Qualys. SSL Labs

SSL Report: api.santiesleo.dev (34.28.193.140)

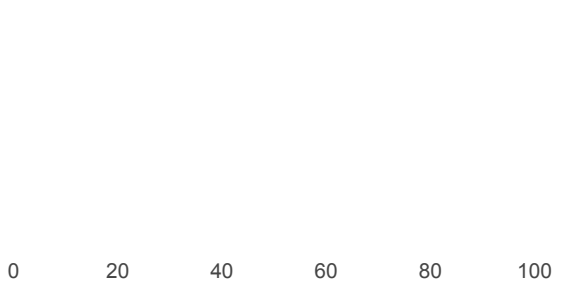
Assessed on: Sun, 23 Nov 2025 06:21:32 UTC | Hide | Clear cache

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 1.3. MORE INFO »

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	api.santiesleo.dev Fingerprint SHA256: aff0002f180b1a66a0cbfb79e86b5135bd28e8b0e080ad026bb6efc92362cba0 Pin SHA256: mm3ubiRkSUYb04cwfrSCosuONumGcf86SKjSHHIOtFA=
Common names	api.santiesleo.dev
Alternative names	api.santiesleo.dev
Serial Number	05c885a22b6970abcd9c60e90f8d4262af88
Valid from	Sat, 22 Nov 2025 20:47:37 UTC
Valid until	Fri, 20 Feb 2026 20:47:36 UTC (expires in 2 months and 28 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/9.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 (2573 bytes)
Chain issues	None

#2

Subject	R12 Fingerprint SHA256: 131fce7784016899a5a00203a9efc80f18ebbd75580717edc1553580930836ec Pin SHA256: kZwN96eHtZftBWrOZUsd6cA4es80n3NzSk/XtYz2EqQ=

Additional Certificates (if supplied)

Valid until	Fri, 12 Mar 2027 23:59:59 UTC (expires in 1 year and 3 months)
Key	RSA 2048 bits (e 65537)
Issuer	ISRG Root X1
Signature algorithm	SHA256withRSA

Certification Paths

Mozilla Apple Android Java Windows

Path #1: Trusted

1	Sent by server	api.santiesleo.dev Fingerprint SHA256: aff0002f180b1a66a0cbfb79e86b5135bd28e8b0e080ad026bb6efc92362cba0 Pin SHA256: mm3ubiRkSUYb04cwfrSCosuONumGcf86SKjSHHIOtFA= RSA 2048 bits (e 65537) / SHA256withRSA **CRL ERROR: IOException occurred**
2	Sent by server	R12 Fingerprint SHA256: 131fce7784016899a5a00203a9efc80f18ebbd75580717edc1553580930836ec Pin SHA256: kZwN96eHtZftBWrOZUsd6cA4es80n3NzSk/XtYz2EqQ= RSA 2048 bits (e 65537) / SHA256withRSA **CRL ERROR: IOException occurred**
3	In trust store	ISRG Root X1 Self-signed Fingerprint SHA256: 96bcec06264976f37460779acf28c5a7cfe8a3c0aae11a8ffcee05c0bddf08c6 Pin SHA256: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M= RSA 4096 bits (e 65537) / SHA256withRSA

Certificate #2: RSA 2048 bits (SHA256withRSA) No SNI

Server Key and Certificate #1

Subject	Kubernetes Ingress Controller Fake Certificate Fingerprint SHA256: edde1f4ad5208615ca0a844945f3add547cd249272a075e5adc70f3b8cc32946 Pin SHA256: fdXyrbzBq3JywImnNtQGeZK327jjo+s2elRFD5YxsCM=
Common names	Kubernetes Ingress Controller Fake Certificate

Server Key and Certificate #1

Alternative names	ingress.local **MISMATCH**
Serial Number	00e423d6151b4db5fd317cc8b9a04fd0aa
Valid from	Sun, 23 Nov 2025 04:07:05 UTC
Valid until	Mon, 23 Nov 2026 04:07:05 UTC (expires in 11 months and 30 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Kubernetes Ingress Controller Fake Certificate Self-signed
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No
Revocation information	None
Trusted	No **NOT TRUSTED** **Mozilla Apple Android Java Windows**

Additional Certificates (if supplied)

Certificates provided	1 (884 bytes)
Chain issues	None

Certification Paths

Click here to expand

Configuration

Protocols

TLS 1.3	Yes

Protocols

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 (suites in server-preferred order)

