

ISPProtect Web Security for Shopware

ISPProtect Web Security für Shopware: Handbuch

Version 1.0.0

2026-11-23

Inhalt

1. **Einführung**
   - Was das Plugin leistet
   - Was das Plugin nicht leistet
   - Kostenlose und kostenpflichtige Teile
   - Voraussetzungen
   - Wer es nutzen kann
   - Aufbau dieses Handbuchs
2. **Installation und erste Schritte**
   - Das Plugin installieren
   - Was die Installation anlegt
   - Das Modul öffnen
   - Erste Schritte
   - Hinter einem Reverse-Proxy oder CDN
   - Zeitplanung
3. **Das Modul in der Administration**
   - Menüeintrag und Seiten
   - Einstellungen auf den Seiten
   - Übersicht
4. **Firewall**
   - Wie die Firewall entscheidet
   - Firewall-Modi
   - Was ein abgewiesener Besucher sieht
   - Sperren
   - Die eigene Adresse des Administrators
   - Adresslisten
   - Eigene Regeln
   - Fallenpfade und Pfade ohne Anfragegrenze
   - Schutz vor dem Aussperren
   - Firewall-Einstellungen
   - Wenn die Firewall selbst ausfällt
   - Grenzen der Firewall
   - OWASP-CRS-Regeln
5. **Dateiscanner**
   - Was ein Scan abdeckt
   - Einen Scan starten und abbrechen
   - Funde
   - Scanner-Einstellungen
6. **Remote-Scan und Lizenz**
   - Modi des Remote-Scans
   - Die Karte Remote-Scan
   - Was gesendet wird und was nie
   - Grenzen und Ablehnungen
   - Funde des Remote-Scans
   - Zugangsdaten und Speicherung
   - Konsole
7. **Anmeldeschutz**
   - Welche Anmeldungen gezählt werden
   - So funktioniert es

- Sperren und Anmeldesperren aufheben
- Gekürzte Adressen
- Einstellungen des Anmeldeschutzes

8. **Zwei-Faktor-Authentifizierung**
   - So funktioniert die Zwei-Faktor-Anmeldung
   - Anmelden
   - Wer die Seite öffnen kann
   - Den zweiten Schritt einrichten
   - Wiederherstellungscodes und Ausschalten
   - Für alle verlangen
   - Grenzen des zweiten Schritts
9. **Sicherheitscheck**
   - Ergebnisse und Punktzahl
   - Prüfungen
   - Aufgeführte Dateien und die Korrektur der Rechte
10. **Ereignisprotokoll und Benachrichtigungen**
    - Das Ereignisprotokoll lesen
    - Was aufgezeichnet wird
    - Ereignisstufen
    - Einstellungen des Ereignisprotokolls
    - Warn-Mails
    - Zusammenfassung per E-Mail
    - Einstellungen der Benachrichtigungen
11. **Einstellungsreferenz**
    - Einstellungen ändern
    - Werttypen
    - Gruppe Firewall
    - Gruppe Anfragelimit
    - Gruppe Fehlende Seiten
    - Gruppe Fallenpfade
    - Gruppe Eigene Regeln
    - Gruppe Sperren
    - Gruppe Anmeldeschutz
    - Gruppe Zwei-Faktor-Authentifizierung
    - Gruppe Ereignisprotokoll
    - Gruppe Benachrichtigungen
    - Gruppe Scanner
    - Gruppe Antwort-Header
    - Gruppe Remote-Scan
    - Gruppe OWASP-CRS-Regeln
12. **Kommandozeile**
    - Übersicht der Befehle
    - Status
    - Sicherheitscheck auf der Konsole
    - Scan auf der Konsole
    - Befehle für Funde
    - Ereignisse auf der Konsole
    - Befehle für Adresslisten
    - Entsperren
    - Einstellungen auf der Konsole
    - Wartung

- Remote-Scan auf der Konsole

I.3. Zurück ins System und Fehlerbehebung

- Ihre eigene Adresse ist gesperrt oder steht auf der Sperrliste
- Ein Benutzername oder eine Adresse ist gesperrt
- Auf der Seite zur Einrichtung der Zwei-Faktor-Anmeldung festgehalten
- Gerät verloren oder von der Zwei-Faktor-Anmeldung ausgesperrt
- Die Firewall weist alles ab
- Eine Regel oder ein Fallenpfad sperrt die Administration
- Alle Besucher haben dieselbe Adresse
- Warnungen, Zusammenfassungen oder Scans laufen nicht
- Mails kommen nicht an
- Meldungen des Plugins
- Die OWASP-CRS-Regeln weisen eine normale Anfrage ab

I.4. Datenschutz und externe Dienste

- Was das Plugin speichert
- Externe Dienste
- Ausschalten

I.5. Das Plugin entfernen

- Deaktivieren
- Deinstallieren
- Was mit einer verbundenen Lizenz geschieht
- Die Dateien entfernen

Einführung

ISPProtect Web Security ist ein Plugin für Shopware 6. Es schützt den Shop und seine Administration mit einer Anfrage-Firewall, einem Anmeldeschutz, einer Zwei-Faktor-Anmeldung für Benutzer der Administration, einem Dateiscanner, einem Sicherheitscheck, einem Ereignisprotokoll und Warnungen per E-Mail.

Was das Plugin leistet

- **Firewall.** Sie prüft jede Anfrage, bevor der Shop sie beantwortet. Sie arbeitet mit Adresslisten, Anfrageraten, Fallenpfaden und Regeln, die Sie selbst schreiben. Siehe Firewall.
- **Anmeldeschutz.** Er zählt fehlgeschlagene Anmeldungen an der Administration und von Kunden der Storefront, sperrt Adressen und Benutzernamen. Siehe Anmeldeschutz.
- **Zwei-Faktor-Authentifizierung.** Benutzer der Administration können einen zweiten Schritt mit einem Code aus einer Authenticator-App hinzufügen. Sie können ihn für jeden Benutzer der Administration verpflichtend machen. Siehe Zwei-Faktor-Authentifizierung.
- **Dateiscanner.** Er führt einfache Prüfungen der Dateien des Shops durch: Änderungen seit dem letzten Scan, ein paar allgemeine Prüfungen auf verdächtigen Code, unerwartete Dateien und installierte Composer-Pakete gegen veröffentlichte Sicherheitshinweise. Der Remote-Scan ist die gründliche Prüfung. Siehe Dateiscanner.
- **Remote-Scan.** Optional fragt der Scanner einen Scan-Dienst nach Code-Dateien. Siehe Remote-Scan und Lizenz.
- **Sicherheitscheck.** Er prüft den Server, PHP und den Shop und gibt eine Punktzahl mit Empfehlungen. Siehe Sicherheitscheck.
- **Ereignisprotokoll und Benachrichtigungen.** Es zeichnet sicherheitsrelevante Ereignisse auf und sendet Warnungen und eine Zusammenfassung per E-Mail. Siehe Ereignisprotokoll und Benachrichtigungen.
- **Antwort-Header.** Er kann den Header mit der PHP-Version entfernen und die Header HSTS und Permissions-Policy senden. Siehe Antwort-Header.

Was das Plugin nicht leistet

- Die Firewall schaut nicht in den Inhalt von Anfragen. Sie hat keine Liste von Angriffsmustern und erkennt keinen eingeschleusten Code oder Skript in einer Anfrage. Sie entscheidet nach Adresse, Anfragerate, Pfad und den Regeln, die Sie schreiben.
- Der Scanner liest Dateien nur. Er löscht, verschiebt, repariert oder isoliert nie eine Datei. Der lokale Scanner führt einfache Prüfungen durch und findet Änderungen. Er ist keine Garantie, dass ein Shop sauber ist. Eine Datei ohne Treffer seiner Prüfungen und Code, der in der Datenbank gespeichert ist, werden nicht gefunden.
- Das Plugin gibt keine Garantie, dass ein Shop sauber oder sicher ist.
- Das Plugin ändert keine Datei des Shopware-Kerns und keine Shopware-Tabelle.

Kostenlose und kostenpflichtige Teile

Alle oben genannten Funktionen arbeiten ohne Lizenz, mit einer Ausnahme. Der Remote-Scan im Modus **Gehosteter Scan-Dienst (Lizenz)** braucht einen Lizenzschlüssel. Der Modus **Lokaler Scan-Dienst (Socket)** braucht keinen Website-Schlüssel. Siehe Remote-Scan und Lizenz.

Voraussetzungen

- Shopware ab 6.7.16.0 innerhalb der Reihe 6.7 (das Plugin verlangt `shopware/core` `>=6.7.16.0 <6.8.0` und nennt keine andere Voraussetzung).
- Eine MySQL- oder MariaDB-Datenbank, wie Shopware sie nutzt. Das Plugin legt eigene Tabellen an, alle mit dem Präfix `ispprotect_`.
- Für die Prüfung auf bekannte Sicherheitslücken muss der Server HTTPS-Verbindungen zu `packagist.org` öffnen können.

- Für Warnungen und die Zusammenfassung per E-Mail müssen die Mail-Einstellungen des Shops funktionieren. Siehe Ereignisprotokoll und Benachrichtigungen.
- Ein laufender Scheduler und Message-Consumer, damit die Wartungsaufgabe läuft. Siehe Zeitplanung.

Wer es nutzen kann

Das Modul **ISPProtect Web Security** wird in der Administration nur Administratoren angezeigt (Benutzern mit dem Administrator-Kennzeichen). Es hat kein Recht, das Sie einer Rolle geben können. Benutzer, die keine Administratoren sind, sehen auf jeder Seite des Moduls außer **Zwei-Faktor** den Text „Dieser Bereich steht nur Administratoren zur Verfügung.“ Die Seite **Zwei-Faktor** ist für das eigene Konto jedes Benutzers der Administration. Siehe Zwei-Faktor-Authentifizierung.

Aufbau dieses Handbuchs

1. Einführung (dieses Kapitel)
2. Installation und erste Schritte
3. Das Modul in der Administration
4. Firewall
5. Dateiscanner
6. Remote-Scan und Lizenz
7. Anmeldeschutz
8. Zwei-Faktor-Authentifizierung
9. Sicherheitscheck
10. Ereignisprotokoll und Benachrichtigungen
11. Einstellungsreferenz
12. Kommandozeile
13. Zurück ins System und Fehlerbehebung
14. Datenschutz und externe Dienste
15. Das Plugin entfernen

Namen von Schaltflächen, Feldern und Tabs sind fett geschrieben, genau so, wie die Administration sie anzeigt. Einstellungsschlüssel, Werte, Befehle und Dateinamen sind als `Code` geschrieben. Konsolenbefehle sind so geschrieben, wie Sie sie im Hauptordner des Shops ausführen, zum Beispiel `bin/console ispprotect:status`.

Installation und erste Schritte

Das Plugin installieren

Der Hersteller liefert das Plugin als Zip-Datei. Sie können es in der Administration oder auf der Konsole installieren.

In der Administration:

1. Öffnen Sie **Erweiterungen > Meine Erweiterungen** und laden Sie die Zip-Datei mit **Erweiterung hochladen** hoch.
2. Klicken Sie beim Plugin auf **Installieren** und danach auf **Aktivieren**.

Auf der Konsole, mit dem Plugin-Ordner in `custom/plugins/ISPProtectWebSecurity` (oder mit Composer installiert als `ispprotect/shopware-web-security`):

```
bin/console plugin:refresh
bin/console plugin:install --activate ISPProtectWebSecurity
bin/console cache:clear
```

Was die Installation anlegt

Die Installation führt eine Datenbankmigration aus, die die Tabellen des Plugins anlegt. Alle beginnen mit `ispprotect_`. Beim Aktivieren und Aktualisieren des Plugins wird geprüft, ob die Tabellen vorhanden sind, fehlende werden angelegt und der Cache-Pool des Plugins wird geleert. Eine neue Version mit `plugin:update` zu installieren führt dieselben Prüfungen aus.

Das Plugin schreibt eine eigene Logdatei, `var/log/ISPProtectWebSecurity.log` (eine rotierende Datei, 14 Dateien werden behalten, Stufe info). Probleme innerhalb des Plugins landen dort.

Das Plugin fällt offen aus: Wenn einer seiner Teile ausfällt, wird die Anfrage oder Anmeldung, die gerade geprüft wird, nicht aufgehalten. Die Ausnahmen sind in den Kapiteln Anmeldeschutz und Zwei-Faktor-Authentifizierung genannt.

Das Modul öffnen

Öffnen Sie im Menü der Administration **Erweiterungen > ISPProtect Web Security**. Nur Administratoren sehen den Eintrag. Das Modul öffnet sich auf dem Tab **Übersicht**. Siehe Das Modul in der Administration.

Erste Schritte

1. Öffnen Sie den Tab **Übersicht**, um den Stand des Schutzes zu sehen.
2. Prüfen Sie den Firewall-Modus auf dem Tab **Firewall**. Die Vorgabe ist **Ein**.
3. Wenn der Shop hinter einem Reverse-Proxy oder CDN steht, setzen Sie `SYMFONY_TRUSTED_PROXIES`, bevor Sie irgendetwas anderes tun. Siehe Hinter einem Reverse-Proxy oder CDN. Sonst sehen alle Besucher wie eine einzige Adresse aus.
4. Tragen Sie unter **Adresse für Benachrichtigungen** auf dem Tab **Einstellungen** einen Empfänger für Warnungen ein. Bleibt das Feld leer, wird die E-Mail-Adresse aus den Basisinformationen des Shops (`core.basicInformation.email`) verwendet.
5. Starten Sie einen ersten Scan mit **Scan starten** auf dem Tab **Scanner** oder führen Sie `bin/console ispprotect:scan` aus. Der erste vollständige Scan hält den aktuellen Stand der Dateien fest. Spätere Scans melden Unterschiede dazu.
6. Richten Sie die Zwei-Faktor-Anmeldung für Ihr eigenes Konto auf dem Tab **Zwei-Faktor** ein, bevor Sie sie für alle verlangen.
7. Öffnen Sie den Tab **Sicherheitscheck** und arbeiten Sie die Ergebnisse durch.
8. Stellen Sie sicher, dass die geplante Aufgabe läuft. Siehe Zeitplanung.

`bin/console isppprotect:status` zeigt den Stand auf der Konsole.

Hinter einem Reverse-Proxy oder CDN

Das Plugin verwendet die Client-Adresse, die Symfony und Shopware melden. Shopware liest die Adresse aus Headern wie `X-Forwarded-For` nur bei Anfragen, die von einem vertrauenswürdigen Proxy kommen. Wenn der Shop hinter einem Reverse-Proxy, einem Load Balancer oder einem CDN steht, setzen Sie die Umgebungsvariable `SYMFONY_TRUSTED_PROXIES` auf die Adressen dieser Proxys, und nur auf diese. Sonst gilt:

- Alle Besucher teilen sich die Adresse des Proxys. Ein einziger schlechter Besucher kann dann zur Sperre des Proxys und aller Besucher dahinter führen, und die fehlgeschlagenen Anmeldungen aller Benutzer addieren sich.
- Oder, wenn Sie jeder Adresse vertrauen (`0.0.0.0/0` , `::/0` oder `REMOTE_ADDR` bei einem öffentlichen Shop), kann ein Besucher seine Adresse mit einem gefälschten Header selbst wählen.

Der Sicherheitscheck hat für beide Fälle die Prüfung „Vertrauenswürdige Proxys passen zum tatsächlichen Aufbau“. Siehe Sicherheitscheck. Wenn Sie sicher sein wollen, dass Ihre Proxys nie abgewiesen werden, tragen Sie ihre Adressen zusätzlich in die Erlaubnisliste ein. Siehe Adresslisten.

Zeitplanung

Das Plugin registriert eine geplante Aufgabe von Shopware, `isppprotect.maintenance` , die alle 5 Minuten läuft. Sie erledigt diese Arbeit:

- Sie sendet ausstehende Warn-Mails.
- Einmal pro Stunde entfernt sie alte Ereignisse, abgelaufene Sperren und abgelaufene Anmeldesperren.
- Sie startet den geplanten Scan, wenn er fällig ist, und bringt einen laufenden Scan pro Lauf um bis zu 20 Sekunden voran.
- Sie erneuert eine verbundene Lizenz, wenn das fällig ist. Siehe Remote-Scan und Lizenz.
- Sie sendet die Zusammenfassung per E-Mail, wenn sie fällig ist.

Läufe, die sich überschneiden, überspringen sich gegenseitig (die Sperre dauert höchstens 15 Minuten). Fehler werden protokolliert und halten den Scheduler nicht an.

Shopware führt geplante Aufgaben nur aus, wenn sein Scheduler und ein Message-Consumer laufen, wie bei jeder Shopware-Aufgabe. Führen Sie zum Beispiel `bin/console scheduled-task:run` und `bin/console messenger:consume` unter einem Prozess-Manager oder per Cron aus. Siehe die Dokumentation von Shopware. Ohne sie laufen Warnungen, die Zusammenfassung per E-Mail, die Bereinigung und der geplante Scan nicht. In diesem Fall können Sie dieselbe Arbeit von Hand oder per Cron ausführen mit:

```
bin/console isppprotect:maintenance
```

Ein Scan, den Sie auf dem Tab **Scanner** starten, läuft weiter, solange diese Seite geöffnet bleibt, auch ohne den Scheduler.

Das Modul in der Administration

Menüeintrag und Seiten

Das Plugin fügt das Modul **ISPProtect Web Security** dem Menü **Erweiterungen** der Administration hinzu. Das Modul zeigt seine Seiten als Tabs in einer Leiste. Die Leiste wird nur Administratoren angezeigt. Die Adresse eines Tabs ist `#/ispprotect/web-security/index/<tab>`. Das Modul öffnet sich auf **Übersicht**.

Seite	Was sie zeigt
Übersicht	Den Stand des Schutzes auf einen Blick.
Firewall	Eine Adresse hinzufügen, die Sperrliste, die Erlaubnisliste und die Sperren die Firewall-Einstellungen und die Karte der OWASP-CRS-Regeln. Siehe Firewall und OWASP-CRS-Regeln.
Anmeldeschutz	Gesperrte Benutzernamen, Anmeldesperren von Adressen, Firewall-Sperren und die Einstellungen des Anmeldeschutzes. Siehe Anmeldeschutz.
Scanner	Einen Scan starten und abbrechen, die Karte des Remote-Scans und die Funde. Siehe Dateiscanner.
Ereignisse	Das Ereignisprotokoll mit Filtern. Siehe Ereignisprotokoll und Benachrichtigungen.
Sicherheitscheck	Alle Ergebnisse der Prüfungen. Siehe Sicherheitscheck.
Einstellungen	Jede Einstellung, nach Bereichen gruppiert. Siehe Einstellungsreferenz.
Zwei-Faktor	Der zweite Schritt Ihres eigenen Kontos. Siehe Zwei-Faktor-Authentifizierung.
Handbuch	Dieses Handbuch, mit einem Link, um es als PDF herunterzuladen.

Benutzer, die keine Administratoren sind, sehen keine Tab-Leiste. Sie sehen auf jeder Seite außer **Zwei-Faktor** den Text „Dieser Bereich steht nur Administratoren zur Verfügung.“

Einstellungen auf den Seiten

Jede Gruppe von Einstellungen ist eine Karte mit den Schaltflächen **Speichern** und **Auf Standard zurücksetzen**. Der Tab **Einstellungen** zeigt alle Gruppen. Die Tabs **Firewall** und **Anmeldeschutz** zeigen die Gruppen, die zu ihnen gehören:

Tab	Gruppen
Firewall	Firewall, Sperren, OWASP-CRS-Regeln
Anmeldeschutz	Anmeldeschutz, Zwei-Faktor-Authentifizierung
Einstellungen	Firewall, Anfragelimit, Fehlende Seiten, Fallenpfade, Eigene Regeln, Sperren, Anmeldeschutz, Zwei-Faktor-Authentifizierung, Ereignisprotokoll, Benachrichtigungen, Scanner, Antwort-Header, Remote-Scan, OWASP-CRS-Regeln

Wie Sie speichern und zurücksetzen, ist in der Einstellungsreferenz beschrieben.

