

Website-Konfiguration

Subscore 86

DNS

83

- **Nameserver** Erforderlich
2 Nameserver sind konfiguriert, 2 davon über IPv6 erreichbar.
- **IPv4-Adresse** Erforderlich
Die Domain löst auf 2 IPv4-Adresse(n) auf, z. B. 104.18.20.211.
- **IPv6-Adresse** Empfohlen
Die Domain löst auf 2 IPv6-Adresse(n) auf, z. B. 2606:4700::6812:14d3.
- **MX-Records** Optional
Für die Domain sind 1 Mail Server (MX) konfiguriert.
- **CAA-Record** Empfohlen · Niedrig
Es ist kein CAA-Record konfiguriert.
[Empfehlung: Ergänzen Sie einen CAA-Record mit Ihrer Zertifizierungsstelle.](#)
- **DNSSEC** Empfohlen · Mittel
DNSSEC ist für diese Domain nicht aktiviert.
[Empfehlung: Aktivieren Sie DNSSEC bei Ihrem DNS-Betreiber und veröffentlichen Sie den DS-Record beim Registrar; reparieren Sie eine gebrochene Kette.](#)

DNS Server

100

- **DNS-Antwort** Erforderlich
Die Nameserver der Domain liefern DNS-Antworten.
- **Nameserver-Redundanz** Erforderlich
Die Domain hat 2 Nameserver.
- **Nameserver antworten** Erforderlich
Alle 2 Nameserver antworten auf Anfragen.
- **Autoritative Antworten** Erforderlich
Alle Nameserver antworten autoritativ für die Zone.
- **SOA-Serial synchron** Empfohlen
Alle Nameserver melden dieselbe SOA-Seriennummer.
- **Offene Rekursion** Erforderlich
Kein Nameserver beantwortet rekursive Anfragen für fremde Domains.
- **Öffentliche NS-Adressen** Erforderlich
Alle Nameserver-Adressen sind öffentlich erreichbar.
- **Netz-Streuung** Empfohlen
Die Nameserver verteilen sich auf 4 unterschiedliche Netze.
- **Nameserver über IPv6** Empfohlen
2 Nameserver sind über IPv6 erreichbar.
- **SOA Refresh** Empfohlen
Der SOA-Refresh-Wert (10800) liegt im empfohlenen Bereich.
- **SOA Retry** Empfohlen
Der SOA-Retry-Wert (3600) liegt im empfohlenen Bereich.
- **SOA Expire** Empfohlen
Der SOA-Expire-Wert (604800) liegt im empfohlenen Bereich.

- **SOA Minimum TTL** Empfohlen
Der SOA-Minimum-TTL-Wert (3600) liegt im empfohlenen Bereich.
- **SOA-Serial-Format** Optional
Die SOA-Seriennummer (2026072406) folgt der üblichen Konvention (JJJJMMTTnn).
- **NS-Abgleich mit Parent** Empfohlen
Die NS-Records der Zone stimmen mit der Delegation beim Parent überein.
- **Glue-Records** Empfohlen
Es werden keine Glue-Records benötigt (keine Nameserver innerhalb der eigenen Zone).
- **Primary beim Parent gelistet** Empfohlen
Der primäre Nameserver (ns0105.secondary.cloudflare.com) ist in der Parent-Delegation enthalten.

