Wolf-Agents Security Report

Email Security Check

Output: en / none / 2026-10-05.2 · Technical results, explanations and sources without additional legal context. · Information checked: 2026-10-05

Target

wolf-agents.com
Scan time: 06 Oct 2026, 22:31 GMT+2 (Europe/Berlin)
Document generated on: 06 Oct 2026, 22:55 GMT+2 (Europe/Berlin)
The explanations in this report were created using AI. Available measurements were collected automatically; assessments follow fixed rules. About their creation: https://wolf-agents.com/ki-hinweis/#english
Measurement catalogue version: 1.9
Report presentation: 2026-10-05.legal-2
Scan ID: 4e500d11-959a-4e48-9f42-ccffcd4e56c3
Report model: 1.10
Confidentiality: for the recipient and third parties named by the recipient
Issued by: Wolf-Agents.com - kontakt@wolf-agents.com

Overall picture

A 118 of 142 points - Good configuration in the external check

21 checks: 11 passed, 0 failed, 2 not assessable, 7 informational, 1 not applicable.
2 of 21 checks cannot be assessed conclusively from the saved data. The full model denominator is retained; measurement failures do not improve the overall ratio. Measurement coverage saved in the run, by possible points: 124 of 142. The group denominators of the points balance total 126; they include 2 possible product points from non-applicable checks. These explain the difference from the saved measurement coverage, which does not count them. The current finding totals may differ because of corrected interpretation.

Start here

Informational, not applicable and passed checks remain in the complete catalogue below. The IDs also identify sections in print.

Confirmed negative findings

No confirmed negative findings in the recorded scope.

Open / not assessable

smtp-tls · not assessable · SMTP TLS certificate
smtp-zertifikat · not assessable · SMTP certificate status

Scope limits

- The check is unauthenticated and is performed exclusively from outside the system.
- Snapshot of the externally visible DNS configuration. No determination of compliance or regulatory applicability, and no examination by an assessment body.
- This is not a penetration test. No vulnerability was actively exploited.
- No source code, infrastructure or process audit.
- A snapshot at the stated time. Subsequent changes are not captured.
- False findings are possible. Upstream CDN, WAF or rate-limiting systems may distort the result.
- Checks without evaluable measurement evidence, for example because a system was unreachable or unresponsive, are shown as “not assessable”, not as “passed”.
- This classification is general information and does not replace legal advice.

- The current DNSSEC measurement checks the responses for MX and TXT at the entered DNS name. AD is validation evidence from the resolver connected over loopback or HTTPS and assumed to validate; the scanner does not validate signatures itself. An authenticated negative response establishes the absence of the queried data, not a mail service. The zone boundary is not separately determined. The query time denotes retrieval; responses may come from the resolver cache. Other MX zones, TLSA, SPF include/redirect targets and DKIM selectors are not automatically confirmed. DNSSEC does not encrypt messages and establishes neither delivery nor the mail provider's resolver operation.
- Static SPF policy analysis at the entered DNS name, including limited include/redirect traversal. No individual message or sender authorisation for MAIL FROM, HELO/EHLO or an empty SMTP reverse path was checked; the input does not establish an actual sender role. RFC 7208 section 2.3 recommends a separate HELO check (SHOULD); section 2.4 uses the MAIL FROM identity postmaster@<HELO> for an empty reverse path. A missing SPF record does not trigger substitution with an arbitrary receiving MX. Additional evaluation requires a reliable sender IP, the HELO/EHLO identity and MAIL FROM, including whether the reverse path is empty. The scanner currently has no complete SPF evaluator equivalent to check_host(). With these inputs, a scenario could be checked without a message; it would confirm the specified scenario, not an observed connection. The scanner's own EHLO at the receiving server does not establish an outgoing HELO identity.
- DNSSEC is a general hardening recommendation (RFC 9364/BCP 237) and a prerequisite for SMTP DANE. In transport profile BSI TR-03108 2.0, sections 4.1.4/4.1.5, validating resolvers and signed receiving and MHS zones are mandatory. BSI TR-03182 1.0, section 4.1.1, recommends signing the sender zone that publishes SPF (SHOULD); section 4.1.2 requires resolver validation at the MHS checking SPF (MUST). The entered name does not establish these mail roles. The external check confirms neither the complete profiles nor a general legal duty to use DNSSEC.

Automated snapshot within the documented scope. Not an audit, certification or legal advice. Statutory rights remain unaffected. Measured on: 06 Oct 2026.

Evidence notation e1: original backslashes are doubled; \u{HEX} represents exactly one Unicode codepoint. Raw evidence explicitly represents every space, control, combining or unsupported character this way. No normalisation. Layout line breaks add no original character. CSV raw fields additionally preserve the complete evidence text; cookie values and local parts of email addresses are hidden as *** there as everywhere.