Übersicht

Die Übersicht zeigt diese Karten:

- **Sicherheitscheck**: die Punktzahl als Zahl von 100 („/ 100“), die Zähler „{fail} fehlgeschlagen, {warn} brauchen Aufmerksamkeit, {ok} in Ordnung“ oder „Nichts braucht Ihre Aufmerksamkeit.“ Der Link **Alle Prüfungen** führt zum Tab **Sicherheitscheck**.

- **Firewall**: der Firewall-Modus und die Zahlen **Aktive Sperren**, **Gesperrte Einträge**, **Erlaubte Einträge** und **Gesperrte Benutzernamen**. Der Link **Firewall** führt zum Tab **Firewall**.
- **Offene Funde**: die Anzahl der offenen Funde des Dateiscanners, mit den Zahlen je Stufe. Der Link **Scanner** führt zum Tab **Scanner**.
- **Letzter Scan**: der Status, das Datum und „{n} Dateien geprüft“ des letzten Scans oder „Es wurde noch kein Scan ausgeführt.“ Die Schaltfläche **Scan starten** startet einen Scan. Während ein Scan läuft, führt der Link „Laufenden Scan ansehen“ zum Tab **Scanner**.
- **Ereignisse der letzten 7 Tage**: die Zahlen je Stufe (**Info**, **Hinweis**, **Warnung**, **Alarm**) und eine Tabelle der letzten Ereignisse mit den Spalten **Zeit**, **Stufe**, **Ereignis** und **Adresse**. Der Link **Ereignisse** führt zum Tab **Ereignisse**.

Firewall

Die Firewall prüft jede Anfrage an die Storefront, die Store API und die Administration, bevor der Shop sie weiterleitet, eine Sitzung startet oder eine Anmeldung prüft. Sie sitzt vor der eigenen Verarbeitung von Shopware. Wenn der HTTP-Cache von Shopware eine Anfrage beantwortet, prüft die Firewall die Anfrage, wenn die Antwort gesendet wird. Seitenteile, die über ESI eingebunden werden (Pfad `/_esi/`), werden nie geprüft.

Die Einstellungen der Firewall stehen auf dem Tab **Firewall** und auf dem Tab **Einstellungen**. Siehe Firewall-Einstellungen.

Wie die Firewall entscheidet

Die Firewall entscheidet in dieser Reihenfolge:

1. Modus **Aus**: Die Anfrage passiert.
2. Eine Adresse auf der Erlaubnisliste: Die Anfrage passiert.
3. Eine Adresse auf der Sperrliste oder der Liste der Sperren: Die Anfrage wird mit Status 403 abgewiesen.
4. Eine Anfrage an einen Fallenpfad: Die Adresse wird gesperrt und die Anfrage wird mit Status 403 abgewiesen.
5. Ihre eigenen Regeln, der Reihe nach. Die erste passende Regel mit der Aktion `block` weist die Anfrage mit Status 403 ab. Eine Regel mit der Aktion `log` zeichnet die Anfrage nur auf.
6. Das Anfragelimit: Eine Adresse, die im Zeitfenster mehr Anfragen sendet als erlaubt, erhält Status 429. Anmeldeanfragen haben ein eigenes, niedrigeres Limit. Wenn eine Adresse innerhalb von 10 Minuten so oft abgewiesen wurde, wie **Sperren nach Abweisungen** angibt, wird sie gesperrt. Der Wert 0 schaltet diese Sperre aus.

Nach der Antwort zählt die Firewall Antworten „nicht gefunden“ (Status 404) je Adresse. Eine Adresse, die im Zeitfenster zu viele davon verursacht, wird gesperrt.

Die Firewall selbst arbeitet mit Adressen, Anfrageraten, Pfaden und den Regeln, die Sie selbst schreiben. Die Suche nach Angriffsmustern wie eingeschleustem SQL- oder Skript-Code ist ein eigener Teil, die OWASP-CRS-Regeln. Siehe OWASP-CRS-Regeln.

Welche Anfragen Anmeldeanfragen sind

Diese drei Pfade zählen für das niedrigere Limit **Anmeldeanfragen pro Zeitfenster** als Anmeldeanfragen:

- `/api/oauth/token`, die Token-Anfrage der Administration und von API-Clients
- `/account/login`, das Anmeldeformular der Storefront
- `/store-api/account/login`, die Anmeldung der Store API

Anfragen an `/api/oauth/token` mit dem Grant-Typ `refresh_token` oder `client_credentials` (Token-Erneuerungen der Administration und von Integrationen) zählen nicht als Anmeldeversuche und verbrauchen das Limit deshalb nicht.

Pfade, die nicht gezählt werden

Das Anfragelimit und die Zählung von „nicht gefunden“ überspringen diese Pfadpräfixe: `/bundles/`, `/theme/`, `/media/`, `/thumbnail/`, `/sitemap/`, `/_esi/`, `/api/_info/` und `/api/_admin/`. Weitere können Sie unter **Pfade ohne Anfragegrenze** eintragen.

Firewall-Modi

Die Einstellung **Firewall-Modus** hat drei Werte:

Wert	Bedeutung
Ein	Anfragen, die gegen eine Regel verstoßen, werden abgewiesen. Das ist die Vorgabe.

Wert	Bedeutung
Nur protokollieren	Die Firewall entscheidet und zeichnet auf, weist aber nie ab und sperrt nie. Eine Abweisung wird als Ereignis `firewall.logged` aufgezeichnet. Nutzen Sie das, um zu sehen, was die Firewall tun würde.
Aus	Die Firewall tut nichts.

Was ein abgewiesener Besucher sieht

Eine abgewiesene Anfrage erhält Status 403 oder 429. Die Antwort ist mit `Cache-Control: no-store, private` markiert und trägt einen Header `Retry-After`.

Sperren

Eine Sperre blockiert eine Adresse und endet nach einiger Zeit. Die erste Sperre einer Adresse dauert so viele Minuten, wie **Sperrdauer (Minuten)** angibt. Jede wiederholte Sperre derselben Adresse innerhalb von 30 Tagen dauert viermal so lang, bis zu **Längste Sperre (Minuten)**.

- IPv6-Adressen werden je /64-Bereich gezählt und gesperrt.
- Loopback-Adressen (zum Beispiel `127.0.0.1`) können nicht gesperrt werden.
- Eine Sperre können Sie auf dem Tab **Firewall** mit **Entfernen**, auf dem Tab **Anmeldeschutz** mit **Sperre aufheben** oder auf der Konsole aufheben. Siehe Adresslisten.

Die eigene Adresse des Administrators

Wenn sich ein Administrator an der Administration anmeldet, ist diese Adresse (bei IPv6: ihr /64-Bereich) 24 Stunden lang geschützt, solange **Adressen von Administratoren schützen** eingeschaltet ist. Eine geschützte Adresse überspringt nur die automatischen Maßnahmen:

- Sperren gelten für sie nicht.
- Sie wird nicht gegen die Fallenpfade, das allgemeine Anfragelimit und die Zählung von „nicht gefunden“ geprüft.

Die Sperrliste und Ihre eigenen Regeln gelten für sie wie für jede andere Adresse. Auch das Limit für Anmeldeanfragen gilt für sie, aber zu viele Anmeldeanfragen von ihr führen nicht zu einer Sperre. Nur die Erlaubnisliste lässt eine Adresse jeden Schritt überspringen. Zu viele fehlgeschlagene Anmeldungen von einer geschützten Adresse sperren die Anmeldung von dieser Adresse für eine Weile. Siehe Anmeldeschutz.

Wenn Sie **Adressen von Administratoren schützen** ausschalten und speichern, warnt Sie die Seite, dass eine Sperrregel, ein Fallenpfad oder das Anfragelimit Sie jetzt aus der Administration aussperren kann.

Adresslisten

Der Tab **Firewall** hat die Karte **Adresse hinzufügen** und die Karte **Einträge**.

In der Karte **Adresse hinzufügen** fügen Sie eine Adresse oder einen Bereich hinzu, zum Beispiel `203.0.113.7` oder `203.0.113.0/24`:

1. Wählen Sie die Liste: **Sperren** oder **Erlauben**. Die Sperren aus dem Abschnitt „Sperren“ weiter oben legt die Firewall selbst an. Auf der Konsole können Sie eine solche Sperre mit `ispprotect:ip:add` hinzufügen.
2. Tippen Sie die Adresse oder den Bereich in **Adresse oder Bereich**.
3. Tippen Sie optional eine **Notiz**.
4. Wählen Sie **Läuft ab**: **Nie**, **Nach 1 Stunde**, **Nach 1 Tag**, **Nach 7 Tagen** oder **Nach 30 Tagen**.
5. Klicken Sie auf **Hinzufügen**.

Wenn die Sperre Ihre eigene Adresse einschließt, fragt die Seite „Diese Sperre schließt Ihre eigene Adresse ein“ und sagt, dass Sie sich beim Speichern möglicherweise aus der Administration aussperren. Klicken Sie auf **Trotzdem sperren**, um sie zu speichern, oder auf **Abbrechen**.

Die Karte **Einträge** hat drei Listen: **Sperrliste**, **Erlaubnisliste** und **Sperren**. Jeder Eintrag zeigt **Adresse oder Bereich**, **Notiz**, **Quelle**, **Erstellt**, **Läuft ab**, **Verstöße** und **Status** (**Aktiv** oder **Abgelaufen**). **Quelle** sagt, was den Eintrag angelegt hat: `manual` für einen Eintrag, den Sie hinzugefügt haben, sonst die automatische Maßnahme (zum Beispiel `rate`, `notfound`, `trap` oder `login`). **Verstöße** zählt wiederholte Sperren der Adresse. Die Schaltfläche **Entfernen** löscht einen Eintrag. Eine leere Liste zeigt „Diese Liste enthält keine Einträge.“

Änderungen der Listen werden im Ereignisprotokoll aufgezeichnet. Auf der Konsole tun `ispprotect:ip:list`, `ispprotect:ip:add` und `ispprotect:ip:remove` dasselbe. Siehe Kommandozeile.

Eigene Regeln

Eine eigene Regel prüft einen Teil der Anfrage mit einem Vergleich und sperrt dann oder protokolliert.

Teil	Bedeutung
`path`	Der Pfad der Anfrage
`query`	Der Query-String
`user_agent`	Die Browser-Kennung
`referer`	Der Referrer
`method`	Die HTTP-Methode
`host`	Der Hostname

Die Vergleiche sind `equals`, `prefix`, `suffix`, `contains` und `regex`. Die ersten vier ignorieren Groß- und Kleinschreibung. Ein regulärer Ausdruck wird ohne Begrenzer geschrieben und passt ohne Beachtung der Groß- und Kleinschreibung. Ein Regelwert darf nicht leer sein und bis zu 500 Bytes lang sein. Sie können bis zu 100 Regeln festlegen.

Das Feld **Eigene Regeln** enthält die Regeln als JSON-Liste. Auf der Konsole enthält `rules.custom` dieselbe Liste. Jede Regel hat diese Schlüssel:

Schlüssel	Bedeutung
`id`	Optional. Buchstaben, Ziffern, `-` und `_`, bis zu 32 Zeichen.
`field`	Einer der Teile in der Tabelle oben
`op`	Einer der Vergleiche oben
`value`	Der Text, mit dem verglichen wird
`action`	`block` oder `log`
`enabled`	Optional. `true`, um die Regel zu verwenden (die Vorgabe), `false`, um sie auszuschalten

Beispiel:

```
bin/console ispprotect:settings:set rules.custom '[{"id":"no-env","field":"path","op":"suffix","value":".en
v","action":"block","enabled":true}]'
```

Fallenpfade und Pfade ohne Anfragegrenze

Fallenpfade und **Pfade ohne Anfragegrenze** sind Listen von Pfaden, einer pro Eintrag. Pfade werden in Kleinbuchstaben verglichen, mit führendem `/` und ohne abschließendes `/`. Ein Eintrag passt auf den ganzen Pfad oder auf den Anfang des Pfads, wenn er auf `*` endet: `/backup/*` passt auf `/backup` und `/backup/x`, aber nicht auf `/backups`. Bei **Pfade ohne**

Anfragegrenze passt jeder Eintrag auf den Anfang des Pfads. Ein Eintrag, der nur aus `/`, `*` und Leerzeichen besteht (er würde die ganze Website abdecken), wird abgelehnt.

Schutz vor dem Aussperren

Nachdem Sie die Einstellungen auf dem Tab **Firewall** gespeichert haben, prüft die Seite Ihre eigene Anfrage und warnt in diesen Fällen:

- „Der Schutz Ihrer eigenen Adresse ist ausgeschaltet. Eine Sperrregel, ein Fallenpfad oder die Anfragebegrenzung kann Sie jetzt aus der Administration aussperren."
- Ein Fallenpfad deckt einen Pfad der Administration ab: „Der Fallenpfad {entry} deckt den Administrationspfad {path} ab. Wer diesen Pfad öffnet, wird gesperrt, auch Sie." Geprüft werden die Pfade `/admin` und `/api/oauth/token`.
- Eine Sperrregel trifft für Ihre eigene Anfrage auf einen Pfad der Administration zu: „Die Sperrregel {rule} trifft für Ihre eigene Anfrage auf den Administrationspfad {path} zu. Sie kann Sie aussperren."

Das sind Warnungen. Die Einstellungen werden trotzdem gespeichert. Wenn Sie ausgesperrt sind, siehe Zurück ins System und Fehlerbehebung.

Firewall-Einstellungen

Der Tab **Firewall** zeigt die Gruppen **Firewall** und **Sperren** der Einstellungen. Die Gruppen **Anfragelimit**, **Fehlende Seiten**, **Fallenpfade** und **Eigene Regeln** stehen auf dem Tab **Einstellungen**. Alle Schlüssel, Vorgaben und Bereiche stehen in der Einstellungsreferenz.

Wenn die Firewall selbst ausfällt

Wenn die Datenbank oder der Cache ausfällt, lässt die Firewall die Anfrage durch und schreibt das Problem in die Logdatei des Plugins. Sie sperrt nicht alle aus wegen eines eigenen Fehlers.

Grenzen der Firewall

- Die Firewall kennt nur die Adresse, die Shopware als Client-Adresse meldet. Hinter einem Reverse-Proxy oder CDN setzen Sie `SYMFONY_TRUSTED_PROXIES`. Siehe Hinter einem Reverse-Proxy oder CDN.
- Die Anfragezähler sind ungefähr, wenn viele Anfragen gleichzeitig eintreffen.
- Gecachte Seiten, die ein Proxy vor Shopware beantwortet, erreichen den Shop nie. Um eine Adresse daran zu hindern, sie abzurufen, brauchen Sie eine Regel in Ihrem Proxy oder Webserver.

OWASP-CRS-Regeln

Das OWASP Core Rule Set (CRS) ist ein weit verbreiteter, offen gepflegter Satz von Regeln, der typische Angriffe auf Webanwendungen erkennt, zum Beispiel SQL-Injection, Cross-Site-Scripting, Versuche, Dateien zu lesen oder Befehle auszuführen, und Anfragen von Scannern und Angriffswerkzeugen. In der Administration sind sie eine Karte, **OWASP-CRS-Regeln**, auf dem Tab **Firewall**. Die CRS-Regeln sind der Teil der Firewall, der nach Angriffsmustern sucht; das Plugin fügt nur zwei eigene Regeln hinzu, für Anfragen, die die CRS-Regeln nicht erkennen (siehe ISPProtect-Regeln). Die Regeln laufen mit einer in PHP geschriebenen Engine des Plugins, ein zusätzliches Programm oder Servermodul ist nicht nötig. Sie sind aus, bis Sie sie installieren.

Die Karte **OWASP-CRS-Regeln** zeigt die installierte Version, den Zeitpunkt der Installation, die aktiven Regeln, die nicht unterstützten Regeln, ob eigene Regeln geladen sind, und die abgeschalteten Regeln. Sie hat die Schaltflächen **CRS 4.25.2 installieren** (oder **Auf CRS 4.25.2 aktualisieren**), **Regeln entfernen** und **Lizenz anzeigen** und das Feld **Regel abschalten**. Darunter stehen die Einstellungen der CRS-Regeln (siehe Einstellungsreferenz).

Die Regeln installieren

1. Öffnen Sie den Tab **Firewall** und klicken Sie in der Karte **OWASP-CRS-Regeln** auf **CRS 4.25.2 installieren**.
2. Das Plugin lädt eine feste Version der Regeln von GitHub (vom CRS-Projekt, in dieser Version des Plugins 4.25.2) über `https` herunter. Ihr Server braucht ausgehenden `https`-Zugriff auf `github.com` und auf den Download-Host, auf den GitHub weiterleitet, und PHP braucht `allow_url_fopen` und OpenSSL. Das Plugin vergleicht den Download mit einer Prüfsumme (SHA-256), die im Plugin eingebaut ist, und weist alles andere ab. Eine neuere Version der Regeln kommt nur mit einer neueren Version des Plugins; sonst wird nie etwas heruntergeladen oder ausgeführt.
3. Bei der ersten Installation setzt das Plugin den Modus (`waf.mode`) auf **Nur protokollieren**.

Die Seite zeigt danach die Version, die Prüfsumme, den Zeitpunkt der Installation, die Zahl der verwendeten Regeln und die Nummern der nicht unterstützten Regeln (siehe Was die CRS-Regeln nicht abdecken). Nach einem Plugin-Update kann die Seite melden, dass eine neue Version der Regeln verfügbar ist. Nach einem Update des Plugins meldet die Karte, wenn eine neue Version der Regeln verfügbar ist, und **Auf CRS aktualisieren** installiert sie. **Regeln entfernen** löscht sie nach Ihrer Bestätigung wieder. Die Regeln liegen in `var/ispprotect/waf`, außerhalb des öffentlichen Ordners.

Mit dem Protokollieren beginnen

Lassen Sie den Modus zuerst auf **Nur protokollieren**. In diesem Modus wird eine passende Anfrage nur ins Ereignisprotokoll geschrieben und nie abgewiesen. Sehen Sie die Einträge einige Tage an, in denen alle Arten von Seiten und Formularen und die Administration und der Storefront benutzt werden, schalten Sie Regeln ab, die normale Anfragen Ihrer Website melden (siehe unten), und stellen Sie den Modus erst dann auf **Blockieren**.

Wert	Wirkung
Aus (`off`)	Anfragen werden nicht mit den CRS-Regeln geprüft. Das ist der Zustand, bis Sie die Regeln installieren.
Nur protokollieren (`log`)	Eine Anfrage, die die Schwelle erreicht, wird als **Anfrage von der Firewall protokolliert** aufgezeichnet und geht durch.
Blockieren (`block`)	Eine Anfrage, die die Schwelle erreicht, wird mit Status 403 abgewiesen und als **Anfrage von der Firewall abgewiesen** aufgezeichnet.

Die CRS-Prüfung hat einen eigenen Modus (`waf.mode`) und hängt nicht vom Firewall-Modus ab. Sie läuft nach den Adresslisten, Sperren und Limits der Firewall: Eine Anfrage von einer Adresse auf der Erlaubnisliste wird nie mit den CRS-Regeln geprüft. Alle anderen werden geprüft, auch angemeldete Administratoren.

Einen Eintrag lesen

Eine Anfrage, die die Schwelle erreicht hat, steht im Ereignisprotokoll mit dem Ereignis **Anfrage von der Firewall protokolliert** oder **Anfrage von der Firewall abgewiesen**. Die Details enthalten:

- die Nummern und die Meldungen der Regeln, die gepasst haben, zum Beispiel `942190` und den Namen des vermuteten Angriffs,
- zu jeder Regel den Namen des Teils der Anfrage, der gepasst hat (zum Beispiel `ARGS:comment`, `REQUEST_COOKIES:name` oder `REQUEST_URI`), und einen kurzen Auszug des Werts, dessen empfindlicher Teil maskiert ist,
- die Gesamtpunktzahl, die Schwelle, die Paranoia-Stufe, die Methode, den Pfad und die Antwort (nie die Query-Zeichenfolge, die Header oder den Inhalt als solchen).

