ANTHROPIC

## Claude for Government (C4G)

# FedRAMP Secure Configuration Guide

Administrative roles, account lifecycle, security settings, and secure defaults for top-level administrative and privileged accounts.

| | |
|---|---|
| **Document title** | **C4G FedRAMP Secure Configuration Guide** |
| **Cloud service offering** | **Claude for Government (C4G), operated on claude.fedstart.com** |
| **Version** | **2.2** |
| **Date** | **November 17, 2026** |
| **Prepared by** | **Anthropic — US Public Sector Compliance** |
| **Satisfies** | **FedRAMP Rev5 Secure Configuration Guide Balance Improvement Release (BIR) — SCG-CSO-RSC, SCG-CSO-AUP, SCG-CSO-PUB, SCG-CSO-SDF, and SCG-ENH-* enhanced capabilities. Mandatory for all FedRAMP Rev5 cloud services as of March 1, 2026.** |
| **Supersedes** | **C4G FedRAMP Secure Configuration Guide v2.1** |
| **Availability** | **Intended for public release** |

## Document Control & Version History

SCG-ENH-VRH (SHOULD): FedRAMP recommends maintaining versioning and a release history for recommended secure-default settings as they change over time. This table satisfies that recommendation.

| Version | Date | Summary of changes |
|---|---|---|
| **1.0** | **Prior release** | **Initial C4G Security Admin Guide. Provided role definitions, account lifecycle procedures (SSO, SCIM), the Compliance API description, and public support links to demonstrate FRR-RSC-01, FRR-RSC-02, and FRR-RSC-09.** |
| **2.0** | **May 27, 2026** | Restructured to the FedRAMP Rev5 Secure Configuration Guide BIR framework and standardized control IDs (SCG-CSO-* / SCG-ENH-*). Specifically:<br>• Added explicit Required vs. Recommended designations.<br>• Added a security-settings reference table (function, security impact, recommended secure default).<br>• Added secure defaults, administrative-account decommissioning, enhanced capabilities, and a requirement traceability matrix.<br>• Added the Admin Seat Tier & Spend Cap Setup as a recommended configuration. |
| 2.1 | July 16, 2026 | Updated for the C4G Claude Desktop release. Specifically:<br>• Aligned role terminology (§1.6, §2.1) with the current Tenant Administrator / Primary Owner / Owner / User model. |

| Version | Date | Summary of changes |
|---|---|---|
| | | • Corrected §2.2 (Usage Analytics is now available in the admin portal; data-export and retention wording updated for device-local conversation storage).<br>• Revised §5 and the related §4 rows: Compliance API is enabled by default and returns governance/audit events only; endpoint-side OpenTelemetry export added.<br>• Added Recommended rows to §4 for Admin Console settings (Cowork egress allowlist, Allowed workspace folders, Product tab enablement, Managed MCP connectors, Organization plugins, Microsoft 365 connector, OTLP telemetry endpoint, Desktop banner), managed-configuration keys (Disable claude.ai sign-in, Auto mode policy, Per-tool approval policy, Auto-update control), and the tenant-restrictions perimeter header.<br>• Corrected internal §7 cross-references to §5. |
| 2.2 | November 17, 2026 | Updated for the retirement of Claude for Government Web and for product changes since v2.1. Specifically:<br>● Replaced the Web procedures in §3 with those for the tenant and organization admin portals.<br>● Replaced the Magic-link login row: the emailed sign-in link cannot be turned off, so §4 now gives compensating steps. |

| Version | Date | Summary of changes |
|---|---|---|
| | | • Corrected audit-record availability in §2.2, §3.4, §4, and §5: the Compliance API serves the most recent 30 days.<br>• Corrected §5: the Compliance API address, how conversation content reaches the model, and what the local audit log provides.<br>• Added the Analytics API (off by default). An organization's Compliance API keys are now admin API keys, and a new key can be given access to usage and cost reports.<br>• Added §4 rows, including Session idle timeout and Maximum session length.<br>• Changed Disable claude.ai sign-in from Recommended to Required (October 13, 2026) and added the deploymentMode key.<br>• Updated §4 setting names, locations, scope, and who configures each setting. |

# Contents

Document Control & Version History 3
Contents 6
1. Introduction 8
1.1 Purpose and scope 8
1.2 Audience 8
1.3 How this guide maps to FedRAMP requirements 8
1.4 How to obtain and use this guide 8
1.5 How to read the designations 8
1.6 Terminology and how administrative accounts are named in C4G 9
2. Administrative roles and permissions 10
2.1 Role definitions 10
2.2 Permissions that behave differently on C4G 10
3. Administrative account lifecycle 11
3.1 Secure access — single sign-on (SSO) 11
Step 1 — First sign-in 11
Step 2 — Verify your domain 11
Step 3 — Configure your identity provider (IdP) 11
Step 4 — Enter your IdP details 11
Step 5 — Test 11
Step 6 — Add routing rules 11
3.2 Configuration — SCIM provisioning 12
Step 1 — Generate a SCIM token 12
Step 2 — Configure your identity provider 12
Step 3 — Place people and verify the first sync 12
3.3 Operation — ongoing administration 13
SCIM troubleshooting 13
3.4 Decommissioning 13
4. Security settings reference table 14
5. Compliance API 30
Activity Feed — governance and audit events 30

Endpoint-side logging (customer-collected) 30
Analytics API — usage and cost reports 31

# 1. Introduction

## 1.1 Purpose and scope

This Secure Configuration Guide tells agency customers of Claude for Government (C4G) how to securely access, configure, operate, and decommission the administrative accounts that control their organization, and explains the security-related settings those accounts manage. It is the C4G response to the FedRAMP Rev5 Secure Configuration Guide Balance Improvement Release (BIR), which became a mandatory requirement for all FedRAMP Rev5 cloud services on March 1, 2026.