Assessment scheme

The following scale applies only to failed checks, not to information, checks that cannot be assessed or non-applicable checks. The terms used for potential impact and response priority follow the BSI practical guide, version 1.2, section 4.1.3. The classification of scanner findings, points and grade follows our documented assessment method. These do not set legal deadlines. high = immediate, medium = short-term, low = medium-term, for information = long-term. Finding interpretation 1.9. Points assess measured configuration characteristics; missing maximum points do not automatically mean a fault. Scoring methodology 1.8: DNSSEC retains 8 of 142 possible points. For A+, both the queried MX and TXT responses must be DNSSEC-validated. Missing confirmation caps the grade at A; an unclear measurement lacks evidence for A+ and is not a measured security defect. If the trusted resolver explicitly reports DNSSEC bogus, the grade is capped at B. SMTP, DANE and certificate points use the limited selection of equal-preference MX targets; a confirmed weaker path is not hidden by a good path, and unmeasured paths remain unknown. Other bonus points do not offset these conditions. The separate 30-point non-sending profile is unchanged and does not measure DNSSEC. The score is product weighting, not a probability of security. Model 1.9 assesses up to 142 security points. BIMI, certificate reference, ARC, gateway and SPF/DKIM provider indications are unweighted; their absence does not lower the security grade. Unmeasured checks remain in the model denominator; measurement coverage is shown separately. The grade follows fixed point thresholds and domain-specific caps, not a percentage extrapolated from the remaining measurements. Deliberately NO CVSS score is assigned - there is no authoritative CVSS rating for configuration findings, and a self-calculated number in the notation of a standard would claim a precision that does not exist.

BSI – Practical guide to information security penetration testing · v1.2 (2016-11), section 4.1.3, pp. 25–26 · checked 2026-10-05 · https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.pdf?__blob=publicationFile&v=3

Status values per check:
[+] passed - confirmed within the stated scope; no deviation demonstrated. [!] failed - finding present. [?] not assessable - no evaluable measurement evidence is available for this check; that is neither a positive nor a negative finding. The individual finding identifies a documented measurement limit or missing saved information. [i] Information - observed configuration signal without a demonstrated security defect. [-] not applicable - not applicable to the observed response context; not a passed security check.

Outgoing email security

79 of 87 points

These checks concern messages sent in the domain's name: whether receiving systems can recognise that a message is authentic and how they should handle forgeries. The points balance includes 2/2 saved product points from non-applicable checks. These values are retained in the assessment; they do not establish a successful measurement of the non-applicable check.

[+] spf · Sender Policy Framework

Status: passed | ID: spf | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 20 points

What is checked: Static SPF policy analysis at the entered DNS name: syntax, limited include/redirect traversal and the effective ending (-all, ~all, ?all). No specific sender IP, MAIL FROM, HELO or null-sender authorisation is checked.

Finding: SPF policy with Hard Fail published

The published SPF policy ends with -all (Hard Fail). 2/10 DNS lookup terms along the statically examined path.

Published sending sources and the final SPF policy are assessed. DMARC alignment was not checked on a message; receivers decide on delivery.

DNS query name: wolf-agents.com. Static SPF policy analysis at the entered DNS name, including limited include/redirect traversal. No individual message or sender authorisation for MAIL FROM, HELO/EHLO or an empty SMTP reverse path was checked; the input does not establish an actual sender role. Product points in the saved run: 20/20.

Evidence:\u{20}v=spf1\u{20}include:spf.tutanota.de\u{20}include:_spf.tem.scaleway.com\u{20}-all

References: BSI APP.5.3.A9 | RFC 7208

References: BSI APP.5.3.A9 · Email clients and servers: extended security measures, standard (S), module p. 5 · IT-Grundschutz, Edition 2023 (2023-02) · checked 5 October 2026 · https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4

References: IETF · RFC 7208: SPF: sender authorisation · checked 5 October 2026 · https://www.rfc-editor.org/rfc/rfc7208

[+] dkim · DomainKeys Identified Mail

Status: passed | ID: dkim | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 20 points

What is checked: Whether a DKIM key can be found in DNS under the selectors that were checked, and which key length or which algorithm it uses.

Finding: Public DKIM keys found

Public DNS keys found: s1: RSA 2048 bits; s2: RSA 2048 bits.

This DNS check does not verify any message signature. Active signing, message integrity and DMARC alignment remain unchecked; further unknown selectors cannot be ruled out. The points assess only the keys found. Product points in the saved run: 20/20.

