Cellebrite Government Cloud FedRAMP Secure Configuration Guide

Cellebrite

Reviewed May 2026

Cellebrite Government Cloud
FedRAMP Secure Configuration Guide

1. Purpose

This Secure Configuration Guide provides federal agencies with public guidance to securely access, configure, operate, and decommission top-level administrative accounts for CGC. It explains security-relevant settings, including those available to privileged roles, and the security implications of configuration choices. This guide supplements the Customer Responsibilities Matrix and other authorization artifacts.

2. Scope and Applicability

Scope: Enterprise-level configuration and administrative account security for CGC, with a focus on top-level administrative accounts and privileged roles.

Audience: Federal customers, integrators, and assessors.

Out of scope: Agency-specific architectures and sensitive implementation details. Detailed artifacts are available to customers under NDA as Option B and Option C.

3. Definitions

Top-level administrative account: An identity that controls enterprise-wide access to the service and can modify global security settings.

Privileged account: An identity with elevated permissions scoped to specific domains or functions.

Secure defaults: CGC baseline security settings enabled by default, with documented implications if changed.

4. Alignment with FedRAMP Rev5 RSC

This public guide addresses the Rev5 Secure Configuration Guide expectations by providing: instructions for top-level administrative accounts, explanations of administrative-only security settings and their implications, privileged account guidance, secure defaults with implications, a verification checklist, and versioning controls.

5. Top-level Administrative Accounts

5.1. Account types and naming

CGC Tenant Owner (top-level): Enterprise control identity for each tenant. Manages tenant-wide security settings, federation, and break-glass. Back-end administrative access is through Amazon WorkSpaces authenticated by Microsoft Entra ID with FIPS YubiKey hardware MFA.

CGC Provider Admin (Cellebrite-managed): Restricted and audited identity for provider support actions. Time-bound, ticket-controlled, with monitoring.

5.2. Secure Access - required steps

- Establish identity federation with the agency IdP using SAML or OIDC. Enforce phishing-resistant MFA. Minimize local accounts.
- Create two break-glass accounts backed by hardware tokens. Store credentials in a FIPS-validated vault. Monitor all use.
- Restrict administrative access paths by conditional access or IP allow lists and use secure administrative workstations if applicable.
- Harden authentication. Prohibit shared credentials. Rotate secrets per policy.
- Enable monitoring and alerting for authentication anomalies, privilege or policy changes, and MFA resets.

5.3. Initial Configuration - required steps

- Confirm secure defaults in Section 8 remain enabled unless a documented risk decision authorizes change.
- Define role boundaries per Section 7 and assign least privilege.
- Configure administrative log export to the agency SIEM with integrity protection and retention.
- Document and test recovery procedures at least annually.

5.4. Operational Use

- Use the Tenant Owner account only for tasks that require enterprise scope and for recovery.
- Use scoped privileged roles for daily administration.
- Review administrative activity weekly and after any significant change.

5.5. Decommissioning

- Revoke federation and disable the Tenant Owner account when deprovisioning a tenant.
- Export required logs, evidence, and configuration snapshots.
- Revoke tokens, rotate or destroy secrets and keys, and remove persistent trust relationships.
- Record completion in a change record and retain for audit.

6. Administrative-only Security Settings and Security Implications

	What it controls	Security implications if changed
Setting (Top-level only)	Which IdP can issue tokens for CGC, SSO to WorkSpaces and consoles	Expanding trust beyond the agency IdP increases risk of unauthorized access. Keep trust limited and enforce phishing-resistant MFA.
Break-glass accounts	Emergency access when SSO is unavailable	Removing break-glass can block recovery. Over-permissive break-glass increases misuse risk. Require hardware tokens and continuous monitoring.
Global session controls	Session lifetimes and re-authentication behavior	Long sessions increase impact of token theft. Shorter sessions increase assurance but affect usability.
Global logging and export	Administrative audit logs and forwarding to SIEM	Disabling export or integrity checks degrades investigations and compliance evidence. Maintain retention and tamper protection.
Key management defaults	Scope and rotation of encryption keys	Weak key policy increases exposure. Use strong rotation and separation of duties.
Admin API token policy	Administrative API access and token scopes	Over-broad scopes increase blast radius. Use least privilege and short token lifetimes.

