

Website configuration

Subscore 93

DNS

90

- **Name servers** Required
2 name servers are configured, 2 of them reachable over IPv6.
- **IPv4 address** Required
The domain resolves to 1 IPv4 address(es), e.g. 20.101.251.232.
- **IPv6 address** Recommended · Low
The domain has no AAAA (IPv6) record.
[Recommendation: Add an AAAA record so IPv6-only clients can reach the site.](#)
- **MX records** Optional
2 mail server(s) (MX) are configured for the domain.
- **CAA record** Recommended · Low
No CAA record is configured.
[Recommendation: Add a CAA record listing your certificate authority.](#)
- **DNSSEC** Recommended
DNSSEC is enabled and the validation chain is intact.

DNS servers

100

- **DNS response** Required
The domain's nameservers deliver DNS responses.
- **Nameserver redundancy** Required
The domain has 2 nameservers.
- **Nameservers responding** Required
All 2 nameservers respond to queries.
- **Authoritative answers** Required
All nameservers answer authoritatively for the zone.
- **SOA serial in sync** Recommended
All nameservers report the same SOA serial number.
- **Open recursion** Required
No nameserver answers recursive queries for foreign domains.
- **Public NS addresses** Required
All nameserver addresses are publicly reachable.
- **Network dispersion** Recommended
The nameservers are spread across 4 different networks.
- **Nameservers over IPv6** Recommended
2 nameservers are reachable over IPv6.
- **SOA refresh** Recommended
The SOA refresh value (28800) is within the recommended range.
- **SOA retry** Recommended
The SOA retry value (7200) is within the recommended range.
- **SOA expire** Recommended
The SOA expire value (1209600) is within the recommended range.

- **SOA minimum TTL** Recommended
The SOA minimum TTL value (86400) is within the recommended range.
- **SOA serial format** Optional
The SOA serial (2019107449) is a valid, increasing integer (as used by many managed-DNS providers).
- **NS match with parent** Recommended
The zone's NS records match the delegation at the parent.
- **Glue records** Recommended
No glue records are needed (no nameservers inside the zone itself).
- **Primary listed at parent** Recommended
The primary nameserver (udns1.cscudns.com) is included in the parent delegation.

HTTP / Security Headers

85

- **Reachability** Required
The site is reachable over HTTPS.
- **IPv6 reachability** Recommended · Low
The domain has no AAAA record, so the web server is not reachable over IPv6.
[Recommendation: Publish an AAAA record and make sure the web server accepts IPv6 connections on port 443.](#)
- **Same website over IPv6** Recommended · Info
The domain has no AAAA record — no IPv6/IPv4 comparison applies.
- **HTTPS redirect** Recommended
Plain HTTP is redirected to HTTPS.
- **HSTS** Recommended
Your web server sends an HSTS policy.
- **Content-Security-Policy** Recommended
A Content-Security-Policy header is set.
- **X-Frame-Options** Recommended
An X-Frame-Options header is set.
- **X-Content-Type-Options** Recommended
The X-Content-Type-Options header is set to nosniff.
- **Referrer-Policy** Recommended
A Referrer-Policy header is set.
- **HTTP compression** Optional
HTTP compression (gzip) is active — a performance plus.
- **security.txt** Recommended · Low
No security.txt file is published.
[Recommendation: Publish a signed `/well-known/security.txt` with at least a `Contact:` and an `Expires:` field.](#)
- **HTTP/2** Recommended
The web server supports HTTP/2.
- **HTTP/3** Optional · Info
The web server does not advertise HTTP/3 (QUIC).
[Recommendation: Optional: enable HTTP/3 in your web server/reverse proxy and make sure UDP port 443 is open in the firewall.](#)
- **Cookie security** Recommended · Low
1 of 1 cookie(s) are missing important security flags.
[Recommendation: Set sensitive cookies with `Secure`, `HttpOnly` and an appropriate `SameSite` value \(`Lax` or `Strict`\). `SameSite=None` only makes sense with `Secure` and only for deliberately cross-site cookies.](#)
- **Mixed content** Required
The page loads no resources over unencrypted HTTP.
- **Subresource integrity** Recommended · Info
The page loads no external scripts/stylesheets where SRI would be relevant.

