SSL Security Test of djs-place.freemyip.com

- ✓ Web Server SSL Test
- ✓ Email Server SSL Test
- ✓ SSL Certificate Test
- ✓ PCI DSS, HIPAA & NIST Test

Free online tool to test SSL security
171,117,085 SSL security tests performed

djs-place.freemyip.com

170 tests running **81,320** tests in 24 hours

☑ Hide from Latest Tests Provided "as is" without any warranty of any kind

Summary of djs-place.freemyip.com:443 (HTTPS) SSL Security Test

djs-place.freemyip.com was tested 3 times during the last 12 months.

Your final score: **A+**

Date/Time: Aug 6th, 2025 01:31:45 GMT-4
Source IP/Port: 71.168.136.174:443
Type: HTTPS

Refresh Test | Download Report

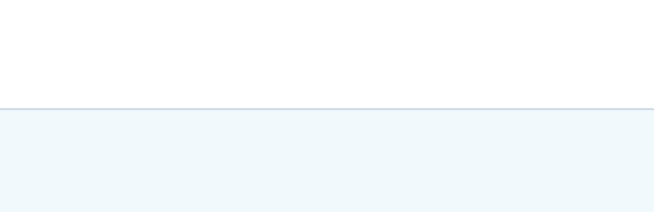
PCI DSS Compliance Test	HIPAA Compliance Test	NIST Compliance Test	Industry Best Practices	External Content Security
COMPLIANT	2 ISSUES FOUND	2 ISSUES FOUND	NO MAJOR ISSUES FOUND	NOT FOUND

The server supports the most recent and secure TLS protocol version of TLS 1.3. Good configuration

Test Certificate

Register to Download

Quality Seal



Register to Install

Discovered Subdomains

For comprehensive subdomain detection, use our ImmuniWeb Discovery product. Information

Hostname	Protocol/Port	Certificate(s)	Tested on	Compliances	Grade
freemyip.com:25	SMTP / 25	The RSA certificate is valid till Sep 14th 2025	Not tested yet	—	—
freemyip.com	IMAP / 143	Not tested yet	Nov 8th, 2019 17:52:33 GMT-5	—	F
freemyip.com	HTTPS / 443	The RSA certificate is valid till Sep 14th 2025	Nov 4th, 2024 07:11:58 GMT-5	PCI DSS	A+
freemyip.com	SMTP / 587	Not tested yet	Nov 8th, 2019 17:53:24 GMT-5	—	C+

SHOW 1 MORE

SSL Certificate Analysis

ECDSA CERTIFICATE INFORMATION

Issuer	ZeroSSL ECC Domain Secure Site CA
Trusted	Yes
Common Name	djs-place.freemyip.com
Key Type/Size	ECDSA 256 bits
Weak Key (Debian)	Secure
Serial Number	84698056177160523234602017514828127959
Signature Algorithm	ecdsa-with-SHA384 Strong
Subject Alternative Names	DNS:djs-place.freemyip.com
Transparency	Yes
Validation Level	DV
CRL	No
OCSP	http://zerossl.ocsp.sectigo.com
OCSP Must-Staple	No
Supports OCSP Stapling	No
Revocation status	Good
Valid From	August 05, 2025 00:00 CET
Valid To	November 03, 2025 23:59 CET

CERTIFICATE CHAIN

Server sends an unnecessary root certificate. Misconfiguration or weakness

Root CA	AAA Certificate Services
Type/Size	RSA 2048 bits
Serial Number	1
Signature	sha1WithRSAEncryption Strong
SHA256	7a7a0fb5d7e2731d77...782bc83ee0ea699ef4
PIN	vRU+17BDT2iGsXvOi7...LXAqjO+jGPdW7L1vM=
Expires in	1,244 days
Comment	Self-signed
Download	

Intermediate CA	USERTrust ECC Certification Authority
Type/Size	ECDSA 384 bits
Serial Number	114849002793238729640937462275813569940
Signature	sha384WithRSAEncryption Strong
SHA256	a6cf64dbb4c8d5fd19...56a87d00cbb3def3ea
PIN	ICGRfpgmOUXIWcQ/HX...FPoDyjvH7ohhQpjzs=
Expires in	1,244 days
Comment	-
Download	

Intermediate CA	ZeroSSL ECC Domain Secure Site CA
Type/Size	ECDSA 384 bits
Serial Number	47475399004980497348775734540896789736
Signature	ecdsa-with-SHA384 Strong
SHA256	1d3cb33b5005cbed04...df700884cad9ba4195
PIN	3fLLVjRIWnCqDqIETU...zmN/Z3Q/jQ8cIaAoc=
Expires in	1,638 days
Comment	-
Download	

Server certificate	djs-place.freemyip.com
Type/Size	ECDSA 256 bits
Serial Number	84698056177160523234602017514828127959
Signature	ecdsa-with-SHA384 Strong
SHA256	b82cc53fdfeff72c1d...6235195ca71729083a
PIN	XACBnFMn+/licwPvoG...lS3wM6El92ESljbUs=
Expires in	90 days
Comment	-
Download	

