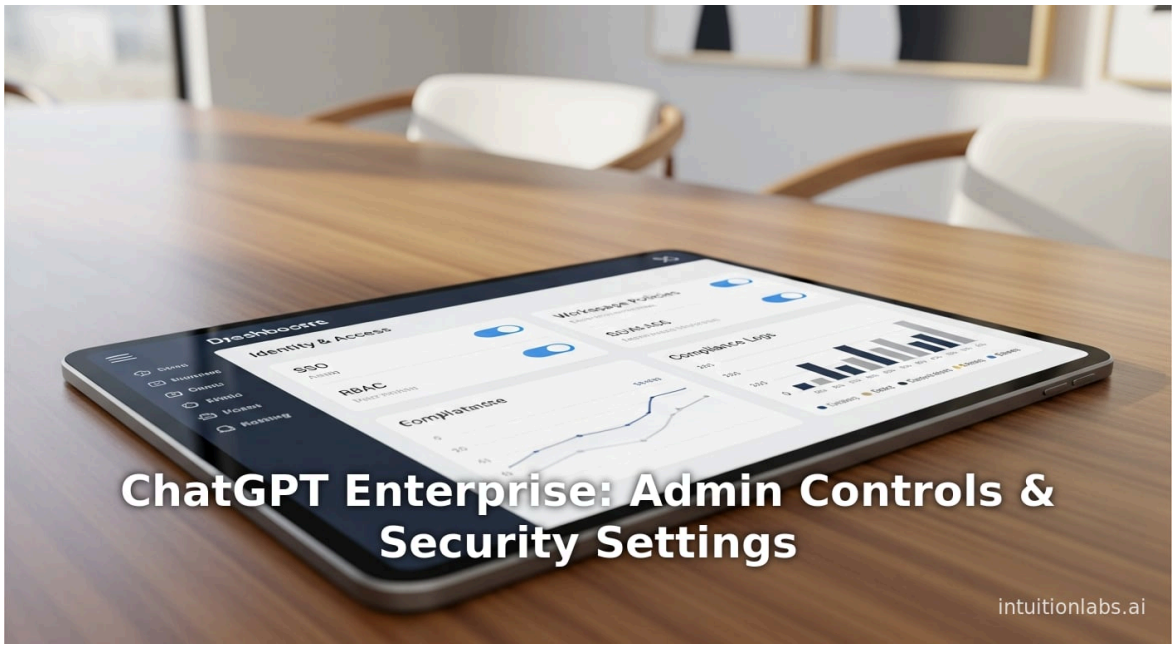
ChatGPT Enterprise: Admin Controls & Security Settings

4/17/2026 • 30 min read

chatgpt enterprise | admin controls | ai governance | data residency | enterprise security | rbac | sso integration | compliance logs | workspace management



Executive Summary

ChatGPT Enterprise (as of April 2026) is OpenAI's premium offering designed to meet the needs of large organizations, providing robust administrative controls, security, and compliance features beyond those in consumer and small-business plans. It builds on the capabilities of the base ChatGPT platform (powered by GPT-4 and GPT-5 models) but adds **enterprise-grade security** (e.g. SOC 2 compliance, end-to-end encryption, data residency, and optional customer-managed encryption keys), **identity and access management** (domain verification, SSO/SAML, SCIM provisioning, IP allowlists), and **fine-grained governance** (workspace policies, audit logs, and role-based access control) ([1] openai.com) ([2] openai.com). Administrators can centrally manage workspaces via a console, assign custom roles to teams, enable or disable specific apps (integrations) and actions, and export detailed usage/compliance logs for analysis ([3] help.openai.com) ([4] help.openai.com). For example, OpenAI's own documentation emphasizes that with Enterprise "you do not train on your business data or conversations," all conversations are "encrypted in transit and at rest," and a specialized **Global Admin Console** provides "domain verification, SSO, and usage insights" for large-scale deployment ([1] openai.com) ([5] help.openai.com). Industry reports confirm the rapid enterprise adoption of ChatGPT: by 2026 ChatGPT reportedly has over **50 million paying users** and ~**900 million weekly active users**, with enterprise contracts contributing roughly **40% of OpenAI's revenue** ([6] www.techradar.com). Real-world evidence suggests significant productivity impact – for instance Asana's data team reported that ChatGPT Enterprise "cut down research time by an average of an hour per day" ([7] openai.com).

In this report, we present an **in-depth survey** of ChatGPT Enterprise's options and controls. We cover its architecture and features, the configurable security and data governance settings, integration options (such as third-party "apps" and custom GPTs), and administrative workflows (identity, roles, billing). We include tables comparing enterprise vs other plans, links to the latest OpenAI documentation, illustrative case studies (e.g. enterprise deployments at Asana, Klarna), and analysis of security/compliance considerations. Wherever possible, claims are backed by official sources or independent analysis ([1] openai.com) ([6] www.techradar.com) (beyondscale.tech). We also consider future directions (e.g. the new Global Admin Console, evolving compliance logs API, broader data-residency) and discuss implications for enterprise IT and governance.

Introduction and Background

Since its public release in late 2022, ChatGPT has seen explosive growth across consumer and professional settings. By early 2024, OpenAI reported **millions of daily users** noting widespread use for tasks from drafting emails to coding. Enterprises quickly adopted the technology informally – one analysis claims roughly *92% of Fortune 500 companies* had employees using ChatGPT by late 2025 (www.humai.blog) – raising concerns about data privacy, compliance, and control within regulated organizations. In response, OpenAI launched **ChatGPT Enterprise** in August 2023 as "another step towards an AI assistant for work that helps with any task" and "protects your company data" ([8] openai.com) ([9] openai.com). The Enterprise edition was explicitly marketed as delivering "enterprise-grade security & privacy" and the **"most powerful version of ChatGPT yet"**, with unlimited higher-speed GPT-4 (and later GPT-5) access, 32k context windows, and advanced data analysis (Code Interpreter) ([1] openai.com) ([10] openai.com).