Eine Anfrage gilt als Angriff, wenn sich die Punktzahlen aller passenden Regeln zur **Anomalie-Schwelle** addieren. Jede Regel gibt je nach Schweregrad Punkte: ein kritischer Treffer 5, ein Fehler 4, eine Warnung 3 und ein Hinweis 2. Bei der Standardschwelle 5 genügt ein kritischer Treffer; bei einem höheren Wert müssen mehrere Regeln passen.

Hat die CRS-Prüfung selbst ein Problem (zum Beispiel sind die kompilierten Regeln nicht lesbar), geht die Anfrage durch und das Ereignis **Problem mit den CRS-Regeln** wird aufgezeichnet, höchstens einmal pro Stunde und Art des Problems.

Eine Regel meldet eine normale Anfrage

Meldet eine Regel Anfragen, die für Ihre Website normal sind (ein Fehlalarm), schalten Sie diese Regel ab:

1. Öffnen Sie den Eintrag im Ereignisprotokoll und notieren Sie Nummer und Meldung der Regel.

2. Tragen Sie in der Karte **OWASP-CRS-Regeln** die Nummer im Feld **Regel abschalten** ein und klicken Sie auf **Abschalten**.

Sie können Regelnummern auch von Hand unter **Abgeschaltete Regeln** (`waf.disabled_rules`) eintragen, eine pro Zeile. Eine abgeschaltete Regel läuft für keine Anfrage mehr, auch nicht für die, bei denen sie recht hatte; schalten Sie nur die falsche Regel ab, nicht eine ganze Gruppe. Haben Sie eine Regel versehentlich abgeschaltet, entfernen Sie ihre Nummer aus der Liste.

Paranoia-Stufe und Schwelle

Die **Paranoia-Stufe** (`waf.paranoia`, 1 bis 4, Standard 1) bestimmt, wie viele Regeln laufen. Stufe 1 enthält die Regeln mit sehr wenigen Fehlalarmen und wird für die meisten Websites empfohlen. Jede höhere Stufe fügt strengere Regeln hinzu, die mehr Angriffe finden und auch mehr normale Anfragen melden, vor allem in Formularen mit freiem Text, in Editoren und in Seiteninhalten. Erhöhen Sie die Stufe erst, wenn die Einträge der Stufe davor sauber sind, jeweils um eine Stufe, und beginnen Sie wieder mit dem Protokollieren.

Die **Anomalie-Schwelle** (`waf.threshold`, 1 bis 100, Standard 5) ist die Punktzahl, ab der eine Anfrage als Angriff gilt. Erhöhen Sie sie nur, wenn Sie in Kauf nehmen, dass einzelne Regeltreffer nicht mehr zählen.

Anfragen, die nicht vollständig geprüft werden können

Manche Anfragen lassen sich nicht vollständig prüfen: Der Inhalt ist größer, als die Engine liest, die Anfrage hat mehr Felder, als sie ansieht, der Inhalt ist nicht lesbar oder die Prüfung dauert zu lange. Ein Angreifer könnte so eine Anfrage nutzen, um die Regeln zu umgehen, daher behandelt das Plugin sie standardmäßig wie einen Angriff: Im Modus **Blockieren** wird sie abgewiesen, im Modus **Nur protokollieren** aufgezeichnet. Der Eintrag zeigt eine dieser Nummern:

Nummer	Bedeutung	Antwort bei Abweisung
`200002`	Der Inhalt war nicht lesbar (zum Beispiel ungültiges JSON oder XML).	400
`200004`	Der Inhalt ist ein Formular-Upload ohne abschließende Begrenzung.	400
`200005`	Das Muster einer Regel stieß an die Grenzen von PHP für reguläre Ausdrücke.	403
`200007`	Mehr Felder, Header, Cookies oder Teile, als die Engine prüft (1000).	403
`200100`	Das Zeitlimit der Anfrage war aufgebraucht, bevor alle Regeln liefen.	403
`200101`	Der Inhalt ist größer als die **Geprüfte Größe des Inhalts**.	413
`200102`	Ein Wert ist länger, als die Engine prüft (65536 Bytes).	403

Sie können diese Nummern wie jede andere Regel abschalten. Zwei Einstellungen sind für die beiden häufigen Fälle da:

- **Geprüfte Größe des Inhalts** (`waf.body_limit`, 1024 bis 1048576 Bytes, Standard 131072 = 128 KiB). Eine größere Anfrage kann nicht vollständig geprüft werden. Ein Speichervorgang mit sehr viel Inhalt kann größer sein und wird dann mit Status 413 und der Nummer `200101` beantwortet. Scheitern große Speichervorgänge im Modus **Blockieren**, erhöhen Sie den Wert, zum Beispiel auf 524288, oder lassen Sie solche Anfragen durch (siehe unten).
- **Zeitlimit pro Anfrage** (`waf.time_budget_ms`, 5 bis 10000 Millisekunden, Standard 200). Die Zeit, die die Regeln für eine Anfrage höchstens brauchen dürfen. Eine normale Seite oder ein Speichervorgang braucht 2 bis 10 Millisekunden, das Speichern von 42 KB Inhalt etwa 100 Millisekunden auf dem Server, auf dem gemessen wurde. Eine Anfrage nahe der Inhaltsgrenze kann bei Paranoia-Stufe 2 den Standard erreichen. Brechen Anfragen mit `200100` ab, erhöhen Sie den Wert. Halten Sie ihn so niedrig, wie Ihre Website es erlaubt: Das Limit ist auch das, was ein Angreifer Ihren Server für eine Anfrage aufwenden lassen kann.
- **Programmcode in einem Formularfeld.** Programmcode, der in ein Formularfeld eingefügt wird (eingerückter PHP- oder Python-Code, etwa 20 bis 40 KB), kann das voreingestellte Zeitlimit von 200 Millisekunden aufbrauchen; die Anfrage wird dann im Modus Blockieren mit `200100` abgelehnt. Erhöhen Sie bei einer Website, auf der Programmcode in Formulare eingefügt wird, das Zeitlimit, schalten Sie `200100` ab oder lassen Sie Anfragen durch, die nicht vollständig geprüft werden können. Normaler Text, HTML und die Speichervorgänge der Editoren, die die Ausnahmen abdecken, sind nicht betroffen.

- **Grenzen der Muster.** Selten bringt ein langes Feld mit Programmcode das Muster einer CRS-Regel über die Grenzen von PHP für reguläre Ausdrücke, und die Anfrage wird mit `200005` abgelehnt. Die Antworten sind dieselben: Schalten Sie `200005` ab oder lassen Sie Anfragen durch, die nicht vollständig geprüft werden können.

Anfragen durchlassen, die nicht vollständig geprüft werden können (`waf.pass_uninspected`, Standard aus) lässt solche Anfragen durch (sie werden trotzdem aufgezeichnet). Große Speichervorgänge funktionieren dann weiter, aber eine präparierte Anfrage, die zu groß oder zu langsam ist, wird nicht mehr vollständig geprüft. Nutzen Sie dies nur, wenn Sie die Limits nicht erhöhen können, oder schalten Sie die einzelne Nummer ab, die das Problem verursacht, zum Beispiel `200100`.

Ein XML-Anfrageinhalt mit einer Entitätsdeklaration oder einem Verweis auf eine externe DTD wird im Modus **Blockieren** auch bei eingeschaltetem **Anfragen durchlassen, die nicht vollständig geprüft werden können** mit `200002` (HTTP 400) abgewiesen. Heruntergeladene CRS-Ausnahmen können weder `200002` noch die Regel `200004` für eine fehlende Multipart-Begrenzung entfernen; beide Nummern lassen sich in den Einstellungen ausdrücklich abschalten.

Ausnahmen für Shopware

Das Plugin bringt eigene Ausnahmeregeln in `rules/shopware-exclusions.conf` mit. Sie werden vor den CRS-Regeln geladen und haben die Nummern 10000 bis 10999. Jede ist auf eine Route und auf benannte Felder begrenzt, und keine schaltet eine ganze Art von Angriffen ab. Sie beseitigen Fehlalarme, die normale Arbeit in der Administration und im Storefront bei den Paranoia-Stufen 1 und 2 ausgelöst hat:

- das Cookie `bearerAuth` der Administration, solange es die Form des Token-Cookies hat,
- die Felder `redirectParameters`, `forwardParameters` und `errorParameters` der Storefront-Formulare, solange sie ein einfaches JSON-Objekt enthalten,
- die Adressfelder von Registrierung, Gastbestellung und Adressbuch sowie die Nachricht des Kontaktformulars und von Produktbewertungen (nur die SQL-Injection-Regeln überspringen diese),
- die E-Mail-Templates sowie Kopf- und Fußzeilen von E-Mails (Twig-Code),
- die Inhalte der Erlebniswelten (Textelemente mit HTML, Einbettungen),
- die Schriftlisten der Theme-Konfiguration, der Medien-Upload (Inhaltstyp der Datei, Adresse eines Uploads per URL) und der Regel-Builder,
- die Textfelder der Seiten von ISPProtect Web Security, nur auf ihrem Speicherweg.

Die CRS-Regeln laufen, bevor Shopware den Token oder die Sitzung prüft, daher kann auch eine nicht angemeldete Anfrage diese Routen nennen. Shopware weist so eine Anfrage selbst ab, die übersprungenen Felder werden also nur für angemeldete Benutzer verarbeitet. Alle anderen Felder, Header und Cookies werden weiter geprüft.

> Pfade werden an ihrem Ende verglichen, ein Shop in einem Unterordner und Verkaufskanal-Domains mit Pfad behalten daher ihre Ausnahmen. Zwei Regeln, für E-Mail-Templates und für die Einstellungen des Plugins, sind am Anfang des Pfads verankert. Ein Shop in einem Unterordner erhält diese beiden nicht. Sie sehen dann mehr Einträge, der Schutz ist aber nicht schwächer.

ISPProtect-Regeln

Das Plugin bringt zwei eigene Regeln in `rules/ispprotect-shopware.conf` mit, mit den Nummern 12000 bis 12999. Sie melden Anfragen, die die CRS-Regeln auf Paranoia-Stufe 1 nicht erkennen. Sie laufen mit den CRS-Regeln, also nur, solange die CRS-Regeln installiert sind und der Modus **Nur protokollieren** oder **Blockieren** ist: nach den CRS-Regeln, vor den Regeln Ihrer eigenen Datei und vor der Entscheidung über die Schwelle. Jeder Treffer zählt als kritisch (5), mit der voreingestellten Schwelle reicht also ein Treffer. Die Karte **OWASP-CRS-Regeln** zeigt in der Zeile **ISPProtect-Regeln in Gebrauch**, wie viele davon laufen.

Regel	Meldet
`12001`	Die Versionsverwaltungsordner von Bazaar (`.bzr/`) und Darcs (`_darcs/`) und die Dateien `CVS/Entries`, `CVS/Root` und `CVS/Repository`. `.git/`, `.svn/`, `.hg/` und `.env` melden die CRS-Regeln selbst.

Regel	Meldet
`12002`	Kopien von PHP- und YAML-Dateien (auch `.phtml`, `.phar`, `.inc`) mit der Endung `.orig` oder `.rej`, einer Zahl (`shopware.yaml.1`) oder einem nummerierten `.bak`, `.old` oder `.save` (`index.php.bak1`) sowie die Emacs-Dateien `#name#` und `.#name`. `.bak`, `.old`, `.save`, `.swp`, `.pem` und `~` melden die CRS-Regeln selbst.

Wann die Regeln helfen:

- Die Regeln sehen nur Anfragen, die den Front-Controller von Shopware (`public/index.php`) erreichen. Mit der `.htaccess`-Datei von Shopware geht eine Anfrage nach einer Datei, die es im öffentlichen Ordner nicht gibt, an Shopware, das mit „nicht gefunden“ antwortet. Die Regeln weisen eine solche Anfrage ab und zeichnen sie mit ihrer Nummer auf, so erscheint eine Suche nach liegen gebliebenen Dateien im Protokoll als das, was sie ist.
- Eine Datei, die es im öffentlichen Ordner gibt, liefert der Webserver ohne Shopware aus, und ein vorhandenes PHP-Skript führt PHP ohne Shopware aus. Diese Anfragen sehen die Regeln nie und können sie nicht aufhalten, auch keine echte Kopie `index.php.orig`.
- Anfragen an die Ordner `media`, `thumbnail`, `theme`, `bundles`, `css`, `fonts` und `js` erreichen Shopware nie: Seine `.htaccess`-Datei und die nginx-Konfiguration der Shopware-Dokumentation beantworten sie ohne Shopware. Deshalb hat das Plugin keine Regel für PHP-Skripte in den Medienordnern; nur der Server kann sie abweisen.

Die eigentliche Abhilfe ist die Konfiguration des Webservers und ein aufgeräumter öffentlicher Ordner: Der Server weist Versionsverwaltungsordner und Kopien von Dateien ab und führt in `media` und `thumbnail` kein PHP aus. Die Prüfung **Keine Sicherungen oder Debug-Dateien im öffentlichen Ordner** des Sicherheitschecks führt Sicherungen und Debug-Dateien auf, die sie im öffentlichen Ordner findet.

Die Regeln werden wie CRS-Regeln abgeschaltet: eine Regel über ihre Nummer (das Feld **Regel abschalten** oder **Abgeschaltete Regeln** in den Einstellungen), beide mit der Zeile `SecRuleRemoveByTag ispprotect` in Ihrer eigenen Regeldatei (siehe unten) oder mit dem Tag `ispprotect/source-disclosure`. Ein Update des Plugins kann geänderte Regeln bringen; das Plugin kompiliert die Regeln dann bei der nächsten Anfrage neu.

Eigene CRS-Regeln

Sie können eigene Regeln in SecLang, der Sprache des CRS, in die Datei `var/ispprotect/rules/own.conf` Ihrer Installation schreiben. Das Plugin legt die Datei nie an. Die Seite zeigt, ob sie in Gebrauch ist. Regeln darin:

- brauchen eine Nummer von 11000 bis 11999; eine Regel mit anderer Nummer wird übersprungen,
- laufen nach den CRS-Regeln und vor der Entscheidung über die Schwelle, eine Regel kann also zur Punktzahl beitragen,
- nutzen die Teilmenge von SecLang, die die Engine unterstützt: `SecRule`, `SecAction`, `SecMarker`, `SecRuleRemoveById`, `SecRuleRemoveByTag`, `SecRuleUpdateTargetById` und `SecRuleUpdateTargetByTag` sowie Ketten. Regeln, die etwas anderes brauchen, werden übersprungen und als nicht unterstützt gezählt.

Ein Beispiel, das für ein PHP-Tag in einem Parameter eine kritische Punktzahl addiert:

```
SecRule ARGS "@rx (?i)<\?php" \
    "id:11001,phase:2,block,t:none,t:urlDecodeUni,\
    msg:'PHP open tag in a parameter',severity:'CRITICAL',\
    setvar:'tx.inbound_anomaly_score_pl1=+%{tx.critical_anomaly_score}'"
```

Das Plugin bemerkt eine geänderte Datei bei der nächsten Anfrage und kompiliert die Regeln neu. Lassen sie sich nicht kompilieren, läuft die CRS-Prüfung nicht, Anfragen gehen durch und das Problem wird als **Problem mit den CRS-Regeln** aufgezeichnet.

Was die CRS-Regeln nicht abdecken

- Das Plugin prüft nur Anfragen. Regeln für Antworten (die „Response“-Phasen des CRS) laufen nicht.
- Regeln, die die Bibliothek libinjection brauchen, laufen nicht, weil PHP sie nicht hat: `941100` und `941101` (XSS) sowie `942100` und `942101` (SQL-Injection). Die übrigen CRS-Regeln für diese Angriffe laufen. Die Seite listet die nicht unterstützten Regeln.

- Die Teil-Header eines Formular-Uploads (`MULTIPART_PART_HEADERS`) sind nicht verfügbar, weil PHP den Upload liest, bevor das Plugin ihn sieht. Dateinamen und Größen werden geprüft.
- Die CRS-Prüfung sieht nur die Anfrage an. Sie scannt keine Dateien und ersetzt keine Updates.

Kosten der Prüfung

Bei einer normalen Anfrage kostet die Prüfung 2 bis 10 Millisekunden. Das Speichern von 42 KB Inhalt dauerte etwa 100 Millisekunden. Ab Paranoia-Stufe 2 und bei großem Inhalt dauert die Prüfung länger; das Zeitlimit stoppt sie beim eingestellten Wert. Programmcode in einem Formularfeld (etwa 20 bis 40 KB eingerückter PHP- oder Python-Code) kann das voreingestellte Zeitlimit von 200 Millisekunden aufbrauchen; normaler Text, HTML und die Speichervorgänge der Editoren, die die Ausnahmen abdecken, nicht.

Wenn die CRS-Regeln Sie aussperren

Schalten Sie die CRS-Prüfung auf der Konsole ab:

```
bin/console ispprotect:settings:set waf.mode off
```

Melden Sie sich danach wieder an, suchen Sie im Ereignisprotokoll die Regel, die das Problem verursacht hat, schalten Sie sie ab und stellen Sie den Modus wieder auf **Nur protokollieren**. Siehe auch Zurück ins System und Fehlerbehebung.

Lizenz und Hinweis

Verwendet das OWASP® Core Rule Set (CRS) 4.25.2, © Trustwave Holdings, Inc. und die Mitwirkenden des OWASP-CRS-Projekts, lizenziert unter der Apache License 2.0. Die Regeln werden direkt vom CRS-Projekt auf GitHub heruntergeladen. OWASP® ist eine eingetragene Marke der OWASP Foundation; ISPProtect ist nicht mit OWASP verbunden und wird nicht von OWASP unterstützt.

Die Seite zeigt denselben Text. Der Lizenztext des CRS ist Teil des Downloads; die Schaltfläche **Lizenz anzeigen** zeigt ihn.

Dateiscanner

Der Scanner führt einfache Prüfungen der Dateien des Shops durch: Änderungen, PHP in Upload-Ordnern, übrig gebliebene Dateien und ein paar allgemeine Prüfungen auf verdächtigen Code. Der Remote-Scan ist die gründliche Prüfung. Der Scanner liest nur. Er löscht, verschiebt, repariert oder isoliert nie eine Datei. Sie entscheiden, was mit jedem Fund geschieht. Der Scanner steht auf dem Tab **Scanner** und auf der Konsole. Siehe Scanner-Einstellungen.

Was ein Scan abdeckt

Ein Scan hat diese Schritte, die die Karte **Fortschritt des Scans** als Phasen zeigt: „Dateien werden gelesen“, „Entfernte Dateien werden gesucht“, „Dateien werden vom Scan-Dienst geprüft“ (nur wenn der Remote-Scan eingeschaltet ist), „Das öffentliche Verzeichnis wird geprüft“, „Bekannte Sicherheitslücken werden geprüft“ und „Der Scan wird abgeschlossen“.

- **Geänderte Dateien.** Der Scanner hält einen Ausgangsstand der Dateien im Hauptordner des Shops (der Projektwurzel) fest: ihre Größe und Prüfsumme. Spätere Scans vergleichen damit. Das ist eingeschaltet, wenn **Geänderte Dateien erkennen** eingeschaltet ist.
- **Verdächtiger Inhalt.** Einfache, allgemeine Prüfungen suchen in den Code-Dateien nach häufigen Anzeichen für Schadcode. Sie erkennen keinen bekannten Schadcode; dafür dient der Remote-Scan. Das ist eingeschaltet, wenn **Nach Schadcode suchen** eingeschaltet ist. Er liest den Inhalt der Ordner `public/theme`, `public/bundles`, `public/media`, `public/thumbnail`, `public/sitemap` und `files` sowie der Code-Dateien der Projektwurzel. Auch Template-Dateien (`twig`, `tpl`, `stub`, `dist`, `template`) zählen als Code-Dateien.
- **Unerwartete Uploads.** PHP-Dateien in den Upload-Ordnern `public/media`, `public/thumbnail` und `files`.
- **Übrig gebliebene Dateien.** Dateien im öffentlichen Ordner, die dort nicht hingehören.
- **Bekannte Sicherheitslücken.** Die installierten Composer-Pakete werden gegen die veröffentlichten Sicherheitshinweise von Packagist geprüft. Das ist eingeschaltet, wenn **Auf bekannte Sicherheitslücken prüfen** eingeschaltet ist. Siehe Datenschutz und externe Dienste.
- **Remote-Scan.** Optional prüft ein Scan-Dienst die Code-Dateien. Siehe Remote-Scan und Lizenz.

