sipPROT 5.4

Fireline Communications Security Protection

sipPROT is Fireline Communications’ advanced SIP security module designed to protect your PBX systems from brute-force attacks, unauthorized SIP registration attempts, SIP INVITE floods, and geographically targeted intrusion attempts. It provides automated firewall rule updates, dynamic blocking, permanent
denylisting, GEO IP filtering, and detailed attack visibility.

Why sipPROT Is Critical

Brute-force SIP attacks are common and can lead to:

- PBX downtime or unreachability
- Unauthorized SIP registration attempts
- Financial loss due to fraudulent call activity

sipPROT actively monitors SIP traffic and blocks malicious IP addresses in real time, providing a security layer specifically optimized for VoIP environments.

How sipPROT Works

When sipPROT detects suspicious SIP activity, it immediately updates firewall rules to block the attacking IP address.

Unlike generic intrusion-prevention systems, sipPROT analyzes live SIP traffic and reacts instantly.

sipPROT also includes GEO IP protection. Incoming IP addresses are compared against a GEO database,and traffic from blocked countries is automatically denied.

Important Note Before Deleting Extensions

Before removing an extension from your PBX, always factory-reset the phone registered to that extension. Failure to do so may cause repeated failed SIP REGISTER attempts, triggering sipPROT blocks and email alerts.

