



FUDO SECURITY

The Modern Management of Privileged Access



Table of Content

01 Introduction: New Challenges, Simpler Solutions

1.1 Digital transformation and the convergence of environments

02 Identity Under Control

2.1 Streamlined Work with Multiple Domains (Kerberos)

2.2 Improved Synchronization with Identity Providers (Entra ID and Okta)

03 Active Threat Protection

3.1 Detection of Compromised Credentials

3.2 Sudo: Privilege Management in Linux Environments

3.3 Modern Authentication Methods and Password Handling

04 Daily Convenience for Users and IT Teams

4.1 RDP: File Transfer in the Web Client

4.2 Streamlining Operations for Administrative Teams

05 ShareAccess: Cloud-Based Resource Access

06 Summary



Introduction: New Challenges, Simpler Solutions

Organizations must continually adapt their IT architecture to support flexible work models. As hybrid work, cloud migration, and third-party collaboration become standard, the traditional network perimeter is less defined. Relying only on conventional solutions like VPNs or basic firewalls can lead to operational challenges and oversight gaps.

Maintaining adequate security is an ongoing process that requires understanding company needs, assessing technological maturity, and aligning tools with business processes. Overly restrictive controls that ignore operational realities often drive users to seek workarounds, reducing the organization's resilience to threats.

Fudo Enterprise 6.1 supports organizations as they adapt to evolving IT environments. It balances Privileged Access Management (PAM) requirements with the daily needs of IT teams and external partners. With flexible identity management, modern authentication, and improved session oversight, Fudo 6.1 is a key tool for reducing risk across the digital ecosystem.



Identity Under Control

Effective identity and permission management across distributed environments requires consistency and minimizing manual, error-prone tasks. Flexible integration mechanisms enable more efficient mapping of organizational structures within the access system.

2.1

Streamlined Work with Multiple Domains (Kerberos)

Large organizations often require support for multiple independent Active Directory domains, each with its own DNS infrastructure. Fudo Enterprise 6.1 adds Kerberos protocol support for multi-domain environments and expands configuration flexibility for network scanners, password change modules, and remote sessions.

Granular Access Control

Administrators can precisely define where Kerberos authentication should apply. Configuration modifications allow this protocol to be independently enabled or disabled for external logins, LDAP directory synchronization, and connections within RDP sessions. This increases deployment flexibility in environments with diverse network rules.

Reducing Automatic Fallbacks to Legacy Protocols

The system allows administrators to disable automatic fallback to less secure authentication methods, such as NTLM or simple LDAP bind. This ensures security policies are not bypassed due to unexpected infrastructure responses.

Multi-Domain Environment Support

A dedicated local DNS handling mechanism allows assigning unique name servers to each domain. This ensures stable operation in complex environments without major changes to the client's network configuration

Automated Network Review (Discovery)

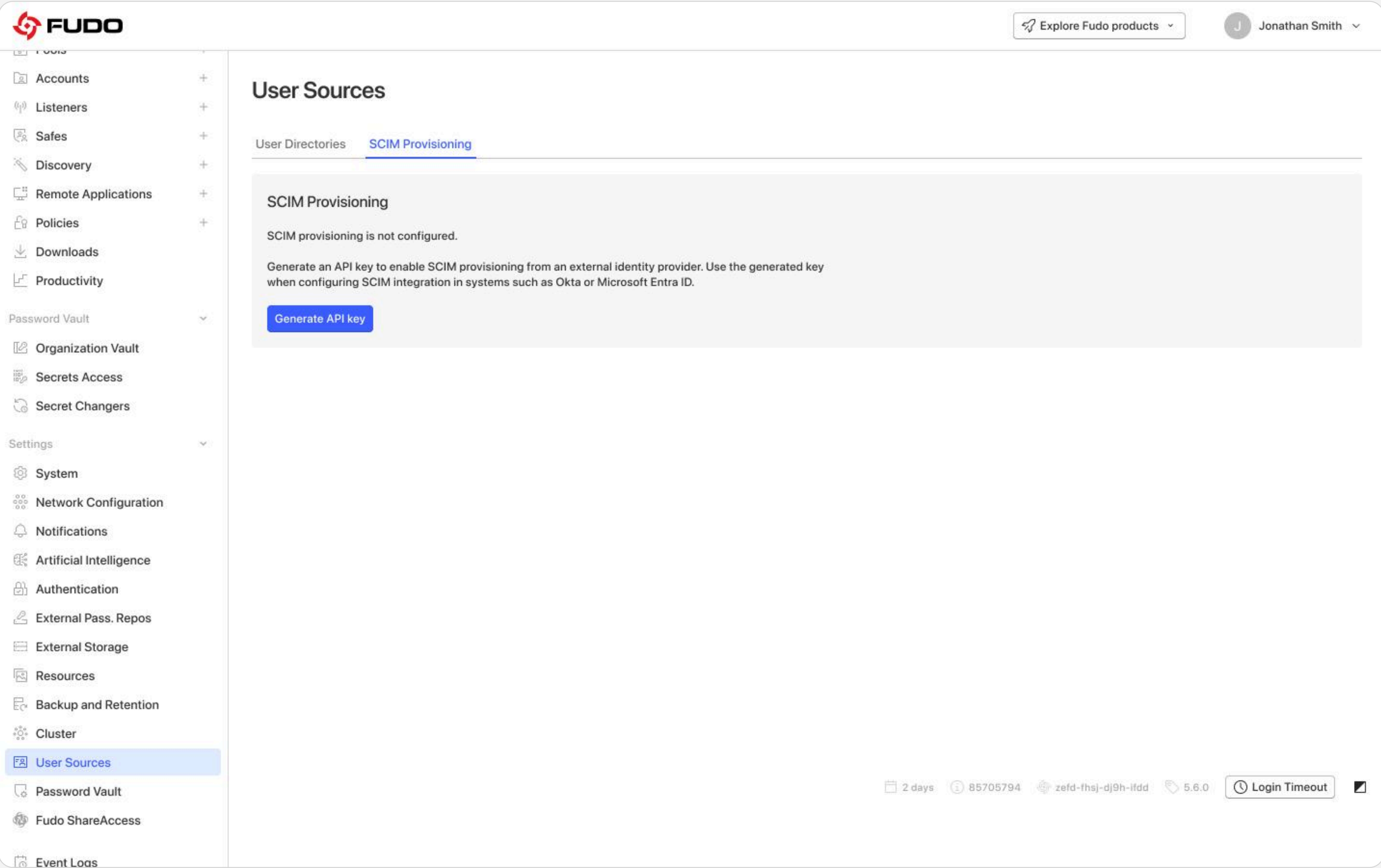
The Discovery module, which maps resources using WinRM and LDAP, now supports Kerberos authentication in version 6.1. Configuring this method for individual scanners enables safer and more predictable identification of new devices and accounts in complex domains.

2.2 Improved Synchronization with Identity Providers (Entra ID and Okta)

Shifting identity management to external cloud providers requires efficient communication of employee permission changes.

