

Bedienung im Alltag

- [Globale Sperrlisten \(Policy Lists\) verstehen](#)
- [Raumregeln und Protections](#)
- [Meldungen \(Reports\) und „Trusted Reporters“](#)
- [Nutzung über den Matrix-Client \(Kontrollraum und Prompts\)](#)
- [Interaktive Prompts im Alltag](#)

Globale Sperrlisten (Policy Lists) verstehen

Wie bereits erwähnt, arbeitet Draupnir mit Banlisten-Räumen, in denen gesperrte Benutzer-IDs und Server verwaltet werden. Ihre eigene Instanz hat mindestens eine solche Liste (Standard-Banliste für Ihre Community).

Einträge in dieser Liste – z.B. `@spamuser:spam.com` oder ganze Homeserver wie `spam.com` – bedeuten, dass Draupnir alle diese Nutzer serverweit aus Ihren Räumen fernhält.

Sie können weitere eigene Listen erstellen (etwa getrennt nach Spam vs. CoC-Verstößen) mit `!draupnir list create ...`.

Wichtig ist: Jede Liste ist technisch gesehen ein Matrix-Raum mit eigener Raum-ID bzw. Alias, und Draupnir hält die Sperreinträge als Raum-State dort fest.

Dies ermöglicht es, Listen mit anderen Communities zu teilen: Andere Draupnir- oder Mjolnir-Bots können Ihre List-Räume abonnieren, und Sie können umgekehrt öffentliche List-Räume Dritter abonnieren.

Durch solches „Abonnieren“ (Watch) werden fremde Banlisten in Ihren Räumen wirksam.

Praktisch heißt das, wenn z.B. eine Nachbargemeinschaft eine Spam-Liste pflegt und Sie diese abonnieren, werden alle dort gelisteten Störenfriede auch in Ihren Räumen gebannt, ohne dass Sie jeden selbst entdecken müssen.

Diese verteilte Moderation hält das Matrix-Netzwerk sicherer.

Hinweis: Welche Listen Sie abonnieren, sollten Sie sorgfältig auswählen – achten Sie darauf, dass die Betreiber vertrauenswürdig und die Listen aktuell sind. Sie können abonnierte Listen jederzeit mit `!draupnir unwatch <Alias>` abbestellen, falls Sie doch nicht passen.

Raumregeln und Protections

Draupnir verfügt über ein Plugin-System für automatische Schutzmechanismen, sogenannte Protections. Viele davon sind standardmäßig aktiviert, um gängige Spam-Muster zu bekämpfen.

Beispiele für solche Regeln:

- **Neue-Mitglieder-Schutz (New Joiner Protection):** Erkennt, wenn viele neue Nutzer in kurzer Zeit einem Raum beitreten und Nachrichten senden, und kann automatisch Gegenmaßnahmen ergreifen.
- **Erste-Nachricht-Bild-Sperre:** Verhindert, dass neu beigetretene Nutzer als erste Nachricht direkt ein Bild oder eine Datei senden.
- **Erwähnungs-Limit (Mention Limit Protection):** Limitiert die Anzahl der Benutzer, die in einer einzelnen Nachricht erwähnt werden können.
- **Voice/Video-Message-Filter:** Kann so eingestellt werden, dass Sprachnachrichten oder bestimmte Medientypen automatisch entfernt werden.
- **Trusted Invite Blocker:** Blockiert serverweit Einladungen von Nutzern oder Homeservern, die auf Sperrlisten stehen.
- **Automatisierte Raum-Schließung (Room Takedown):** Kann im Extremfall einen Raum gezielt unzugänglich machen.

Die meisten dieser Protections lassen sich ein- oder ausschalten und oft auch konfigurieren.

Als Raum-Admin können Sie z.B. per Befehl `!draupnir protections` eine Liste aller verfügbaren Module erhalten. Mit `!draupnir enable <ProtectionName>` oder `disable` können einzelne Module gesteuert werden.

Einige erweiterte Einstellungen erfolgen über `!draupnir config ...` Befehle. Details finden Sie bei Bedarf in der offiziellen Protections-Dokumentation des Draupnir-Projekts.

Meldungen (Reports) und „Trusted Reporters“

Matrix bietet Benutzern die Möglichkeit, anstößige oder regelwidrige Inhalte über die Melden-Funktion dem Raum-Admin bzw. Server-Admin zu melden.

Draupnir kann – sofern entsprechend konfiguriert – diese Meldungen auswerten und darauf reagieren.

Insbesondere gibt es eine Protection namens **Trusted Reporters**. Hier können Sie bestimmte User Ihrer Community als „Trusted“ markieren.

Wenn dann genügend dieser vertrauenswürdigen Nutzer dieselbe Nachricht melden, kann Draupnir automatisch Maßnahmen ergreifen.

Zum Beispiel könnte ab einer Meldeschwelle von drei vertrauenswürdigen Reports die gemeldete Nachricht automatisch vom Bot redigiert werden.

Es lassen sich auch Schwellen für automatische Banns definieren.

