FedRAMP

Secure Configuration Guide

Kovr Nova

CSP Name	Kovr.AI Corp
CSO Name	Kovr Nova
FedRAMP Package ID	F1206111371
FedRAMP Impact Level	Moderate
Document Version	1.0
Effective Date	March 1, 2026
Classification	Public

Kovr.AI Corp
11921 Freedom Dr, Suite 730, Reston VA 20190

1. Purpose and Scope

1.1 Document Purpose

This Secure Configuration Guide (SCG) provides federal agency customers with guidance for securely configuring Kovr Nova in compliance with FedRAMP requirements. This document addresses FedRAMP SCG requirements as defined in the FedRAMP Rev5 Balance Improvement Release (v0.9.0-beta, February 2026).

1.2 System Overview

CSP Name	Kovr.AI Corp
CSO Name	Kovr Nova
Service Model	Software as a Service (SaaS)
Deployment Model	Commercial Cloud (Multi-Tenant)
FedRAMP Impact Level	Moderate
FIPS 199 Categorization	Moderate
Infrastructure Provider	Knox Systems (FedRAMP Moderate)
Fully Operational Date	August 2025

1.3 Intended Audience

This document is intended for federal agency Information System Security Officers (ISSOs), Authorizing Officials (AOs) and their designated representatives, agency IT administrators responsible for Kovr Nova configuration, third-party assessment organizations (3PAOs), and compliance and audit personnel.

2. How to Obtain and Use This Guide

Requirement: SCG-CSO-AUP (MUST)

2.1 Document Availability

This SCG is available through the following channels:

Knox SCG Page	https://knoxsystems.com/secure-configuration-guides
FedRAMP Package	F1206111371
Direct Request	security@kovr.ai

2.2 How to Use This Guide

Agency customers should use this guide to review administrative account types and select appropriate roles for personnel, verify settings against secure defaults documented in this guide, establish account lifecycle procedures aligned with agency policies, and document any operational considerations in agency authorization documentation.

2.3 Version Notification

Customers will be notified of SCG updates through the Knox SCG page at https://knoxsystems.com/secure-configuration-guides.

2.4 Security Contact

For questions regarding this SCG or Kovr Nova security:

System Owner / ISSO	Sri Iyer, CTO
Email	sri@kovr.ai
Phone	(571) 497-5687
Address	11921 Freedom Dr, Suite 730, Reston VA 20190

3. Top-Level Administrative Accounts

Requirement: SCG-CSO-RSC Item 1 (MUST)

This section provides instructions for securely accessing, configuring, operating, and decommissioning top-level administrative accounts.

3.1 Administrative Account Types

Kovr Nova uses a single top-level administrative role. In the Kovr Nova interface, this role is labeled "Admin" in the user management screens and role selection dropdown.

Account Type	Purpose	Max Count	MFA Required	Security Impact
Admin	Top-level administrative role. Manages all settings, users, compliance frameworks, evidence, and assessments.	Unlimited	Yes	Medium

Security Impact Rationale: Kovr Nova is a compliance management platform that does not process or store sensitive PII, financial data, or classified information. The blast radius of administrative access is limited to compliance documentation and workflow management.

3.2 Account Access (Creation and Provisioning)

3.2.1 Initial Account Setup

During customer onboarding, Kovr provisions the initial Admin account through the following process:

1. Customer designates authorized personnel during contract execution.
2. Kovr sends account invitations to designated email addresses.
3. Administrator completes MFA enrollment (TOTP, or CAC/PIV).
4. Account activates upon first successful login.

3.2.2 Additional Administrator Creation

To create additional Admin accounts:

1. Navigate to Settings in the Kovr Nova application.
2. Select Create User.
3. Enter user name and email address.
4. Select "Admin" as the role.
5. The system sends invitation emails (expires in 24 hours).
6. The new administrator completes MFA enrollment and activates the account.