Key differentiators of ChatGPT Enterprise (versus consumer or basic plans) include **data controls and guarantees**: for example, OpenAI commits that "we do not train our models on your data by default," and that users "own and control" their inputs/outputs ([2] openai.com). Enterprise customers can specify **data residency** (choosing one of 10 global regions for data storage) and even use **customer-managed encryption keys (EKM)** to encrypt all content ([11] help.openai.com) ([12] www.techradar.com). Administratively, the Enterprise plan introduces a secure multi-user environment (workspaces) with granular permissions. A new **Global Admin Console** (announced in late 2025) allows an organization to centrally manage multiple workspaces and deployments across ChatGPT and OpenAI's API platform, including domain verification and SSO configuration spanning all accounts ([5] help.openai.com) ([13] help.openai.com).

The result is that, by April 2026, ChatGPT Enterprise has become a major force in AI adoption. OpenAI reports ~50 million paying customers and the company's *$2 billion/month* revenue reflects this enterprise demand – about 40% of revenue comes from business clients ([6] www.techradar.com). Tech Radar notes that OpenAI's APIs now process **15 billion tokens per minute**, underscoring massive usage by enterprises and developers ([14] www.techradar.com). This popularity has led to an ecosystem of third-party consulting, security auditing (e.g. [25]), and integration with enterprise compliance tools (e.g. Microsoft Purview ([15] learn.microsoft.com)). In the sections that follow, we explore **all aspects** of ChatGPT Enterprise configuration and control, with liberal citation of official documentation (mainly OpenAI's Help Center and blog) and industry analysis.

ChatGPT Enterprise and Plan Comparison

ChatGPT Enterprise builds on OpenAI's core ChatGPT platform but adds features tailored to organizational needs.Table 1 contrasts the *key administrative and security features* available in ChatGPT Enterprise relative to the standard Business (formerly "Team") plan and individual/Plus plans. (Note: OpenAI renamed "ChatGPT Team" to "ChatGPT Business" in Aug 2025; this table treats Business as the mid-range subscription.) Only the Enterprise plan offers the full suite of governance controls (domain SSO, SCIM, RBAC, compliance logs, etc.) identified below ([1] openai.com) ([16] help.openai.com).

Feature / Capability	ChatGPT Enterprise	ChatGPT Business (Team)	Free/Plus Personal
SSO & Domain Verification	Yes – full SAML/OIDC support; domain ownership required for SSO ([17] help.openai.com)	Yes – supports SAML SSO (with domain verification)	No
SCIM User Provisioning	Yes – SCIM directory sync (Okta, Azure AD, etc.) to auto-provision users/groups ([18] help.openai.com)	Limited – manual/user-managed (no SCIM)	No
Role-Based Access Control (RBAC)	Yes – create custom roles/groups, granular feature permissions ([16] help.openai.com) ([4] help.openai.com)	No (single default admin/member roles only)	No
IP Allowlisting	Yes – restrict login access to whitelisted IP addresses ([19] help.openai.com)	No	No
City/Region Data Residency	Yes – choose one of 10 global regions for data storage ([12] www.techradar.com)	Partial – Business customers share same regions as Ent. (see [58])	No
Customer-Managed Encryption Keys (EKM)	Soon – integrate with AWS/Azure/GCP KMS ([11] help.openai.com)	No	No
Privacy/Data Handling	Full enterprise commitments: no training on your data by default; AES-256/TLS encryption; SOC 2, ISO 27001 compliance ([2] openai.com) ([1] openai.com)	Similar encryption & compliance, but data-handling defaults as in Plus (not enterprise pledges)	Data may be used (unless user opts out)
Analytics & Audit Logs	Yes – workspace usage analytics; Compliance Logs API (export immutable chat/auth logs) ([20] help.openai.com) ([21] help.openai.com)	No – no built-in audit/log export beyond basic usage stats	No
Max Token/Context Window	32K tokens (32k context for chat/GPT-4) ([10] openai.com)	8K–16K tokens (depending on model)	4K–8K (GPT-3.5 default)
GPT Model Access	Unlimited GPT-4 and (optional) GPT-5 models, faster speed; Codex (code) and browsing agents; advanced tools (no caps) ([10] openai.com)	GPT-4 access (may be capped or slower), no premium Codex seats unless separately purchased	GPT-4 → Plus plan; GPT-3.5 only on Free
Custom GPTs & Plugins	Yes – create and manage internal GPTs; enterprise may vet or restrict public GPTs; enterprise code/plugins isolated ([4] help.openai.com)	Yes – also available, but fewer admin controls to review public GPTs	Yes (Plus has custom GPTs)
3rd-Party "Apps" & Connectors	Enabled/Disabled by admin (off by default); full control per-app and per-action ([22] help.openai.com) ([23] help.openai.com)	Enabled by default; limited admin blocking	Enabled by default (user opt-in through store)
Workspace Roles	Multiple built-in roles (Owner, Admin, custom) with seats controls ([24] help.openai.com); allocate seats via SCIM	Owners/Admins vs members; no custom roles; seats by invite only	N/A
Seat Types & Spend Controls	Yes – dedicated "ChatGPT" vs "Codex" seat types; admins set defaults and budget/spend controls ([24] help.openai.com) ([25] help.openai.com)	Business seats (no seat differentiation); no spend controls setup	N/A

Feature / Capability	ChatGPT Enterprise	ChatGPT Business (Team)	Free/Plus Personal
AI Policy Modal	Yes – define an organization-wide AI usage policy; shown to users on login update ([26] help.openai.com)	No	No

Table 1: Comparing key administrative, security, and feature differences between ChatGPT Enterprise and other plans (data from OpenAI documentation and announcements). Sources: OpenAI help docs and blogs ([1] openai.com) ([16] help.openai.com) ([12] www.techradar.com).

The table highlights that **only the Enterprise tier** offers true enterprise-grade controls like domain SSO, SCIM provisioning, RBAC, IP whitelisting, dedicated data-residency/keys, and compliance log exports. Non-Enterprise plans (Business or personal) lack these features or offer them in much more limited form. For example, SCIM auto-provisioning is an Enterprise-only feature ([18] help.openai.com), and while Plus or Business users can create chat logs, only Enterprise customers can export detailed **immutable audit logs** through the Compliance API ([20] help.openai.com). Moreover, Enterprise customers benefit from the largest context windows and model access (e.g. 32K tokens contexts and prioritized GPT-5 models) ([10] openai.com), reflecting their higher usage needs.

