

Verschlüsselung (E2EE): was geht, was nicht

Verschlüsselung beachten:

Im AppService-Modus unterstützt Draupnir aktuell keine Ende-zu-Ende-Verschlüsselung (E2EE).

Das bedeutet, dass Ihr Kontrollraum unverschlüsselt sein muss – andernfalls könnte der Bot Ihre Kommandos nicht lesen.

Auch geschützte Räume, die e2e-verschlüsselt sind, stellen eine Einschränkung dar:

Draupnir kann in solchen Räumen zwar grundsätzlich noch Benutzer anhand ihrer IDs bannen oder bekannte Spam-Server blockieren, jedoch keine Inhalte prüfen.

Funktionen, die Nachrichteninhalte analysieren (z.B. Wortfilter oder das Erkennen eines ersten Bild-Posts), greifen in E2EE-Räumen nicht zuverlässig, da Draupnir die verschlüsselten Events nicht entschlüsseln kann.

Dennoch kann Draupnir grundlegende Protektionen in verschlüsselten Räumen ausführen, solange diese keine Klartext-Inhalte benötigen.

Fazit: Für öffentliche Räume, die moderiert werden sollen, empfiehlt es sich, auf Verschlüsselung zu verzichten, oder zumindest die Limitierungen im Hinterkopf zu behalten.

Der Kontrollraum selbst sollte immer unverschlüsselt und nur für Sie (und ggf. Mit-Administratoren) zugänglich sein.

Revision #2

Created 2026-01-07 21:44:14 UTC by pacey

Updated 2026-01-07 22:25:42 UTC by pacey