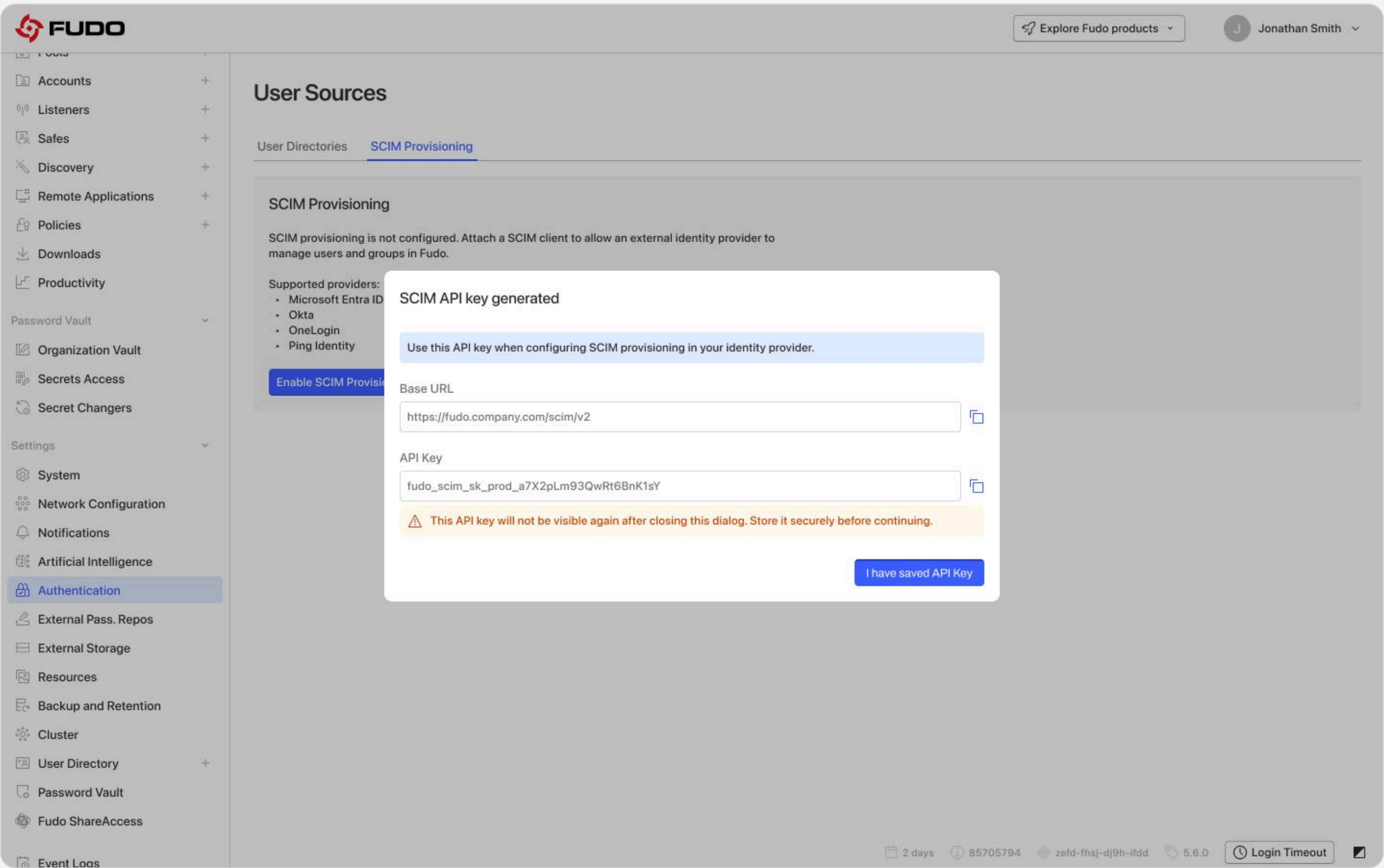
SCIM 2.0 Standard

Implementing support for the SCIM protocol enables receiving identity change messages directly from providers such as Microsoft Entra ID or Okta. The system efficiently responds to events sent by the identity provider, reducing the need for cyclical database querying.

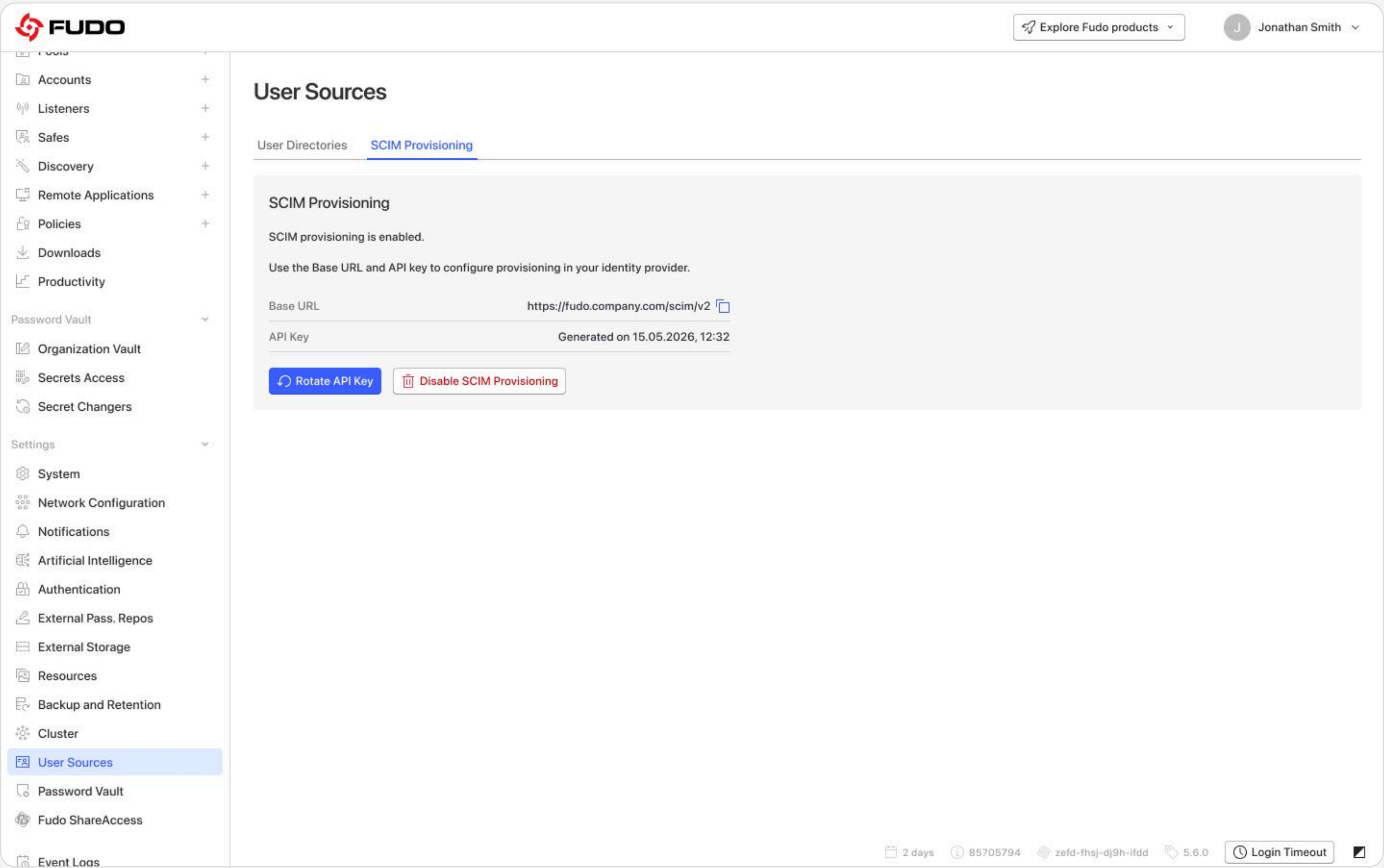


The new SCIM Provisioning tab in the Fudo management console. Generating an API key enables seamless integration with external identity providers, such as Microsoft Entra ID or Okta, to automate user provisioning.

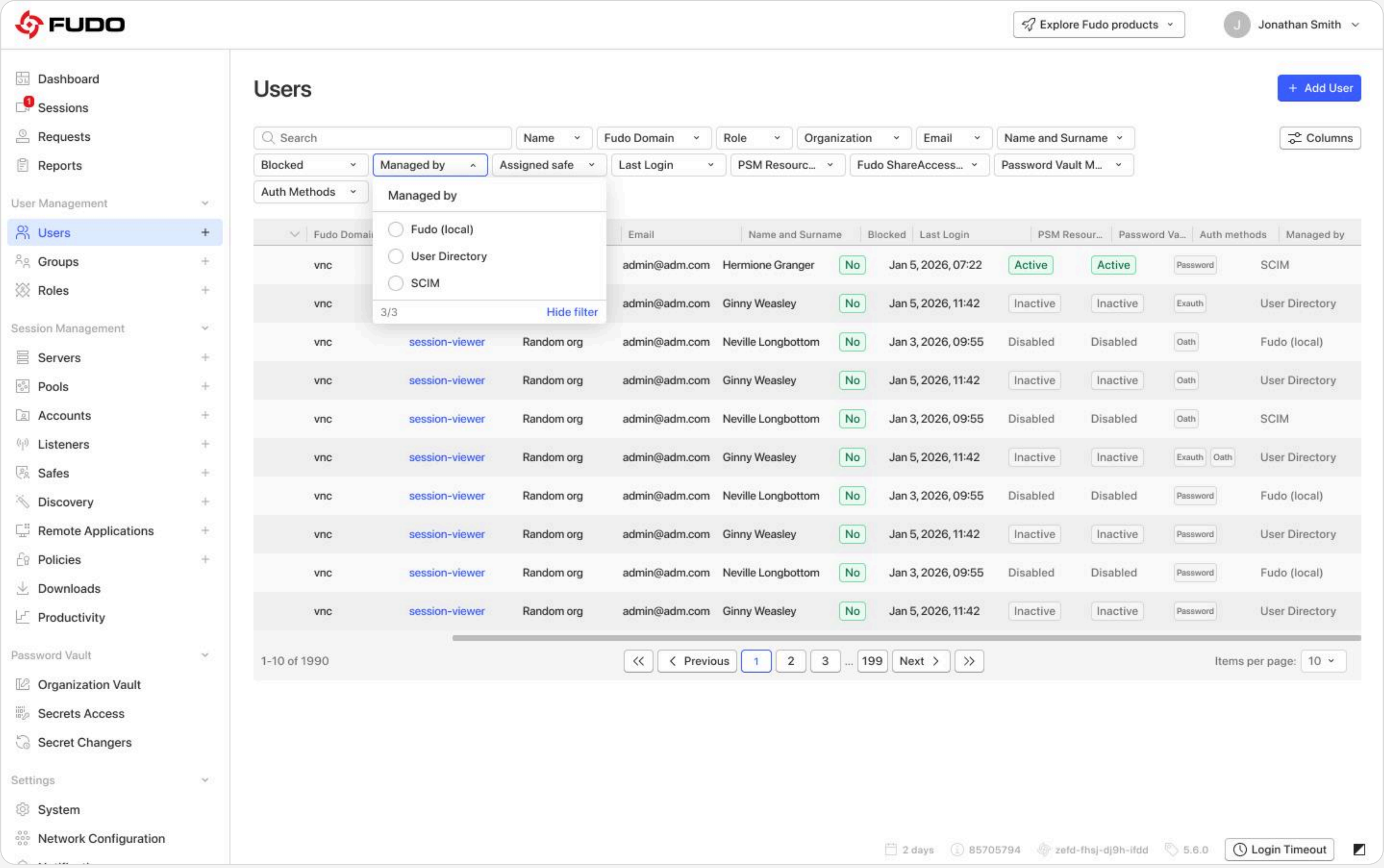
THE MODERN MANAGEMENT OF PRIVILEGED ACCESS