Identity and Access Management

A cornerstone of enterprise administration is **centralized access control**. ChatGPT Enterprise provides *single sign-on (SSO)* and *user provisioning* to integrate with corporate identity systems. Administrators must verify their organization's domain (via a DNS TXT record) before enabling SSO ([27] help.openai.com). Once verified, the Global Admin Console (or local Workspace "Identity & access" settings) allows configuration of SAML/OIDC connections to an IdP (e.g. Okta, Azure AD, Google Workspace) ([17] help.openai.com) ([27] help.openai.com). This means users log in with corporate credentials, and administrators can force SSO enforcement or make it optional. OpenAI's docs warn that "users will be locked out if SSO is not set up correctly" and recommend testing carefully during rollout ([28] help.openai.com).

Once SSO is established, **SCIM provisioning** can be enabled to automate user and group management ([18] help.openai.com). ChartGPT's SCIM integration (via WorkOS) supports leading providers (Okta, Entra ID/Azure AD, Google Workspace, OneLogin, etc.) ([18] help.openai.com). With SCIM turned on, assigning or removing a user in the company directory automatically invites or deactivates the account in ChatGPT. Administrators can sync directory groups as ChatGPT "Projects" or to assign RBAC roles (see below) ([29] academy.openai.com) ([30] help.openai.com). Slack/governance tools: Company's SCIM sync typically runs every ~30–40 minutes; and owners can distinguish SCIM-provisioned accounts from manually added users in the workspace settings ([31] help.openai.com) ([30] help.openai.com). Importantly, SCIM is only available on high-tier (Enterprise/Custom) plans ([32] help.openai.com), reinforcing its enterprise focus.

In addition, Enterprise workspaces can enforce **IP allowlisting**. This lets administrators restrict ChatGPT access to corporate networks or VPN IP ranges. The release notes state that "Enterprise and Edu workspaces can now enable IP allowlisting to control which IP addresses can access ChatGPT and the Compliance API" ([19] help.openai.com). When turned on, only logins from approved networks are permitted. (IP allowlisting is always enforced on Compliance API access and is specific to ChatGPT web access; it does not cover the OpenAI API endpoints ([19] help.openai.com) ([33] help.openai.com).) This control is particularly valuable for highly regulated industries to ensure that only known internal networks can reach the ChatGPT service.

Finally, identity controls include the ability to create organizational **groups** and **custom roles**. As described below, these interoperate with SSO/SCIM. For example, synced directory groups can populate ChatGPT user groups, and those groups can be assigned roles or projects in ChatGPT. Administrators can even require Multi-Factor Authentication (MFA) via their IdP for ChatGPT logins, although OpenAI's console does not manage MFA itself (the IdP does that). In sum, ChatGPT Enterprise integrates tightly with existing corporate identity providers to bring ChatGPT logins under enterprise IT policies ([17] help.openai.com) ([18] help.openai.com).

Workspace Administration and RBAC

Within ChatGPT Enterprise, users belong to a **Workspace** – an organization-wide environment managed by Owners and Admins. The Workspace Settings interface (accessed via chatgpt.com/admin) gives fine control over how ChatGPT is used. As OpenAI documentation explains, from the Settings area "workspace owners and admins can manage members, seat defaults, feature access, GPT governance, apps, analytics, and identity controls" ([3] help.openai.com). Key components include:

- **Workspace Profile:** Owners can update the workspace's name, display image, and domain identifier. A policy modal (editable under "General") can be configured to present organization-specific AI usage guidelines to all users every 30 days ([34] help.openai.com). This helps enforce internal AI policies or compliance reminders.
- **Members and Groups:** Owners/administrators can invite or remove users, assign them *seat types* (e.g. ChatGPT seat vs Codex seat), and view pending invites. If SCIM is on, most provisioning is automatic into a default seat type (configurable by the admin); the docs note that admins should set a default seat type *before* enabling SCIM, since "SCIM-provisioned users follow the workspace's default seat type" ([35] help.openai.com). Users can be organized into **groups** (either created in ChatGPT or synced from the directory). Groups simplify assigning permissions to teams – for example a "Marketing" group might have access to certain GPTs or apps, while "Developers" have others.
- **Permissions & Roles:** Under the "Permissions & roles" tab, admins set feature access controls. There is a workspace-wide "default role" that applies to all users without a custom role. More importantly, ***custom roles*** can be defined and assigned to one or more groups. The RBAC documentation (updated Jan 2026) explains: *"Workspace Owners will gain RBAC functionality…where they can create custom roles with granular permissions"* ([16] help.openai.com). Administrators can create roles (e.g. "Engineer"), toggle which ChatGPT features those roles allow, and then assign roles to groups ([36] help.openai.com). Permissible toggles include: enabling use of the ChatGPT agent mode, the Canvas coding tool, Codex (code assistant) and its internet access, creating/reusing **Custom GPTs**, sharing knowledge via Memory, and even data/actions like web search or sending emails via apps ([4] help.openai.com). In effect, RBAC lets the organization safely enable sophisticated features for vetted teams while disabling them for others.

For example, an admin could create a role permitting only *read-only* actions in certain connected apps, or restrict GPT creation to a "Dev" group. The RBAC FAQ confirms this: *"Permissions include: Canvas (code execution and network access), ChatGPT agent, Codex use, Apps, GPTs (creation, editing, sharing), Project creation, Record (memory notes), Search (web/agent mode), [and] Shared projects"* ([37] help.openai.com). Role inheritance is additive, so a user in multiple groups has the union of those permissions. By default, thread/actions access can also be controlled: admins "can control access to apps on a per-app basis and for select apps, on a per-action basis" ([38] help.openai.com).