## 1.2 Audience

The primary audience is the agency customer's top-level administrators (Tenant Administrators and Primary Owners) and the privileged administrators (Owners) they delegate to. Identity, security, and compliance staff configuring SSO, SCIM, and audit integrations are secondary audiences.

## 1.3 How this guide maps to FedRAMP requirements

FedRAMP standardized the Secure Configuration Guide control identifiers in the v0.9.0-beta release. The former identifiers used by the prior version of this document map to the current ones as follows:

- **FRR-RSC-01 / FRR-RSC-02** → SCG-CSO-RSC — the content of the Secure Configuration Guide itself (admin-account lifecycle and security-setting explanations).
- FRR-RSC-03 →
- **FRR-RSC-09** → SCG-CSO-PUB — public availability of the guide.
- **FRR-RSC-04** → **SCG-CSO-SDF; FRR-RSC-05–08, 10** → **SCG-ENH-CMP / EXP / API / MRG / VRH** — secure defaults and the enhanced capabilities, addressed in §5.

Section 8 provides a full requirement traceability matrix.

## 1.4 How to obtain and use this guide

> **SCG-CSO-AUP (MUST) & SCG-CSO-PUB (SHOULD):** Providers must include instructions in the FedRAMP authorization package explaining how to obtain and use the Secure Configuration Guide, and should make it publicly available.

This guide is publicly available on the Anthropic Trust Center (trust.anthropic.com), under FedRAMP resources, and upon request through your Anthropic representative or fedramp@anthropic.com. The supporting C4G documentation linked throughout (claude.com/docs/government) is likewise publicly accessible and is intended to remain at stable URLs.

## 1.5 How to read the designations

Throughout this guide, each configuration item carries one of two designations:

- **Required** — the customer should apply this as part of the baseline secure configuration of C4G. These are the controls that protect the confidentiality and integrity of the agency's data and access.
- **Recommended** — an optional hardening or operational enhancement that improves governance but is not part of the minimum secure baseline.

> **Note:** These designations describe the customer's configuration expectation. They are distinct from FedRAMP's own MUST/SHOULD designations for what the provider must document, which are tracked separately in the traceability matrix. Under FedRAMP, settings operated only by top-level administrative accounts are Required to document; settings operated by other privileged accounts are Recommended to document.

## 1.6 Terminology and how administrative accounts are named in C4G

- **Top-level administrative account** — in C4G this is the Tenant Administrator, who controls identity, provisioning, and compliance settings for the whole tenant, and the Primary Owner, the highest role within one organization.
- **Privileged account** — an organization Owner, who operates specific security-related settings but does not control the entire offering.
- **User** — a standard, non-privileged user.

Role definitions and permissions are documented at claude.com/docs/government/org-admin/users (organization roles) and claude.com/docs/government/tenant-admin/admins (Tenant Administrators).

Claude Desktop offers Chat, Cowork, and Code; Code sessions are those in its Code tab, and Claude Code is the separate command-line tool. Claude for Microsoft 365 is an Office add-in, separate from the Microsoft 365 connector. Early-access products are requested from your Anthropic representative. The web portal (your C4G address followed by /gateway) holds the tenant and organization admin portals, and Config is under Settings in each.

# 2. Administrative roles and permissions

> **SCG-CSO-RSC (MUST) — Required:** Instructions on how to securely access, configure, operate, and decommission top-level administrative accounts that control enterprise access to the entire cloud service offering.

## 2.1 Role definitions

C4G uses role-based access control. At the tenant level, Tenant Administrators control identity, routing, and cross-organization settings. Within each organization there are exactly three roles: Primary Owner and Owner are the administrative accounts, and User is the standard non-privileged role. There is no separate Admin role in C4G. Roles and their permissions are documented on the pages linked in §1.6. An organization can have up to three active Primary Owners. Assign every administrator the least-privileged role that allows them to do their job, and keep the set of top-level administrators small and explicitly named.

General account-management procedures are documented in the C4G administrator guide at claude.com/docs/government/overview.

## 2.2 Permissions that behave differently on C4G

Several capabilities available in the commercial product are handled differently on C4G. Administrators should plan around the following:

- **Request Data Exports** — governance and audit events are available through the Compliance API (see §5). Conversation content is stored on the user's device, not in the service, and is retrieved through the customer's endpoint-management or eDiscovery tooling.
- **Membership Management** — members join by signing in through SSO or through SCIM, and accounts are deactivated through SCIM. Roles and seat tiers are set by group mappings or in the admin portal.
- **Usage Analytics** — available on the Analytics page in the admin portal (content-free usage metering: requests, tokens, active users, spend, credit burndown). The Analytics API provides read-only programmatic access to an organization's requests, tokens, and estimated cost. It is off by default (see §4 and §5).
- **Data Retention controls** — server-side governance and audit events are retrieved through the Compliance API, which serves the most recent 30 days (see §5); conversation content is retained locally on user devices under agency endpoint policy.

# 3. Administrative account lifecycle

This section covers the four lifecycle phases FedRAMP requires for top-level administrative accounts: secure access, configuration, operation, and decommissioning.

## 3.1 Secure access — single sign-on (SSO)

A Tenant Administrator configures SSO (SAML 2.0 or OIDC) once for the whole tenant, on the Identity and access page of the tenant admin portal, so that members authenticate through the agency's identity provider (IdP). Full steps are at claude.com/docs/government/tenant-admin/identity-and-access.

### Step 1 — First sign-in

The first Tenant Administrator opens the C4G address followed by /gateway (for example, claude.fedstart.com/gateway), enters their work email, and selects "Email me a sign-in link".

### Step 2 — Verify your domain

1. Under Domains, confirm that your email domain is verified.
2. To add one, enter it in "Claim a domain", publish the DNS TXT record shown, and select "Verify now".
3. Verify the domain of your own email address first, and keep the record in place.

> **Note:** A verified domain can belong to only one tenant. Each subdomain is verified separately.

