Secure Configuration Guide (SCG)

Resilinc Cloud Service Offering (CSO)
FedRAMP Rev5 Alignment

Effective Date: February 27, 2026

Version: 1.0

1. Purpose

This Secure Configuration Guide (SCG) provides instructions for securely accessing, configuring, operating, and decommissioning administrative and privileged accounts within the Resilinc Cloud Service Offering (CSO). This guide aligns with FedRAMP Rev5 requirements for cloud services listed in the FedRAMP Marketplace.

2. Scope

This guide applies to all FedRAMP-authorized deployments of the Resilinc CSO and addresses:

- Top-Level Administrative Accounts (Required)
- Privileged Accounts (Recommended)
- Security-related settings and implications
- Secure defaults
- API access management
- Logging and monitoring of administrative activity
- Secure decommissioning procedures
- Enhanced configuration capabilities

3. Definitions

Top-Level Administrative Account: Company Admin (Super User) with enterprise-wide authority.

Privileged Account: Any account assigned elevated licenses allowing modification of data, risk configurations, workflows, assessments, API integrations, or event management.

Standard User: A user without elevated configuration privileges.

4. Top-Level Administrative Accounts (Required)

4.1 Account Identification

The Top-Level Administrative Account is the Company Admin (Super User).

4.2 Secure Access

Authentication is provided via Single Sign-On (SSO). Password resets must be performed through the organization's Identity Provider (IdP). SSO users cannot reset passwords via the Resilinc portal.

Multi-Factor Authentication (MFA) may be enabled under Administration → Company Settings → Additional Settings. Disabling MFA increases risk of credential compromise and privilege escalation.

4.3 Secure Configuration

Administrative tools are located under the Administration menu. Company Admins may manage users, configure global settings, manage risk configurations, and administer API access.

4.4 Secure Operation

Company Admins should periodically review user roles and licenses, enforce least privilege, monitor API key generation, review risk configuration changes, and ensure MFA remains enabled.

4.5 Secure Decommissioning

Decommissioning must be performed by another active Company Admin or authorized Resilinc personnel. Remove the Company Admin role, remove licenses, mark the account Inactive or Blocked, disable SSO access, and regenerate or revoke API keys as applicable.

5. Privileged Accounts (Recommended)

Privileged Accounts include users assigned any of the following licenses: DATA_LOAD, API_ACCESS, WORKFLOWS, RISK_PRIORITIZATION, RISK_MITIGATION, WHAT_IF, CUSTOM_SURVEY, SUPPLY_CHAIN_VISIBILITY_SURVEY, EVENTWAR_ROOM.

Privileged accounts should use MFA, follow least privilege principles, and have elevated licenses removed when no longer required.

6. Persona-Based Recommended Configurations (Recommended)

Resilinc maintains a separate Persona-Based Recommended Configuration Guide outlining recommended license assignments and notification settings by role. Customers should align assignments with persona baselines.

7. Logging and Monitoring

Resilinc logs user management actions, global configuration changes, risk configuration updates, MFA enable/disable actions, and API key generation and resets. Logging supports auditability and anomaly detection.

8. Secure Default Configuration (Recommended)

Upon provisioning, MFA should be enabled, only necessary licenses assigned, risk weights validated, and API access restricted to authorized users.

9. Versioning and Release History (Recommended)

Version: 1.0

Effective Date: February 27, 2026

Summary of Changes: Initial Release.