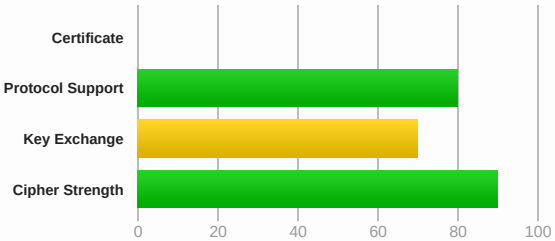
SSL Report: ihmshimla.ac.in (164.100.211.110)

Assessed on: Sat, 24 Oct 2026 06:23:27 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's certificate is not trusted, see below for details.

This server does not support Forward Secrecy with the reference browsers. Grade capped to B. MORE INFO »

This server does not support TLS 1.3. MORE INFO »

This server does not support PQC (Post-Quantum Cryptography) key exchange.

DNS Certification Authority Authorization (CAA) Policy found for this domain. MORE INFO »

Certificate #1: RSA 2048 bits (SHA384withRSA)

Server Key and Certificate #1

Subject	ihmshimla.ac.in Fingerprint SHA256: 574a537a1d117581bb26fe211f167cfa507226fe10721c9149c31980db94916d Pin SHA256: 46RewDYHsB4muc5aJwvy7ItyTOkg+Pg93ZXdbCUZfog=
Common names	ihmshimla.ac.in
Alternative names	www.ihmshimla.ac.in ihmshimla.ac.in www.ihmshimla.nic.in ihmshimla.nic.in
Serial Number	2f2737aa0f241427f9e20fb4fec3e7
Valid from	Thu, 08 Oct 2026 04:23:01 UTC
Valid until	Wed, 06 Jan 2027 04:23:01 UTC (expires in 2 months and 12 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	EM DV TLS CA - G2A-1 AIA: http://repository.emsign.com/certs/EMDVTLSCAG2A1EE.p7c
Signature algorithm	SHA384withRSA
Extended Validation	No
Certificate Transparency	**Yes (certificate)**
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.emsign.com?EMDVTLSCAG2A1.crl OCSP: http://ocsp-a.emsign.com
Revocation status	Revoked **INSECURE**

Server Key and Certificate #1

DNS CAA	**Yes** policy host: ihmshimla.ac.in issue: emsign.com flags:0
Trusted	No **NOT TRUSTED** (Why?) **Mozilla Apple Android Java Windows**

Additional Certificates (if supplied)

Certificates provided	3 (5090 bytes)
Chain issues	None

#2

Subject	EM DV TLS CA - G2A-1 Fingerprint SHA256: 3f13597d3355d341bd09328aee567d7f4e002d9919b986f9962daff197ea75d1 Pin SHA256: zrUpja649ZJ5SAtGACyJ93Vcw6FpUUsRuBC+/BlaANg=
Valid until	Mon, 28 May 2040 07:16:12 UTC (expires in 13 years and 7 months)
Key	RSA 4096 bits (e 65537)
Issuer	emSign Root TLS CA - G1
Signature algorithm	SHA384withRSA

#3

Subject	emSign Root TLS CA - G1 Fingerprint SHA256: 9b913476eab476e21e0887dbcde44345d1359d28116b83b7cd3e87bd807ebf68 Pin SHA256: 7OKONSic6GIcckB5SeUFAFKtRgfMMy6vm1RgKarL+3o=
Valid until	Sat, 09 Jul 2039 18:30:00 UTC (expires in 12 years and 8 months)
Key	RSA 4096 bits (e 65537)
Issuer	emSign Root CA - G1
Signature algorithm	SHA256withRSA

Certification Paths

Click here to expand

Configuration

Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

Cipher Suites

TLS 1.2 (suites in server-preferred order)

TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) **WEAK**	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) **WEAK**	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK**	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 2048 bits FS	256
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 secp384r1 (eq. 7680 bits RSA) FS	256

