Souvera Shield – Admin

Bedienungsanleitung für Administratoren der Souvera-Shield-App. Fokus auf die zusätzlichen Admin-Ansichten in Nextcloud (Audit-Log, DMARC & Mail-Test, Whitelist/Blacklist-Verwaltung, Nutzeranfragen). Installation, Server-Konfiguration und CLI-Tätigkeiten werden vom Hoster erledigt und sind nicht Teil dieser Doku.

12. Reputation Management

Reputation Management

Der Menüpunkt **:balance_scale: Reputation** ist ein zusätzliches Admin- Werkzeug für Mitglieder der Gruppe `souvera-admins`. Er zeigt dir den DMARC/SPF/DKIM-Zustand deiner Workspace-Domain und die Ergebnisse des wöchentlichen Reputations-Tests über **provider.tools**.

> :bulb: Wenn du den Menüpunkt nicht siehst, bist du (noch) nicht in der Gruppe `souvera-admins`. Bitte deinen Hoster darum, dich hinzuzufügen.

Es gibt genau eine Domain – und die ist fix

Souvera Shield überwacht **immer nur die eine Domain deines Workspace**. Diese Domain ist bereits durch deinen Hoster in der Konfiguration hinterlegt (dieselbe, die auch für Proxmox Mail Gateway benutzt wird). Du kannst sie **nicht in der Oberfläche ändern** – das verhindert versehentliche Fehler.

> **:camera_with_flash: Screenshot-Platzhalter**
> *Reputation-Management-Seite mit dem großen Rep-Card oben. Domain-Feld zeigt 'example.com' als reinen Text (kein Editier-Icon).*

Die Seite auf einen Blick

Die Seite ist in **zwei Bereiche** getrennt:

1. **DMARC** – Aktueller Zustand von DMARC-, SPF-, DKIM-Records im DNS
2. **Mail-Test** – Historie der Reputationstests + Button für Sofort-Test

Bereich 1: DMARC

Zeigt in einer Karte alle wichtigen Informationen auf einen Blick:

Feld	Bedeutung
Domain	Die überwachte Workspace-Domain (nur Anzeige)
Absender für Tests	E-Mail-Adresse, aus deren Namen der wöchentliche Test versendet wird
provider.tools-Status	Grüne Pille "Verifiziert" oder gelbe "Nicht verifiziert"
Letzter DMARC-Check	Zeitstempel des letzten Checks (oder "Nie")
DMARC-Record	Grüne Pille "Gefunden" + der raw Record aus dem DNS
SPF-Record	dito
DKIM-Record	dito, mit Liste aller gefundenen Selektoren
Letzter Score	Punktzahl des jüngsten abgeschlossenen Mail-Tests

> **:camera_with_flash: Screenshot-Platzhalter**
> *Nahaufnahme der Rep-Card: acht Felder in einem Grid-Layout. DMARC-, SPF- und DKIM-Felder zeigen grüne Pillen 'Gefunden' und darunter den raw Record in monospace Font.*

„Re-check now"

Ein Klick auf **„Re-check now"** startet sofort einen DNS-Lookup der Domain über provider.tools. Ergebnis erscheint direkt in der Karte.

„Nicht verifiziert"-Hinweis

Falls die Domain bei provider.tools nicht als **verifiziert** markiert ist, siehst du eine gelbe Pille. In dem Fall bitte den Hoster, die Verifikation abzuschließen – **Souvera Shield legt keine Domains bei provider.tools an**.

> **:camera_with_flash: Screenshot-Platzhalter**
> *Rep-Card mit gelber 'Nicht verifiziert'-Pille im provider.tools-Status-Feld. Tooltip zeigt: 'The domain is not (yet) verified at provider.tools. Ask your hoster to complete the verification.'*

Bereich 2: Mail-Test

Zeigt die Historie aller durchgeführten Reputationstests. Neue Einträge kommen oben hinzu. Spalten:

- **Wann** – Startzeitpunkt
- **Status** – *Warte auf Mail*, *Warte auf Ergebnis*, *Abgeschlossen*, *Fehler*
- **Score** – Punktzahl (nur bei abgeschlossenen Tests)
- **SPF / DKIM / DMARC** – Ergebnis pro Prüfung (`PASS`, `FAIL`, `NONE`)
- **Trigger** – *Manuell* (von dir gestartet) oder *Wöchentlich* (Cron)
- **Aktion** – *Aktualisieren* (nur bei laufenden Tests), *Details*

> **:camera_with_flash: Screenshot-Platzhalter**
> *Mail-Test-Historie mit 8 Einträgen. Zwei sind noch 'Warte auf Mail' (gelbe Badges), fünf sind abgeschlossen (grüne PASS-Pillen), einer ist auf Fehler (rot).*

