RELEASE NOTES

SERVERware 4.6

bicom
SYSTEMS

wiki.bicomsystems.com

Table of Contents

sipPROT

sipPROT in SERVERware 4.6 comes with a complete makeover, including various enhancements, a faster in-memory database and an updated user interface aimed at boosting the overall functionality and user experience of sipPROT.

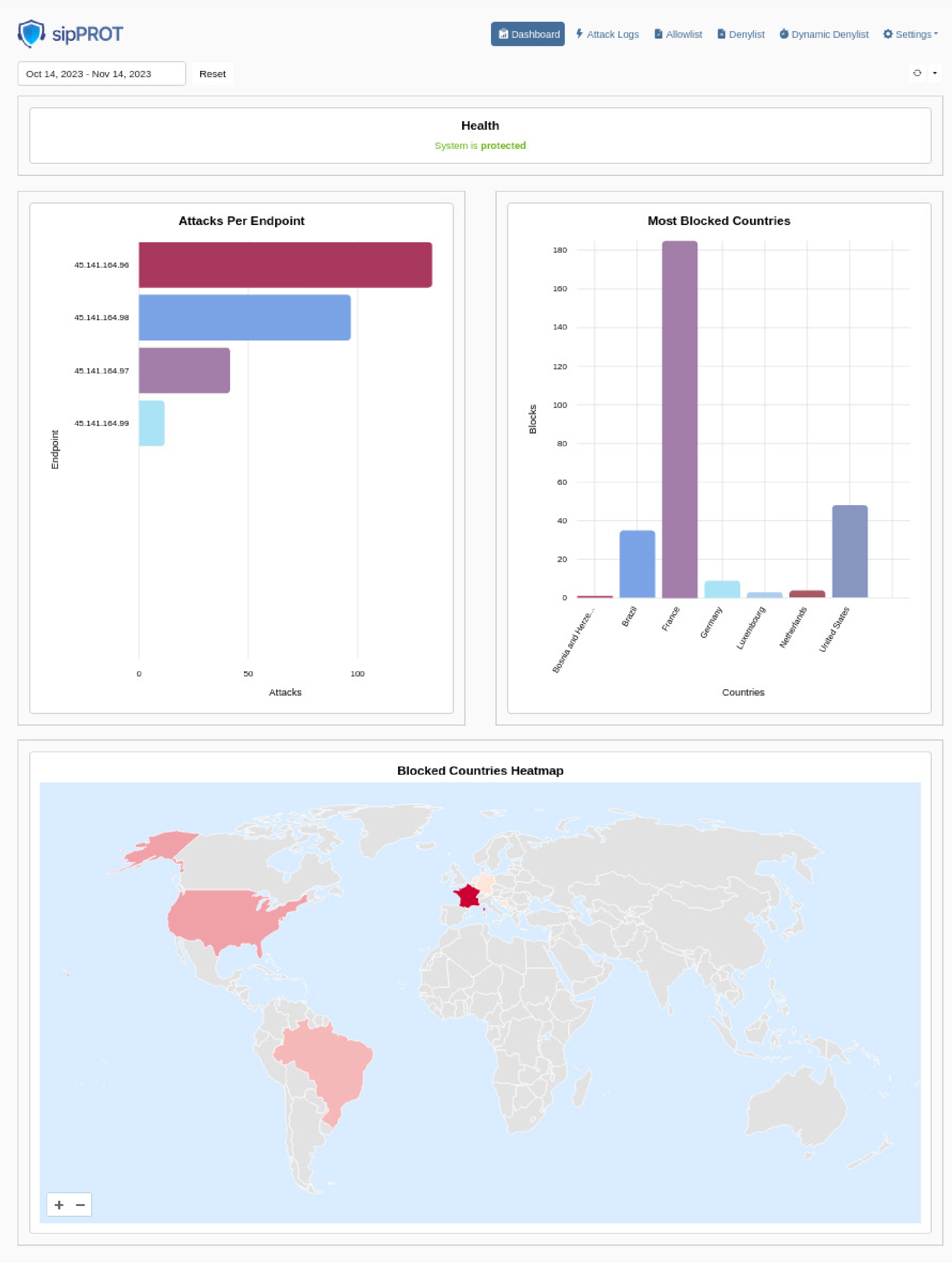
sipPROT Dashboard

The sipPROT Dashboard was added to provide a clear overview of blocked attacks, Geo-IP data and overall health status of the firewall.

The attacks per endpoint chart shows the number of attacks for each VPS on the system, or rather, their IPs that were under attack. Hovering on each bar will display the number of attacks which helps administrators see which VPS is most susceptible to them.

The Most Blocked Countries chart shows the number of IPs that were blocked from each country so that administrators can use the data to adjust geo-ip protection policies accordingly.

The Blocked Countries Heatmap visually illustrates the countries with the highest number of blocked IP addresses with the intensity of the color indicating the severity of IP address blocks.The darker the color, the greater the number of blocked IPs.



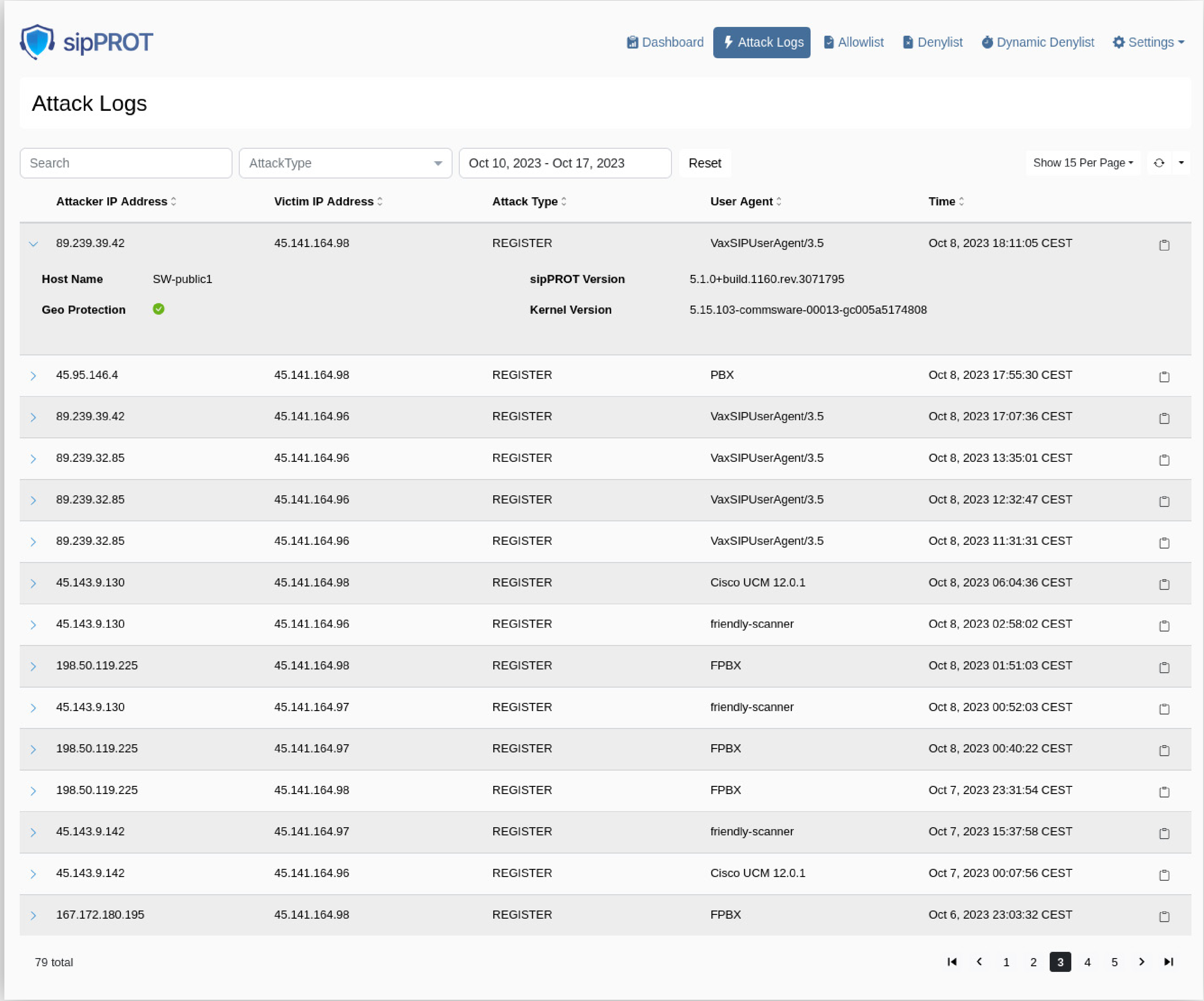
Oct 14, 2023 - Nov 14, 2023

Health

System is protected

Attack Logs

sipPROT's Attack Logs will display logs of all SIP attacks on the system with the intention to provide a better insight into the security of the entire system and allow administrators to apply additional measures if necessary.



Attack Logs

Attacker IP Address	Victim IP Address	Attack Type	User Agent	Time
89.239.39.42	45.141.164.98	REGISTER	VaxSIPUserAgent/3.5	Oct 8, 2023 18:11:05 CEST
45.95.146.4	45.141.164.98	REGISTER	PBX	Oct 8, 2023 17:55:30 CEST
89.239.39.42	45.141.164.96	REGISTER	VaxSIPUserAgent/3.5	Oct 8, 2023 17:07:36 CEST
89.239.32.85	45.141.164.96	REGISTER	VaxSIPUserAgent/3.5	Oct 8, 2023 13:35:01 CEST
89.239.32.85	45.141.164.96	REGISTER	VaxSIPUserAgent/3.5	Oct 8, 2023 12:32:47 CEST
89.239.32.85	45.141.164.96	REGISTER	VaxSIPUserAgent/3.5	Oct 8, 2023 11:31:31 CEST
45.143.9.130	45.141.164.98	REGISTER	Cisco UCM 12.0.1	Oct 8, 2023 06:04:36 CEST
45.143.9.130	45.141.164.96	REGISTER	friendly-scanner	Oct 8, 2023 02:58:02 CEST
198.50.119.225	45.141.164.98	REGISTER	FPBX	Oct 8, 2023 01:51:03 CEST
45.143.9.130	45.141.164.97	REGISTER	friendly-scanner	Oct 8, 2023 00:52:03 CEST
198.50.119.225	45.141.164.97	REGISTER	FPBX	Oct 8, 2023 00:40:22 CEST
198.50.119.225	45.141.164.98	REGISTER	FPBX	Oct 7, 2023 23:31:54 CEST
45.143.9.142	45.141.164.97	REGISTER	friendly-scanner	Oct 7, 2023 15:37:58 CEST
45.143.9.142	45.141.164.96	REGISTER	Cisco UCM 12.0.1	Oct 7, 2023 00:07:56 CEST
167.172.180.195	45.141.164.98	REGISTER	FPBX	Oct 6, 2023 23:03:32 CEST

Host Name	SW-public1	**sipPROT Version**	5.1.0+build.1160.rev.3071795
Geo Protection	✓	**Kernel Version**	5.15.103-commsware-00013-gc005a5174808