View of the generated SCIM API key and Base URL in the Fudo panel.

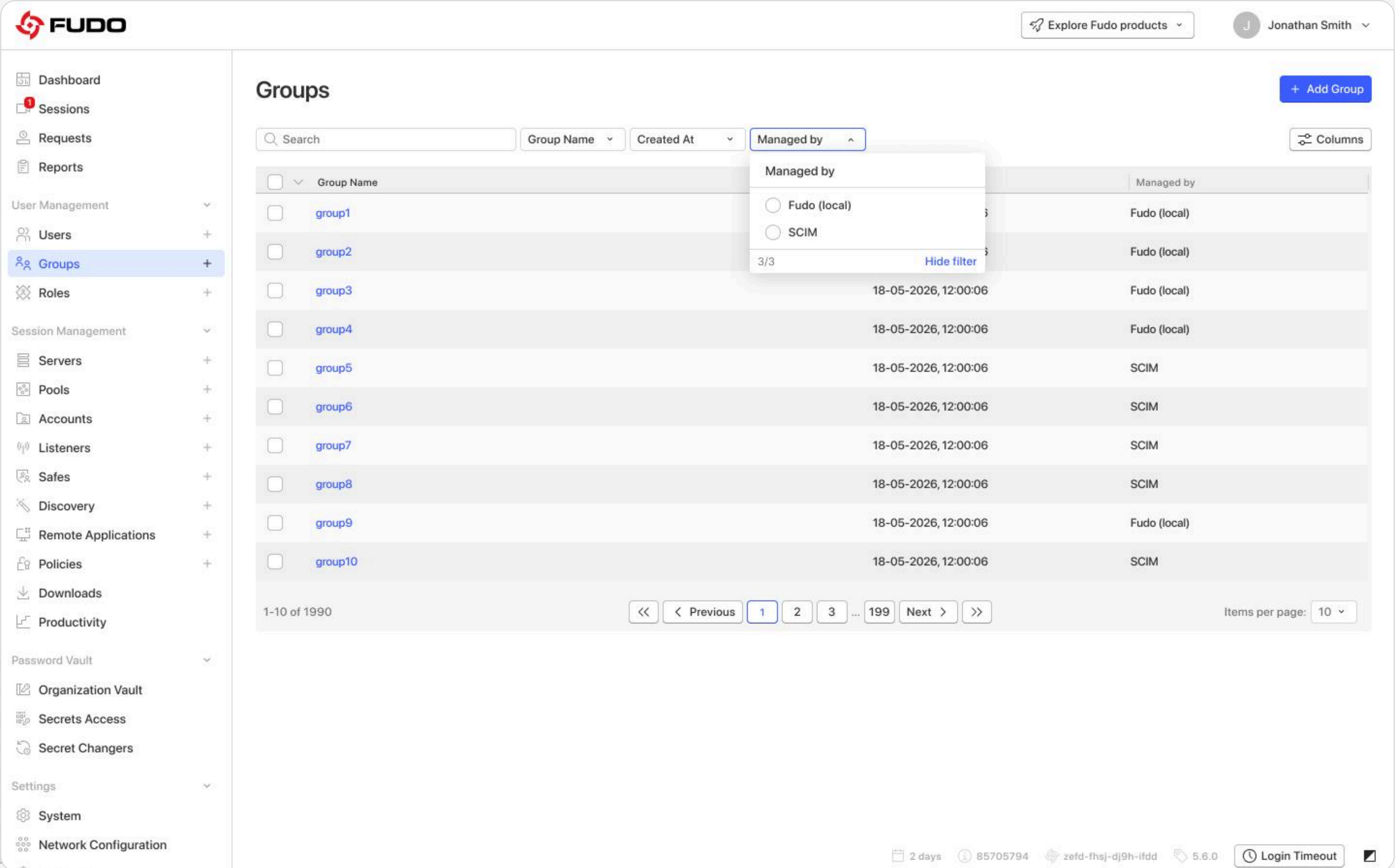


The active SCIM Provisioning screen in Fudo Enterprise 6.1, allowing administrators to view endpoint details and manage authentication keys.



User management screen with a dropdown filter for identity sources (Managed by). Enables quick identification and segmentation of local, domain, and real-time SCIM-synced users.

THE MODERN MANAGEMENT OF PRIVILEGED ACCESS



Group directory screen with a dropdown filter for identity sources (Managed by) in Fudo Enterprise 6.1 Facilitates quick identification and oversight of local groups versus SCIM-synced groups.

Identity Lifecycle Support

Employment changes, promotions, or transfers recorded in the primary system are reflected in Fudo without delay. When an employee leaves, integration rules disable accounts and revoke access promptly.

Data Integrity Protection

Objects synchronized via SCIM are protected from accidental local changes in the Fudo interface. Centralized credential management helps maintain consistent permissions across the enterprise.

Active Threat Protection

3.1 Detection of Compromised Credentials

Privileged access oversight is most effective when passive recording is combined with solutions that enable early anomaly detection.

Compromised or weak passwords remain a common source of incidents. Fudo Enterprise 6.1 includes a feature to audit credentials stored in the Password Vault.

On-Premises Processing of Breach Databases

Administrators can upload lists of known leaked credentials directly to the system. All analysis is performed locally on the appliance, ensuring private data and password structures remain within the client's secure environment.

