FUDO SECURITY

Real-Time Intelligence and Live Supervision:

Modernizing Privileged Session Governance with Fudo 6.2



Dear Readers,

We are pleased to present this whitepaper on our latest platform, Fudo 6.2, our answer to the challenges of tomorrow.

For more than 20 years, we have been delivering cybersecurity technologies, and today our solutions protect organizations in over 30 countries worldwide. Europe, however, remains our main focus and strategic direction.

We are living in a time of unprecedented change. A rapidly evolving geopolitical situation, global unrest, and new legal regulations have created a new reality. In this reality, digital sovereignty has become the foundation of national and business security. For us, digital sovereignty means concrete action: building economic patriotism and investing deliberately in European innovation.

In this document, we outline the architecture and capabilities of Fudo 6.2. Our platform is expanding rapidly, and more innovative products are on the way. Fudo Security's ambition is to become the first-choice PAM solution in the European Union.

The coming period is the best and most important moment for cybersecurity vendors in more than two decades, and we are ready for it.

Enjoy the read,

Paweł Dawidek
CEO, Fudo Security

1.0 Executive Summary

1.1 Modern Privileged Access Management Challenges

Corporate IT environments have evolved from static, perimeter-based networks to distributed, hybrid ecosystems. Organizations now rely on multi-cloud infrastructure, third-party contractors, remote teams, and automated processes. While this flexibility supports operations, it also creates new security and management challenges related to privileged access.

Standard Privileged Access Management platforms record session data effectively, but reviewing extensive session logs after incidents is mostly reactive. Security teams often lack real-time inspection capabilities, making session logs passive rather than proactive tools. Additionally, external vendors and contractors need elevated access, creating tension between compliance and agility. Implementing protective controls without burdensome approvals or complex workflows remains a challenge, especially with evolving regulations such as NIS2 and DORA.

1.2 Fudo 6.2 Architectural Overview

Fudo 6.2 addresses these challenges by emphasizing real-time monitoring, contextual policy enforcement, and ecosystem flexibility over passive session recording. As a proxy-based enterprise PAM solution, it integrates language models and custom inference engines into active connections. This enables real-time evaluation of terminal commands, contextual risk scoring, and automated policy enforcement based on severity.

In addition to artificial intelligence, this release introduces mandatory live supervision, requiring supervisor presence before critical sessions begin. It also adds granular network controls through Policy-Based Access Control, dynamic Just-In-Time access workflows, and optional Hardware Security Module integration for enhanced cryptographic protection. Unified credential vaulting is now available across mobile devices and more desktop browsers.

1.3 Business Value & Risk Mitigation Approach

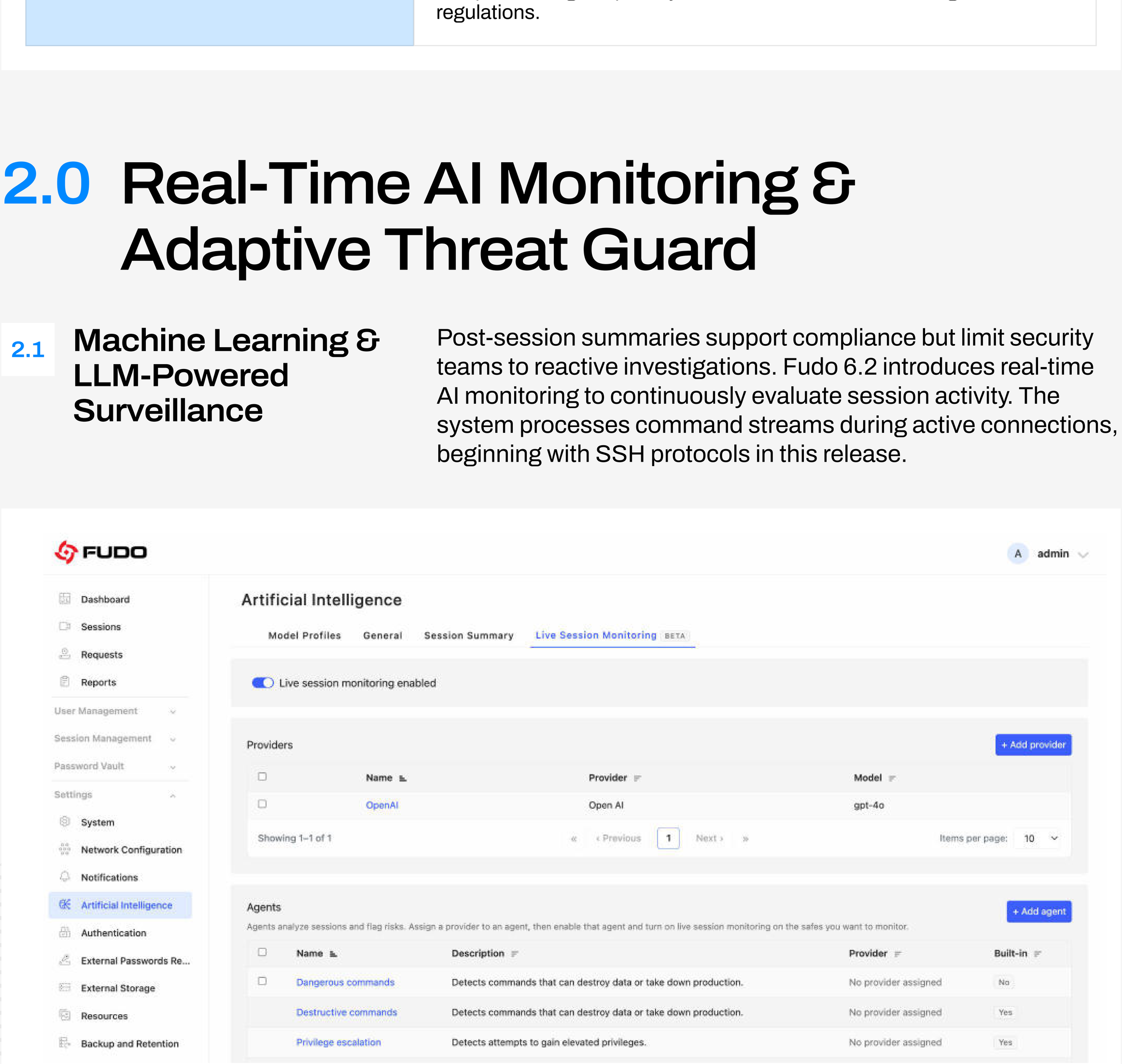
The platform helps organizations manage privileged access risk while keeping administrative overhead low. Instead of claiming to eliminate all operational risk, version 6.2 focuses on improving visibility and supporting compliance. Real-time AI analysis reduces detection time for anomalies, such as unauthorized file transfers, by identifying them during active sessions. User-friendly interfaces and integrated ticketing workflows also reduce the manual workload for administrators.