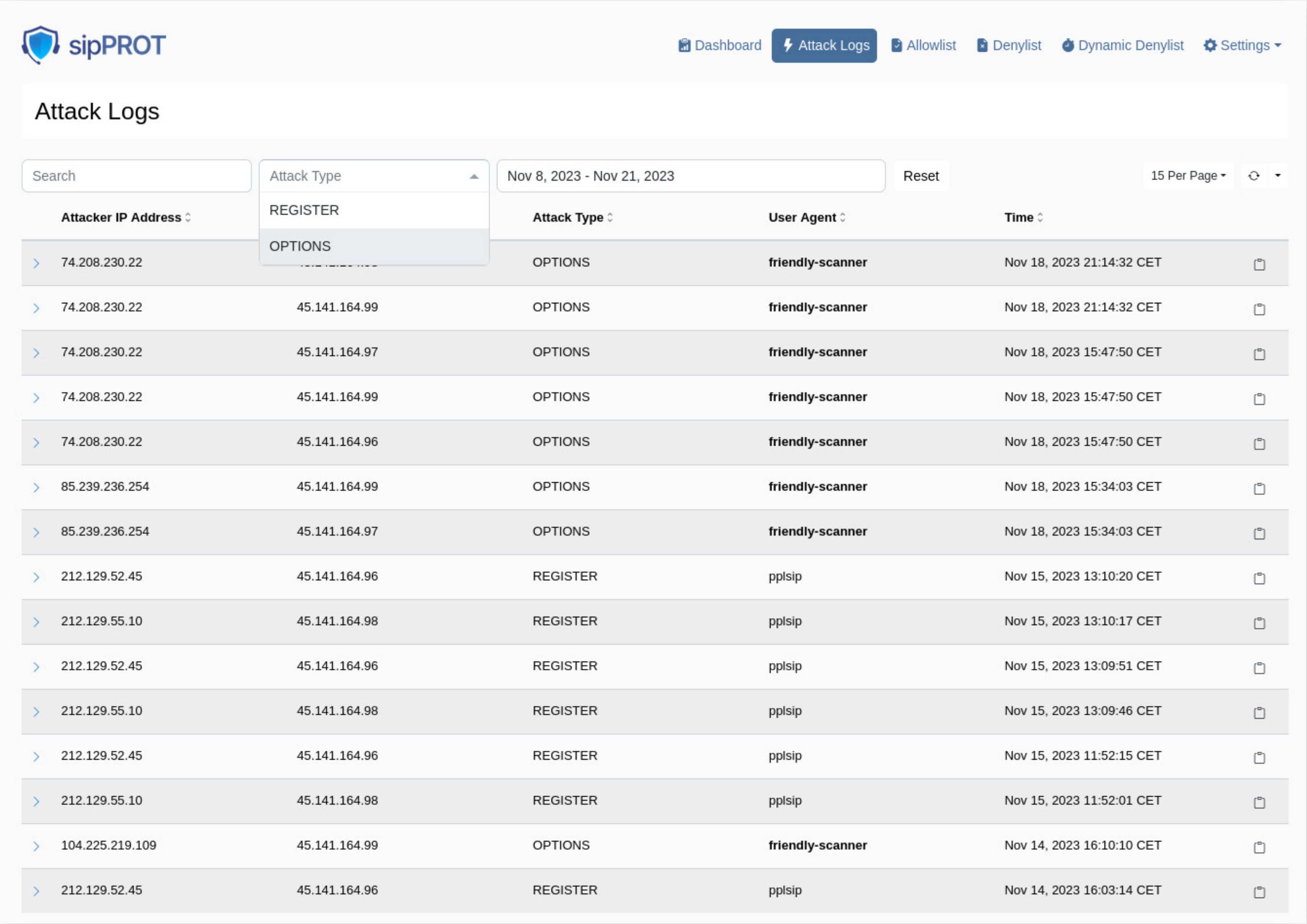
79 total

1 2 3 4 5

The logs will show the attacker's and the victim's IP addresses, the attack type, the user agent and the date and time of the attack. By clicking on the symbol in front of each log, administrators can find more information, namely on which host the attack was detected, whether Geo-IP protection is available on that host and the host's sipPROT and kernel versions.

The logs can be filtered either by utilizing the search bar or by choosing the attack type to be presented from the drop down menu next to the bar.

sipPROT's attack logs will differentiate between two types of attack, REGISTER and OPTIONS.



Attack Logs

Attacker IP Address		Attack Type	User Agent	Time
74.208.230.22	[illegible]	OPTIONS	**friendly-scanner**	Nov 18, 2023 21:14:32 CET
74.208.230.22	45.141.164.99	OPTIONS	**friendly-scanner**	Nov 18, 2023 21:14:32 CET
74.208.230.22	45.141.164.97	OPTIONS	**friendly-scanner**	Nov 18, 2023 15:47:50 CET
74.208.230.22	45.141.164.99	OPTIONS	**friendly-scanner**	Nov 18, 2023 15:47:50 CET
74.208.230.22	45.141.164.96	OPTIONS	**friendly-scanner**	Nov 18, 2023 15:47:50 CET
85.239.236.254	45.141.164.99	OPTIONS	**friendly-scanner**	Nov 18, 2023 15:34:03 CET
85.239.236.254	45.141.164.97	OPTIONS	**friendly-scanner**	Nov 18, 2023 15:34:03 CET
212.129.52.45	45.141.164.96	REGISTER	pplsip	Nov 15, 2023 13:10:20 CET
212.129.55.10	45.141.164.98	REGISTER	pplsip	Nov 15, 2023 13:10:17 CET
212.129.52.45	45.141.164.96	REGISTER	pplsip	Nov 15, 2023 13:09:51 CET
212.129.55.10	45.141.164.98	REGISTER	pplsip	Nov 15, 2023 13:09:46 CET
212.129.52.45	45.141.164.96	REGISTER	pplsip	Nov 15, 2023 11:52:15 CET
212.129.55.10	45.141.164.98	REGISTER	pplsip	Nov 15, 2023 11:52:01 CET
104.225.219.109	45.141.164.99	OPTIONS	**friendly-scanner**	Nov 14, 2023 16:10:10 CET
212.129.52.45	45.141.164.96	REGISTER	pplsip	Nov 14, 2023 16:03:14 CET

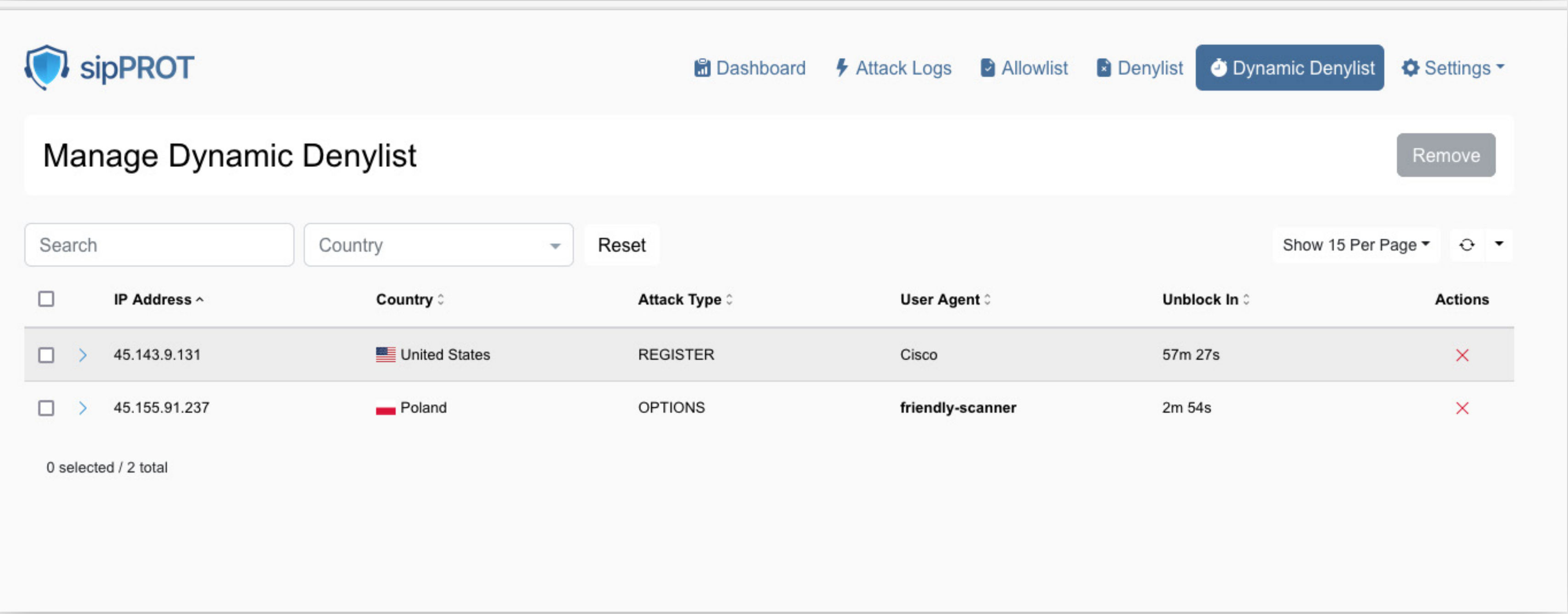
Known user agents will be singled out in bold letters on the logs. Logs are kept for three months.

IP Addresses Lists - Improved Dynamic Denylist

The dynamic denylist functionality has been further enhanced so that when an address is dynamically blocked on one host, that information is shared among all hosts within the cluster.

Addresses that end up permanently blocked through the dynamic denylist functionality (by exceeding the block threshold) will appear in the denylist.

The dynamic denylist has been further enhanced so it shows the user agent device of the blocked address. If it's a known user agent device, it will appear in bold letters.



Manage Dynamic Denylist

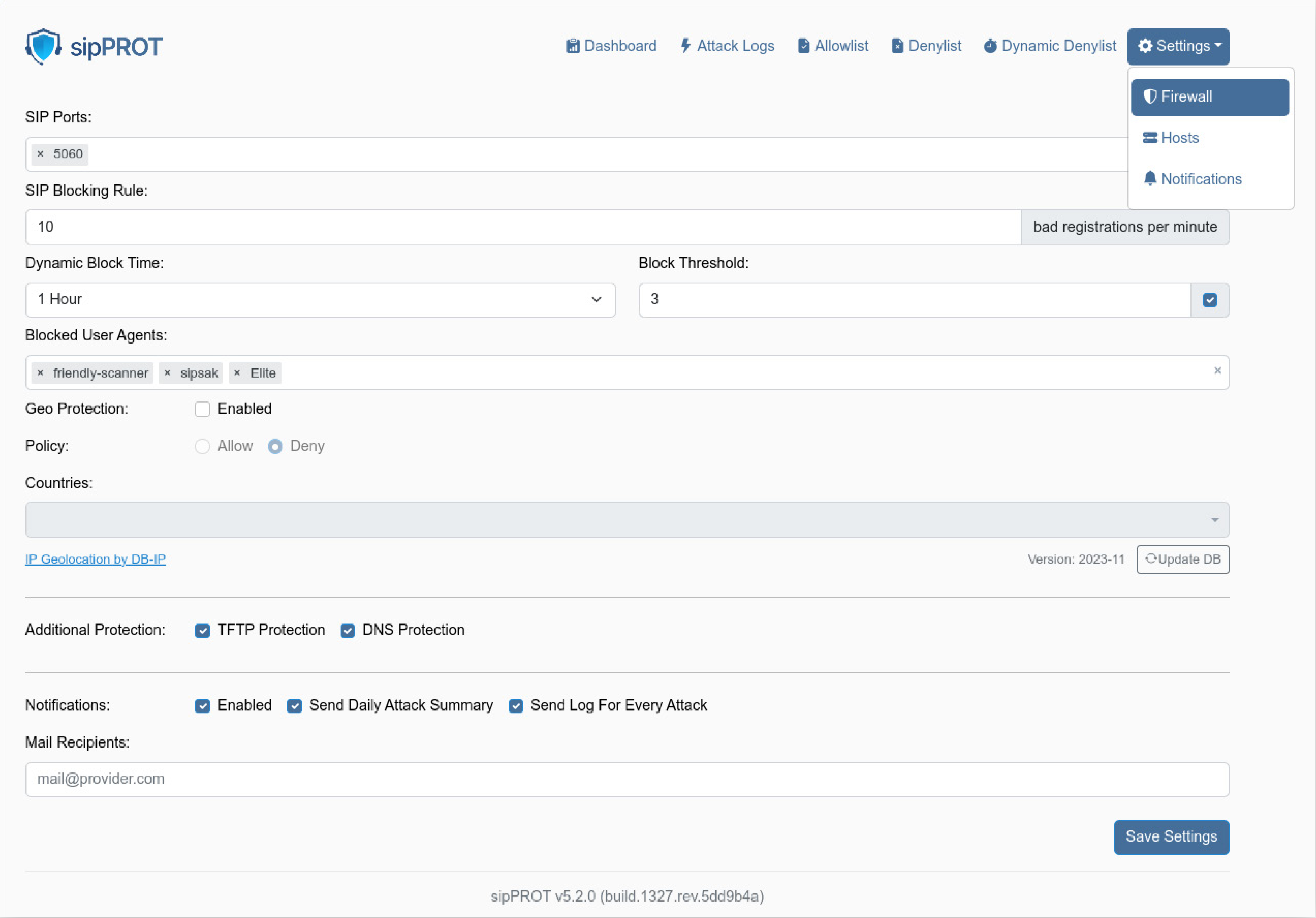
□	IP Address	Country	Attack Type	User Agent	Unblock In	Actions
□	45.143.9.131	United States	REGISTER	Cisco	57m 27s	✕
□	45.155.91.237	Poland	OPTIONS	**friendly-scanner**	2m 54s	✕

0 selected / 2 total

Settings

General sipPROT settings can be found under Settings → Firewall.

The Host menu provides sipPROT with information for each host in the cluster. Administrators will be able to monitor the health of sipPROT and the Geo-IP service on each host. They will be able to exclude a host from sipPROT with a single click.