Accessing sipPROT from Business or Contact Center Systems

- **PBX Admin Portal:** Admin Settings → sipPROT → Settings

---

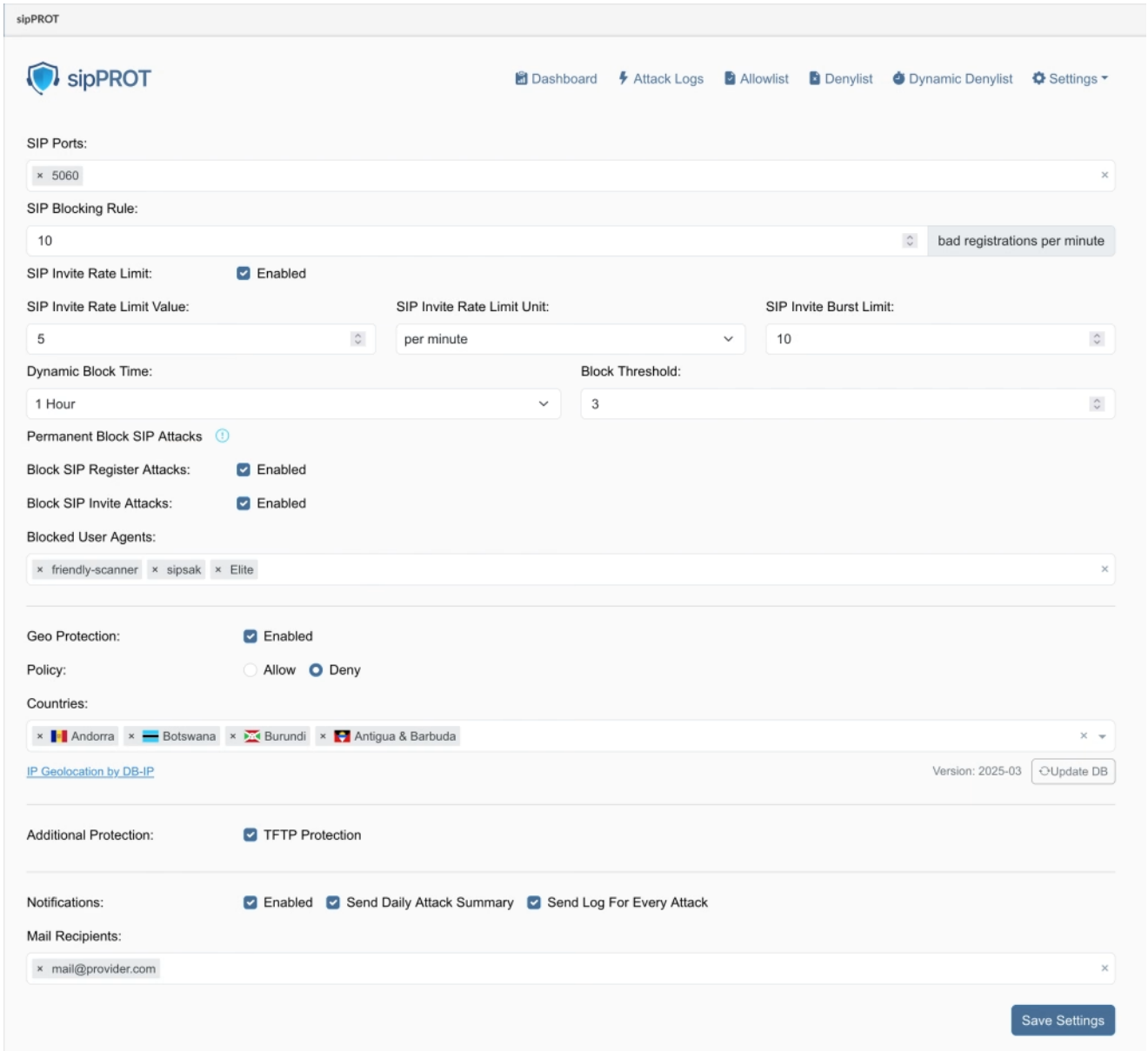
sipPROT Dashboard Overview

The dashboard provides real-time visibility into system security:

- **Health Status** – Indicates whether sipPROT is running properly.
- **Attacks Per Endpoint** – Shows targeted IPs or PBX instances.

- **Most Blocked Countries** – Displays geographic origin of blocked IPs.
- **Heatmap** – Visual representation of attack density by region.

All widgets support date filtering and auto-refresh intervals.



sipPROT Settings

Firewall Configuration

- **SIP Ports** – Define monitored SIP ports (e.g., 5060 or 5060–5062).
- **SIP Blocking Rule** – Maximum unauthorized registrations per minute.
- **Dynamic Block Time** – Duration of temporary blocks.
- **Block Threshold** – Number of dynamic blocks before permanent denylisting.
- **Blocked User Agents** – List of SIP user agents to reject.

GEO Protection

- **Allow Mode** – Only selected countries are permitted.
- **Deny Mode** – Selected countries are blocked entirely.

SIP INVITE Rate Limiting

- **Rate Limit** – Max INVITEs per minute before blocking.
- **Burst Limit** – Allowed initial burst of INVITEs.

Permanent Blocking

- **Register Attack Blocking** – Permanently blocks repeated SIP REGISTER attacks.
- **Invite Attack Blocking** – Permanently blocks repeated SIP INVITE attacks.