Operational Objective	System Capabilities & Mitigation Approach
Real-Time Oversight	Integrates AI analysis to reduce the log review burden and introduces live supervision for controlled vendor access. Automated pause or terminate policies help limit the exposure window during suspicious events.
Operational Efficiency	Provides unified interfaces across the User Access Gateway and browser extensions. Dynamic Just-In-Time workflows reduce the need for manual daily policy adjustments.
Governance & Compliance	Offers structured access justifications, multi-format syslog exports, and compliance-aligned privacy controls that accommodate regional labor regulations.

2.0 Real-Time AI Monitoring & Adaptive Threat Guard

2.1 Machine Learning & LLM-Powered Surveillance

Post-session summaries support compliance but limit security teams to reactive investigations. Fudo 6.2 introduces real-time AI monitoring to continuously evaluate session activity. The system processes command streams during active connections, beginning with SSH protocols in this release.



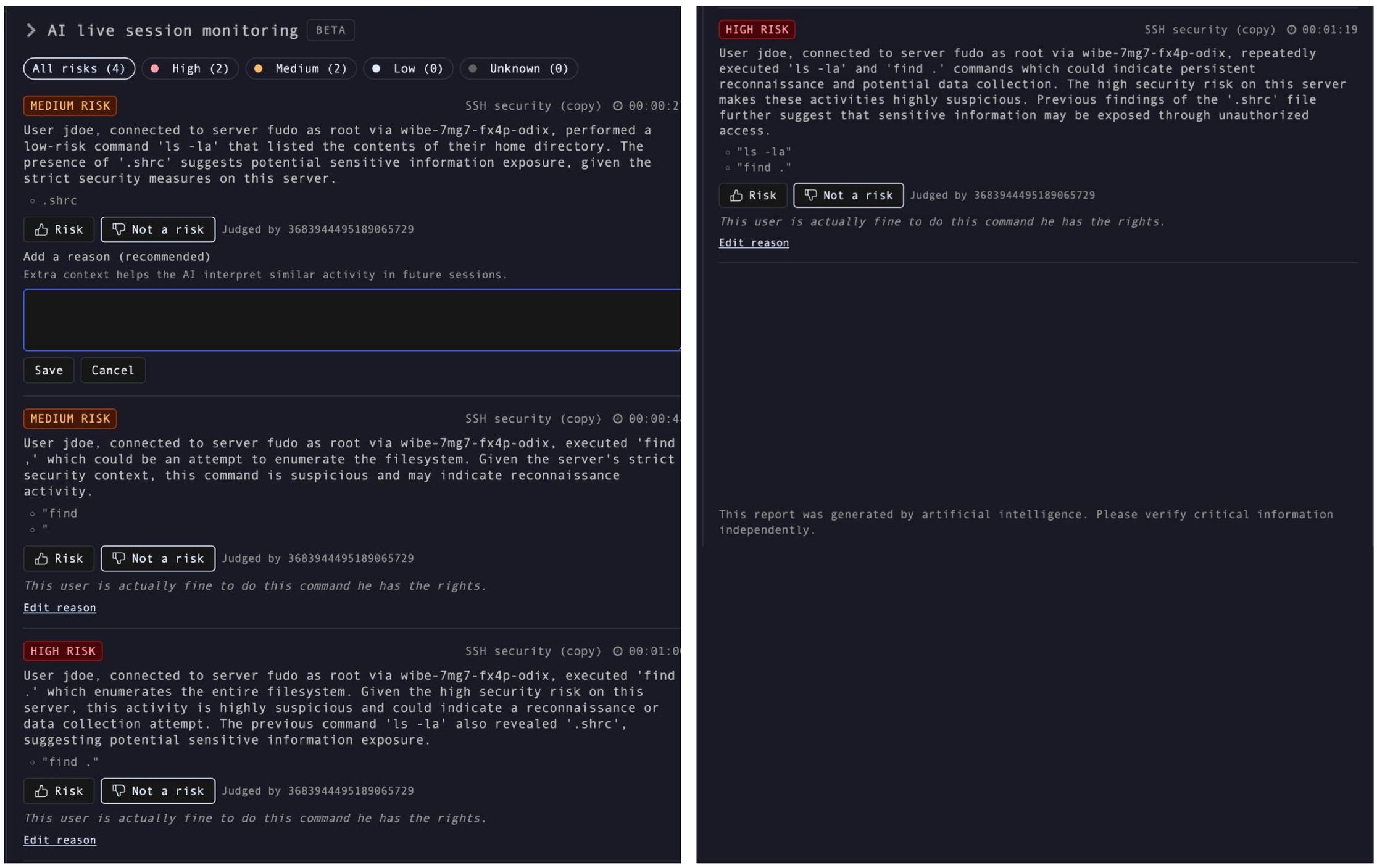
DASHBOARD OF THE ARTIFICIAL INTELLIGENCE FEATURES

The inference engine analyzes terminal commands within their structural context. It considers the user's operational role, the target asset's function, and organizational guardrails. By combining terminal inputs, screen outputs, and background information, the system distinguishes routine tasks from those requiring further review.

Component	Function in AI Evaluation
Context Aggregator	Supplies the model with background data regarding the user’s role, the target asset’s function, and organizational policies.
Inference Engine	Processes the terminal input and screen output against the provided context using local or cloud-based Large Language Models.
Policy Trigger	Generates real-time severity badging, collects human-in-the-loop judgments, and executes automated actions based on the evaluation.

2.2 Threat Detection & Data Exfiltration Prevention

During active sessions, the monitoring engine continuously compares terminal interactions to configured risk profiles. If command patterns suggest misuse, such as staging sensitive files for transfer, the system generates a risk finding within seconds, categorizes the event by severity, and provides a concise explanation in the dashboard. Monitoring effectiveness depends on stream visibility; commands within encrypted binaries or non-interactive tools that do not expose content may not be evaluated.