SIP Ports: × 5060

SIP Blocking Rule: 10 bad registrations per minute

Dynamic Block Time: 1 Hour

Block Threshold: 3 ☑

Blocked User Agents: × friendly-scanner × sipsak × Elite

Geo Protection: □ Enabled

Policy: ○ Allow ● Deny

Countries:

IP Geolocation by DB-IP

Version: 2023-11

Additional Protection: ☑ TFTP Protection ☑ DNS Protection

Notifications: ☑ Enabled ☑ Send Daily Attack Summary ☑ Send Log For Every Attack

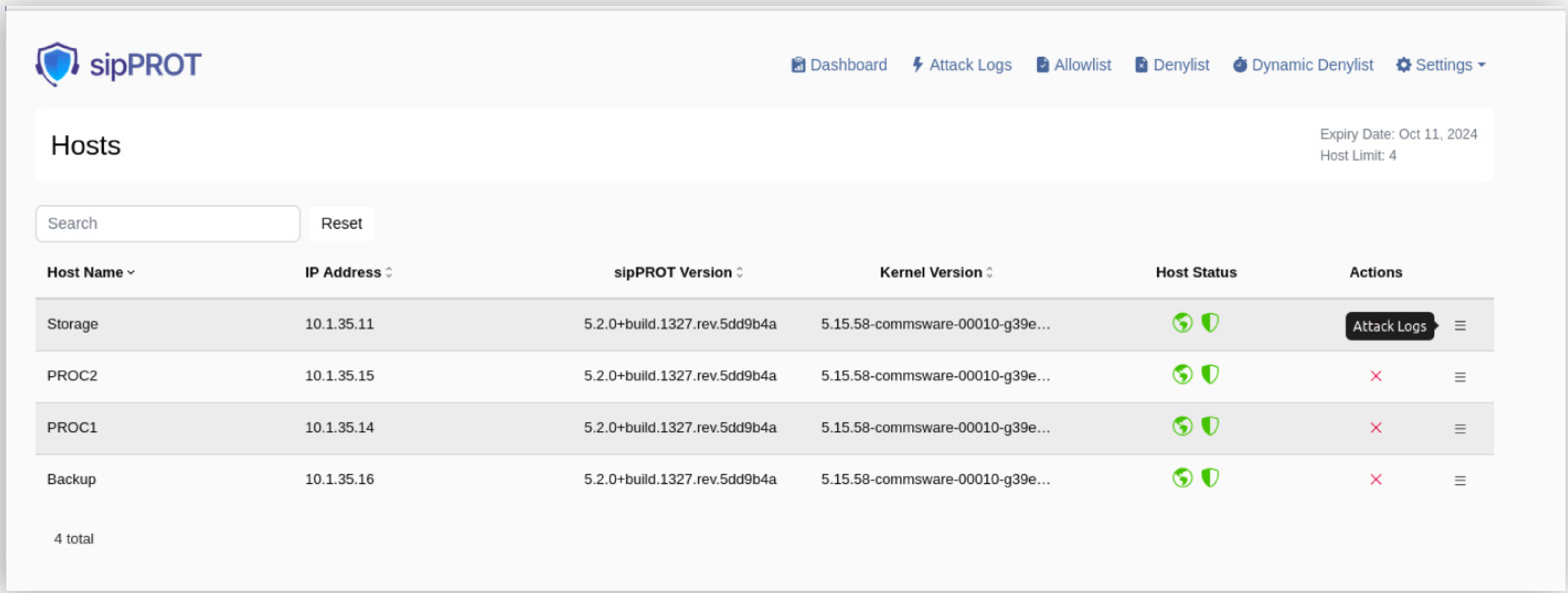
Mail Recipients: mail@provider.com

sipPROT v5.2.0 (build.1327.rev.5dd9b4a)

Hosts

sipPROT's Hosts page will provide general information on which hosts in the cluster sipPROT is running, the IP addresses, sipPROT and kernel versions of each host as well as whether geo protection is active on those hosts.

The Host page additionally holds license information, like the expiry date of sipPROT and the number of hosts allowed in the license.



Hosts

Expiry Date: Oct 11, 2024
Host Limit: 4

Host Name	IP Address	sipPROT Version	Kernel Version	Host Status	Actions	
Storage	10.1.35.11	5.2.0+build.1327.rev.5dd9b4a	5.15.58-commswware-00010-g39e…	🌐 🛡	Attack Logs	≡
PROC2	10.1.35.15	5.2.0+build.1327.rev.5dd9b4a	5.15.58-commswware-00010-g39e…	🌐 🛡	×	≡
PROC1	10.1.35.14	5.2.0+build.1327.rev.5dd9b4a	5.15.58-commswware-00010-g39e…	🌐 🛡	×	≡
Backup	10.1.35.16	5.2.0+build.1327.rev.5dd9b4a	5.15.58-commswware-00010-g39e…	🌐 🛡	×	≡

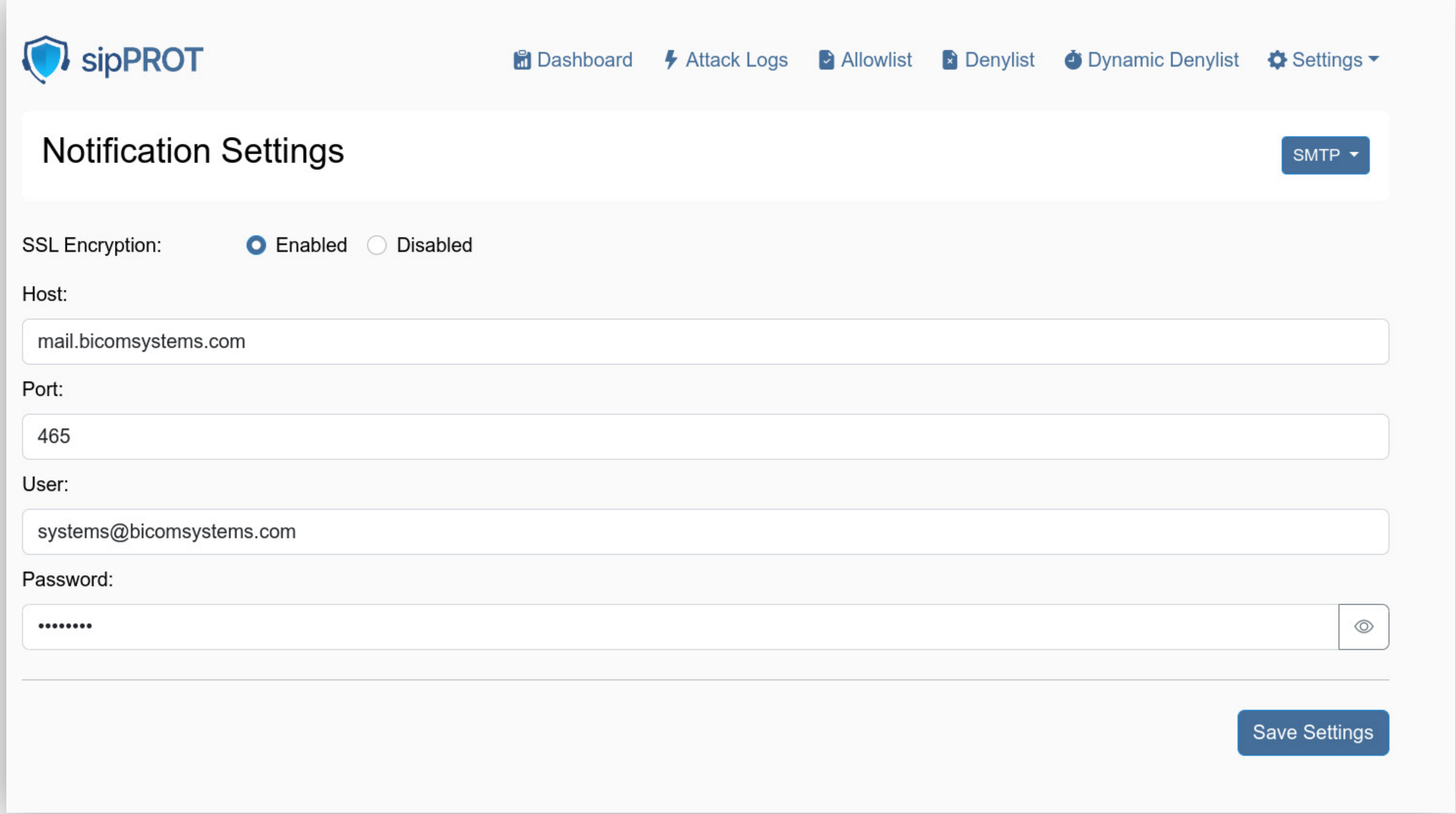
4 total

The Actions button will allow administrators to remove hosts from the list in case sipPROT is not active on those hosts. Internal services will constantly check the availability of hosts, and will mark a host inactive if there is no response within fifteen seconds.

The button on the far right will redirect to attack logs.

Notifications

sipPROT administrators will be able to configure SMTP settings for notifications sent out by sipPROT.



Notification Settings

SSL Encryption: ● Enabled ○ Disabled

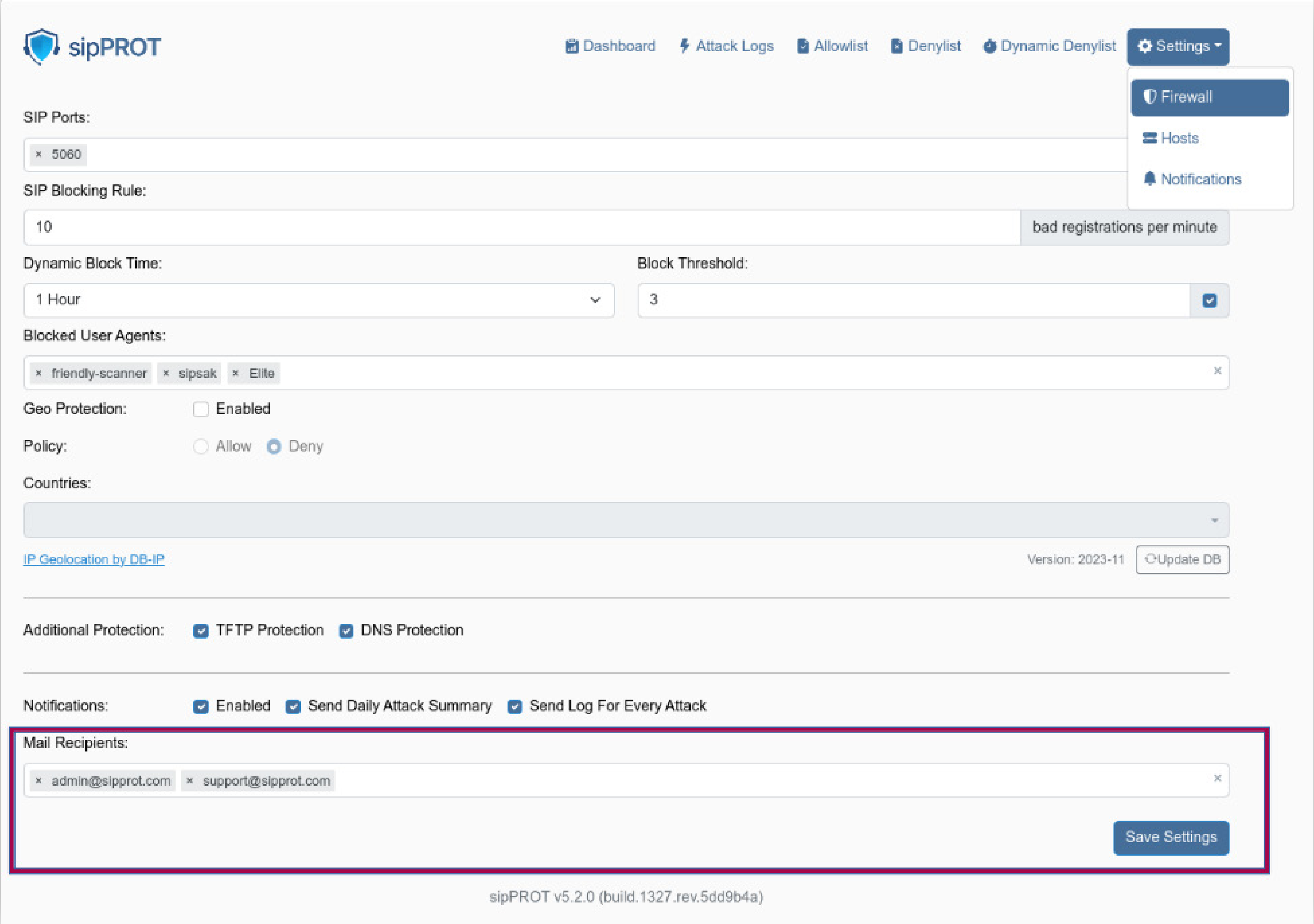
Host: mail.bicomsystems.com

Port: 465

User: systems@bicomsystems.com

Password: ••••••••

Under Firewall settings administrators can enter the email addresses of all sipPROT notification recipients.