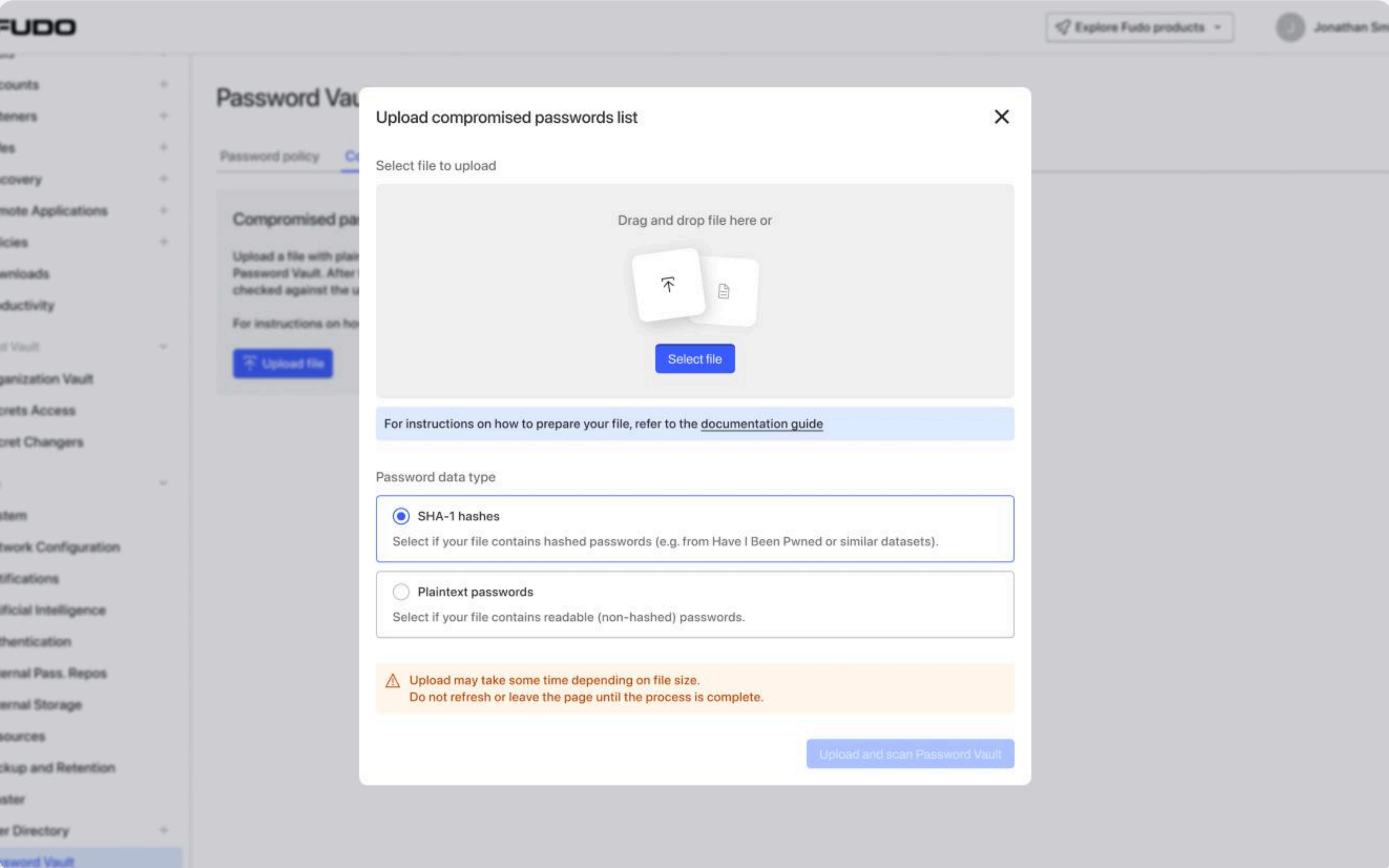
THE MODERN MANAGEMENT OF PRIVILEGED ACCESS

Password Verification in Operational Processes

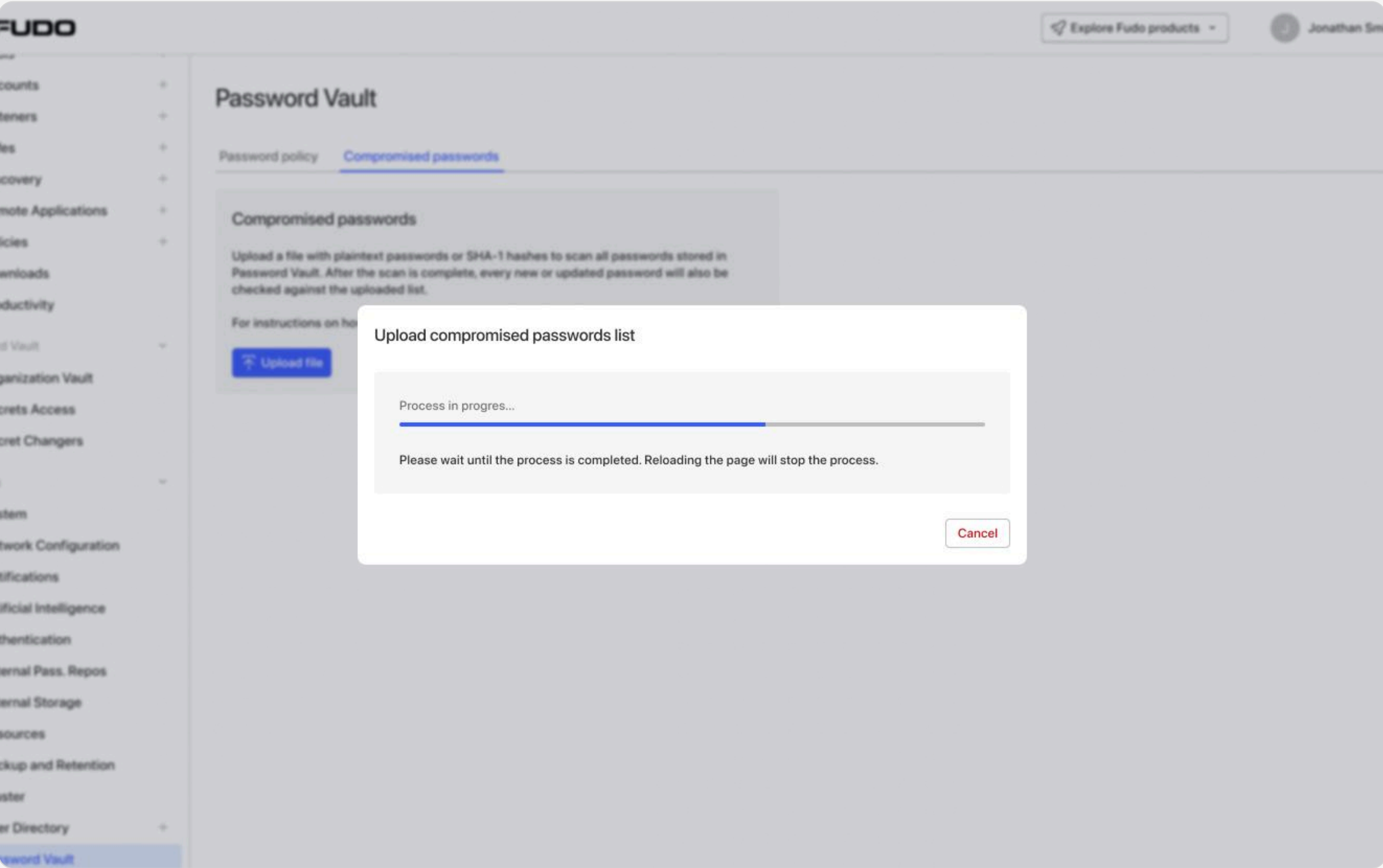
The system performs verification both during breach database imports and during ongoing operations such as creating or editing records. If a weak or previously leaked password is identified, Fudo flags it with a visual warning, making it easier to decide whether to change the secret.

Compliance with Industry Recommendations

This functionality aligns with best practices and identity management guidelines, such as NIST SP 800-63B, which recommend checking proposed credentials against registries of known breaches.

