm	SHA256withRSA
---------------------	---------------

Extended Validation	No
---------------------	----

Certificate Transparency	Yes (certificate)
--------------------------	--------------------------

OCSP Must Staple	No
------------------	----

Revocation information	CRL CRL: http://r12.c.lencr.org/87.crl
------------------------	---

Revocation status	Validation error CRL ERROR: IOException occurred
-------------------	---

DNS CAA	No (more info)
---------	----------------------------------

Trusted	Yes Mozilla Apple Android Java Windows
---------	--



Additional Certificates (if supplied)

Certificates provided	2 (2657 bytes)
-----------------------	----------------

Chain issues	None
--------------	------

#2

Additional Certificates (if supplied)

Subject	R12
	Fingerprint SHA256: 131fce7784016899a5a00203a9efc80f18ebbd75580717edc1553580930836ec
	Pin SHA256: kZwN96eHzftBWrOZUsd6cA4es80n3NzSk/XtYz2EqQ=
Valid until	Fri, 12 Mar 2027 23:59:59 UTC (expires in 1 year and 4 months)
Key	RSA 2048 bits (e 65537)
Issuer	ISRG Root X1
Signature algorithm	SHA256withRSA

**Certification Paths**[Click here to expand](#)**Certificate #2: RSA 2048 bits (SHA256withRSA) No SNI**[Click here to expand](#)**Configuration****Protocols**

TLS 1.3	No
TLS 1.2	Yes*
TLS 1.1	No
TLS 1.0	No*
SSL 3	No
SSL 2	No

(*) Experimental: Server negotiated using No-SNI

**Cipher Suites**

# TLS 1.2 (server has no preference)	
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 4096 bits FS 128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp521r1 (eq. 15360 bits RSA) FS 128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 4096 bits FS 256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp521r1 (eq. 15360 bits RSA) FS 256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa8)	ECDH secp521r1 (eq. 15360 bits RSA) FS 256

**Handshake Simulation**

Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp521r1 FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp521r1 FS
Android 6.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Android 8.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Android 8.1	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Android 9.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp521r1 FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 69 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Chrome 70 / Win 10	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Chrome 80 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS

Handshake Simulation

Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 62 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Firefox 73 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Googlebot Feb 2018	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH 4096 FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH 4096 FS
IE 11 / Win Phone 8.1 R		Server sent fatal alert: handshake_failure	
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH 4096 FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
Edge 16 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
Edge 18 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Java 8u161	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Java 11.0.3	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Java 12.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
OpenSSL 1.0.1l R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp521r1 FS
OpenSSL 1.0.2s R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
OpenSSL 1.1.0k R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
OpenSSL 1.1.1c R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
Safari 6 / iOS 6.0.1		Server sent fatal alert: handshake_failure	
Safari 7 / iOS 7.1 R		Server sent fatal alert: handshake_failure	
Safari 7 / OS X 10.9 R		Server sent fatal alert: handshake_failure	
Safari 8 / iOS 8.4 R		Server sent fatal alert: handshake_failure	
Safari 8 / OS X 10.10 R		Server sent fatal alert: handshake_failure	
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 12.1.2 / MacOS 10.14.6 Beta R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
Safari 12.1.1 / iOS 12.3.1 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
Apple ATS 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp521r1 FS

Not simulated clients (Protocol mismatch)

[Click here to expand](#)

- (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 sometimes 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).
(All) Certificate trust is not checked in handshake simulation, we only perform TLS handshake.

**Protocol Details**

Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Mitigated server-side (more info)
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info)
GOLDENDOODLE	No (more info)
OpenSSL 0-Length	No (more info)
Sleeping POODLE	No (more info)

Protocol Details

Downgrade attack prevention	Unknown (requires support for at least two protocols, excl. SSL2)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
ROBOT (vulnerability)	No (more info)
Forward Secrecy	Yes (with most browsers) ROBUST (more info)
ALPN	Yes h2 http/1.1
NPN	Yes h2 http/1.1
Session resumption (caching)	No (IDs assigned but not accepted)
Session resumption (tickets)	No
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No (more info)
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No (more info)
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
ECDH public server param reuse	No
Supported Named Groups	secp256r1, secp384r1, secp521r1, x25519, x448 (Server has no preference)
SSL 2 handshake compatibility	Yes

**HTTP Requests**1 <https://www.isegurosdesaludadeslas.com/> (HTTP/1.1 302 Moved Temporarily)**Miscellaneous**

Test date	Sun, 09 Nov 2025 08:29:20 UTC
Test duration	71.477 seconds
HTTP status code	302
HTTP forwarding	https://adeslas.isalud.com
HTTP server signature	nginx
Server hostname	12.231.242.35.bc.googleusercontent.com