SIP Ports: × 5060

SIP Blocking Rule: 10 bad registrations per minute

Dynamic Block Time: 1 Hour

Block Threshold: 3 ☑

Blocked User Agents: × friendly-scanner × sipsak × Elite

Geo Protection: □ Enabled

Policy: ○ Allow ● Deny

Countries:

Version: 2023-11

Additional Protection: ☑ TFTP Protection ☑ DNS Protection

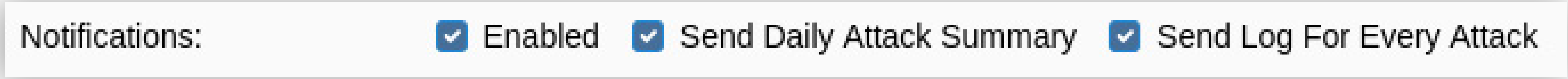
Notifications: ☑ Enabled ☑ Send Daily Attack Summary ☑ Send Log For Every Attack

Mail Recipients: × admin@sipprot.com × support@sipprot.com

sipPROT v5.2.0 (build.1327.rev.5dd9b4a)

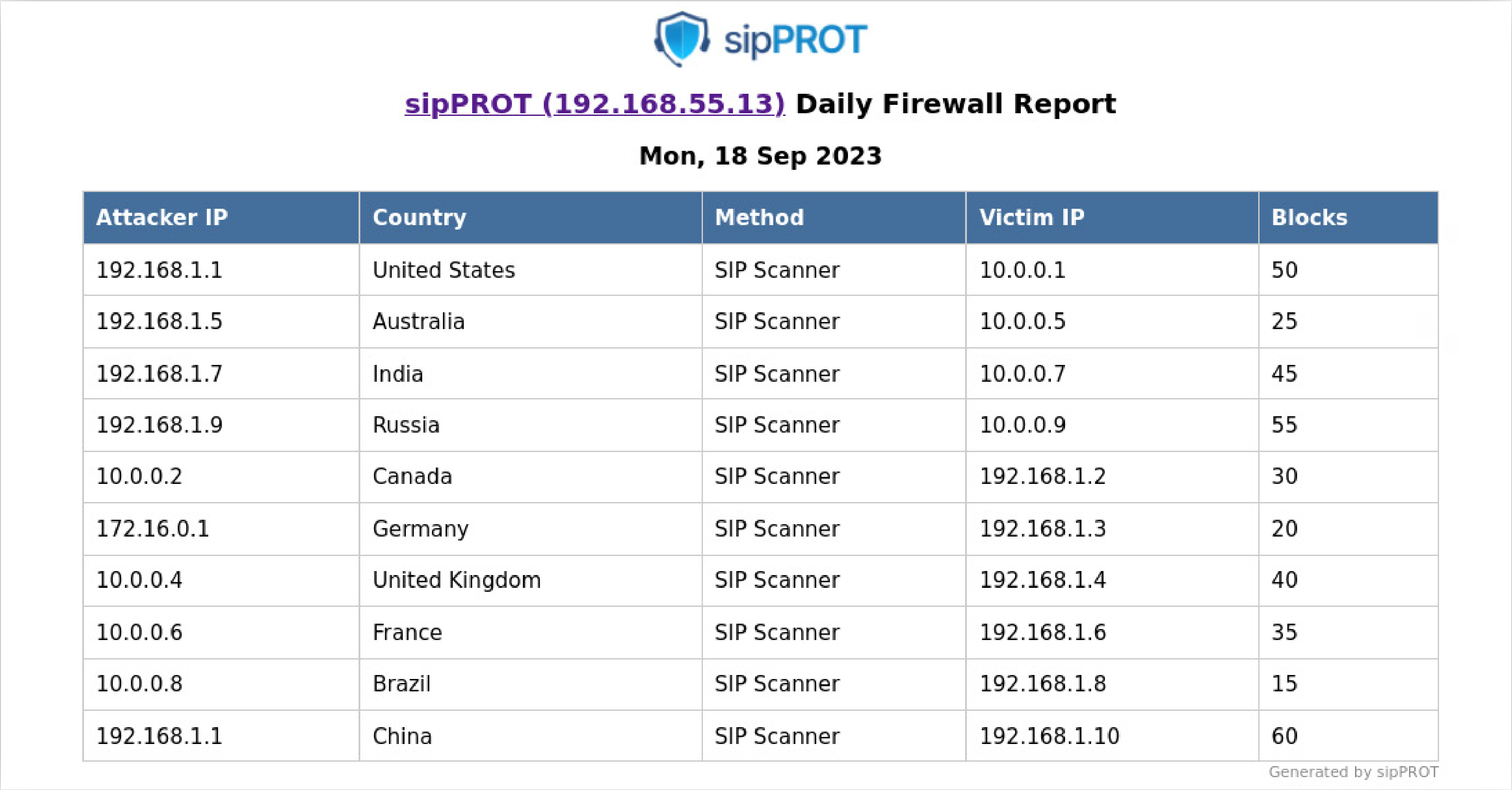
Reporting Service

Administrators can choose the type of reports they want to receive from sipPROT.



Notifications: ☑ Enabled ☑ Send Daily Attack Summary ☑ Send Log For Every Attack

The daily reports will provide a list of blocked attacks for the day along with some additional information. The administrators can navigate to the SERVERware GUI by clicking on the link in the report.



sipPROT

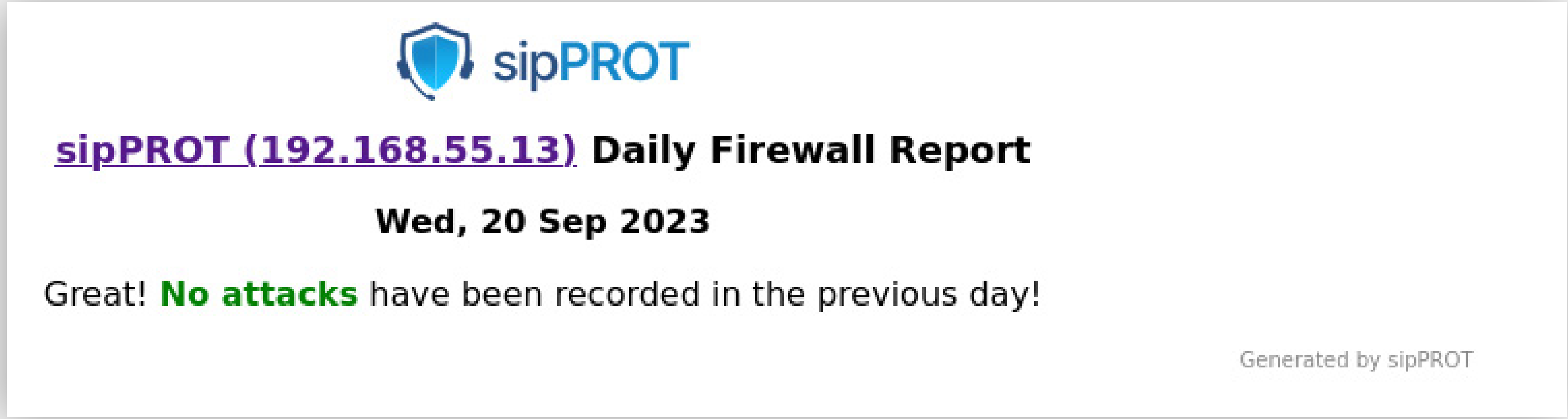
sipPROT (192.168.55.13) Daily Firewall Report

Mon, 18 Sep 2023

Attacker IP	Country	Method	Victim IP	Blocks
192.168.1.1	United States	SIP Scanner	10.0.0.1	50
192.168.1.5	Australia	SIP Scanner	10.0.0.5	25
192.168.1.7	India	SIP Scanner	10.0.0.7	45
192.168.1.9	Russia	SIP Scanner	10.0.0.9	55
10.0.0.2	Canada	SIP Scanner	192.168.1.2	30
172.16.0.1	Germany	SIP Scanner	192.168.1.3	20
10.0.0.4	United Kingdom	SIP Scanner	192.168.1.4	40
10.0.0.6	France	SIP Scanner	192.168.1.6	35
10.0.0.8	Brazil	SIP Scanner	192.168.1.8	15
192.168.1.1	China	SIP Scanner	192.168.1.10	60

Generated by sipPROT

In case no attacks occurred that day, a notification like the one below will be sent out.



sipPROT

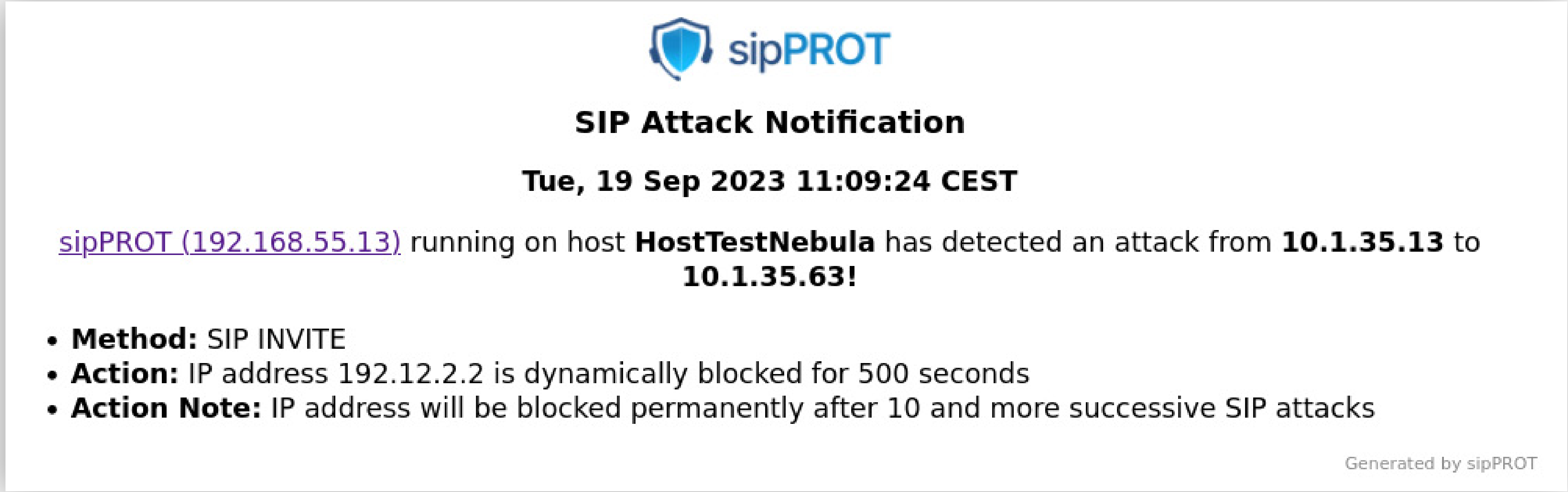
sipPROT (192.168.55.13) Daily Firewall Report

Wed, 20 Sep 2023

Great! **No attacks** have been recorded in the previous day!

Generated by sipPROT

In the event of an ongoing attack on the system, sipPROT will notify the administrators immediately together with the attacker's and the victim's IP addresses, method of attack, as well as what actions were taken.



SIP Attack Notification

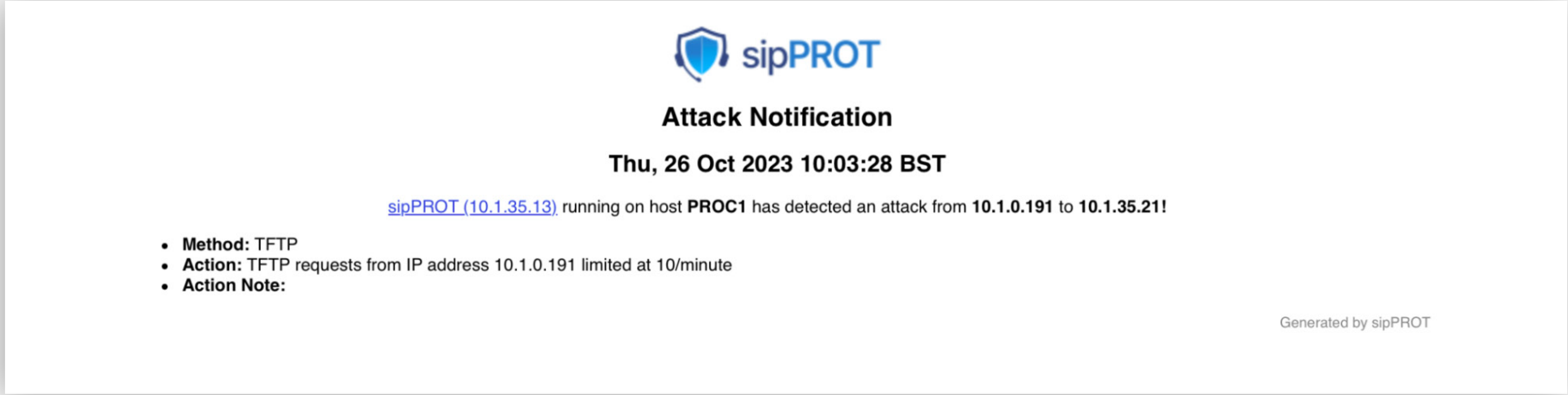
Tue, 19 Sep 2023 11:09:24 CEST

sipPROT (192.168.55.13) running on host **HostTestNebula** has detected an attack from **10.1.35.13** to **10.1.35.63!**

- **Method:** SIP INVITE
- **Action:** IP address 192.12.2.2 is dynamically blocked for 500 seconds
- **Action Note:** IP address will be blocked permanently after 10 and more successive SIP attacks

Generated by sipPROT

TFTP attacks will also prompt an email notification from sipPROT.



