Checkvanta

# watson.ch

Security and configuration report

Generated on: 25/07/2026, 04:15:30 UTC

87
Overall score

## Website configuration

Subscore 84

### DNS

83

- **Name servers** Required
  4 name servers are configured, 4 of them reachable over IPv6.
- **IPv4 address** Required
  The domain resolves to 4 IPv4 address(es), e.g. 51.89.11.70.
- **IPv6 address** Recommended
  The domain resolves to 4 IPv6 address(es), e.g. 2a01:4f8:2b02:24b::2.
- **MX records** Optional
  5 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

100

- **DNS response** Required
  The domain's nameservers deliver DNS responses.
- **Nameserver redundancy** Required
  The domain has 4 nameservers.
- **Nameservers responding** Required
  All 4 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 8 different networks.
- **SOA refresh** Recommended
  The SOA refresh value (3600) is within the recommended range.
- **SOA retry** Recommended
  The SOA retry value (900) 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 (300) is within the recommended range.

- **SOA serial format** Optional · Low
  The SOA serial number (1782891088) does not follow the common convention (YYYYMMDDnn).
  Recommendation: If you maintain the zone yourself: use the YYYYMMDDnn format and increment the serial on every change.
- **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 (dns1.watson.ch) is included in the parent delegation.

## HTTP / Security Headers 61

- **Reachability** Required
  The site is reachable over HTTPS.
- **IPv6 reachability** Recommended
  The web server is reachable over IPv6 (2a01:4f8:2b02:eaf::2).
- **HTTPS redirect** Recommended
  Plain HTTP is redirected to HTTPS.
- **HSTS** Recommended · Medium
  Your web server does not send an HSTS policy.
  Recommendation: HSTS requires that your site works fully over HTTPS, including a valid certificate from a publicly trusted authority. Proceed step by step:

  1. Make sure your site works fully over HTTPS now and permanently (e.g. with a reliable certificate-rollover process).
  2. Raise the HSTS lifetime gradually. After each step, check carefully for reachability problems and wait out the full `max-age` before moving to the next.
  3. Repeat steps 1–2 for every subdomain you want to protect. Only use `includeSubDomains` once you are sure that all (nested) subdomains support HTTPS reliably.
  4. Use `preload` only with great care — it is hard to undo and can break reachability of the whole domain and its subdomains.
- **Content-Security-Policy** Recommended · Medium
  No Content-Security-Policy header is set.
  Recommendation: Define a Content-Security-Policy that only allows the sources your site actually needs.
- **X-Frame-Options** Recommended · Low
  No X-Frame-Options header is set.
  Recommendation: Send X-Frame-Options: DENY or SAMEORIGIN, or an equivalent frame-ancestors CSP directive.
- **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 · Low
  HTTP compression (gzip) is active — a performance plus.
  Recommendation: Enable HTTP compression (gzip or Brotli) for text responses to improve load time and bandwidth.
- **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
  The web server advertises HTTP/3 (QUIC) via the Alt-Svc header.
- **Cookie security** Recommended · Info
  The homepage sets no cookies that could be assessed.
- **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 90

- **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 (3072 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 · Low
  No DANE (TLSA) records are published for HTTPS.
  Recommendation: With DNSSEC in place, publish TLSA records at `_443._tcp.<host>` that match your certificate, and rotate them together with the certificate.
- **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.

## Mail configuration

Subscore **95**

### Mail 90

- **Mail servers (MX)** Required
  The domain has 5 mail server(s) (MX).
- **SPF** Recommended
  An SPF record with a soft-fail policy (~all) is published.
- **DKIM** Recommended
  DKIM is set up, but the 1024-bit key is only marginally sufficient.

- **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
  All mail servers have an IPv6 address.
- **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
  No mail server accepts mail to foreign recipients for relaying (no open relay).

## 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.