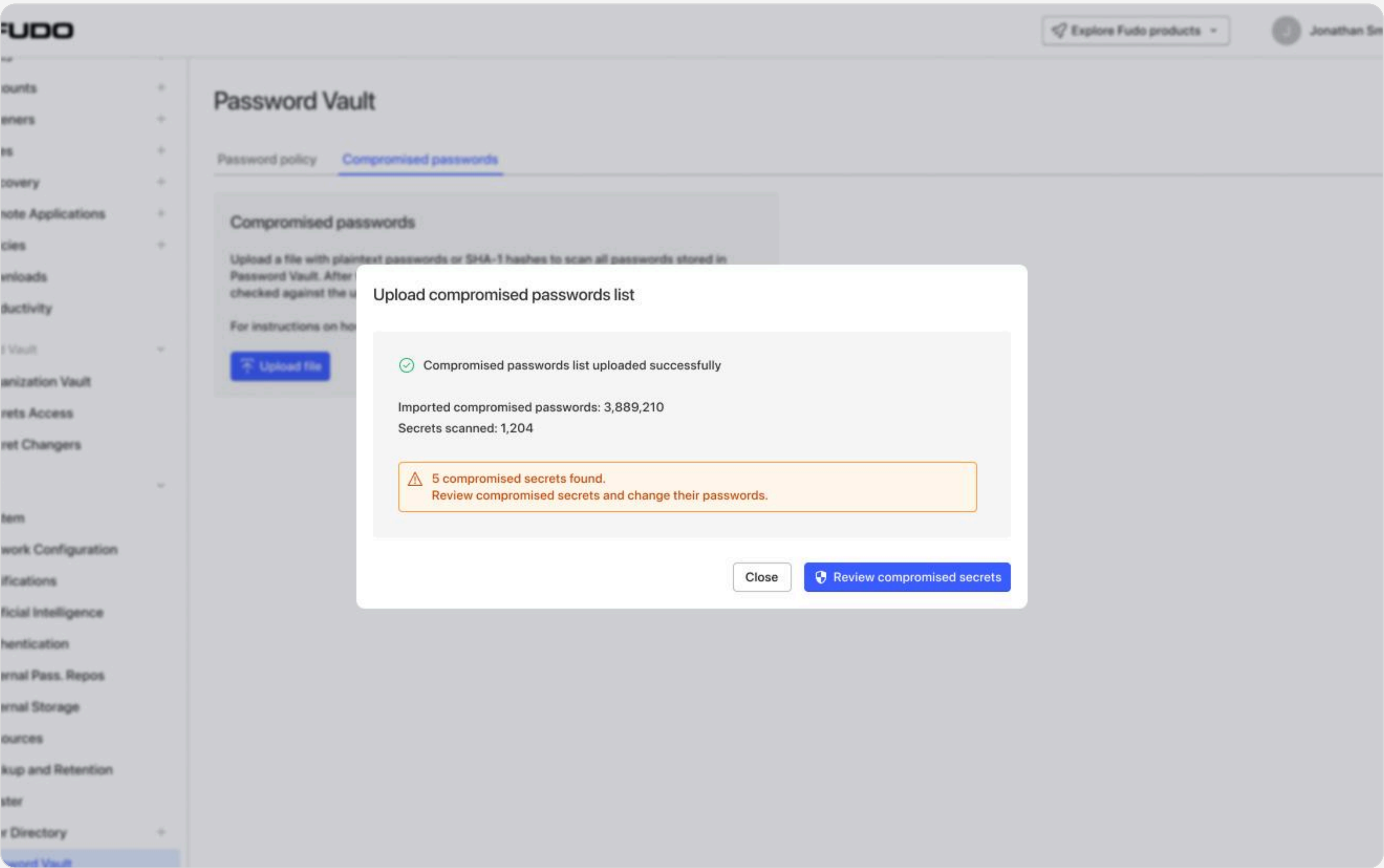


Upload screen for compromised credentials in SHA-1 hash or plain text format. Triggers a cross-check of stored Password Vault secrets against known breach records.

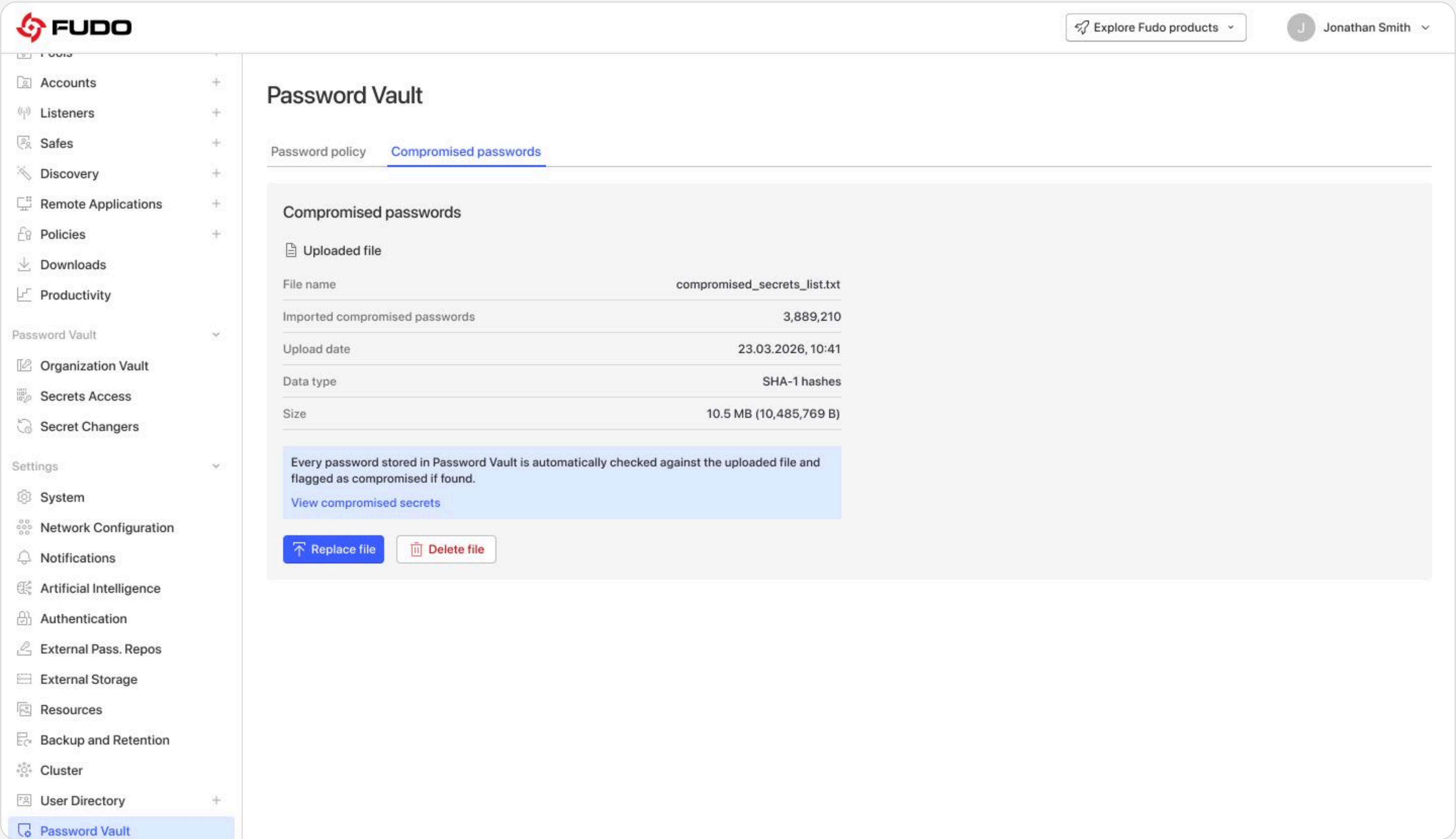


Progress indicator for the upload and automated scanning of the Password Vault against a breach database in Fudo Enterprise 6.1.

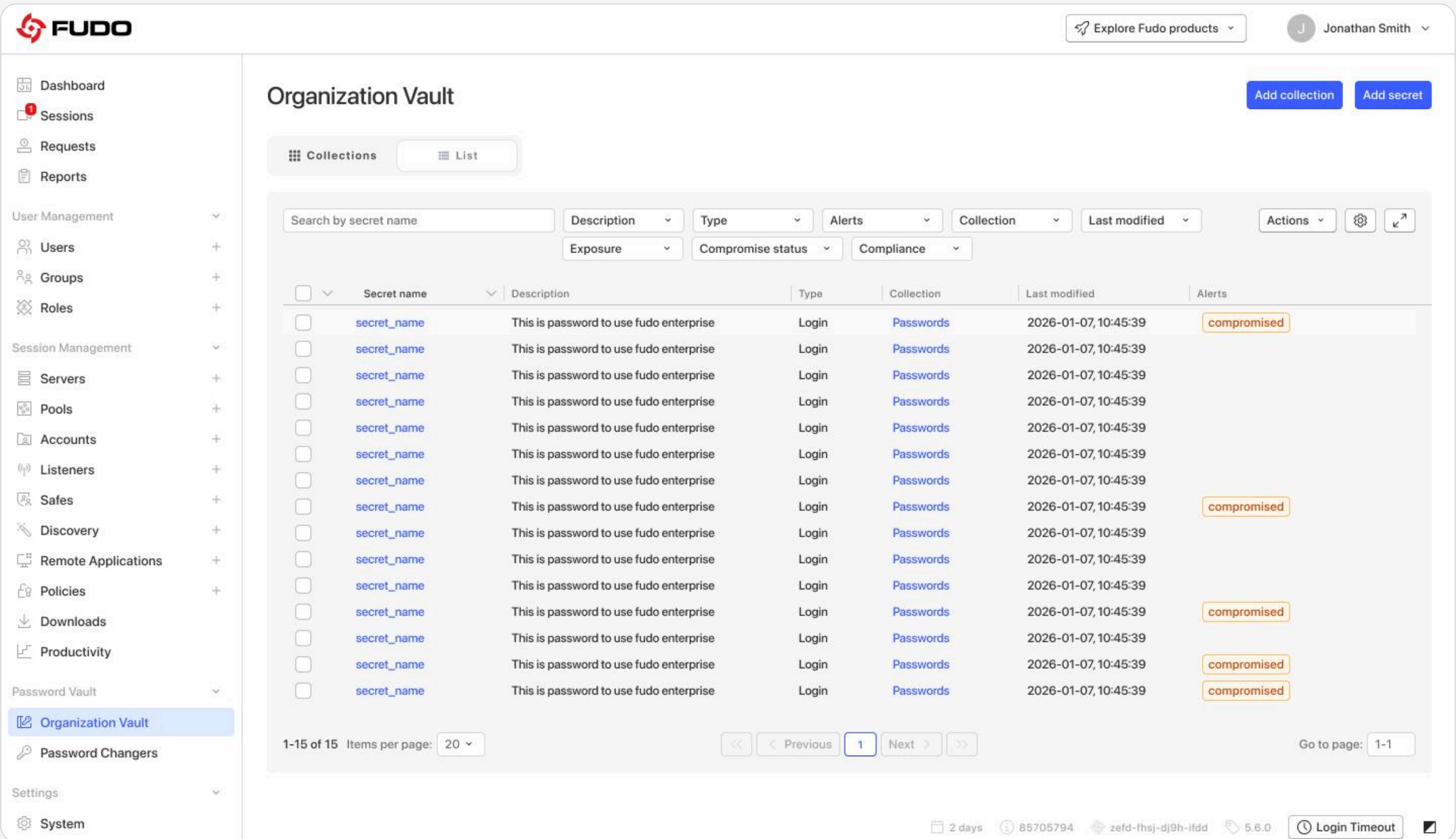
THE MODERN MANAGEMENT OF PRIVILEGED ACCESS



Upload completion screen showing detected compromised secrets in the Password Vault with direct access to remediation options.