Attack Notification

Thu, 26 Oct 2023 10:03:28 BST

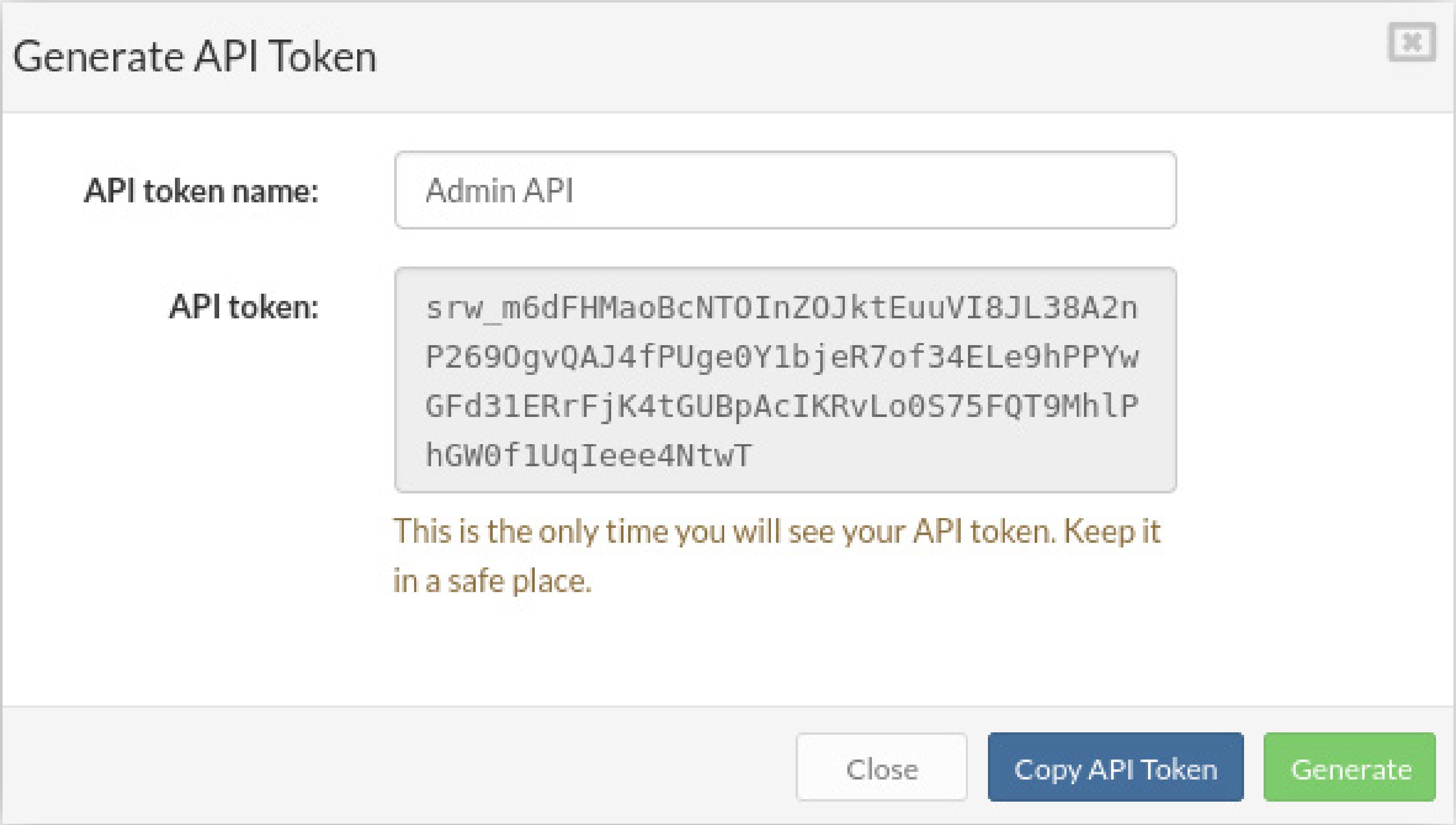
sipPROT (10.1.35.13) running on host **PROC1** has detected an attack from **10.1.0.191** to **10.1.35.21!**

- **Method:** TFTP
- **Action:** TFTP requests from IP address 10.1.0.191 limited at 10/minute
- **Action Note:**

Generated by sipPROT

API Token Implementation

Users in SERVERware can now create API tokens that are tied to their user and will have all the user's permissions. Each user can create a maximum of 10 tokens. As a security measure, the token will only be visible upon creation.



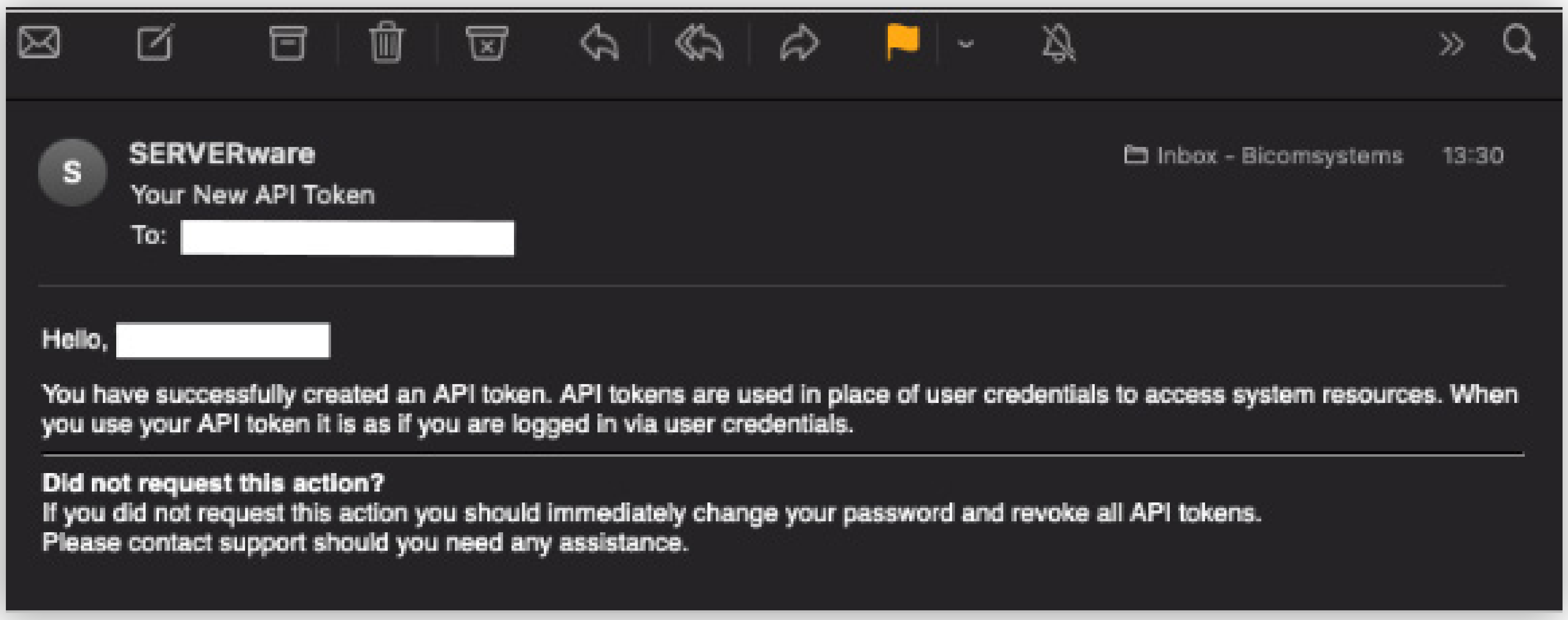
API token name: Admin API

API token:

```
srw_m6dFHMaoBcNTOInZOJktEuuVI8JL38A2n
P269OgvQAJ4fPUge0Y1bjeR7of34ELe9hPPYw
GFd31ERrFjK4tGUBpAcIKRvLo0S75FQT9MhlP
hGW0f1UqIeee4NtwT
```

This is the only time you will see your API token. Keep it in a safe place.

Additionally, an email notification is sent to the user who generated the token, informing them of the token along with a warning of what to do in case they were not the ones who generated the token.



SERVERware
Your New API Token
To: [redacted]

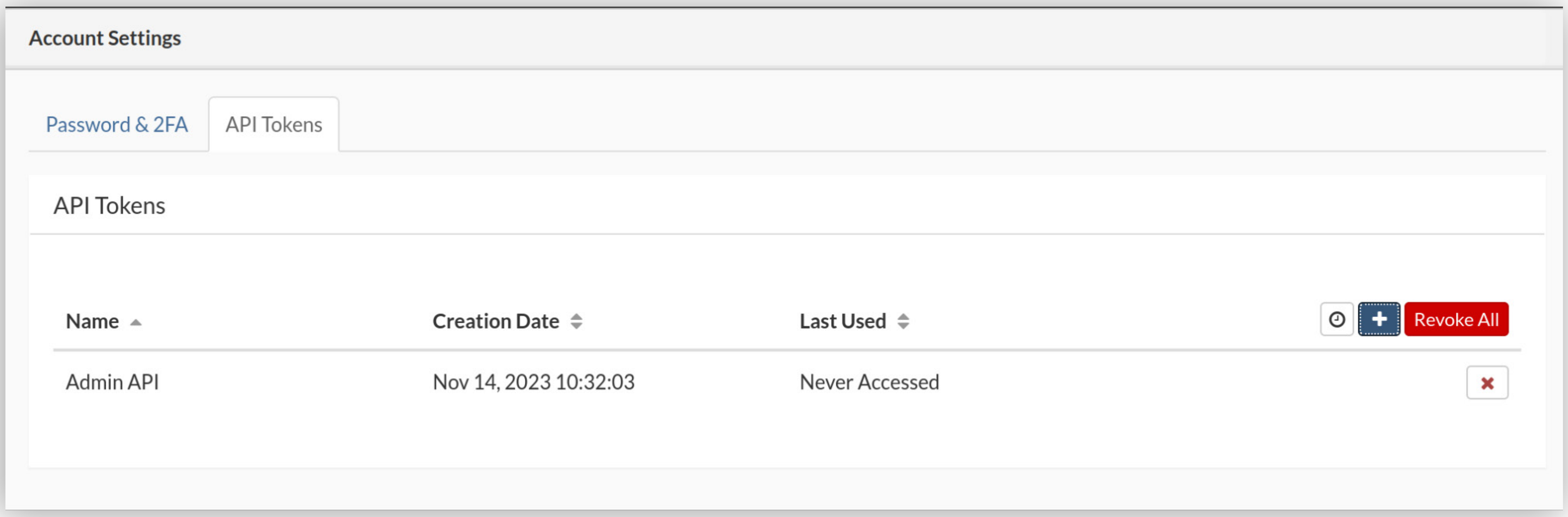
Inbox - Bicomsystems 13:30

Hello, [redacted]

You have successfully created an API token. API tokens are used in place of user credentials to access system resources. When you use your API token it is as if you are logged in via user credentials.

Did not request this action?
If you did not request this action you should immediately change your password and revoke all API tokens.
Please contact support should you need any assistance.

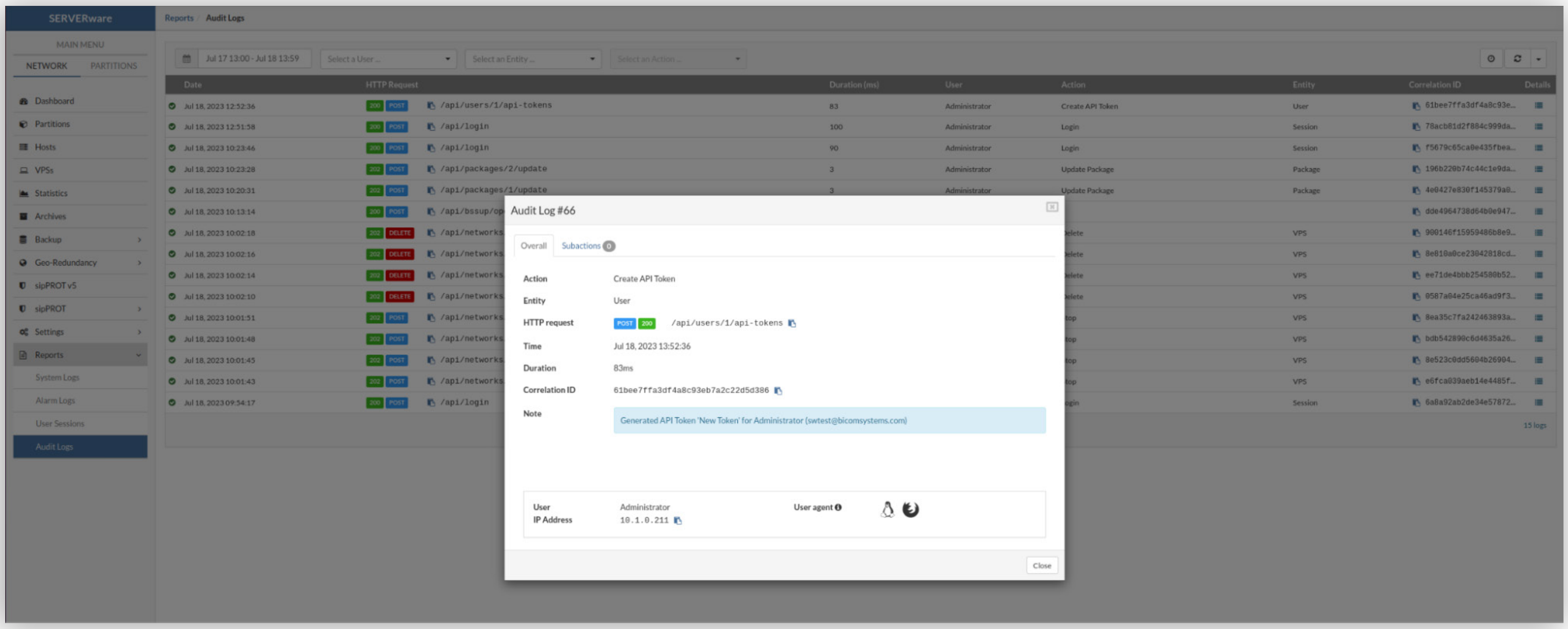
The API tokens interface shows the list of all tokens, when they were created and the last time they were used. It's possible to revoke individual tokens, or to revoke them all.



