PENTAGON BUSINESS COM

Pentacomm

The communications appliance
for modern organizations

A full PBX, integrated call center, carrier trunking, compliant call recording, and live operational visibility — unified in one multi-tenant, standards-based appliance you own and control.

Product & Technical Overview · Revised 2026-11
Built on open standards · On-premises or private cloud · www.pentacomm.ro

IN BRIEF

One platform for every conversation

Pentacomm consolidates the systems an organization normally buys separately — a phone system, a contact-center suite, a session border controller, and a call recorder — into a single, self-contained appliance managed from one web console. It runs on your own hardware or private cloud, so calls, recordings, and customer data never leave your control.

Because Pentacomm is multi-tenant at its core, one appliance can serve many departments, sites, or customers in complete isolation. And because it speaks open telecom standards end to end, it interoperates with any SIP carrier and any standards-based phone or browser — with no proprietary lock-in at the protocol layer.

WHY IT MATTERS

What your organization gains

- **Consolidate the stack —** Replace a PBX, a call-center platform, an SBC, and a recording server with one system — fewer vendors, fewer integrations, lower total cost.
- **Own your data —** Deployed on-premises or in your private cloud. Media and recordings stay inside your perimeter, encrypted and under your keys.
- **Compliance-ready —** GDPR consent prompts, caller opt-out, pause / mask recording, retention periods you set, and a full audit trail are built in — not bolted on.
- **No lock-in —** Standards-based SIP and WebRTC mean you keep your carriers, your numbers, and your phones. Switch providers without switching platforms.
- **Scales by tenant —** Service providers and multi-site enterprises host many isolated organizations on a single, database-enforced multi-tenant platform.
- **Fast to deploy —** A signed installer image and a guided first-boot wizard take a clean server to a live system.

CAPABILITIES

Everything a modern voice platform needs

Each area below is production-ready today and managed from the same console, with role-based access for administrators, supervisors, and agents.

Phone system (PBX)

Extensions, ring groups, inbound and outbound routing with trunk failover, weekly business-hours modes and holidays, voicemail with message-waiting indication, and class-of-service dialing controls. Call forwarding set from the phone or the portal, call park, intercom, and wake-up calls and reminders.

Standard IVR auto-attendant

Multi-level, menu-driven auto-attendants — DTMF menus, time-of-day routing down to the individual key, per-key announcements, and directed call handling to extensions, queues, voicemail or sub-menus. A caller who presses nothing or a wrong key can be sent straight on — to an operator, a queue or another menu — and a key can take them back to the previous menu. A short ring before answering keeps mobile callers from missing the start of the greeting. Key-press and call-flow analytics show how callers actually move through the menus.

Integrated call center

Queues and agents, an in-browser WebRTC softphone (no plugins), a live wallboard, supervisor KPI reports and QA scoring, scheduled callbacks, and self-service agent and supervisor portals.

Audio conference bridge

Multi-party audio conferencing with PIN-protected rooms, moderator controls (mute, kick, lock), scheduling with dial-out to invitees, and a live web console — secured by the same SRTP media edge.

Carrier trunks & secure media

SIP trunks in register, auth, or peer mode with ordered failover, per-trunk caller-ID rules and a per-trunk call limit. A carrier can sit on its own network interface or port, and an existing PBX can connect as a peer. The trunk page and the dashboard show whether each trunk is actually registered with the carrier, and why not. A hardened media edge terminates SRTP / DTLS so every leg is encrypted.

Fax server

Inbound and outbound fax over T.38 (with G.711 / T.30 fallback) — a web fax inbox, PDF send with cover pages, and an email notice with a secure link, encrypted at rest per tenant. Runs on the same appliance, with no fax hardware and no separate fax server. A licensable module.

Recording & compliance

Per-tenant call recording encrypted with dedicated keys. GDPR consent announcements, DTMF opt-out, periodic beep, supervisor pause / mask, and retention periods you set per category, enforced by a daily sweep.

Visibility & reporting

Searchable call-detail records with CSV, XLSX, and PDF export; a real-time dashboard of live calls and registrations, and of the server itself — CPU, memory, disk, network ports and services — with anything that needs attention listed at the top; an audit log plus an access log of who opened which recording, voicemail or fax; and live diagnostics for operations teams.

