[Admin] SkyShaper Technologies FedRAMP Secure Configuration Guide

July 2026

FedRAMP Rev5 mandates the Secure Configuration Guidelines ("SCG") requirements for all Cloud Service Providers, published at https://www.fedramp.gov/2026/providers/rev5/rules/secure-configuration-guide/. This Secure Configuration Guide ("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.

This Guide is intended for privileged Users, such as Tenant Managers and Compliance Officers.

Table of Contents

Revision Log

DATE	VERSION	MANUAL SECTION	REVISION	AUTHOR
07/01/2026	1.0	All	User Guide created	Tech Writing Team

1 Overview

SkyShaper Technologies is independently assessed and verified by a Third Party Assessment Organization (3PAO) annually to provide security and privacy protections equivalent to FedRAMP Moderate impact level. This Secure Configuration Guide ("Guide") covers FedRAMP's SCG requirements, which apply to all FedRAMP Marketplace Cloud Service Offerings ("CSO") regardless of impact level. This Guide aligns SkyShaper Technologies administrative and privileged account configuration to the FedRAMP Moderate baseline.

SkyShaper Technologies provides SkyShaper SaaS Tools as a software-as-a-service that configures computational and data access platforms for use among research groups and similar entities. SkyShaper SaaS Tools is delivered across multiple FedRAMP-authorized commercial cloud (Amazon Web Services ("AWS") and Azure) and the data centers owned by the SkyShaper as a Cloud Service Provider. SkyShaper is responsible for managing majority of controls and configurations within AWS, Azure, and data centers owned by SkyShaper in accordance to strict federal agency and industry standards (e.g., DISA, CIS Benchmarks), but some configurations are dependent on the tenants.

This Guide describes SkyShaper SaaS Tools platform capabilities and recommended secure configuration that all SkyShaper SaaS Tools tenants can apply.

1.1 Roadmap

The remainder of this Guide covers how SkyShaper SaaS Tools implements each of the SCG 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); and
5. *Enhanced Capabilities* (Section 6).

2 Recommended Secure Configuration (SCG-CSO-RSC)

This section includes the Recommended Secure Configuration requirement from the FedRAMP SCG and SkyShaper SaaS Tools' implementation.

2.1 SCG-CSO-RSC Requirements

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 SkyShaper SaaS Tools Recommendations and Instructions

SkyShaper SaaS Tools supports all requirements in SCG-CSO-RSC. SkyShaper SaaS Tools defines the following administrative and privileged accounts, which includes Tenant Managers, Data Holder Compliance Officers ("DH-CO"), and Project Compliance Officers ("P-CO"):

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	DH-CO	Grants data access permissions to Projects under the governing data agreement
Tenant — project governance	P-CO	Controls Project Environment membership and User access to data and folders, controls data and file transfer permissions for the Project

Identity federation, encryption and key management, tenant-space provisioning, platform administration, and audit functions are operated by SkyShaper SaaS Tools (the provider), not by the customer. These aspects are addressed in SkyShaper SaaS Tools' 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):

SkyShaper SaaS Tools uses the following procedures to secure top-level administrative accounts:

- **Access:** Enforce multifactor authentication (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 the rules of 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; SkyShaper SaaS Tools records all account actions in tamper-proof audit logging; re-validate the account's identity at tenant-defined intervals, with a maximum interval of one year.
- **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 SkyShaper SaaS Tools 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
Regulating account use to one individual per account	Prevents repudiation issues caused by shared use of account by more than one individual

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

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

PRIVILEGED ROLE	SETTINGS IT CONTROLS	SECURITY IMPLICATION
DH-CO	Data access permissions to Projects, per governing data agreement	Over-granting exposes confidential Data Holder data beyond the agreement
P-CO	Project Environment membership and User access to data and folders, data and file transfer permissions for the Project	Controls who operates within a Project and affects data-pooling approvals, controls what data and files can be transferred to and from the Project Environment

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 (SCG-CSO-AUP)

This section includes the Use Instructions requirement from the FedRAMP SCG and SkyShaper SaaS Tools' implementation.

3.1 SCG-CSO-AUP Requirements

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

3.2 SkyShaper SaaS Tools Implementation

SkyShaper SaaS Tools supports SCG-CSO-AUP by providing access to the Guide to Users without requiring the Users to log in to SkyShaper SaaS Tools systems. This Guide resides on the SkyShaper website.

4 Public Guidance (SCG-CSO-PUB)

This section includes the Public Guidance requirement from the FedRAMP SCG and SkyShaper SaaS Tools' implementation.

4.1 SCG-CSO-PUB Requirements

Providers SHOULD make the Secure Configuration Guide available publicly.

4.2 SkyShaper SaaS Tools Implementation

This Guide is available to customers publicly through the SkyShaper website. Through this website, Users can access the Guide without going through the SkyShaper SaaS Tools systems.

5 Secure Defaults (SCG-CSO-SDF)

This section includes the Secure Defaults requirement from the FedRAMP SCG and SkyShaper SaaS Tools' implementation.

5.1 SCG-CSO-SDF Requirements

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

5.2 SkyShaper SaaS Tools Implementation

SkyShaper SaaS Tools 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	FIDO2-compliant or stronger MFA solution,
RBAC	Deny-by-default, least privilege
Identity revalidation	Enabled, interval set to tenant requirements

The following settings are standard across SkyShaper SaaS Tools and cannot be adjusted by top-level administrative or privileged accounts:

AREA	SECURE DEFAULT
Authentication	Federated identity / SSO and credential/assurance options configurable to tenant requirements. SkyShaper SaaS Tools 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
Apps-Platform isolation	Enabled; cross-platform transfer through approved mechanisms only
Audit logging	Enabled and tamper-proof, audit functions maintained by SkyShaper SaaS Tools

6 Enhanced Capabilities

These recommendations apply to all cloud service offerings in the FedRAMP Marketplace for enhanced capabilities (“ENH”) related to the SCG. Each subsection includes the FedRAMP recommendation and SkyShaper SaaS Tools' implementation

6.1 Comparison Capability (SCG-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.

6.1.1 SkyShaper SaaS Tools Implementation

SkyShaper SaaS Tools 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. For more information on these settings, refer to Section 2.2.

6.2 Export Capability (SCG-ENH-EXP)

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

6.2.1 SkyShaper SaaS Tools Implementation

SkyShaper SaaS Tools 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 (SCG-ENH-API)

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

6.3.1 SkyShaper SaaS Tools Implementation

SkyShaper SaaS Tools does not offer API to view and adjust security settings at this time.

6.4 Machine-Readable Guidance (SCG-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.

6.4.1 SkyShaper SaaS Tools Implementation

SkyShaper SaaS Tools provides a machine-readable PDF version of this Guide that customer or third-party tooling can use to compare against current settings through the SkyShaper website.

6.5 Versioning and Release History (SCG-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.

6.5.1 SkyShaper SaaS Tools Implementation

SkyShaper SaaS Tools maintains versioning and a release history for the recommended secure default settings in this Guide, updated as those defaults are adjusted over time. The Revision Log table in this Guide details the release history.