Der Scanner überspringt immer den Ordner `var`, die Ordner `node_modules` und `.git` und die Pfade unter **Ausgenommene Pfade**. Das Plugin schaut nicht in die Datenbank.

Der erste Scan

Der erste vollständige Scan mit eingeschaltetem **Geänderte Dateien erkennen** hält den aktuellen Stand der Dateien fest. Er meldet keine geänderten oder neuen Dateien. Spätere Scans melden die Unterschiede. Dateien von Composer-Paketen, die Sie aktualisieren, werden nicht als geändert gemeldet.

Ausgenommene Pfade

Ausgenommene Pfade nimmt Pfade relativ zum Hauptordner des Shops an, einen pro Eintrag, zum Beispiel `public/uploads-test`. Ein Eintrag deckt den Ordner und alles darunter ab. Ein führendes `./` und `/` werden ignoriert. **Größte geprüfte Datei (KB)** legt die Größe fest, ab der eine Datei nicht gelesen wird. Die Vorgabe ist 5120.

Einen Scan starten und abbrechen

Auf dem Tab **Scanner** hat die Karte **Scan** die Schaltfläche **Scan starten**. Während ein Scan läuft, heißt die Schaltfläche **Scan abbrechen**, und die Karte zeigt den Status (**Läuft**, **Abgeschlossen**, **Fehlgeschlagen** oder **Abgebrochen**) und die Zähler **Dateien**, **Größe**, **Skripte** und **Funde**. Ein abgebrochener Scan zeigt „Der Scan wurde abgebrochen.“

Ein Scan läuft in Schritten von bis zu 200 Dateien. Solange der Tab **Scanner** geöffnet ist, bringt die Seite den Scan voran. Ist die Seite geschlossen, bringt die geplante Aufgabe ihn pro Lauf um bis zu 20 Sekunden voran. Siehe Zeitplanung. Ein Scan, dessen Position sich 6 Stunden nicht bewegt hat, gilt als tot.

Auf der Konsole startet `bin/console ispprotect:scan` einen Scan und zeigt seinen Fortschritt. Siehe Kommandozeile.

Geplanter Scan

Wenn **Zeitplan der Dateiprüfung** auf **Täglich** oder **Wöchentlich** steht, startet die geplante Aufgabe einen Scan, wenn er fällig ist. **Uhrzeit der Dateiprüfung** ist die Stunde, ab der ein Scan starten darf. Die Stunde zählt in UTC. Ein täglicher Scan startet höchstens einmal pro Kalendertag (UTC). Ein wöchentlicher Scan startet, wenn in den letzten 7 Tagen kein Scan gestartet wurde. Der Wert **Aus** schaltet den Zeitplan aus.

Funde

Die Karte **Funde** listet die Funde auf. Sie können nach **Stufe ab** und **Art** filtern. Jede Zeile zeigt die Art, die Datei oder das Paket (**Datei oder Paket**), eine Zeilennummer („Zeile {line}“), wenn es eine gibt, **Zuerst gesehen** und den Status.

Arten und Stufen

Art	Stufe	Bedeutung
Geänderte Datei	2	Eine Datei weicht vom Ausgangsstand ab.
Neue Datei	2	Eine Datei ist nicht im Ausgangsstand.
Entfernte Datei	1	Eine Datei des Ausgangsstands ist weg.
Verdächtiger Inhalt	3 oder 2	Eine Code-Datei hat einen Treffer der Inhaltsprüfung. Stufe 3 für Schadcode, Stufe 2 für verdächtig.
Unerwarteter Upload	3	Eine PHP-Datei in einem Upload-Ordner.
Bekannte Schwachstelle	3 bis 1	Ein Paket hat einen veröffentlichten Sicherheitshinweis. Kritisch und hoch ist Stufe 3, niedrig ist Stufe 1, alle anderen Stufe 2.
Übrig gebliebene Datei	2	Eine Datei im öffentlichen Ordner, die dort nicht hingehört.
Vom Scan-Dienst gefundener Schadcode	3	Der Scan-Dienst meldet Schadcode.

Die Stufen des Plugins sind 1 bis 3. Für jeden Fund der Stufe 3 zeichnet der Scan ein Ereignis `scan.finding` auf (höchstens 20 pro Scan), und das Plugin sendet eine Warn-Mail. Siehe Ereignisprotokoll und Benachrichtigungen.

Status eines Fundes

Ein Fund ist **Offen**, **Ignoriert** oder **Behoben**. Ein Fund wird **Behoben**, wenn ihn ein späterer Scan nicht mehr meldet oder wenn Sie ihn übernehmen.

Aktionen für einen Fund

- **Ignorieren** nimmt einen offenen Fund aus der Zahl der offenen Funde. Bei einem Fund zu einer Datei bleibt der Fund ignoriert, solange sich der Inhalt der Datei nicht ändert. Ändert sich die Datei, ist der Fund wieder offen.
- **Nicht mehr ignorieren** macht einen ignorierten Fund wieder offen.
- **Übernehmen** wird für geänderte, neue und entfernte Dateien angeboten. Es macht den aktuellen Stand zum neuen Ausgangsstand. Eine geänderte oder neue Datei wird nur übernommen, wenn sie noch den Inhalt hat, den der Scan gesehen hat. Hat sie sich nach dem Scan geändert, wird nichts übernommen. Eine geänderte Datei behält ihren alten Eintrag im Ausgangsstand, bis Sie sie übernehmen.
- **Alle Änderungen übernehmen** übernimmt alle offenen und ignorierten Funde der Arten geändert, neu und entfernt, in Stapeln von 200. Eine Rückfrage fragt „Alle geänderten, neuen und entfernten Dateien übernehmen?“ und sagt „{count} Funde werden zum neuen Ausgangsstand. Übernehmen Sie sie nur, wenn Sie wissen, dass die Änderungen von Ihnen stammen.“ Klicken Sie auf „{count} Funde übernehmen“. Das Ergebnis sagt „{accepted} übernommen, {skipped} übersprungen, weil sich die Datei nach dem Scan geändert hat.“
- **Zeilen zeigen** zeigt unter der Zeile des Funds die Zeilen seiner Datei, so wie die Datei jetzt ist: höchstens 4 Zeilen vor und nach der Zeile des Funds, die Zeile des Funds ist markiert. Nennt der Fund keine Zeile, werden die ersten Zeilen der Datei gezeigt. **Zeilen ausblenden** schließt sie. Es wird nichts geändert.

Übernehmen Sie eine Änderung nur, wenn Sie wissen, dass sie von Ihnen stammt, zum Beispiel nach einem Update oder einem Deployment.

Zeilen einer Datei

Statt der Zeilen erscheint ein Hinweis, wenn die Datei nach dem Scan entfernt oder verschoben wurde, wenn sie Passwörter oder Schlüssel enthalten kann, wenn der Pfad ein symbolischer Link ist, keine reguläre Datei ist, mehr als eine harte Verknüpfung hat oder aus dem Hauptordner des Shops hinausführt, oder wenn die Datei größer als 5 MB ist. Dateien, die Passwörter oder Schlüssel enthalten können, sind zum Beispiel `.env`-Dateien, `.htaccess`, `config/jwt`, Schlüsseldateien, Datenbank-Dumps und der Ordner `var`: die Dateien, die der Remote-Scan nie oder nur geschwärzt sendet, siehe Remote-Scan und Lizenz. Das gilt auch für Sicherungen und Kopien von Editoren solcher Dateien, zum Beispiel `.env.bak` oder `.env.swp`. Der Inhalt von Archiven und Datenbank-Dumps (zum Beispiel `.sql`, `.sql.gz`, `.zip`, `.tar.gz`) und von übrig gebliebenen Dateien wird nie angezeigt. Ein Hinweis sagt auch, wenn die Datei nach dem letzten Sehen des Funds geändert wurde, und wenn eine Zeile nach 500 Zeichen abgeschnitten wurde. Zeichen, die nicht sicher angezeigt werden können (Steuerzeichen, unsichtbare Zeichen und Zeichen, die die Schreibrichtung ändern), erscheinen als `�`. Nur Administratoren sehen die Zeilen.

Scanner-Einstellungen

Die Einstellungen stehen in der Gruppe **Scanner** auf dem Tab **Einstellungen**. Alle Schlüssel, Vorgaben und Bereiche stehen in der Einstellungsreferenz.

Remote-Scan und Lizenz

Der Remote-Scan ist optional und standardmäßig ausgeschaltet. Mit ihm fragt der Dateiscanner zusätzlich einen Scan-Dienst nach den Code-Dateien des Shops. Der Dienst kennt Prüfsummen von Dateien, die als harmlos oder als schädlich bekannt sind, und kann so Schadcode finden, den die einfachen lokalen Prüfungen nicht finden. Der Remote-Scan ist die gründliche Prüfung. Alles andere am Scanner funktioniert ohne ihn. Der lokale Scan ist im Dateiscanner beschrieben.

Ein Scan hängt nie vom Remote-Teil ab. Wenn der Dienst nicht erreichbar ist oder ablehnt, wird der lokale Scan trotzdem fertig, und der Scan hält fest, dass der Remote-Teil fehlgeschlagen ist oder nur teilweise lief. Nach einem internen Fehler des Remote-Teils erhält das Ereignisprotokoll außerdem einen Hinweis mit dem Grund `remote_failed`.

Den Modus stellen Sie auf dem Tab **Einstellungen** ein (**Remote-Scan**, Schlüssel `remote.mode`) und die Verbindung pflegen Sie in der Karte **Remote-Scan** auf dem Tab **Scanner**.

Modi des Remote-Scans

Wert	Was er tut
`off`	Sendet nichts. Das ist die Vorgabe.
`daemon`	Nutzt einen Scan-Dienst auf demselben Server, über den Socket in **Socket des lokalen Scan-Dienstes** (Vorgabe `/run/ispprotect/scand.sock`). Er braucht keinen Zugangstoken und sendet nichts an einen anderen Computer.
`service`	Nutzt einen Scan-Dienst, den Sie selbst betreiben, unter der Adresse in **Adresse des Scan-Dienstes**. Er braucht einen Zugangstoken. Die Adresse muss HTTPS verwenden; einfaches HTTP wird nur auf der Loopback-Adresse akzeptiert.
`license`	Nutzt den gehosteten Scan-Dienst. Er braucht eine verbundene Lizenz, also einen Lizenzschlüssel aus dem Lizenzportal.

Nur der gehostete Scan-Dienst (`license`) braucht einen Lizenzschlüssel. Der lokale Scan-Dienst (`daemon`) braucht keinen Schlüssel für die Website.

Der gehostete Scan-Dienst unter `https://scan.ispprotect.com` und die Lizenz-API unter `https://license.ispprotect.com` sind eingebaut; Sie brauchen nur den Lizenzschlüssel. Die Einstellung **Adresse des gehosteten Scan-Dienstes** (`remote.hosted_url`) ist eine optionale Überschreibung zum Testen und bleibt normalerweise leer. `remote.portal_url` überschreibt sie nur für eine andere Portal-Installation, mit `ispprotect:settings:set` auf der Konsole. Die Konto-Konsole unter `https://console.ispprotect.com` ist nicht die Scan-API.

Der Remote-Scan braucht die eingeschaltete Inhaltsprüfung des Scanners (`scanner.content`). Der Remote-Teil läuft zwischen der Prüfung auf entfernte Dateien und der Prüfung des öffentlichen Ordners. Der Modus wird gelesen, wenn der Scan startet. Wenn Sie den Modus ändern, während ein Scan läuft, endet der Remote-Teil dieses Scans, und der nächste Scan nutzt den neuen Modus.

Die Karte Remote-Scan

Die Karte auf dem Tab **Scanner** zeigt den Modus und einen kurzen Hilfetext dazu sowie den Link **Modus in den Einstellungen ändern**. Wenn der Modus nicht `off` ist, zeigt sie auch die verwendete Adresse. Im Modus `daemon` oder `service` zeigt sie den Socket oder die Adresse des Scan-Dienstes, oder **Nicht gesetzt**, wenn die Einstellung leer ist.

Die Schaltfläche **Verbindung testen** erscheint, wenn der Modus nicht `off` ist. Sie fragt den Dienst nach seinem Status und zeigt diese Angaben, soweit der Dienst sie meldet:

Angabe	Bedeutung
Engine	Die Scan-Engine des Dienstes.
Signaturen	Die Anzahl der Signaturen.

Angabe	Bedeutung
Signatursatz	Der verwendete Satz.
Geladen	Wann der Dienst ihn geladen hat.
Größte Datei	Die größte Datei, die der Dienst annimmt.
Upload pro Tag	Wie viel der Dienst pro Tag annimmt.
Anfragen pro Minute	Wie viele Anfragen pro Minute der Dienst annimmt.

Der Test ändert nichts. Die drei letzten Grenzen sind die des Dienstes, nicht die des Plugins.

Zugangstoken

Im Modus `service` hat die Karte den Abschnitt **Zugangstoken**. Er zeigt einen von drei Zuständen:

- **Gespeichert, endet auf** und die letzten vier Zeichen.
- **Kein Zugangstoken gespeichert**.
- **Gespeichert, aber nicht lesbar; geben Sie ihn erneut ein**.

Um einen Token zu speichern, tippen Sie ihn in **Neuer Zugangstoken** und klicken auf **Token speichern**. Der Token wird verschlüsselt gespeichert und nie wieder angezeigt. Lassen Sie das Feld leer, um den aktuellen Token zu behalten. **Token entfernen** löscht ihn. Das Feld nimmt bis zu 4112 Zeichen. Dasselbe können Sie auf der Konsole mit `ispprotect:remote token:set` und `ispprotect:remote token:clear` tun, siehe Kommandozeile.

Lizenz

Im Modus `license` hat die Karte den Abschnitt **Lizenz**. Er zeigt **Verbunden** oder **Nicht verbunden**.

Die eingebaute Adresse der Lizenz-API ist standardmäßig verfügbar. Wenn sie durch eine ungültige Einstellung `remote.portal_url` ersetzt wurde, kann der Abschnitt **Verbinden** nicht anbieten. Korrigieren Sie die Einstellung zuerst auf der Konsole.

Wenn die Lizenz nicht verbunden ist, tippen Sie den Schlüssel in **Lizenzschlüssel** (bis zu 96 Zeichen) und klicken auf **Verbinden**. Der Schlüssel wird einmal an das Lizenzportal gesendet und verschlüsselt gespeichert. Er wird nie wieder angezeigt.

Wenn die Lizenz verbunden ist, zeigt der Abschnitt:

Angabe	Bedeutung
Lizenzschlüssel	Der Schlüssel wird als **endet auf** und seine letzten vier Zeichen angezeigt.
Tarif	Der Tarif der Lizenz.
Lizenz gültig bis	Das Ende der Lizenz.
Websites	Die genutzten Websites und die Websites, die die Lizenz erlaubt, als „{used} von {limit}“.
Host dieser Website	Der Hostname, unter dem diese Website gezählt wird.
Zugang gültig bis	Das Ende des aktuellen Zugangs zum Dienst. Er ist als **Abgelaufen** markiert, wenn die Zeit vorbei ist.
Erneuerung	Ob der Zugang automatisch erneuert wird und wann er zuletzt erneuert wurde.

Eine verbundene Website wird im Lizenzportal gezählt.

Das Plugin erneuert seinen Zugang selbst aus der geplanten Wartung, siehe Zeitplanung. Es erneuert etwa einmal am Tag und noch einmal, wenn der Zugang innerhalb von zwei Tagen abläuft. Ein vorübergehender Fehler wird später erneut versucht. Das geschieht in jedem Modus, solange ein Lizenzschlüssel gespeichert ist. Die Zeile **Erneuerung** sagt eines davon:

- **Wird etwa einmal täglich automatisch erneuert.**
- **Die letzte Erneuerung ist fehlgeschlagen; der nächste Versuch folgt automatisch.**

- **Die automatische Erneuerung ist angehalten. Verwenden Sie „Jetzt prüfen“.**

Nach einer klaren Ablehnung durch das Lizenzportal hält die automatische Erneuerung an, bis Sie auf **Jetzt prüfen** klicken oder einen neuen Schlüssel eingeben. **Jetzt prüfen** (Konsole: `isprotect:remote refresh`) erneuert den Zugang sofort.

Wenn die Uhr des Servers falsch geht, sendet das Portal einen Zugang, der nach der Uhr des Servers bereits abgelaufen ist. Die Karte sagt dann, dass die Uhr falsch zu gehen scheint. Korrigieren Sie die Systemzeit und klicken Sie auf **Jetzt prüfen**.

Trennen verlangt eine Bestätigung mit der Frage **Lizenz trennen?**. Wenn Sie bestätigen, wird die Website im Lizenzportal freigegeben und der Schlüssel von diesem Server entfernt. Der gehostete Scan-Dienst kann nicht genutzt werden, bis Sie wieder eine Lizenz verbinden. Der Schlüssel wird in jedem Fall entfernt, auch wenn das Portal nicht erreichbar ist. Auch das Deinstallieren des Plugins mit seinen Daten gibt die Website frei, siehe Das Plugin entfernen.

Was gesendet wird und was nie

Für jede nicht leere Code-Datei in den Ordnern, die der Scanner auf Inhalt liest, sendet das Plugin zwei Dinge: die SHA-256-Prüfsumme und einen Namenshinweis. Der Namenshinweis ist der Dateiname ohne Pfad, oder nur `file.` und die Endung, wenn der Name zu lang oder unbrauchbar ist. Nur Dateien mit einem Namen in UTF-8 werden gesendet.

Nur Dateien, die der Dienst nicht kennt, werden hochgeladen. Sie werden nur innerhalb der **Upload-Grenze je Scan (MB)** (`remote.upload_mb`, Vorgabe 200, bis 4096) und innerhalb der Grenzen des Dienstes hochgeladen. Beim Wert `0` sendet das Plugin nur Prüfsummen und lädt nichts hoch. Dateien, die größer sind als **Größte geprüfte Datei (KB)** des Scanners (`scanner.max_file_kb`), werden nicht gesendet. Im Modus `daemon` bleibt das alles auf dem Server.

Das Folgende wird nie gesendet, obwohl der lokale Scanner diese Dateien trotzdem prüft:

- die Konfigurationsdateien `.htaccess`, `.user.ini` und `.env*`;
- Dateien mit dem Namen einer Konfigurations- oder Zugangsdatendatei, etwa `parameters.yml`, `auth.json`, `.htpasswd`, `.npmrc`, `.netrc` und Dateien mit privaten Schlüsseln wie `id_rsa`, sowie Kopien, deren Name mit `wp-config`, `localconfig`, `parameters.y` oder `config.local` beginnt, außer den unten genannten PHP-Dateien;
- Dateien mit der Endung `pem`, `key`, `crt`, `p12`, `pfx`, `jks`, `kdbx`, `sql`, `sqlite`, `db` oder `ini`;
- alles in den Ordnern `config/jwt`, `config/secrets`, `var`, `.git` und `.ssh` und alles unterhalb eines Ordners namens `.git` oder `.ssh` an beliebiger Stelle;
- der ganze Shopware-Ordner `config` und die Datei `deploy.php`, weil das Plugin sie auf dieser Plattform als geschützt markiert;
- Dateien in `config/packages` mit „secret“ im Namen;
- Dateien, deren Name mit einem Leerzeichen oder einem anderen Leerraum beginnt oder endet, etwa `wp-config.php`;
- Dateien, deren Name einer Konfigurationsdatei nur ähnelt und die keine PHP-Dateien sind, etwa `local_config.yml`, `wp_config.php.bak` oder `wpconfig.txt`, auch mit einem unsichtbaren oder nicht lateinischen Zeichen im Namen;
- die Pfade, die Sie unter **Nicht an den Scan-Dienst gesendete Pfade** (`remote.exclude`) auflisten.