Evidence:\u{20}s1:\u{20}v=DKIM1;\u{20}k=rsa;\u{20}h=sha256;\u{20}p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4d/jridMLV9rZ/lBiDYA17BWKWIHnvLzCVGoFcOENqxLym8ro869rgp82mcxobr2kPyd+sfAS/REOoZ+pkf1wnyywQrf4r9i1O9Bnop4/WsRXTlfgKtaIOtwyhgsv9JH5KpxeQxHwl9CEHhqJuFJp808gbqRZt6PDp2YetB23EyJ5kp/jpn5/aCvVpC27+jnQH6NoYN8wNsC6cTSA1EhL1etUwJrZUwRtf8S2PIDJOm1/CUtc9a/d3sZk15LDtUUbODrQMrj5mzMzHPYp43MwLFRlvSa/O+xIx8esNxwnDa7PH6PZLB8lhtkY49/4ofKV5BQKMGmGmyn+rgYDHD8iwIDAQAB\u{A}\u{A}s2:\u{20}v=DKIM1;\u{20}k=rsa;\u{20}h=sha256;\u{20}p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4d/jridMLV9rZ/lBiDYA17BWKWIHnvLzCVGoFcOENqxLym8ro869rgp82mcxobr2kPyd+sfAS/REOoZ+pkf1wnyywQrf4r9i1O9Bnop4/WsRXTlfgKtaIOtwyhgsv9JH5KpxeQxHwl9CEHhqJuFJp808gbqRZt6PDp2YetB23EyJ5kp/jpn5/aCvVpC27+jnQH6NoYN8wNsC6cTSA1EhL1etUwJrZUwRtf8S2PIDJOm1/CUtc9a/d3sZk15LDtUUbODrQMrj5mzMzHPYp43MwLFRlvSa/O+xIx8esNxwnDa7PH6PZLB8lhtkY49/4ofKV5BQKMGmGmyn+rgYDHD8iwIDAQAB 2kPyd+sfAS/REOoZ+pkf1wnyywQrf4r9i1O9Bnop4/WsRXTlfgKtaIOtwyhgsv9JH5KpxeQxHwl9CEHhqJuFJp808gbqRZt6PDp2YetB23EyJ5kp/jpn5/aCvVpC27+jnQH6NoYN8wNsC6cTSA1EhL1etUwJrZUwRtf8S2PIDJOm1/CUtc9a/d3sZk15LDtUUbODrQMrj5mzMzHPYp43MwLFRlvSa/O+xIx8esNxwnDa7PH6PZLB8lhtkY49/4ofKV5BQKMGmGmyn+rgYDHD8iwIDAQAB

References: BSI APP.5.3.A9 | RFC 6376 | RFC 8301 | RFC 8463

References: BSI APP.5.3.A9 · Email clients and servers: extended security measures, standard (S), module p. 5 · IT-Grundschutz, Edition 2023 (2023-02) · checked 5 October 2026 · https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4

References: IETF · RFC 6376: DKIM: signatures · checked 5 October 2026 · https://www.rfc-editor.org/rfc/rfc6376

References: IETF · RFC 8301: DKIM keys · checked 5 October 2026 · https://www.rfc-editor.org/rfc/rfc8301

References: IETF · RFC 8463: DKIM with Ed25519 · checked 5 October 2026 · https://www.rfc-editor.org/rfc/rfc8463

Technical snapshot within the stated scope; no compliance attestation.

[+] dmarc · Domain-based Message Authentication

Status: passed | ID: dmarc | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 35 points

What is checked: Which DMARC policy is published in the DNS path checked and applies to the name examined (p/sp/np, inheritance and test mode t=y). Message authentication and recipient handling are not checked.

Finding: DMARC policy reject

The selected policy requests rejection of messages that fail DMARC.

Policy source: _dmarc.wolf-agents.com; local record. Published: p=reject, sp=not specified, np=not specified.

An absent sp is not a defect: the relevant inherited namespace uses p=reject where np is not applicable.

Without np, sp applies to non-existent subdomains, falling back to p.

Valid records at the subdomain itself take precedence; their presence was not fully surveyed.

Alignment settings: SPF s, DKIM s; both r and s conform to the standard.

Aggregate reporting destinations published: ***@wolf-agents.com. This establishes neither report generation, delivery nor analysis.

Failure reporting destinations (ruf) published: ***@wolf-agents.com. The scan checks neither the generation nor the content of such reports.

Product weighting for the DNS configuration: quarantine conforms to the standard; additional points for reject reflect stricter product weighting. A point difference alone does not justify remedial action.

The DNS policy was checked. Message signatures, SPF/DKIM success, alignment, acceptance, rejection and actual receiver handling were not checked. Receivers decide according to their own rules. Product points in the saved run: 35/35.