HTTP / Security-Header

61

- **Erreichbarkeit** Erforderlich
Die Seite ist über HTTPS erreichbar.
- **IPv6-Erreichbarkeit** Empfohlen
Der Webserver ist über IPv6 erreichbar (2606:4700::6812:14d3).
- **Gleiche Website über IPv6** Empfohlen
IPv6 und IPv4 liefern dieselbe Website aus (Textähnlichkeit 100%).
- **HTTPS-Redirect** Empfohlen
Einfaches HTTP wird auf HTTPS umgeleitet.
- **HSTS** Empfohlen · Mittel
Ihr Webserver sendet keine HSTS-Richtlinie.
Empfehlung: HSTS setzt voraus, dass Ihre Website vollständig über HTTPS funktioniert – inklusive eines gültigen Zertifikats einer öffentlich vertrauenswürdigen Zertifizierungsstelle. Gehen Sie schrittweise vor:
 1. Stellen Sie sicher, dass Ihre Website jetzt und dauerhaft vollständig über HTTPS funktioniert (z. B. mit einem verlässlichen Zertifikats-Rollover-Prozess).
 2. Erhöhen Sie die HSTS-Gültigkeitsdauer stufenweise. Prüfen Sie nach jeder Stufe auf Erreichbarkeitsprobleme und warten Sie die volle `max-age`-Dauer ab, bevor Sie zur nächsten Stufe wechseln.
 3. Wiederholen Sie Schritt 1–2 für jede Subdomain, die Sie absichern möchten. Nutzen Sie `includeSubDomains` nur, wenn wirklich alle (verschachtelten) Subdomains HTTPS zuverlässig unterstützen.
 4. Nutzen Sie `preload` nur mit grosser Vorsicht — es ist schwer rückgängig zu machen und kann die Erreichbarkeit der gesamten Domain samt Subdomains beeinträchtigen.
- **Content-Security-Policy** Empfohlen · Mittel
Es ist kein Content-Security-Policy-Header gesetzt.
Empfehlung: Definieren Sie eine Content-Security-Policy, die nur die tatsächlich benötigten Quellen erlaubt.
- **X-Frame-Options** Empfohlen
Ein X-Frame-Options-Header ist gesetzt.
- **X-Content-Type-Options** Empfohlen
Der X-Content-Type-Options-Header ist auf nosniff gesetzt.
- **Referrer-Policy** Empfohlen · Niedrig
Es ist kein Referrer-Policy-Header gesetzt.
Empfehlung: Senden Sie eine Referrer-Policy wie strict-origin-when-cross-origin oder no-referrer.
- **HTTP-Kompression** Optional
HTTP-Kompression (gzip) ist aktiv – ein Performance-Pluspunkt.
- **security.txt** Empfohlen · Niedrig
Es ist eine security.txt veröffentlicht, ihr fehlt aber ein Contact-Feld.
Empfehlung: Veröffentlichen Sie eine signierte `.well-known/security.txt` mit mindestens einem `Contact:`- und einem `Expires:`-Feld.
- **HTTP/2** Empfohlen
Der Webserver unterstützt HTTP/2.

- **HTTP/3** Optional · Info
Der Webserver kündigt kein HTTP/3 (QUIC) an.
Empfehlung: Optional: Aktivieren Sie HTTP/3 in Ihrem Webserver/Reverse Proxy und stellen Sie sicher, dass UDP-Port 443 in der Firewall geöffnet ist.
- **Cookie-Sicherheit** Empfohlen · Niedrig
1 von 1 Cookie(s) fehlen wichtige Sicherheits-Flags.
Empfehlung: Setzen Sie sensible Cookies mit `Secure`, `HttpOnly` und einem passenden `SameSite`-Wert (`Lax` oder `Strict`).
`SameSite=None` ist nur mit `Secure` und nur für bewusst seitenübergreifende Cookies sinnvoll.
- **Mixed Content** Erforderlich
Die Seite bindet keine Ressourcen über unverschlüsseltes HTTP ein.
- **Subresource Integrity** Empfohlen · Info
Die Seite bindet keine externen Skripte/Stylesheets ein, für die SRI sinnvoll wäre.

RPKI

100

- **RPKI (Webserver)** Empfohlen
Die Route-Origin-Autorisierung des Webserver ist per RPKI gültig.
- **RPKI (Nameserver)** Empfohlen
Die Route-Origin-Autorisierung der Nameserver ist per RPKI gültig.

