Multi User/Tenant Agents

cirriussolutions
YOUR SILVER LINING IN THE CLOUD

Multi Tenancy

Multi User

- Multiple individual users interact with the same AI agent within a shared tenant (organization), with role-based access control and personalized context

Internal Sales AI Assistant (Single Company)

Company: Acme Corp
Users: Sales reps, Sales managers, RevOps

Agent capabilities:

Sales reps ask: "Summarize my open deals."

Manager asks: "Show team pipeline risk."

RevOps asks: "Generate QBR report."

How it works:

All users share the same CRM data (tenant-level data).

Each user sees only data allowed by their role.

The agent remembers individual user preferences (e.g., preferred dashboard format).

Shared company documents (pricing, positioning) are accessible to everyone internally.

Multi Client/Branch

Multi-Client / Multi-Branch: A single AI system serves multiple independent organizations or business units, with strict data isolation and tenant-scoped configuration, memory, and tooling.

AI Support Agent SaaS Platform

Platform serves: Acme Corp, Beta Logistics, North Region Branch, South Region Branch

Agent capabilities: Answers customer support questions, Pulls order status, Escalates tickets

How it works:

Acme's customers only access Acme data.

Beta Logistics has entirely separate documents, workflows, tone, escalation rules.

North Branch uses different pricing rules than South Branch.

Each tenant has:

Separate knowledge base

Separate tool credentials

Separate memory

Custom branding & tone

cirriussolutions
YOUR SILVER LINING IN THE CLOUD

	Multi-User	Multi-Tenant
Memory	Separate "user memory" from "org memory" (preferences vs shared facts/processes). Scope every memory write with (tenant_id, user_id, app_id, purpose) so you never "remember" in the wrong place. RBAC-aware retrieval: the agent should only retrieve memories the user is allowed to see. Guardrails for shared memory writes: only promote items to org memory via rules ("verified", "approved", or "system-generated").	Hard isolation by tenant: memory stores must be partitioned or keyed so cross-tenant retrieval is impossible. No shared embeddings across tenants unless strongly partitioned (and you're confident in enforcement). Tenant-configured retention (some clients require short retention or none). Migration & deletion: support tenant offboarding with complete memory purge.
Documents	Tenant-wide KB + user-specific files (e.g., "my notes") as separate sources. Doc-level permissions enforced at retrieval time (not just at upload time). Versioning matters: the agent should cite "which version" it used and prefer latest approved docs. Avoid accidental training leakage: don't let private docs become globally searchable.	Per-tenant document stores (or strict partitioning) with tenant-scoped indexing. Tenant-specific policies & tone embedded in configuration, not mixed into shared docs. Connector credentials are tenant-scoped (Salesforce/Drive/Jira per tenant). Branch nuance: allow inheritance (global client docs) + overrides (branch-specific SOPs).
Logging	Log by user identity (who asked, what tools ran, what data was accessed). Record retrieval provenance: which memories/docs were fetched and why. Redact sensitive content in logs by default; store references/IDs over raw text. Audit trail for escalations and writes: especially when the agent saves memory or updates CRM.	Tenant-scoped logs with strict access controls (Client A can't see Client B's telemetry). Compliance-friendly logs: retention windows, export tools, and searchable audit trails per tenant. Incident forensics: capture tool calls + retrieval sets, but minimize stored user content. Metrics segmentation: quality, latency, and cost tracked per tenant for billing and SLAs.



cirriussolutions

YOUR SILVER LINING IN THE CLOUD

Golden Rule

Multi-User: "Same data pool, different permissions."

Multi-Tenant: "Different data pools, no overlap—ever."

cirriussolutions
YOUR SILVER LINING IN THE CLOUD