2.3 Automated Mitigation Policies & Contextual Judgments

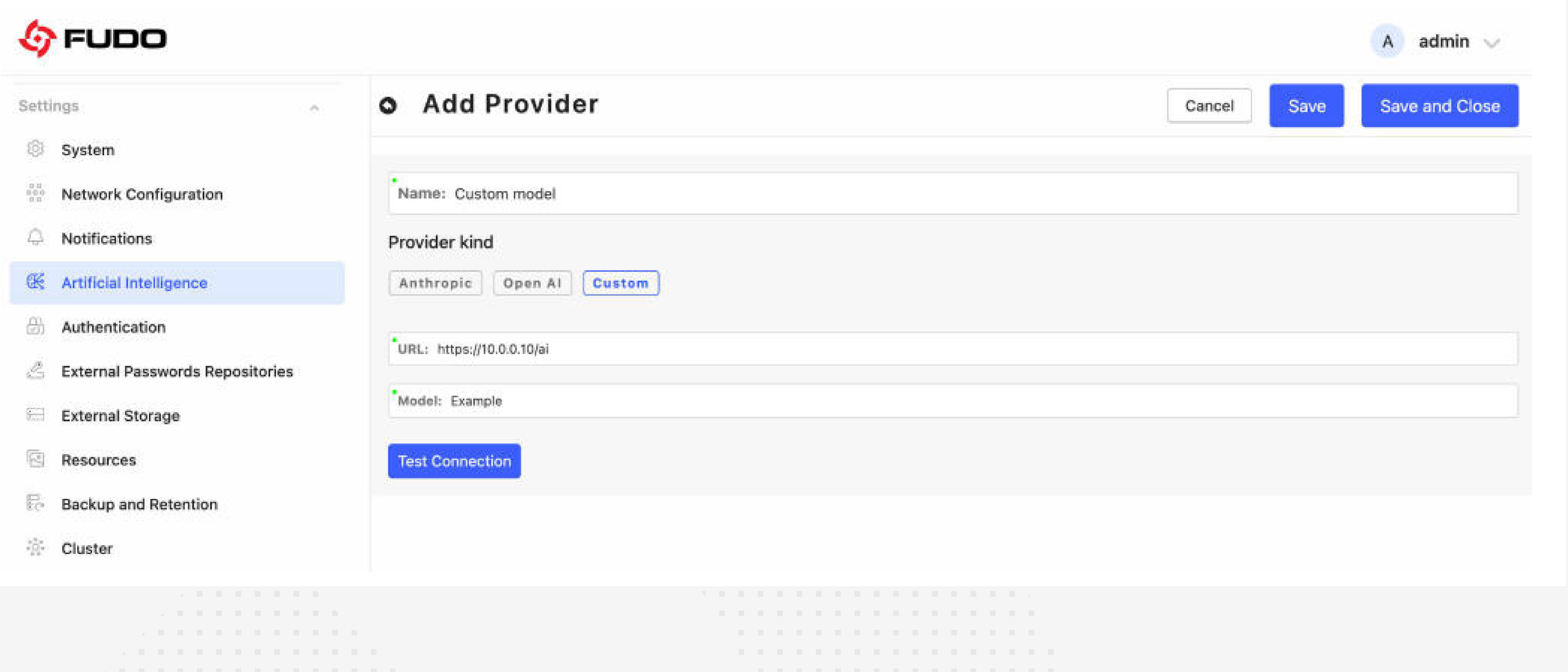
Security administrators can attach automated policy rules to targeted Safes to enable timely responses. Policies set thresholds, such as the number of findings needed to trigger actions, which may include notifications, pausing, or terminating connections. Administrators can start with conservative thresholds to monitor model performance before enabling active session interruptions.

To accommodate unique workflows and reduce false positives, the system uses a structured feedback mechanism. When an activity is flagged, administrators review the session playback in Fudo Player and provide a judgment, either confirming a risk or validating legitimate activity. These judgments are saved as historical context for future sessions with the same user and host, helping the model recognize authorized procedures.

Automation & Feedback Parameter	Operational Configuration
Severity Thresholds	Policies can be triggered based on Medium/High, or High risk categorizations identified by the agent.
Automated Actions	Depending on confidence levels, the system can notify administrators, pause graphical sessions, block users or terminate terminal connections.
Human Judgments	Player-exclusive review buttons allow administrators to provide feedback, which is saved as persistent context for future evaluations.

2.4 Enterprise AI Deployment Models

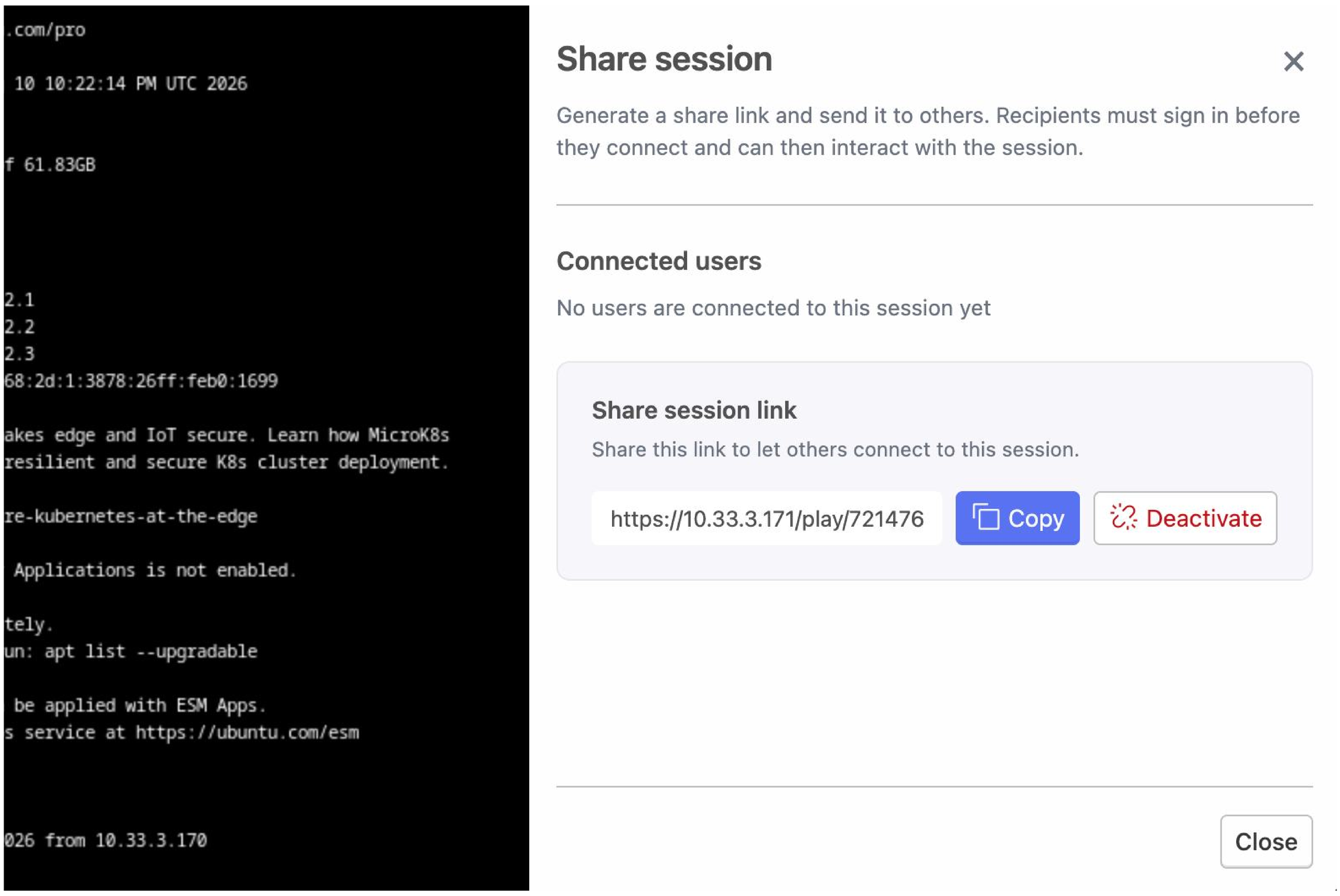
Enterprise organizations face diverse regulatory requirements, so AI deployment must be flexible. Fudo 6.2 supports multi-agent configurations, enabling concurrent specialized monitoring profiles. For example, one agent can monitor data exfiltration while another checks for service misconfigurations. The platform integrates with commercial cloud models and supports on-premises or private cloud inference. Local deployment ensures session transcripts remain within the organization's network, meeting data sovereignty requirements.