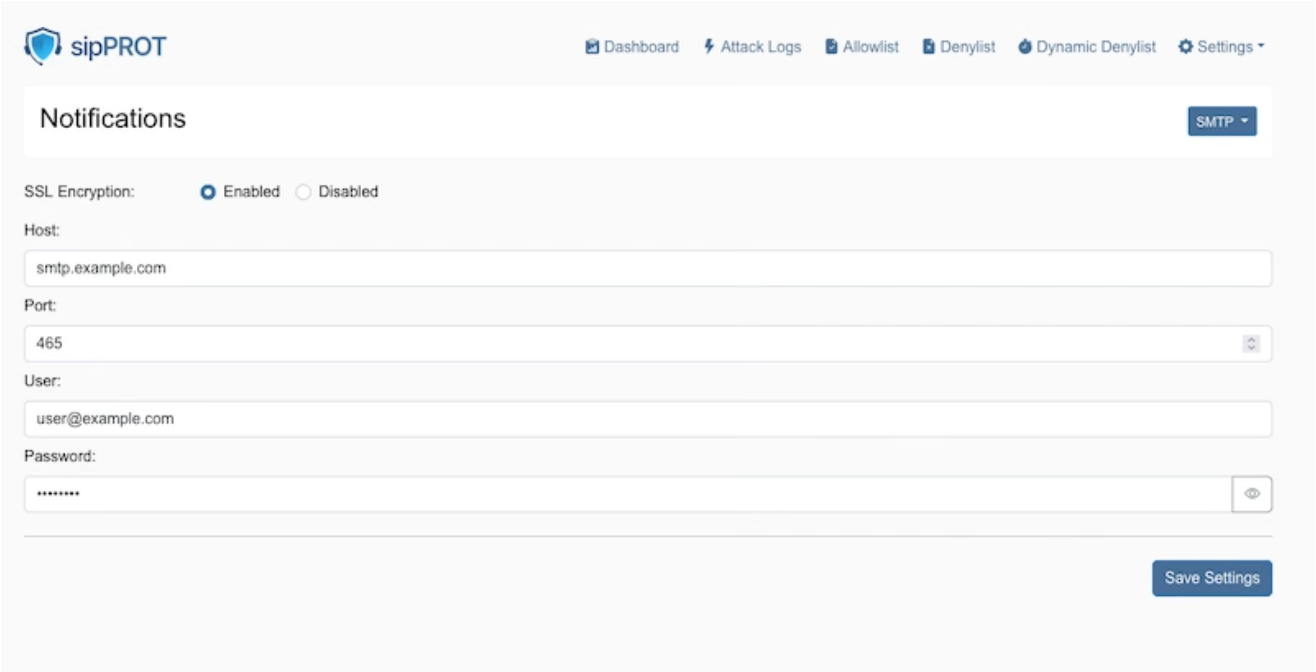
Additional Protections

- **TFTP Protection** – Rate-limits TFTP brute-force attempts.
- **DNS Protection** – Protects older systems from DNS resolver vulnerabilities.

Notifications

- **Daily Attack Summary**
- **Per-Attack Notifications**
- **Multiple Email Recipients**

SMTP settings must be configured correctly for notifications to function.