### Step 3 — Configure your identity provider (IdP)

Create an application in your IdP using the Redirect URI / ACS URL and SP Entity ID / Audience values shown under Single sign-on.

### Step 4 — Enter your IdP details

For SAML, paste the IdP metadata XML; the IdP must sign the assertion. For OIDC, enter the client ID, client secret, and endpoints. Use Attribute mapping if email or name arrive under other names. The IdP must send an email address on a verified domain. Paste new SAML metadata whenever the IdP rotates its signing certificate.

> **Warning:** Saving takes effect immediately for everyone, including you.

### Step 5 — Test

Select "Test sign-in" to check the connection with your own account while you stay signed in.

### Step 6 — Add routing rules

Create an organization if none exists, then add routing rules that place people in organizations. A new person whom no rule matches cannot sign in. Check with "Preview routing".

> **Note:** Add at least one more Tenant Administrator on the Admins page. Primary Owners and Tenant Administrators can still request an emailed sign-in link after SSO is connected (see Emailed sign-in link in §4).

## 3.2 Configuration — SCIM provisioning

Use SCIM to automatically provision, update, and deactivate members from your IdP. A Tenant Administrator connects it once for the whole tenant. Prerequisites: a verified domain, admin access to your IdP, and the users and groups you intend to provision.

### Step 1 — Generate a SCIM token

1. On the Identity and access page, under SCIM provisioning, copy the SCIM base URL and select “Generate token”.
2. Save the token immediately — it will not be shown again. Store it in a secrets manager.

### Step 2 — Configure your identity provider

The general pattern applies across IdPs: create an application, enter the SCIM URL and token, configure attribute mappings, and assign users and groups. Using Microsoft Entra as an example:

1. In Azure, go to Microsoft Entra ID → Enterprise Applications and create your own application (select “Integrate any other application you don’t find in the gallery”).
2. Go to Provisioning → Get started and set Provisioning Mode to Automatic.
3. Under Admin Credentials, select Bearer Authentication, then set the Tenant URL to the SCIM base URL and the Secret Token to the token from Step 1.
4. Click Test Connection to confirm a success message. If it fails, contact Anthropic with the error.
5. Review attribute mappings — these map your user attributes into the SCIM attributes Claude can ingest. Send, as the primary email, the address each person signs in with; a different address can create a second account, and deactivation then does not reach the account the person uses.
6. Go to Users and groups and assign the users or groups to provision.
7. Return to Provisioning, set Provisioning Status to On, and click Save.

> **Note:** For other IdPs, look for “SCIM provisioning” or “automated provisioning” in your IdP’s documentation — the flow is similar.

### Step 3 — Place people and verify the first sync

1. Trigger an initial sync in your IdP (or wait for the automatic cycle). Synced groups appear under Directory groups.
2. On the Identity and access page, add provisioning rules, the routing rules that place directory groups in organizations.
3. In each organization, map groups to seat tiers and roles under Group mappings. Make the first role mapping a group that holds all Owners, mapped to Owner; an Owner left out of it can lose admin access.
4. Check placement with “Preview routing” and “Synced, not routed”, then confirm members on each organization’s Users page.

SCIM changes, rule changes, and mapping changes are applied automatically without manual review.

## 3.3 Operation — ongoing administration

Manage day-to-day membership entirely from your IdP:

- **Add users:** assign them to the Claude application and the appropriate groups in your IdP.
- **Remove users:** unassign or disable them in your IdP; SCIM deactivates the linked C4G account and ends its sessions. C4G refuses to deactivate a Primary Owner, the only active Tenant Administrator, or an account not yet linked to the directory, so watch your IdP's provisioning log and resend the deactivation once the cause is fixed. SCIM does not deactivate an account your directory never sent, so provision everyone who can sign in.
- **Update information:** name and email changes sync automatically.

### SCIM troubleshooting

- **Test Connection fails:** double-check the Tenant URL and token, and generate a new token if needed. You may need Anthropic to allowlist your IdP's IP address.
- **Duplicate user error:** another user your IdP has synced has the same userName, email, or externalId. Correct the duplicate in your IdP. Existing C4G accounts link by email address and do not need to be removed.
- **Users stuck as inactive:** check the IdP attribute mapping for the "active" field.

For unresolved issues, reach out to your Anthropic contact.

## 3.4 Decommissioning

Decommission administrative access promptly and completely when staff change roles, leave, or when the organization itself is wound down.

- **Offboard an administrator:** first remove the access SCIM does not manage. For a Tenant Administrator, another Tenant Administrator removes them on the Admins page. For a Primary Owner, change their role on the organization's Users page, promoting another Primary Owner first if they are the only one. If they are leaving, deactivate them in your IdP. If they are staying as a User, remove them from any group mapped to Owner, then set their role to User on the Users page if it has not changed. Confirm the result on the Users page, and use "Sign out everywhere" if a departing person's account is still active.
- **Rotate or revoke SCIM tokens:** when an administrator who held a token leaves, or whenever exposure is suspected, generate a new token, switch the IdP to it, and revoke the old one. The old token works until it is revoked.
- **Revoke admin API keys:** an Owner, Primary Owner, or Tenant Administrator should revoke an admin API key (see §4) when it is no longer needed, when someone who has it changes role or leaves, or whenever exposure is suspected; a revoked key stops working immediately. Keys do not expire, and they are not tied to the person who created them, so revoke them separately from that person's account. Tenant Administrators revoke keys created in the tenant admin portal. Anthropic can also revoke a key created in either portal.

- **Control the emailed sign-in link:** it cannot be turned off, so remove the Primary Owner role and Tenant Administrator access from anyone who no longer needs them, and treat each use after setup as a break-glass event.
- **Organization wind-down:** before closing the organization, export any governance and audit records that must be retained to your SIEM or archive (the Compliance API serves only the most recent 30 days; see §5), deactivate in your IdP everyone who should lose access (otherwise, members whom a provisioning rule places in another organization are reactivated there), address locally-stored conversation content on user devices per your agency's endpoint data-handling policy, then coordinate account closure with your Anthropic Account Team. C4G refuses to deactivate a Primary Owner while the organization is open, so resend that deactivation as soon as it is closed.

