

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > compliance.insight.gov.in

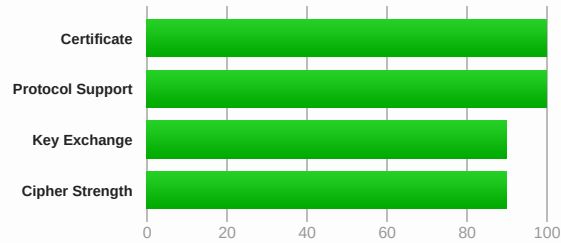
SSL Report: compliance.insight.gov.in (125.18.251.103)

Assessed on: Mon, 26 Oct 2026 08:04:58 UTC | **HIDDEN** | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



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

This server supports TLS 1.3. [MORE INFO »](#)

This server does not support 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	compliance.insight.gov.in Fingerprint SHA256: 39870d52b88f9df1df461cf40537af8ab7aa84cf4282128cb7f7fa25bf3af45 Pin SHA256: PsbeNHlfrInTO+Q1765T0r1JQsMhtnhtWTV9QnTMIW6M=
Common names	compliance.insight.gov.in
Alternative names	compliance.insight.gov.in www.compliance.insight.gov.in
Serial Number	6bf7e3edbe80ca20b402ba22bc3f45bf
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 12 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Sectigo Public Server Authentication CA DV R36 AIA: http://crt.sectigo.com/SectigoPublicServerAuthenticationCADVR36.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://ocsp.sectigo.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows



Additional Certificates (if supplied)



Certificates provided	4 (6518 bytes)
Chain issues	Contains anchor
#2	
Subject	Sectigo Public Server Authentication CA DV R36 Fingerprint SHA256: 8c54c334b66ba4e426772af4a3f9136c19a1aec729fdb28c535c07a5a4ef22e0 Pin SHA256: a9khLOZJxlnJyrxstg/P+seiDCm+Yf3OsrXyFocBal0=
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/BogbTFymEYq0QSFxwSgVCaZcl09Q=
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

#4	
Subject	USERTrust RSA Certification Authority In trust store Fingerprint SHA256: e793c9b02fd8aa13e21c31228accb08119643b749c898964b1746d46c3d4cbd2 Pin SHA256: x4QzPSC810K5/cMjb05Qm4k3Bw5zBn4ITdO/nEW/Td4=
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 Self-signed
Signature algorithm	SHA384withRSA



Certification Paths



Click here to expand

Configuration



Protocols

TLS 1.3	Yes
TLS 1.2	No
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_256_GCM_SHA384 (0x1302)	ECDH x25519 (eq. 3072 bits RSA)	FS	256
TLS_AES_128_GCM_SHA256 (0x1301)	ECDH x25519 (eq. 3072 bits RSA)	FS	128



Handshake Simulation

Android 8.1	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519	FS
-----------------------------	---	---------	------------------------	-------------	----

Handshake Simulation

Android 9.0	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519	FS
Chrome 69 / Win 7	R	Server sent fatal alert: handshake_failure			
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
Chrome 131 / Win 10	R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Firefox 62 / Win 7	R	Server sent fatal alert: handshake_failure			
Firefox 73 / Win 10	R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Firefox 135 / Win 10	R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Edge 131 / Win 10	R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 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 1.1.0k	R	Server sent fatal alert: handshake_failure			
OpenSSL 1.1.1c	R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Opera 117 / Win 10	R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Safari 12.1.2 / MacOS 10.14.6	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519	FS
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

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

ROBOT (vulnerability)	No (more info)
Forward Secrecy	Yes (with most browsers) ROBUST (more info)
ALPN	Yes http/1.1
Session resumption (tickets)	No
OCSP stapling	No
Strict Transport Security (HSTS)	Yes max-age=31536000; includeSubdomains;
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)
Supported Named Groups	x25519, secp256r1, secp384r1, secp521r1, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1 (server preferred order)
PQC Key Exchange	Not Supported
Supported PQC Groups	-
SSL 2 handshake compatibility	No
0-RTT enabled	No



HTTP Requests



- <https://compliance.insight.gov.in/> (HTTP/1.1 301 Moved Permanently)
- <https://compliance.insight.gov.in/compliance/> (HTTP/1.1 302 Found)



Miscellaneous

Test date	Mon, 26 Oct 2026 08:03:47 UTC
Test duration	70.761 seconds
HTTP status code	302
HTTP forwarding	http://compliance.insight.gov.in PLAINTEXT
HTTP server signature	Web Server
Server hostname	compliance.insight.gov.in

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.