Information screen for an uploaded breach file displaying import metrics and continuous automated verification status in Fudo 6.1.



The Organization Vault list view in Fudo Enterprise 6.1, highlighting compromised credentials with prominent alert tags for efficient remediation.

3.2

Sudo: Privilege Management in Linux Environments

Managing administrative privileges on Linux servers is challenging due to dispersed configuration files.

Whitelisting: Explicit Consent Model

A dedicated sudo plugin changes how permissions are granted. Instead of blocking specific commands, the default policy restricts execution and allows only commands explicitly approved by administrators.

The plugin communicates with the Fudo system through an API. Rights verification occurs outside the local operating system, reducing the risk of users bypassing established rules.

Each use of a privilege-escalating command can be logged and linked to email or mobile app alerts, giving security teams greater visibility into operations on critical servers.

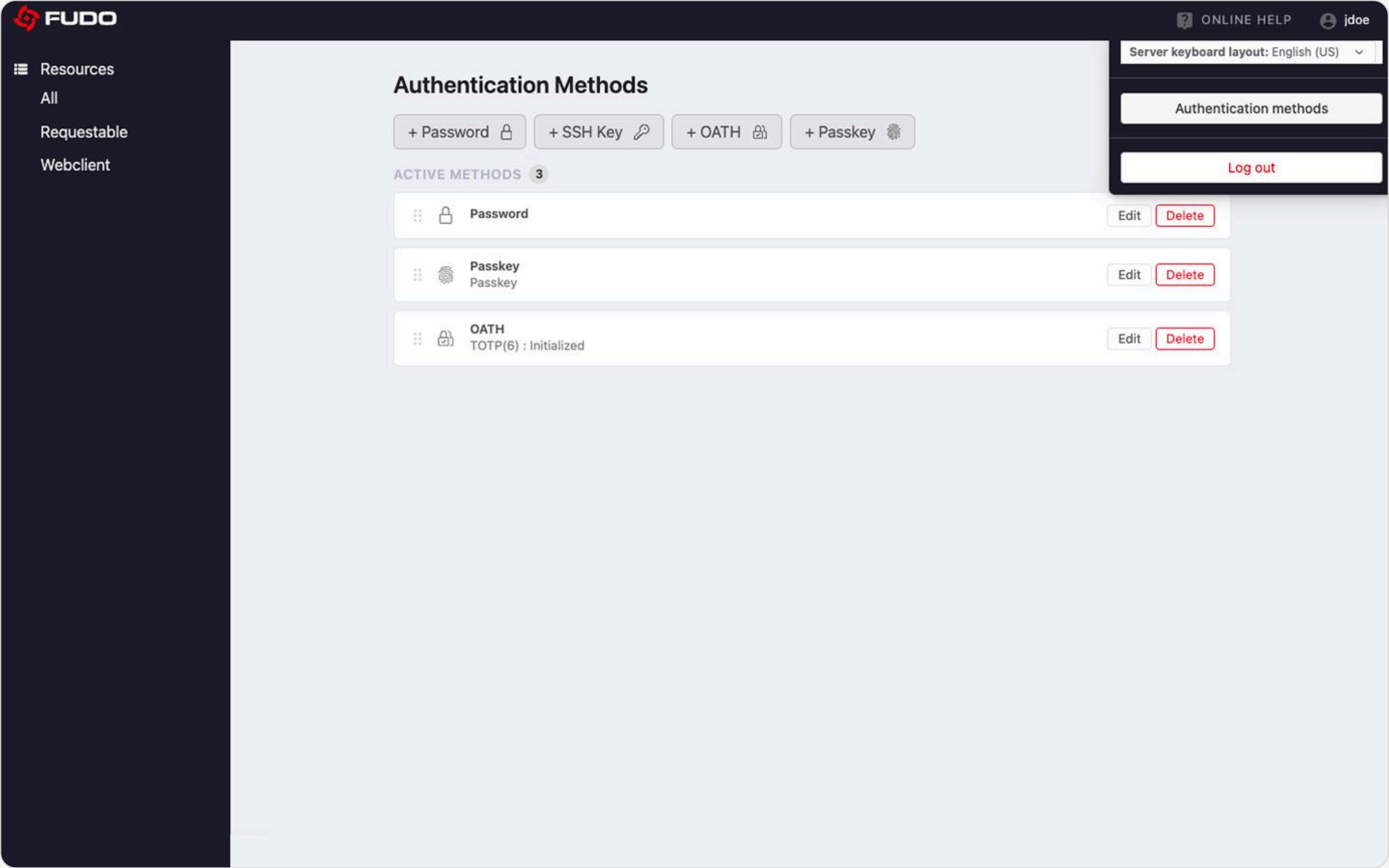
3.3

Modern Authentication Methods and Password Handling

Adopting phishing-resistant authentication methods is essential for organizational resilience

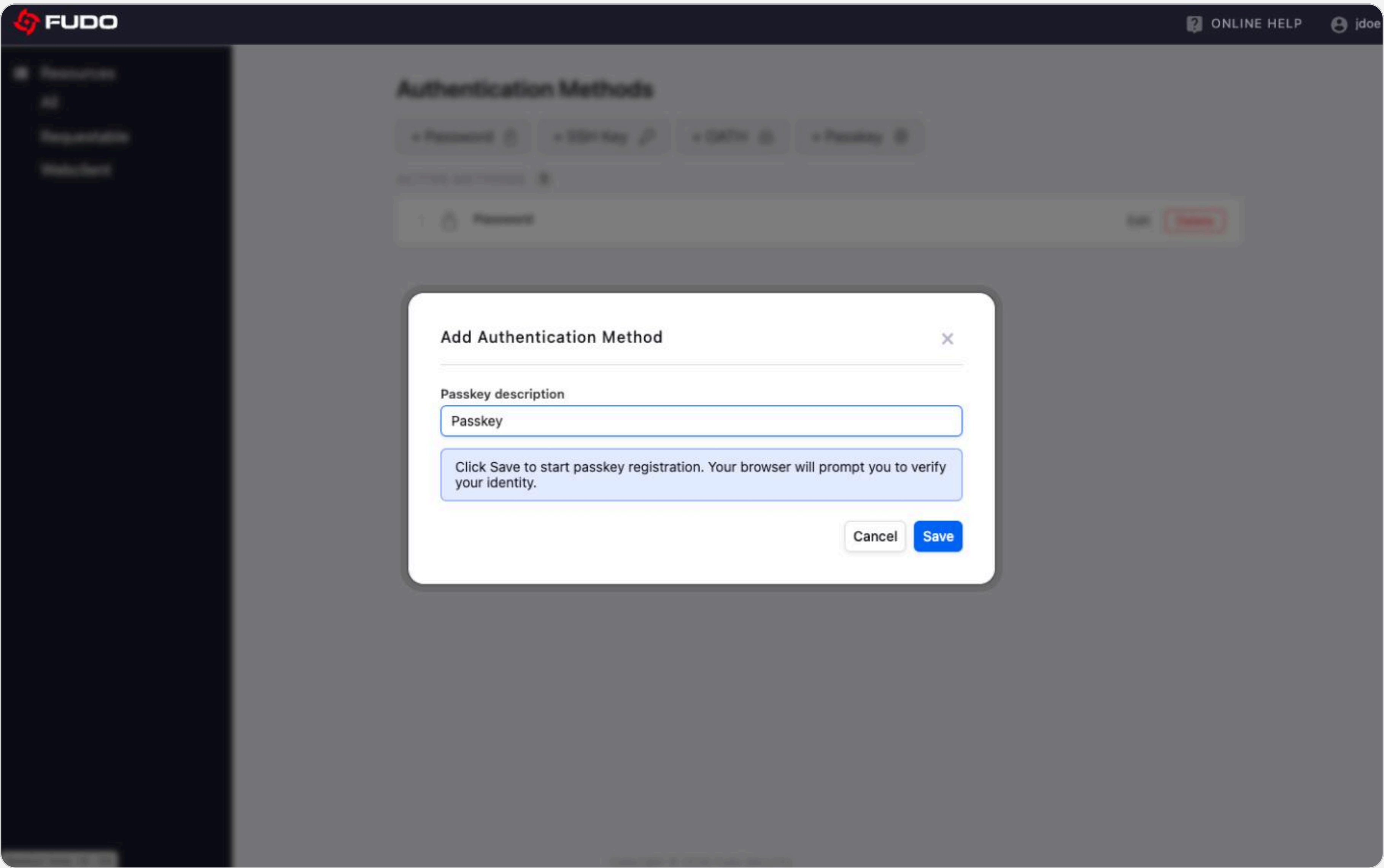
FIDO2 Standard and Passwordless Access

Fudo 6.1 supports passwordless logins using the FIDO2 standard. Users can use hardware keys, such as YubiKey, and built-in biometric features, managing credentials through a self-service portal.