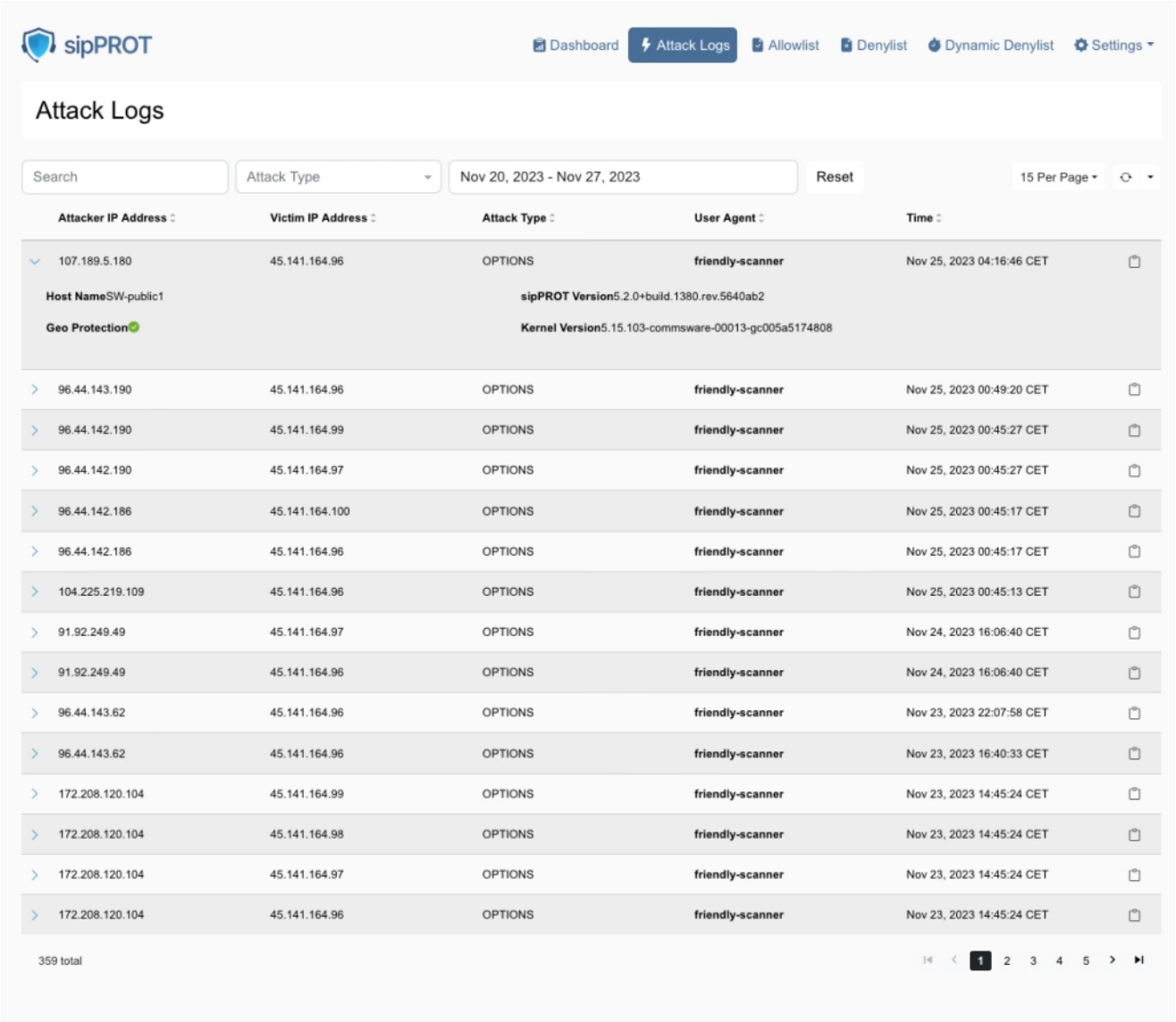


Attack Logs

The Attack Logs page displays:

- Attacker IP
- Victim IP
- Attack Type (REGISTER or OPTIONS)
- User Agent
- Timestamp

Logs can be filtered, searched, paginated, and inspected for detailed information.