Root CA	USERTrust ECC Certification Authority
Type/Size	ECDSA 384 bits
Serial Number	123013823720199481456569720443997572134
Signature	ecdsa-with-SHA384 Strong
SHA256	4ff460d54b9c86dabf...aa86e06adcd2a9ad7a
PIN	ICGRfpgmOUXIWcQ/HX...FPoDyjvH7ohhQpjzs=
Expires in	4,549 days
Comment	Self-signed
Download	

PCI DSS Compliance Test of djs-place.freemyip.com

Reference: PCI DSS 4.0.1, Requirement 4.2

CERTIFICATES ARE TRUSTED

All the certificates provided by the server are trusted. Good configuration

SUPPORTED CIPHERS

List of all cipher suites supported by the server:

TLSV1.3

- TLS_CHACHA20_POLY1305_SHA256 Good configuration
- TLS_AES_256_GCM_SHA384 Good configuration
- TLS_AES_128_GCM_SHA256 Good configuration

TLSV1.2

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 Good configuration
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 Good configuration

SUPPORTED PROTOCOLS

List of all SSL/TLS protocols supported by the server:

- TLSv1.2 Good configuration
- TLSv1.3 Good configuration

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

- P-384 (secp384r1) (384 bits) Good configuration
- P-256 (prime256v1) (256 bits) Good configuration

POODLE OVER TLS

The server is not vulnerable to POODLE over TLS. Not vulnerable

GOLDENDOODLE

The server is not vulnerable to GOLDENDOODLE. Not vulnerable

ZOMBIE POODLE

The server is not vulnerable to Zombie POODLE. Not vulnerable

SLEEPING POODLE

The server is not vulnerable to Sleeping POODLE. Not vulnerable

0-LENGTH OPENSSL

The server is not vulnerable 0-Length OpenSSL. Not vulnerable

CVE-2016-2107

The server is not vulnerable to CVE-2016-2107. Not vulnerable

SERVER DOES NOT SUPPORT CLIENT-INITIATED INSECURE RENEGOTIATION

The server does not support client-initiated insecure renegotiation. Good configuration

ROBOT

The server is not vulnerable to ROBOT vulnerability. Not vulnerable

MARVIN ATTACK

The system is not vulnerable to the Marvin Attack, as no TLS_RSA cipher suites using PKCS#1 v1.5 are enabled. Not vulnerable

HEARTBLEED

The server version of OpenSSL is not vulnerable to Heartbleed attack. Not vulnerable

CVE-2014-0224

The server is not vulnerable to CCS Injection. Not vulnerable

CVE-2021-3449

The server is not vulnerable to CVE-2021-3449 (OpenSSL Maliciously Crafted Renegotiation Vulnerability). Not vulnerable

HIPAA and NIST Compliance Test

Reference: HIPAA, Security Rule (Ref. NIST SP 800-52: "Guidelines for the Selection and Use of TLS Implementations")

X.509 CERTIFICATES ARE IN VERSION 3

All the X509 certificates provided by the server are in version 3. Good configuration

SERVER DOES NOT SUPPORT OCSP STAPLING

The server is not configured to support OCSP stapling for its ECDSA certificate, which is required for enhanced verification of the certificate's revocation status. Reconfigure or upgrade your web server to enable OCSP stapling. Non-compliant with NIST guidelines

SUPPORTED CIPHERS

Consider dropping support for all non-compliant protocols. List of all cipher suites supported by the server:

TLSV1.3

- TLS_CHACHA20_POLY1305_SHA256 Non-compliant with NIST guidelines
- TLS_AES_256_GCM_SHA384 Good configuration
- TLS_AES_128_GCM_SHA256 Good configuration

TLSV1.2

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 Good configuration
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 Good configuration

SUPPORTED PROTOCOLS

List of all SSL/TLS protocols supported by the server:

- TLSv1.2 Good configuration
- TLSv1.3 Good configuration

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

- P-384 (secp384r1) (384 bits) Good configuration
- P-256 (prime256v1) (256 bits) Good configuration

EC_POINT_FORMAT EXTENSION

The server supports the EC_POINT_FORMAT TLS extension. Good configuration

Industry Best Practices Test of djs-place.freemyip.com

DNSCAA

This domain does not have a Certification Authority Authorization (CAA) record. Information

CERTIFICATES HAVE A VALIDITY PERIOD OF 398 DAYS OR LESS

All the server certificates provided have been validated for less than 398 days (13 months). Good configuration

CERTIFICATES DO NOT PROVIDE EV

The ECDSA certificate provided is NOT an Extended Validation (EV) certificate. Information

TLS 1.3 SUPPORTED

The server supports TLS 1.3 which is the only version of TLS that currently has no known flaws or exploitable weaknesses. Good configuration

TLS 1.3 EARLY DATA (0-RTT)

Server's TLS 1.3 Early Data (RFC 8446, page 17) is not enabled. Information

SERVER DOES NOT HAVE CIPHER PREFERENCE

The server does not prefer cipher suites. We advise to enable this feature in order to enforce usage of the best cipher suites selected. Misconfiguration or weakness