Nur in geschwärzter Form gesendet werden PHP-Konfigurationsdateien mit dem Namen `wp-config.php`, `localconfig.php` oder `config.local.php`, Kopien, deren Name mit `wp-config` beginnt und auf `.php` endet, sowie PHP-Dateien, deren Name einer Konfigurationsdatei nur ähnelt (etwa `local_config.php`, `wp_config.php` oder `my-wp-config.php`, auch mit einem unsichtbaren oder nicht lateinischen Zeichen, mit einer Endung, die PHP ausführt, wie `.php`, `.phtml` oder `.inc`), wenn sie nicht in einem der oben genannten Ordner liegen. Shopware legt keine solche Datei außerhalb von `config` ab. Eine im Shop-Ordner liegen gebliebene `wp-config.php` oder `config.local.php`, etwa nach einem Umzug von einem anderen System, wird auf diese Weise gesendet. Bevor die Prüfsumme gebildet und die Datei hochgeladen wird, werden in einer solchen Datei alle Zeichenketten, Zahlen und Kommentare ersetzt: jede Zeichenkette durch `ISPP_REDACTED`, jede Zahl durch `0`, der Text jedes Kommentars durch `ISPP_REDACTED`, ein Variablenname in einer Zeichenkette (etwa `"pa$word"`) durch `$ISPP_REDACTED`, jeder Name innerhalb von `{$...}` oder `${...}` in einer Zeichenkette durch `ISPP_REDACTED`. Erhalten bleiben nur die Struktur des Codes, die Namen (Funktionen, Variablen, Konstanten) und die Konstantennamen in `define()` (in einer Datei mit einer `namespace`-Deklaration, einem `use`-Import oder PHP-8-Attributen werden auch diese ersetzt), sodass Passwörter und andere Werte den Server nie verlassen. Von Angreifern eingefügter Code wird weiterhin an seiner Struktur gefunden: Der Dienst sieht Aufrufe wie

`eval()`, `base64_decode()` oder `include`, aber nicht ihren wörtlichen Inhalt. Nachgefragt wird die Prüfsumme der geschwärzten Form; die der Originaldatei wird nie gesendet. Der Dienst kann eine leere Zeichenkette und die führenden Leerzeichen einer Zeile in einer Zeichenkette erkennen, aber keinen Wert lesen. Eine Datei, die sich nicht sicher schwärzen lässt (sie lässt sich nicht einlesen, ist größer als 1 MB, enthält `__halt_compiler` oder verwendet ein kurzes Öffnungs-Tag `<?` oder beginnt mit `<?xml`, deren Bedeutung von der PHP-Einstellung `short_open_tag` abhängt), wird gar nicht gesendet. In der geschwärzten Form gefundene Schadsoftware wird für die echte Datei gemeldet, mit dem Hinweis, dass sie in geschwärzter Form geprüft wurde.

Namen und Pfade werden in Kleinbuchstaben verglichen, sodass eine andere Schreibweise nicht durchkommt.

Die Karte zeigt eine Zeile dazu, was den Server im verwendeten Modus verlässt. Die Datenschutzseite dieses Kapitels steht in Datenschutz und externe Dienste.

Grenzen und Ablehnungen

Das Plugin arbeitet innerhalb dieser Grenzen. Der Dienst kann strengere setzen, und **Verbindung testen** zeigt sie.

- **Upload-Grenze je Scan (MB)**: Höchstens so viel Dateiinhalt verlässt den Server in einem Scan. Dateien, die nicht hineinpassen, bleiben wartend, und der nächste Scan sendet sie.
- Der Dienst hat eigene Grenzen für die Größe einer Datei, für den Upload pro Tag und für die Anfragen pro Minute.

Wenn der Dienst ablehnt oder nicht genutzt werden kann, läuft der Scan lokal weiter, und die Karte **Letzter Scan** zeigt einen Zustand und einen Grund. Die Zustände sind:

Zustand	Bedeutung
Vom Scan-Dienst geprüft	Der Remote-Teil lief bis zum Ende.
Teilweise vom Scan-Dienst geprüft	Der Remote-Teil endete vorzeitig, mit einem Grund.
Scan-Dienst nicht verfügbar	Der Remote-Teil konnte nicht laufen.
Remote-Scan aus	Der Modus ist `off`.

Die Gründe sind unter anderem:

- Der Scan-Dienst war nicht erreichbar.
- Der Scan-Dienst hat die Zugangsdaten nicht akzeptiert.
- Der Scan-Dienst ist noch nicht bereit, zum Beispiel weil er noch seine Signaturen lädt.
- Der Scan-Dienst ist ausgelastet oder hat um eine Pause gebeten. Der Scan versucht es später erneut. Er wartet begrenzt lange und verlässt den Remote-Teil, wenn die Wartezeiten nicht enden.
- Das Kontingent des Scan-Dienstes ist aufgebraucht. Das Plugin sendet dann keine weitere Datei in diesem Scan, fragt aber weiterhin die Prüfsummen der übrigen Dateien ab, sodass bekannte Urteile gemeldet werden. Die nicht gesendeten Dateien folgen in einem späteren Scan.
- Eine Datei war für den Scan-Dienst zu groß.
- Die Upload-Grenze dieses Scans wurde erreicht. Die übrigen Dateien folgen im nächsten Scan.
- Der Scan-Dienst hat den Zugriff verweigert: Der Daemon lässt diesen Server-Benutzer nicht zu, oder die Zugangsdaten umfassen den Remote-Scan nicht.
- Es ist keine gültige Adresse und kein gültiger Socket gesetzt, oder es fehlt ein Zugangstoken oder eine verbundene Lizenz.
- Die Einstellung des Remote-Scans wurde geändert, während der Scan lief.

Letzter Scan

Der Abschnitt **Letzter Scan** der Karte zeigt den Zustand und die Zähler des letzten Scans:

Zähler	Bedeutung
Abgefragt	Dateien, deren Prüfsumme abgefragt wurde.

Zähler	Bedeutung
Unauffällig	Dateien, die der Dienst als harmlos kennt.
Hochgeladen	Dateien, die hochgeladen wurden, weil der Dienst sie nicht kannte.
Schadcode	Dateien, die der Dienst als Schadcode gemeldet hat.
Übersprungen	Dateien, die nicht gesendet wurden, zum Beispiel weil sie zu groß oder nicht lesbar waren oder sich beim Senden geändert haben.
Nicht geprüft	Dateien, die der Dienst in diesem Scan nicht geprüft hat.
Größe des Uploads	Die Größe dessen, was hochgeladen wurde.

Dieselben Zähler zeigt `ispprotect:remote status`.

Funde des Remote-Scans

Von dem Dienst gemeldeter Schadcode ist ein Fund der Art **Vom Scan-Dienst gefundener Schadcode**, mit dem Namen der Erkennung, auf Stufe 3. Sie kann nicht als neuer Ausgangsstand übernommen werden, deshalb deckt **Alle Änderungen übernehmen** sie nicht ab. Sie wird geschlossen, wenn ein späterer Scan die Datei sauber oder entfernt findet. Die Liste der Funde steht im Dateiscanner.

Zugangsdaten und Speicherung

Der Zugangstoken und der Lizenzschlüssel werden verschlüsselt in der Datenbank gespeichert. Der Schlüssel dafür wird aus dem Anwendungsgeheimnis (`APP_SECRET`) des Shops abgeleitet. Sie werden nie wieder angezeigt, nie in ein Log, in ein Ereignis oder in eine Antwort der Administration-API geschrieben und nie an den Browser zurückgesendet. Die Seite zeigt nur, ob sie gesetzt sind, und die letzten vier Zeichen.

Wenn sich das Anwendungsgeheimnis ändert, lassen sich der gespeicherte Token und die Lizenzdaten nicht mehr lesen. Die Karte sagt das dann, und Sie geben sie erneut ein. Wenn der Shop keine verschlüsselten Werte speichern kann, zum Beispiel weil das Anwendungsgeheimnis zu kurz ist, sagt die Karte das, und es lässt sich kein Token und kein Schlüssel speichern.

Änderungen am Token und an der Lizenz werden im Ereignisprotokoll aufgezeichnet, nie mit einem Geheimnis. Die Ereignisse sind `remote.token_set`, `remote.token_cleared`, `remote.license_connected`, `remote.license_refreshed`, `remote.license_disconnected` und `remote.license_failed`.

Konsole

Der Befehl `ispprotect:remote` erledigt alles, was die Karte tut. Seine Aktionen, die Art, wie ein Geheimnis übergeben wird, und die Exit-Codes stehen in der Kommandozeile. Wenn eine Verbindung nicht funktioniert, siehe Zurück ins System und Fehlerbehebung.

Anmeldeschutz

Der Anmeldeschutz zählt fehlgeschlagene Anmeldungen und reagiert darauf. Er deckt die Administration (Benutzer) und die Storefront (Kunden) ab. Die Einstellungen stehen auf dem Tab **Anmeldeschutz** und auf dem Tab **Einstellungen**. Siehe Einstellungen des Anmeldeschutzes.

Welche Anmeldungen gezählt werden

Das Plugin hält die beiden Bereiche getrennt. In den Tabellen der Administration und im Ereignisprotokoll wird der Bereich als `admin` oder `customer` angezeigt.

- **Administration** (`admin`): jede Anmeldung an der Administration über die Token-Anfrage `/api/oauth/token` mit Benutzername und Passwort.
- **Kunden** (`customer`): die Anmeldungen mit Zugangsdaten über das Formular der Storefront (`/account/login`) und über die Store API (`/store-api/account/login`). Gastbestellungen, die Übernahme eines Kontos durch einen Administrator und eine Anmeldung per Kunden-ID werden nicht gezählt. Das eigene Anfragelimit von Shopware für Kundenanmeldungen arbeitet weiter.

So funktioniert es

Fehlgeschlagene Anmeldungen werden je Adresse (IPv6: je /64-Bereich) und je Benutzername gezählt. Benutzernamen werden in normalisierter Form verglichen und sind höchstens 190 Zeichen lang.

- Wenn eine Adresse innerhalb von **Zeitfenster für Anmeldungen (Minuten)** **Fehlgeschlagene Anmeldungen pro Adresse** Fehlversuche erreicht, wird die Adresse in der Firewall gesperrt. Siehe Sperren.
- Wenn ein Benutzername innerhalb des Zeitfensters **Fehlgeschlagene Anmeldungen pro Benutzername** Fehlversuche erreicht, wird der Benutzername für **Sperrdauer für Benutzernamen (Minuten)** gesperrt. Solange er gesperrt ist, wird sogar das richtige Passwort abgewiesen. Eine abgewiesene Kundenanmeldung sieht aus wie ein falsches Passwort.
- Für die Sperre eines Benutzernamens gibt es eine Ausnahme: ein Adressbereich, von dem sich das Konto in den letzten 90 Tagen angemeldet hat (soweit das Ereignisprotokoll das noch enthält). Von dort bleibt der Name offen, bis während der Sperre **Fehlgeschlagene Anmeldungen pro Benutzername** weitere Fehlversuche aus diesem Bereich gekommen sind.
- Adressen auf der Erlaubnisliste werden nie gezählt, gesperrt oder blockiert. Ein Eintrag der Erlaubnisliste lässt eine gesperrte Adresse passieren, solange er besteht, hebt die Sperre aber nicht auf.
- Eine erfolgreiche Anmeldung setzt den Zähler der Fehlversuche dieses Benutzernamens zurück. Eine erfolgreiche Anmeldung an der Administration setzt auch den Zähler der Fehlversuche der Adresse zurück. Eine Kundenanmeldung tut das nicht, weil jeder ein Kundenkonto registrieren kann.
- Wenn Kunden an Verkaufskanäle gebunden sind, wird jedes Konto für sich gezählt: der Benutzername erscheint dann als `<Adresse> [sales channel <ID>]` in der Liste der Sperren und im Ereignisprotokoll, und eine Anmeldung über einen Verkaufskanal setzt nie den Zähler der Fehlversuche eines Kontos mit derselben Adresse in einem anderen Verkaufskanal zurück. Entsperren Sie ein solches Konto mit diesem vollen Namen.
- Eine eingegebene Adresse, zu der es im Verkaufskanal kein Konto gibt, die aber wie ein solcher Name endet (`... [sales channel <ID>]`), wird als `<eingegebener Text> [unknown account]` gezählt und zählt so nie gegen das gebundene Konto.
- Eine Anmeldung ohne Client-Adresse wird trotzdem nach dem Benutzernamen gezählt und gesperrt, wie in der Administration.
- Ein abgewiesener Versuch wird als `login.refused` aufgezeichnet, höchstens einmal pro Minute.

Geschützte Adressen von Administratoren

24 Stunden, nachdem sich ein Administrator angemeldet hat, ist die Adresse geschützt (wenn **Adressen von Administratoren schützen** bei dieser Anmeldung eingeschaltet war). Zu viele fehlgeschlagene Anmeldungen von einer geschützten Adresse sperren sie nicht in der Firewall. Stattdessen sperren sie die Anmeldung von dieser Adresse. Die Sperre gilt für den Bereich, in dem die Fehlversuche passiert sind, sodass der Rest des Shops erreichbar bleibt. Sie dauert

so lange wie **Sperrdauer für Benutzernamen (Minuten)**. Wenn die vorherige Sperre derselben Adresse innerhalb von 30 Tagen begann, dauert die Sperre viermal so lang, bis zu **Längste Sperre (Minuten)**. Sie gilt, bis sie endet, auch wenn die 24 Stunden Schutz vorher enden. Einträge der Sperrliste gelten weiterhin für die Adresse.

Das Plugin speichert von einer solchen Adresse nur einen Hash, deshalb wird die Adresse nicht in einer Liste angezeigt. Das Ereignis `login.address_locked` nennt sie, in gekürzter Form, wenn **Adressen im Protokoll kürzen** eingeschaltet ist. Siehe Ereignisprotokoll und Benachrichtigungen.

Was der Besucher sieht

- Ein gesperrter Benutzername in der Administration: die eigene Meldung von Shopware, dass es zu viele Versuche gab.
- Eine abgewiesene Adresse in der Administration: der Fehler 1103 mit Status 403.
- Ein abgewiesener Kunde: dieselbe Meldung wie bei falschen Zugangsdaten.

Wenn das Plugin seine Daten nicht lesen oder schreiben kann, wird die Anmeldung durchgelassen. Die Ausnahme ist die Prüfung des zweiten Schritts bei einem Benutzer, der einen hat. Siehe Zwei-Faktor-Authentifizierung.

Neue Adressen

Nachdem sich ein Administrator von einer Adresse angemeldet hat, die dasselbe Konto in den letzten 90 Tagen nicht benutzt hat, zeichnet das Plugin das Ereignis `login.new_address` auf. Bei eingeschaltetem **Bei Anmeldung von neuen Adressen warnen** (die Vorgabe) hat das Ereignis die Stufe **Alarm**, und eine Warn-Mail wird gesendet. Bei ausgeschalteter Einstellung hat es die Stufe **Hinweis**. Es wird nur für ein Konto aufgezeichnet, das sich schon einmal angemeldet hat, nicht für seine erste Anmeldung. Kunden haben kein solches Ereignis.

Sperren und Anmeldesperren aufheben

Der Tab **Anmeldeschutz** hat diese Karten:

- **Gesperrte Benutzernamen**: die Spalten **Benutzername**, **Bereich**, **Gesperrt seit** und **Gesperrt bis**. Die Schaltfläche **Entsperren** hebt die Sperre auf. Die Meldung lautet „{name} wurde entsperrt.“
- **Anmeldesperren von Adressen**: die Sperren geschützter Adressen. Weil nur ein Hash der Adresse gespeichert wird, entsperren Sie, indem Sie die Adresse eintippen. Geben Sie die **IP-Adresse** ein (IPv4 oder IPv6; eine IPv6-Sperre deckt ihren /64-Bereich ab), wählen Sie den Bereich (**Alle Bereiche** oder einen Bereich) und klicken Sie auf **Adresse entsperren**. Das setzt auch den Zähler der Fehlversuche der Adresse zurück. Eine Sperre der Adresse in der Firewall bleibt bestehen. Die Karte zeigt höchstens 200 Sperren, die, die zuerst enden („Angezeigt werden die {shown} Sperren, die zuerst enden, von insgesamt {total}.“), mit den Spalten **Bereich**, **Gesperrt seit**, **Gesperrt bis** und **Minuten**. Die Meldung lautet „Die Anmeldung von {address} ist wieder möglich.“ oder „Für {address} wurde keine Anmeldesperre gefunden.“
- **Firewall-Sperren**: Sperren von Adressen. Die Schaltfläche **Sperre aufheben** beendet eine Sperre.

Einen Benutzernamen auf diesem Tab zu entsperren setzt auch den Zähler der falschen Zwei-Faktor-Codes dieses Benutzers zurück. Auf der Konsole zu entsperren tut das nicht. Jede aufgehobene Sperre wird als `login.unlocked` oder `login.address_unlocked` aufgezeichnet.

Auf der Konsole:

```
bin/console ispprotect:unlock <user name>
bin/console ispprotect:unlock --address=<address>
bin/console ispprotect:unlock <user name> --realm=admin
```

Die Optionen und Exit-Codes stehen in der Kommandozeile.

Gekürzte Adressen

Bei eingeschaltetem **Adressen im Protokoll kürzen** kürzt das Plugin Adressen, bevor es sie im Ereignisprotokoll speichert: IPv4-Adressen verlieren die letzte Zahl (sie wird 0), IPv6-Adressen behalten ihre ersten 48 Bits. Das Ereignis einer Sperre eines Benutzernamens enthält dann keinen Bereich. Der Vergleich mit bekannten Adressen verwendet die gekürzten Bereiche. Siehe Datenschutz und externe Dienste.

Einstellungen des Anmeldeschutzes

Die Einstellungen stehen in den Gruppen **Anmeldeschutz** und **Zwei-Faktor-Authentifizierung** auf dem Tab **Anmeldeschutz** und auf dem Tab **Einstellungen**. Alle Schlüssel, Vorgaben und Bereiche stehen in der Einstellungsreferenz.

Zwei-Faktor-Authentifizierung

Benutzer der Administration können ihre Anmeldung mit einem zweiten Schritt schützen. Sie können ihn auch für jeden Benutzer der Administration verpflichtend machen. Kunden der Storefront haben keinen zweiten Schritt.

So funktioniert die Zwei-Faktor-Anmeldung

- Der zweite Schritt ist ein zeitbasierter Code (6 Ziffern, alle 30 Sekunden wechselnd) aus einer Authenticator-App. Ein Code aus dem benachbarten Zeitschritt wird akzeptiert, um Zeitunterschiede auszugleichen. Jeder Code funktioniert einmal.
- Bei der Einrichtung erhält der Benutzer 10 Wiederherstellungscodes. Jeder besteht aus 4 Gruppen zu je 4 Zeichen. Sie werden einmal angezeigt. Jeder funktioniert einmal, anstelle eines App-Codes. Das Plugin speichert nur Hashes davon.
- Der Schlüssel der App wird verschlüsselt gespeichert, mit einem Schlüssel, der aus `APP_SECRET` des Shops abgeleitet wird.
- Nach 5 falschen Codes innerhalb von 15 Minuten wird jeder Code dieses Benutzers abgewiesen, bis die 15 Minuten vorbei sind. Ein richtiger Code setzt den Zähler zurück. Ein falscher Code ist auch eine fehlgeschlagene Anmeldung: Er zählt für **Fehlgeschlagene Anmeldungen pro Adresse** und **Fehlgeschlagene Anmeldungen pro Benutzername** und kann den Benutzernamen sperren. Siehe Anmeldeschutz.

Anmelden

Nach dem Passwort wird ein Benutzer mit zweitem Schritt in einem Dialog nach einem Code gefragt. Der Dialog akzeptiert den 6-stelligen Code oder einen Wiederherstellungscode. Derselbe Code wird für den Dialog „Passwort bestätigen“ von Shopware gebraucht.

Die Anmeldeanfrage antwortet mit diesen Fehlern des Plugins:

Code	Status	Bedeutung
1101	401	Ein Code ist erforderlich. Das wird nicht als Fehlversuch gezählt.
1102	401	Der Code ist falsch. Er zählt als Fehlversuch der Adresse und des Benutzernamens.
1103	403	Die Adresse wird abgewiesen.
1104	503	Der zweite Schritt ist nicht verfügbar.
1105	429	Zu viele falsche Codes.

