

HSB IPBX Security Guide

Oct 7, 2026 · @jabed

Phone systems reachable from the internet are a favourite target for toll fraud: attackers guess extension passwords and make expensive international calls on your account. HSB IPBX has the protection built in; this guide shows how to switch it on and keep it that way.

Go-live checklist

Tick every item before the PBX handles real calls; each is explained below.

- ☐ Admin password changed from the factory default
- ☐ Console password (`hsbadmin`) changed
- ☐ Every extension shows **Strong** under Password Health
- ☐ Voicemail PINs changed from the default
- ☐ Firewall turned on
- ☐ GeoIP limited to your country, if any SIP port is reachable from the internet
- ☐ International and premium numbers limited with Dial Permission or PIN sets
- ☐ Web dashboard (8080), SSH (22) and provisioning (8181) **not** forwarded on the router
- ☐ A backup made and stored off the PBX

Passwords

Weak extension passwords are the most common way phone systems get abused.

Account	Where to change it	Rule
Web admin	Prompted at first sign-in; later System → Security Center → Admin Password	At least 10 characters, used nowhere else
Console <code>hsbadmin</code>	Console menu option 6	Long and unique
Extensions	System → Security Center → Password Health	Shown as <i>Strong</i> : 12+ characters, not a default, not shared

Account	Where to change it	Rule
HSB-Call Wave agents	Add-ons → HSB-Call Wave	8+ characters, one per agent
Voicemail PINs	Each user, from their phone with *97	Not the default PIN

Password Health lists every extension as Strong or Weak with the reason. **Fix all weak passwords** replaces the weak ones with random 16-character passwords and shows them once — copy or print the list. Phones set up through Phone Provisioning receive the new password automatically; other phones and gateways must be updated by hand.

Firewall

A new installation has the firewall **off**, with the standard rules already prepared. Turn it on before the PBX is connected to the internet.

1. Open **System → Security Center → Firewall**.
2. Click **Turn on** and confirm.

Turning it on always keeps these ports open, so you can't lock yourself out:

Port	Purpose
22/tcp	Support access (SSH)
8080/tcp	Web dashboard and HSB-Call Wave
8089/tcp	Encrypted WebRTC
5060/udp, 5061/tcp	SIP phones and trunks
10000–20000/udp	Call audio
8181/tcp	Phone provisioning — local networks only

+ **Add rule** allows or denies a port, a port range (for example 10000:20000, TCP or UDP) from any address, one IP or a network such as 192.168.1.0/24. **Delete** removes a rule; **Restore HSB default rules** puts the standard ones back.

Country blocking, Fail2Ban and blacklist

GeoIP Policy (Security Center) accepts SIP connections only from the countries you choose — most attacks come from abroad.

1. Tick **Enable GeoIP policy**.
2. Tick your country (and any country where you have remote phones or your SIP provider). Other countries: type their two-letter codes, for example `MY, ID`.
3. Optional: also protect the web and WebRTC ports (8080, 8089).
4. **Save and apply**. The result line shows how many networks were loaded.

Your local network, the PBX itself and your SIP trunk provider are **always** allowed. The country lists are downloaded once and re-applied at every restart.

Fail2Ban watches for repeated failed sign-ins and blocks those addresses automatically. **IP Blacklist** blocks addresses you name yourself. Both are under Security Center.

Connecting safely to the internet

Most offices need **no** port forwarding at all: the PBX reaches your SIP provider with outgoing connections only.

Situation	What to open on the router
Office phones only, SIP trunk	Nothing
Remote desk phones or softphones over the internet	UDP 5060 and 10000–20000 to the PBX — with the firewall on, GeoIP limited, and strong passwords
Remote HSB-Call Wave agents	Nothing — use Cloud remote access (HSB IPBX-50 and above), set up with Hidden Systems Security

Never forward:

- **8080** (web dashboard) — admin access belongs inside the office
- **22** (SSH)
- **8181** (phone provisioning) — it hands out phone passwords

Also limit expensive calls: **Outbound Control** → **Dial Permission** blocks international or premium numbers for extensions that don't need them, and **PIN Sets** ask for a PIN before such calls.

Backups and warning signs

Backups: make one under **Maintenance** → **Backup** after setup and after every big change, and keep a copy off the PBX (another computer or cloud storage). Software updates also make their own backup automatically before installing.

Signs that something is wrong — act at once:

- Calls to unknown international numbers in **Reports** → **Call Log**, especially at night or on weekends
- An unexpectedly high bill from your SIP provider
- Many failed sign-ins or blocked addresses in **System Logs** or Fail2Ban
- Extensions registered from addresses you don't recognise (console option 4)

What to do: reset the affected extension passwords (Password Health), turn on the firewall and GeoIP if they're off, ask your SIP provider to block international calls temporarily, and contact support@hiddensystemssecurity.com · +973 16609158.