STIG-Aligned Deployment Guide

Security Implementation Guidance for the Sepio Platform

Executive Summary

This guide provides STIG-aligned configuration guidance for customers deploying the Sepio Platform in customer-managed environments, including on-premises, IaaS, and air-gapped deployments. It maps selected DISA STIG control intents to Sepio platform capabilities, recommended configurations, and customer operational responsibilities.

The guide is intended to support secure implementation, audit preparation, and ongoing security operations for organizations that require high-assurance deployment practices. It should be used alongside Sepio technical documentation, customer security policies, applicable operating system STIGs, and formal assessment procedures.

Important note

This guide is intended to help customers deploy and operate the Sepio Platform in a manner aligned with DISA STIG security principles. It is not an official DISA STIG, does not replace formal STIG assessment procedures, and does not by itself establish compliance. Final compliance depends on the customer environment, implementation, validation, and ongoing security operations.

Intended Audience

- Security architects and system owners responsible for high-assurance environments.
- Platform administrators deploying or operating Sepio in customer-managed infrastructure.
- Compliance, audit, and risk teams preparing for STIG-aligned assessments.
- Security engineers validating access control, logging, cryptography, monitoring, backup, and recovery practices.

Document Objective

This document provides security configuration guidance and deployment recommendations for the Sepio Platform in customer-managed environments, including on-premises, infrastructure-as-a-service, and air-gapped deployments. The guidance follows the intent of the Defense Information Systems Agency Security Technical Implementation Guide framework and applies selected STIG control objectives to Sepio deployment and operation.

The document focuses on operational and configuration recommendations rather than certification claims. It assumes a customer-managed deployment model in which the customer controls the underlying operating system, identity services, network architecture, infrastructure services, backup procedures, and security operations.

All recommendations should be reviewed against the customer approved baseline, mission requirements, system security plan, and applicable organizational policies.

Sepio Platform Overview and Security Posture

The Sepio Platform provides hardware asset visibility and risk management using patented Layer 1 physical-layer fingerprinting technology. Sepio helps identify and assess risk across IT, OT, IoT, and peripheral devices in enterprise environments.

Sepio is designed to support the expectations of regulated and high-assurance customers through secure-by-design principles, role-based access control, centralized audit logging, secure communications, configuration governance, and continuous asset risk monitoring. Sepio also maintains documented security policies, continuous risk management processes, independent security testing, and customer-facing security documentation through the Sepio Trust Center.

In customer-managed deployments, Sepio can be configured to align with STIG security principles when combined with appropriate operating system hardening, customer network controls, identity provider controls, certificate management, logging, backup, and operational security practices.

Why Sepio Matters in STIG-Aligned Environments

STIG-aligned environments depend on trusted configuration, controlled access, secure communications, auditability, and continuous operational discipline. Sepio extends this discipline to the hardware layer by helping organizations discover, verify, and monitor connected assets, including devices that may be unmanaged, misclassified, or operating outside expected policy.

By providing hardware-level visibility and risk context, Sepio helps security teams strengthen the integrity of high-assurance environments where unknown, unauthorized, or misrepresented devices can create operational and compliance risk.

How to use this guide

- Use this guide as a planning and validation aid during Sepio deployment design, implementation, and audit preparation.
- Apply the relevant Sepio application settings together with customer-managed operating system, network, identity, certificate, monitoring, backup, and recovery controls.
- Validate the underlying operating system and infrastructure against the customer approved STIG baseline using approved assessment processes and tools.
- Maintain ongoing review of logs, configuration changes, vulnerabilities, backups, and recovery procedures as part of continuous security operations.

Reference documentation

Sepio operators should use Sepio technical documentation for authoritative product configuration guidance, including installation procedures, security settings, integrations, logging, backup, and operational best practices.

Shared Responsibility Model

STIG alignment is achieved through a combination of Sepio platform capabilities, customer configuration, and continuous customer validation. The following model summarizes the recommended division of responsibilities for customer-managed deployments.