## 4. Security settings reference table

SCG-CSO-RSC (MUST): Explanations of security-related settings operated by top-level administrative accounts (Required to document) and by other privileged accounts (Recommended to document), together with their security implications.

The table below lists the admin-controlled security settings, the account that operates each, its security impact, and the recommended secure value. Settings are described in more detail at claude.com/docs/government/config/settings. The Designation column reflects the customer configuration expectation defined in §1.5: settings marked Required form the C4G secure baseline; settings marked Recommended are optional hardening, integration, or governance controls that agencies enable according to mission need.

Settings on the Config page can be set for the tenant, and most can also be set for an organization or a directory group, where the more specific value usually wins. To enforce a value for everyone, a Tenant Administrator sets it on the tenant Config page and selects “Must use this value”, which locks it. Where a row refers to roles, apply the value to the organizations or directory groups that hold those job roles; only one group's settings apply to each person, and an organization's value overrides a tenant-wide group's unless that is locked. Most changes reach a member’s app when it next restarts.

| Setting | Function | Configured by | Security impact | Recommended value (secure default) | Designation |
|---|---|---|---|---|---|
| **Single Sign-On (SSO)** | **Federates authentication to the customer IdP over SAML 2.0 or OIDC, once for the whole tenant. Members authenticate via SSO; Primary Owners and Tenant Administrators can also use the emailed sign-in link.** | **Top-level admin (Tenant Administrator)** | **Centralizes authentication and applies the agency's IdP controls (MFA, conditional access) at sign-in. How long a C4G session lasts is set by Session idle timeout and Maximum session length, not by the IdP. Without SSO, members cannot sign in.** | **Enabled for the tenant. Verify the domain (DNS TXT) before enabling.** | **Required** |

| | | | | | |
|---|---|---|---|---|---|
| **Emailed sign-in link** | **Single-use link to the web portal, emailed on request to Primary Owners and Tenant Administrators, before and after SSO is connected. It expires within one hour and cannot be turned off.** | **Not configurable. Eligibility follows the Primary Owner role and the Tenant Administrator list.** | **A non-SSO access path for top-level admins, and the recovery path if SSO fails. It does not go through the IdP, so IdP MFA and conditional access do not apply; access rests on the administrator's mailbox.** | **Keep both roles to a small named set, protect their mailboxes with agency MFA, and alert in the SIEM on user.signed_in events whose method is magic_link, using a key created in the tenant admin portal so that every Tenant Administrator is covered.** | **Required** |
| **Domain verification** | **Proves ownership of the email domain via a DNS TXT challenge before SSO/SCIM.** | **Top-level admin (Tenant Administrator)** | **Prevents another organization from claiming your domain and asserting identities for it. A verified domain can belong to only one tenant.** | **Completed and verified before enabling SSO.** | **Required** |
| **SCIM provisioning / deprovisioning** | **Automatically creates, updates, and disables member accounts from the IdP via SCIM 2.0.** | **Top-level admin (Tenant Administrator)** | **Ensures timely deprovisioning on offboarding and consistent account state. A SCIM deactivation ends the member's sessions; blocking someone's sign-in at the IdP without one leaves their existing sessions usable. Manual processes risk orphaned accounts and access creep.** | **Enabled; verify placement, roles, and seats after the first sync (see §3.2).** | **Required** |

| | | | | | |
|---|---|---|---|---|---|
| **Role & seat assignment (least privilege)** | **Maps IdP groups to the Owner or User role and to seat tiers. Primary Owner and Tenant Administrator are granted in the admin portal, not through groups. They can also grant an Owner role that mappings do not remove; the Users page marks it as protected from group mappings.** | **Top-level / privileged admin** | **Over-provisioned roles enlarge the attack surface and the blast radius of a compromised account.** | **Grant the minimum role needed; keep top-level admins to a small named set; review periodically.** | **Required** |
| **Multi-factor authentication (MFA)** | **Enforced at the customer IdP as part of SSO. It does not apply to the emailed sign-in link.** | **Top-level admin (at IdP)** | **Primary defense against credential theft for both standard and privileged accounts.** | **Enforce phishing-resistant MFA at the IdP for all C4G users, especially administrators.** | **Required** |
| **Session idle timeout** | **Signs a member out after a period without use, in the Claude apps and the web portals. Using Claude renews the session. The tenant sets the value; organizations and directory groups can shorten it but not lengthen it. When it is shortened, members already signed in keep the time they have left. Set at Config → Sessions and access → Session idle timeout.** | **Top-level / privileged admin** | **A longer timeout leaves an unused session usable for longer on a lost or unattended device. It does not end a session that stays in use, including one held by someone disabled only at the IdP; Maximum session length, “Sign out everywhere”, or a SCIM deactivation does. A value above 12 hours is the agency's decision and responsibility.** | **Set it explicitly at the tenant: 720 minutes (12 hours) or less.** | **Required** |
| **SCIM token (handling)** | **Bearer token the IdP uses to call the SCIM endpoint. More than one can be active, so it can be rotated without an outage.** | **Top-level admin (Tenant Administrator)** | **A leaked SCIM token allows external manipulation of membership. The token is displayed only once.** | **Store in a secrets manager; on exposure or staff change, generate a new token and revoke the old one.** | **Required** |