Backup & restore

Complete, incremental, encrypted backups on a daily schedule or on demand, managed from the console. Restore onto the same appliance or a replacement, carry a backup on a USB drive, and unlock it with a recovery key only you hold.

Guarded upgrades

Administrators see what a new release brings before installing it, then install or schedule it with one button, together with any waiting Debian security updates. The appliance waits for live calls to end, takes a snapshot, checks its health afterwards and rolls everything back together if anything fails. Debian security updates arrive only after passing the same checks.

Network from the console

Multiple network interfaces, VLANs, routes, DNS and time are set from the web console and applied without a reboot. A change that cuts off the administrator is reverted automatically unless confirmed.

Built-in firewall & intrusion prevention

A perimeter firewall with automated intrusion-prevention jails that detect and block SIP scanners, credential brute-force, and web-login abuse — with allow / block lists and per-jail tuning from the console. Every block rule is checked against the firewall each minute and repaired if it slipped. Premium-rate and toll-fraud destinations are barred by default, and a PBX or carrier on a trunk cannot use phone feature codes.

Security & multi-tenancy

Strict per-tenant isolation enforced in the database, role-based access control, two-factor sign-in, TLS throughout, and a perpetual offline license bound to the machine to prevent cloning.

WHAT SETS PENTACOMM APART

Engineered for control, compliance, and trust

- **One appliance, the whole stack —** Installed from a signed image with a guided setup wizard. There is no sprawl of servers to integrate — the PBX, call center, trunking, recording, and reporting are one coherent system.
- **Standards-first, not vendor-first —** A standards-conformant SIP edge and secure WebRTC softphones mean interoperability with any carrier and any compliant device. Your investment is protected against any single vendor's roadmap.
- **Compliance designed in —** Recording consent, opt-out, pause / mask, retention, encryption, and audit logging are core features — giving legal and compliance teams the controls they need without custom work.
- **Multi-tenant by architecture —** Tenant isolation is enforced at the database layer, not left to application convention. One customer can never see another's data.
- **Continuously validated —** An automated SIP call-flow test suite exercises real scenarios on every release, and each release is an immutable, exactly pinned package set — so what you install is what was tested, and an upgrade that fails its final check reverts itself.
- **Support on your terms —** Remote support rides an encrypted tunnel the appliance opens outward — no VPN, no inbound port. Every session is emailed to your administrators and written to the audit log; you can require approval per session or switch it off.
- **You keep ownership —** On-premises or private-cloud deployment keeps numbers, recordings, and customer data inside your control.

THE BOTTOM LINE

Fewer vendors. Lower cost. Full control of your data — and the compliance evidence to prove it.

TECHNICAL ARCHITECTURE

How Pentacomm is built

Pentacomm is a layered, single-appliance stack. A SIP proxy handles all signalling at the network edge; a media relay is the sole path for audio, so the media/application server never faces the public network. A REST backend drives configuration and real-time control, and every tenant's data is isolated in the database.

Core components

OpenSIPS	SIP edge — proxy and registrar. Terminates SIP-over-UDP/TCP, SIP-TLS and SIP-over-WebSocket (WSS); performs request validation, authentication, per-source flood protection and NAT keepalive.
FreeSWITCH	Back-to-back user agent and application server — dialplan, IVR, voicemail, recording, conferencing and fax. Reachable only over the internal loopback; never exposed to the public network.
rtpengine	Media edge — the single public RTP/SRTP path for every leg (carrier, desk phone, browser, mobile). Terminates DTLS-SRTP and SDES-SRTP; the application server stays on plain RTP behind it.
FastAPI backend	REST API and control plane — drives OpenSIPS (MI) and FreeSWITCH (ESL), renders configuration, streams live events, and validates the offline license.
Angular frontend	Web admin console plus dedicated agent and supervisor portals, and a browser WebRTC softphone (sip.js) — no plugins or desktop client required.
PostgreSQL	System of record with row-level security per tenant and dedicated least-privilege roles for the app, the CDR writer and the recording encryptor.