3.3 Account Configuration

After account creation, the following configuration is required:

- Configure MFA method(atleast two required with one primary): Email, TOTP authenticator app, or CAC/PIV smart card.
- Set password meeting complexity requirements (minimum 15 characters, mixed case, number, special character).
- Review and accept terms of use.

3.4 Account Operation

The following security requirements apply to all Admin account sessions:

- MFA required for all sessions.
- Session idle timeout: Enabled
- Maximum session duration: Enabled
- Password rotation: Enabled

3.5 Account Decommissioning

To remove an Admin account:

1. Navigate to Settings, then User Management.
2. Locate the account and select Delete.

3. Confirm deletion action.
4. Active sessions terminate at the next session timeout.
5. Audit log entry generated automatically.

Note: Kovr Nova does not support account disabling; accounts must be deleted for permanent removal.

4. Administrative Account Security Settings

Requirement: SCG-CSO-RSC Item 2 (MUST)

This section documents security-related settings and their security implications. All settings in Kovr Nova are enforced platform defaults and cannot be modified by customers, ensuring a consistent security posture across all tenants.

4.1 Authentication Settings

Setting	Value	Configurable	Impact
Multi-Factor Authentication	Required (TOTP, or CAC/PIV)	No (Enforced)	High
SSO Integration	Enabled	Yes	High
Password Minimum Length	Enabled	No (Enforced)	High
Password Complexity	Upper, lower, number, special	No (Enforced)	High
Password Expiration	Enabled	No (Enforced)	High

4.2 Session Management Settings

Setting	Value	Configurable	Impact
Session Idle Timeout	Enabled	No (Enforced)	Medium
Maximum Session Duration	Enabled	No (Enforced)	Medium
Concurrent Session Limit	Unlimited	No (Enforced)	Medium

4.3 Account Lockout Settings

Setting	Value	Configurable	Impact
Failed Login Threshold	Enabled	No (Enforced)	High
Lockout Duration	Until Kovr admin unlocks	No (Enforced)	High

4.4 Access Control Settings

Setting	Value	Configurable	Impact
Role-Based Access Control	Enabled	No (Enforced)	Medium
IP Address Allowlisting	Not supported	N/A	N/A
Geographic Restrictions	Not supported	N/A	N/A
Time-Based Restrictions	Not supported	N/A	N/A

Note: IP, geographic, and time-based restrictions should be enforced at the respective Identity Provider (IdP) level for agencies/customers requiring these controls.

4.5 Audit and Logging Settings

Setting	Value	Configurable	Impact
Audit Logging	Enabled	No (Enforced)	Medium
Audit Log Retention	Enabled	No (Enforced)	Medium
Login/Logout Events	Logged	No (Enforced)	Medium
Failed Login Attempts	Logged	No (Enforced)	Medium
Certificate Auth Events	Logged (CAC/PIV)	No (Enforced)	Medium
Configuration Changes	Logged	No (Enforced)	Medium
User Management Events	Logged	No (Enforced)	Medium
Data Access Events	Logged	No (Enforced)	Medium
Evidence Uploads/Changes	Logged	No (Enforced)	Medium
Compliance Activities	Logged	No (Enforced)	Medium
Log Export Capability	Not supported through the app.	N/A	N/A

4.6 Data Protection Settings

Setting	Value	Configurable	Impact
Encryption at Rest	Enabled	No (Enforced)	Medium

Encryption in Transit	TLS 1.2 minimum	No (Enforced)	Medium
Key Management	Knox managed	No (Enforced)	Medium
Customer-Managed Keys (BYOK)	Not supported	N/A	N/A
Data Backup Frequency	Enabled	No (Enforced)	Medium
Backup Encryption	Enabled	No (Enforced)	Medium
Data Export	Reports and artifacts	Yes	Medium

5. Privileged Account Settings

Requirement: SCG-CSO-RSC Item 3 (SHOULD)

This section documents privileged accounts beyond the top-level Admin role.