Sepio Provides	Customer Configures	Customer Validates
Application security controls, RBAC, audit logging, secure communications, documented deployment guidance, integration options, and product release guidance.	Identity provider integration, MFA policy, TLS certificates, network segmentation, firewall rules, SIEM/SOAR forwarding, VM/OS hardening, backups, and recovery procedures.	Approved STIG baseline, SCAP/SCC checks where applicable, patch compliance, audit log review, operational procedures, exception handling, and compensating controls.
Product documentation, recommended settings, and operational guidance for Sepio-managed application components.	Customer-owned infrastructure and environmental controls required to operate Sepio securely.	Evidence collection, audit preparation, control validation, continuous monitoring, and periodic reassessment.

STIG Control-by-Control Mapping

The following mapping summarizes selected STIG control intents, relevant Sepio capabilities, recommended customer configurations, and customer validation responsibilities. The mapping should be tailored to the customer approved baseline and deployment architecture.

STIG Control	Control Intent	Sepio Configuration Guidance	Customer Responsibility
AC-2 Account Management	Manage lifecycle of user accounts	Configure RBAC users via Sepio UI; disable unused accounts; leverage customer's SSO/SAML **Relevant instructions:** → Users Management → SAML IdP Configuration → User Types	Create, disable, and maintain RBAC users' access to UI
AC-3 Access Enforcement	Enforce approved authorizations	Enforces access based on assigned roles and scopes (sites, asset groups) via Sepio UI; leverage customer's SSO/SAML **Relevant instructions:** → Users Management → SAML IdP Configuration	Define and enforce access policies
AC-5 Separation of Duties	Prevent conflict of roles	Define separate administrative, operational, and read-only roles in Sepio UI **Relevant instructions:** → Users Management	Assign non-overlapping roles

STIG Control	Control Intent	Sepio Configuration Guidance	Customer Responsibility
AC-6 Least Privilege	Limit privileges to minimum necessary	Define separate administrative, operational, and read-only roles in Sepio UI **Relevant instructions:** → Users Management	Review role assignments
IA-2 Identification and Authentication	Uniquely identify and authenticate users	Rely on enterprise IdP credential lifecycle; configure account lockout thresholds **Relevant instructions:** → SAML IdP Configuration → Authentication and Authorization	Integrate IdP, enforce MFA
IA-5 Authenticator Management	Protect and manage credentials	Rely on enterprise IdP credential lifecycle; configure account lockout thresholds **Relevant instructions:** → SAML IdP Configuration → Authentication and Authorization	Enforce password/MFA policies

STIG Control	Control Intent	Sepio Configuration Guidance	Customer Responsibility
AU-2 Auditable Events	Define events to be logged	Configure RBAC users via Sepio UI; disable unused accounts; leverage customer's SSO/SAML **Relevant instructions:** → Event logs → Syslog configuration → Logs operation and retention	Select events and retention
AU-6 Audit Review and Analysis	Review and analyze logs	Export or forward Sepio logs to SIEM for correlation and review **Relevant instructions:** → CEF Operations → Syslog configuration → Splunk Integration	Monitor logs via SIEM
AU-12 Audit Generation	Generate audit records	Sepio generates audit logs for user and system actions **Relevant instructions:** → Post-Installation Checklist → Events and Logging System	Ensure logging is enabled

STIG Control	Control Intent	Sepio Configuration Guidance	Customer Responsibility
CM-2 Baseline Configuration	Maintain secure baselines	A system baseline is established using STIGs. In customer-hosted deployments, the system owner defines, approves, and enforces the operating system, network, and infrastructure baseline. Sepio provides documented reference architectures and configuration guidance to support establishment and maintenance of the approved baseline. Baseline validation may be performed by the system owner using approved STIG assessment tools such as the SCAP Compliance Checker (SCC) **Relevant tools:** **Definition of the OS baseline requirements** → Ubuntu 24.04 LTS Security Technical Implementation Guide **To validate the OS against the STIG** → MITRE Ubuntu 24.04 LTS Security Technical Implementation Guide	Define, approve, enforce, and document the system baseline; validate compliance and approve baseline changes

