

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

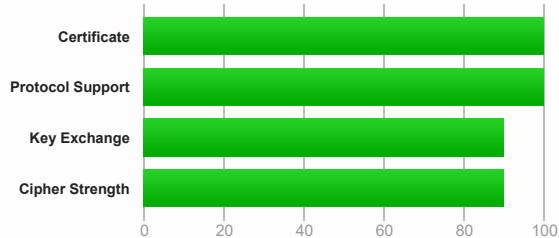
# SSL Report: ealbo.com (144.76.78.213)

Assessed on: Wed, 27 Mar 2024 07:59:58 UTC | [Hide](#) | [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.

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



<b>Subject</b>	*.ealbo.com Fingerprint SHA256: 0002ec3f4934634c5495b4d21bf510e13802c6841bbb96d77f698c2e4d87e58d Pin SHA256: ta5yR9hzO/4gsObgAE/dBkYUHhbTpPEqwUMpqwU7d1w=
<b>Common names</b>	*.ealbo.com
<b>Alternative names</b>	*.ealbo.com ealbo.com ealbo.neatalerts.com www.ealbo.neatalerts.com
<b>Serial Number</b>	049f3fa488233beaa1da6569842a62315f33
<b>Valid from</b>	Sat, 17 Feb 2024 15:24:44 UTC
<b>Valid until</b>	Fri, 17 May 2024 15:24:43 UTC (expires in 1 month and 20 days)
<b>Key</b>	RSA 2048 bits (e 65537)
<b>Weak key (Debian)</b>	No
<b>Issuer</b>	R3 AIA: <a href="http://r3.i.lencr.org/">http://r3.i.lencr.org/</a>
<b>Signature algorithm</b>	SHA256withRSA
<b>Extended Validation</b>	No
<b>Certificate Transparency</b>	Yes (certificate)
<b>OCSP Must Staple</b>	No
<b>Revocation information</b>	OCSP OCSP: <a href="http://r3.o.lencr.org/">http://r3.o.lencr.org</a>
<b>Revocation status</b>	Good (not revoked)
<b>DNS CAA</b>	No ( <a href="#">more info</a> )
<b>Trusted</b>	Yes Mozilla Apple Android Java Windows



### Additional Certificates (if supplied)



<b>Certificates provided</b>	2 (2619 bytes)
<b>Chain issues</b>	None

### Additional Certificates (if supplied) ⬇️

#2

<b>Subject</b>	R3 Fingerprint SHA256: 67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd Pin SHA256: jQJtBlh0grw0/1TkHSumWb+Fs0Ggogr621gT3PvPKG0=
<b>Valid until</b>	Mon, 15 Sep 2025 16:00:00 UTC (expires in 1 year and 5 months)
<b>Key</b>	RSA 2048 bits (e 65537)
<b>Issuer</b>	ISRG Root X1
<b>Signature algorithm</b>	SHA256withRSA



#### Certification Paths +

[Click here to expand](#)

### Certificate #2: RSA 2048 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

<b># TLS 1.3 (server has no preference)</b> <span style="float: right;">-</span>		
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
<b># TLS 1.2 (suites in server-preferred order)</b> <span style="float: right;">-</span>		
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 (0xc0a8)	ECDH x25519 (eq. 3072 bits RSA) FS	256



#### Handshake Simulation

<a href="#">Android 4.4.2</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Android 5.0.0</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Android 6.0</a>	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Android 7.0</a>	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
<a href="#">Android 8.0</a>	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
<a href="#">Android 8.1</a>	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH x25519 FS
<a href="#">Android 9.0</a>	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH x25519 FS
<a href="#">BingPreview Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Chrome 49 / XP SP3</a>	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
<a href="#">Chrome 69 / Win 7 R</a>	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS