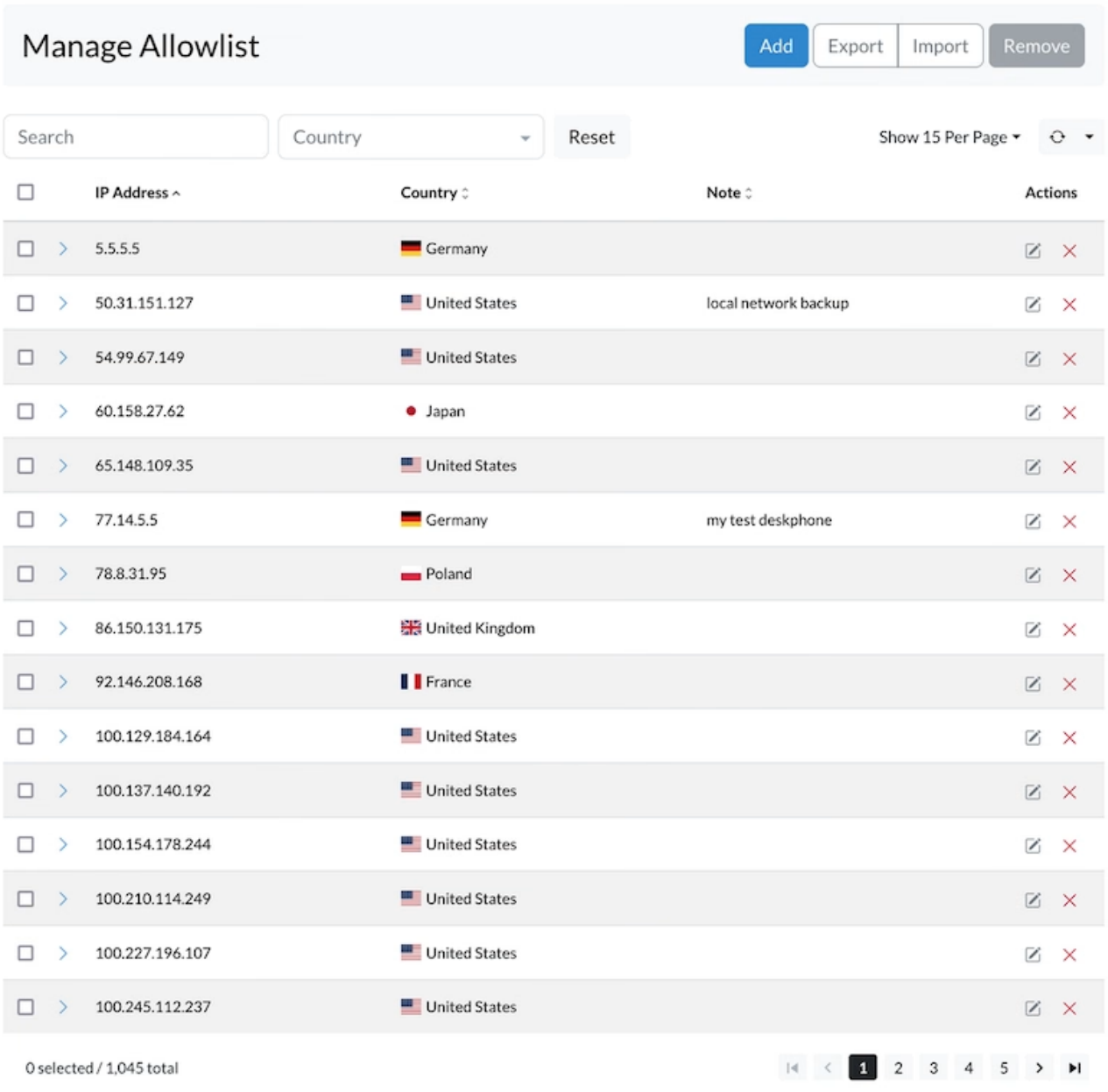


Allow & Deny Lists

Allowlist

IP addresses in the allowlist always bypass sipPROT blocking.

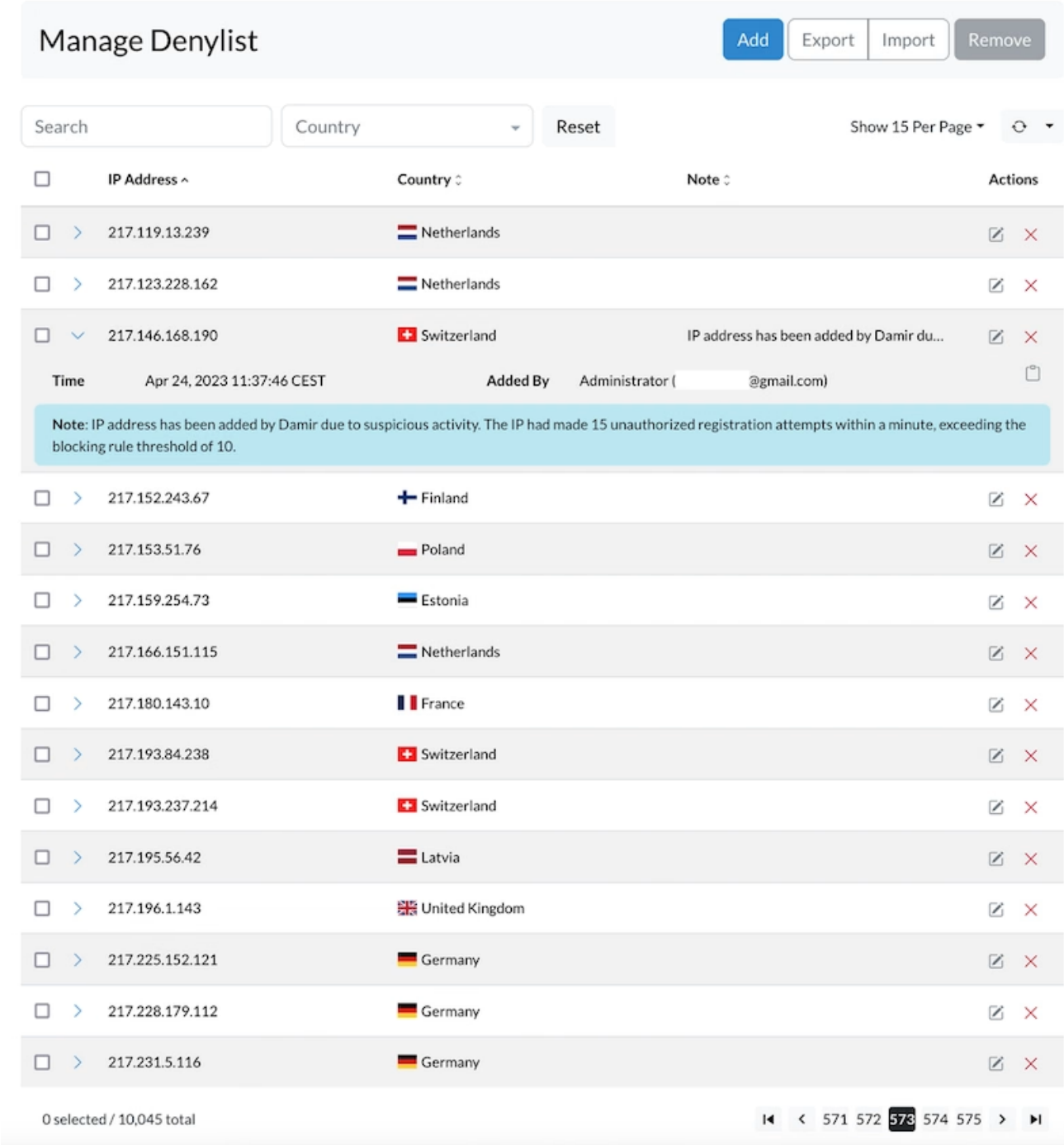
- Add single IPs
- Import/export CSV
- Bulk delete
- Country-based search