- **Seat Defaults and Spend Controls:** Alongside roles, admins manage **seats**. Seats grant service access: a "ChatGPT seat" for the chat interface, or a "Codex seat" for coding jobs (if purchased). Administrators can set how many seats of each type exist and assign them. Enterprise also allows *spend controls*: budgets and rate limits on token usage per chat or project. This is a new feature; for instance, in April 2026 OpenAI announced a new "Codex seat" model (credit-based billing for code usage) and a discount on chat seat pricing ([25] help.openai.com). Under Spend Controls, admins can cap monthly usage to prevent surprise overages – especially important as model usage (e.g. GPT-4 tokens) is metered. The workspace settings enable assigning free preview credits or credits for Codex, and they handle any billing/shipping of credits ([25] help.openai.com).

In summary, the Workspace settings UI exposes nearly all administrative controls in a business-friendly interface. The end-to-end flow is: corporate IT sets up identity (SSO/SCIM, domain), then workspace Owners invite or import users under that domain, define groups and roles, and then toggle feature flags to enforce company policy. The flexibility of RBAC and Groups ensures large enterprises can scale ChatGPT usage securely. (For an example workflow, see the Q&A in OpenAI's RBAC doc ([39] help.openai.com) and enterprise SSO guide ([17] help.openai.com).)

Data Security, Privacy, and Compliance Controls

A crucial appeal of ChatGPT Enterprise is its **data governance and security assurances**. OpenAI's enterprise privacy commitments emphasize that **customer data** (inputs like prompts and outputs like generated text) remains under customer control. Key guarantees include "We do not train our models on your data by default" and "you own your inputs and outputs" ([2] openai.com). All content is encrypted in transit (TLS 1.2+) and at rest (AES-256) ([40] openai.com) ([41] www.techradar.com). Conversations and files can be stored in customer-chosen regions to meet jurisdictional requirements ([12] www.techradar.com). In practice, this means that neither prompts nor responses from ChatGPT Enterprise enter OpenAI's public training pipeline, and admins can adjust how long logs are kept.

Specifically, Enterprise admins can configure **data retention**. Within workspace settings, owners can choose how long chat histories and memory are retained (e.g. number of days, or never). By default, data is not shared with human reviewers – and in compliance mode, customer content is locked to the Enterprise logs only. The OpenAI Compliance Platform (for Enterprise) allows exporting logs and data to an enterprise SIEM or e-discovery system ([20] help.openai.com). According to OpenAI, the Compliance Logs Platform provides "append-only compliance log events" and a stateful query API, enabling archives of all chat/auth events ([20] help.openai.com). Logs are retained for 30 days by default on OpenAI's side ([42] help.openai.com), but customers can offload them to storage to meet longer-term retention needs.

Besides retention, enterprises may need **external key management**. In Dec 2025 OpenAI announced **Enterprise Key Management (EKM)**: the ability to use the organization's own cloud KMS (Google, AWS, Azure) to encrypt all customer content ([11] help.openai.com). With EKM enabled, even OpenAI's services cannot decrypt the data without the enterprise's permission. This feature "allows organizations to encrypt all customer content using their own external Key Management System," adding a strong compliance layer ([11] help.openai.com). Initially available for Enterprise/Edu workspaces (with API to follow), EKM lets regulated industries (finance, government) meet strict data sovereignty demands.

From a compliance standpoint, ChatGPT Enterprise also provides **detailed audit logs**. All admin actions (workspace changes, role edits, SSO logins) can be traced. In mid-2025 OpenAI integrated ChatGPT logs with its broader "OpenAI Compliance Logs Platform" for enterprises ([43] help.openai.com). Released Dec 2025, this consolidation means workspace modifications, authentication activities, and even Codex usage become queryable audit data ([43] help.openai.com). These logs can be fed into SIEM and eDiscovery tools. For example, Microsoft Purview (for customers on Azure AD/Entra) captures ChatGPT interactions in the unified audit log ([15] learn.microsoft.com). Purview's DSPM (Data Security Posture Management) can then analyze ChatGPT prompts and responses alongside other enterprise data flows ([15] learn.microsoft.com). This cross-tool integration lets legal/compliance teams search for AI usage (even including AI-generated emails stored in Exchange) and apply governance policies (retention or deletion) on AI-generated content ([44] learn.microsoft.com) ([45] learn.microsoft.com).

Finally, admins can disable or restrict advanced features that pose risk. For instance, the **Web Browsing (Agent) mode** is powerful but can pull in external content. ChatGPT Enterprise/Edu lets organizations request domain blocklists for the agent; an admin can contact OpenAI to block browsing or actions to specific sites or subdomains ([46] help.openai.com). This prevents the agent from accessing classified intranets or competitor websites. Similarly, admins can review and disable insecure plugins or app integrations (e.g. apps that send data to third parties). In release notes, OpenAI explicitly notes "Available to [Enterprise] admins: review app actions, set RBAC, enable/disable new actions or connectors" (for Slack, SharePoint, etc.) ([47] help.openai.com) ([48] help.openai.com). In short, the combination of encryption, keys, residency, retention policies, and audit logging in ChatGPT Enterprise underpins a compliance framework that meets industry standards (GDPR, HIPAA, SOC2, etc.).

Integrations, Customization, and Tools

Beyond basic chat, Enterprise editions provide extensive integration options and toolkits:

- **Premium Models and Tools**: Enterprise users get **unlimited, high-speed GPT-4** (and GPT-5) usage with extended context windows (32K tokens) ([10] openai.com). The advanced **Codex** code engine (formerly Code Interpreter) is included without usage caps; in 2026 OpenAI even introduced **"Codex seats"** for scaled coding: organizations can purchase usage-based Codex licenses separate from normal chat seats ([25] help.openai.com). Enterprise admins can enable or disable Codex access per role. In December 2025, OpenAI released **GPT-5-codex**, a variant of GPT-5 optimized for agentic coding, which is used behind the scenes in Codex and will gradually become available everywhere Codex is used ([49] help.openai.com). This means firms can run automated code analysis and generation tasks within ChatGPT, controlled by admin settings.