Wer die Seite öffnen kann

Der Eintrag des Moduls wird nur Administratoren angezeigt. Benutzer, die keine Administratoren sind, haben keinen Menüeintrag. Sie erreichen ihre eigene Seite unter `#/ispprotect/web-security/index/twofactor`, oder sie werden dorthin geleitet, wenn der Shop den zweiten Schritt verlangt. Auf jeder anderen Seite des Moduls sehen sie „Dieser Bereich steht nur Administratoren zur Verfügung.“

Den zweiten Schritt einrichten

Öffnen Sie den Tab **Zwei-Faktor**. Die Karte „Ihr Konto“ zeigt **Zwei-Faktor-Anmeldung** als **Ein**, **Aus** oder „Einrichtung nicht abgeschlossen“, die Zahl der übrigen Wiederherstellungscodes („Verbleibende Wiederherstellungscodes“) und die **Regel des Shops** („Für alle Benutzer verpflichtend“ oder „Nicht verpflichtend“).

1. Klicken Sie auf **Einrichtung starten**.
2. „Passwort bestätigen“ und klicken Sie auf **Weiter**. Das Passwort wird einmal verwendet und nicht gespeichert.

3. „Schlüssel in die Authenticator-App eintragen“: Die Seite zeigt den **Schlüssel** als Text und als **Einrichtungslink**. Sie zeigt keinen QR-Code, damit nichts von einer anderen Seite abgerufen wird. Der Name des Shops ist der Aussteller in der App.
4. Geben Sie den ersten Code in **Code aus der App** ein und klicken Sie auf **Einschalten**.
5. „Ihre Wiederherstellungscodes“: Die Seite zeigt die Wiederherstellungscodes einmal an. Klicken Sie auf **Alle Codes kopieren**, bewahren Sie sie sicher auf und klicken Sie dann auf **Ich habe sie gespeichert**. Vorher können Sie die Seite nicht verlassen.

Eine unfertige Einrichtung können Sie mit „Unfertige Einrichtung verwerfen“ verwerfen. Das ist nicht möglich, solange der Shop den zweiten Schritt verlangt. Wenn Sie die Einrichtung erneut starten, ersetzt sie eine unfertige.

Wiederherstellungscodes und Ausschalten

- **Neue Codes erstellen** („Neue Wiederherstellungscodes“) erzeugt 10 neue Codes und ersetzt die alten. Sie brauchen einen aktuellen Code.
- **Ausschalten** („Zwei-Faktor-Anmeldung ausschalten“) entfernt Ihren zweiten Schritt. Sie brauchen einen aktuellen Code. Tippen Sie im Feld „Aktueller Code (aus der App oder ein Wiederherstellungscode)“ einen Code aus der App oder einen Wiederherstellungscode.
- Die Seite warnt „Nur noch {count} Wiederherstellungscode(s) übrig.“, wenn nur noch wenige übrig sind.
- Fehler, die Sie sehen können: „Der Code ist falsch oder wurde bereits verwendet.“ und „Zu viele falsche Codes. Warten Sie {seconds} Sekunden und versuchen Sie es erneut.“

Das Ausschalten wird nicht angeboten, solange der Shop den zweiten Schritt verlangt. Die Seite sagt „Ein Administrator kann die Pflicht unter „Anmeldeschutz“ aufheben.“

Für alle verlangen

Die Einstellung **Zweiten Anmeldeschritt verlangen** (`twofactor.required` , Vorgabe aus) steht in der Gruppe **Zwei-Faktor-Authentifizierung**, auf dem Tab **Anmeldeschutz** und auf dem Tab **Einstellungen**.

Solange sie eingeschaltet ist:

- Ein Benutzer ohne zweiten Schritt kann sich weiterhin mit dem Passwort anmelden. Die Administration hält diesen Benutzer dann auf der Seite zur Einrichtung fest.
- Jede andere Anfrage dieses Benutzers an die Administration-API wird mit Status 403 und dem Code `ISPPROTECT__TWOFACTOR_SETUP_REQUIRED` abgewiesen. Ausnahmen sind die Einrichtungsrouten des Plugins und fünf lesende Startrouten, die die Administration braucht, um die Seite anzuzeigen (`api.info.entity-schema` , `api.info.config` , `api.info.me` , `api.config_me.get` und `api.consents.fetch`).
- Ein Benutzer, der schon einen zweiten Schritt hat, wird nicht aufgehalten.

Integrationen und Zugangsschlüssel sind nicht betroffen, weil ihre Token zu keinem Benutzer gehören. Auch die Store API ist nicht betroffen.

Das Formular warnt „Sie haben für Ihr eigenes Konto keine Zwei-Faktor-Anmeldung eingerichtet. Wenn Sie diese Pflicht einschalten, werden Sie sofort aufgefordert, sie einzurichten.“, wenn Sie die Pflicht einschalten, während Ihr eigenes Konto keinen zweiten Schritt hat. Richten Sie zuerst Ihren eigenen zweiten Schritt ein.

Neben der Einstellung zeigt das Formular immer „Aus der Administration ausgesperrt? Führen Sie auf dem Server aus:“ mit dem Befehl zur Wiederherstellung. Siehe Gerät verloren oder von der Zwei-Faktor-Anmeldung ausgesperrt.

Grenzen des zweiten Schritts

- Er deckt die Passwort-Anmeldung der Administration ab. Der Refresh-Token-Ablauf, Client Credentials (Integrationen und Zugangsschlüssel), der Authorization-Code-Grant und der SSO-Grant von Shopware fragen nicht nach einem Code. Bei einem Benutzer, der sich per Single Sign-on anmeldet, entscheidet der Identity-Provider.
- Die Pflicht gilt weiterhin für jede Anfrage eines Benutzers, auch mit Token aus den Refresh- und SSO-Grants.

- Wenn sich die Einstellung nicht lesen lässt, wird die Pflicht nicht durchgesetzt. Wenn sich der Zustand des zweiten Schritts nicht lesen lässt, während die Pflicht eingeschaltet ist, erhält die Anfrage Status 503 mit dem Code `ISPPROTECT__TWOFACTOR_UNAVAILABLE`.
- Wenn Sie `APP_SECRET` ändern, lassen sich die gespeicherten Schlüssel nicht mehr entschlüsseln, und Benutzer mit zweitem Schritt kommen an der Codeprüfung nicht vorbei. Planen Sie eine Änderung von `APP_SECRET` mit Blick darauf.
- Das Plugin hat keinen Konsolenbefehl, der den zweiten Schritt eines einzelnen Benutzers entfernt. Die Administration hat dafür keine Schaltfläche.

Sicherheitscheck

Der Sicherheitscheck testet den Server, PHP, den Shop und die Einstellungen des Plugins. Er ändert nichts, außer mit der Schaltfläche **Rechte korrigieren** (siehe Aufgeführte Dateien und die Korrektur der Rechte). Er läuft, wenn Sie den Tab **Sicherheitscheck** öffnen, und mit `bin/console ispprotect:checkup`.

Ergebnisse und Punktzahl

Jede der 22 Prüfungen hat eines von vier Ergebnissen:

Ergebnis	Bedeutung
In Ordnung	Die Prüfung ist bestanden.
Unbekannt	Das Plugin konnte es nicht feststellen. Die Prüfung wird nicht bewertet.
Beachten	Eine Schwachstelle. Sie zählt in der Punktzahl zur Hälfte.
Problem	Eine schwerwiegende Schwachstelle. Sie zählt in der Punktzahl voll.

Jedes Ergebnis hat eine Empfehlung, was zu ändern ist. Eine Prüfung, die mit einem Fehler abbricht, zeigt „Eine Prüfung konnte nicht abgeschlossen werden“.

Die Punktzahl ist eine Zahl von 0 bis 100. Sie ist der gewichtete Anteil der Prüfungen, die in Ordnung sind, unter den bewerteten. Jede Prüfung hat ein Gewicht von 1 bis 5. Ein Ergebnis **Beachten** verliert die Hälfte seines Gewichts, ein Ergebnis **Problem** das ganze. **Unbekannt** wird ignoriert. Der Tab zeigt die Punktzahl und die Zähler „{n} fehlgeschlagen“, „{n} brauchen Aufmerksamkeit“, „{n} zur Information“ und „{n} in Ordnung“. Die Übersicht zeigt eine Kurzform. Siehe Übersicht.

Auf der Konsole gibt der Befehl eine Tabelle und die Punktzahl aus. Er endet mit Exit-Code 1, wenn mindestens eine Prüfung das Ergebnis **Problem** hat, sonst mit 0.

Prüfungen

Server und PHP

Prüfung	Wann sie nicht besteht
PHP {version} erhält Sicherheitsupdates	**Problem** nach dem Ende der Sicherheitsunterstützung der Version, **Beachten** in den letzten 90 Tagen davor. Die Enddaten im Plugin sind 2026-12-31 für PHP 8.2, 2027-12-31 für 8.3, 2028-12-31 für 8.4 und 2029-12-31 für 8.5.
PHP zeigt Besuchern keine Fehlermeldungen an	`display_errors` ist eingeschaltet.
PHP verrät seine Version nicht	`expose_php` ist eingeschaltet. Die Empfehlung nennt die Option **PHP-Version verbergen**.
PHP lädt keinen Code von fremden Servern	`allow_url_include` ist eingeschaltet.
Genug freier Speicherplatz	**Beachten** unter 5 Prozent frei, **Problem** unter 1 Prozent.

Die drei Prüfungen zu PHP-Optionen können die Einstellungen des Webservers nur lesen, wenn Sie den Tab **Sicherheitscheck** öffnen. Auf der Konsole, die andere PHP-Einstellungen haben kann, zeigen sie stattdessen einen Hinweis statt eines Ergebnisses.

Shop und Dateien

Prüfung	Wann sie nicht besteht
Das Anwendungsgeheimnis ist lang und kein Beispielwert	**Problem**, wenn `APP_SECRET` kürzer als 32 Bytes oder ein Beispielwert ist.
Produktivmodus ohne Debugging	**Beachten**, wenn Debugging eingeschaltet ist oder die Umgebung nicht `prod` ist.
Die Adresse der Seite nutzt HTTPS	**Beachten**, wenn nicht. **Unbekannt**, wenn keine Adresse gesetzt ist.
Dateien mit Passwörtern und Schlüsseln sind für andere Benutzer nicht lesbar	**Beachten**, wenn andere Benutzer sie lesen können.
Keine Datei und kein Ordner im Code ist für alle beschreibbar	**Beachten**, wenn etwas für alle beschreibbar ist. **Unbekannt**, wenn die Suche an ihrer Grenze angehalten hat.
Keine Sicherungen oder Debug-Dateien im öffentlichen Ordner	**Beachten**, wenn sie welche findet.
Der Web-Installer liegt nicht auf dem Server	**Unbekannt** (Information), wenn `shopware-installer.phar.php` im öffentlichen Ordner liegt.
Vertrauenswürdige Proxys passen zum tatsächlichen Aufbau	**Problem** oder **Beachten**, wenn jeder Adresse vertraut wird oder ein weitergeleiteter Header von einer Adresse kommt, der nicht vertraut wird. **Unbekannt**, wenn sich das nicht feststellen lässt. Siehe Hinter einem Reverse-Proxy oder CDN.

Konten

Prüfung	Wann sie nicht besteht
Administratoren nutzen die Zwei-Faktor-Authentifizierung	**Beachten**, wenn ein Administrator keinen zweiten Schritt hat.
Wenige Administrator-Konten	**Beachten** bei mehr als 5 Administratoren.
Keine Integration hat Administrator-Zugriff	**Beachten**, wenn eine Integration ein Administrator ist.
Passwörter der Administration haben eine sinnvolle Mindestlänge	**Beachten**, wenn die Mindestlänge unter 12 liegt. Die Vorgabe von Shopware ist 8.

Plugin

Prüfung	Wann sie nicht besteht
Die Firewall ist eingeschaltet	**Beachten** im Modus **Nur protokollieren**, **Problem** im Modus **Aus**.
Der Anmeldeschutz ist eingeschaltet	**Problem**, wenn er ausgeschaltet ist.
Warnungen haben einen Empfänger	**Beachten**, wenn sich kein Empfänger finden lässt. Siehe Einstellungen der Benachrichtigungen.
Der Dateiscan lief in den letzten {days} Tagen	**Beachten**, wenn der letzte vollständige Scan älter als 8 Tage ist oder der Zeitplan ausgeschaltet ist. **Unbekannt**, wenn noch kein Scan gelaufen ist.
Keine offenen Funde mit hoher Stufe	**Problem** bei einem offenen Fund der Stufe 3, **Beachten** bei einem der Stufe 2.

Aufgeführte Dateien und die Korrektur der Rechte

Drei Prüfungen führen unter ihrem Hinweis auf, was sie gefunden haben: **Dateien mit Passwörtern und Schlüsseln sind für andere Benutzer nicht lesbar**, **Keine Datei und kein Ordner im Code ist für alle beschreibbar** und **Keine Sicherungen oder Debug-Dateien im öffentlichen Ordner**. Die Namen sind relativ zum Projektordner, bei den Dateien im öffentlichen

Ordner relativ zu diesem. Die Listen stehen auf dem Tab **Sicherheitscheck** und in der Ausgabe von `bin/console ispprotect:checkup`. Die Liste der für alle beschreibbaren Pfade hat höchstens 20 Einträge, die der Dateien im öffentlichen Ordner höchstens 50. Eine längere Liste endet mit „Die Liste zeigt nur die ersten {count} Einträge."

Hat die Prüfung **Dateien mit Passwörtern und Schlüsseln sind für andere Benutzer nicht lesbar** das Ergebnis **Beachten**, entzieht die Schaltfläche **Rechte korrigieren** den aufgeführten Dateien alle Rechte für „andere", wie `chmod o-rwx`. Besitzer und Gruppe behalten ihre Rechte. Die Schaltfläche nimmt die Dateinamen aus der Prüfung selbst, nie aus dem Browser, und ändert nur eine Datei, die

- eine normale Datei direkt im Projektordner ist, kein Link und kein Ordner, keinen zweiten Namen (Hardlink) hat und
- dem Benutzer gehört, unter dem PHP läuft.

Die Schaltfläche erscheint, wenn sich mindestens eine aufgeführte Datei ändern lässt. Für jede andere Datei nennt die Meldung den Befehl, den Sie im Projektordner ausführen, zum Beispiel `chmod o-rwx .env`. Danach läuft die Prüfung erneut und zeigt das neue Ergebnis. Die Änderung steht im Audit-Log als „Dateirechte durch den Checkup geändert", mit den Namen der geänderten und der nicht geänderten Dateien.

Ein Programm, das diese Dateien unter einem anderen Benutzerkonto liest, zum Beispiel ein Cronjob, muss nach der Änderung zur Gruppe der Datei gehören.

Die beiden anderen Prüfungen haben keine Schaltfläche. Entziehen Sie den aufgeführten Pfaden das Schreibrecht für „andere", zum Beispiel mit `chmod o-w`, und löschen Sie die aufgeführten Dateien im öffentlichen Ordner oder verschieben Sie sie von dort.

Ereignisprotokoll und Benachrichtigungen

Das Plugin zeichnet sicherheitsrelevante Ereignisse in einer eigenen Datenbanktabelle auf und sendet Warnungen und eine Zusammenfassung per E-Mail.

Das Ereignisprotokoll lesen

Der Tab **Ereignisse** zeigt die Karte **Ereignisprotokoll** mit 25 Einträgen pro Seite. Die Spalten sind **Zeit**, **Stufe**, **Ereignis**, **Benutzername**, **Adresse** und **Details**. Wenn nichts passt, sagt die Seite „Keine Ereignisse gefunden.“

Sie können nach **Typ**, **Stufe ab**, **Von**, **Bis**, **Benutzername** und **Adresse** filtern. Klicken Sie auf **Filter anwenden**, um zu filtern, und auf **Zurücksetzen**, um den Filter zu löschen.

Auf der Konsole zeigt `bin/console ispprotect:events` die neuesten Ereignisse:

```
bin/console ispprotect:events
bin/console ispprotect:events --type login.failure --since 60 --limit 100
bin/console ispprotect:events --since "2026-11-01 12:00"
```

`--since` nimmt eine Anzahl von Minuten oder ein Datum in UTC. `--limit` ist 1 bis 500 (Vorgabe 50). Siehe Kommandozeile.

Was aufgezeichnet wird

- Anmeldungen, Fehlversuche, Abweisungen, Anmeldungen von neuen Adressen, Sperren von Benutzernamen und Adressen und aufgehobene Sperren
- Änderungen und Fehlversuche bei der Zwei-Faktor-Anmeldung
- Sperren und Änderungen der Adresslisten
- Abweisungen durch die Firewall und Entscheidungen im Modus **Nur protokollieren**
- Änderungen der Einstellungen des Plugins
- Scans und Funde
- Änderungen im Shop, die für die Sicherheit wichtig sind: Benutzer der Administration, Rollen und Rollenzuweisungen, Integrationen und Zugangsschlüssel, Systemkonfiguration, Installationen, Updates, Aktivierungen und Entfernungen von Plugins und Apps sowie Anfragen zur Passwort-Wiederherstellung für Benutzer der Administration. Kunden sind von diesen Änderungsereignissen nicht abgedeckt.

Das Protokoll speichert nur die Namen geänderter Felder, nie ihre Werte. Eine Änderung einer Einstellung listet die Schlüsselnamen auf, nicht die Werte.

Ereignisstufen

Jedes Ereignis hat eine Stufe: **Info**, **Hinweis**, **Warnung** oder **Alarm**.

Einstellungen des Ereignisprotokolls

Die Gruppe **Ereignisprotokoll** auf dem Tab **Einstellungen** hat zwei Einstellungen.

- **Protokolleinträge aufbewahren (Tage)**: wie lange ein Ereignis aufbewahrt wird. Die Wartungsaufgabe entfernt ältere Ereignisse einmal pro Stunde.
- **Adressen im Protokoll kürzen**: Wenn eingeschaltet, werden Adressen gekürzt, bevor sie gespeichert werden. IPv4-Adressen verlieren die letzte Zahl (sie wird 0). IPv6-Adressen behalten ihre ersten 48 Bits. Die Einstellung ändert keine Ereignisse, die schon gespeichert sind.

Alle Schlüssel, Vorgaben und Bereiche stehen in der Einstellungsreferenz.

Warn-Mails

Das Plugin sendet eine Mail für Ereignisse der Stufe **Alarm**. Das sind:

- ein Fund der Stufe 3 des Scans (höchstens 20 Ereignisse pro Scan)
- eine Anmeldung von einer neuen Adresse, wenn **Bei Anmeldung von neuen Adressen warnen** eingeschaltet ist

Es gibt höchstens eine Mail pro Ereignistyp und Stunde. Sie sagt, wie viele Ereignisse warten, und listet bis zu 10 davon auf. Wenn eine Mail nicht gesendet werden kann, bleiben die Ereignisse ungesendet, dieser Typ wartet 15 Minuten, und das Plugin zeichnet das Ereignis `system.notice` mit dem Grund `mail_failed` auf.

Sofortige Warnungen schaltet die Warn-Mails ein und aus.

Zusammenfassung per E-Mail

Die Zusammenfassung per E-Mail deckt einen Zeitraum ab und enthält die Ereignisse nach Typ, Sperren und Anmeldesperren, offene Funde nach Stufe, die Punktzahl des Sicherheitschecks und Probleme. **Zusammenfassung per E-Mail** stellt sie auf **Aus**, **Täglich** oder **Wöchentlich**.

Einstellungen der Benachrichtigungen

Die Gruppe **Benachrichtigungen** auf dem Tab **Einstellungen** hat drei Einstellungen: **Adresse für Benachrichtigungen**, **Sofortige Warnungen** und **Zusammenfassung per E-Mail**.

Wenn **Adresse für Benachrichtigungen** leer ist, verwendet das Plugin die E-Mail-Adresse aus den Basisinformationen des Shops (`core.basicInformation.email`). Wenn es keinen Empfänger gibt, werden Warnungen ohne Mail als erledigt markiert. Der Sicherheitscheck zeigt dann „Warnungen haben einen Empfänger“ als **Beachten**.