Denylist

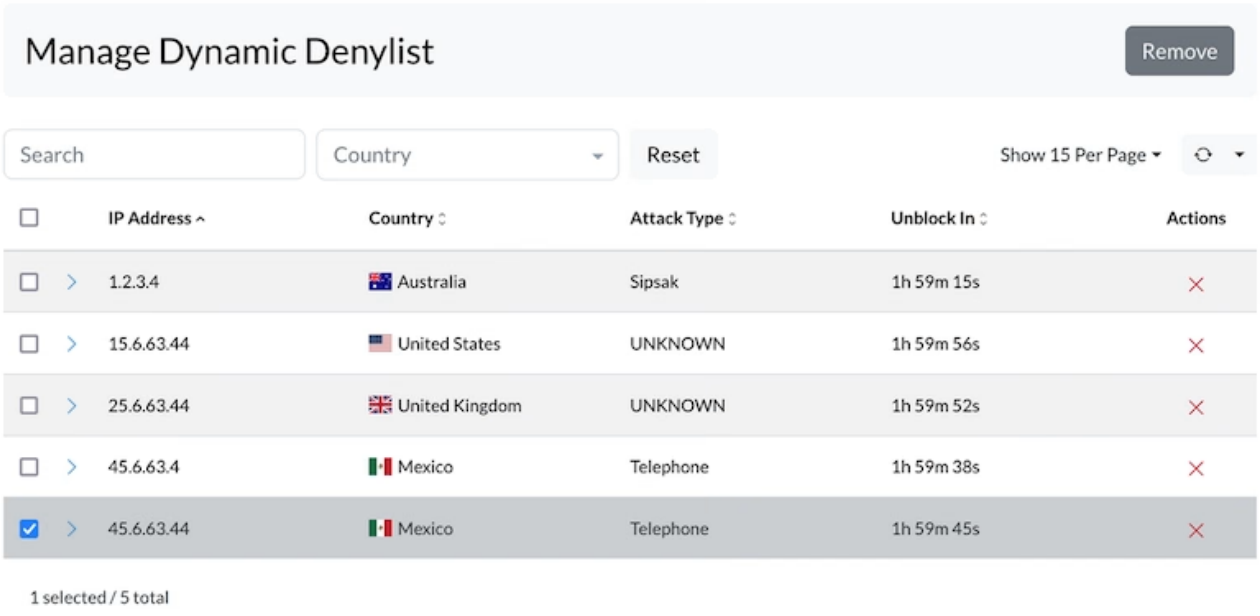
IP addresses in the denylist are permanently blocked unless also present in the allowlist.