Evidence:\u{20}v=DMARC1;\u{20}p=reject;\u{20}aspf=s;\u{20}adkim=s;\u{20}rua=mailto:***@wolf-agents.com;\u{20}ruf=mailto:***@wolf-agents.com;\u{20}fo=1

References: BSI APP.5.3.A9 | RFC 9989 | RFC 9990

References: BSI APP.5.3.A9 · Email clients and servers: extended security measures, standard (S), module p. 5 · IT-Grundschutz, Edition 2023 (2023-02) · checked 5 October 2026 · https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4

References: IETF · RFC 9989: DMARC: policies and alignment · checked 5 October 2026 · https://www.rfc-editor.org/rfc/rfc9989

References: IETF · RFC 9990: DMARC aggregate reports · checked 5 October 2026 · https://www.rfc-editor.org/rfc/rfc9990

[i] bimi · Brand Indicators for Message Identification

Status: Information | ID: bimi | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: Whether a BIMI record is published in DNS and points to a logo file that supporting email programs can display next to the message.

Finding: BIMI logo URL published

The check reads the logo URL from the DNS record. The logo file, receiver display and rights to the brand are not retrieved or validated. An empty l= can intentionally disable BIMI. Logo display also depends on DMARC and the receiver's rules. Product points in the saved run: 0/0.

Evidence:\u{20}v=BIMI1;\u{20}l=https://wolf-agents.com/bimi-logo.svg

[i] vmc · Verified Mark Certificate

Status: Information | ID: vmc | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: Whether the BIMI record specifies an HTTPS certificate URL. The certificate type (VMC/CMC), content and validity are not retrieved or validated.

Finding: No certificate reference for BIMI found

No usable HTTPS address for a brand certificate was found in the BIMI record. This is an optional brand display feature and not evidence of an email security vulnerability. Product points in the saved run: 0/0.

Recommendation [vmc]: Only if BIMI display is desired, check the current certificate requirements of your target receivers. This scanner does not validate brand certificates.

[i] arc · Authenticated Received Chain

Status: Information | ID: arc | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: Limited hints from DKIM-like tags at the selector name arc._domainkey or a recorded MX provider association. No message, ARC header, cryptographic chain validation or trust assessment is checked.

Finding: ARC cannot be verified by a domain check

No recognised name/tag indication of ARC was detected at the examined name arc._domainkey. Other selectors and message paths were not examined; this does not prove that ARC is absent. ARC can convey earlier authentication results through intermediaries. This domain check examined no message, header, signature or ARC chain. ARC is an unweighted observation (0/0) in this run; its absence is not a defect and does not lower the security grade. Standards status on 9 September 2026: RFC 8617 is Experimental. The active working-group draft draft-ietf-dmarc-arc-to-historic-00 proposes Historic status; that classification has not yet been adopted. DKIM2 is also a draft, with no promised migration date. This does not imply an automatic recommendation to disable ARC. Product points in the saved run: 0/0.

Recommendation [arc]: A separate selector named arc is not required. ARC uses DNS key queries similar to DKIM; this does not require reuse of an ordinary DKIM key. For mailing lists or forwarding, you can have a message received under controlled conditions examined separately: ARC-Seal, ARC-Message-Signature and ARC-Authentication-Results are initially only headers. ARC validation checks, among other things, complete and consistent ARC sets and cryptographic signatures; trust in intermediaries must then be assessed separately. A copied cv=pass is a statement in the message, not a result calculated by the domain check. Even a validated chain guarantees neither harmless content nor successful delivery.

References: RFC 8617

References: IETF · RFC 8617: ARC: forwarded authentication results (experimental) · checked 5 October 2026 · https://www.rfc-editor.org/rfc/rfc8617

Technical snapshot within the stated scope; no compliance attestation.

[i] dkim-ed25519 · DKIM modern cryptography

Status: Information | ID: dkim-ed25519 | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 5 points

What is checked: Whether the DKIM keys that were found use modern algorithms — Ed25519 or RSA with a sufficient key length.

Finding: Additional DKIM cryptography not established

Only the public keys found are assessed. An RSA/Ed25519 pair enables parallel signatures; actual dual signing and receiver compatibility are not established without messages. RSA-2048 meets the recommendation in RFC 8301. Additional bonus points reflect product weighting, not an obligation to switch. Product points in the saved run: 0/5.

References: RFC 8463

References: IETF · RFC 8463: DKIM with Ed25519 · checked 5 October 2026 · https://www.rfc-editor.org/rfc/rfc8463

[i] dkim-redundanz · DKIM selector redundancy

Status: Information | ID: dkim-redundanz | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 3 points

What is checked: Whether multiple different DKIM keys are published under the selectors checked. Active use and the rotation process are not demonstrated.