Voraussetzung ist, dass Abuse Reporting in Ihrer Draupnir-Instanz aktiviert ist und der Bot regelmäßig neue Reports vom Server abfragt.

Im Alltag bedeutet dies: Wenn Sie Meldungen erhalten, können Sie entweder selbst tätig werden oder – falls Trusted Reporters aktiv sind – darauf vertrauen, dass Draupnir bei einer Häufung von Meldungen reagiert.

Alle eingehenden Reports aus Ihren geschützten Räumen kann Draupnir auch im Kontrollraum protokollieren (je nach Konfiguration), sodass Sie einen Überblick über gemeldete Inhalte haben.

Beachten Sie, dass diese Features meist mit erweiterten Rechten einhergehen und u.U. nicht in jeder Draupnir-Instanz auf Gemeinschaftsservern aktiviert sind.

Nutzung über den Matrix-Client (Kontrollraum und Prompts)

Die Interaktion mit Draupnir erfolgt vollständig über Matrix – es gibt keine separate Web-Oberfläche im klassischen Sinne, sondern Sie bedienen den Bot bequem in Ihrem Matrix-Client (z.B. Element Web/Desktop) durch Nachrichten und vom Bot bereitgestellte Bedienelemente im Chat.

Im Kontrollraum (Ihrer Verwaltungs- und Listenraum) können Sie Befehle eintippen. Alle Kommandos beginnen mit `!draupnir`. Eine Liste erhalten Sie mit `!draupnir help`, die Ihnen einen Überblick über mögliche Aktionen gibt.

Hier einige wichtige Basisbefehle:

`!draupnir rooms list` – listet alle Räume auf, die aktuell vom Bot geschützt werden.

`!draupnir rooms add/remove <Raum>` – fügt einen Raum dem Schutz hinzu bzw. entfernt ihn (siehe Abschnitt Provisionierung).

`!draupnir list create <Kurzname> <Alias>` – erstellt eine neue Policy-Liste (Banliste) mit einem internen Kurznamen und einem Matrix-Alias.

`!draupnir watch <Alias>` – abonniert eine externe Policy-Liste (siehe globale Sperrlisten unten).

`!draupnir ban <User> <Grund>` – bannt einen Benutzer auf allen geschützten Räumen (fügt ihn zur Banliste hinzu).

`!draupnir unban <User>` – hebt einen solchen Bann wieder auf.

Interaktive Prompts im Alltag

Die meisten dieser Aktionen können aber, wie erwähnt, komfortabler durchgeführt werden: Draupnir nutzt ein interaktives Prompt-System, das eng mit dem Matrix-Client zusammenarbeitet.

Räume schützen:

Statt `!draupnir rooms add ...` manuell einzugeben, können Sie einfach den Bot in einen Raum einladen. Der Bot postet daraufhin im Kontrollraum eine Meldung à la „Soll Raum XYZ geschützt werden?“ mit Auswahlmöglichkeiten. Bestätigen Sie mit „OK“ (z.B. als Reaktion oder Button), erledigt Draupnir den Rest für Sie.

Bann propagieren:

Wenn Sie in einem vom Bot überwachten Raum über die übliche Matrix-Funktion einen Störenfried bannen (z.B. via Kontextmenü „Nutzer entfernen“ in Element), registriert Draupnir dies. Im Kontrollraum erscheint dann eine Meldung, die sinngemäß fragt: „Benutzer @abc:example.com wurde in Raum XYZ gebannt. Soll dieser Bann der globalen Liste hinzugefügt werden?“

Wenn Sie zustimmen, wird der Nutzer zur Policy-Liste hinzugefügt und damit in allen geschützten Räumen gebannt. So müssen Sie nicht in jedem Raum einzeln tätig werden – Draupnir synchronisiert es automatisch.

Entbannung:

Ähnlich verhält es sich, wenn Sie jemanden in einem Raum entbannen. Draupnir fragt nach, ob der Eintrag auch aus der globalen Bannliste entfernt werden soll. So können Sie False Positives schnell korrigieren, ohne mühsam an vielen Stellen händisch Anpassungen vorzunehmen.

Listen abonnieren:

Auch beim Abonnieren von Sperrlisten hilft Draupnir interaktiv. Wenn Sie den Bot in einen Raum einladen, der als Policy-List eines anderen Projekts dient, erkennt Draupnir dies in der Regel und fragt, ob er diese Liste beobachten soll. (Alternativ nutzt man `!draupnir watch` wie oben erwähnt.)

Insgesamt ist die Bedienung darauf ausgelegt, möglichst viel über normale Client-Interaktionen zu steuern, sodass klassische Chat-Administratoren intuitiv mit Draupnir arbeiten können. Falls eine Aktion mal nicht über Prompts ausgelöst wird, oder Sie ein Problem per Kommando lösen müssen, steht Ihnen jederzeit `!draupnir help` zur Verfügung sowie die ausführliche Moderatordokumentation des Draupnir-Projekts (siehe Abschnitt 6 für Links).