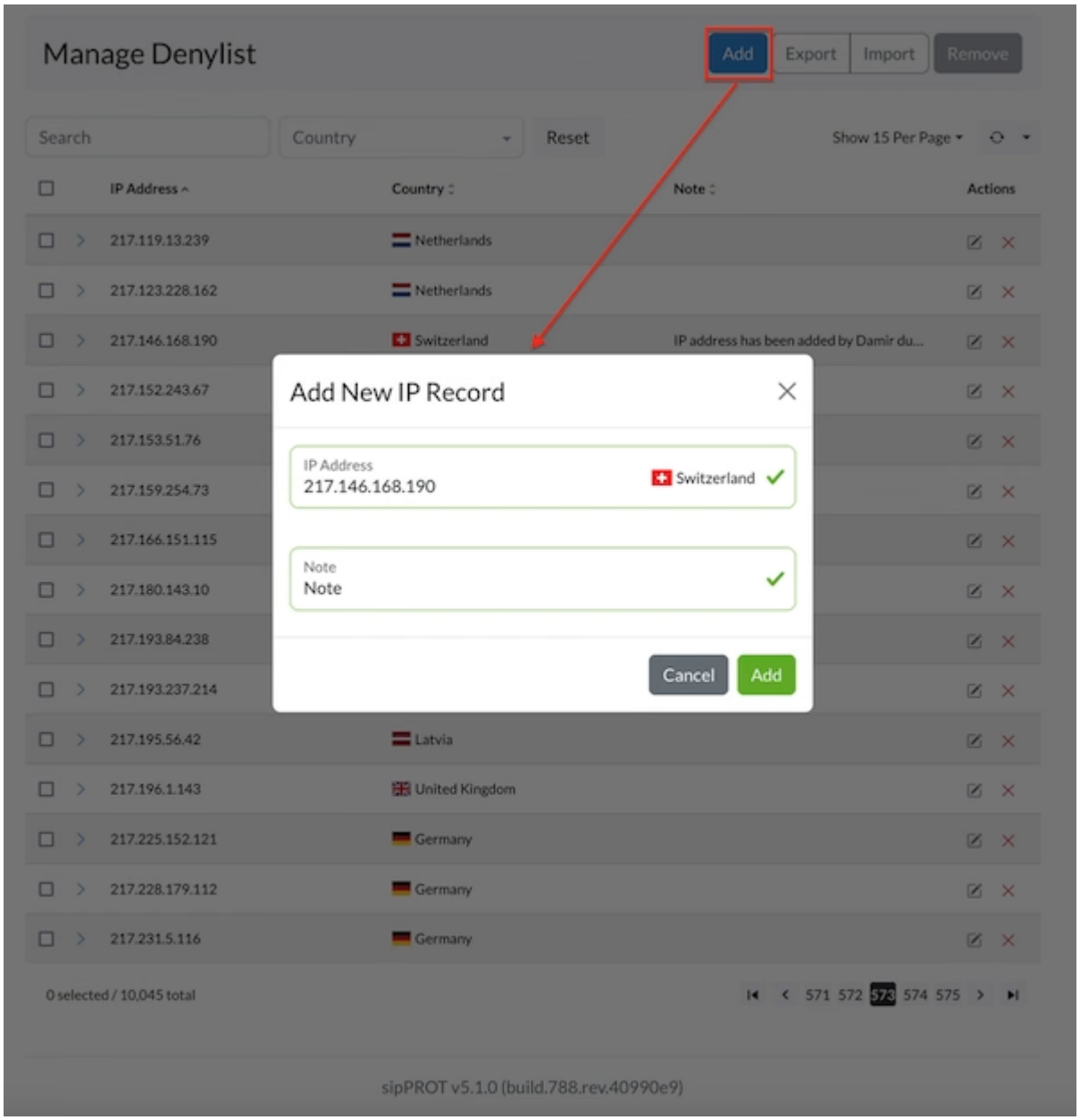
- Manual add
- CSV import/export
- Bulk removal



Dynamic Denylist

Automatically populated with IPs that violate sipPROT rules.
Temporary blocks reset if attacks continue,
and repeated offenders become permanently blocked.