Finding: 1 distinct DKIM key found

Multiple published keys can prepare a controlled change. Identical keys under different selectors are not counted more than once. DNS establishes neither active use nor independent sending services or uninterrupted rotation. Safe rotation is also possible with one current selector by publishing a new key in good time. Product points in the saved run: 0/3.

Recommendation [dkim-redundanz]: Publish the new public key before switching signatures. Retain the old key for messages still in transit and consider DNS TTLs and transit times. Then check signatures on actual messages.

[+] spf-qualitaet · SPF quality

Status: passed | ID: spf-qualitaet | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 2 points

What is checked: Whether the SPF record manages without outdated mechanisms and stays within the permitted number of DNS lookups.

Finding: SPF structure without the deprecated PTR mechanism

The examined SPF records include sending sources through include. This can make external services easier to maintain; own servers may equally be authorised directly by IP, a or mx. Product points in the saved run: 2/2.

References: RFC 7208

References: IETF · RFC 7208: SPF: sender authorisation · checked 5 October 2026 · https://www.rfc-editor.org/rfc/rfc7208

[i] spf-dkim-abdeckung · SPF-DKIM provider indications

Status: Information | ID: spf-dkim-abdeckung | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: Whether known SPF destination names and DKIM selector names match. Includes resolved through redirect are also considered; actual message sending is not checked.

Finding: Known SPF providers and DKIM selector names found

SPF target names and known DKIM selector names are associated heuristically. Own servers, unknown providers and custom or dynamic selectors are permitted. Even matching names establish neither the association of a key with the sending service nor actual DKIM signatures or DMARC alignment. This optional indication earns no security or bonus points. Product points in the saved run: 0/0.

References: RFC 6376 | RFC 8301 | RFC 8463

References: IETF · RFC 6376: DKIM: signatures · checked 5 October 2026 · https://www.rfc-editor.org/rfc/rfc6376

References: IETF · RFC 8301: DKIM keys · checked 5 October 2026 · https://www.rfc-editor.org/rfc/rfc8301

References: IETF · RFC 8463: DKIM with Ed25519 · checked 5 October 2026 · https://www.rfc-editor.org/rfc/rfc8463

[-] dmarc-report-auth · DMARC report authorisation

Status: not applicable | ID: dmarc-report-auth | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 2 points

What is checked: Whether external recipients of DMARC reports have authorised receipt — demonstrable through an authorisation record in their domain.

Finding: Reports addressed to the same domain

***@wolf-agents.com is specified as a report target within the policy domain. The DNS reference establishes no actual report generation or delivery. Product points in the saved run: 2/2.

References: RFC 9989 | RFC 9990

References: IETF · RFC 9989: DMARC: policies and alignment · checked 5 October 2026 · https://www.rfc-editor.org/rfc/rfc9989

References: IETF · RFC 9990: DMARC aggregate reports · checked 5 October 2026 · https://www.rfc-editor.org/rfc/rfc9990

Incoming email security

15 of 15 points

These checks examine configured receiving destinations and published transport and reporting policies for incoming email.

[+] mx · Mail Exchange Records

Status: passed | ID: mx | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: MX names and priorities, including null MX, and stored provider name patterns. The additional PTR check covers at most the first IPv4 address of the first MX and may be skipped or incomplete. Active protection, SMTP reachability, A/AAAA fallback and delivery are not checked.

Finding: MX records found in DNS

1 MX record(s) observed: 10 mail.tutanota.de. The first MX name matches the saved name pattern mail.tutanota.de of Tutanota / Tuta (Germany) (Cloud_Privacy). This is a name match, not evidence of purchased protective features, enabled tenant policies or successful filtering.

One explicit MX target was observed.

PTR/FCrDNS was not conclusively measured in this MX finding. Provider attribution cannot replace this measurement.

MX DNS records establish neither active protective features, SMTP reachability nor successful delivery. A separately saved SMTP measurement applies only to its host, time and connection segment. Product points in the saved run: 0/0.

Evidence:\u{20}10\u{20}mail.tutanota.de

[+] mta-sts · MTA Strict Transport Security

Status: passed | ID: mta-sts | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 10 points

What is checked: DNS version marker and id tag, limited HTTPS retrieval, policy parsing, published mode and max_age, and MX name matching where inputs are available. No full RFC validation, SMTP certificate check or observation of application by external senders.

Finding: MTA-STS enforce published; MX names covered

A DNS version marker with an id tag and content accepted by the policy parser are documented. This confirms the checked characteristics, not complete RFC compliance or operational acceptance.

DNS: _mta-sts.wolf-agents.com; 1 record(s) with version marker, recognised id=20260524. Candidate count and id marker are not a complete DNS syntax check.