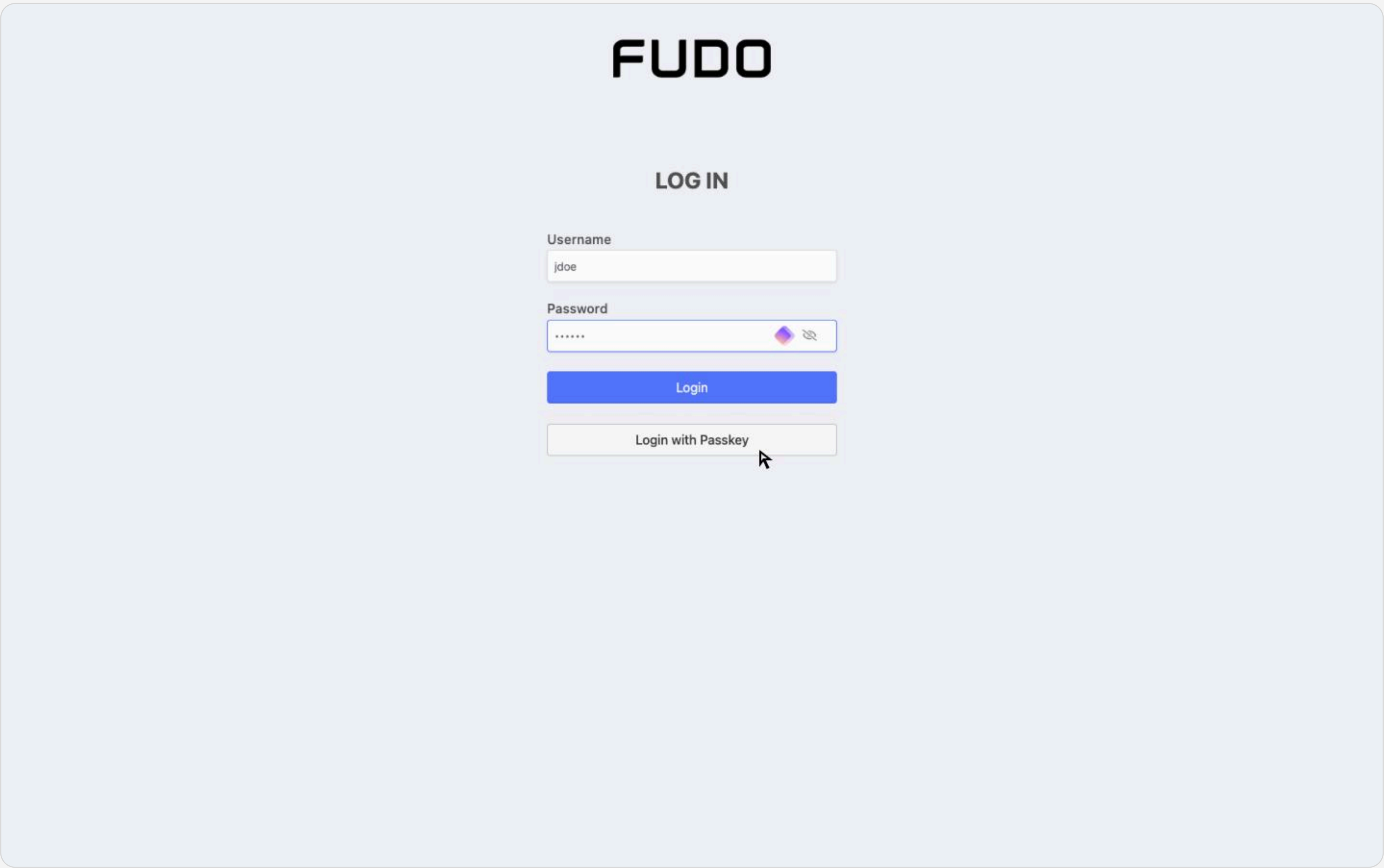


The authentication methods configuration screen in the Fudo 6.1 user portal, supporting Passwords, SSH Keys, OATH tokens, and Passkeys.

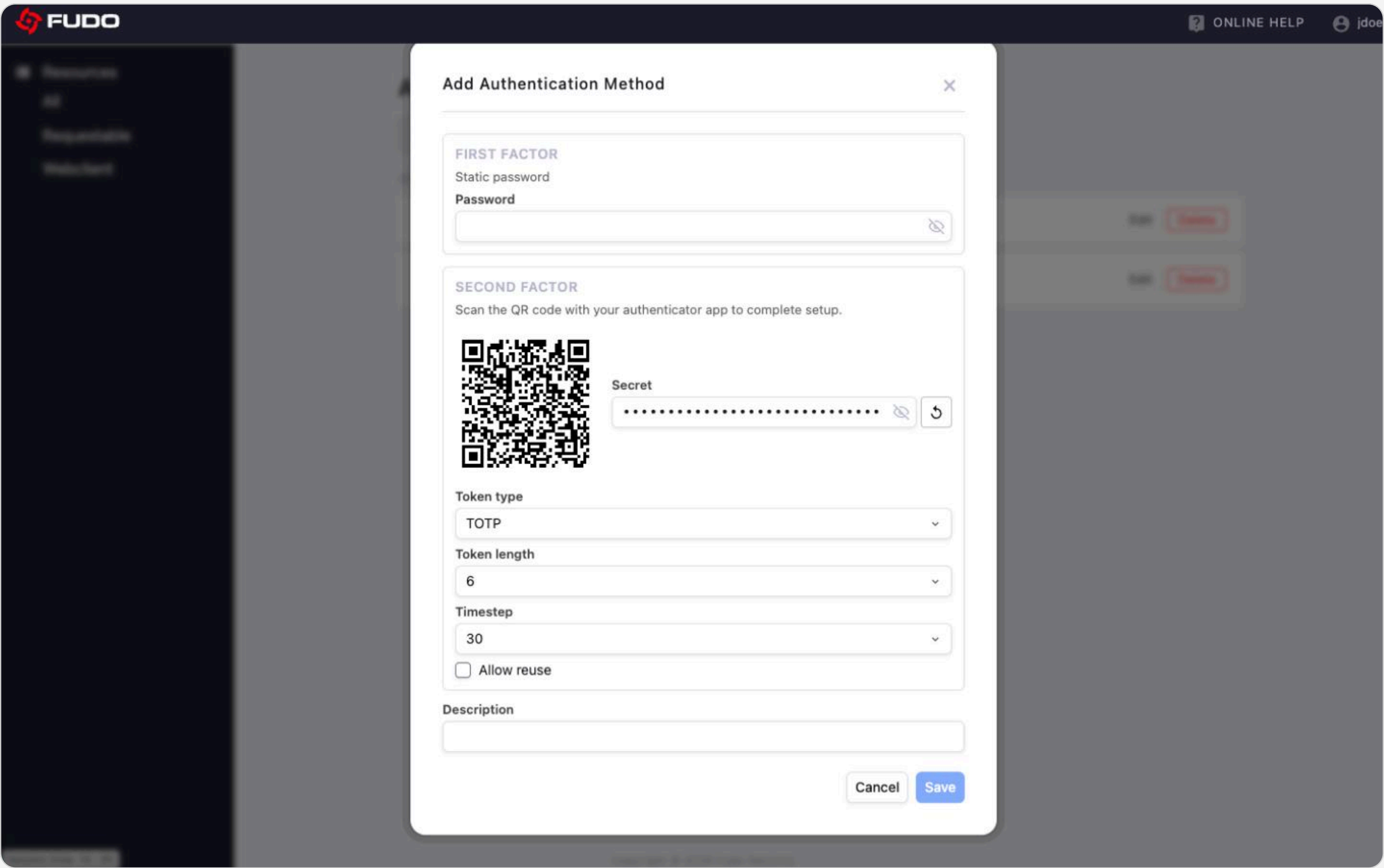
THE MODERN MANAGEMENT OF PRIVILEGED ACCESS