3.0 Dynamic Session Control & Mandatory Live Supervision

3.1 Next-Generation Session Sharing

Granting temporary access to active sessions requires balancing agility and security. Fudo 6.2 updates session sharing by integrating authentication into the User Access Gateway. Users can generate share links for their active sessions from the resource panel, enabling peer review or collaboration without administrative involvement. These links maintain a clear separation between Management and Gateway access, ensuring viewers are properly authenticated before accessing the stream.

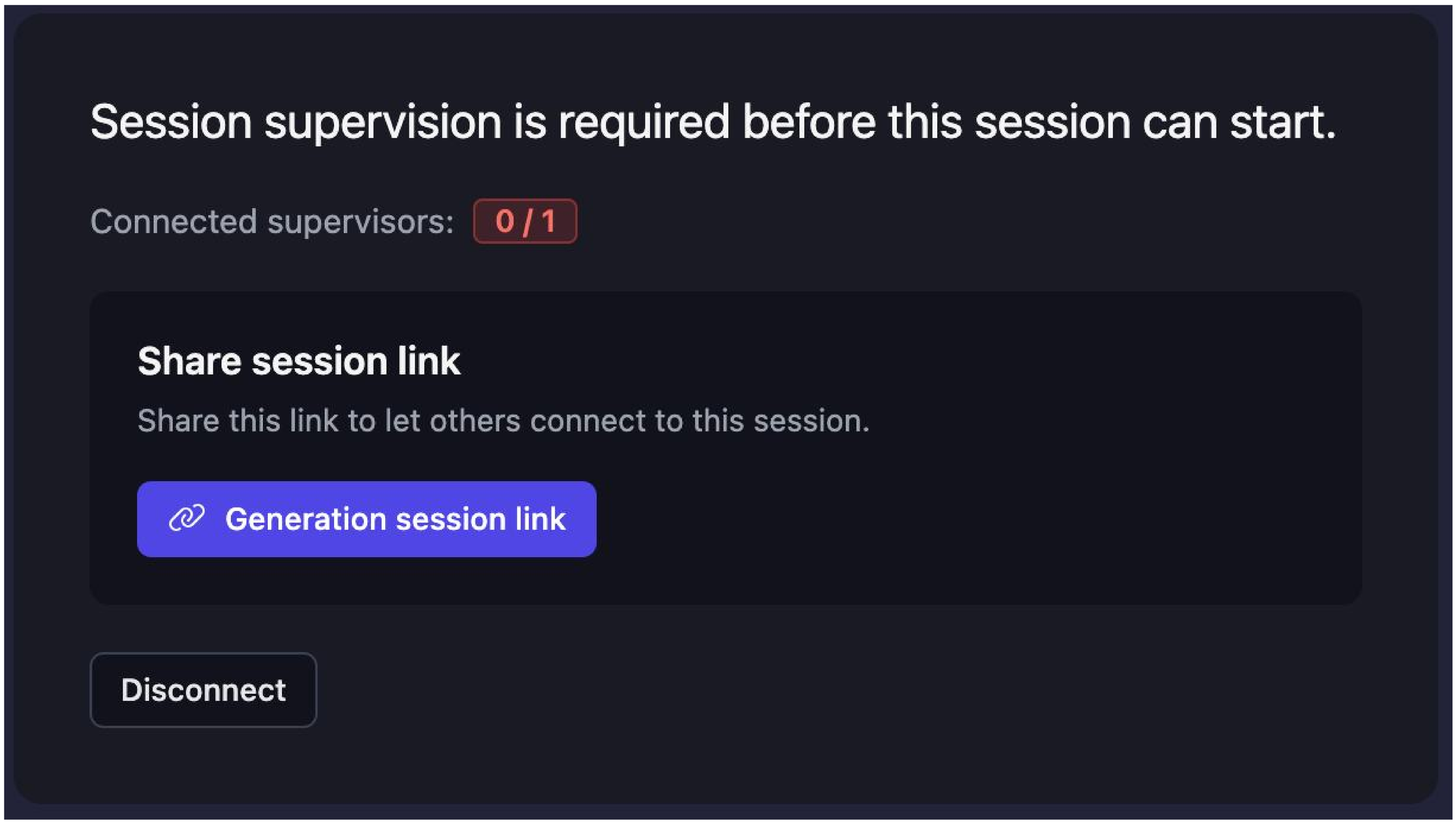


Share Link Type	Access Characteristics
Time Window Share	Access is bounded by scheduled start and end limits. Available via the Management interface with options for anonymous or authenticated viewing.
Live Session Share	Access lifetime is tied directly to the active session duration and expires upon closure. Generated via the Gateway and always requires authentication.

3.2 Live Supervision Architecture

Live Supervision builds on session sharing by enforcing conditional access. A privileged session cannot connect to the target resource until the required number of authorized supervisors join the monitoring stream. When a user starts a covered session, they receive a prompt and must share a generated link with designated supervisors. Once supervisors authenticate and enter the player view, the connection is released and operations can begin.

Because this feature relies on real-time visual or terminal stream rendering, it supports interactive protocols including RDP, SSH, VNC, and rendered HTTPS. It does not apply to discrete database query protocols.



3.3 Mid-Session Dynamics & Audit Oversight

If a supervisor disconnects during an active task, the system responds based on the protocol. After a brief grace period, the system intervenes to prevent unsupervised activity. For graphical protocols such as RDP and VNC, the system pauses the session and preserves the application state for up to 300 seconds (or less if the Safe's inactivity limit triggers sooner) while waiting for the supervisor to return. For terminal protocols like SSH, the system terminates the session to prevent unmonitored commands.