HTTPS response: HTTP 200, readable policy content accepted by the parser.

Saved mode: enforce. A sender applying this policy must meet the specified MX/TLS/certificate conditions and must not deliver under this policy if those conditions fail.

Saved policy MX patterns: mail.tutanota.de.

MX inputs to this comparison: 10 mail.tutanota.de.

All MX names saved in the comparison match the policy patterns.

max_age: 86400 seconds (1 day). The lifetime describes the intended sender cache, not a measured period of protection.

Retrieving the policy over HTTPS is not a STARTTLS or SMTP certificate check of the MX servers. Actual sender application, message sending, delivery and receipt of reports were not checked here; separate SMTP findings apply only to their own host, measurement time and scope. Product points in the saved run: 10/10.

Evidence:\u{20}DNS-Record:\u{A}v=STSv1;\u{20}id=20260524\u{A}\u{A}Policy-Datei:\u{A}version:\u{20}STSv1\u{D}\u{A}mode:\u{20}enforce\u{D}\u{A}mx:\u{20}mail.tutanota.de\u{D}\u{A}max_age:\u{20}86400

Recommendation [mta-sts]: Check the documented policy characteristics and intended message path under controlled conditions. Reporting must be set up and checked separately at the intended TLS-RPT destination.

References: BSI APP.5.3.A9 | RFC 8461

References: BSI APP.5.3.A9 · Email clients and servers: extended security measures, standard (S), module p. 5 · IT-Grundschutz, Edition 2023 (2023-02) · checked 5 October 2026 · https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4

References: IETF · RFC 8461: MTA-STS: published transport policy · checked 5 October 2026 · https://www.rfc-editor.org/rfc/rfc8461

Technical snapshot within the stated scope; no compliance attestation.

[+] tls-rpt · TLS Reporting

Status: passed | ID: tls-rpt | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 5 points

What is checked: TXT version marker, number of matching TLS-RPT records, rua fields and limited characteristics of mailto: and https: destinations. This is not full RFC validation; report generation, transmission, receipt, analysis and alerting are not checked.

Finding: TLS-RPT policy with reporting destination found in DNS

A record with v=TLSRPTv1 and 1 rua field(s) was found. Reporting destinations recognised as usable: mailto:***@wolf-agents.com. The check covers TXT version markers, the number of matching records, rua fields and limited URI characteristics (mailto address or HTTPS host without credentials). It is not complete RFC validation. Generation by sending systems, target reachability, transmission, actual receipt, analysis and alerts were not tested. Product points in the saved run: 5/5.

Evidence:\u{20}v=TLSRPTv1;\u{20}rua=mailto:***@wolf-agents.com

Recommendation [tls-rpt]: At the intended reporting destination, check actual receipt and analysis of TLS reports and the required alerts with its operator. Sending systems must also generate and transmit reports; DNS publication alone does not establish this operation.

References: BSI APP.5.3.A13 | RFC 8460

References: BSI APP.5.3.A13 · Email clients and servers: TLS reporting, high (H), module p. 6 · IT-Grundschutz, Edition 2023 (2023-02) · checked 5 October 2026 · https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4

References: IETF · RFC 8460: TLS-RPT: SMTP transport security reporting · checked 5 October 2026 · https://www.rfc-editor.org/rfc/rfc8460

[i] seg-provider · Secure Email Gateway

Status: Information | ID: seg-provider | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: Whether MX names match known gateway provider patterns. Active filtering and its effectiveness are not checked.

Finding: No known provider pattern in the MX names

The observed MX names match none of this detector’s gateway provider patterns. For context, detection uses known MX patterns; it does not cover unlisted or individually hosted gateways. An absent provider indication is not a security defect and does not affect the grade. Product points in the saved run: 0/0.

DNS security & further hardening

24 of 24 assessable points (16 further points cannot be assessed)

This group contains limited DNS, TLSA, SMTP and further hardening findings. In scoring methodology 1.8 of this run, DNSSEC is also a condition for the top grade. Points and observations do not confirm complete protection or delivery.

[+] dnssec · DNS Security Extensions

Status: passed | ID: dnssec | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 8 points

What is checked: DNSSEC validation evidence for MX and TXT responses at the entered name through the trusted resolver channel. Positive, negative, unauthenticated and uncertain responses are distinguished; this is not a complete zone or mail-path check.

Finding: MX and TXT responses DNSSEC-validated

MX wolf-agents.com: RRset present; DNSSEC-validated (AD). RCODE: 0. Measurement time: 2026-10-06T20:31:45.616Z. Resolver channel: loopback-udp. RRset names: wolf-agents.com.