- **Custom GPTs and Plugins**: Custom GPTs ("GPT-powered apps") allow teams to build specialized assistants with their own instructions and behavior. In Enterprise, these are first-class objects: admins can see all workspace GPTs (with metadata) and must approve any external actions they trigger. The RBAC system in Workspace Settings governs who can create, share or delete these GPTs ([4] help.openai.com). Plugins (integrations packaged as GPTs) from the ChatGPT plugin store are available but can be restricted. Because plugins may call external APIs, enterprises treat them as potential data exfiltration pathways – policy must govern which plugins are trusted. Admins can disable plugins entirely at the workspace level, or selectively allow only IT-vetted plugins.

- **First-Party "Apps" (Connectors)**: ChatGPT Enterprise comes with a library of productivity app connectors to fetch or act on data from business systems. Examples include Google Drive/Sheets/Docs, Microsoft Outlook/Teams/SharePoint, Slack, Zoom, Atlassian, Salesforce, Shopify, Zendesk, and many others. Administrators control these connectors in the "Apps" tab of workspace settings. By default (unlike Business, where apps are on), Enterprise starts with connectors **disabled**; admins selectively enable needed ones ([50] help.openai.com). For each enabled connector, admins review and approve the specific **actions** it can take. OpenAI's release notes describe a refreshed UI where admins can "enable actions, including sync where supported" for each connector ([51] help.openai.com). For example, in late 2025 admins could deploy a new **Atlassian Rovo** connector, which brings Jira/Confluence context into ChatGPT (and even allows creating Jira issues via chat) ([52] help.openai.com). Google's connector was unified under "Google Drive" so that Docs/Sheets/Slides are accessed via one interface ([22] help.openai.com). In all cases, admins decide who can link and use each app (via roles) and can turn off any undesired write actions.

- **Company Knowledge and MCP**: A notable feature for enterprises is **Company Knowledge**. This allows loading organizational documents (via approved connectors) into ChatGPT as background knowledge. In November 2025 OpenAI updated Company Knowledge to support **custom MCP connectors**: organizations can bring in internal data sources (e.g. proprietary databases) via self-built connectors ([53] help.openai.com). Once enabled, allowable content from these sources is indexed and cited in ChatGPT answers. Administrators govern which connectors' data is available and to whom. There is also a developer mode where an organization's data scientists can build and test new connectors using OpenAI's Model Context Protocol (MCP) and then have them reviewed and published to their workspace. In short, enterprises gain a searchable knowledge repository integrated into ChatGPT, expanding its utility for company-specific Q&A.

- **Canvas & Projects**: New collaboration tools in ChatGPT, like the Canvas coding environment and shared Projects, are also under policy. Admins can disable the Canvas (which executes code) for certain roles under RBAC ([37] help.openai.com). Shared Projects (file-and-instruction sets sharable among users) were introduced in 2025; in Enterprise these can be shared across teams, but admins could limit sharing settings.

- **Memory and Fine-Tuning**: Enterprise customers can use ChatGPT's "Memory" to store organization-specific facts and preferences. Admins have the option to disable memory altogether for privacy, or moderate what types of memory can be written. Similarly, although not widely offered as of April 2026, any future fine-tuning of models would be restricted: custom models created via the OpenAI API are private to the customer ([54] openai.com).

Table 2 (below) summarizes the main **administration panes and settings** in a ChatGPT Enterprise workspace, and the scope of what each controls. It highlights how virtually every aspect of the AI assistant's behavior and integrations can be adjusted by administrators.

Workspace Setting	Function	Administration Scope	Documentation
General	Workspace name/image; AI policy modal	Set org ID, logo, and configure a modal shown every 30 days with usage policy/terms ([34] help.openai.com)	OpenAI Help (Workspace Settings) ([34] help.openai.com)
Members & Groups	Manage user invitations, removals, group membership	Add/remove users or admins; assign seats (ChatGPT vs Codex); create groups (manual or via SCIM) ([55] help.openai.com)	OpenAI Help (Members)
Permissions & Roles	Enable/disable core features; set RBAC	Toggle access to ChatGPT agent, Canvas, Codex, GPT creations, memory, tool use; create custom roles for groups ([37] help.openai.com)	OpenAI RBAC Guide ([16] help.openai.com)
Billing & Seats	View invoices and seat usage; purchase add-ons	Add/change ChatGPT or Codex seat types; set pass/fail rate limits or budgets (spend controls) ([25] help.openai.com)	Release Notes (Codex seats) ([25] help.openai.com)
GPTs	Manage custom GPT assistants	Review/transfer/delete GPTs; view system prompt and actions for internal/custom GPTs ([35] help.openai.com)	OpenAI Help (GPT management)
Apps & Connectors	Enable/disable integrations; configure actions	Select which apps/connectors (e.g. Slack, Google Drive) are available; assign to roles; enable sync; create custom MCP apps ([35] help.openai.com)	OpenAI Help (Apps management)
Workspace Analytics	Usage metrics and trends	View daily/weekly active users, messages/user, seat count, GPT usage, etc. ([21] help.openai.com)	OpenAI Help (Workspace Analytics) ([21] help.openai.com)
Identity & Access	Authentication and provisioning settings	Configure SSO (link to IdP), domain verification, SCIM provisioning, IP allowlists ([17] help.openai.com) ([19] help.openai.com)	OpenAI Help (SSO/SCIM)
Compliance & Logs	Data export and auditing options	Enable Compliance API; download ChatGPT audit logs; set retention time; integrate with SIEM tools ([20] help.openai.com)	OpenAI Help (Compliance API) ([20] help.openai.com)

Table 2: Key ChatGPT Enterprise workspace settings relevant to administrative control. Each pane in Workspace Settings (as highlighted in the OpenAI help docs) corresponds to strategic control over features, user access, data retention, and integrations ([21] help.openai.com) ([20] help.openai.com).

Case Studies and Real-World Examples

While OpenAI does not publicly detail enterprise deployments, several customer testimonials and reports illustrate ChatGPT Enterprise in action. OpenAI's launch announcement quotes executives from major adopters: **Klarna**'s CEO praised ChatGPT Enterprise as empowering employees to serve 150 million customers, while **Asana** reported it "cut down research time by an average of an hour per day" for its data teams ([7] openai.com) ([7] openai.com). Other early enterprise users include Block (Square), Canva, Carlyle Group, Estée Lauder, PwC, and Zapier ([56] openai.com), indicating use cases across finance, design, consulting, and tech.