RPKI

100

- **RPKI (web server)** Recommended
The route-origin authorisation of the web server is RPKI-valid.
- **RPKI (nameservers)** Recommended
The route-origin authorisation of the nameservers is RPKI-valid.

TLS

95

- **HTTPS reachable** Required
An HTTPS service is reachable and completed a TLS handshake.
- **TLS versions** Required
Only modern TLS versions (1.2 and/or 1.3) are offered.
- **Cipher suite** Required
The negotiated cipher suite (TLS_AES_128_GCM_SHA256) provides forward secrecy.
- **Certificate** Required
The certificate is trusted and valid for this host.
- **Certificate key** Required
The certificate uses a strong RSA key (4096 bits).
- **Certificate signature** Required
The certificate uses a secure signature algorithm (SHA256-RSA).
- **OCSP stapling** Recommended · Low
The server does not staple an OCSP response.
[Recommendation: Enable OCSP stapling on the web server.](#)
- **DANE (HTTPS)** Optional · Info
No DANE (TLSA) records are published for HTTPS — an optional bonus for the web, not a shortcoming.
- **Cipher order** Recommended
With TLS 1.3 the server chooses from a small set of uniformly strong suites — ordering is not a concern.
- **Key exchange** Required
The key exchange uses ECDHE with hash SHA256 — forward secrecy is provided.
- **TLS compression** Required
TLS 1.3 has no record compression — the weakness does not apply.
- **Renegotiation** Required
TLS 1.3 removed renegotiation entirely — no attack surface.
- **Extended Master Secret** Recommended
TLS 1.3's key schedule supersedes Extended Master Secret — the weakness does not apply.
- **TLS 1.3 0-RTT (early data)** Optional
The server does not accept 0-RTT — the safest default.

Mail configuration

Subscore **67**

Mail

28

- **Mail servers (MX)** Required
The domain has 2 mail server(s) (MX).
- **SPF** Recommended · Medium
No SPF record is published.
[Recommendation: Publish an SPF record that lists your legitimate senders and ends in `-all` \(hard fail\). Keep the number of DNS lookups within the limit of ten.](#)
- **DKIM** Recommended
DKIM is set up: the domain's `\_domainkey` namespace contains selectors — the individual selector names cannot be enumerated from DNS.

- **DMARC** Recommended
A DMARC record with an enforcing policy (p=reject) is published.
- **BIMI** Optional · Info
The domain does not publish a BIMI record.
Recommendation: Optional: publish an SVG logo (SVG Tiny PS) at an HTTPS URL and a TXT record `default.\_bimi.<domain>` with `v=BIMI1; l=<logo URL>`. An enforcing DMARC policy (`p=quarantine` or `p=reject`) is required; some providers additionally require a paid VMC certificate.
- **MTA-STS** Recommended · Low
The domain publishes no MTA-STS policy.
Recommendation: Publish the TXT record `\_mta-sts.<domain>` plus a valid policy file at `https://mta-sts.<domain>/well-known/mta-sts.txt` with `version`, `mode`, `max\_age` and your `mx` entries. Start with `mode: testing` and switch to `mode: enforce` after reviewing the reports.
- **TLS-RPT** Optional · Low
The domain publishes no TLS-RPT record.
Recommendation: Publish a TXT record `\_smtp.\_tls.<domain>` with `v=TLSRPTv1; rua=mailto:tls-reports@<domain>` (or an HTTPS reporting URL).
- **MX over IPv6** Recommended · Low
No mail server has an IPv6 address.
Recommendation: Publish AAAA records for your MX hosts and make sure they accept SMTP over IPv6.
- **STARTTLS** Required
All mail servers offer STARTTLS with a valid certificate.
- **Mail TLS version** Required
All mail servers negotiate a modern TLS version (1.2 or 1.3).
- **DANE (SMTP)** Recommended · Low
No DANE (TLSA) records are published for the mail servers.
Recommendation: With DNSSEC in place, publish TLSA records at `\_25.\_tcp.<mx>` that match each mail server's certificate, and rotate them together with the certificate.
- **Cipher suite (mail)** Recommended
All mail servers use cipher suites with forward secrecy.
- **Mail server certificate** Required
All mail servers present a valid certificate matching the hostname.
- **Mail server key** Required
The certificate keys of all mail servers are sufficiently strong.
- **Mail server signature** Required
The certificates of all mail servers use a secure signature.
- **TLS compression (mail)** Required
No mail server has TLS compression enabled.
- **Renegotiation (mail)** Required
All mail servers support secure renegotiation or use TLS 1.3.
- **Extended Master Secret (mail)** Recommended
All mail servers support Extended Master Secret or use TLS 1.3.
- **Reverse DNS (PTR)** Recommended
All checked mail server IPs have a PTR record.
- **Open relay** Required · Critical
2 mail server(s) accepted relaying to a foreign destination (open relay).
Recommendation: Configure your mail server to allow relaying only for authenticated users or your own domains (`smtpd\_relay\_restrictions` in Postfix, etc.) and to reject foreign recipients without authentication.

