

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

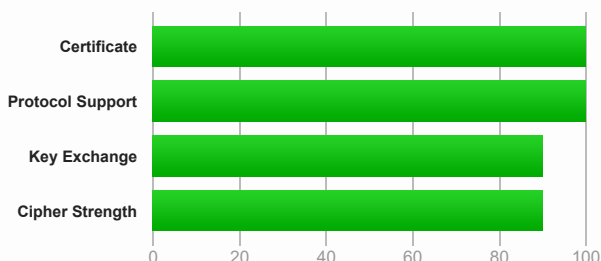
SSL Report: [www.electrohuila.com.co](#) (45.151.120.29)

Assessed on: Fri, 23 Jan 2026 14:15:05 UTC | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



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 1.3. [MORE INFO »](#)

Certificate #1: RSA 4096 bits (SHA256withRSA)



Server Key and Certificate #1



Subject	electrohuila.com.co Fingerprint SHA256: a437c948eda7938a4a101b9cb7ae23f7796faa148d80c887bf4285724ff1940c Pin SHA256: ScybQwGRB3/YawGV3+IMDkPpDLNo5H6EUeevw5G0CW0=
Common names	electrohuila.com.co
Alternative names	electrohuila.com.co www.electrohuila.com.co
Serial Number	06c98fb75b08035991add925ebef62488135
Valid from	Wed, 17 Dec 2025 11:35:57 UTC
Valid until	Tue, 17 Mar 2026 11:35:56 UTC (expires in 1 month and 21 days)
Key	RSA 4096 bits (e 65537)
Weak key (Debian)	No
Issuer	R13 AIA: http://r13.c.lencr.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL CRL: http://r13.c.lencr.org/54.crl
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows



Additional Certificates (if supplied)



Certificates provided	2 (2863 bytes)
Chain issues	None
#2	
Subject	R13 Fingerprint SHA256: d3b128216a843f8ef1321501f5df52a5df52939ee2c19297712cd3de4d419354 Pin SHA256: AISQhgtJirc8ahLyekmtX+lw+v46yPYRLJt9Cq1GIB0=
Valid until	Fri, 12 Mar 2027 23:59:59 UTC (expires in 1 year and 1 month)
Key	RSA 2048 bits (e 65537)
Issuer	ISRG Root X1
Signature algorithm	SHA256withRSA



Certification Paths



Click here to expand

Certificate #2: RSA 4096 bits (SHA256withRSA) No SNI



Click here to expand

Configuration



Protocols

TLS 1.3	Yes
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 1.3 (server has no preference)			[-]
TLS_AES_128_GCM_SHA256 (0x1301)	ECDH x25519 (eq. 3072 bits RSA) FS		128
TLS_AES_256_GCM_SHA384 (0x1302)	ECDH x25519 (eq. 3072 bits RSA) FS		256
TLS_CHACHA20_POLY1305_SHA256 (0x1303)	ECDH x25519 (eq. 3072 bits RSA) FS		256
# TLS 1.2 (suites in server-preferred order)			[-]
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH x25519 (eq. 3072 bits RSA) FS		128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH x25519 (eq. 3072 bits RSA) FS		256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH x25519 (eq. 3072 bits RSA) FS	WEAK	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH x25519 (eq. 3072 bits RSA) FS	WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH x25519 (eq. 3072 bits RSA) FS	WEAK	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)		WEAK	128

Cipher Suites

TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK	256



Handshake Simulation

Android 4.4.2	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Android 5.0.0	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Android 6.0	RSA 4096 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Android 7.0	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Android 8.0	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Android 8.1	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH x25519 FS
Android 9.0	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH x25519 FS
BingPreview Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Chrome 49 / XP SP3	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Chrome 69 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Chrome 70 / Win 10	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519 FS
Chrome 80 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519 FS
Firefox 31.3.0 ESR / Win 7	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 47 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 49 / XP SP3	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 62 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Firefox 73 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519 FS
Googlebot Feb 2018	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
IE 11 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
IE 11 / Win 8.1 R	RSA 4096 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
IE 11 / Win Phone 8.1 R	RSA 4096 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
IE 11 / Win Phone 8.1 Update R	RSA 4096 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
IE 11 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Edge 15 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Edge 16 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Edge 18 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Edge 13 / Win Phone 10 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Java 8u161	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Java 11.0.3	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH secp256r1 FS
Java 12.0.1	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH secp256r1 FS
OpenSSL 1.0.1l R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
OpenSSL 1.0.2s R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
OpenSSL 1.1.0k R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
OpenSSL 1.1.1c R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Safari 6 / iOS 6.0.1	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
Safari 7 / iOS 7.1 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
Safari 7 / OS X 10.9 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
Safari 8 / iOS 8.4 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
Safari 8 / OS X 10.10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
Safari 9 / iOS 9 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Safari 10 / iOS 10 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Safari 10 / OS X 10.12 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS

Handshake Simulation

Safari 12.1.2 / MacOS 10.14.6 Beta R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH x25519	FS
Safari 12.1.1 / iOS 12.3.1 R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH x25519	FS
Apple ATS 9 / iOS 9 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Yahoo Slurp Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
YandexBot Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	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) TLS 1.2 : 0xc027
GOLDENDOODLE	No (more info) TLS 1.2 : 0xc027
OpenSSL 0-Length	No (more info) TLS 1.2 : 0xc027
Sleeping POODLE	No (more info) TLS 1.2 : 0xc027
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
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	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
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

Protocol Details

Incorrect SNI alerts	No
Uses common DH primes	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
ECDH public server param reuse	No
Supported Named Groups	x25519, secp256r1, secp384r1 (server preferred order)
SSL 2 handshake compatibility	Yes
0-RTT enabled	No



HTTP Requests



1 <https://www.electrohuila.com.co/> (HTTP/1.1 200 OK)

	Connection	close
	Content-Type	text/html
	Last-Modified	Wed, 21 Jan 2026 19:06:56 GMT
	Etag	"a6d1-697123d0-c20bf4eb03f0f015;;;"
	Accept-Ranges	bytes
	Content-Length	42705
	Date	Fri, 23 Jan 2026 14:13:00 GMT
1	Server	LiteSpeed
	platform	hostinger
	panel	hpanel
	Retry-After	60
	Content-Security-Policy	upgrade-insecure-requests
	alt-svc	h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"



Miscellaneous

Test date	Fri, 23 Jan 2026 14:12:47 UTC
Test duration	137.962 seconds
HTTP status code	200
HTTP server signature	LiteSpeed
Server hostname	-