Independent analyses suggest broad savings and ROI. For example, a recent survey (HumAI Blog, Dec 2025) claims Fortune 500 savings of *40+ minutes daily per employee* and "millions in ROI" via productivity gains across drafting and brainstorming tasks (www.humai.blog). In the healthcare sector, OpenAI announced **ChatGPT for Healthcare** in Jan 2026, which is a compliant, HIPAA-safe instance of ChatGPT Enterprise with integrations to medical records ([57] www.tomsguide.com). This exemplifies how vertical use cases (finance compliance, legal drafting, coding assistance at software firms) leverage enterprise ChatGPT with strict controls.

In practical terms, companies often start by restricting the model's scope. A common pilot might enable ChatGPT for non-PII tasks under a monitored channel, while IT departments analyze logs for leaks or compliance issues. Security firms recommend that enterprises *explicitly define what not to chatpenalize* – for example, forbidding sharing of customer data or proprietary code in prompts (beyondscale.tech) (beyondscale.tech). As one case shows, even well-intentioned developers at Samsung accidentally leaked proprietary source code into ChatGPT in 2023, prompting the company to

tighten usage (e.g. file size limits) (beyondscale.tech). This incident highlighted the need for policy and training (rather than solely tech fixes) to prevent sensitive data exfiltration.

On the analytics side, administrators report using the Workspace Analytics dashboard to monitor adoption. Typical metrics under watch include monthly active users, peak usage times, and which features (like file uploads or code assistant) are most used. These insights can guide internal training or detect bottlenecks in AI usage.

Overall, available anecdotes suggest that when governed properly, ChatGPT Enterprise can accelerate workflows (for research, code review, content revision) without sacrificing security. As one tech buyer magazine noted: ChatGPT has become "a catch-all copilot for email, knowledge management, customer support, and development" in enterprises ([58] www.techradar.com), with OpenAI's enterprise tools moving beyond proof-of-concept to mission-critical applications.

Security, Governance, and Risk Perspectives

While OpenAI adds many controls, enterprise security teams emphasize that **governance cannot rely solely on technical safeguards**. A detailed security guide by the firm BeyondScale (April 2026) argues that ChatGPT Enterprise's infrastructure security is strong (SOC 2, encryption, SSO), but the real attack surface is "the prompt channel" – i.e. what users type (beyondscale.tech). In their research, BeyondScale found that **34.8% of enterprise ChatGPT inputs contained sensitive data** (code, PII, financials) – more than triple the 11% rate from 2023 (beyondscale.tech). OpenAI's controls (logs, encryption) cannot automatically block these leaks. The Samsung example above illustrated this: no breach occurred, but confidential code was unknowingly sent off to ChatGPT. (beyondscale.tech).

To mitigate, BeyondScale recommends enterprises implement clear **AI usage policies** and education. They list action items such as: "Is there a written acceptable use policy that explicitly defines what categories of data cannot be entered into ChatGPT prompts?" and "Is any AI-aware DLP deployed to monitor or block sensitive data entering AI interfaces?" (beyondscale.tech). In practice, this has led some companies to route ChatGPT web traffic through supervised proxy or DLP systems that scan for corporate data. Modern DLP solutions (firewalls or endpoint agents) are starting to add "ChatGPT-aware" modules to catch sensitive information in prompts or outputs.

Another risk vector is **API key sprawl**: employees may create personal OpenAI API keys (outside the enterprise subscription) and build stealth integrations, bypassing corporate controls (beyondscale.tech). The BeyondScale report points out that this undermines governance – such usage would not appear in the ChatGPT Enterprise logs. The cure, they say, is to inventory all OpenAI usage across the company and maybe restrict external API calls. Secret-cracking research found AI-assisted code commits leak secrets at higher rates, underscoring the need to manage keys centrally (beyondscale.tech).

A further concern is the **Custom GPT and plugin ecosystem**. BeyondScale warns these are the "highest-risk component" of any deployment (beyondscale.tech). A study cited revealed 95% of Custom GPTs had inadequate protections against prompt injection attacks (beyondscale.tech). More alarmingly, security researchers demonstrated (and later patched) a vulnerability in February 2026 where a malicious custom GPT could use DNS tunneling from the code execution sandbox to exfiltrate conversation data (beyondscale.tech). Plugins add similar risk: any plugin that calls an external service could leak prompt contents out of ChatGPT's vault (and plugin data isn't protected by OpenAI's enterprise guarantees, unlike core ChatGPT data). To counter this, enterprises often disable plugins entirely or only whitelist approved ones, and conduct security reviews of any GPTs that use external APIs. RBAC is used to restrict publishing and sharing of GPTs: by default, new internal GPTs can be set private and cannot be made public without admin review (beyondscale.tech).

In summary, from a governance standpoint, ChatGPT Enterprise equips IT teams with many tools, but **policy and oversight remain crucial**. Most experts agree that technical controls must be complemented by organizational measures: explicit user training, classification of sensitive categories, regular auditing of logs (via the Compliance API),

and eventual incident response plans for AI misuse. The combination of OpenAI's built-in controls (SSO, RBAC, encryption, logs) and a disciplined security posture is what enables safe scaling of generative AI in business.

Implications and Future Directions

ChatGPT Enterprise represents a pivotal shift in how organizations adopt AI. The breadth of administrative controls and integrations shows that enterprises want both power and accountability from AI. **Looking forward**, several trends emerge:

- **Unified Admin Management:** In 2026 OpenAI introduced the **Global Admin Console** (at admin.openai.com) to address large organizations' needs for a tenant-level control plane. A Tenant can include multiple ChatGPT workspaces and API organizations, all under one SSO and verified domains ([5] help.openai.com) ([59] help.openai.com). Global Admins can manage domains and SSO for all sub-accounts, and add other Global Admin users ([13] help.openai.com). This development signals that OpenAI is moving toward enterprise IT norms (e.g. Azure's multi-tenant management) and will likely expand central policies. Future implications: multi-workspace analytics, corporate-wide security dashboards, and delegating privileges across business units.