## Handshake Simulation

<a href="#">Chrome 70 / Win 10</a>	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519	FS
<a href="#">Chrome 80 / Win 10</a> R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519	FS
<a href="#">Firefox 31.3.0 ESR / Win 7</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Firefox 47 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Firefox 49 / XP SP3</a>	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Firefox 62 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519	FS
<a href="#">Firefox 73 / Win 10</a> R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519	FS
<a href="#">Googlebot Feb 2018</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519	FS
<a href="#">IE 11 / Win 7</a> R	Server sent fatal alert: handshake_failure				
<a href="#">IE 11 / Win 8.1</a> R	Server sent fatal alert: handshake_failure				
<a href="#">IE 11 / Win Phone 8.1</a> R	Server sent fatal alert: handshake_failure				
<a href="#">IE 11 / Win Phone 8.1 Update</a> R	Server sent fatal alert: handshake_failure				
<a href="#">IE 11 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Edge 15 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519	FS
<a href="#">Edge 16 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519	FS
<a href="#">Edge 18 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519	FS
<a href="#">Edge 13 / Win Phone 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Java 8u161</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Java 11.0.3</a>	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Java 12.0.1</a>	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">OpenSSL 1.0.1l</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">OpenSSL 1.0.2s</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">OpenSSL 1.1.0k</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519	FS
<a href="#">OpenSSL 1.1.1c</a> R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519	FS
<a href="#">Safari 6 / iOS 6.0.1</a>	Server sent fatal alert: handshake_failure				
<a href="#">Safari 7 / iOS 7.1</a> R	Server sent fatal alert: handshake_failure				
<a href="#">Safari 7 / OS X 10.9</a> R	Server sent fatal alert: handshake_failure				
<a href="#">Safari 8 / iOS 8.4</a> R	Server sent fatal alert: handshake_failure				
<a href="#">Safari 8 / OS X 10.10</a> R	Server sent fatal alert: handshake_failure				
<a href="#">Safari 9 / iOS 9</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Safari 9 / OS X 10.11</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Safari 10 / iOS 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Safari 10 / OS X 10.12</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Safari 12.1.2 / MacOS 10.14.6 Beta</a> R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH x25519	FS
<a href="#">Safari 12.1.1 / iOS 12.3.1</a> R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH x25519	FS
<a href="#">Apple ATS 9 / iOS 9</a> R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Yahoo Slurp Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">YandexBot Jan 2015</a>	RSA 2048 (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

<b>Secure Renegotiation</b>	<b>Supported</b>
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Mitigated server-side ( <a href="#">more info</a> )
POODLE (SSLv3)	No, SSL 3 not supported ( <a href="#">more info</a> )
POODLE (TLS)	No ( <a href="#">more info</a> )

## Protocol Details

Zombie POODLE	No ( <a href="#">more info</a> )
GOLDENDOODLE	No ( <a href="#">more info</a> )
OpenSSL 0-Length	No ( <a href="#">more info</a> )
Sleeping POODLE	No ( <a href="#">more info</a> )
<b>Downgrade attack prevention</b>	<b>Yes, TLS_FALLBACK_SCSV supported</b> ( <a href="#">more info</a> )
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No ( <a href="#">more info</a> )
Ticketbleed (vulnerability)	No ( <a href="#">more info</a> )
OpenSSL CCS vuln. (CVE-2014-0224)	No ( <a href="#">more info</a> )
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No ( <a href="#">more info</a> )
ROBOT (vulnerability)	No ( <a href="#">more info</a> )
<b>Forward Secrecy</b>	<b>Yes (with most browsers) ROBUST</b> ( <a href="#">more info</a> )
ALPN	Yes h2 http/1.1
NPN	No
<b>Session resumption (caching)</b>	<b>No (IDs assigned but not accepted)</b>
Session resumption (tickets)	Yes
<b>OCSP stapling</b>	<b>Yes</b>
<b>Strict Transport Security (HSTS)</b>	<b>Yes</b> max-age=15552000
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No ( <a href="#">more info</a> )
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No ( <a href="#">more info</a> )
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, secp384r1 (server preferred order)
SSL 2 handshake compatibility	No
0-RTT enabled	No



## HTTP Requests



1 <https://ealbo.com/> (HTTP/1.1 200 OK)



## Miscellaneous

Test date	Wed, 27 Mar 2024 07:58:42 UTC
Test duration	75.494 seconds
HTTP status code	200
HTTP server signature	LiteSpeed
Server hostname	davos.orcwebhosting.com