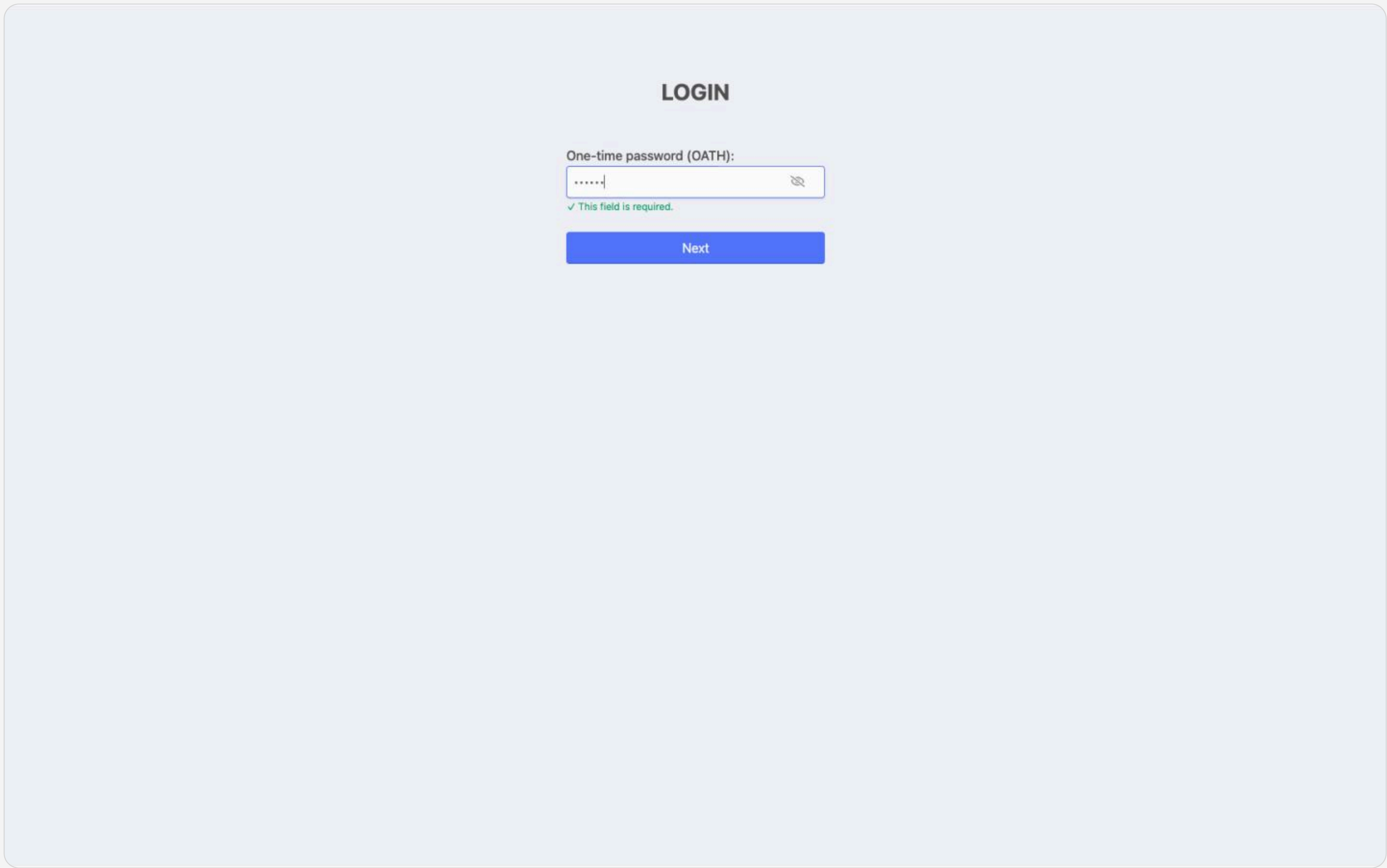
The Passkey registration setup screen in Fudo Enterprise 6.1, guiding users through the pairing of hardware security keys or biometrics.



The Fudo Enterprise 6.1 login screen displaying dual authentication paths, including standard credentials and passwordless Passkey sign-in.



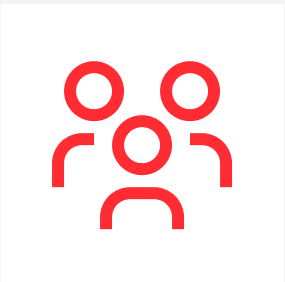
The OATH authentication configuration screen in Fudo Enterprise 6.1, featuring QR code scanning for TOTP authenticators and token reuse settings (Allow reuse).



The OATH one-time password entry screen in Fudo 6.1 for multi-factor authentication verification.

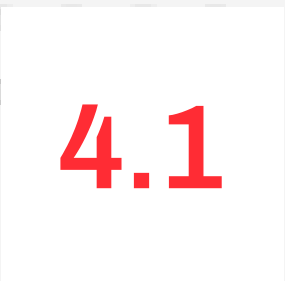
Login Automation via Browser Extension

A browser extension integrated with the Password Vault simplifies secure credential autofill in web applications. This removes the need to manually copy passwords or store them in unsecured files.



Daily Convenience for Users and IT Teams

Effective security mechanisms should not place excessive operational burdens on users or administrative teams.



4.1 RDP: File Transfer in the Web Client

File exchange between local devices and remote servers is a routine administrative task. Fudo Enterprise 6.1 expands the RDP Web Client to support bidirectional file transfers directly in the browser.

Direct File Uploads and Downloads

Users can upload files to the target server and download them to their local device through the RDP Web Client's intuitive interface, including drag-and-drop. Uploaded files appear as a dedicated input drive in the remote session, and a modified toolbar enables real-time transfer tracking.

Automated Resource Cleanup

After the session ends, the transfer directory can be automatically cleared, reducing the risk of leaving confidential or unnecessary data on the target server.

4.2

Streamlining Operations for Administrative Teams

As infrastructure grows, administrators must manage an increasing number of objects.

Bulk Operations

The Fudo administrative panel enables bulk editing, status changes, and policy assignments for multiple objects at once. This streamlines routine tasks and reduces time spent on repetitive requests.

TOTP Reuse Within Time Window

Allowing reuse of the same time-based one-time password (TOTP) code within its validity window eases administrative tasks. This accelerates work when starting multiple sessions or logging into distributed resources in quick succession, removing the need to wait for a new token.

ShareAccess: Cloud-Based Resource Access

Collaboration with third parties, such as auditors, service technicians, or software vendors, requires secure resource sharing without complex procedures.

SaaS Model

The cloud-based Fudo ShareAccess service requires no additional appliance installation on the client's local infrastructure or software deployment on vSaaS Model The cloud-based Fudo ShareAccess service does not require appliance installation on the client's infrastructure or software deployment on vendor workstations.a specific application or server that the user accesses within a browser window. This limits visibility to the rest of the infrastructure.

Time-Bound Access Control and Credential Protection

External vendors authenticate through the portal and perform tasks within a set time window. Credentials are injected without being exposed to the user, reducing the risk of unauthorized use outside the designated channel.



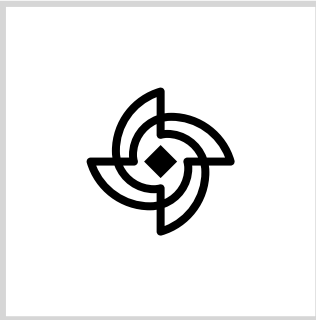


Summary

6.1

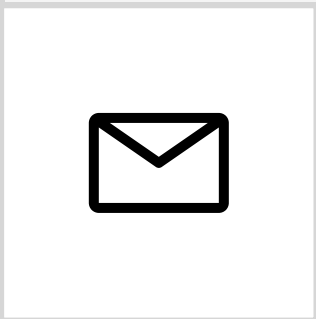
The Modern Management of Privileged Access

Selecting the right Privileged Access Management solution requires considering each organization's unique needs and technological maturity. Fudo Enterprise 6.1 provides a flexible toolkit for building a secure IT environment, offering modern authentication, cloud integration, and workflow enhancements for both administrators and end users.



www.fudosecurity.com

>



Talk to Sales

>

Contact us at
sales@fudosecurity.com