Die Mails werden über den Mail-Dienst von Shopware gesendet, mit dem ersten aktiven Storefront-Verkaufskanal und dem Namen des Shops als Absendernamen. Der Mailversand hängt deshalb von den Mail-Einstellungen des Shops ab. Die Mails sind reiner Text. Die geplante Aufgabe sendet sie. Siehe Zeitplanung.

Einstellungsreferenz

Einstellungen ändern

Auf dem Tab **Einstellungen** steht jede Einstellung des Plugins in einer Karte je Gruppe. Die Tabs **Firewall** und **Anmeldeschutz** zeigen die Gruppen, die zu ihnen gehören. Siehe Das Modul in der Administration.

Jede Karte hat zwei Schaltflächen:

- **Speichern** speichert die Einstellungen der Karte. Die Meldung lautet „{group}: Einstellungen gespeichert.“ Wenn ein Wert falsch ist, lautet die Meldung „Es wurde nichts gespeichert. Korrigieren Sie die markierten Felder.“ Wenn sich nichts geändert hat, lautet sie „Es gibt keine Änderungen zu speichern.“
- **Auf Standard zurücksetzen** fragt „Diesen Bereich auf Standard zurücksetzen?“ Klicken Sie zur Bestätigung auf **Zurücksetzen**. Die Meldung lautet „{group}: Standardwerte wiederhergestellt.“

Auf der Konsole zeigt `ispprotect:settings:get [key]` eine Einstellung oder alle, und `ispprotect:settings:set <key> <value>` ändert eine:

```
bin/console ispprotect:settings:get firewall.mode
bin/console ispprotect:settings:set firewall.mode log
bin/console ispprotect:settings:set trap.paths '["/wp-login.php","/backup/*"]'
```

Der Wert wird als JSON gelesen, wenn er gültiges JSON ist, sonst als Text. Eine Einstellung, die eine Liste ist, oder die Regeln werden als JSON angegeben. Jede Änderung wird als Ereignis `settings.changed` aufgezeichnet, nur mit den Schlüsselnamen.

Werttypen

- Eine Ja-Nein-Einstellung akzeptiert auf der Konsole `1`, `0`, `true`, `false`, `on`, `off`, `yes` und `no`.
- Eine Liste (**Fallenpfade**, **Pfade ohne Anfragegrenze**, **Ausgenommene Pfade**, **Nicht an den Scan-Dienst gesendete Pfade**) enthält höchstens 500 Einträge zu je höchstens 255 Bytes.
- Eine Zahl außerhalb ihres Bereichs wird abgelehnt.

Gruppe Firewall

Bezeichnung	Schlüssel	Vorgabe	Bedeutung
Firewall-Modus	`firewall.mode`	`on`	`off`, `log` oder `on`. Siehe Firewall-Modi.
Adressen von Administratoren schützen	`firewall.allow_admin_ip`	ein	Schützt die Adresse eines angemeldeten Administrators 24 Stunden lang vor Sperren und automatischen Maßnahmen.

Gruppe Anfragelimit

Bezeichnung	Schlüssel	Vorgabe	Bedeutung
Anfragen pro Adresse begrenzen	`rate.enabled`	ein	Schaltet das Anfragelimit ein oder aus.
Anfragen pro Zeitfenster	`rate.limit`	600	Anfragen, die eine Adresse im Zeitfenster senden darf (30 bis 100000).
Zeitfenster (Sekunden)	`rate.window`	60	Länge des Zeitfensters (10 bis 3600).
Anmeldeanfragen pro Zeitfenster	`rate.signin_limit`	30	Niedrigeres Limit für Anmeldeanfragen (5 bis 1000).

Bezeichnung	Schlüssel	Vorgabe	Bedeutung
Pfade ohne Anfragegrenze	`rate.exempt_prefixes`	leer	Pfadpräfixe, die das Limit nicht zählt.
Sperren nach Abweisungen	`rate.ban_after`	3	Abweisungen innerhalb von 10 Minuten, die zu einer Sperre führen (0 bis 100). 0 bedeutet keine Sperre.

Gruppe Fehlende Seiten

Bezeichnung	Schlüssel	Vorgabe	Bedeutung
Antworten „nicht gefunden“ überwachen	`notfound.enabled`	ein	Zählt Antworten „nicht gefunden“ (Status 404) je Adresse.
Antworten „nicht gefunden“ pro Zeitfenster	`notfound.limit`	40	Anzahl, die zu einer Sperre führt (5 bis 10000).
Zeitfenster für „nicht gefunden“ (Sekunden)	`notfound.window`	300	Länge des Zeitfensters (60 bis 3600).

Gruppe Fallenpfade

Bezeichnung	Schlüssel	Vorgabe	Bedeutung
Fallenpfade	`trap.paths`	leer	Pfade, die kein Besucher öffnen sollte. Eine Adresse, die einen öffnet, wird gesperrt. Siehe Fallenpfade und Pfade ohne Anfragegrenze.

Gruppe Eigene Regeln

Bezeichnung	Schlüssel	Vorgabe	Bedeutung
Eigene Regeln	`rules.custom`	leer	Eine JSON-Liste mit höchstens 100 Regeln. Siehe Eigene Regeln.

Gruppe Sperren

Bezeichnung	Schlüssel	Vorgabe	Bedeutung
Sperrdauer (Minuten)	`ban.base_minutes`	15	Dauer der ersten Sperre (1 bis 10080).
Längste Sperre (Minuten)	`ban.max_minutes`	10080	Obergrenze für wiederholte Sperren und wiederholte Anmeldesperren von Adressen (1 bis 525600).

Gruppe Anmeldeschutz

Bezeichnung	Schlüssel	Vorgabe	Bedeutung
Anmeldeschutz	`login.enabled`	ein	Schaltet den Anmeldeschutz ein oder aus.
Fehlgeschlagene Anmeldungen pro Adresse	`login.ip_limit`	5	Fehlversuche, die zu einer Sperre führen (2 bis 1000).
Fehlgeschlagene Anmeldungen pro Benutzername	`login.user_limit`	10	Fehlversuche, die zu einer Anmeldesperre führen (2 bis 1000).
Zeitfenster für Anmeldungen (Minuten)	`login.window_minutes`	15	Zählfenster (1 bis 1440).

Bezeichnung	Schlüssel	Vorgabe	Bedeutung
Sperrdauer für Benutzernamen (Minuten)	`login.lock_minutes`	15	Dauer einer Anmeldesperre (1 bis 1440).
Bei Anmeldung von neuen Adressen warnen	`login.alert_new_address`	ein	Macht das Ereignis einer Anmeldung von einer neuen Adresse zu einem Alarm. Siehe Anmeldeschutz.

Gruppe Zwei-Faktor-Authentifizierung

Bezeichnung	Schlüssel	Vorgabe	Bedeutung
Zweiten Anmeldeschritt verlangen	`twofactor.required`	aus	Verlangt von jedem Benutzer der Administration einen zweiten Schritt. Siehe Zwei-Faktor-Authentifizierung.

Gruppe Ereignisprotokoll

Bezeichnung	Schlüssel	Vorgabe	Bedeutung
Protokolleinträge aufbewahren (Tage)	`audit.retention_days`	90	Wie lange ein Ereignis aufbewahrt wird (1 bis 3650).
Adressen im Protokoll kürzen	`audit.anonymize_ip`	aus	Speichert gekürzte Adressen.

Gruppe Benachrichtigungen

Bezeichnung	Schlüssel	Vorgabe	Bedeutung
Adresse für Benachrichtigungen	`notify.email`	leer	Empfänger der Mails. Leer verwendet die E-Mail-Adresse des Shops.
Sofortige Warnungen	`notify.alerts`	ein	Sendet Warn-Mails.
Zusammenfassung per E-Mail	`notify.digest`	`daily`	`off`, `daily` oder `weekly`.

Gruppe Scanner

Bezeichnung	Schlüssel	Vorgabe	Bedeutung
Zeitplan der Dateiprüfung	`scanner.schedule`	`daily`	`off`, `daily` oder `weekly`.
Uhrzeit der Dateiprüfung	`scanner.hour`	3	Stunde (UTC), ab der der geplante Scan starten darf (0 bis 23).
Geänderte Dateien erkennen	`scanner.baseline`	ein	Vergleicht mit dem Ausgangsstand.
Nach Schadcode suchen	`scanner.content`	ein	Liest die Dateien für die einfachen Prüfungen auf verdächtigen Code.
Auf bekannte Sicherheitslücken prüfen	`scanner.advisories`	ein	Fragt Sicherheitshinweise für die installierten Pakete ab.
Ausgenommene Pfade	`scanner.exclude`	leer	Pfade relativ zum Hauptordner des Shops, die nicht gescannt werden.
Größte geprüfte Datei (KB)	`scanner.max_file_kb`	5120	Größte Datei, die gelesen wird (64 bis 102400).

Gruppe Antwort-Header

Das Plugin kann die Header der Antworten des Shops ändern.

Bezeichnung	Schlüssel	Vorgabe	Bedeutung
PHP-Version verbergen	`headers.hide_php_version`	ein	Entfernt den Header `X-Powered-By`.
HTTPS erzwingen (HSTS)	`headers.hsts`	aus	Sendet `Strict-Transport-Security` bei HTTPS-Anfragen.
HSTS-Dauer (Sekunden)	`headers.hsts_max_age`	31536000	Lebensdauer des HSTS-Headers (300 bis 63072000).
Header Permissions-Policy	`headers.permissions_policy`	leer	Wert des Headers `Permissions-Policy`, bis zu 1024 Bytes. Leer sendet keinen.

Schalten Sie HSTS nur ein, wenn der ganze Shop und alle Subdomains, auf die Sie sich verlassen, über HTTPS funktionieren.

Gruppe Remote-Scan

Bezeichnung	Schlüssel	Vorgabe	Bedeutung
Remote-Scan	`remote.mode`	`off`	`off`, `daemon`, `service` oder `license`. Siehe Remote-Scan und Lizenz.
Socket des lokalen Scan-Dienstes	`remote.socket`	`/run/ispprotect/scand.sock`	Absoluter Pfad des Sockets (Modus `daemon`), höchstens 107 Bytes.
Adresse des Scan-Dienstes	`remote.service_url`	leer	Adresse Ihres eigenen Scan-Dienstes (Modus `service`). HTTPS, oder HTTP nur auf der Loopback-Adresse.
Adresse des gehosteten Scan-Dienstes	`remote.hosted_url`	leer	Optionale Überschreibung des eingebauten gehosteten Scan-Dienstes `https://scan.ispprotect.com` (Modus `license`). Normalerweise leer; eine HTTPS-Adresse nur eintragen, um eine andere Installation zu nutzen, etwa zum Testen.
Adresse des Lizenzportals	`remote.portal_url`	leer (nutzt `https://license.ispprotect.com`)	Überschreiben Sie die eingebaute Lizenz-API-Adresse nur für eine andere Portal-Installation auf der Konsole.
Upload-Grenze je Scan (MB)	`remote.upload_mb`	200	Höchster Dateiinhalt, den ein Scan hochlädt (0 bis 4096). 0 sendet nur Prüfsummen.
Nicht an den Scan-Dienst gesendete Pfade	`remote.exclude`	leer	Pfade, deren Dateien nie gesendet werden.

Gruppe OWASP-CRS-Regeln

Die Gruppe steht auf dem Tab **Firewall** unter der Karte **OWASP-CRS-Regeln** und auf dem Tab **Einstellungen**. Die Regeln müssen installiert sein, damit der Modus **Nur protokollieren** oder **Blockieren** wirkt. Siehe OWASP-CRS-Regeln.

Bezeichnung	Schlüssel	Standard	Bedeutung
Modus der CRS-Regeln	`waf.mode`	`off`	`off`, `log` oder `block`. Die erste Installation der Regeln setzt `log`. Siehe Mit dem Protokollieren beginnen.
Paranoia-Stufe	`waf.paranoia`	`1`	1 bis 4. Höhere Stufen führen mehr Regeln aus und melden mehr normale Anfragen. Siehe Paranoia-Stufe und Schwelle.

Bezeichnung	Schlüssel	Standard	Bedeutung
Anomalie-Schwelle	`waf.threshold`	`5`	Punktzahl, ab der eine Anfrage als Angriff gilt (1 bis 100).
Abgeschaltete Regeln	`waf.disabled_rules`	leer	Regelnummern, die nicht ausgeführt werden, eine pro Zeile (bis zu 500). Eine Regelnummer ist eine ganze Zahl, zum Beispiel `942190`.
Geprüfte Größe des Inhalts	`waf.body_limit`	`131072`	Bytes eines Anfrageinhalts, die geprüft werden (1024 bis 1048576). Ein größerer Inhalt wird mit Status 413 abgewiesen, sofern nicht geprüfte Anfragen durchgelassen werden.
Zeitlimit pro Anfrage	`waf.time_budget_ms`	`200`	Höchstzahl an Millisekunden, die die Regeln für eine Anfrage brauchen dürfen (5 bis 10000).
Anfragen durchlassen, die nicht vollständig geprüft werden können	`waf.pass_uninspected`	aus	Lässt Anfragen durch, die zu groß, zu langsam oder nicht lesbar sind. Sie werden trotzdem aufgezeichnet. Siehe Anfragen, die nicht vollständig geprüft werden können.

Kommandozeile

Das Plugin fügt der Shopware-Konsole 13 Befehle hinzu. Führen Sie sie im Hauptordner des Shops aus, als der Benutzer, der den Shop betreibt:

```
bin/console list ispprotect
bin/console help ispprotect:scan
```

Alle Befehle verwenden die Exit-Codes 0 (erledigt), 1 (Fehler oder ein Fund, der Aufmerksamkeit braucht) und 2 (falsche Verwendung), wie die folgenden Abschnitte sagen.

Übersicht der Befehle

Befehl	Was er tut
`ispprotect:status`	Zeigt Firewall-Modus, Sperren, Anmeldesperren, Funde und Scans.
`ispprotect:checkup`	Führt den Sicherheitscheck aus.
`ispprotect:scan`	Startet einen Dateiscan und zeigt seinen Fortschritt.
`ispprotect:findings`	Listet die offenen Funde des Dateiscanners.
`ispprotect:events`	Zeigt die neuesten Ereignisse des Ereignisprotokolls.
`ispprotect:ip:list`	Listet erlaubte, gesperrte und mit einer Sperre belegte Adressen.
`ispprotect:ip:add`	Fügt der Erlaubnisliste, der Sperrliste oder der Liste der Sperren eine Adresse oder einen Bereich hinzu.
`ispprotect:ip:remove`	Entfernt eine Adresse oder einen Bereich aus der Erlaubnisliste, der Sperrliste und der Liste der Sperren.
`ispprotect:unlock`	Hebt die Anmeldesperre eines Benutzernamens oder einer Adresse auf.
`ispprotect:settings:get`	Zeigt eine Einstellung oder alle Einstellungen.
`ispprotect:settings:set`	Ändert eine Einstellung.
`ispprotect:maintenance`	Führt die Wartung einmal aus: Warnungen, Bereinigung, Scan und Zusammenfassung per E-Mail.
`ispprotect:remote`	Remote-Scan: Zustand, Verbindungstest, Zugangstoken und Lizenz.

Status

```
bin/console ispprotect:status
```

Die Ausgabe zeigt, ob die Firewall und der Anmeldeschutz eingeschaltet sind, die Zahl der aktiven Sperren und Anmeldesperren, die offenen Funde (mit denen der Stufe 3), den letzten vollständigen Scan, einen laufenden Scan und die Ereignisse der letzten 24 Stunden mit Stufe 2 oder höher. Der Exit-Code ist 0.

Sicherheitscheck auf der Konsole

```
bin/console ispprotect:checkup
```

Gibt die Ergebnisse und die Punktzahl aus. Er hat keine Optionen. Exit-Code 1, wenn mindestens eine Prüfung das Ergebnis **Problem** hat, sonst 0. Siehe Sicherheitscheck.

Scan auf der Konsole

```
bin/console ispprotect:scan [--budget=SECONDS] [--no-wait]
```

Startet einen Scan oder setzt einen laufenden fort und zeigt seinen Fortschritt. Ohne Optionen arbeitet er, bis der Scan fertig ist.

Option	Bedeutung
`--budget=SECONDS`	Hält nach etwa so vielen Sekunden an (höchstens 86400). Die geplante Aufgabe setzt den Scan fort.
`--no-wait`	Startet den Scan nur und kehrt zurück.

Exit-Codes: 0, wenn der Scan ohne Funde der Stufe 2 oder höher fertig ist, wenn `--no-wait` verwendet wird und wenn das Budget aufgebraucht ist. 1, wenn der Scan fehlgeschlagen ist oder offene Funde der Stufe 2 oder höher bestehen. 2 bei einem falschen `--budget`.

Befehle für Funde

```
bin/console ispprotect:findings [--all] [--accept=ID] [--accept-all]
```

Option	Bedeutung
(keine)	Listet die offenen Funde, höchstens 500. Exit-Code 1, wenn offene Funde der Stufe 2 oder höher bestehen, sonst 0.
`--all`	Listet auch ignorierte und behobene Funde.
`--accept=ID`	Übernimmt die geänderte, neue oder entfernte Datei dieses Fundes als neuen Ausgangsstand. Exit-Code 0, wenn übernommen. 1, wenn sich die Datei nach dem Scan geändert hat oder der Fund nicht gefunden wurde. 2 bei einer ungültigen ID.
`--accept-all`	Übernimmt jede geänderte, neue und entfernte Datei. Exit-Code 1, wenn einige übersprungen wurden, sonst 0.

Ereignisse auf der Konsole

```
bin/console ispprotect:events [--type=TYPE] [--since=SINCE] [--limit=LIMIT]
```

`--since` ist eine Anzahl von Minuten oder ein Datum in UTC (zum Beispiel `"2026-11-01 12:00"`). `--limit` ist 1 bis 500 (Vorgabe 50). Exit-Code 2 bei einem falschen Wert, sonst 0.

Befehle für Adresslisten

```
bin/console ispprotect:ip:list
bin/console ispprotect:ip:add <kind> <address> [--minutes=N] [--reason=TEXT]
bin/console ispprotect:ip:remove <address>
```

- `<kind>` ist `allow`, `block` oder `ban`. `<address>` ist eine IP-Adresse oder ein CIDR-Bereich.
- `--minutes=N` ist die Lebensdauer, 1 bis 5256000. Ohne sie läuft der Eintrag nie ab. `--reason=TEXT` ist eine Notiz.
- `ispprotect:ip:add` endet mit 2 bei einer falschen Art, Adresse oder Zahl, mit 1, wenn der Eintrag nicht gespeichert wurde (zum Beispiel eine Sperre einer Loopback-Adresse), sonst mit 0.
- `ispprotect:ip:remove` entfernt die Adresse aus allen drei Listen. Es endet mit 2 bei einer ungültigen Adresse, mit 1, wenn nichts gefunden wurde, sonst mit 0.
- `ispprotect:ip:list` endet mit 0.

Entsperren

```
bin/console ispprotect:unlock [<user name>] [--address=IP] [--realm=NAME]
```

Geben Sie entweder einen Benutzernamen oder `--address` an. `--realm` ist der Bereich: `admin` oder `customer`. Ohne `--realm` wird die Sperre in jedem Bereich aufgehoben, der eine hat. Exit-Code 0, wenn eine Sperre aufgehoben wurde, 1, wenn nichts gesperrt war, 2, wenn sowohl Benutzername als auch `--address` oder keines von beiden angegeben wurde oder die Adresse ungültig ist.

```
bin/console ispprotect:unlock admin
bin/console ispprotect:unlock --address=203.0.113.7
bin/console ispprotect:unlock --address=203.0.113.7 --realm=admin
```

Der Befehl hebt keine Sperre der Firewall auf. Verwenden Sie dafür `ispprotect:ip:remove`. Er setzt den Zähler der falschen Zwei-Faktor-Codes nicht zurück. Siehe Anmeldeschutz.

Einstellungen auf der Konsole

```
bin/console ispprotect:settings:get [<key>]
bin/console ispprotect:settings:set <key> <value>
```

`settings:get` ohne Schlüssel zeigt jede Einstellung. Ein unbekannter Schlüssel ergibt Exit-Code 2. `settings:set` liest den Wert als JSON, wenn er gültig ist, sonst als Text. Ein unbekannter Schlüssel oder ein abgelehnter Wert ergibt Exit-Code 2. Siehe Einstellungsreferenz.