7. Privileged Accounts - Roles and Implications

Role	Key permissions	Security settings controlled	Controls and monitoring
SRE Team	IAM, consoles, infrastructure and tooling administration	Federation parameters, audit logging, alerting, platform services	Hardware-based MFA, change approvals, weekly activity review, Splunk ES alerts
Customer Support Team	Customer onboarding and scoped tenant support	Scoped diagnostics and tenant setup	Ticket-bound access, session recording, post-activity review
Security Team	Threat detection and incident response	GuardDuty, SIEM use cases, response workflows	On-call rotation, playbooks, evidence capture
Global Government Compliance Director	Oversight and access reviews	Access review cadence, SoD and approvals	Monthly privileged reviews, six-month non-privileged reviews

8. Secure Defaults and Implications

Area	CGC secure default	If changed
Encryption at rest	Enabled using cloud-native KMS with customer-scoped keys where applicable	Reduced data protection. Requires AO risk acceptance.
Encryption in transit	TLS 1.2 or higher across all supported interfaces and service mesh	Downgrade or legacy ciphers increase interception risk.
Admin audit logging	CloudTrail, VPC Flow Logs, GuardDuty to Splunk ES	Reduced visibility and impaired forensics.
Least privilege	Default roles scoped by function and SoD	Broader grants increase blast radius.
Account lockout policy	Three failed attempts in 30 minutes with lockout	Higher thresholds increase brute force risk. If agency policy differs, document AO decision.
Inactivity logout	Fifteen minute inactivity timeout with re-authentication	Longer timeouts increase token exposure window.

9. Verification Checklist

- [ ] Top-level account protected with phishing-resistant MFA and vaulted credentials
- [ ] Federation configured with agency IdP and local accounts minimized
- [ ] Two hardware-token break-glass accounts created and monitored
- [ ] Admin-only settings match Section 6
- [ ] Privileged roles assigned per Section 7 and time-bound for risky tasks
- [ ] Secure defaults in Section 8 verified against current configuration
- [ ] Administrative logs exported to SIEM with integrity and retention enforced
- [ ] Decommissioning steps documented and tested

10. Customer Responsibilities

The following responsibilities derive from the CGC Customer Responsibilities Matrix. Agencies remain accountable for meeting their own policies and AO expectations.

Key responsibilities include:

- **Identity and access management** - establish and maintain the Customer Administrator account, create and manage user accounts, define role membership, and conduct account reviews each month for privileged users and every six months for non-privileged users.
- **Federation and MFA** - federate the agency IdP using SAML or OIDC, enforce phishing-resistant MFA, and manage PIV or CAC integration when required.
- **Session and banner controls** - configure session termination and device lock policies consistent with agency policy and ensure FedRAMP-compliant system use notification is displayed and acknowledged for federated logons.
- **Password and authenticator rules** - establish and enforce password and authenticator content rules, including checks against commonly used or compromised passwords and secure recovery processes.
- **Account monitoring** - monitor customer-managed administrator accounts, disable high-risk accounts within required timeframes, and audit account lifecycle actions within the CGC application.
- **Least privilege and SoD** - implement and document separation of duties and least privilege within the tenant, including any shared or group account usage rules.
- **Incident coordination** - follow agency processes for incident handling and reporting, including information spillage identification and coordinated notification to Cellebrite as required.

11. Operational and Decommissioning Procedures

- **Operational**: use top-level accounts only when enterprise scope is required and for recovery, use scoped roles for day-to-day work, and monitor administrative activity continuously.
- **Decommissioning**: revoke federation, disable top-level accounts, export logs and evidence, revoke tokens, rotate or destroy keys and secrets, remove trust relationships, and record completion in a change record.

12. Versioning, Publication, and Change History

CGC maintains a public changelog for this guide. Updates occur when administrative controls or secure defaults change. Each version includes a summary of changes, effective date, and validity window.

Appendix A - Quick Start Checklist

- [ ] Top-level account protected with phishing-resistant MFA and vaulted credentials
- [ ] Federation configured with agency IdP and local accounts minimized
- [ ] Two hardware-token break-glass accounts created and monitored
- [ ] Admin-only settings match Section 6
- [ ] Privileged roles assigned per Section 7 and time-bound for risky tasks
- [ ] Secure defaults in Section 8 verified against current configuration
- [ ] Administrative logs exported to SIEM with integrity and retention enforced
- [ ] Decommissioning steps documented and tested

8065 Leesburg Pike, Suite T3-302, Vienna, VA 22182 USA / Tel. +1 201 848 8552 www.cellebrite.com