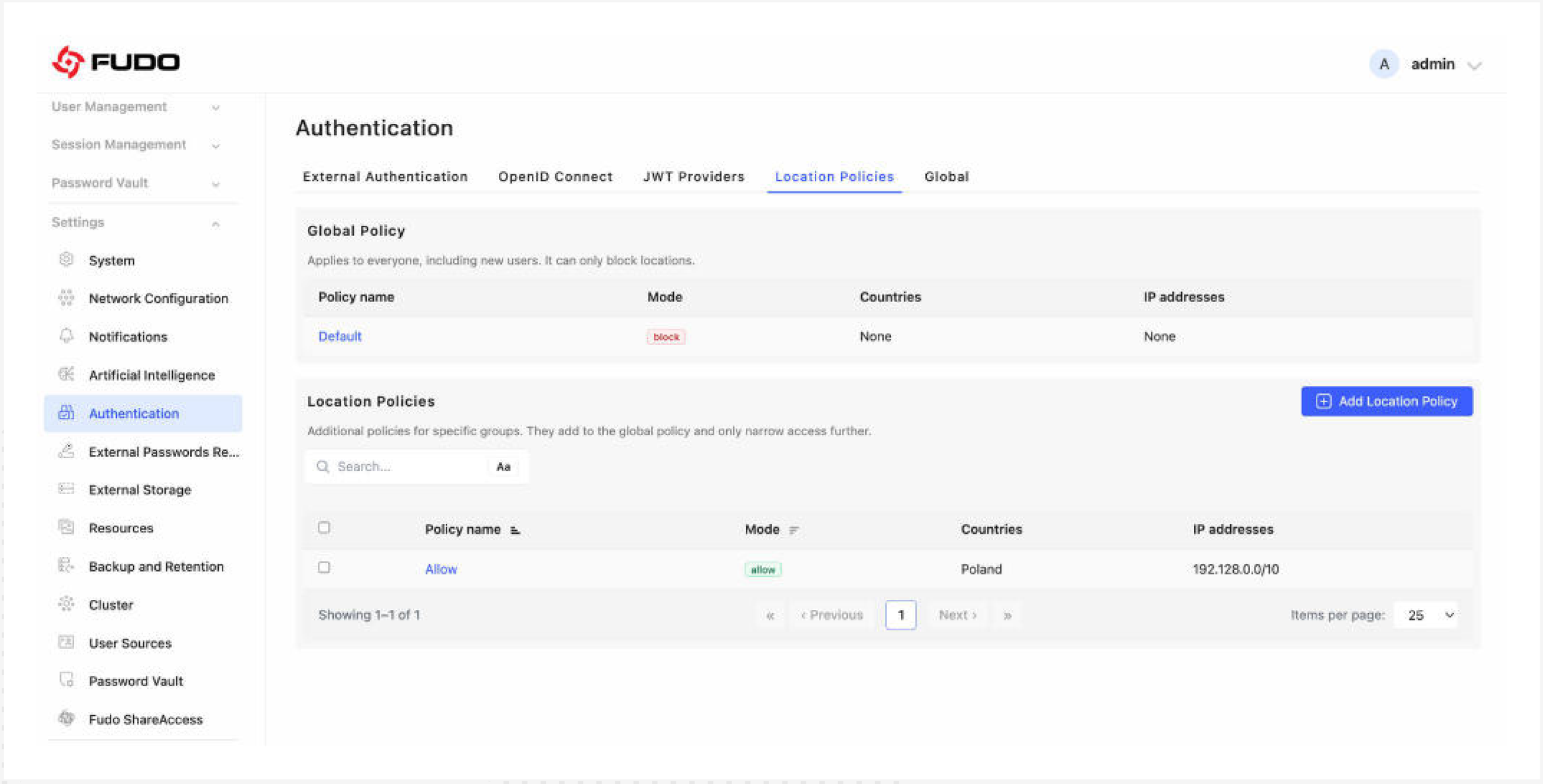
To ensure accountability, the platform records detailed access history for each share link. Administrators can review the link lifecycle, verify viewer identities and source IPs, and track timestamps for connection events and control handovers.

Disconnect Action	Protocols	Operational Behavior
Pause	**EDP, VNC**	Displays a pause overlay; preserves the backend connection and application state for up to 300 seconds (or until the Safe's inactivity limit is reached) until the supervisor rejoins.
Terminate	**SSH, Telnet, HTTPS (rendered)**	Closes the underlying session connection after a short grace period (~10 seconds) to prevent unsupervised activity.

4.0 Zero-Trust Access Policies & Granular Security Controls

4.1 Policy-Based Access Control & Geofencing

Relying only on static credentials is risky in distributed environments. Fudo 6.2 addresses this with Policy-Based Access Control in the authentication layer. Administrators can restrict access by network location, IP subnet, or geographic region. The system evaluates client IPs against location policies to block unauthorized attempts early, though while standard connection attempts are evaluated before credential verification, API calls are verified after authentication.



Access Control Component	Implementation Detail
Global Location Policy	Applies baseline network access rules across the entire system instance for all users.
Custom Policies	Assigned to specific user groups, evaluating incoming IPs against defined subnets or GeoIP regions to determine explicit Allow or Block actions.
Anti-Lockout Protection	Prevents active administrators from accidentally blocking their own current network subnet.

4.2 Time-Based Just-In-Time Access Integration

Balancing security and operational availability requires flexible scheduling. Fudo 6.2 combines daily access schedules with dynamic Just-In-Time request workflows. During scheduled hours, connections initialize as usual. Outside these windows, gateway controls are disabled, but users can request access directly from the interface. Once approved, temporary access is granted for a set period, removing the need to manually adjust permanent schedules.

4.3 Policy UI & Structured JIT Formatting

The schedule management interface now features an interactive visual scheduler instead of text-heavy inputs. Administrators can set access windows on a weekly grid using drag-and-drop actions, adjust time boundaries, and replicate schedules across days.

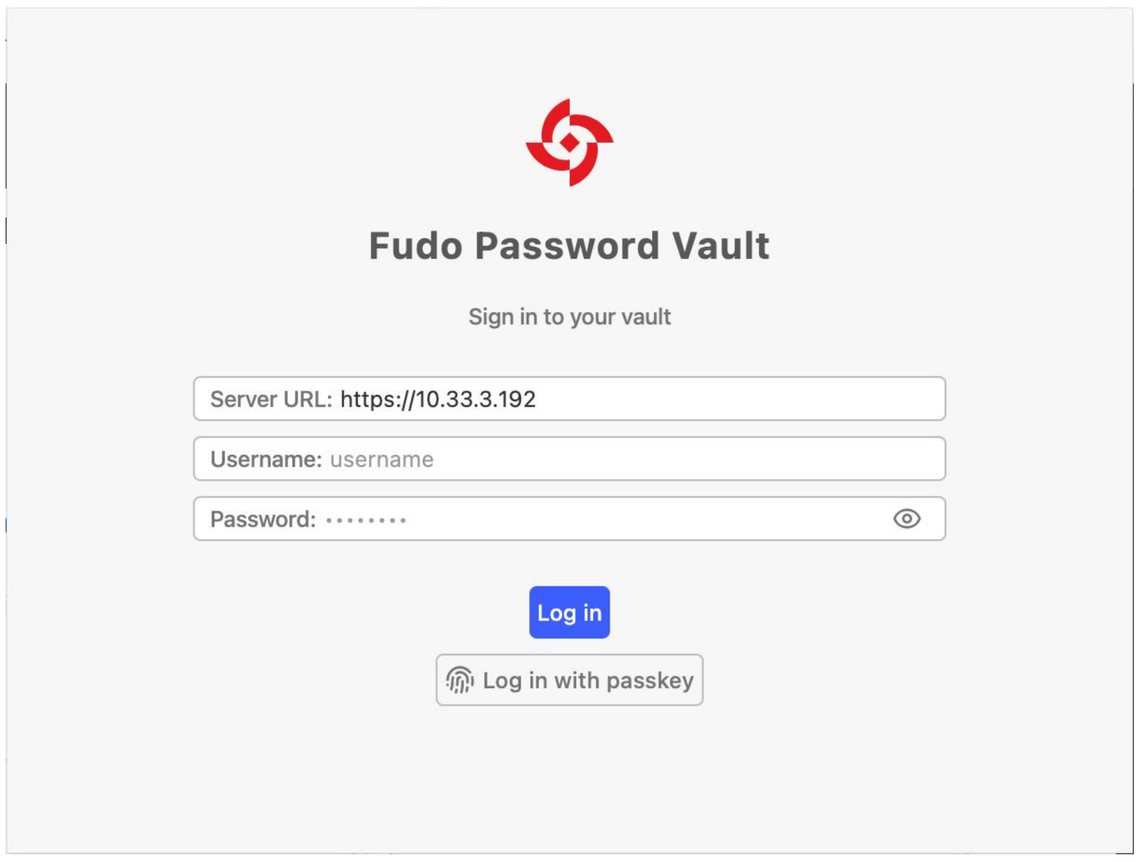
Unstructured text fields in Just-In-Time requests can complicate compliance tracking. The updated platform allows administrators to configure global structured reason formats, enabling users to choose the appropriate template from a dropdown menu in the User Access Gateway. Formats are defined using three distinct field types: standard text fields, numeric inputs, and constant fields prefilled by the administrator that cannot be altered by the user. Fudo validates user entries locally against these field requirements prior to submission, which helps organizations maintain data consistency when manually correlating access requests with external IT Service Management systems such as Jira or ServiceNow.