TLS

100

- **HTTPS erreichbar** Erforderlich
Ein HTTPS-Dienst ist erreichbar und hat einen TLS-Handshake abgeschlossen.
- **TLS-Versionen** Erforderlich
Es werden nur moderne TLS-Versionen (1.2 und/oder 1.3) angeboten.
- **Cipher Suite** Erforderlich
Die ausgehandelte Cipher Suite (TLS_AES_128_GCM_SHA256) bietet Forward Secrecy.
- **Zertifikat** Erforderlich
Das Zertifikat ist vertrauenswürdig und für diesen Host gültig.
- **Zertifikatsschlüssel** Erforderlich
Das Zertifikat verwendet einen starken RSA-Schlüssel (2048 Bit).
- **Zertifikatssignatur** Erforderlich
Das Zertifikat verwendet einen sicheren Signaturalgorithmus (SHA256-RSA).
- **OCSP-Stapling** Empfohlen
Der Server liefert eine OCSP-Antwort per Stapling mit.
- **DANE (HTTPS)** Optional · Info
Für HTTPS sind keine DANE-(TLSA-)Records veröffentlicht – für Web ein optionaler Bonus, kein Mangel.
- **Cipher-Reihenfolge** Empfohlen
Mit TLS 1.3 wählt der Server aus einem kleinen Satz durchweg sicherer Verfahren – die Reihenfolge ist unkritisch.
- **Key Exchange** Erforderlich
Der Schlüsselaustausch nutzt ECDHE mit Hash SHA256 – Forward Secrecy ist gegeben.
- **TLS-Kompression** Erforderlich
TLS 1.3 kennt keine Record-Kompression – die Schwachstelle entfällt.
- **Renegotiation** Erforderlich
TLS 1.3 hat Renegotiation vollständig entfernt – kein Angriffsvektor.
- **Extended Master Secret** Empfohlen
Der Schlüsselplan von TLS 1.3 ersetzt Extended Master Secret – die Schwäche entfällt.
- **TLS 1.3 0-RTT (Early Data)** Optional
Der Server akzeptiert kein 0-RTT – die sicherste Voreinstellung.

Mail-Konfiguration

Subscore 90

Mail

- **Mail Server (MX)** Erforderlich
Die Domain hat 1 Mail Server (MX).
- **SPF** Empfohlen · Mittel
Es ist kein SPF-Record veröffentlicht.
[Empfehlung: Veröffentlichen Sie einen SPF-Record, der Ihre legitimen Absender auflistet und mit `all` \(Hard Fail\) endet. Halten Sie die Zahl der DNS-Lookups unter dem Limit von zehn.](#)
- **DKIM** Empfohlen
DKIM ist eingerichtet, der Schlüssel ist mit 1024 bit aber nur knapp ausreichend.
- **DMARC** Empfohlen
Es ist ein DMARC-Record mit durchsetzender Policy (p=reject) veröffentlicht.
- **BIMI** Optional · Info
Die Domain veröffentlicht keinen BIMI-Record.
[Empfehlung: Optional: Veröffentlichen Sie ein SVG-Logo \(SVG Tiny PS\) unter einer HTTPS-URL und einen TXT-Record `default.\\_bimi.<domain>` mit `v=BIMI1;I=<Logo-URL>`. Voraussetzung ist eine DMARC-Policy `p=quarantine` oder `p=reject`; für einige Anbieter zusätzlich ein kostenpflichtiges VMC-Zertifikat.](#)
- **MTA-STS** Empfohlen · Niedrig
Die Domain veröffentlicht keine MTA-STS-Policy.
[Empfehlung: Veröffentlichen Sie den TXT-Record `\\_mta-sts.<domain>` sowie eine gültige Policy-Datei unter `https://mta-sts.<domain>/.well-known/mta-sts.txt` mit `version`, `mode`, `max\\_age` und Ihren `mx`-Einträgen. Beginnen Sie mit `mode: testing` und wechseln Sie nach Prüfung der Reports auf `mode: enforce`.](#)
- **TLS-RPT** Optional
Die Domain veröffentlicht einen gültigen TLS-RPT-Record.
- **MX über IPv6** Empfohlen
Alle Mail Server haben eine IPv6-Adresse.
- **STARTTLS** Erforderlich
Alle Mail Server bieten STARTTLS mit gültigem Zertifikat.
- **Mail-TLS-Version** Erforderlich
Alle Mail Server handeln eine moderne TLS-Version aus (1.2 oder 1.3).
- **DANE (SMTP)** Empfohlen · Niedrig
Für die Mail Server sind keine DANE-(TLSA-)Records veröffentlicht.
[Empfehlung: Veröffentlichen Sie bei aktivem DNSSEC TLSA-Records unter `\\_25.\\_tcp.<mx>`, die zum Zertifikat jedes Mail Servers passen, und rotieren Sie sie gemeinsam mit dem Zertifikat.](#)
- **Cipher Suite (Mail)** Empfohlen
Alle Mailserver nutzen Cipher Suites mit Forward Secrecy.
- **Mailserver-Zertifikat** Erforderlich
Alle Mailserver präsentieren ein gültiges, zum Hostnamen passendes Zertifikat.
- **Mailserver-Schlüssel** Erforderlich
Die Zertifikatsschlüssel aller Mailserver sind ausreichend stark.
- **Mailserver-Signatur** Erforderlich
Die Zertifikate aller Mailserver verwenden eine sichere Signatur.
- **TLS-Kompression (Mail)** Erforderlich
Kein Mailserver hat TLS-Kompression aktiviert.
- **Renegotiation (Mail)** Erforderlich
Alle Mailserver unterstützen sichere Renegotiation bzw. nutzen TLS 1.3.
- **Extended Master Secret (Mail)** Empfohlen
Alle Mailserver unterstützen Extended Master Secret bzw. nutzen TLS 1.3.
- **Reverse DNS (PTR)** Empfohlen
Alle geprüften Mailserver-IPs haben einen PTR-Record.