API Tokens

Name ▲	Creation Date ⬍	Last Used ⬍	
Admin API	Nov 14, 2023 10:32:03	Never Accessed	✖

Actions executed with API tokens are documented in the Audit log, mainly POST, PUT and DELETE methods with the name and email of the user to whom the token belongs.



Date	HTTP Request			Duration (ms)	User	Action	Entity	Correlation ID	Details
Jul 18, 2023 12:52:36	200	POST	/api/users/1/api-tokens	83	Administrator	Create API Token	User	61bee7ffa3df4a8c93e...	☰
Jul 18, 2023 12:51:58	200	POST	/api/login	100	Administrator	Login	Session	78acb81d2f884c999da...	☰
Jul 18, 2023 10:23:46	200	POST	/api/login	90	Administrator	Login	Session	f5679c65ca0e435fbea...	☰
Jul 18, 2023 10:23:28	202	POST	/api/packages/2/update	3	Administrator	Update Package	Package	196b220b74c44c1e9da...	☰
Jul 18, 2023 10:20:31	202	POST	/api/packages/1/update	3	Administrator	Update Package	Package	4e0427e830f145379a0...	☰
Jul 18, 2023 10:13:14	200	POST	/api/bssup/op					dde4964738d64b0e947...	☰
Jul 18, 2023 10:02:18	202	DELETE	/api/networks			elete	VPS	900146f15959486b8e9...	☰
Jul 18, 2023 10:02:16	202	DELETE	/api/networks			elete	VPS	8e810a0ce23042818cd...	☰
Jul 18, 2023 10:02:14	202	DELETE	/api/networks			elete	VPS	ee71de4bbb254580b52...	☰
Jul 18, 2023 10:02:10	202	DELETE	/api/networks			elete	VPS	0587a04e25ca46ad9f3...	☰
Jul 18, 2023 10:01:51	202	POST	/api/networks			top	VPS	8ea35c7fa242463893a...	☰
Jul 18, 2023 10:01:48	202	POST	/api/networks			top	VPS	bdb542890c6d4635a26...	☰
Jul 18, 2023 10:01:45	202	POST	/api/networks			top	VPS	8e523c0dd5604b26904...	☰
Jul 18, 2023 10:01:43	202	POST	/api/networks			top	VPS	e6fca039aeb14e4485f...	☰
Jul 18, 2023 09:54:17	200	POST	/api/login			ogin	Session	6a8a92ab2de34e57872...	☰

15 logs

Audit Log #66

Overall | Subactions 0

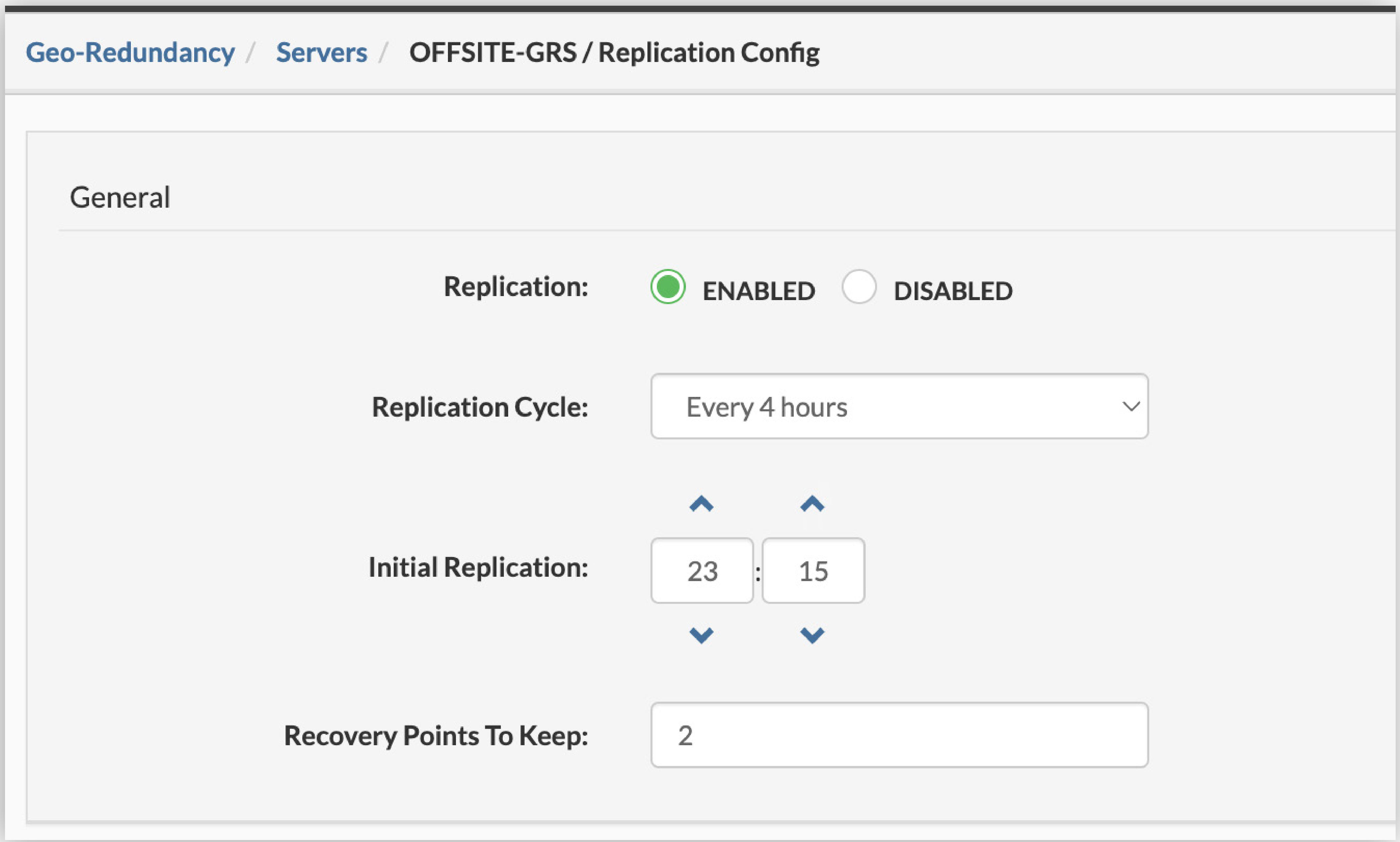
Action	Create API Token
Entity	User
HTTP request	POST 200 /api/users/1/api-tokens
Time	Jul 18, 2023 13:52:36
Duration	83ms
Correlation ID	61bee7ffa3df4a8c93eb7a2c22d5d386
Note	Generated API Token 'New Token' for Administrator (swtest@bicomsystems.com)

User	Administrator	User agent
IP Address	10.1.0.211	

Close

Set a Start Time for Replications

SERVERware administrators are now able to schedule replications on the hour. This is useful for scenarios where there are multiple replication cycles, so administrators can schedule each cycle separately to avoid unnecessary load on the network and the hosts.



Geo-Redundancy / Servers / OFFSITE-GRS / Replication Config

General

Replication: ● ENABLED ○ DISABLED

Replication Cycle: Every 4 hours

Initial Replication: 23 : 15

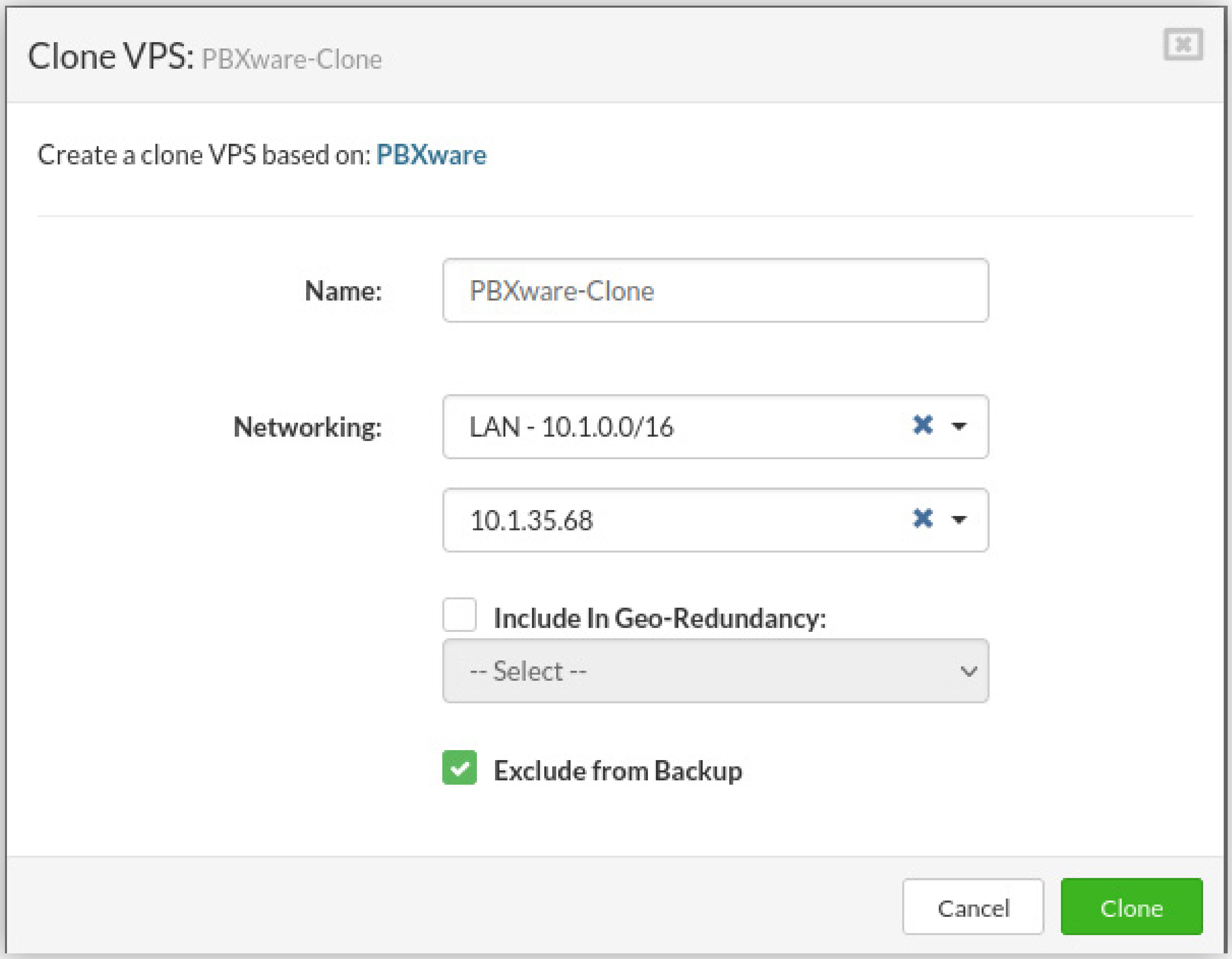
Recovery Points To Keep: 2

The Initial Replication defines the time the first scheduled replication job will start. The number of replications after that is defined by the replication cycle field.

Scheduling replications is only available for cycles from every two hours and up.

Exclude Clone from Backup in Clone VPS Popup

When cloning VPSs, administrators will be able to select whether that clone will be excluded from the next backup cycle or not, directly from the Clone VPS pop-up window.