- **Expanded Compliance Features:** OpenAI has steadily added features: data residency (10 regions as of late 2025) ([12] www.techradar.com), compliance log integrations (e.g. connectors with CrowdStrike, GlobalRelay) ([60] help.openai.com), and EKM ([11] help.openai.com). We expect more: for instance, after decoupling the stateful audit route, they may add more integrations (e.g. Splunk, and real-time alerting), as well as advanced DLP integrations. The move to align with tools like Microsoft Purview ([15] learn.microsoft.com) suggests future tighter coupling with enterprise compliance platforms.

- **Enhanced AI Collaboration:** The integration of advanced AI agents, code tools, and knowledge graphs will continue. OpenAI's mention of building an "AI superapp" combining ChatGPT, Codex, browsing, and other agentic AI ([14] www.techradar.com)points to a future where ChatGPT Enterprise might unify all work-related AI tasks. For example, one might imagine a unified interface where a single agent can read emails, query databases, generate documents, and write code, all within corporate controls. This will necessitate even finer-grained controls (e.g. per-AI-agent policies) and raises questions about human-AI teaming and oversight.

- **Market and Competition:** The enterprise AI market remains dynamic. OpenAI's dominance (78–80% of enterprise AI usage as of early 2026 ([61] www.techradar.com)) drives innovation, but competitors like Anthropic and Google are also enhancing their offerings. Gartner analysts predict that by 2027, conversational AI assistants will reach ubiquitous status in businesses ([62] www.gartner.com). Enterprises will have to evaluate data flows across multiple LLM providers. The breadth of ChatGPT Enterprise's tooling sets a high bar, so competing products will need comparable admin ecosystems.

- **Regulatory Landscape:** As governments scrutinize AI, enterprise controls will be under the microscope. The data breach lawsuit where 20 million ChatGPT logs were ordered to be handed over (NYT vs OpenAI) highlights how data residency and logging will attract regulation ([63] www.techradar.com). Enterprises must prepare to handle such requests, and OpenAI's Enterprise compliance tools (log exports, retention interfaces) will be essential. We may see formal certifications or audit reports (e.g. FedRAMP, HIPAA validation) added as well.

In conclusion, ChatGPT Enterprise offers a rich platform for organizations to leverage generative AI while maintaining control. The combination of official documentation and real-world analysis shows a continuously evolving system. Today's capabilities – from SSO and RBAC to data encryption and compliance APIs – address many of the pitfalls that general-purpose ChatGPT lacks. For IT leaders, staying current with OpenAI's updates (via the help center release notes and admin console) is critical. The trajectory suggests that by 2026 and beyond, managing AI will become a core part of IT governance, with ChatGPT Enterprise as a leading example.

All claims and data above are drawn from OpenAI's official documentation and credible analyses. Key sources include OpenAI's Help Center articles (linked throughout this report) ([3] help.openai.com) ([16] help.openai.com) ([20] help.openai.com), OpenAI's product announcements ([1] openai.com) ([12] www.techradar.com), financial/industry reporting ([6] www.techradar.com), and security research (beyondscale.tech) (beyondscale.tech). Readers should consult the latest OpenAI documentation for up-to-date details on enterprise features (links provided above) and consider independent expert guidance (e.g. security assessments) when deploying ChatGPT in a corporate environment.

External Sources

[1] https://openai.com/index/introducing-chatgpt-enterprise/#:~:You%2...

[2] https://openai.com/policies/api-data-usage-policies?%25253Butm_content=17950474&%25253Butm_medium=email&%25253Butm_source=hs_email#:~:You%2...

[3] https://help.openai.com/en/articles/8411955-managing-workspace-settings-in-chatgpt-enterprise#:~:From%...

[4] https://help.openai.com/articles/11750701#:~:You%2...

[5] https://help.openai.com/en/articles/12289294-global-admin-console#:~:The%2...

[6] https://www.techradar.com/pro/we-are-growing-revenue-four-times-faster-than-the-companies-who-defined-the-internet-and-mobile-eras-openai-says-its-making-usd2-billion-a-month-mostly-from-enterprise-users#:~:As%20...

[7] https://openai.com/index/introducing-chatgpt-enterprise/#:~:,%E2%...

[8] https://openai.com/index/introducing-chatgpt-enterprise/#:~:We%E2...

[9] https://openai.com/index/introducing-chatgpt-enterprise/#:~:Prote...

[10] https://openai.com/index/introducing-chatgpt-enterprise/#:~:ChatG...

[11] https://help.openai.com/en/articles/10128477-chatgpt-enterprise-edu-release-notes%23.webm#:~:Enter...

[12] https://www.techradar.com/pro/openai-now-lets-business-customers-choose-where-their-chatgpt-data-is-hosted#:~:Eligi...

[13] https://help.openai.com/en/articles/12289294-global-admin-console#:~:...

[14] https://www.techradar.com/pro/we-are-growing-revenue-four-times-faster-than-the-companies-who-defined-the-internet-and-mobile-eras-openai-says-its-making-usd2-billion-a-month-mostly-from-enterprise-users#:~:reven...

[15] https://learn.microsoft.com/en-us/purview/ai-chatgpt-enterprise#:~:Like%...

[16] https://help.openai.com/articles/11750701#:~:RBAC%...

[17] https://help.openai.com/en/articles/10472980-enabling-sso-on-chatgpt#:~:In%20...

[18] https://help.openai.com/en/articles/10011769#:~:Which...

[19] https://help.openai.com/en/articles/10128477-chatgpt-enterprise-edu-release-notes%23.webm#:~:IP%20...

[20] https://help.openai.com/es-es/articles/9261474-openai-compliance-platform-for-enterprise-customers#:~:The%2...

[21] https://help.openai.com/en/articles/8411955-managing-workspace-settings-in-chatgpt-enterprise#:~:Works...

[22] https://help.openai.com/en/articles/11509118-admin-controls-security-and-compliance-in-connectors-enterprise-edu-and-team?hsPreviewerApp=page#:~:For%2...

[23] https://help.openai.com/en/articles/10128477-chatgpt-enterprise-edu-release-notes%23.webm#:~:Intro...

