SSL Report: hrms.licindia.in (52.85.132.122)

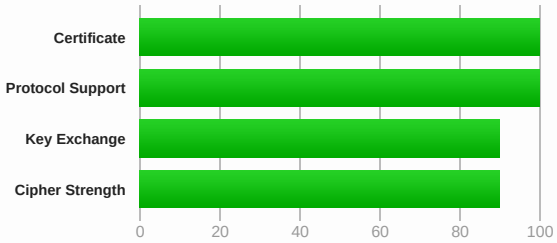
Assessed on: Sun, 25 Oct 2026 09:10:19 UTC | **HIDDEN** | Clear cache

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 »

This server supports PQC (Post-Quantum Cryptography) key exchange.

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	*.hrms.licindia.in Fingerprint SHA256: 875da8d18b674597c56f4fa09d9284137ff5f24fd54eabbac66701f4422d81a2 Pin SHA256: 3vcbaKbyd07jzax88iOhhe/R38EZyJUt1+zWR2Pro/Q=
Common names	*.hrms.licindia.in
Alternative names	*.hrms.licindia.in hrms.licindia.in
Serial Number	00a87acc355966a169d2e57ef20fb4f029
Valid from	Thu, 22 Oct 2026 00:00:00 UTC
Valid until	Sat, 08 May 2027 23:59:59 UTC (expires in 6 months and 13 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Sectigo Public Server Authentication CA OV R36 AIA: http://crt.sectigo.com/SectigoPublicServerAuthenticationCAOVR36.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	**Yes (certificate)**
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.sectigo.com/SectigoPublicServerAuthenticationCAOVR36.crl OCSP: http://ocsp.sectigo.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)

Server Key and Certificate #1

Trusted	**Yes** Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	3 (5154 bytes)
Chain issues	None

#2

Subject	Sectigo Public Server Authentication CA OV R36 Fingerprint SHA256: 6542d176bed50f193c0ce297ae44ecd8a0a86bec2ede682769344059b4e78530 Pin SHA256: KqkYYX5LYAYP7XGemqzbtPPIA8x7BS/BbOIcAXf3j2k=
Valid until	Fri, 21 Mar 2036 23:59:59 UTC (expires in 9 years and 4 months)
Key	RSA 3072 bits (e 65537)
Issuer	Sectigo Public Server Authentication Root R46
Signature algorithm	SHA384withRSA

#3

Subject	Sectigo Public Server Authentication Root R46 Fingerprint SHA256: 92f351bf3d54164dfa8dd8f9e1139d3150349786485d2b9eecd00e2971c1e6c5 Pin SHA256: Douxi77vs4G+Ib/BogbTFymEYq0QSFXwSgVCaZcI09Q=
Valid until	Mon, 18 Jan 2038 23:59:59 UTC (expires in 11 years and 2 months)
Key	RSA 4096 bits (e 65537)
Issuer	USERTrust RSA Certification Authority
Signature algorithm	SHA384withRSA

Certification Paths

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

Cipher Suites

TLS 1.3 (suites in server-preferred order)

TLS_AES_128_GCM_SHA256 (0x1301)	X25519MLKEM768 (eq. 3072 bits RSA)	FS	128
TLS_AES_256_GCM_SHA384 (0x1302)	X25519MLKEM768 (eq. 3072 bits RSA)	FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303)	X25519MLKEM768 (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_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_128_GCM_SHA256	ECDH x25519	FS	
Android 9.0	-	TLS 1.3	TLS_AES_128_GCM_SHA256	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	
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_128_GCM_SHA256	ECDH x25519	FS	
Chrome 80 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519	FS	
Chrome 131 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	PQC X25519MLKEM768	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_128_GCM_SHA256	ECDH x25519	FS	
Firefox 135 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	PQC X25519MLKEM768	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	Protocol or cipher suite mismatch					
IE 11 / Win 8.1 R	Protocol or cipher suite mismatch					
IE 11 / Win Phone 8.1 R	Protocol or cipher suite mismatch					
IE 11 / Win Phone 8.1 Update R	Protocol or cipher suite mismatch					
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 131 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	PQC X25519MLKEM768	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_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 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_128_GCM_SHA256	ECDH x25519	FS	
Opera 117 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	PQC X25519MLKEM768	FS	
Safari 6 / iOS 6.0.1	Protocol or cipher suite mismatch					
Safari 7 / iOS 7.1 R	Protocol or cipher suite mismatch					
Safari 7 / OS X 10.9 R	Protocol or cipher suite mismatch					
Safari 8 / iOS 8.4 R	Protocol or cipher suite mismatch					
Safari 8 / OS X 10.10 R	Protocol or cipher suite mismatch					
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_128_GCM_SHA256	ECDH x25519	FS	
Safari 12.1.1 / iOS 12.3.1 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	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	

Handshake Simulation

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)

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)
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)	**No (IDs assigned but not accepted)**
Session resumption (tickets)	Yes
OCSP stapling	**Yes**
Strict Transport Security (HSTS)	**Yes** max-age=31536000; includeSubDomains; preload
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, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
ECDH public server param reuse	No
Supported Named Groups	X25519MLKEM768, SecP256r1MLKEM768, x25519, secp256r1, secp384r1 (server preferred order)

Protocol Details

PQC Key Exchange	**Supported**
Supported PQC Groups	X25519MLKEM768, SecP256r1MLKEM768
SSL 2 handshake compatibility	No
0-RTT enabled	No

HTTP Requests

1 **https://hrms.licindia.in/** (HTTP/1.1 200 OK)

Miscellaneous

Test date	Sun, 25 Oct 2026 09:08:02 UTC
Test duration	68.389 seconds
HTTP status code	200
HTTP server signature	-
Server hostname	server-52-85-132-122.phx52.r.cloudfront.net

SSL Report v2.4.3

Copyright © 2009-2026 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.