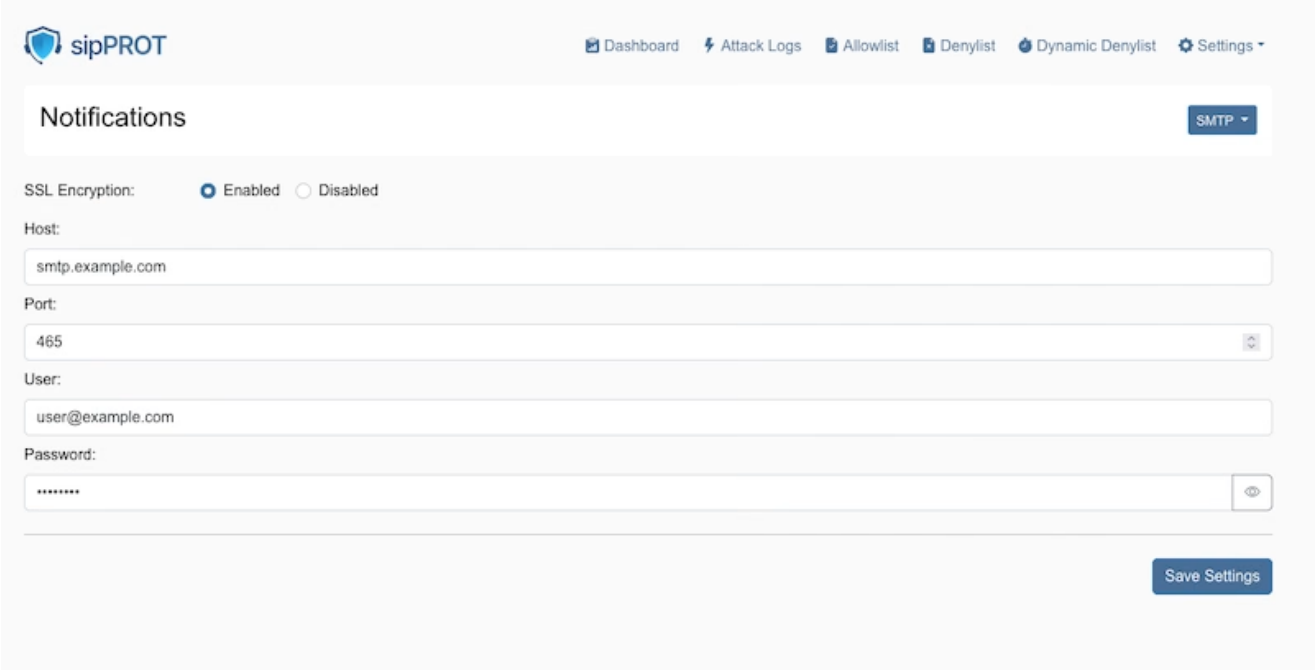



Manage Denylist
Add
Export
Import
Remove
Search
Country
Reset
Show 15 Per Page
IP Address
Country
Note
Actions
217.119.13.239
Netherlands
217.123.228.162
Netherlands
217.146.168.190
Switzerland
IP address has been added by Damir du...
217.152.243.67
217.153.51.76
217.159.254.73
217.166.151.115
217.180.143.10
217.193.84.238
217.193.237.214
217.195.56.42
Latvia
217.196.1.143
United Kingdom
217.225.152.121
Germany
217.228.179.112
Germany
217.231.5.116
Germany
Add New IP Record
IP Address
217.146.168.190
Switzerland
Note
Note
Cancel
Add
0 selected / 10,045 total
571 572 573 574 575
sipPROT v5.1.0 (build.788.rev.40990e9)

Notifications & SMTP Configuration

Configure secure email delivery using SSL/TLS:

- SMTP host
- Port
- Username
- Password



---

sipPROT CLI

sipPROT includes a command-line interface with autocomplete support.

```
sipprot status
sipprot version
sipprot list
sipprot settings
```

Use flags such as --allow, --deny, --dynamic for detailed list output.

Summary

sipPROT is a critical security component for Fireline Communications PBX deployments, providing real-time SIP attack protection, GEO filtering, dynamic blocking, permanent denylisting, and comprehensive monitoring tools.