Blacklist

- **Spamhaus ZEN** Required
Not listed on Spamhaus ZEN (zen.spamhaus.org).

100

- **Spamhaus DBL** Required
Not listed on Spamhaus DBL (dbl.spamhaus.org).
- **Barracuda** Required
Not listed on Barracuda (b.barracudacentral.org).
- **SpamCop** Required
Not listed on SpamCop (bl.spamcop.net).
- **PSBL** Required
Not listed on PSBL (psbl.surriel.com).
- **OSPAM** Required
Not listed on OSPAM (bl.ospam.org).
- **BLOCKLIST.DE** Required
Not listed on BLOCKLIST.DE (bl.blocklist.de).
- **SURBL multi** Recommended
Not listed on SURBL multi (multi.surbl.org).
- **SEM FRESH** Recommended
Not listed on SEM FRESH (fresh.spameatingmonkey.net).
- **SEM Blacklist** Recommended
Not listed on SEM Blacklist (bl.spameatingmonkey.net).
- **SEM Backscatter** Recommended
Not listed on SEM Backscatter (backscatter.spameatingmonkey.net).
- **SPFBL** Recommended
Not listed on SPFBL (dnsbl.spfbl.net).
- **GBUdb Truncate** Recommended
Not listed on GBUdb Truncate (truncate.gbudb.net).
- **SpamRATS RATS-Spam** Recommended
Not listed on SpamRATS RATS-Spam (spam.spamrats.com).
- **SpamRATS RATS-Dyna** Recommended
Not listed on SpamRATS RATS-Dyna (dyna.spamrats.com).
- **SpamRATS RATS-NoPtr** Recommended
Not listed on SpamRATS RATS-NoPtr (nptr.spamrats.com).
- **JustSpam** Recommended
Not listed on JustSpam (dnsbl.justspam.org).
- **Fabel Spamsources** Recommended
Not listed on Fabel Spamsources (spamsources.fabel.dk).
- **s5h.net** Recommended
Not listed on s5h.net (all.s5h.net).
- **DroneBL** Recommended
Not listed on DroneBL (dnsbl.dronebl.org).
- **InterServer RBL** Recommended
Not listed on InterServer RBL (rbl.interserver.net).
- **Mailspike** Recommended
Not listed on Mailspike (z.mailspike.net).
- **UCEPROTECT Level 1** Recommended
Not listed on UCEPROTECT Level 1 (dnsbl-1.uceprotect.net).
- **UCEPROTECT Level 2** Optional
Not listed on UCEPROTECT Level 2 (dnsbl-2.uceprotect.net).
- **UCEPROTECT Level 3** Optional
Not listed on UCEPROTECT Level 3 (dnsbl-3.uceprotect.net).

RPKI (mail)

- **RPKI (mail servers)** Recommended

The route-origin authorisation of the mail servers is RPKI-valid.