| | | | | | |
|---|---|---|---|---|---|
| **Admin API key (scope & handling)** | **Read-only credential that customer tooling sends to the Compliance API or the Analytics API. Each key is limited to one organization's data and can read the Compliance activity feed, Usage and cost reports, or both; this is chosen when the key is created and cannot be changed afterward. Created at Settings → Admin API keys in the organization admin portal. Separately, Tenant Administrators can create keys at Settings → Compliance API keys in the tenant admin portal, which read the audit events of every organization in their tenant and of the tenant itself; handle them the same way. If that page is not shown, ask your Anthropic representative.** | **Top-level / privileged admin** | **A leaked key lets its holder read whatever the key can read (the organization's audit events, its usage and cost reports, or both) until it is revoked. A leaked key from the tenant admin portal exposes the audit events of the whole tenant. The key is displayed only once. It does not expire and is not tied to the person who created it.** | **Store in a secrets manager; choose only what the tool needs to read; issue a separate key for each tool; rotate on your agency's schedule; revoke on exposure, and when someone who has the key changes role or leaves.** | **Required** |
| **Compliance API enablement** | **Dedicated interface for governance and audit events; enabled by default for every C4G organization. An Owner, Primary Owner, or Tenant Administrator issues admin API keys that can read the Compliance activity feed. Set at Config → Admin Console → Compliance API (Tenant Administrators only).** | **Top-level admin (Tenant Administrator)** | **Provides the audit trail required for federal accountability; without it, investigation and configuration-change review are impaired.** | **Leave On (the default). For audit tools, issue keys that can read only the Compliance activity feed; restrict use to authorized administrators.** | **Required** |

| | | | | | |
|---|---|---|---|---|---|
| **Audit logging — Activity Feed** | **Governance and audit-event trail (sign-ins, provisioning, configuration changes, admin actions) with actor and timestamp. Sign-in events also carry the IP address.** | **Top-level / privileged admin (via Compliance API)** | **Enables detection, investigation, and accountability; each record carries identifying metadata.** | **Retrieve regularly and export to the agency SIEM for monitoring and alerting. Use a key created in the tenant admin portal to include tenant-level events (see §5).** | **Required** |
| **Data retention (records)** | **Governance and audit-event records, retrieved on C4G through the Compliance API (not the standard UI). The API serves the most recent 30 days of activity. C4G is not the agency's long-term archive. In Claude Desktop, conversation content is stored on the user's device.** | **Not configurable. A top-level or privileged admin sets up the export.** | **Supports audits and accountability. Records not exported within 30 days of the event cannot be retrieved through the Compliance API.** | **Compliance API on (default). Agency responsibility: export records before they are 30 days old, and keep them as long as agency policy requires.** | **Required** |
| **Audit-log export to SIEM** | **Exports Compliance API activity records into the customer's SIEM or archival tooling.** | **Top-level / privileged admin** | **Centralizes monitoring and enables archival beyond the 30 days the Compliance API serves.** | **Configure automated export into the agency SIEM.** | **Required** |

| | | | | | |
|---|---|---|---|---|---|
| **Disable claude.ai sign-in (disableDeploymentModeChooser, deploymentMode)** | **Managed-configuration keys delivered via MDM that remove the claude.ai sign-in option from the desktop client, leaving only the C4G deployment sign-in. A device set up by hand, without a profile, does not have this protection.** | **IT / endpoint admin (via MDM)** | **Prevents users on managed devices from signing into the commercial service, which is outside the FedRAMP boundary, and keeps the device on the agency's configuration.** | **Set disableDeploymentModeChooser to true and deploymentMode to 3p alongside bootstrapUrl, all in one machine-wide profile: computer-level on macOS, HKLM on Windows, the root-owned managed-settings file on Linux. On macOS, move the keys you still need from any user-level profile into it, then remove the user-level profile. On Linux, add deploymentMode only once the device runs Claude Desktop 4.16336.0 or later. Reference AC-20, SC-7.** | **Required** |

| | | | | | |
|---|---|---|---|---|---|
| **Admin Seat Tier & Spend Cap Setup** | **Seat tiers (Anthropic-managed or self-managed) set the models each member can use and their 5-hour and 7-day spend limits. Tenant Administrators can also set 5-hour and 7-day spend caps on each organization's usage of self-managed tiers. Requests are refused once a limit or cap is reached. Low-balance alerts are automatic.** | **Top-level / privileged admin** | **Cost-governance control. Limits runaway usage and supports budget oversight; it is an operational control rather than a confidentiality/integrity control, hence Recommended.** | **Configure seat tiers; set optional organization spend caps aligned to budget.** | **Recommended** |
| **Analytics API enablement** | **Makes an organization's content-free usage and cost reports available through a read-only API. Off by default. When it is off, requests are refused. Turning it off does not revoke keys, so revoke those that should not work if it is turned back on. Set at Config → Admin Console → Analytics API, by an Owner or Primary Owner for their organization, or by a Tenant Administrator for any one organization or as the default for organizations that have not set their own. The Compliance API setting does not control it.** | **Top-level / privileged admin** | **Usage and cost reports can identify members by user ID, name, and email address. They contain no conversation content, files, or anything users type into Claude, and they leave the service when customer tooling requests them.** | **Leave Off (the default) unless there is a reporting need. To keep it off for every organization, a Tenant Administrator sets it to Off on the tenant Config page and selects "Must use this value"; without that, an organization can turn it on for itself.** | **Recommended** |
| **Maximum session length** | **Ends a session a fixed time after sign-in, even while it is in use, so the member goes back through the IdP. No maximum applies unless one is set. Set at Config → Sessions and access → Maximum session length.** | **Top-level / privileged admin** | **Without a maximum, a session in regular use can continue for weeks without the IdP's policies being applied again.** | **The agency's re-authentication interval.** | **Recommended** |

| | | | | | |
|---|---|---|---|---|---|
| **Web search** | **Queries the live web and returns top results, letting Claude answer with current information beyond its training data. If enabled, the user approves each search Claude runs while “Require approval for each search” is On (the default). Set at Config → Integrations → Web search.** | **Top-level / privileged admin** | **Introduces an outbound path for prompt-derived content and an inbound path for untrusted external content. Queries generated from user input leave the FedRAMP boundary for an external search provider; returned content enters the model's context unvalidated.** | **Disabled by default. Enable only for roles with a documented mission need; leave blocked for roles handling data not cleared for external query. Keep "Require approval for each search" On (the default) and acknowledge the data-flow disclosure before enabling. Treat model output citing external sources as unvalidated. Reference AC-20, SA-9, SC-7.** | **Recommended** |