Wartung

```
bin/console ispprotect:maintenance
```

Führt einmal aus, was die geplante Aufgabe alle 5 Minuten ausführt: Sie sendet ausstehende Warnungen, bereinigt alte Daten (einmal pro Stunde), erneuert eine verbundene Lizenz, startet und bringt den Scan voran und sendet die Zusammenfassung per E-Mail. Exit-Code 1, wenn einer der Schritte fehlschlägt, sonst 0. Siehe Zeitplanung.

Remote-Scan auf der Konsole

```
bin/console ispprotect:remote [<action>]
```

Aktion	Bedeutung
`status`	Zeigt den Modus, die Adresse des Scan-Dienstes, ob Geheimnisse gespeichert werden können, den Zugangstoken und den Lizenzschlüssel (nur ihre letzten vier Zeichen), ob die Website verbunden ist, die Lizenzdaten und die Zähler des letzten Remote-Scans. Das ist die Vorgabe.
`test`	Fragt den Scan-Dienst des aktuellen Modus nach seinem Zustand. Exit-Code 1, wenn das fehlschlägt.
`token:set`	Speichert den Zugangstoken Ihres eigenen Scan-Dienstes.
`token:clear`	Entfernt den Zugangstoken.
`connect`	Verbindet diese Website mit einer Lizenz des gehosteten Scan-Dienstes.
`refresh`	Erneuert den Zugang der Lizenz jetzt.
`disconnect`	Gibt diese Website im Lizenzportal frei und entfernt die lokalen Lizenzdaten.

Der Zugangstoken und der Lizenzschlüssel werden nie von der Kommandozeile übernommen, weil die Kommandozeile für andere Benutzer des Servers sichtbar ist und in der Shell-History landet. Übergeben Sie sie per Pipe oder tippen Sie sie an der verdeckten Eingabeaufforderung:

```
bin/console ispprotect:remote connect < key.txt
```

Exit-Codes: 0, wenn erledigt, 1, wenn die Aktion fehlgeschlagen ist (auch wenn es keine verdeckte Eingabeaufforderung und keine Eingabe per Pipe gibt), 2 bei einer unbekannten Aktion, zusätzlichen Argumenten oder einem Geheimnis in einem falschen Format. `disconnect` endet mit 0, auch wenn die Freigabe im Portal fehlschlägt. Es gibt dann eine Warnung aus, weil die lokalen Daten in jedem Fall entfernt werden. Siehe Remote-Scan und Lizenz.

Zurück ins System und Fehlerbehebung

Jede Aussperrung lässt sich auf der Konsole des Servers rückgängig machen. Führen Sie die Befehle im Hauptordner des Shops aus. Wenn Sie sich nicht an der Administration anmelden können, brauchen Sie Zugriff auf den Server.

Ihre eigene Adresse ist gesperrt oder steht auf der Sperrliste

Anzeichen: Seiten antworten für Sie mit Status 403 oder 429, oder die Administration lädt nicht. Mögliche Ursachen: eine Sperre durch die Firewall, ein Eintrag in der Sperrliste oder eine Sperrregel.

1. Finden Sie den Eintrag:

```
bin/console ispprotect:ip:list
```

1. Entfernen Sie ihn. Das entfernt die Adresse aus der Erlaubnisliste, der Sperrliste und der Liste der Sperren:

```
bin/console ispprotect:ip:remove 203.0.113.7
```

Wenn der Eintrag ein Bereich ist, der Ihre Adresse abdeckt, entfernen Sie den Bereich genau so, wie ihn die Liste zeigt. Sperren enden nach ihrer Dauer von selbst. Wenn Ihre Adresse wegen eines Proxys gesperrt wurde, siehe Alle Besucher haben dieselbe Adresse.

Um Ihre Adresse vor automatischen Maßnahmen sicher zu machen, tragen Sie sie in die Erlaubnisliste ein:

```
bin/console ispprotect:ip:add allow 203.0.113.7 --reason="office"
```

Ein Benutzername oder eine Adresse ist gesperrt

Anzeichen: Die Administration antwortet „zu viele Versuche“ für einen Benutzernamen oder mit dem Fehler 1103 mit Status 403 für eine Adresse, auch mit dem richtigen Passwort. Ein Kunde sieht die Meldung für falsche Zugangsdaten.

```
bin/console ispprotect:unlock admin
bin/console ispprotect:unlock --address=203.0.113.7
```

Fügen Sie `--realm=admin` oder `--realm=customer` hinzu, um nur einen Bereich aufzuheben. Eine Sperre der Adresse in der Firewall heben Sie mit `ispprotect:ip:remove` auf. Oder öffnen Sie den Tab **Anmeldeschutz** von einem anderen Konto aus. Siehe Sperren und Anmeldesperren aufheben.

Auf der Seite zur Einrichtung der Zwei-Faktor-Anmeldung festgehalten

Anzeichen: Nach der Anmeldung zeigt die Administration nur die Seite **Zwei-Faktor**, und andere Anfragen antworten mit dem Code `ISPPROTECT__TWOFACTOR_SETUP_REQUIRED`. Der Shop verlangt einen zweiten Schritt, Ihr Konto hat keinen, und Sie können ihn nicht einrichten. Heben Sie die Pflicht auf:

```
bin/console ispprotect:settings:set twofactor.required false
```

Gerät verloren oder von der Zwei-Faktor-Anmeldung ausgesperrt

Wenn Sie noch einen Wiederherstellungscode haben, verwenden Sie ihn anstelle des Codes aus der App. Jeder Wiederherstellungscode funktioniert einmal.

Ohne Wiederherstellungscode und mit verlorener App gibt es keinen Konsolenbefehl, der den zweiten Schritt eines einzelnen Benutzers entfernt. Ein anderer Administrator kann ihn für diesen Benutzer über die Route der Administration-API `POST /api/_action/ispprotect/twofactor/user/{userId}/disable` ausschalten. Der Aufrufer braucht das Recht, Benutzer zu aktualisieren, und ein kürzlich bestätigtes Passwort, und kann sie nicht für das eigene Konto verwenden. Die Administration hat dafür keine Schaltfläche. Der Aufruf wird als Ereignis `account.changed` aufgezeichnet.

Die Pflicht mit `twofactor.required` aufzuheben entfernt den zweiten Schritt eines Benutzers nicht, der schon einen hat.

Wenn Sie `APP_SECRET` des Shops geändert haben, lassen sich die gespeicherten Schlüssel des zweiten Schritts nicht entschlüsseln, und Benutzer mit zweitem Schritt kommen an der Codeprüfung nicht vorbei. Stellen Sie das alte `APP_SECRET` wieder her.

Die Firewall weist alles ab

Wenn Sie die Ursache nicht finden, schalten Sie die Firewall aus, melden Sie sich an und reparieren Sie dann die Einstellungen:

```
bin/console ispprotect:settings:set firewall.mode off
```

Setzen Sie den Modus auf `log`, um zu sehen, was die Firewall ohne Abweisungen tun würde. Siehe Firewall-Modi.

Eine Regel oder ein Fallenpfad sperrt die Administration

Anzeichen: Nachdem Sie eine Sperrregel oder einen Fallenpfad gespeichert haben, wird die Anmeldeseite oder die Administration abgewiesen. Entfernen Sie die Einstellung:

```
bin/console ispprotect:settings:set rules.custom '[]'
bin/console ispprotect:settings:set trap.paths '[]'
```

Entfernen Sie dann Ihre eigene Adresse aus der Liste der Sperren, wie unter Ihre eigene Adresse ist gesperrt oder steht auf der Sperrliste.

Alle Besucher haben dieselbe Adresse

Anzeichen: Die Firewall sperrt eine Adresse und niemand erreicht den Shop, oder der Tab Ereignisse zeigt für jeden Besucher dieselbe Adresse. Der Shop steht hinter einem Reverse-Proxy oder CDN, und Shopware kennt den Proxy nicht. Setzen Sie `SYMFONY_TRUSTED_PROXIES` auf die Adressen Ihrer Proxys. Siehe Hinter einem Reverse-Proxy oder CDN. Heben Sie dann die Sperre der Proxy-Adresse auf, wie unter Ihre eigene Adresse ist gesperrt oder steht auf der Sperrliste.

Warnungen, Zusammenfassungen oder Scans laufen nicht

Die geplante Aufgabe `ispprotect.maintenance` läuft nur, wenn der Scheduler von Shopware und ein Message-Consumer laufen. Testen Sie sie einmal mit:

```
bin/console ispprotect:maintenance
```

Wenn das funktioniert, läuft der Scheduler oder der Consumer nicht. Siehe Zeitplanung. Die Prüfung „Der Dateiscan lief in den letzten {days} Tagen“ im Sicherheitscheck zeigt dasselbe Problem. Siehe Sicherheitscheck.

Mails kommen nicht an

Prüfen Sie **Adresse für Benachrichtigungen**, **Sofortige Warnungen** und **Zusammenfassung per E-Mail** und die Mail-Einstellungen des Shops. Eine fehlgeschlagene Mail wird als Ereignis `system.notice` mit dem Grund `mail_failed` aufgezeichnet, und die Ereignisse bleiben ungesendet. Siehe Einstellungen der Benachrichtigungen.

Meldungen des Plugins

- Status 503 mit dem Code `ISPPROTECT__API_UNAVAILABLE`: Das Plugin konnte seine Daten für eine Anfrage der Administration nicht lesen oder schreiben. Prüfen Sie die Datenbank und die Datei `var/log/ISPProtectWebSecurity.log`.
- Status 503 mit dem Code `ISPPROTECT__TWOFACTOR_UNAVAILABLE` oder Anmeldefehler 1104: Der Zustand des zweiten Schritts lässt sich nicht lesen. Prüfen Sie die Datenbank und die Logdatei.
- Das Plugin schreibt seine eigenen Probleme in `var/log/ISPProtectWebSecurity.log`.

Die OWASP-CRS-Regeln weisen eine normale Anfrage ab

Die OWASP-CRS-Regeln können eine normale Anfrage abweisen (ein Fehlalarm). Die Anfrage wird mit Status 403 beantwortet, bei einer nicht vollständig prüfbaren Anfrage mit 413 oder 400. Den Hintergrund finden Sie unter OWASP-CRS-Regeln.

1. Öffnen Sie den Tab **Ereignisse** und suchen Sie den Eintrag **Anfrage von der Firewall abgewiesen** (oder **Anfrage von der Firewall protokolliert**, im Modus **Nur protokollieren**). Notieren Sie die Regelnummern in den Details.
2. Schalten Sie die falsche Regel ab: Tragen Sie ihre Nummer in dem Feld **Regel abschalten** auf der Karte **OWASP-CRS-Regeln** auf dem Tab **Firewall** ein. Eine abgeschaltete Regel läuft für keine Anfrage mehr, schalten Sie daher nur die Regel ab, die das Problem verursacht hat.
3. Scheitert das Speichern von sehr viel Inhalt mit Status 413 und der Nummer `200101`, erhöhen Sie **Geprüfte Größe des Inhalts** (`waf.body_limit`), zum Beispiel auf 524288.
4. Brechen Anfragen mit der Nummer `200100` ab, erhöhen Sie **Zeitlimit pro Anfrage** (`waf.time_budget_ms`) oder schalten Sie die Nummer `200100` ab. Programmcode in einem Formularfeld (etwa 20 bis 40 KB) kann das voreingestellte Limit von 200 Millisekunden aufbrauchen. Anfragen, die mit der Nummer `200005` abgelehnt werden (selten überschreitet ein langes Feld mit Programmcode die Grenzen von PHP für reguläre Ausdrücke), behandeln Sie genauso: Schalten Sie `200005` ab oder lassen Sie Anfragen durch, die nicht vollständig geprüft werden können.

Um die Ursache zu finden, ohne Besucher auszusperren, stellen Sie **Modus der CRS-Regeln** auf **Nur protokollieren**: Anfragen werden dann nur aufgezeichnet.

Können Sie sich nicht mehr anmelden, schalten Sie die CRS-Regeln auf der Konsole ab, melden Sie sich an und schalten Sie danach die Regel ab:

```
bin/console ispprotect:settings:set waf.mode off
```

Datenschutz und externe Dienste

Was das Plugin speichert

Das Plugin speichert seine Daten in eigenen Tabellen in der Datenbank des Shops, alle mit dem Präfix `ispprotect_`. Es speichert:

- die Adresslisten, Sperren und Anmeldesperren
- Fehlerzähler
- das Ereignisprotokoll mit Adressen und Benutzernamen, für **Protokolleinträge aufbewahren (Tage)**. Bei eingeschaltetem **Adressen im Protokoll kürzen** werden Adressen gekürzt, bevor sie gespeichert werden. Siehe Einstellungen des Ereignisprotokolls.
- den Ausgangsstand und die Funde des Dateiscanners
- den zweiten Schritt von Benutzern der Administration: den Schlüssel (verschlüsselt) und die Hashes der Wiederherstellungscodes
- einen Zugangstoken und einen Lizenzschlüssel des Remote-Scans, verschlüsselt

Von einer Adresse mit Anmeldesperre für eine geschützte Adresse eines Administrators wird nur ein Hash gespeichert.

Das Ereignisprotokoll speichert die Namen geänderter Felder, nie ihre Werte. Das Plugin ändert keine Tabellen von Shopware.

Externe Dienste

Das sind die externen Dienste, die das Plugin kontaktieren kann. Die Seite für den zweiten Schritt zeigt keinen QR-Code, damit nichts von einer anderen Seite abgerufen wird.

Packagist

Wenn **Auf bekannte Sicherheitslücken prüfen** eingeschaltet ist, fragt jeder Scan `https://packagist.org/api/security-advisories/` nach den installierten Composer-Paketen. Das Plugin sendet Paketnamen. Die Antworten werden zwischengespeichert. Wenn Packagist nicht erreichbar ist, wird die Prüfung übersprungen, und das Plugin zeichnet das Ereignis `system.notice` auf. Schalten Sie die Prüfung aus, um die Anfrage zu verhindern.

Scan-Dienst und Lizenzportal (Remote-Scan)

Der Remote-Scan ist standardmäßig ausgeschaltet. Nur wenn Sie einen anderen Modus als **Aus** wählen, kontaktiert das Plugin einen Scan-Dienst.

- **Lokaler Scan-Dienst (Socket)**: ein Dienst auf demselben Server. Nichts verlässt den Server.
- **Eigener Scan-Dienst**: Ihr eigener Dienst unter der Adresse, die Sie setzen.
- **Gehosteter Scan-Dienst (Lizenz)**: der gehostete Scan-Dienst unter `https://scan.ispprotect.com` und die Lizenz-API unter `https://license.ispprotect.com`. An die Konto-Konsole unter `https://console.ispprotect.com` sendet das Plugin keine Anfragen.

An einen Scan-Dienst sendet das Plugin die SHA-256-Prüfsumme und einen Namenshinweis jeder nicht leeren Code-Datei, die es prüft, und lädt eine Datei nur hoch, wenn der Dienst ihre Prüfsumme nicht kennt, bis zur **Upload-Grenze je Scan (MB)**. Dateien mit Geheimnissen, etwa Schlüssel, `.env`-Dateien und Datenbank-Dumps, werden nie gesendet. Einige PHP-Konfigurationsdateien werden nur in geschwärzter Form gesendet, wobei alle Zeichenketten, Zahlen und Kommentare ersetzt sind. Die genaue Liste und was das Lizenzportal erhält, stehen unter Was gesendet wird und was nie.

OWASP-CRS-Regeln (GitHub)

Das Plugin lädt die OWASP-CRS-Regeln von `github.com` (und dem Download-Host, auf den GitHub weiterleitet) nur herunter, wenn Sie auf **CRS 4.25.2 installieren** oder **Auf CRS aktualisieren** klicken, nie im Hintergrund. Die Anfrage verlangt eine feste Datei, das Regelarchiv des CRS-Projekts. Nichts über Ihren Shop, dessen Besucher oder deren Anfragen wird gesendet. Der Download wird mit einer im Plugin eingebauten Prüfsumme verglichen. Anfragen an Ihren Shop werden auf Ihrem Server geprüft und nie irgendwohin gesendet.

Mail

Warn-Mails und die Zusammenfassung per E-Mail gehen über den Mail-Dienst von Shopware an die **Adresse für Benachrichtigungen**. Was nach dem Verlassen des Shops mit ihnen geschieht, hängt von den Mail-Einstellungen des Shops ab.

Ausschalten

Sie können jede Nutzung ausschalten: **Auf bekannte Sicherheitslücken prüfen** aus, **Remote-Scan Aus**, **Sofortige Warnungen** aus und **Zusammenfassung per E-Mail Aus**. Siehe Einstellungsreferenz.

Das Plugin entfernen

Deaktivieren

Das Deaktivieren des Plugins hält die Firewall, den Anmeldeschutz und die Prüfung des zweiten Schritts an, weil sie als Teil des Plugins laufen. Die Daten bleiben. Beim erneuten Aktivieren des Plugins wird geprüft, ob die Tabellen vorhanden sind, und der Cache-Pool des Plugins wird geleert.

Deinstallieren

Beim Deinstallieren wird gefragt, ob die Benutzerdaten behalten werden sollen. Öffnen Sie in der Administration **Erweiterungen > Meine Erweiterungen** und wählen Sie beim Plugin **Deinstallieren**. Auf der Konsole:

```
bin/console plugin:uninstall --keep-user-data ISPProtectWebSecurity
bin/console plugin:uninstall ISPProtectWebSecurity
```

- **Daten behalten** (der Dialog der Administration ohne „alle Daten löschen“ oder `--keep-user-data`): Die Tabellen bleiben. Alle Einstellungen, Adresslisten, Sperren, Anmeldesperren, das Ereignisprotokoll, die Scan-Ergebnisse und die Geheimnisse des zweiten Schritts der Benutzer bleiben. Sie werden wieder verwendet, wenn Sie das Plugin erneut installieren. Es wird nichts an das Lizenzportal gesendet, und eine verbundene Lizenz bleibt verbunden.
- **Daten löschen** (der Dialog mit „alle Daten löschen“ oder `plugin:uninstall` ohne `--keep-user-data`): Das Plugin löscht alle seine Tabellen und leert seinen Cache-Pool. Einstellungen, Listen, das Ereignisprotokoll, Funde und der zweite Schritt jedes Benutzers sind weg. Danach melden sich Benutzer nur mit dem Passwort an.

Das Plugin ändert keine Tabelle und keine Datei von Shopware, deshalb muss sonst nichts bereinigt werden. Shopware entfernt seine eigenen Migrationseinträge beim Deinstallieren. Die Logdatei `var/log/ISPProtectWebSecurity.log` bleibt in beiden Fällen. Löschen Sie sie selbst, wenn Sie sie nicht brauchen.

Was mit einer verbundenen Lizenz geschieht

Wenn Sie die Daten löschen und ein Lizenzschlüssel gespeichert ist, gibt das Plugin zuerst die Website im Lizenzportal frei. Das geschieht in jedem Modus des Remote-Scans. Es ist ein einziger Aufruf mit kurzem Timeout, sodass die Website nicht mehr auf das Website-Limit Ihrer Lizenz zählt.

Wenn das Portal nicht erreichbar ist oder ablehnt, geht die Deinstallation weiter, und das Plugin zeigt keine Meldung. Geben Sie die Website selbst im Lizenzportal frei, unter der Adresse, die Sie mit Ihrer Lizenz erhalten haben.

Um eine Website vor der Deinstallation freizugeben, verwenden Sie **Trennen** auf dem Tab **Scanner** oder `bin/console ispprotect:remote disconnect`. Siehe Remote-Scan und Lizenz.

Die Dateien entfernen

Entfernen Sie nach der Deinstallation den Code:

- Wenn Sie das Plugin mit Composer installiert haben: `composer remove ispprotect/shopware-web-security`.
- Sonst löschen Sie den Ordner `custom/plugins/ISPProtectWebSecurity`.

Führen Sie dann `bin/console cache:clear` aus.