STIG Control	Control Intent	Sepio Configuration Guidance	Customer Responsibility
CM-6 Configuration Settings	Restrict configuration changes	Configuration settings are established using this document as benchmark and implemented by the system owner. Sepio provides documented and configurable application-level security settings, including access control, authentication integration, logging, and cryptographic options	Implement, enforce, monitor, control, approve any deviations of configuration settings
CM-7 Least Functionality	Disable unnecessary functions	The underlying operating system is configured in accordance with the DISA Ubuntu 24.04 LTS STIG to enforce least functionality. STIG compliance may be validated using approved assessment tools. Any required deviations from STIG-recommended settings are documented, formally approved by the system owner, and mitigated through compensating security controls	Harden OS and services

STIG Control	Control Intent	Sepio Configuration Guidance	Customer Responsibility
IA-7 Cryptographic Module Authentication	Protect authentication mechanisms	The Sepio platform includes an Authentication service (Auth UI) that handles user authentication and OAuth/ OIDC token issuance. Authentication traffic is restricted to secure channels only; the reverse proxy (Nginx) is configured to accept connections exclusively over HTTPS (TCP 443). Internal service-to-service communication is encrypted using TLS version 1.2 or higher. Cryptographic operations rely on operating-system-provided cryptographic libraries and customer-approved trust anchors. Authentication relies exclusively on authenticated cryptographic mechanisms. Only TLS 1.2 and TLS 1.3 are permitted; legacy protocols and unauthenticated or weak cipher suites (e.g., RC4, 3DES, ADH) are disabled to prevent downgrade or unauthenticated crypto paths	Configure and enforce approved cryptographic modules, certificate authorities

STIG Control	Control Intent	Sepio Configuration Guidance	Customer Responsibility
SC-7 Boundary Protection	Monitor and control communications	When deployed in a customer managed environment, Sepio Platform operates within network boundaries enforced by customer controlled segmentation and firewall rules. Sepio exposes only documented management and API interfaces, supports deployment behind network security controls, and does not bypass or weaken boundary protections **Relevant information:** → Sepio's Connectivity Diagram	Configure firewalls and segmentation
SC-12 Cryptographic Key Establishment	Protect cryptographic keys	Sepio relies on OS-provided cryptographic services and customer-managed certificates for cryptographic key establishment and management, supporting secure key rotation and trust anchoring without embedding customer keys **Relevant instructions:** → Sepio Installation on customer owned infrastructure	Manage OS certificates and keys

STIG Control	Control Intent	Sepio Configuration Guidance	Customer Responsibility
SC-13 Cryptographic Protection	Protect data in transit	Authentication relies exclusively on authenticated cryptographic mechanisms. Only TLS 1.2 and TLS 1.3 are permitted; legacy protocols and unauthenticated or weak cipher suites (e.g., RC4, 3DES, ADH) are disabled to prevent downgrade or unauthenticated crypto paths	Enforce TLS policies
SI-2 Flaw Remediation	Identify and remediate vulnerabilities	Sepio maintains a documented vulnerability and patch management process covering Sepio-provided software components, including severity-based prioritization, SLAs, customer notification, and verification of remediation. In customer-hosted deployments, patching and maintenance of the underlying OS and infrastructure are the responsibility of the system owner **Additional Information:** → Sepio platform release notes	Patch OS and dependencies

STIG Control	Control Intent	Sepio Configuration Guidance	Customer Responsibility
SI-4 System Monitoring	Detect security events	Generate security events and forward to SIEM/SOAR platforms **Relevant instructions:** → CEF Operations → SysLog configuration → Splunk Integration → Events and Logging System	Integrate monitoring and alerts
CP-9 System Backup	Protect system data backups	Support backup of Sepio VM and configuration data **Relevant instructions:** → Back, Redundancy and High Availability	Configure secure backups
CP-10 System Recovery	Recover system after failure	Restore Sepio from backup in accordance with customer DR procedures **Relevant instructions:** → Back, Redundancy and High Availability	Test recovery procedures

Summary

This guide provides STIG-aligned configuration guidance for deploying the Sepio Platform in customer-managed environments. By implementing the recommendations in this document and applying appropriate operating system, network, identity, cryptographic, monitoring, backup, and operational security controls, customers can deploy Sepio in a manner consistent with DISA STIG security principles.

Final compliance depends on customer implementation, validation, continuous security operations, and applicable assessment procedures. Sepio should be used as part of a broader high-assurance security architecture that includes approved baselines, secure configuration management, access control, audit logging, monitoring, vulnerability remediation, backup, and recovery practices.