| | | | | | |
|---|---|---|---|---|---|
| **Allowed network hosts** | **Hostname allowlist for shell commands and web-page fetches in Chat and Cowork, for the sandboxed shell commands of Code sessions on macOS and Linux, and for those of Claude Code while Shell command sandbox is On. With no hosts listed (the default), fetches and package installs from those tools fail. It does not limit web search, connectors, hooks, plugin code, hosts a plugin declares for its tools, or the app's own connections. In Code sessions and Claude Code, rely on it only for sandboxed shell commands. Other traffic from those two, such as web fetch and unsandboxed commands (all commands on native Windows), can reach other hosts. A saved list, even an empty one, also limits what pages in the Code tab's preview load (Claude Desktop 6.6395.0 or later). Set at Config → Sessions and access → Allowed network hosts.** | **Top-level / privileged admin** | **Constrains data-exfiltration and command-and-control paths from model-authored code. Broad allowlists reintroduce those risks, and "*" leaves Code's shell commands unsandboxed unless Allowed workspace folders is set.** | **Save a list rather than leaving the setting untouched, and keep it empty unless a mission need exists (on an untouched setting, “Must use this value” at the tenant saves an empty list and stops organizations and groups from adding hosts). Add only specific hosts or agency-domain wildcards. Do not use "*". Where Code or Claude Code is on, turn Web fetch off or, if users need it, turn on “Require approval for each fetch” (Config → Integrations); either choice also applies to Chat and Cowork. On Windows, rely on agency network controls for shell commands in Code and Claude Code, or turn those products off. Reference SC-7, AC-4.** | **Recommended** |

| | | | | | |
|---|---|---|---|---|---|
| **Allowed workspace folders** | **Restricts which local folders users may pick for Cowork and Code; the desktop client refuses folders outside the list. Any folder is allowed by default. Set at Config → Sessions and access → Allowed workspace folders.** | **Top-level / privileged admin** | **Limits the local data the model and sandbox VM can read or write; an unrestricted list exposes any user-selected path. It does not stop shell commands in Code sessions from reading other files the user can open or, on Windows, from changing them.** | **Scope to designated working directories only, not a whole home folder; check “Block all workspace folders” for roles that do not need access. Where Code is on, also turn on “Block reads outside workspace folders”; on Windows it can only ask before a shell command reads elsewhere. Reference AC-3, AC-6.** | **Recommended** |
| **Product availability** | **Settings that decide which products members get: Claude Desktop (Chat, Cowork, and the Code tab, all on by default), and the Claude Code command-line tool and Claude for Microsoft 365 (both off by default, in early access). “Claude Desktop home” sets Chat, file analysis, and Cowork together; members who have Cowork also get Chat and file analysis. Set at Config → Product availability.** | **Top-level / privileged admin** | **Cowork, and file analysis in Chat, run code in a local sandbox VM. Code and Claude Code run commands on the workstation itself, under the user's account, with no sandbox on Windows. Disabling them removes those attack surfaces for roles that do not need agentic execution. These settings do not revoke an account's access; deactivate the account to do that.** | **Enable only what each role requires. For roles limited to conversational use, set Claude Desktop home to “Chat only” (or “Simple” if they need file analysis) and turn Code off. Leave Claude Code and Claude for Microsoft 365 off until the agency has early access; the settings that restrict them appear in Config only then. Reference CM-7.** | **Recommended** |

| | | | | | |
|---|---|---|---|---|---|
| **Managed MCP connectors** | **Administrator-added Model Context Protocol connectors delivered to users at tenant, organization, or group scope. End users cannot modify them. Separate settings govern connectors that users add themselves (“Let members add their own connectors” and “Member-added connectors”). Set at Config → Integrations → Connectors.** | **Top-level / privileged admin** | **Each connector is an outbound HTTPS path from the endpoint to the configured address and grants the model access to that system's data and actions. If a connector uses a shared secret, every member's app receives it, so scope it accordingly.** | **Add only vetted connectors with a documented mission need; pair with per-tool approval policy so Claude's write/send actions require user confirmation. Reference SA-9, AC-20.** | **Recommended** |
| **Organization plugins** | **Administrator-uploaded plugin packages (skills, commands, subagents, hooks, connectors) delivered to users as “Auto-install” or “Members choose”. Set at Config → Integrations → Plugins.** | **Top-level / privileged admin** | **Plugins can add executable behavior and connector access; an unreviewed plugin widens the effective tool surface. Hooks and local connectors run under the user's account, outside the sandbox.** | **Review plugin contents before upload, especially plugins marked “Runs code”; prefer “Members choose” over “Auto-install”.** | **Recommended** |
| **Microsoft 365 connector** | **Connector for Teams, Outlook, OneDrive, and SharePoint, built into Claude Desktop and run on each user's device. Users sign in with their own Microsoft account through an application the agency registers in its Entra tenant; Microsoft Graph calls and sign-in tokens do not pass through an Anthropic service. What Claude reads is then sent to the model like the rest of the conversation. Permissions are chosen under Access on the card and must also be consented in Microsoft Entra. Set at Config → Integrations → Microsoft 365.** | **Top-level / privileged admin (with Entra admin)** | **Grants the model access to agency mail, files, and chat. Write permissions let it send mail and Teams messages and change calendars, files, and mailbox rules; the user approves each write action Claude takes.** | **Disabled by default. Consent to read scopes narrowly; enable write only where required and only after Entra admin review. Reference AC-20, SA-9.** | **Recommended** |