SERVER PREFERRED CIPHER SUITES

Preferred cipher suite for each protocol supported (except SSLv2). Expected configuration are ciphers allowed by PCI DSS and enabling PFS:

ALWAYS-ON SSL

The HTTP version of the website redirects to the HTTPS version. Good configuration

SERVER PROVIDES HSTS WITH LONG DURATION

The server provides HTTP Strict Transport Security for more than 6 months: 63072000 seconds Good configuration

HSTS PRELOAD

This domain does not support HSTS Preload, which means it may not enforce HTTPS connections strictly and could be more vulnerable to security threats like protocol downgrade attacks. Information

TLS_FALLBACK_SCSV

The server supports TLS_FALLBACK_SCSV extension for protocol downgrade attack prevention. Good configuration

SERVER DOES NOT SUPPORT CLIENT-INITIATED SECURE RENEGOTIATION

The server does not support client-initiated secure renegotiation. Good configuration

SERVER-INITIATED SECURE RENEGOTIATION

The server supports secure server-initiated renegotiation. Good configuration

SERVER DOES NOT SUPPORT TLS COMPRESSION

TLS compression is not supported by the server. Good configuration

External Content Privacy and Security Analysis

No External Content appears to be loaded by the website. Information

Need More? Upgrade to ImmuniWeb® AI Platform

Get remediation advice and ensure compliance with ImmuniWeb AI Platform:

Attack Surface Management | Web Security Scanning | Cybersecurity Compliance Services

FREE DEMO | ASK A QUESTION

Why Choosing ImmuniWeb® AI Platform

Feel the difference. Get the results.

Reduce Complexity
All-in-one platform for 20 synergized use cases
LEARN MORE

Optimize Costs
All-in-one model & AI automation reduce costs by up to 90%
LEARN MORE

Validate Compliance
Letter of conformity from law firm confirming your compliance
LEARN MORE

The award-winning ImmuniWeb® AI Platform helps over 1,000 companies from over 50 countries to test, secure and protect their web and mobile applications, APIs and microservices, cloud and networks, to prevent data breaches and reduce third-party risk, and to comply with regulatory requirements.

Use Cases
API Penetration Testing
API Security Scanning
Attack Surface Management
Cloud Penetration Testing
Cloud Security Posture Management
Continuous Automated Red Teaming
Continuous Breach & Attack Simulation
Continuous Penetration Testing
Continuous Threat Exposure Management
Cyber Threat Intelligence
Dark Web Monitoring
Mobile Penetration Testing
Mobile Security Scanning
Network Security Assessment
Penetration Testing-as-a-Service
Phishing Websites Takedown
Third-Party Risk Management
Threat-Led Penetration Testing
Web Penetration Testing
Web Security Scanning

ImmuniWeb® AI Platform
ImmuniWeb® Discovery
ImmuniWeb® Neuron
ImmuniWeb® Neuron Mobile
ImmuniWeb® On-Demand
ImmuniWeb® MobileSuite
ImmuniWeb® Continuous
Customer Success
Integrations

Community Edition Free
Email Security Test
Website Security Test
Website Privacy Test
SSL Security Test
Mobile App Security Test
Dark Web Exposure Test
Cloud Security Test

Partners
Partner Program
Partner Directory
Partner Portal

Resources
Cybersecurity Webinars
Cybercrime Investigations Weekly
Application Penetration Testing
Automated Penetration Testing
Attack Surface Management
Dark Web Monitoring
Ecommerce Security
CWE Knowledge Base
Security Advisories

OWASP Top 10
Broken Access Control
Cryptographic Failures
Injection
Insecure Design
Security Misconfiguration
Vulnerable and Outdated Components
Identification and Authentication Failures
Software and Data Integrity Failures
Security Logging and Monitoring Failures
Server-Side Request Forgery

Compliance Services
EU & UK GDPR
Singapore PDPA
Hong Kong PDPO
South Africa POPIA
Brazil LGPD
HIPAA / HITECH
FTCA, GLBA, FCRA / FACTA
NIST SP 800, FISMA, CMMC
New York SHIELD, NYDFS
California CCPA, CPRA
ISO 27001 / ISO 27002
Singapore MAS
PCI DSS

Newsletter
Join our 58,969 subscribers:

Geneva HQ
+41 22 560 6800
sales@immuniweb.com
Quai de l'Ile 13
Geneva, CH-1204
Switzerland

London
+44 20 4534 7678
sales@immuniweb.com
4/4a Bloomsbury Square
London WC1A 2RP
United Kingdom

Washington, D.C.
+1 720 605 9147
sales@immuniweb.com
1500 K Street, 2nd Floor
Washington, D.C. 20005
United States

Dubai
+971 04 291 2320
sales@immuniweb.com
8th Floor, Sheikh Rashid Tower
DWTC, Sheikh Zayed Rd, Dubai
United Arab Emirates

Copyright © 2025 ImmuniWeb SA | Terms of Use | Privacy Policy