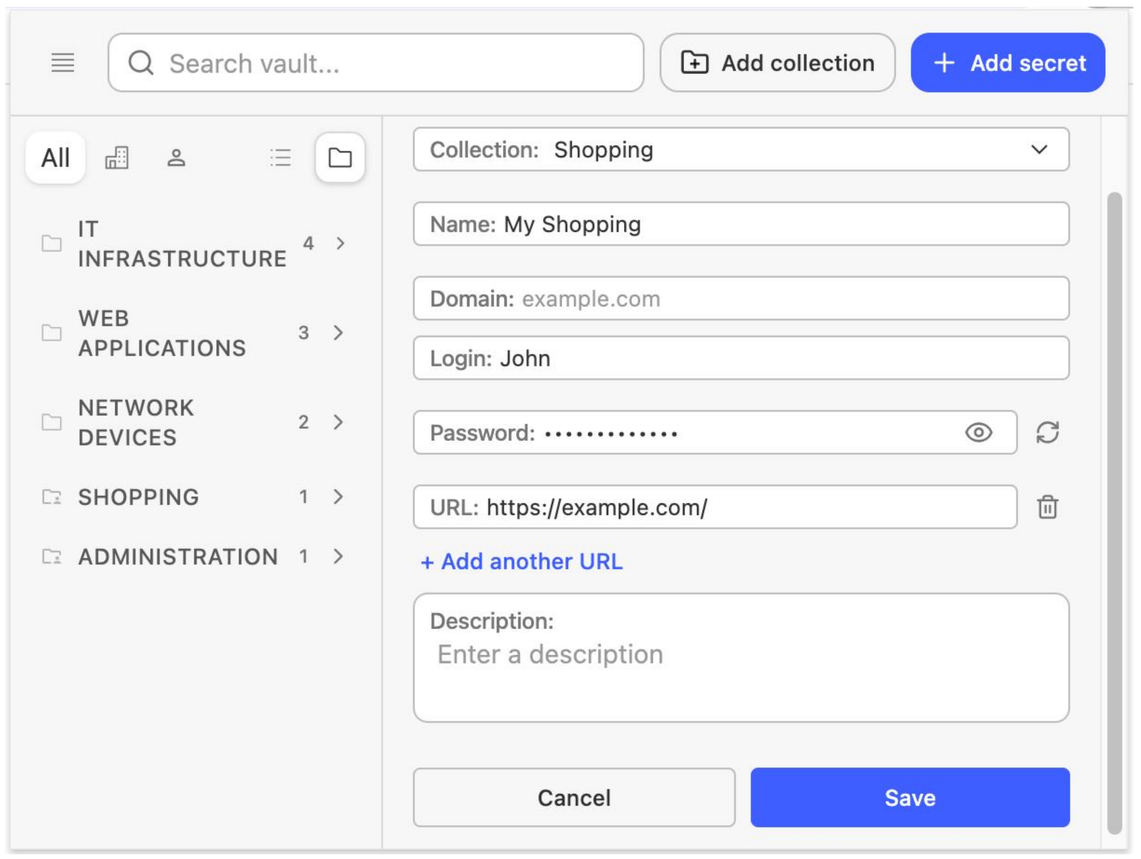
5.0 Enterprise Credential Vaulting & Mobile Access Ecosystem

5.1 Cross-Browser Password Vault Extension

Credential management can be cumbersome when users manually transfer complex passwords between repositories and web interfaces. The updated Fudo Password Vault browser extension brings management capabilities directly to the user's environment. It supports Chrome, Firefox, Safari, and now

Microsoft Edge. Multi-factor authentication aligns with the primary gateway, allowing authentication via SMS, push notifications, or biometric Passkeys. Once authenticated, users receive contextual autofill tooltips and can create personal collections from the browser panel.





Extension Feature	Operational Detail
Browser Support	Compatible with Chrome, Firefox, Safari, and Microsoft Edge.
Authentication Parity	Supports SMS OTP, Duo Push, and WebAuthn/Passkey biometric standards.
Inline Usability	Provides contextual autofill tooltips on input focus and allows quick secret addition.

5.2 Mobile Access Ecosystem & Vault Partitioning

To support remote administration, the Fudo Officer mobile app now includes dedicated vault management. A shared data partition connects the web portal, browser extension, and mobile app, ensuring secrets created in one interface sync across the user's environment. Mobile vault access is now available to standard business users, allowing them to manage authorized enterprise secrets on the go.

5.3 Secret Lifecycle & Hierarchical Collections

Secret management needs vary between individual credentials and organizational assets. Personal vaults offer flexibility, including nested sub-collections for grouping keys by project or environment. Organizational vaults follow centralized access policies and administrative Safes. Both types support various secret formats, including logins, SSH keys, certificates, API keys, and notes. Users can request temporary access to restricted organizational secrets from the mobile app, creating an auditable trail for off-schedule use.

Vault Category	Scope & Structural Characteristics
Personal Vaults	User-managed credentials supporting multi-level hierarchical sub-collections.
Organizational Vaults	Centrally managed corporate assets structured by administrative Safes and policies.
Supported Formats	Accommodates logins, SSH keys, certificates, API keys, and notes.

