GeoIP and Fail2Ban Filters

Configure country filters, rate limits, Fail2Ban behavior, and blocked or trusted addresses.

Use **Admin > GeoIP and Fail2Ban Filters** to manage geoip and fail2ban filters.

This page is a starting point for administrators: review existing records, add only the objects needed by the deployment, and keep names consistent across tenants, routing, and provisioning. The source form exposes these main blocks or fields: GeoIP allowed countries, Locate IP Address, Enable VoIP Fail2Ban, Enable web interface Fail2Ban, Fail2Ban max attempts, Notify ban activity, Notify address, Notify sender address.

Typical Workflow

1. Open the menu entry and confirm whether the record already exists.
2. Create or edit the record with a descriptive name and only the required options first.
3. Save the record and reopen it to verify the stored values.
4. Check dependent objects before deleting anything that may be used by routing, billing, provisioning, or reporting.

Documentation Example

For documentation and testing, use names prefixed with **Docs Demo**. Existing PBX nodes should be reused as examples; do not create additional nodes unless the deployment actually requires them.

Errors reported

The checkgeoipf2b.php script can report an error if the configuration data is incorrect, like in this case, when there is an extra space in the -- jump ACCEPT string.

GeoIP/Fail2Ban - All Tenants

⚠ danielgraystone:

```
iptables-restore --test failed with return code 2
Executable: /usr/sbin/iptables-restore
stderr:
  iptables-restore v1.4.21: unknown arguments found on commandline
  Error occurred at line: 783
  Try `iptables-restore -h&#039; or &#039;iptables-restore --help&#039; for more information.
Ruleset context:
  Around reported line 783:
     780: -A CustomRules --protocol tcp --dst 127.0.0.1 --jump ACCEPT
     781: -A CustomRules --protocol udp --src 127.0.0.1 --jump ACCEPT
     782: -A CustomRules --protocol udp --dst 127.0.0.1 --jump ACCEPT
  &gt;  783: -A CustomRules --protocol icmp --src 127.0.0.1 -- jump ACCEPT
     784: -A CustomRules --protocol icmp --dst 127.0.0.1 --jump ACCEPT
     785: -A CustomRules --protocol udp --dst 172.17.0.1 --jump ACCEPT
     786: -A CustomRules --protocol udp --src 172.17.0.1 --jump ACCEPT
```

Main Fields

Field or block	Purpose
GeoIP allowed countries	Review this value in relation to the object being configured and the tenant or system scope where it is used.
Locate IP Address	Review this value in relation to the object being configured and the tenant or system scope where it is used.
Enable VoIP Fail2Ban	Review this value in relation to the object being configured and the tenant or system scope where it is used.
Enable web interface Fail2Ban	Review this value in relation to the object being configured and the tenant or system scope where it is used.
Fail2Ban max attempts	Review this value in relation to the object being configured and the tenant or system scope where it is used.
Notify ban activity	Review this value in relation to the object being configured and the tenant or system scope where it is used.
Notify address	Review this value in relation to the object being configured and the tenant or system scope where it is used.
Notify sender address	Review this value in relation to the object being configured and the tenant or system scope where it is used.
Whitelisted IPs	Review this value in relation to the object being configured and the tenant or system scope where it is used.

Field or block	Purpose
Autowhitelist from Tenants IP Restrictions	Review this value in relation to the object being configured and the tenant or system scope where it is used.
Autowhitelist from Tenants IP Registration	Review this value in relation to the object being configured and the tenant or system scope where it is used.
Allow SIP connections from only Allowed IP	Review this value in relation to the object being configured and the tenant or system scope where it is used.
Block known SIP scanners - Edit	Review this value in relation to the object being configured and the tenant or system scope where it is used.
SIP Scanners	Review this value in relation to the object being configured and the tenant or system scope where it is used.
Blocked IPs	Review this value in relation to the object being configured and the tenant or system scope where it is used.

Revision #3
Created 2026-06-02 21:57:13 UTC by Admin
Updated 2026-06-04 10:29:09 UTC by Admin