[Admin] SkyShaper FedRAMP Security Configuration Guide

Summer 2026

[Text]

Table of Contents

1 Overview

FedRAMP Rev5 mandates the Secure Configuration Guide (SCG) requirements for all Cloud Service Providers, published at https://www.fedramp.gov/docs/rev5/balance/secure-configuration-guide/. This guide provides the instructions and guidelines below for customers to meet these requirements. Customers are responsible for ensuring their services are configured appropriately to meet them.

SST is authorized at the FedRAMP Moderate impact level. The SCG requirements (SCG-CSO- and SCG-ENH-) apply to all FedRAMP Marketplace cloud services regardless of impact level; this guidance aligns SST's administrative and privileged account configuration to the FedRAMP Moderate baseline.

SST is delivered across multiple FedRAMP-authorized environments: commercial cloud (AWS and Azure) and the CSO's own data centers. Settings owned at the AWS and Azure layers are governed by those providers' Secure Configuration Guides and are inherited. Controls within the CSO's own data centers are owned by SkyShaper and are addressed in this guidance.

This guidance describes platform capabilities and recommended secure configuration that apply to all tenants. Where a setting depends on a tenant's own request, such as identity assurance levels, accepted credential types, or revalidation intervals, SST provides the configurable capability and a secure recommendation while the specific value is selected by each tenant.

1.1 Roadmap

The remainder of this user guide cover’s how SST responds to each of the SGC requirements put forth by the FedRAMP program:

1. *Recommended Secure Configuration* (Section 2)
2. *Use Instructions* (Section 3)
3. *Public Guidance* (Section 4)
4. *Secure Defaults* (Section 5)
5. *Enhanced Capabilities* (Section 6)

2 Recommended Secure Configuration

This section includes the Recommended Secure Configuration requirement from the FedRAMP SCG and SST's response.

2.1 SCG-CSO-RSC

Providers MUST create, maintain, and make available recommendations for securely configuring their cloud services (the Secure Configuration Guide), including at least:

- **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.
- **Required:** Explanations of security-related settings that can be operated only by top-level administrative accounts, and their security implications.
- **Recommended:** Explanations of security-related settings that can be operated only by privileged accounts, and their security implications.

2.2 SST Recommendations and Instructions

SST supports all requirements in SCG-CSO-RSC. SST defines the following administrative and privileged accounts:

Scope	Account / role	Why it is top-level or privileged
Enterprise (top-level)	Tenant Managers	Provisions and manages the tenant's DH-CO and P-CO accounts
Tenant — data governance	Data Holder Compliance Officer (DH-CO)	Grants data access to Data Source folders under the governing data agreement
Tenant — project governance	Project Compliance Officer (P-CO)	Controls Project Environment membership and roles

Identity federation, encryption and key management, tenant-space provisioning, platform administration, and audit functions are operated by SST (the provider), not by the customer. They are addressed in SST's System Security Plan and are out of scope for this customer-facing guide.

2.2.1 Securely access, configure, operate, and decommission the top-level administrative account (Required):

SST uses the following procedures to secure top-level administrative accounts:

- **Access:** Enforce MFA; authenticate through the tenant's approved sign-in. Assign the account to named individuals only; prohibit shared use.
- **Configure:** Provision and assign the tenant's DH-CO and P-CO accounts under least privilege, granting each only the scope its governance role requires.
- **Operate:** Limit the account's use to provisioning and managing DH-CO and P-CO accounts; SST records all account actions in tamper-proof audit logging; re-validate the account's identity at tenant-defined intervals.
- **Decommission:** Revoke credentials immediately on role change or offboarding; reassign or retire the DH-CO and P-CO accounts it manages; the audit trail of these actions is retained.

2.2.2 Security-related settings operated only by the top-level account, and their implications (Required):

The following table explains the setting SST operates with and the related security implications.

Setting	Security implication
Provisioning and assignment of DH-CO and P-CO accounts	Determines who holds the privileged compliance-officer roles in the tenant, over-assignment, or failure to revoke, grants unwarranted data- and project-governance authority

2.2.3 Security-related settings operated only by privileged accounts, and their implications (Recommended):

The following table explains the security-related settings that SST operates with and their related implications.

