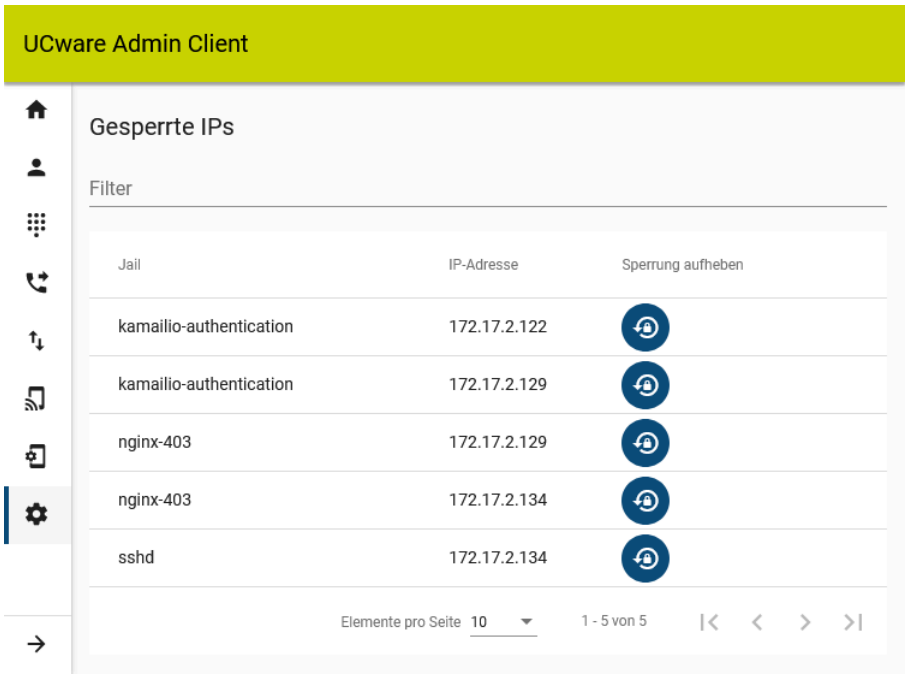
Admin-Client, System, Sperre

IP-Sperren aufheben

Grundlagen

Der UCware Server erkennt potenzielle Angreifer anhand der Art und der Häufigkeit ihrer Anfragen und sperrt verdächtige IP-Adressen automatisch. Dies kann unter bestimmten Voraussetzungen dazu führen, dass vertrauenswürdige Geräte oder Clients nicht mehr auf die Telefonanlage zugreifen können.

In diesem Fall können Sie die zugehörigen IP-Adressen im Admin-Client wie folgt entsperren:



1. Rufen Sie die Seite **System > Gesperrte IPs** auf.
2. Klicken Sie im Eintrag der gewünschten IP-Adresse auf .

Hinweis:
Das Entsperren einer IP-Adresse, hebt die zugehörige Blockade in **allen Jails** auf.

Erweitert

Hinweis:
Für detaillierte Informationen zu Fail2Ban lesen Sie die Hersteller-Dokumentation.

Der UCware Server verwendet das Intrusion-Prevention-System **Fail2Ban** zum Sperren verdächtiger IP-Adressen. Dieses basiert im Wesentlichen auf drei Komponenten:

- Filter enthalten reguläre Ausdrücke zum Durchsuchen von Log-Dateien.
- Aktionen lösen vordefinierte Skripte aus – beispielsweise zum Sperren von IP-Adressen nach Suchtreffern im Log.
- Jails ergeben sich aus den Zusammenspiel eines Filters mit einer oder mehreren Aktionen.

Auf dem UCware Server sind standardmäßig die folgenden **Jails** definiert:

Jail-Bezeichnung	Bedingung für IP-Sperre	Dauer der IP-Sperre
`kamailio-authentication`	5 fehlgeschlagene Versuche in 60 Sekunden	7200 Sekunden / 2 Stunden
`nginx-403`	5 fehlgeschlagene Versuche in 30 Sekunden	
`sshd`	5 fehlgeschlagene Versuche in 600 Sekunden	600 Sekunden

Sie können die Standard-Konfiguration bei Bedarf anpassen und um eigene Filter, Aktionen und Jails erweitern. Die dadurch ausgelösten IP-Sperren werden ebenfalls im Admin-Client angezeigt und lassen sich dort bei Bedarf aufheben. Für vertrauenswürdige IP-Adressen existiert darüber hinaus eine Whitelist-Funktion.

From:
https://wiki.ucware.com/ - **UCware-Dokumentation**

Permanent link:
https://wiki.ucware.com/adhandbuch/system/gesperrte_ips

Last update: **20.07.2023 14:14**