[24] https://help.openai.com/en/articles/8411955-managing-workspace-settings-in-chatgpt-enterprise#:~:Works...

[25] https://help.openai.com/en/articles/11391654-chatgpt-team-release-notes#:~:New%2...

[26] https://help.openai.com/en/articles/8411955-managing-workspace-settings-in-chatgpt-enterprise#:~:When%...

[27] https://help.openai.com/en/articles/10472980-enabling-sso-on-chatgpt#:~:Domai...

[28] https://help.openai.com/en/articles/10472980-enabling-sso-on-chatgpt#:~:%E2%9...

[29] https://academy.openai.com/public/clubs/admins-6o6xf/resources/scim#:~:3,fea...

[30] https://help.openai.com/en/articles/10011769#:~:In%20...

[31] https://help.openai.com/en/articles/10011769#:~:Can%2...

[32] https://help.openai.com/en/articles/10011769#:~:SCIM%...

[33] https://help.openai.com/en/articles/10128477-chatgpt-enterprise-edu-release-notes%23.webm#:~:Note%...

[34] https://help.openai.com/en/articles/8411955-managing-workspace-settings-in-chatgpt-enterprise#:~:Owner...

[35] https://help.openai.com/en/articles/8411955-managing-workspace-settings-in-chatgpt-enterprise#:~:...

[36] https://help.openai.com/articles/11750701#:~:Membe...

[37] https://help.openai.com/articles/11750701#:~:%2A%2...

[38] https://help.openai.com/articles/11750701#:~:Note%...

[39] https://help.openai.com/articles/11750701#:~:What%...

[40] https://openai.com/policies/api-data-usage-policies?%25253Butm_content=17950474&%25253Butm_medium=email&%25253Butm_source=hs_email#:~:Compr...

[41] https://www.techradar.com/pro/openai-now-lets-business-customers-choose-where-their-chatgpt-data-is-hosted#:~:The%2...

[42] https://help.openai.com/es-es/articles/9261474-openai-compliance-platform-for-enterprise-customers#:~:Data%...

[43] https://help.openai.com/en/articles/10128477-chatgpt-enterprise-edu-release-notes%23.webm#:~:The%2...

[44] https://learn.microsoft.com/en-us/purview/ai-chatgpt-enterprise#:~:Data%...

[45] https://learn.microsoft.com/en-us/purview/ai-chatgpt-enterprise#:~:Becau...

[46] https://help.openai.com/en/articles/10128477-chatgpt-enterprise-edu-release-notes%23.webm#:~:Websi...

[47] https://help.openai.com/en/articles/10128477-chatgpt-enterprise-edu-release-notes%23.webm#:~:Admin...

[48] https://help.openai.com/en/articles/10128477-chatgpt-enterprise-edu-release-notes%23.webm#:~:ChatG...

[49] https://help.openai.com/en/articles/10128477-chatgpt-enterprise-edu-release-notes%23.webm#:~:We%E2...

[50] https://help.openai.com/en/articles/10128477-chatgpt-enterprise-edu-release-notes%23.webm#:~:For%2...

[51] https://help.openai.com/en/articles/11509118-admin-controls-security-and-compliance-in-connectors-enterprise-edu-and-team?hsPreviewerApp=page#:~:app%2...

[52] https://help.openai.com/en/articles/10128477-chatgpt-enterprise-edu-release-notes%23.webm#:~:Addin...

[53] https://help.openai.com/en/articles/10128477-chatgpt-enterprise-edu-release-notes%23.webm#:~:Custo...

[54] https://openai.com/policies/api-data-usage-policies?%25253Butm_content=17950474&%25253Butm_medium=email&%25253Butm_source=hs_email#:~:%2A%2...

[55] https://help.openai.com/en/articles/8411955-managing-workspace-settings-in-chatgpt-enterprise#:~:Use%2...

[56] https://openai.com/index/introducing-chatgpt-enterprise/#:~:Since...

[57] https://www.tomsguide.com/ai/chatgpt/openai-launches-chatgpt-health-bringing-medical-records-and-wellness-data-into-chatgpt#:~:2026,...

[58] https://www.techradar.com/pro/openai-models-are-the-favorites-for-enterprise-users-right-now-but-anthropic-isnt-far-behind#:~:model...

[59] https://help.openai.com/en/articles/12289294-global-admin-console#:~:Intro...

[60] https://help.openai.com/es-es/articles/9261474-openai-compliance-platform-for-enterprise-customers#:~:To%20...

[61] https://www.techradar.com/pro/openai-models-are-the-favorites-for-enterprise-users-right-now-but-anthropic-isnt-far-behind#:~:2026,...

[62] https://www.gartner.com/en/documents/6273683#:~:Predi...

[63] https://www.techradar.com/ai-platforms-assistants/chatgpt/your-chatgpt-chats-could-be-less-private-than-you-thought-heres-what-a-new-openai-court-ruling-means-for-you#:~:2025,...

DISCLAIMER

The information contained in this document is provided for educational and informational purposes only. We make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability of the information contained herein.

Any reliance you place on such information is strictly at your own risk. In no event will IntuitionLabs.ai or its representatives be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from the use of information presented in this document.

This document may contain content generated with the assistance of artificial intelligence technologies. AI-generated content may contain errors, omissions, or inaccuracies. Readers are advised to independently verify any critical information before acting upon it.

All product names, logos, brands, trademarks, and registered trademarks mentioned in this document are the property of their respective owners. All company, product, and service names used in this document are for identification purposes only. Use of these names, logos, trademarks, and brands does not imply endorsement by the respective trademark holders.

IntuitionLabs.ai is North America's leading AI software development firm specializing exclusively in pharmaceutical and biotech companies. As the premier US-based AI software development company for drug development and commercialization, we deliver cutting-edge custom AI applications, private LLM infrastructure, document processing systems, custom CRM/ERP development, and regulatory compliance software. Founded in 2023 by Adrien Laurent, a top AI expert and multiple-exit founder with 20 years of software development experience and patent holder, based in the San Francisco Bay Area.

This document does not constitute professional or legal advice. For specific guidance related to your business needs, please consult with appropriate qualified professionals.