Score-Farben

- □□ **Grün (≥ 8.0)** – ausgezeichnete Reputation
- □□ **Gelb (5.0 – 7.9)** – akzeptabel, aber es gibt Verbesserungspotenzial
- □□ **Rot (< 5.0)** – schlechte Reputation, kann Zustellprobleme geben

„Run mail test now" – Sofort-Test

Startet **manuell** einen Test. Ablauf:

1. Souvera Shield öffnet eine Test-Session bei provider.tools
2. Sendet **eine einzige** Test-Mail vom konfigurierten Absender an die Test-Empfänger-Adresse (`xyz@chk.provider.tools`)
3. Nach 10-30 Sekunden ruft ein Hintergrund-Job das Ergebnis ab. Du kannst auch in der Tabelle auf **Aktualisieren** klicken, um sofort zu pollen.

> :warning: Der Test läuft maximal **1 Stunde**. Kommt in dieser Zeit keine Mail bei provider.tools an, wird der Test als **abgelaufen** markiert (Status „Fehler"). Ursache ist meist ein SMTP-Relay-Problem.

> **:camera_with_flash: Screenshot-Platzhalter**
> *Bestätigungs-Dialog nach Klick auf 'Run mail test now' mit Text 'Souvera Shield will send one test e-mail through the mail server and wait for provider.tools to analyse it. Results usually arrive within 30 seconds.' und Buttons 'Cancel' / 'OK'.*

„Details" eines Tests

Öffnet ein Modal mit allen technischen Daten des Tests:

- Test-ID bei provider.tools (nützlich für Support-Anfragen)
- Test-Empfänger-Adresse
- Start-, Sende-, und Abschluss-Zeitpunkt
- Fehlermeldung (falls Status „Fehler")
- Score sowie SPF/DKIM/DMARC-Ergebnis

> **:camera_with_flash: Screenshot-Platzhalter**
> *Modal-Fenster 'Mail test details' als Definitions-Liste. Beispielhaft: Score 8.5, SPF pass, DKIM pass, DMARC pass, Trigger manual.*

Der wöchentliche Job

Jeden **Sonntag** läuft automatisch **ein** Test für die konfigurierte Domain. Du musst nichts tun – das Ergebnis erscheint einfach in der Historie.

Wenn der API-Token oder die Domain fehlt

Falls dein Hoster den provider.tools-Token noch nicht gesetzt hat oder keine Domain konfiguriert ist, siehst du oben ein **gelbes Info-Banner**:

> „provider.tools API token is not configured yet – reputation checks are disabled. Please contact your hoster."

bzw.

> „No mail domain is configured for this workspace. Please contact your hoster."

In dem Fall bitte den Hoster – du selbst brauchst dich damit nicht zu befassen.

>

> **:camera_with_flash: Screenshot-Platzhalter**
> *Reputation-Seite mit gelbem Warnbanner ganz oben. Karte und Tabelle darunter sind entweder ausgegraut oder zeigen 'No data yet.'*

Neu ab v3.5.0: Der Reputations-Score (0–100)

Ganz oben auf der Seite siehst du jetzt einen **Gesamt-Score von 0 bis 100** in einem farbigen Ring (grün ≥ 80, orange ≥ 60, rot darunter). Er wird aus fünf Komponenten berechnet – daneben siehst du für jede Komponente einen Balken mit Einzelwert und Gewichtung:

Komponente	Gewicht	Datenquelle
DMARC-Reports	30 %	DKIM-/SPF-Pass-Raten aus den echten Reports der Empfänger
Letzter Mail-Test	25 %	Punktzahl des jüngsten abgeschlossenen Tests
Blacklists	20 %	120+ DNS-Blacklists – geprüft werden IP *und* Domain
Infrastruktur-Checks	15 %	Ergebnis der Zustellbarkeits-Checks (siehe unten)
Offene Vorfälle	10 %	Abzüge für offene kritische Vorfälle und Warnungen

> :bulb: **Keine erfundenen Zahlen:** Komponenten ohne echte Datenbasis (z. B. noch kein Mail-Test gelaufen) werden ausgegraut angezeigt und aus der Berechnung ausgeschlossen. Gibt es noch gar keine Daten, zeigt die Seite das ehrlich an, statt einen Wert zu schätzen.

Über den Button **„Analyse jetzt ausführen"** startest du jederzeit einen kompletten Analyse-Lauf (Checks, Score, Vorfälle). Automatisch passiert das einmal täglich im Hintergrund. Unter dem Score siehst du den **Score-Verlauf** der letzten Tage als Balken.

[SCREENSHOT] Score-Ring mit Komponenten-Balken und Button „Analyse jetzt ausführen".

