Aembit NIST SP 800-171 Rev 3 Compliance Guide

Aembit's Workload IAM platform helps organizations secure non-human identity and access. Aembit is dedicated to providing the security controls needed globally to ensure that organizations are able to meet their compliance requires. This summarized guide, and many others like it, are provided by Aembit to help organizations map specific compliance controls with Aembit capabilities. For more detailed information, please reach out to your local Aembit team.

3.1 Access Control

Control		Summarized Requirement	How Aembit Supports This Control
3.1.1	Account Management	Manage system accounts (e.g., create, enable, modify, disable, remove).	Aembit automatically mints ephemeral tokens (credentials) for workloads based on cryptographically verified environment attributes (e.g., AWS instance metadata). These ephemeral tokens expire in minutes and cannot be reused, effectively managing machine/service accounts without manual intervention.
3.1.2	Access Enforcement	Enforce approved authorizations for logical access to information and resources.	Aembit policy-driven enforcement allows credentials only if the workload meets defined posture and identity checks (e.g., correct cloud role, geo-location, day/time conditions, EDR posture). If any requirement fails, Aembit does not authorize access and does not inject credentials.
3.1.5	Least Privilege	Employ least privilege, limiting privileges to the minimum necessary.	Aembit issues narrowly scoped, short-lived credentials per workload. Each workload only gains the minimum access (e.g., to specific services/APIs) required, reducing attack surface and preventing broad or persistent privileges.
3.1.6	Privileged Account Management	Apply extra protections and limitations for privileged accounts/functions.	If a workload needs privileged access, Aembit enforces stricter posture checks (e.g., verified EDR posture, limited IP ranges). Privileged credentials never reside in code or config files—they're ephemeral and minted when needed.
3.1.12	Remote Access	Enforce requirements to protect remote access to organizational systems.	Aembit can incorporate GeoIP checks, time-based rules, and EDR posture to verify a remote workload's legitimacy before issuing credentials. If any condition fails (e.g., unapproved location), remote access is denied or immediately revoked

3.3 Audit and Accountability

Control		Summarized Requirement	How Aembit Supports This Control
3.3.1	Event Logging	Log events (e.g., security-relevant actions) that occur in the system.	Aembit logs each credential issuance event, including requesting workload identity attributes, posture checks, timestamp, and whether issuance was granted or denied. Logs may be exported to be used in SIEM/SOARs.
3.3.3	Audit Record Generation	Generate audit records that facilitate the reconstruction of events.	For every credential request, Aembit captures who/what (the workload identity), when (timestamp), where (metadata/posture signals), and outcome (issued/denied). Aembit logs also include sanitized

			response metadata. These records can be exported to a SIEM for correlation and analysis.
3.3.7	Time Stamps	Use and protect accurate time stamps in audit records.	Aembit automatically includes precise time stamps (based on its secure control plane) with each event. Because ephemeral credentials also rely on time-based expiration, time synchronization is inherently required and monitored.

3.5 Identification and Authentication

	Control	Summarized Requirement	How Aembit Supports This Control
3.5.1	User (or Service Account) Identification and Authentication	Require users or service accounts to be uniquely identified and authenticated before accessing resources.	Aembit issues ephemeral credentials to workloads (i.e., "service accounts") after cryptographic verification. Each workload has a unique identity derived from AWS/Azure metadata or Kubernetes tokens, ensuring no shared/anonymous accounts.
3.5.2	Device Identification and Authentication	Authenticate devices before allowing connections.	Aembit verifies device/workload posture (e.g., AWS instance ID, container labels, EDR signals) prior to credential issuance. If the attributes don't match, the device is denied authentication and cannot access resources.
3.5.3	Multi-Factor Authentication	Implement MFA for access to privileged or sensitive accounts.	Although typically user-centric, Aembit can enforce multiple posture factors (e.g., verified cloud role + CrowdStrike posture) for workload identity, effectively providing "MFA" for privileged machine/service access.
3.5.4	Replay-Resistant Authentication	Prevent the replay of authentication information.	Aembit short-lived tokens are cryptographically bound to the current environment posture and expire within minutes. They cannot be reused outside their brief validity window, preventing replay attacks.
3.5.5	Identifier Management	Manage how system or service account identifiers are established, used, and retired.	Service accounts in Aembit are ephemeral and automatically created and retired when needed. No long-lived or static identifiers remain in the environment, minimizing the risk of credential sprawl.

3.13 System and Communications Protection

	Control	Summarized Requirement	How Aembit Supports This Control
3.13.15	Session Authenticity	Protect the authenticity of communications sessions.	Aembit's ephemeral tokens are cryptographically tied to the verified workload identity. If posture or identity changes (e.g., a workload becomes compromised), Aembit denies new tokens, thereby preserving session authenticity and integrity.