TXT wolf-agents.com: RRset present; DNSSEC-validated (AD). RCODE: 0. Measurement time: 2026-10-06T20:31:45.618Z. Resolver channel: loopback-udp. RRset names: wolf-agents.com.

The current DNSSEC measurement checks the responses for MX and TXT at the entered DNS name. AD is validation evidence from the resolver connected over loopback or HTTPS and assumed to validate; the scanner does not validate signatures itself. An authenticated negative response establishes the absence of the queried data, not a mail service. The zone boundary is not separately determined. The query time denotes retrieval; responses may come from the resolver cache. Other MX zones, TLSA, SPF include/redirect targets and DKIM selectors are not automatically confirmed. DNSSEC does not encrypt messages and establishes neither delivery nor the mail provider’s resolver operation. Product points in the saved run: 8/8.

Evidence:\u{20}wolf-agents.com\u{20}IN\u{20}MX\u{20}10\u{20}mail.tutanota.de.\u{A}wolf-agents.com\u{20}IN\u{20}TXT\u{20}"v=spf1\u{20}include:spf.tutanota.de\u{20}include:_spf.tem.scaleway.com\u{20}-all"\u{A}wolf-agents.com\u{20}IN\u{20}TXT\u{20}"google-site-verification=qn_HX0HbTp5w4HUg4H-xan_QuSKtPrL6M9YSZqyYJag"\u{A}wolf-agents.com\u{20}IN\u{20}TXT\u{20}"t-verify=1f523ee67b0a2d1bd3411818a20c05ee"

References: BSI TR-03108 2.0, 4.1.4/4.1.5 (transport profile) | BSI TR-03182 1.0, 4.1.1/4.1.2 (separate SPF roles) | RFC 4033 | RFC 4035 | RFC 9364

References: BSI TR-03108 · Secure Email Transport · v2.0 (2023-06-01), 4.1.4–4.1.5 · checked 5 October 2026 · https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03108/TR03108.pdf?__blob=publicationFile&v=3

References: BSI TR-03182 · Email Authentication · v1.0 (2024-01-24), 4.1.1–4.1.2 · checked 5 October 2026 · https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03182/BSI-TR-03182.pdf?__blob=publicationFile&v=6

References: IETF · RFC 4033: DNSSEC: introduction · checked 5 October 2026 · https://www.rfc-editor.org/rfc/rfc4033

References: IETF · RFC 4035: DNSSEC: protocol · checked 5 October 2026 · https://www.rfc-editor.org/rfc/rfc4035

References: IETF · RFC 9364: DNSSEC: deployment guidance · checked 5 October 2026 · https://www.rfc-editor.org/rfc/rfc9364

Technical snapshot within the stated scope; no compliance attestation.

[+] dane · DNS-based Authentication of Named Entities

Status: passed | ID: dane | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 10 points

What is checked: Whether distinct MX hosts at the lowest numerical preference, within the documented measurement limit, publish DNSSEC-validated TLSA records with supported SMTP parameters. Certificate matching and MX hosts at other preference levels are not checked.

Finding: DNSSEC-validated SMTP TLSA record found

A DNSSEC-validated TLSA record with supported SMTP parameters was found for mail.tutanota.de. The certificate data was not compared with the SMTP certificate actually presented. Only this MX host was checked; further MX targets and actual message flow are not thereby confirmed. The only selected MX at the lowest numeric preference was measured (mail.tutanota.de). Product points in the saved run: 10/10.

Evidence:\u{20}_25._tcp.mail.tutanota.de\u{20}TLSA\u{20}3\u{20}0\u{20}1\u{20}d141f8f3a4aac2e4d2677aafcc723d8e5cc7b146e968c3aea348ed93996bbe6f

References: BSI APP.5.3.A9 | RFC 6698 | RFC 7672

References: BSI APP.5.3.A9 · Email clients and servers: extended security measures, standard (S), module p. 5 · IT-Grundschutz, Edition 2023 (2023-02) · checked 5 October 2026 · https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4

References: IETF · RFC 6698: DANE/TLSA · checked 5 October 2026 · https://www.rfc-editor.org/rfc/rfc6698

References: IETF · RFC 7672: DANE for SMTP · checked 5 October 2026 · https://www.rfc-editor.org/rfc/rfc7672

[+] caa · Certificate Authority Authorization

Status: passed | ID: caa | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 2 points

What is checked: Whether CAA entries in DNS determine which certification authorities may issue certificates for the domain at all.

Finding: CAA fully configured

Permitted CAs: pki.goog, letsencrypt.org, globalsign.com, sectigo.com, digicert.com, comodoca.com. The optional reporting target is: mailto:***@wolf-agents.com. Actual reports and the complete certificate issuance process were not checked.

