1266 W Paces Ferry Rd NW | Suite 674
Atlanta GA 30327
86borders.com

FedRAMP 20x Class C (20xC) Secure Configuration & Governance Guide [86B-CAC-SCG]

FedRAMP 20x Class C (20xC) Secure Configuration & Governance Guide

Use-Case Variant: Internal Employee Access Only (No External Customer Agent Surface)

FedRAMP Document Classification: UNCLASSIFIED / CUI

Governance Standard: FedRAMP 20x Class C Baseline | OMB M-24-15 | NIST SP 800-53 Rev. 5 | OMB M-21-31

1. Document Overview & Scope

This guide establishes mandatory security parameters, administrative controls, and continuous compliance standards for the cloud application under the **FedRAMP 20x Class C (20xC)** baseline.

Scope Restriction: This platform operates under a restricted internal boundary. External customer agents and third-party contractors are **explicitly blocked** from accessing the CSP SaaS interface, management consoles, and underlying endpoints. All administrative, operational, and data-management functions are performed exclusively by authenticated **internal employees** over corporate zero-trust network paths.

1266 W Paces Ferry Rd NW | Suite 674
Atlanta GA 30327
86borders.com

Table of Contents

Document History

Approved By	Approval Date	Comments:	Version
M. Buford	Aug 26, 2026	Initail	v1

1266 W Paces Ferry Rd NW | Suite 674
Atlanta GA 30327
86borders.com

2. FedRAMP 20xC Shared Responsibility Matrix

Under this internal-only model, customer security responsibilities shift heavily toward internal identity management, device compliance, and access governance:

Security Domain	CSP Responsibilities	Internal Agency/Employee Responsibilities
Physical & Environmental	Data center perimeter defense, hardware destruction, environmental redundancy.	*Inherited from CSP.* No action required.
Infrastructure & Hypervisor	Bare-metal hardening, hypervisor isolation, OS patching, core network backbone security.	*Inherited from CSP.* No action required.
Identity & Access Control	IAM engine availability, platform API endpoints.	Internal PIV/CAC & FIDO2 enforcement, strict internal RBAC, SCIM auto-deprovisioning, quarterly internal access reviews.
Data Protection & Keys	Core encryption engine maintenance, HSM physical security.	Customer-Managed Encryption Keys (CMEK) provisioning, key rotation, internal object access controls.
Network Isolation	SaaS endpoint availability.	Strict blocking of public ingress; restriction of all traffic to internal enterprise VPN/SD-WAN IPs.
Audit Log & SecOps	Platform-level logging, hypervisor security monitoring.	Continuous log export to Agency SIEM (OMB M-21-31

		EL3), internal SOC monitoring, internal threat hunting.

3. Account Lifecycle & Internal Administrative Controls

3.1 Initial Account Provisioning

1. **Internal Account Binding:** Accounts may only be created for validated internal employees using corporate/agency email domains (e.g., `employee-name@agency.com`).
2. **FIPS 140-3 Token Binding:** Initialization must occur within an isolated session requiring initial credential setup to be immediately bound to a hardware FIPS 140-3 Level 3 token (e.g., YubiKey 5 Series FIPS) issued directly to the internal employee.
3. **No External Account Creation:** Tenant settings must hard-block self-registration, external guest invitations, or federated connections from external customer agent identity providers.

3.2 Privileged & Internal Access Governance

- **Strict Least Privilege:** Privileged functions are granted via Role-Based Access Control (RBAC) templates enforcing strict separation of duties.
- **Just-In-Time (JIT) Elevation:** Administrative actions require JIT elevation, capped at a maximum of **4 hours**, tied to an approved internal CCB ticket.
- **Automated Offboarding:** Identity lifecycle triggers via SCIM automatically lock credentials within **< 1 hour** of an internal employee's HR status change.

3.3 Authentication & Zero Trust Enforcements

- **NIST SP 800-63B AAL3:** Internal access requires **PIV/CAC-derived credentials** or **FIDO2 / WebAuthn hardware tokens**.
- **Managed Device Requirement:** Authentication policies must mandate that access originates from an agency-managed, compliant endpoint (enforced via device posture checks/EDR state).
- **Prohibited Channels:** External agent access endpoints, public registration portals, SMS, voice MFA, and unbound TOTP apps are strictly disabled.