Handshake Simulation

Android 4.4.2	RSA 2048 (SHA384)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Android 5.0.0	RSA 2048 (SHA384)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Android 6.0	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Android 7.0	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Android 8.0	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Android 8.1	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Android 9.0	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
BingPreview Jan 2015	RSA 2048 (SHA384)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Chrome 49 / XP SP3	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Chrome 69 / Win 7 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Chrome 70 / Win 10	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Chrome 80 / Win 10 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Chrome 131 / Win 10 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA384)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Firefox 47 / Win 7 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 49 / XP SP3	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 62 / Win 7 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Firefox 73 / Win 10 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Firefox 135 / Win 10 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Googlebot Feb 2018	RSA 2048 (SHA384)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
IE 11 / Win 7 R	RSA 2048 (SHA384)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
IE 11 / Win 8.1 R	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA384)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
IE 11 / Win 10 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DH 2048 FS
Edge 15 / Win 10 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Edge 16 / Win 10 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Edge 18 / Win 10 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Edge 131 / Win 10 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DH 2048 FS
Java 8u161	RSA 2048 (SHA384)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Java 11.0.3	RSA 2048 (SHA384)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Java 12.0.1	RSA 2048 (SHA384)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
OpenSSL 1.0.1l R	RSA 2048 (SHA384)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
OpenSSL 1.0.2s R	RSA 2048 (SHA384)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
OpenSSL 1.1.0k R	RSA 2048 (SHA384)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
OpenSSL 1.1.1c R	RSA 2048 (SHA384)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Opera 117 / Win 10 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA384)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA384)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA384)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA384)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Safari 8 / OS X 10.10 R	RSA 2048 (SHA384)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Safari 9 / iOS 9 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Safari 10 / iOS 10 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA384)	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	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Safari 12.1.1 / iOS 12.3.1 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS

Handshake Simulation

Apple ATS 9 / iOS 9 R	RSA 2048 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA384)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
YandexBot Jan 2015	RSA 2048 (SHA384)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	No 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 : 0x002f
GOLDENDOODLE	No (more info) TLS 1.2 : 0x002f
OpenSSL 0-Length	No (more info) TLS 1.2 : 0x002f
Sleeping POODLE	No (more info) TLS 1.2 : 0x002f
Downgrade attack prevention	Unknown (requires support for at least two protocols, excl. SSL2)
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	**With some browsers** (more info)
ALPN	Yes h2 http/1.1
NPN	No
Session resumption (caching)	**No (IDs assigned but not accepted)**
Session resumption (tickets)	No
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
Incorrect SNI alerts	No
Uses common DH primes	No
DH public server param (Ys) reuse	No
ECDH public server param reuse	**Yes**
Supported Named Groups	x25519, secp256r1, secp384r1 (server preferred order)

Protocol Details

PQC Key Exchange	Not Supported
Supported PQC Groups	-
SSL 2 handshake compatibility	No

HTTP Requests

1 **https://ihmshimla.ac.in/** (HTTP/1.1 200 OK)

Miscellaneous

Test date	Sat, 24 Oct 2026 06:21:29 UTC
Test duration	118.200 seconds
HTTP status code	200
HTTP server signature	-
Server hostname	-

Why is my certificate not trusted?

There are many reasons why a certificate may not be trusted. The exact problem is indicated on the report card in bright red. The problems fall into three categories:

1. Invalid certificate
2. Invalid configuration
3. Unknown Certificate Authority

1. Invalid certificate

A certificate is invalid if:

- It is used before its activation date
- It is used after its expiry date
- Certificate hostnames don't match the site hostname
- It has been revoked
- It has insecure signature
- It has been blacklisted

2. Invalid configuration

In some cases, the certificate chain does not contain all the necessary certificates to connect the web server certificate to one of the root certificates in our trust store. Less commonly, one of the certificates in the chain (other than the web server certificate) will have expired, and that invalidates the entire chain.

3. Unknown Certificate Authority

In order for trust to be established, we must have the root certificate of the signing Certificate Authority in our trust store. SSL Labs does not maintain its own trust store; instead we use the store maintained by Mozilla.

If we mark a web site as not trusted, that means that the average web user's browser will not trust it either. For certain special groups of users, such web sites can still be secure. For example, if you can securely verify that a self-signed web site is operated by a person you trust, then you can trust that self-signed web site too. Or, if you work for an organisation that manages its own trust, and you have their own root certificate already embedded in your browser. Such special cases do not work for the general public, however, and this is what we indicate on our report card.

4. Interoperability issues

In some rare cases trust cannot be established because of interoperability issues between our code and the code or configuration running on the server. We manually review such cases, but if you encounter such an issue please feel free to contact us. Such problems are very difficult to troubleshoot and you may be able to provide us with information that might help us determine the root cause.

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.