Neu: Provider-Reputation (Google, Microsoft, Yahoo, GMX/Web.de)

Vier Karten zeigen, wie die großen Mail-Provider deine Mails sehen – berechnet aus den DMARC-Reports, die genau dieser Provider für deine Domain geschickt hat: Nachrichten-Volumen, DKIM- und SPF-Pass-Rate und ein Urteil (**Gut** / **Gefährdet** / **Kritisch**). Hat ein Provider im gewählten Zeitraum keine Reports geschickt, steht dort „Keine Reports dieses Providers im gewählten Zeitraum".

[SCREENSHOT] Vier Provider-Karten mit Pass-Raten und Urteils-Pille.

Neu: Zustellbarkeits-Checks mit Erklärung und Lösungsweg

Eine aufklappbare Liste prüft alle wichtigen Standards: SPF-Record, DMARC-Policy, SPF-/DKIM-Alignment, DKIM-Signatur, PTR/Reverse-DNS, HELO-Banner & STARTTLS, MTA-STS, TLS-RPT, BIMI, One-Click-Unsubscribe sowie Blacklist-Prüfungen für IP und Domain.

- Jede Zeile hat eine Status-Pille: **OK**, **Warnung**, **Fehlgeschlagen**, **Optional** oder **Keine Daten**.
- Beim Aufklappen erklärt jeder Check verständlich, **was das Problem ist** und **wie du es behebst** – inklusive der tatsächlich beobachteten Werte (DNS-Record, IP, PTR, Listungen …).
- Über **„Checks neu ausführen"** erzwingst du eine frische Prüfung (sonst werden die Ergebnisse bis zu 6 Stunden zwischengespeichert).

[SCREENSHOT] Check-Liste mit einer aufgeklappten Warnung inkl. Problem/Lösungsweg.

Neu: Versandquellen – legitim, unbekannt oder missbräuchlich

Die Tabelle **Versandquellen** zeigt, wer im Namen deiner Domain Mails verschickt – klassifiziert aus den echten DMARC-Daten:

- **Legitim** – besteht SPF oder DKIM aligned (≥ 90 %)
- **Unbekannt** – gemischte Ergebnisse, oft Weiterleitungen oder Mailinglisten
- **Potenziell missbräuchlich** – besteht beides nicht bei relevantem Volumen (mögliches Spoofing/Phishing in deinem Namen)

Erkennt die Analyse einen **ungewöhnlichen Volumen-Anstieg** (mögliches kompromittiertes Konto), erscheint darüber ein deutlicher Warnhinweis.

[SCREENSHOT] Quellen-Tabelle mit Klassifizierungs-Pillen.

Neu: Reputations-Vorfälle mit Historie und Maßnahmen

Erkannte Probleme (Blacklist-Listung, schwache DMARC-Pass-Rate, Anomalien, fehlgeschlagene Checks oder Mail-Tests) werden automatisch als **Vorfall** angelegt. Die Tabelle lässt sich nach **Offen** / **Behoben** / **Alle** filtern. Der Detail-Dialog zeigt zu jedem Vorfall:

- **Was ist passiert** – verständliche Ursache inkl. SMTP-Fehler-Diagnose
- **Lösungsweg** – konkrete Empfehlung
- **Betroffen** – Domain und ggf. IPs
- **Historie & Maßnahmen** – wann erkannt, erneut erkannt, automatisch oder manuell behoben

Ist ein Zustand bei der nächsten Analyse nicht mehr feststellbar, wird der Vorfall **automatisch als behoben markiert** (und bei Rückfall wieder geöffnet – die Historie bleibt erhalten). Mit **„Als behoben markieren"** kannst du Vorfälle auch manuell schließen.

[SCREENSHOT] Vorfall-Dialog mit Maßnahmen-Historie und Behoben-Button.

Neu: Beschwerden & Feedback-Loops

Unter dem Score siehst du, wie viele **forensische DMARC-Reports (RUF)** eingegangen sind und ob eine RUF-Adresse im DMARC-Record veröffentlicht ist. Echte Beschwerderaten von Google und Microsoft gibt es nur in deren eigenen Portalen – registriere deine Domain dafür bei **Google Postmaster Tools** und **Microsoft SNDS**. Souvera Shield zeigt hier bewusst keine geschätzten Werte an.

Geändert ab v3.5.0: So wird der Mail-Test versendet

Der Reputations-Test läuft weiterhin über **deinen Stalwart-Mailserver** (nur so misst provider.tools die echte Reputation deiner Infrastruktur). Neu: Souvera Shield legt dafür automatisch das Postfach `postmaster@<deine-domain>` in Stalwart an und versendet den Test angemeldet über den Submission-Port. Du musst dafür nichts tun – schlägt etwas fehl, siehst du in der Mail-Test-Historie eine verständliche Diagnose, die genau benennt, was dein Hoster prüfen

muss.