4. Secure Baseline Configuration Settings

4.1 Network Perimeter & Access Restriction

- **Zero Public Exposure:** The SaaS interface, control plane, and APIs must have **0.0.0.0/0 ingress blocked entirely**.
- **Internal IP / TIC 3.0 Restriction:** Access is restricted exclusively to Agency Trusted Internet Connection (TIC 3.0) IP ranges, internal SD-WAN egress points, or private connectivity endpoints.
- **Public Agent Block:** Requests originating outside internal agency network ranges must be dropped at the edge without rendering authentication interfaces.

4.2 Cryptography & Data Protection

- **Data-in-Transit (NIST SP 800-52 Rev. 2):** Enforce **TLS 1.3** (or TLS 1.2 using FIPS-approved ciphers like `ECDHE-ECDSA-AES256-GCM-SHA384`). Unencrypted HTTP is disabled.
- **Data-at-Rest (FIPS 140-3):** Mandatory AES-256 bit encryption backed by Amazon Key Management System (KMS) managed via FIPS 140-3 Level 3 HSMs.

4.3 Auditing & Logging (OMB M-21-31)

- **Internal Action Tracking:** Audit logs must track all internal employee activities, system configuration changes, and data access events.
- **Retention & Export:** Maintain logs for **365 days** (min. 90 days active/hot storage) and continuously stream events in JSON/syslog format via mTLS to the internal Agency SIEM.

5. Security Impact Analysis Matrix

Feature / Setting	Default Value	Internal-Only Required Value	Regulatory Mapping	Security Impact
SaaS Edge Exposure	Public Internet	**Blocked (Internal TIC 3.0 / VPN Only)**	**OMB M-19-26** (AC-17, AC-21)	Completely eliminates external threat vectors by dropping external agent traffic at the network edge.

User Onboarding	Open / Self-Serve	**Internal SCIM Provisioning Only**	**NIST SP 800-53** (IA-2, IA-4)	Prevents unauthorized external registration; ensures only active employees hold credentials.
Authentication Standard	Basic MFA / Passwords	**Mandatory PIV/CAC or FIDO2 (AAL3)**	**NIST SP 800-63B** (IA-2(1), IA-8)	Prevents credential theft, credential stuffing, and AiTM phishing against internal staff.
Device Compliance	Any Browser	**Agency-Managed Endpoint Only**	**NIST SP 800-53** (AC-19, CM-8)	Blocks access from non-compliant or personal unmanaged devices.
Session Inactivity	8 Hours	**15 Minutes Limit**	**NIST SP 800-53** (AC-11, AC-12)	Protects unattended internal workstations from unauthorized access.

6. Continuous Monitoring & Operational Security

6.1 Automated Compliance & Remediation

- System inventories, internal patch states, and configuration baselines must continuously stream in **OSCAL format** to the **FedRAMP 20x Continuous Assurance Dashboard**.

- **Vulnerability SLAs:** Critical and High vulnerabilities must be remediated within **30 days**; Medium vulnerabilities within **90 days**.

6.2 Internal Incident Escalation

- **Critical Incidents:** Confirmed security breaches, compromised internal admin accounts, or unauthorized network probes must be reported to the SOC within **1 hour**.
- **General Support & Escalations:**
  - **General Inquiries & Issues:** Email info@fedramp.gov for standard support, agency liaison questions, or updating security inbox addresses.
  - **Security & Incident Reporting:** Email fedramp_security@gsa.gov for urgent security concerns, emergency communications, or reporting confirmed/suspected incidents.

1266 W Paces Ferry Rd NW | Suite 674
Atlanta GA 30327
86borders.com

Document ID	86B-CAC-SCG
Summary	86Borders' FedRAMP 20x Class C (20xC) Secure Configuration & Governance Guide
Word Count	1296
FedRAMP Layer	Secure Configuration Guide
File Location	86Borders Confluence Directory
KSIs / Rulesets Answered	SCG-CSO-AUP SCG-CSO-PUB SCG-CSO-RSC SCG-CSO-SDF SCG-ENH-API SCG-ENH-CMP SCG-ENH-EXP SCG-ENH-MRG SCG-ENH-VRH
Version	v1
Date of Last Update	Aug 26, 2026