Clone VPS: PBXware-Clone

Create a clone VPS based on: PBXware

Name: PBXware-Clone

Networking: LAN - 10.1.0.0/16

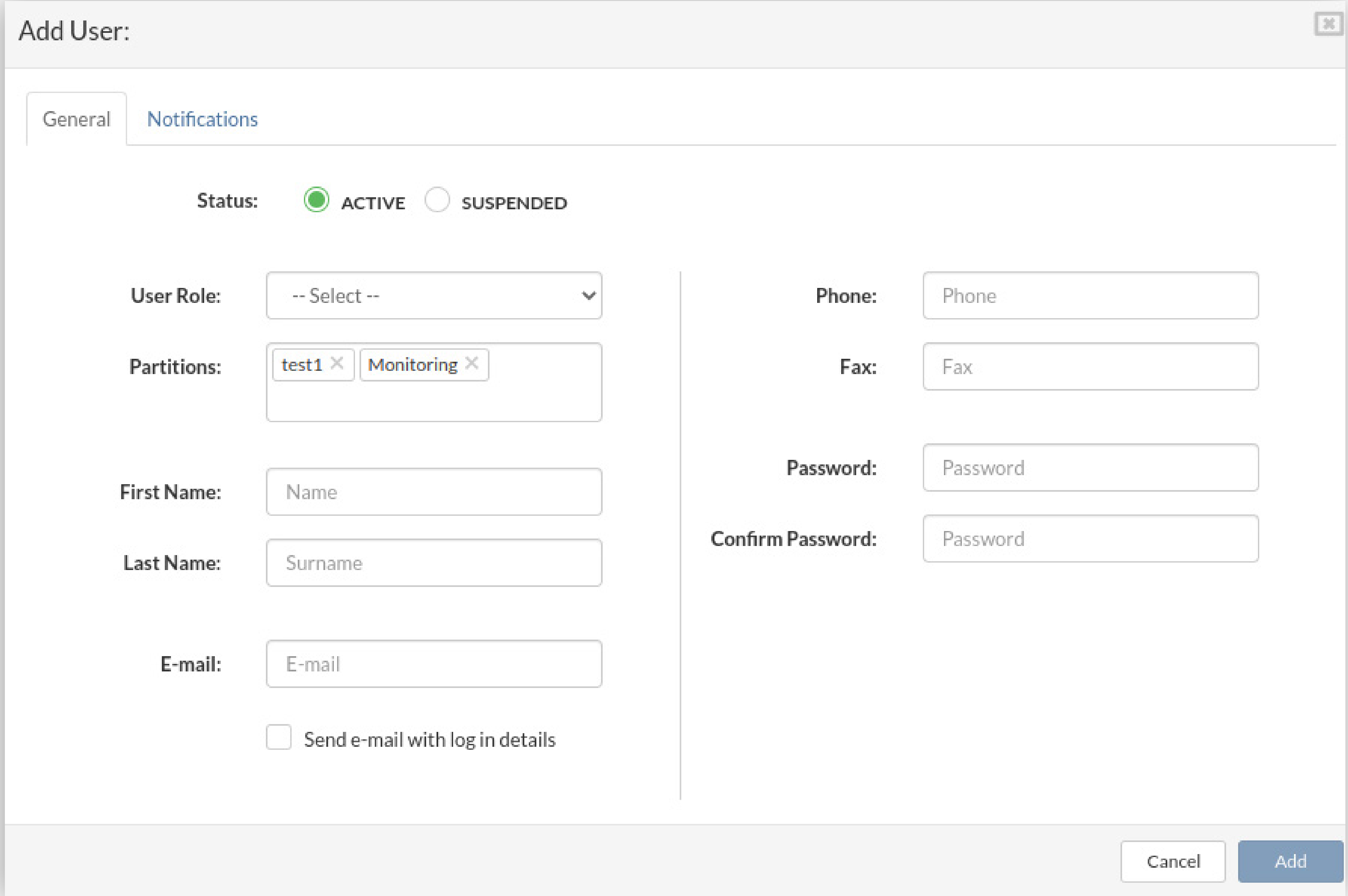
10.1.35.68

□ Include In Geo-Redundancy: -- Select --

☑ Exclude from Backup

Add User to Partition Upon User Creation

SERVERware administrators will now be able to add users to partitions upon user creation. The users will be able to sign into their partition immediately.



Status: ● ACTIVE ○ SUSPENDED

User Role: -- Select --

Partitions: test1 × Monitoring ×

First Name: Name

Last Name: Surname

E-mail: E-mail

□ Send e-mail with log in details

Phone: Phone

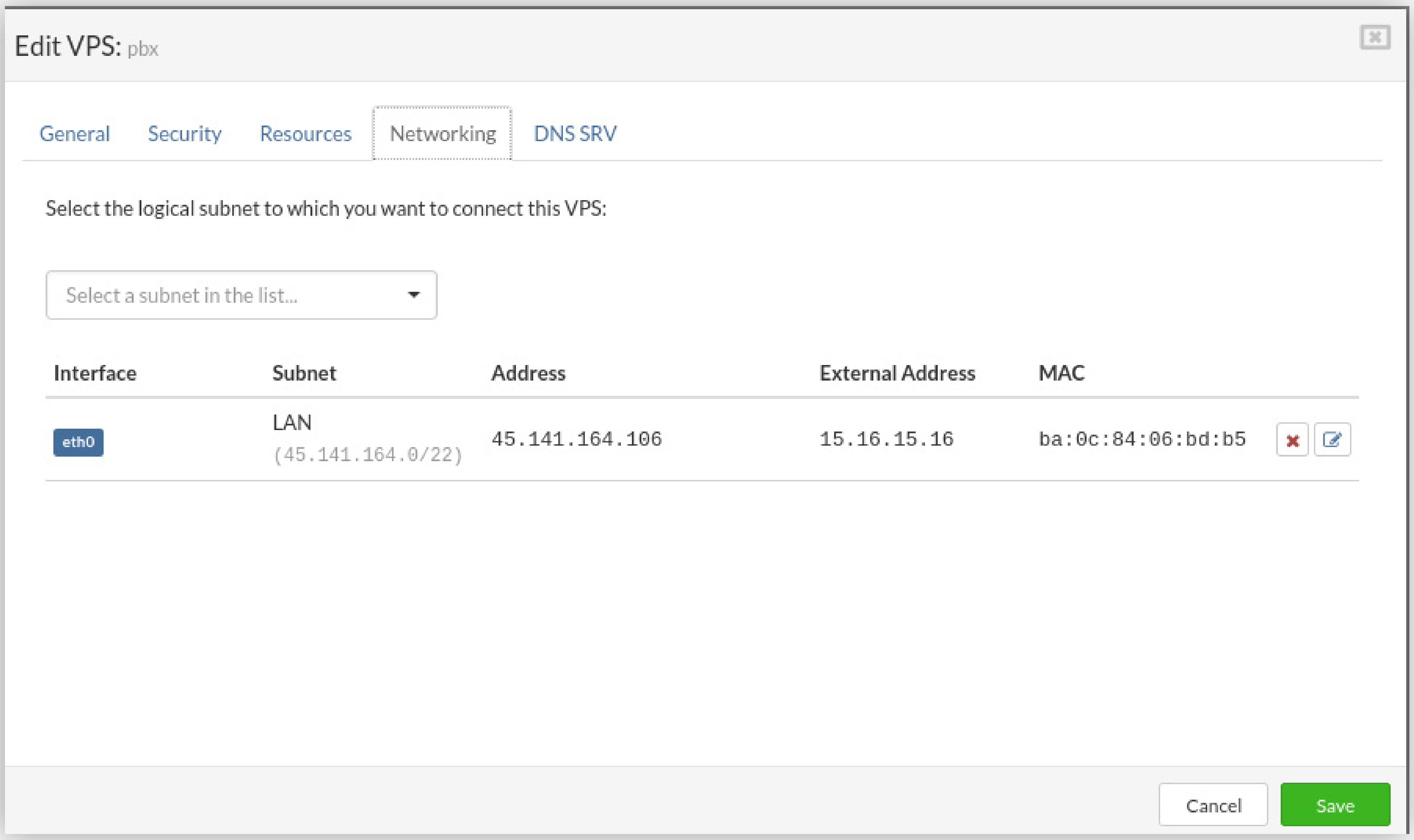
Fax: Fax

Password: Password

Confirm Password: Password

Edit VPS MAC Address through the GUI

SERVERware administrators will be able to edit the MAC addresses for VPSs through the SERVERware GUI.

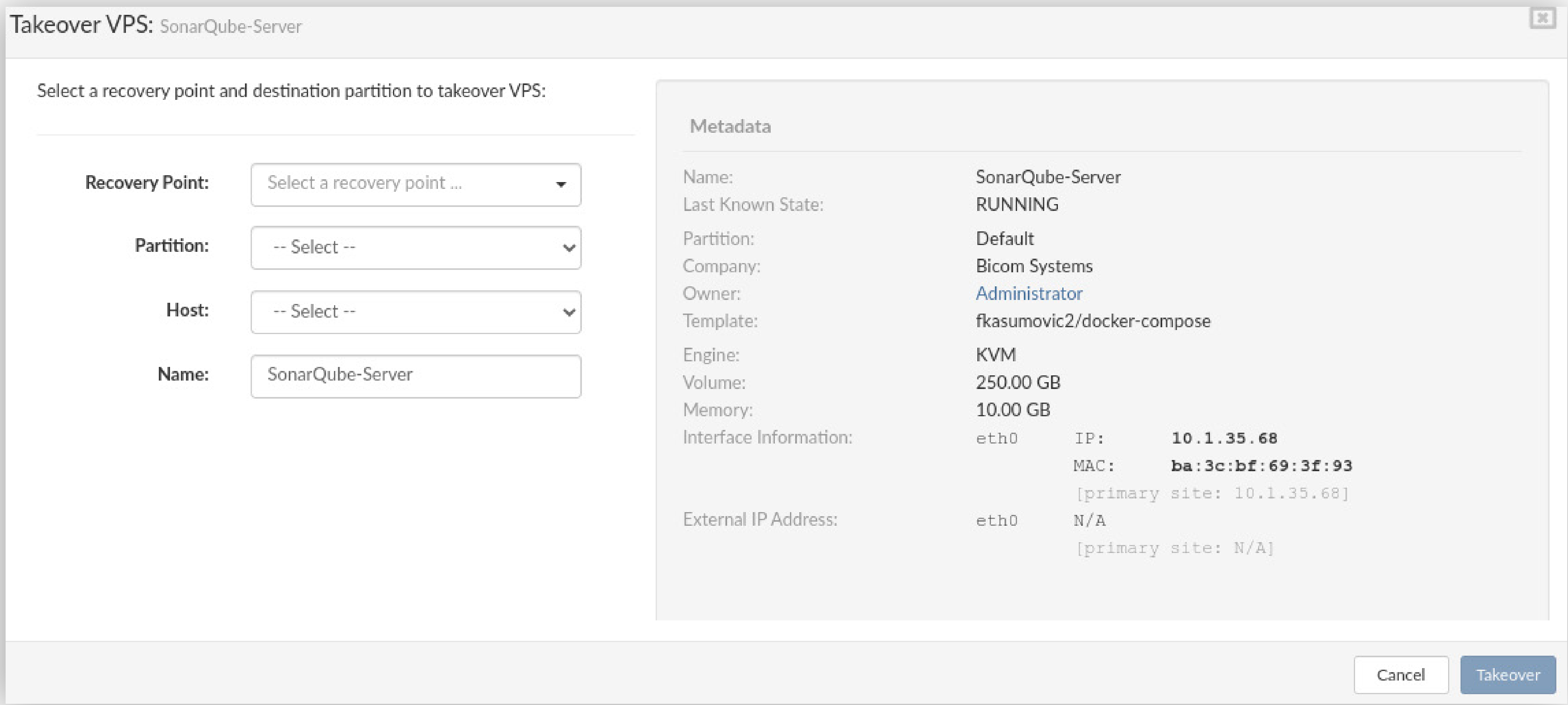


Select the logical subnet to which you want to connect this VPS:

Select a subnet in the list...

Interface	Subnet	Address	External Address	MAC
eth0	LAN (45.141.164.0/22)	45.141.164.106	15.16.15.16	ba:0c:84:06:bd:b5

The MAC address will be preserved on takeover, unless it is already in use on the cluster, in which case a new one will be generated as it worked thus far.



Select a recovery point and destination partition to takeover VPS:

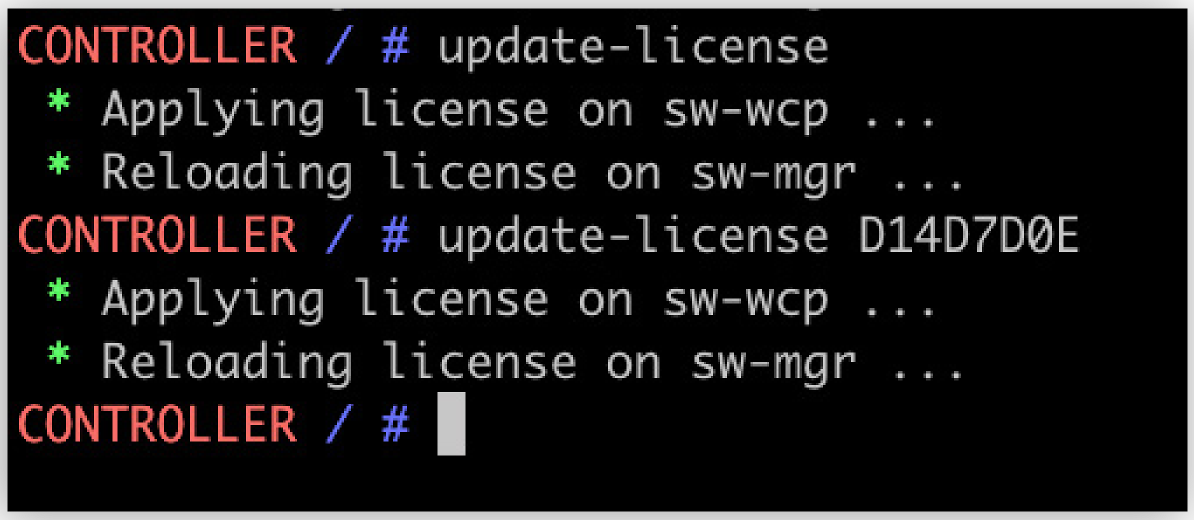
Recovery Point:	Select a recovery point ...
Partition:	-- Select --
Host:	-- Select --
Name:	SonarQube-Server