5.1 Privileged Role Definitions

Account Type	Purpose	Max Count	MFA Required	Security Impact
None	There is no other privileged account other than the “Admin” role. Two other non-privileged roles available are: **Member:** Create and edit compliance content, evidence, and assessments. **Auditor:** Read-only access to compliance data (beta).	Unlimited	Yes	Low

5.2 Role Assignment Procedures

To assign roles to users, navigate to Settings, select Create User, enter user name and email address, select the appropriate role (Member or Auditor), and save to send the invitation.

5.3 Access Review Requirements

Agency customers are responsible for periodic access reviews per agency policy, review upon personnel changes, annual recertification of all accounts, and documentation of access review results.

6. Secure Default Settings

Requirement: SCG-CSO-SDF (SHOULD)

6.1 Default Setting Confirmation

All security settings listed in this SCG are configured to secure default values at initial account provisioning. Kovr Nova enforces all security settings platform-wide; customers cannot modify or relax security controls.

6.2 Enforced Security Posture

Unlike platforms that allow customers to adjust security settings, Kovr Nova maintains a consistent, enforced security baseline across all tenants. This approach eliminates configuration drift, ensures consistent security posture for all federal customers, reduces risk of misconfiguration, and simplifies compliance verification.

Appendix A: FedRAMP Requirements Traceability

Requirement ID	Obligation	Description	SCG Section
SCG-CSO-RSC (1)	MUST	Admin account lifecycle instructions	Section 3
SCG-CSO-RSC (2)	MUST	Admin account security settings	Section 4
SCG-CSO-AUP	MUST	Instructions to obtain/use SCG	Section 2
SCG-CSO-RSC (3)	SHOULD	Privileged account settings	Section 5
SCG-CSO-PUB	SHOULD	Public availability	Section 2
SCG-CSO-SDF	SHOULD	Secure defaults	Section 6
SCG-ENH-CMP	SHOULD	Comparison capability	Appendix B
SCG-ENH-EXP	SHOULD	Export capability	Appendix B
SCG-ENH-API	SHOULD	API capability	Appendix B
SCG-ENH-MRG	SHOULD	Machine-readable format	Appendix B
SCG-ENH-VRH	SHOULD	Version history	Appendix C

Appendix B: Enhanced Capabilities

Requirements: SCG-ENH-CMP, SCG-ENH-EXP, SCG-ENH-API, SCG-ENH-MRG (all SHOULD)

B.1 Comparison Capability (SCG-ENH-CMP)

Feature Available	No
Rationale	Not applicable. All settings are platform-enforced secure defaults and cannot be modified by customers.

B.2 Export Capability (SCG-ENH-EXP)

Feature Available	No
Rationale	Not applicable. All settings are platform-enforced and cannot be modified by customers.

B.3 API Capability (SCG-ENH-API)

Feature Available	No
Rationale	Not applicable. All settings are platform-enforced and cannot be modified by customers.

B.4 Machine-Readable Format (SCG-ENH-MRG)

Format Available	Planned
Format Type	OSCAL (planned)
Notes	OSCAL machine-readable version is planned for a future release.

Appendix C: Version History

Requirement: SCG-ENH-VRH (SHOULD)

Version	Date	Author	Changes
1.0	March 1, 2026	Sri Iyer, CTO	Initial release

Appendix D: Glossary

Term	Definition
AAL	Authenticator Assurance Level per NIST SP 800-63B
AO	Authorizing Official
CAC	Common Access Card - DoD smart card for identification and authentication
CSO	Cloud Service Offering
CSP	Cloud Service Provider
FIDO2	Fast Identity Online 2 - passwordless authentication standard

ISSO	Information System Security Officer
MFA	Multi-Factor Authentication
PIV	Personal Identity Verification - federal smart card standard per FIPS 201
RBAC	Role-Based Access Control
SaaS	Software as a Service
SCG	Secure Configuration Guide
SSO	Single Sign-On
TOTP	Time-based One-Time Password
3PAO	Third-Party Assessment Organization

Appendix E: Document Approval

Prepared by:	Sri Iyer, CTO	Date: March 1, 2026
Approved by:	Sri Iyer, CTO	Date: March 1, 2026

End of Document