

# BLUEHUB UC SIP PROTECTION

The Protector That Your System  
Deserves



# WHAT IS BLUEHUB UC SIP PROTECTION?

Bluehub UC SIP Protection is an additional security feature of the Bluehub UC PBX Software that detects and blocks SIP attacks in real-time without user intervention, enhancing your security.

Bluehub UC SIP Protection defends against SIP and TFTP attacks using scanner protection, anomaly detection, and brute force protection to safeguard the system from prevalent cyber threats.

# ESSENTIAL BLUEHUB UC SIP PROTECTION FEATURES & BENEFITS

## **DYNAMIC BLOCKING AND UNBLOCKING**

Bluehub UC SIP Protection swiftly blocks potential threats by automatically locking down IP addresses. The adjustable lock duration prevents permanent lockouts due to dynamic IPs. This requires minimal manpower for maintenance, freeing up resources for other tasks.

## **MANAGEMENT OF ALLOWLISTS AND DENYLISTS**

Bluehub UC SIP Protection includes a time-saving feature for system admins to import/export allow and deny lists in .csv format. It allows adding notes to IP addresses, bulk removal from lists, and defining multiple SIP ports for protection.

## **AUTO-PROVISIONING ATTACK DETECTION**

Bluehub UC SIP Protection secures auto-provisioning in SIP systems with TFTP Brute Force Attack detection, preventing potential attacks from redirecting requests and disrupting the system.



# BLUEHUB UC SIP PROTECTION PRODUCT OVERVIEW

All of this serves to greatly improve their workflow and eliminates a lot of the tedium from their day-to-day duties.

## Allowlist IP Addresses

[Remove](#) [Export CSV](#) [Import CSV](#)

<input type="checkbox"/> IP Address ↕	Country ↕	Note ↕	
<input type="checkbox"/> 12.6.3.8	United States		<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> 15.8.7.88	United States	Allowed by admin	<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> 15.68.58.22	Germany		<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> 80.69.48.43	Azerbaijan		<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> 83.23.6.22	Poland		<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> 95.19.6.88	Spain		<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> 98.63.5.5	United States		<input type="checkbox"/> <input type="checkbox"/>

Showing: 7 Item(s)



# BLUEHUB UC SIP PROTECTION PRODUCT OVERVIEW

The screenshot displays the configuration interface for Bluehub UC SIP Protection. The left sidebar shows a 'MAIN MENU' with categories 'NETWORK' and 'DOMAINS'. Under 'NETWORK', the 'sipPROT' option is selected, and its 'General' sub-tab is active. The main content area is titled 'General' and contains the following settings:

- Protocol:** UDP
- SIP Ports:** 5060
- SIP Blocking Rule:** 10 (bad registration per minute)
- Dynamic Block Time:** 1 Hour
- Block Threshold:** 0
- Blocked User Agents:** friendly-scanner, sipsak, Elite
- Blocked Countries:** China (CN), Afghanistan (AF), Russian Federation (RU), Pakistan (PK), India (IN), Kazakhstan (KZ), Bulgaria (BG)
- Additional Protections:** TFTP Protection (checked), DNS Protection (checked)
- Notifications:** Send Daily Attack Summary (checked), Send Log For Every Attack (unchecked)

At the bottom, it indicates 'Limited to: 100 instance(s) - Expiry date: Sep 16, 2041' and a 'Save & Apply' button.

## GEOIP BLOCKING

Make full use of Bluehub UC SIP Protection by implementing GeoIP blocking to block entire country IP ranges during SIP attacks or for other security reasons.





# 24/7 EXPERT SUPPORT AT YOUR FINGERTIPS

Rest assured with round-the-clock support. Our highly trained experts are always available to address any system-related issues or questions that you may have, ensuring seamless operations and peace of mind.

## Phone

+ 1300 868 178

## Email Address

[sales@bluehubuc.com.au](mailto:sales@bluehubuc.com.au)