6.0 Platform Architecture & Enterprise Security Enhancements

6.1 Hardware Security Module (HSM) Integration

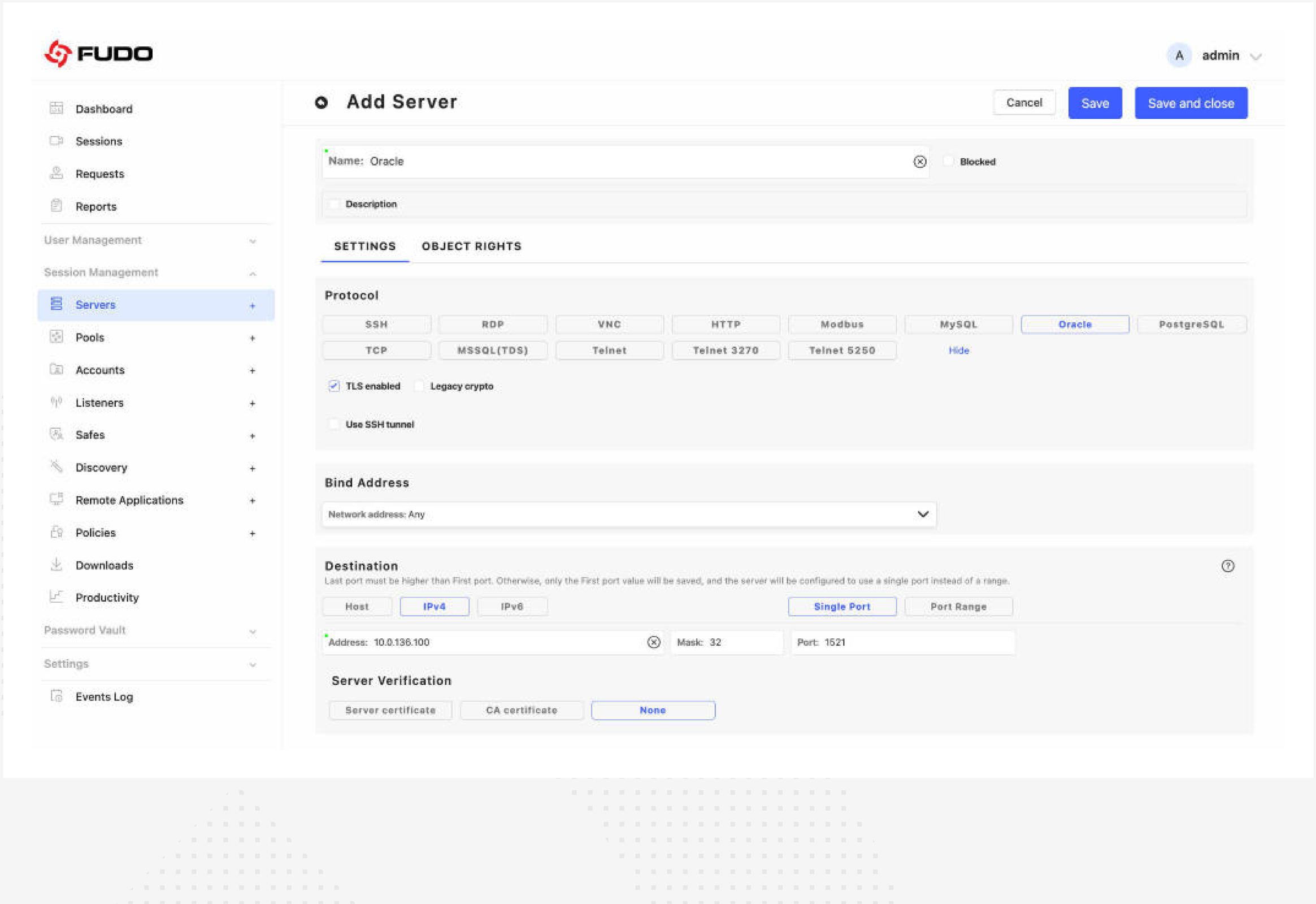
System-level encryption relies on master cryptographic keys to protect sensitive data such as credentials and session dumps. Fudo 6.2 offers optional integration with external Hardware Security Modules using PKCS#11, enabling security teams to offload Master Key protection to dedicated hardware. During initialization, the platform connects to the HSM server using vendor-specific binaries and certificates to authorize Master Key access. The HSM must be reachable during system cold boot to mount encrypted storage, adding an extra layer of protection against unauthorized local access.

HSM Integration Stage	Operational Detail
1. Configuration	Administrator uploads an HSM bundle containing client binaries and TLS certificates.
2. Authentication	Operator provides the required token Label and PIN to establish the cryptographic handshake.
3. Boot Unwrapping	Fudo requests authorization from the HSM server to unwrap the Master Key during system startup.

6.2 Native Oracle Database Protocol Support (BETA)

Database protocol proxying requires specialized parsing to inspect raw traffic, separate operational commands from sensitive results, and capture structured audit logs. Fudo 6.2 adds native proxying for the Oracle Database protocol as a Beta feature. This Beta release allows organizations to test proxying in their environments and provide feedback to improve the parsing engine.

Protocol-level proxying removes the need for host-based logging agents. This approach typically captures raw database interactions without changing the Oracle Database server configuration. However, the proxy does not support Oracle's Advanced Security Option (ASO) encryption; if ASO is enforced, server or client settings must be adjusted. For TLS-encrypted environments, the proxy currently supports only SQL*Plus client connections.



Oracle Proxy Capability	Technical Implementation Details
Account Architecture Support	Currently implemented for Forward Account configurations.
Supported Database Versions	Validated against Oracle Database 19c, 21c, and 23ai.
Session Inspection	Captures inbound SQL queries and outbound database responses.
Audit Trail Rendering	Logs SQL execution history within the Fudo Session Player for structured review.

While the Oracle proxy module is in Beta, administrators should note several constraints. Currently, only Oracle SQL*Plus is officially supported for connections. The system does not support “noraw” session recording mode, so it records the full raw session stream. Interactive sharing of live sessions is not yet available for this protocol.

6.3 Next-Generation RDP Engine

Remote Desktop Protocol sessions often include complex graphics and video, which can challenge older proxy systems. Fudo 6.2 introduces a high-performance RDP proxy engine to improve rendering efficiency and responsiveness. The new architecture supports Full HD video streaming with less frame degradation and optimized buffer management for lower latency. During the transition, the new engine runs alongside the legacy RDP stack, allowing administrators to test client connections before full adoption, with the caveat that the new engine is not implemented for Standard RDP Security (Non-TLS).

RDP Engine Characteristic	Operational Benefit
Video & Frame Processing	Supports smooth Full HD playback and complex graphical interfaces typical in OT environments.
Latency Management	Optimizes buffering to reduce input lag during highly interactive sessions.
Deployment Strategy	Coexists with the legacy engine to facilitate phased testing and gradual migration.