Network interfaces

443 / TCP	HTTPS — admin console, REST API and WebRTC signalling proxy (TLS).
5060 / UDP,TCP	SIP signalling (OpenSIPS), advertising the appliance address. Listeners are configurable — a carrier can be given its own interface, address or port.
5061 / TCP	SIP-TLS for native encrypted desk phones (IANA sips port).
7443 / TCP	SIP-over-WebSocket Secure (WSS) for browser softphones.
24576–32767 / UDP	RTP / SRTP media range served by rtpengine for every call leg.

Security posture

- TLS everywhere — SIP-TLS, WSS and HTTPS; certificates managed on-box, IP-SAN aware for softphones.
- Encrypted media end to end — DTLS-SRTP for WebRTC and SDES-SRTP for SIP-TLS, with rtpengine as the sole crypto edge.
- Hardened SIP edge — RFC 3261 request validation before authentication, per-source rate limiting, dead-binding reaping, and SHA-256 digest authentication negotiated with phones that support it.
- Built-in perimeter firewall — automated intrusion-prevention jails detect and block SIP scanners, credential brute-force and web-login abuse, with allow / block lists and per-jail tuning from the console.
- Database-enforced multi-tenancy — PostgreSQL row-level security, not application-level filtering.
- Encrypted recordings — chunked AES-256-GCM with per-tenant keys and a dedicated encryptor role.
- Two-factor sign-in — TOTP (RFC 6238) for console accounts, enforceable installation-wide, with one-time backup codes.
- Support access under your control — an outbound-only encrypted tunnel, short-lived engineer certificates, an email notice and an audit entry for every session, optional approval per session, and an off switch only you hold.
- Offline, machine-bound licensing — a perpetual, RSA-signed license verified on the appliance without calling home.

DEPLOYMENT & OPERATIONS

Simple to stand up, straightforward to run

Platform & delivery

Base OS	Debian 13 (Trixie) appliance — bare-metal, or a virtual machine on VMware, Proxmox, KVM or your private cloud.
Delivery	A signed installer image (ISO), then native Debian packages via a managed apt channel — with Debian itself served from a tested, pinned snapshot.
Data store	PostgreSQL with row-level security per tenant.
Audio	G.711 A-law end to end, with no transcoding in the call path; T.38 for fax.
Endpoints	Browser WebRTC softphone (sip.js) on desktop and mobile browsers; standards-based desk phones and SIP softphones over SIP-TLS; and PentaPhone, our Android softphone, set up by scanning a QR code and woken by push (RFC 8599).
Releases	Semantic-versioned, CI-gated builds validated by an automated SIP call-flow suite; each release is an immutable package set, installed as one guarded step that reverts itself on failure.
Sizing	Capacity follows the cores, memory and storage you give the appliance. We size each deployment to its traffic and recording profile.

- Delivered as a self-contained appliance — a signed installer image brings up the entire stack on a clean server.
- Runs on-premises or in your private cloud. An air-gapped installation works too: it simply has no remote-support channel.
- One web console for administrators, with search, a phone layout and built-in help in English and Romanian; a self-service portal where extension users manage their own voicemail and call forwarding; and purpose-built consoles for call-center agents and supervisors.
- A modular licensing model: the phone system — voicemail and audio conferencing included — is the base, and you switch on advanced modules such as the call center, call recording or fax as your needs grow.
- Regular, tested releases, installed or scheduled from the console and rolled back automatically if anything fails.

STANDARDS & INTEROPERABILITY

Supported standards (RFC)

Pentacomm implements the relevant IETF and W3C standards rather than proprietary variants, so it interoperates with any compliant carrier, phone or browser. The tables below list the standards the platform conforms to, grouped by area.

