Checkvanta

swiss.com

Security and configuration report

Generated on: 25/07/2026, 14:24:38 UTC

81
Overall score

Website configuration

Subscore **88**

DNS

73

- **Name servers** Required · Low
  2 name servers are configured, but none is reachable over IPv6.
  Recommendation: Configure at least two name servers and make sure they are also reachable over IPv6.
- **IPv4 address** Required
  The domain resolves to 1 IPv4 address(es), e.g. 146.216.3.74.
- **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 · Medium
  DNSSEC is not enabled for this domain.
  Recommendation: Enable DNSSEC at your DNS operator and publish the DS record at your registrar; fix any broken chain.

DNS servers

88

- **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 2 different networks.
- **Nameservers over IPv6** Recommended · Medium
  No nameserver of the domain has an IPv6 address (AAAA).
  Recommendation: Make sure at least two nameservers have an AAAA record and answer DNS queries over IPv6 on port 53.
- **SOA refresh** Recommended
  The SOA refresh value (14400) is within the recommended range.
- **SOA retry** Recommended
  The SOA retry value (1800) 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 (900) is within the recommended range.
- **SOA serial format** Optional
  The SOA serial number (2026072401) follows the common convention (YYYYMMDDnn).
- **NS match with parent** Recommended
  The zone's NS records match the delegation at the parent.
- **Glue records** Recommended
  The glue records at the parent match the nameservers' actual addresses.
- **Primary listed at parent** Recommended
  The primary nameserver (ns1.swiss.com) is included in the parent delegation.

HTTP / Security Headers 90

- **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
  A security.txt file with a contact address is published.
- **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 95

- **RPKI (web server)** Recommended · Low
  No RPKI authorisation (ROA) exists for the IP addresses of the web server.
  Recommendation: Publish a ROA (Route Origin Authorisation) for the IP prefixes of the web server with your network operator or RIR, authorising the correct announcing ASN and maximum prefix length. For an "invalid" result, check the ASN and max prefix length in the existing ROA.
- **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_ECDHE_RSA_WITH_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
  The server enforces its own cipher-suite order.
- **Key exchange** Required
  The key exchange uses ECDHE with hash SHA256 — forward secrecy is provided.
- **TLS compression** Required
  TLS compression is disabled.
- **Renegotiation** Required
  The server supports secure renegotiation and rejects client-initiated renegotiation.
- **Extended Master Secret** Recommended
  The server supports Extended Master Secret (RFC 7627).
- **TLS 1.3 0-RTT (early data)** Optional · Info
  The server does not use TLS 1.3, so 0-RTT does not apply.

Mail configuration

Subscore 65

Mail 23

- **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 · Low
  1 of 2 mail server IPs are missing a PTR record.
  Recommendation: Have the IP owner (host/provider) create a PTR record pointing to your mail server's hostname — ideally with a matching forward record (A/AAAA) back to the same IP.

- **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 100

- **Spamhaus ZEN** Required
  Not listed on Spamhaus ZEN (zen.spamhaus.org).
- **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).
- **0SPAM** Required
  Not listed on 0SPAM (bl.0spam.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 (noptr.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) 100

- **RPKI (mail servers)** Recommended
  The route-origin authorisation of the mail servers is RPKI-valid.