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_AES_128_GCM_SHA256 (0x1301)	ECDH x25519 (eq. 3072 bits RSA) FS	128

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_CHACHA20_POLY1305_SHA256 (0xcca8)	ECDH x25519 (eq. 3072 bits RSA) FS	256

Handshake Simulation

Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 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_AES_128_GCM_SHA256 ECDH x25519 FS
Android 8.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Android 8.1	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS
Android 9.0	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS

Handshake Simulation

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	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS
Chrome 80 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 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
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	-	TLS 1.3	TLS_AES_256_GCM_SHA384 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	Server sent fatal alert: handshake_failure		
IE 11 / Win 8.1 R	Server sent fatal alert: handshake_failure		
IE 11 / Win Phone 8.1 R	Server sent fatal alert: handshake_failure		
IE 11 / Win Phone 8.1 Update R	Server sent fatal alert: handshake_failure		
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Edge 16 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Edge 18 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Java 8u161	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Java 11.0.3	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp256r1 FS
Java 12.0.1	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp256r1 FS
OpenSSL 1.0.1l R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 1.0.2s R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 1.1.0k R	RSA 2048 (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	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		

Handshake Simulation

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_128_GCM_SHA256 ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 12.1.2 / MacOS 10.14.6 Beta R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS
Safari 12.1.1 / iOS 12.3.1 R	-	TLS 1.3	TLS_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_128_GCM_SHA256 ECDH secp256r1 FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS

Not simulated clients (Protocol mismatch)

Android 2.3.7 No SNI [2]	Protocol mismatch (not simulated)
Android 4.0.4	Protocol mismatch (not simulated)
Android 4.1.1	Protocol mismatch (not simulated)
Android 4.2.2	Protocol mismatch (not simulated)
Android 4.3	Protocol mismatch (not simulated)
Baidu Jan 2015	Protocol mismatch (not simulated)
IE 6 / XP No FS [1] No SNI [2]	Protocol mismatch (not simulated)
IE 7 / Vista	Protocol mismatch (not simulated)
IE 8 / XP No FS [1] No SNI [2]	Protocol mismatch (not simulated)
IE 8-10 / Win 7 R	Protocol mismatch (not simulated)
IE 10 / Win Phone 8.0	Protocol mismatch (not simulated)
Java 6u45 No SNI [2]	Protocol mismatch (not simulated)
Java 7u25	Protocol mismatch (not simulated)
OpenSSL 0.9.8y	Protocol mismatch (not simulated)
Safari 5.1.9 / OS X 10.6.8	Protocol mismatch (not simulated)
Safari 6.0.4 / OS X 10.8.4 R	Protocol mismatch (not simulated)

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

Handshake Simulation

(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)
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

Protocol Details

Session resumption (tickets)	No
OCSP stapling	No
Strict Transport Security (HSTS)	**Yes** max-age=15724800; includeSubDomains
HSTS Preloading	**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, 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, x448, secp521r1, secp384r1 (server preferred order)
SSL 2 handshake compatibility	No
0-RTT enabled	No

HTTP Requests

1 https://api.santiesleo.dev/ (HTTP/1.1 404 Not Found)

1	**Date**	Sun, 23 Nov 2025 06:21:00 GMT
	Content-Type	application/json
	Content-Length	129
	Connection	close
	Vary	Origin
	Vary	Access-Control-Request-Method
	Vary	Access-Control-Request-Headers
	Strict-Transport-Security	max-age=15724800; includeSubDomains

1 **https://api.santiesleo.dev/** (HTTP/1.1 404 Not Found)

X-Content-Type-Options	nosniff
X-Frame-Options	DENY
X-XSS-Protection	1; mode=block
Referrer-Policy	strict-origin-when-cross-origin

Miscellaneous

Test date	Sun, 23 Nov 2025 06:20:51 UTC
Test duration	40.830 seconds
HTTP status code	404
HTTP server signature	-
Server hostname	140.193.28.34.bc.googleusercontent.com

SSL Report v2.4.1

Copyright © 2009-2025 Qualys, Inc. All Rights Reserved. Privacy Policy. Terms and Conditions

Try Qualys for free! Experience the award-winning Qualys Cloud Platform and the entire collection of Qualys Cloud Apps, including certificate security solutions.