SIP signalling

RFC 3261	Session Initiation Protocol (SIP) — core signalling.
RFC 3264	SDP offer/answer model.
RFC 4566	Session Description Protocol (SDP).
RFC 3311	SIP UPDATE method.
RFC 3515 / 5589	SIP REFER method and call-transfer call control.
RFC 3891	SIP "Replaces" header — attended transfer.
RFC 3842	Message-summary event — voicemail MWI.
RFC 3323 / 3325	Caller privacy (CLIR) and P-Asserted-Identity — trusted caller identity.
RFC 4916	Connected identity in SIP.
RFC 5626	Managing client-initiated connections (outbound) & keepalive.
RFC 5658	Record-Route fix for dialogs behind NAT.
RFC 6665	SIP-specific event notification (SUBSCRIBE/NOTIFY).
RFC 7118	SIP over WebSocket transport.
RFC 7616 / 8760	HTTP and SIP digest authentication with SHA-256.
RFC 8599	Push-notification support for SIP (mobile wake-up).

Media & fax

RFC 3550 / 3551	RTP and the audio/video profile (RTP/AVP).
RFC 2833 / 4733	DTMF carried as RTP telephone-event.
RFC 3711	Secure RTP (SRTP) — media encryption.

RFC 4568	SDES — SDP security descriptions for SRTP keying.
RFC 5763 / 5764	DTLS-SRTP — WebRTC media keying.
ITU-T G.711	A-law audio (PCMA).
ITU-T T.38	Real-time fax over IP, carried over UDPTL (T.38 Annex D).
RFC 3362	The image/t38 media type in SDP — T.38 negotiation.
ITU-T T.30 / T.4 / T.6	Group 3 fax protocol over a G.711 leg, and the G3/G4 page encodings.

Security, PKI & identity

TLS 1.2 / 1.3	Transport security for SIP-TLS, WSS and HTTPS.
RFC 5280	X.509 certificate and CRL profile.
RFC 6125	Service identity verification in TLS.
RFC 5116 / 3394	AEAD (AES-GCM) and AES key-wrap — recording encryption.
RFC 6238	Time-based one-time passwords (TOTP) — two-factor sign-in.
RFC 7519 / 8725	JSON Web Token (JWT) and JWT best current practice.
RFC 6749	OAuth 2.0 authorization framework (token model).

Web & data

RFC 9110	HTTP semantics and status codes.
RFC 6455	The WebSocket protocol.
RFC 6585	Additional HTTP status codes (e.g. 429 rate-limit).
RFC 7233	HTTP range requests — media streaming.
RFC 8259	JSON data interchange format.
RFC 3339	Date/time on the Internet (ISO 8601 timestamps).
RFC 3986	Uniform Resource Identifier (URI) syntax.

PRODUCT ROADMAP

Where Pentacomm is heading

The platform evolves on a published roadmap. The following capabilities are in active development, building on the same standards-based foundation.

IN DEVELOPMENT

Visual IVR designer

A drag-and-drop call-flow builder — design menus, prompts, business-hours branches, queue and voicemail targets on a visual canvas, with no scripting. Publishes straight to the live dialplan, on top of the standard IVR that ships today.

IN DEVELOPMENT

AI IVR

Conversational, natural-language self-service — speech-to-text, intent understanding and text-to-speech let callers be routed and served by voice, with graceful hand-off to a live agent.

More licensable modules on the roadmap

Hotel link	Hospitality / PMS integration — wake-up calls, room status and check-in/out, minibar posting and per-room call billing, linked to the property management system.
Voicemail transcription	Speech-to-text transcripts delivered with voicemail.
Video conferencing	Multi-party video on top of the conference bridge.

WHO IT IS FOR

Built for organizations that run on the phone

- **Multi-site enterprises —** consolidating fragmented phone systems onto one managed platform with consistent policy and reporting across locations.
- **Contact centers —** that need queues, a browser softphone, live wallboards, supervisor QA, and recording with compliance controls in one place.
- **Service providers & resellers —** hosting many customers on a single multi-tenant appliance, each fully isolated, each independently administered.
- **Regulated organizations —** in finance, healthcare, and the public sector that require on-premises control, GDPR compliance, and a complete audit trail.

GET STARTED

Take control of your communications.

See Pentacomm running on a live appliance and map it to your environment. Talk to us about a proof-of-concept, licensing, and deployment.

Pentagon Business COM
Product & deployment enquiries
www.pentagon.ro
www.pentacomm.ro