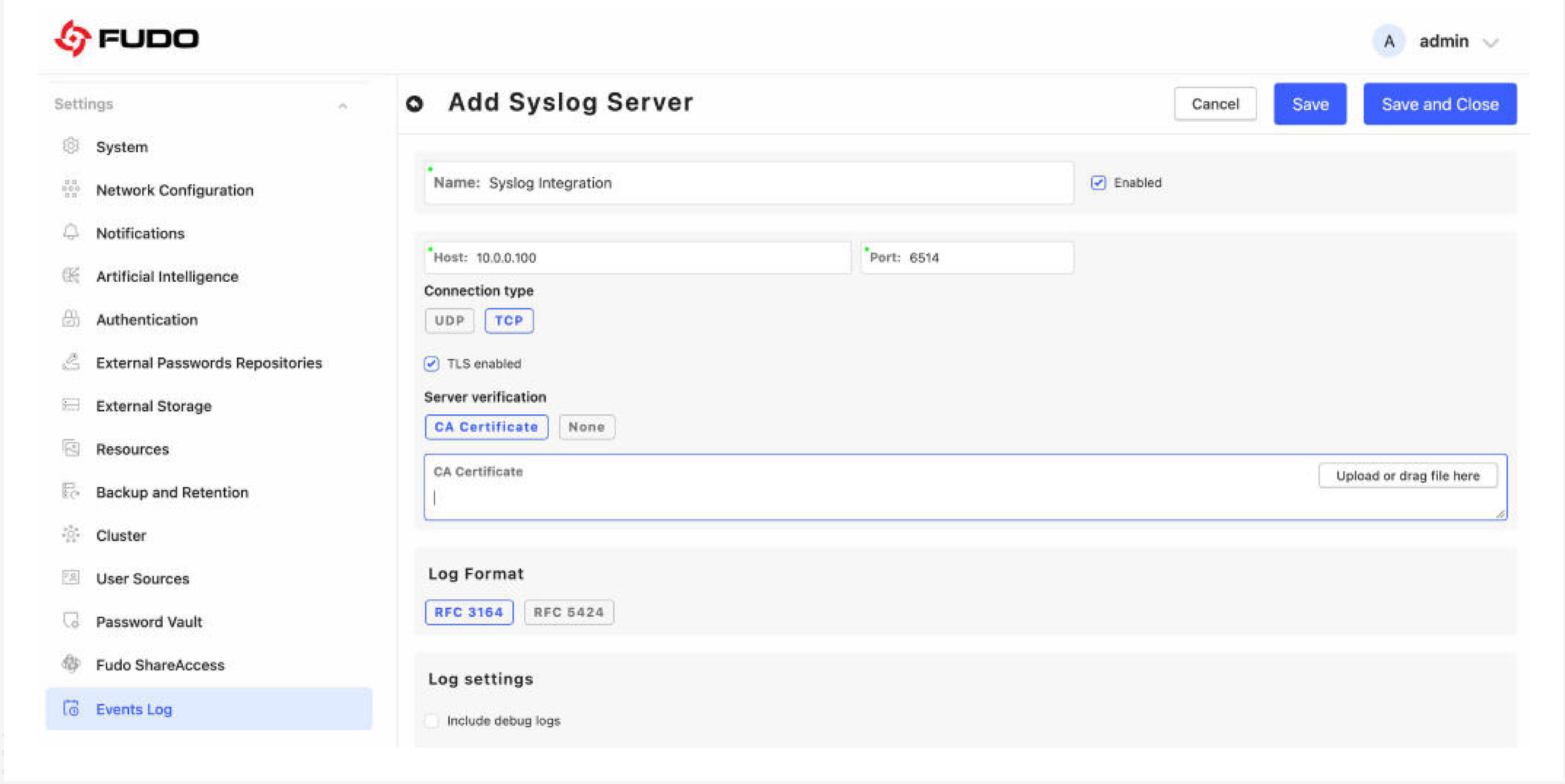
7.0 Identity Integrations, Governance & Compliance

7.1 Advanced Identity & Token Authentication

Enterprise identity infrastructure often combines legacy directory services with modern cloud Identity Providers. The updated framework supports native JSON Web Token validation for programmatic and API-driven authentication. It also introduces custom OpenID Connect scopes, allowing administrators to route user identities to different database backends based on operational scope. For network appliances, a simple toggle enables automatic domain suffix addition to outbound RADIUS authentication packets.

7.2 Enterprise Event Logging

Security Information and Event Management platforms require consistent, well-structured log ingestion for real-time threat visibility. The updated Syslog exporter supports both legacy BSD-style headers and modern structured formats with high-precision ISO timestamps and detailed metadata. This flexibility ensures compatibility with older collectors and reduces parsing overhead for modern SIEM solutions.



Integration Area	Enhancement Details
Identity & Access	Adds JWT support, OIDC custom scopes for environment routing, and RADIUS domain appending.
Event Logging	Supports dual-RFC Syslog formats to accommodate both legacy collectors and modern structured SIEM platforms.

7.3 Privacy Controls & Compliance Governance

Privileged access monitoring is essential but may conflict with local labor or privacy laws restricting productivity tracking. To address this, the platform allows organizations to disable productivity-tracking features at the licensing level. Enabling this privacy flag removes dashboards, time graphs, and efficiency metrics, while maintaining essential security logging for incident investigations and compliance with local agreements.

7.4 Administrative Restrictions & Usability

This release introduces refinements to enhance administrative control and usability. Security teams can restrict users from adding or deleting specific multi-factor authentication methods, while modification remains always available. The interface hides workspace tabs for unlicensed modules. Administrators can also adjust the OCR engine's confidence threshold and use native key-mapping support for French keyboard layouts during session recording.

Usability Refinement	Operational Function
UAG Restrictions	Allows administrators to lock down self-service MFA modifications and dynamically hide unlicensed modules.
OCR Adjustments	Provides a configurable confidence threshold to optimize text recognition accuracy for varying screen resolutions.

8.0 Implementation Strategy & Architecture Best Practices

8.1 Deployment Architecture & High Availability Planning

Integrating the updated platform requires assessing network topology and performance dependencies. High Availability clusters should ensure proxy availability and session recording continuity during maintenance. With Hardware Security Module integration, each node needs reliable, low-latency connectivity to the HSM, and boot sequences must ensure the HSM is reachable before proxy nodes start.

Deploying real-time AI monitoring also requires evaluating inference latency. Organizations using cloud-hosted APIs must allow outbound connections through corporate firewalls. For air-gapped deployments with local inference servers, hardware should be located within the same data center segment to minimize network latency.

Architecture Component	Deployment Consideration
High Availability	Requires synchronized boot sequences and consistent network paths across all active cluster nodes.
HSM Dependency	External key management appliances must be fully initialized and reachable prior to proxy node startup.
AI Inference	Demands stable bandwidth for cloud models or localized GPU hardware for low-latency on-premises evaluation.

8.2 Migration & Recommended Upgrade Pathways

Upgrading an existing environment should follow a phased approach to ensure system stability and policy alignment. After standard pre-upgrade backups, administrators should apply the release image to a secondary cluster node to verify service status before a full rollout.

After upgrading, introduce new features incrementally. Transition Target Safes to the new RDP engine selectively to test rendering stability across operating systems. Deploy real-time AI agents in notification-only mode at first, allowing security teams to review findings and refine prompts before enabling automated session terminations. Staggering these rollouts enhances privileged access visibility while maintaining operational stability.