Recommendation: an issuewild tag is needed only for different wildcard rules; without it, issue also applies to wildcards. Product points in the saved run: 2/2.

Evidence:\u{20}0\u{20}issue\u{20}"pki.goog"\u{A}0\u{20}issue\u{20}"letsencrypt.org"\u{A}0\u{20}issue\u{20}"globalsign.com"\u{A}0\u{20}issue\u{20}"sectigo.com"\u{A}0\u{20}iodef\u{20}"mailto:***@wolf-agents.com"\u{A}0\u{20}issue\u{20}"digicert.com"\u{A}0\u{20}issue\u{20}"comodoca.com"

References: RFC 8659

References: IETF · RFC 8659: CAA: certificate authority authorisation · checked 5 October 2026 · https://www.rfc-editor.org/rfc/rfc8659

Technical snapshot within the stated scope; no compliance attestation.

[?] smtp-tls · SMTP TLS certificate

Status: not assessable | ID: smtp-tls | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 13 points

What is checked: Whether distinct MX hosts at the lowest numerical preference, within the documented measurement limit, offer an encrypted SMTP connection, which TLS version was observed for each host and whether each certificate matches its host name. Measured equal-preference MX targets: mail.tutanota.de. Unmeasured equal-preference targets: none. Backup preference levels: none. SMTP measurement time: mail.tutanota.de: 2026-10-06T20:31:59.422Z.

Finding: SMTP measurement not fully completed

Examined MX/host: mail.tutanota.de. STARTTLS offer: not conclusively measured. TLS handshake: not conclusively confirmed.

TLS version: not documented. Certificate trust chain: not documented; hostname match: not documented.

SMTP measurement time: 2026-10-06T20:31:59.422Z. Measurement limit/error: Socket-Zeitüberschreitung.

Test locations: primary: partial measurement, attempt from 2026-10-06T20:31:46.398Z until 2026-10-06T20:31:56.444Z, measurement error: Socket-Zeitüberschreitung; Fallback: partial measurement, attempt from 2026-10-06T20:31:49.400Z until 2026-10-06T20:31:59.421Z, measurement error: Socket-Zeitüberschreitung. Success at a fallback location does not complete the finding at the other location.

The finding applies to this observed connection segment from the test location. Further MX hosts, fallback locations and transport paths are not fully established. No end-to-end encryption or actual delivery was checked. A connection, EHLO or handshake error alone does not prove a lack of encryption capability. The only selected MX at the lowest numeric preference was measured (mail.tutanota.de). The weight of 13 points denotes the catalogue maximum for this check that cannot be assessed, no earned points and no confirmed deduction. The saved 0/0 product points indicate the measurement failure, not the catalogue weight. Product points in the saved run: 0/0.

Recommendation [smtp-tls]: Investigate the recorded measurement limit using server logs and the test location before assuming a TLS misconfiguration.

References: BSI APP.5.3.A2

References: BSI APP.5.3.A2 · Email clients and servers: secure operation, basic (B), module pp. 3–4 · IT-Grundschutz, Edition 2023 (2023-02) · checked 5 October 2026 · https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4

[?] smtp-zertifikat · SMTP certificate status

Status: not assessable | ID: smtp-zertifikat | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 3 points

What is checked: How long the observed TLS certificates of the bounded set of equal-preference MX hosts remain valid and whether their remaining validity allows an orderly renewal.

Finding: Certificate check could not be performed

No mail server certificate data was available for this scan (SMTP test unavailable). This is not a finding about your certificate. The only selected MX at the lowest numeric preference was measured (mail.tutanota.de). The weight of 3 points denotes the catalogue maximum for this check that cannot be assessed, no earned points and no confirmed deduction. The saved 0/0 product points indicate the measurement failure, not the catalogue weight. Product points in the saved run: 0/0.

[+] ptr-fcrdns · Reverse DNS / FCrDNS

Status: passed | ID: ptr-fcrdns | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 4 points

What is checked: Whether a PTR name exists for the first IPv4 address found for the primary MX, and whether its A records contain the original IP address (forward-confirmed reverse DNS).

Finding: FCrDNS fully correct

The checked IPv4 address confirms the reverse DNS entry: 185.205.69.214 → mail.w14.tutanota.de → 185.205.69.214. For FCrDNS, the PTR name need not match the MX name. The primary MX host is checked (receiving direction); different outgoing servers, further addresses and IPv6 are not covered. Product points in the saved run: 4/4.

References: RFC 1035

References: IETF · RFC 1035: DNS resource records · checked 5 October 2026 · https://www.rfc-editor.org/rfc/rfc1035

Technical snapshot within the stated scope; no compliance attestation.