- **Open Relay** Erforderlich
Kein Mailserver nimmt Mail an fremde Empfänger zur Weiterleitung an (kein Open Relay).

Blacklist

100

- **Spamhaus ZEN** Erforderlich
Nicht auf Spamhaus ZEN gelistet (zen.spamhaus.org).
- **Spamhaus DBL** Erforderlich · Info
Spamhaus DBL (dbl.spamhaus.org) konnte von unserem Standort aus nicht zuverlässig abgefragt werden.
- **Barracuda** Erforderlich
Nicht auf Barracuda gelistet (b.barracudacentral.org).
- **SpamCop** Erforderlich
Nicht auf SpamCop gelistet (bl.spamcop.net).
- **PSBL** Erforderlich
Nicht auf PSBL gelistet (psbl.surriel.com).
- **OSPAM** Erforderlich
Nicht auf OSPAM gelistet (bl.ospam.org).
- **BLOCKLIST.DE** Erforderlich
Nicht auf BLOCKLIST.DE gelistet (bl.blocklist.de).
- **SURBL multi** Empfohlen
Nicht auf SURBL multi gelistet (multi.surbl.org).
- **SEM FRESH** Empfohlen
Nicht auf SEM FRESH gelistet (fresh.spameatingmonkey.net).
- **SEM Blacklist** Empfohlen
Nicht auf SEM Blacklist gelistet (bl.spameatingmonkey.net).
- **SEM Backscatter** Empfohlen
Nicht auf SEM Backscatter gelistet (backscatter.spameatingmonkey.net).
- **SPFBL** Empfohlen
Nicht auf SPFBL gelistet (dnsbl.spfbl.net).
- **GBUdb Truncate** Empfohlen
Nicht auf GBUdb Truncate gelistet (truncate.gbudb.net).
- **SpamRATS RATS-Spam** Empfohlen
Nicht auf SpamRATS RATS-Spam gelistet (spam.spamrats.com).
- **SpamRATS RATS-Dyna** Empfohlen
Nicht auf SpamRATS RATS-Dyna gelistet (dyna.spamrats.com).
- **SpamRATS RATS-NoPtr** Empfohlen
Nicht auf SpamRATS RATS-NoPtr gelistet (noptr.spamrats.com).
- **JustSpam** Empfohlen
Nicht auf JustSpam gelistet (dnsbl.justspam.org).
- **Fabel Spamsources** Empfohlen
Nicht auf Fabel Spamsources gelistet (spamsources.fabel.dk).
- **s5h.net** Empfohlen
Nicht auf s5h.net gelistet (all.s5h.net).
- **DroneBL** Empfohlen
Nicht auf DroneBL gelistet (dnsbl.dronebl.org).
- **InterServer RBL** Empfohlen
Nicht auf InterServer RBL gelistet (rbl.interserver.net).
- **Mailspike** Empfohlen
Nicht auf Mailspike gelistet (z.mailspike.net).

- **UCEPROTECT Level 1** Empfohlen
Nicht auf UCEPROTECT Level 1 gelistet (dnsbl-1.uceprotect.net).
- **UCEPROTECT Level 2** Optional
Nicht auf UCEPROTECT Level 2 gelistet (dnsbl-2.uceprotect.net).
- **UCEPROTECT Level 3** Optional
Nicht auf UCEPROTECT Level 3 gelistet (dnsbl-3.uceprotect.net).

RPKI (Mail)

100

- **RPKI (Mailserver)** Empfohlen
Die Route-Origin-Autorisierung der Mailserver ist per RPKI gültig.