Privileged role	Settings it controls	Security implication
DH-CO (Data Holder Compliance Officer)	Read / read-write grants to specific Data Holder folders per the governing data agreement	Over-granting exposes confidential Data Holder data beyond the agreement
P-CO (Project Compliance Officer)	Project Environment membership and roles	Controls who operates within a Project and affects data-pooling approvals

General privileged-account guidance: enforce least privilege consistent with applicable data agreements and tenant policy, require MFA, re-validate identity at tenant-specified intervals, and maintain separation of duties between the DH-CO and P-CO roles.

3 Use Instructions

This section includes the Use Instructions requirement from the FedRAMP SCG and SST's response.

3.1 SGC-CSO-AUP

Providers ~~MU~~ST include instructions in the FedRAMP authorization package that explain how to obtain and use the Secure Configuration Guide.

3.2 SST Response

SST supports SCG-CSO-AUP by providing access to the SST Secure Configuration User Guide to Users without requiring the Users to log in ~~to S~~ST systems. This SST Secure Configuration User Guide resides on the SST marketing website, separate from the SST User Platform and User Security Platform.

4 Public Guidance

This section includes the Public Guidance requirement from the FedRAMP SCG and SST's response.

4.1 SGC-CSO-PUB

Providers SHOULD make the Secure Configuration Guide available publicly.

4.2 SST Response

This document is the SST Secure Configuration Guide. SST makes it available to its customers publicly through the SST marketing website. Through this website, Users can access the document without going through the SST User Platform or SST User Security Platform.

5 Secure Defaults

This section includes the Secure Defaults requirement from the FedRAMP SCG and SST's response.

5.1 SGC-CSO-SDF

Providers SHOULD set all settings to their recommended secure defaults for top-level administrative accounts and privileged accounts when initially provisioned.

5.2 SST Response

SST applies the following secure defaults to top-level administrative and privileged accounts at initial provisioning, so that new accounts never start in a weak or misconfigured state:

Area	**Recommended secure default**
Authentication	MFA required, federated identity / SSO and credential/assurance options configurable to tenant requirements. SST will accommodate tenant-specified configurations provided they meet the FedRAMP Moderate baseline — IAL2, AAL2, and FAL2 per NIST SP 800-63.
Encryption at rest	AES-256, FIPS 140-3 validated, enabled
Encryption in transit	TLS 1.3 (TLS 1.2 minimum), AES-256, FIPS 140-3 validated, enabled
RBAC	Deny-by-default, least privilege
Apps-Platform isolation	Enabled; cross-platform transfer through approved mechanisms only
Audit logging	Enabled and tamper-proof, audit functions maintained by SST
Identity revalidation	Enabled, interval set to tenant requirements

6 Enhanced Capabilities

These recommendations apply to all cloud service offerings in the FedRAMP Marketplace for enhanced capabilities related to the SCG. Each subsection includes the FedRAMP recommendation and SST's response

6.1 Comparison Capability

6.1.1 SGC-ENH-CMP

Providers SHOULD offer the capability to compare all current settings for top-level administrative accounts and privileged accounts to the recommended secure defaults.

6.1.2 SST Response

SST provides a configuration-comparison view that evaluates the current settings of top-level administrative and privileged accounts against the recommended secure defaults in this guide, surfacing deviations for remediation.

6.2 Export Capability

6.2.1 SGC-ENH-EXP

Providers SHOULD offer the capability to export all security settings in a machine-readable format.

6.2.2 SST Response

SST supports export of security settings for administrative and privileged accounts in an, machine-readable format suitable for audit evidence, drift detection, and compliance tooling.

6.3 API Capability

6.3.1 SGC-ENH-API

Providers SHOULD offer the capability to view and adjust security settings via an API or similar capability.

6.3.2 SST Response

SST does not offer API to view and adjust security settings at this time.

6.4 Machine-Readable Guidance

6.4.1 SGC-ENH-MRG

Providers SHOULD also provide the Secure Configuration Guide in a machine-readable format that can be used by customers or third-party tools to compare against current settings.

6.4.2 SST Response

SST provides an version of this guidance that customer or third-party tooling can use to compare against current settings.

6.5 Versioning and Release History

6.5.1 SGC-ENH-VRH

Providers SHOULD provide versioning and a release history for recommended secure default settings for top-level administrative accounts and privileged accounts as they are adjusted over time.

6.5.2 SST Response

SST maintains versioning and a release history for the recommended secure default settings in this guide, updated as those defaults are adjusted over time.

DO NOT DELETE ANYTHING BELOW THIS LINE

Please do not delete these endnotes.