| | | | | | |
|---|---|---|---|---|---|
| **Telemetry endpoint (OTLP)** | **Destination for the OpenTelemetry export from Claude Desktop, Claude Code, and Claude for Microsoft 365 (tool name, connector, outcome, duration; content-bearing fields by opt-in). Data goes only to the customer's collector. Set at Config → Compliance and telemetry → Telemetry endpoint.** | **Top-level / privileged admin** | **Provides the customer-side audit and DLP feed for tool and connector activity that the Compliance API does not cover.** | **Point at the agency's OTLP collector, and confirm that events arrive after setup and after app updates. Leave content capture off unless required for DLP and the collector is appropriately protected. Every member's app receives the Telemetry headers, so use a send-only credential. Reference AU-6, AU-12.** | **Recommended** |
| **Desktop banner (classification strip)** | **Persistent banner across the top of the desktop client with custom text, colors, and link; separate from the fixed U.S. Government system-use notice. Set at Config → Appearance → Claude Desktop banner.** | **Top-level / privileged admin** | **Supports AC-8 system-use / classification marking; misuse could imply an incorrect handling level.** | **Set to the agency's approved classification or handling banner text; verify delivery on a pilot device. Reference AC-8.** | **Recommended** |

| | | | | | |
|---|---|---|---|---|---|
| **Auto mode** | **Governs whether users can use Auto mode, in which Claude approves or blocks most actions itself, in Cowork, Code sessions, and Claude Code. Blocked by default. When Allowed, new Code sessions start in Auto mode unless the user has chosen another mode. A signed-in app takes this setting from C4G, not from the MDM profile. Set at Config → Integrations → Auto mode, available once the agency has the Claude Code settings (early access).** | **Top-level / privileged admin** | **When enabled, the model can execute tool and connector actions without per-action user approval, removing the primary human-in-the-loop containment control.** | **Leave Blocked (the default). Enable only for narrowly scoped, low-sensitivity roles with compensating monitoring. Reference AC-6, CM-7.** | **Recommended** |
| **Per-tool approval policy** | **The Web search, Web fetch, and Shell commands cards turn each tool on or off for Claude and can require the user's approval each time Claude uses it (by default, required for Web search only). For each administrator-added connector, Tool policy sets a tool on (the user approves each use by Claude) or off (blocked) in Claude Desktop and Claude Code. Users cannot loosen these settings. Claude for Microsoft 365 does not enforce these approvals and does not receive a connector that has a tool switched off. Set at Config → Integrations.** | **Top-level / privileged admin** | **Enforces human approval for Claude's write/send/execute actions and removes tools not needed for the mission. Where approval is not required, shell commands and web fetches can run without a prompt. Connector tools not listed in Tool policy, including any the server adds later, stay under each user's control.** | **In Tool policy, switch write/send tools on (approval each time Claude uses them) and unused tools off; leave read tools unlisted. Do not apply connectors with write/send tools to Claude for Microsoft 365. Turn on “Require approval for each command” where agency policy requires a prompt, and set Web fetch as the Allowed network hosts row recommends. Reference AC-6, CM-7.** | **Recommended** |

| | | | | | |
|---|---|---|---|---|---|
| **Auto-update control (Block automatic updates, disableAutoUpdates)** | **Disables the desktop client's in-app updater on macOS and Windows so the agency's software-distribution pipeline controls versioning. Set in two places: a signed-in app follows Config → Compliance and telemetry → Block automatic updates, and the disableAutoUpdates key, set beside bootstrapUrl in the MDM profile, applies when the app starts with no user signed in.** | **Top-level / privileged admin (Config page) and IT / endpoint admin (via MDM)** | **Agency-managed updates support change control and pre-deployment testing; disabling without a refresh cadence risks stale, unpatched clients.** | **Leave auto-update on unless agency policy requires IT-managed versioning; if it does, turn on both, lock the Config setting at the tenant, and refresh at least monthly. C4G can stop serving an older version sooner, so watch claude.com/docs/government/changelog for minimum versions. Reference CM-3, SI-2.** | **Recommended** |
| **Tenant restrictions header (Anthropic-Allowed-Tenant-Ids)** | **Header injected by the customer's TLS-inspecting outbound proxy, listing the allowed tenant IDs; the C4G service refuses requests from accounts in any other tenant. Traffic that bypasses the proxy is not restricted.** | **Network / perimeter admin** | **Blocks use of other C4G tenants (including another agency's) from the agency network; complements blocking claude.ai at the perimeter.** | **Configure the proxy to overwrite (not append) the header on traffic to your C4G domains; block claude.ai (root host only) at the perimeter. Reference SC-7, AC-20.** | **Recommended** |
| **Bypass-permissions mode** | **Whether users can use the mode that skips permission prompts in Claude Desktop, Claude Code, and Claude for Microsoft 365. Blocked by default. Set at Config → Integrations → Bypass-permissions mode.** | **Top-level / privileged admin** | **When Allowed, Claude can act without asking, including commands that run as the user.** | **Leave Blocked.** | **Recommended** |

| | | | | | |
|---|---|---|---|---|---|
| **Member-added connectors, plugins, and skills** | **Four “Let members …” switches decide whether users can add their own local connectors, plugins, and plugin marketplaces (all off by default) or create skills (on by default). “Member-added connectors” (None by default) governs the connectors that users add in Code sessions or Claude Code, and those that plugins carry; it applies once the agency has the Claude Code settings (early access). Set at Config → Integrations.** | **Top-level / privileged admin** | **Local connectors, plugin hooks, and mods (code that a plugin runs inside a Chat, Cowork, Code, or Claude Code session) run under the user's account, outside the sandbox, without administrator review.** | **Leave connectors, plugins, and marketplaces off and Member-added connectors at None. Without the Claude Code settings, turn Code off for roles that must not add connectors or hooks. To stop users' own mods, in Chat and Cowork too, deploy the device file under “Stop user-installed mods from loading” at claude.com/docs/third-party/claude-desktop/code.** | **Recommended** |
| **Terminal panel tools** | **Lets Claude run commands in the Code tab's Terminal panel. On by default. Set at Config → Integrations → Terminal panel tools.** | **Top-level / privileged admin** | **These commands run as the user, outside any sandbox. The app asks for approval of each by default.** | **Turn off unless needed.** | **Recommended** |
| **Scheduled tasks** | **Lets users set up tasks that Claude runs on a schedule. On by default. Set at Config → Product availability → Scheduled tasks.** | **Top-level / privileged admin** | **Tasks run unattended and use the same tools and connectors as other sessions.** | **Turn off for roles that do not need them.** | **Recommended** |
| **Organization Analytics connector** | **Lets Owners query their organization's usage from Claude Desktop. Off by default. Set at Config → Admin Console → Organization Analytics connector.** | **Top-level / privileged admin** | **Usage data, including members' email addresses, enters the Owner's conversation.** | **Leave Off unless needed; lock it at the tenant to keep it off.** | **Recommended** |