Metadata

```
Name:                    SonarQube-Server
Last Known State:        RUNNING
Partition:               Default
Company:                 Bicom Systems
Owner:                   Administrator
Template:                fkasumovic2/docker-compose
Engine:                  KVM
Volume:                  250.00 GB
Memory:                  10.00 GB
Interface Information:   eth0   IP:    10.1.35.68
                                MAC:   ba:3c:bf:69:3f:93
                                [primary site: 10.1.35.68]
External IP Address:     eth0   N/A
                                [primary site: N/A]
```

Ability to Refresh the SERVERware License through the Controller CLI

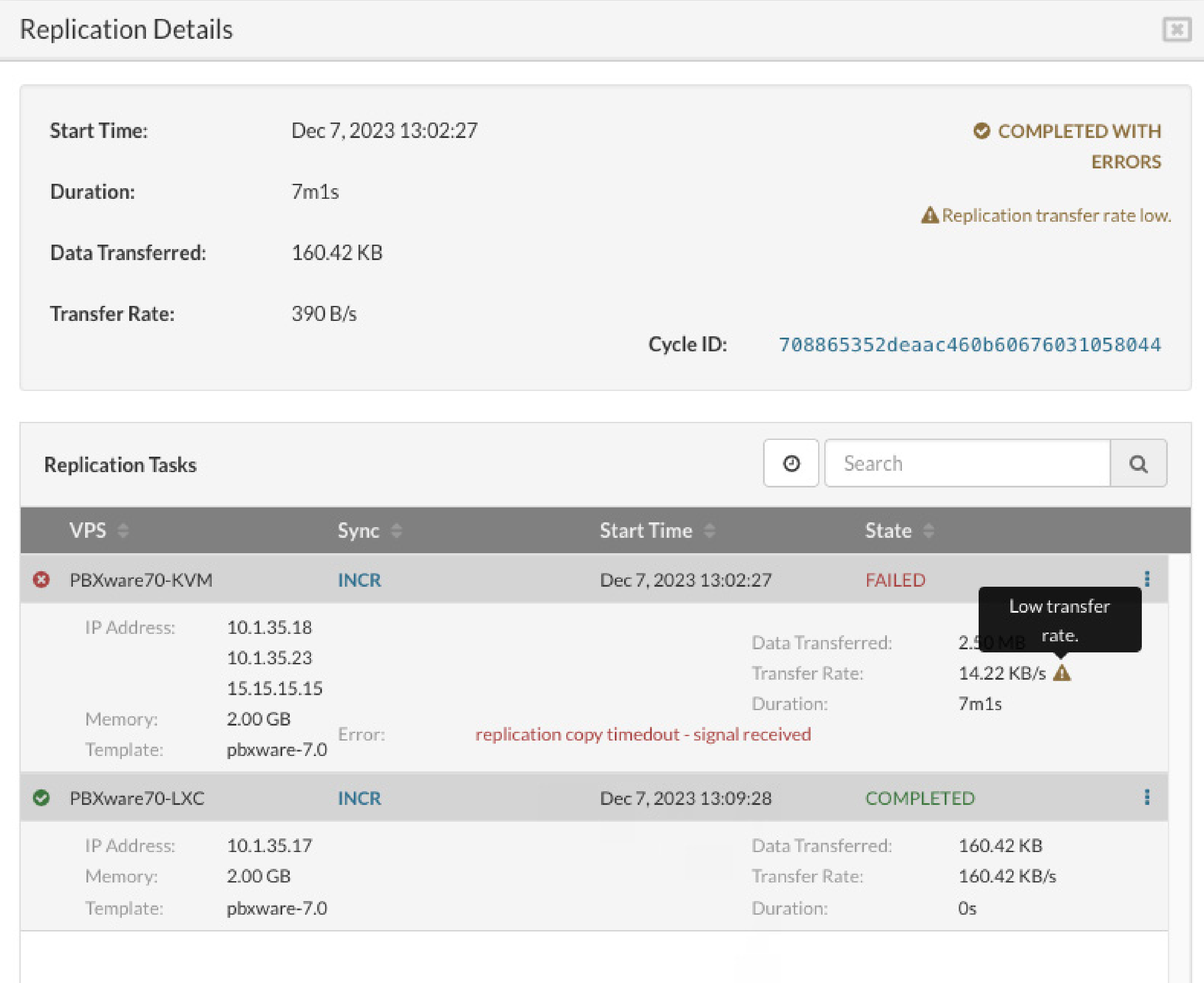
CLI users will be able to refresh the SERVERware license through the Controller command line interface. update-license will send a request to the licensing server through the sw-wcp service. The command can also be used to replace the SERVERware license by sending the new license as an argument of the command.



```
CONTROLLER / # update-license
 * Applying license on sw-wcp ...
 * Reloading license on sw-mgr ...
CONTROLLER / # update-license D14D7D0E
 * Applying license on sw-wcp ...
 * Reloading license on sw-mgr ...
CONTROLLER / #
```

Added a Warning for Insufficient Bandwidth for Replications

In case the network speed is too low for successful replications, a warning will be displayed notifying the administrator while the replication is in progress. Once the replication is completed, the notification will also appear on the Replication Details side panel. The warning will be triggered in case the transfer rate is less than 25 Mbps.



Replication Details

Start Time:	Dec 7, 2023 13:02:27
Duration:	7m1s
Data Transferred:	160.42 KB
Transfer Rate:	390 B/s
Cycle ID:	708865352deaac460b60676031058044

COMPLETED WITH ERRORS

⚠ Replication transfer rate low.

Replication Tasks

VPS	Sync	Start Time	State
✖ PBXware70-KVM	INCR	Dec 7, 2023 13:02:27	FAILED
✔ PBXware70-LXC	INCR	Dec 7, 2023 13:09:28	COMPLETED

PBXware70-KVM:

IP Address: 10.1.35.18
10.1.35.23
15.15.15.15

Memory: 2.00 GB

Template: pbxware-7.0

Data Transferred: 2.50 MB

Transfer Rate: 14.22 KB/s ⚠

Duration: 7m1s

Error: replication copy timedout - signal received

Low transfer rate.

PBXware70-LXC:

IP Address: 10.1.35.17

Memory: 2.00 GB

Template: pbxware-7.0

Data Transferred: 160.42 KB

Transfer Rate: 160.42 KB/s

Duration: 0s

Bug Fixes & Improvements:

- BSSUP default port changed to 2244.
- Removed the Archive Service from the License tab.
- Removed PBXware v4 and v5 from the Templates catalog.
- When using 2FA, for each code, the associated user's email will be provided for authentication.
- Modified syslog to use reopen instead of reload to reopen files after rotation.
- Extended VPS stop action from 15 seconds to 60 seconds to prevent database corruption.
- Added a virtualization check that will display a warning in the GUI in case hardware-assisted virtualization is not active on the host (disabling KVM engine for VPSs).
- Fixed a bug where sipPROT would block the country that the IP was accessing from.
- Fixed a bug where the install wizard exits from the install menu when selecting the wrong installation type.
- Fixed a bug where the resource view on the edit VPS window does not show VPS storage info.
- Fixed a bug where adding a backup job would cause traceback exception errors in the CLI.
- Fixed a bug where the VPS List View gets broken during and after VPS rename/move actions
- Fixed a bug in the UI where a list of VPS backups was not refreshed when switching Backup datasets.
- Fixed a bug where a missing URL in the config file would cause the BI reporting to throw an error out.
- Fixed a bug where processing commands through SAGA would periodically produce unpredictable outcomes.
- Fixed a bug where lxc-stop did not gracefully shutdown VPSs on the PBXware v7 template.
- Added a fix that enables local DNS caching in SERVERware.

- Fixed a bug that caused the VPS cloning action to time out during heavy IO load on the system.
- Fixed a bug where Redis failed to start on storage failover.
- Fixed a bug where VPS creation from an OCI image fails to reset the default password.
- Fixed a bug where resuming a replication failed due to a snapshot mismatch.
- Fixed a bug where KVMs (Firecracker) were not running on AMD CPUs.
- Fixed a bug where KVM VPSs connected to the network with the wrong MAC address.
- Updated EULA.
- Changed the logout icon.
- Fixed a bug where sw-connector logged exception errors when collecting top 5 processes during high CPU usage.

CONTACT BICOM SYSTEMS TODAY
to find out more about our services

Bicom Systems (USA)
2719 Hollywood Blvd
B-128
Hollywood, Florida
33020-4821
United States
Tel: +1 (954) 278 8470
Tel: +1 (619) 760 7777
Fax: +1 (954) 278 8471

Bicom Systems (CAN)
Hilyard Place
B-125
Saint John, New Brunswick
E2K 1J5
Canada
Tel: +1 (647) 313 1515
Tel: +1 (506) 635 1135

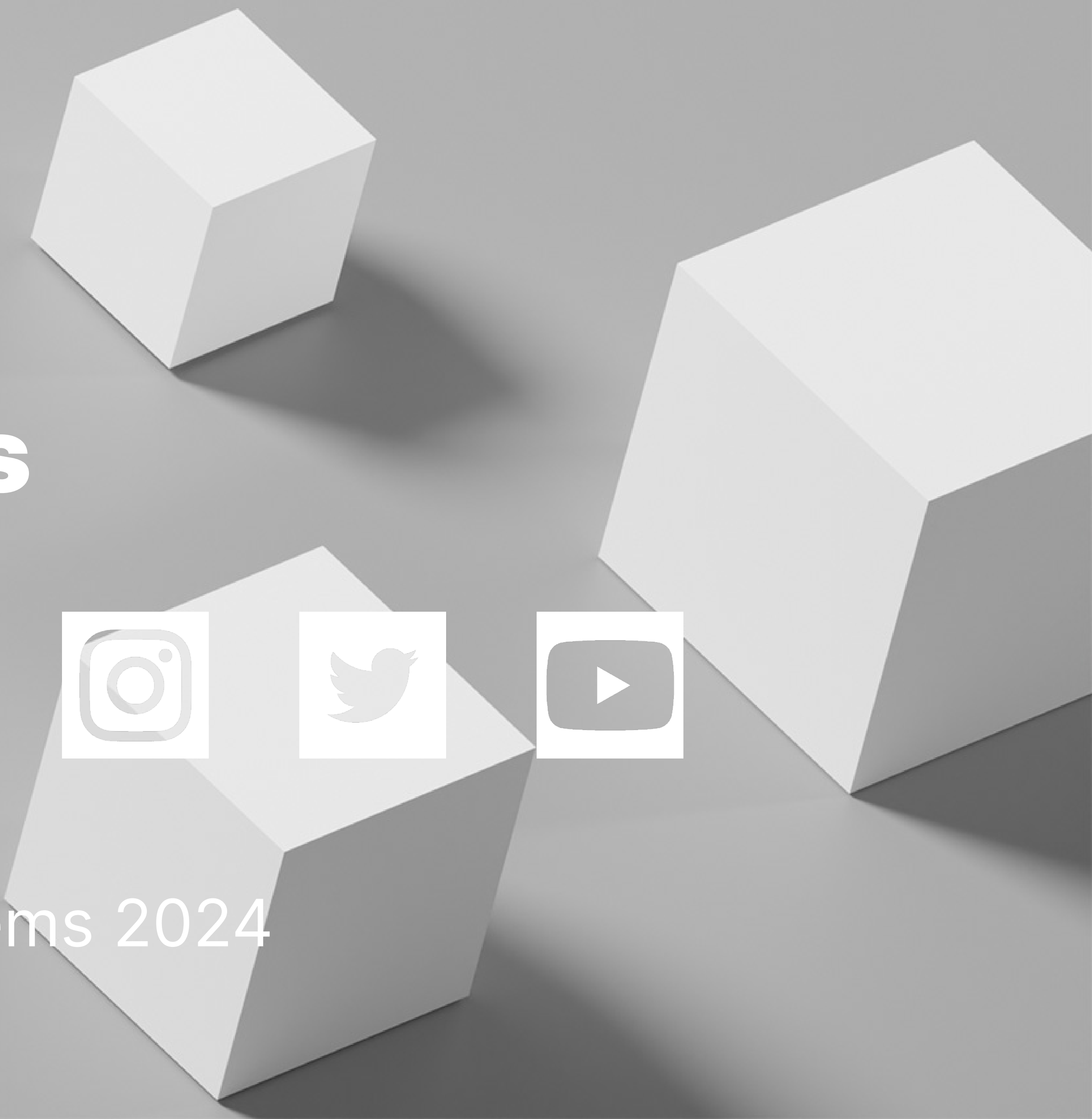
Bicom Systems (UK)
Unit 5 Rockware BC
5 Rockware Avenue
Greenford
UB6 0AA
United Kingdom
Tel: +44 (0) 20 33 99 88 00

Bicom Systems (FRA)
c/o Athena Global Services
Telecom
229 rue Saint-Honoré – 75001
Paris
Tel : +33 (0) 185 001 000
www.bicomsystems.fr
sales@bicomsystems.fr

Bicom Systems (ITA)
Via Marie Curie 3
50051 Castelfiorentino
Firenze
Italy
Tel: +39 0571 1661119
Email: sales@bicomsystems.it

Bicom Systems (RSA)
12 Houtkapper Street
Magaliessig
2067
South Africa
Tel: +27 (10) 0011390

email: sales@bicomsystems.com



Follow us

bicom SYSTEMS