| | | | | | |
|---|---|---|---|---|---|
| **Claude Code settings (early access)** | **Shell command sandbox, blocked shell commands, managed and member-added hooks, plugin sources, sideloaded plugins, version limits, and opening from the browser. They govern Claude Code, and most also reach Code sessions. Set at Config → Claude Code.** | **Top-level / privileged admin** | **These settings control what can run on the workstation. Once the agency has early access, they block member-added hooks, plugin sources, and sideloading by default; blocking hooks also stops mods, except in Chat and Cowork. Until then, members' own hooks and mods can run in Code sessions, outside the sandbox.** | **Set Shell command sandbox to On, which sandboxes the command-line tool's shell commands on devices that can run the sandbox (not native Windows; Linux and WSL need bubblewrap and socat installed). The default, “Left to the device”, leaves them unsandboxed unless the device's own Claude Code settings turn the sandbox on. Off also removes the sandbox from Code sessions. Keep the other defaults.** | **Recommended** |
| **Claude for Microsoft 365 settings (early access)** | **Attach files to chat, Accept all edits, and File access rules by Purview sensitivity label. Set at Config → Sessions and access.** | **Top-level / privileged admin** | **Accept all edits (allowed by default) lets users switch to a mode in which Claude makes most edits to the open file without asking. No files are blocked until rules are set.** | **Add File access rules for labels not cleared for Claude; turn off Accept all edits where review is required.** | **Recommended** |

# 5. Compliance API

The Compliance API is a dedicated interface for C4G customers that provides programmatic access to governance and audit events recorded inside the FedRAMP boundary. It returns identity, session, provisioning, and configuration events; it does not return conversation content, tool calls, or usage metrics. Conversation content is stored on the user's device (see §2.2), so eDiscovery and DLP for that content are performed through the customer's endpoint tooling rather than through this API. The OpenTelemetry export can also feed DLP review, but it is not a complete record of a session.

The Compliance API is enabled by default for every C4G organization and is served from your C4G deployment host at GET /gateway-api/v1/compliance/activities. A key created in an organization's admin portal returns that organization's events; a key created in the tenant admin portal returns the events of every organization in the tenant together with tenant-level events, such as changes to SSO, the Tenant Administrator list, and tenant-wide settings. An Owner, Primary Owner, or Tenant Administrator can create an admin API key that can read the Compliance activity feed, described below.

**Activity Feed — governance and audit events**

- Authentication events (sign-ins, and an administrator signing a member out everywhere). Use your IdP's logs for failed authentication.
- Administrative actions (user provisioning, permission changes, configuration changes, API-key issuance and revocation). The record of a new key's creation states what the key can read, and the record of a revocation by Anthropic gives its reason.
- Each record includes a timestamp and the actor: user ID and email address for the agency's own users, and no individual identity for actions by Anthropic or automated systems, including directory sync. Sign-in records also include the sign-in method and IP address.

**Endpoint-side logging (customer-collected)**

- Conversation content, uploaded files, and tool inputs/outputs are stored on the user's device. The app does not encrypt them, so protection at rest depends on full-disk encryption. Model requests carry that content through the service to the model endpoint (see claude.com/docs/government/security/security-and-data-handling).
- Chat and Cowork sessions write a local audit log (audit.jsonl) that records prompts, responses, tool inputs and results, and permission decisions. It is deleted with its session. Code sessions do not write it.
- The desktop application can export OpenTelemetry events (tool name, connector, outcome, duration; content-bearing fields optionally, by administrator opt-in) to the customer's own collector for DLP and monitoring. Do not rely on content capture alone as a record of user input. This data goes only to the customer's collector, never to Anthropic.

Customers can export Compliance API events directly into their own SIEM tools for centralized analysis, for long-term archival if required by their agency's policies, or for integration with their existing compliance workflows. The API serves the most recent 30 days of activity, so an export that falls more than 30 days behind cannot recover the missed events. The event schema, pagination pattern, and SIEM-polling guidance are documented at claude.com/docs/government/org-admin/compliance-api.

### Analytics API — usage and cost reports

The Analytics API, a separate read-only API, gives customer tooling access to one organization's content-free usage metering: requests, tokens, and estimated cost, by time period, product, model, and member. It is off by default. An Owner, a Primary Owner, or a Tenant Administrator turns it on with the Analytics API setting (see §4), and any of them can create, in the organization admin portal, an admin API key that can read Usage and cost reports. Only such a key can call it; keys created before the Analytics API was introduced and keys created in the tenant admin portal cannot.

Reports by member identify members by user ID, name, and email address, including members whose accounts are deactivated; people who have moved to another organization appear by user ID only. Reports contain no conversation content, files, or anything users type into Claude. Changes to the setting made for the organization, the creation of its keys, and their revocation, including by Anthropic, are recorded in its Activity Feed. The tenant restrictions header (see §4) applies to Analytics API requests too. Parameters, fields, and limits are documented at claude.com/docs/government/org-admin/analytics-api.