

Keeper Security Launches ServiceNow Workflow Integration for Governed, Self-Service Vault Management

LONDON, UNITED KINGDOM, May 20, 2026 /EINPresswire.com/ -- New integration brings Keeper Vault operations – including access requests, record storage and endpoint privilege management approvals – directly into ServiceNow's Service Catalog and Flow Designer

[Keeper Security](#), the leading zero-trust and zero-knowledge identity security and Privileged Access Management (PAM) platform, today announces the availability of the Keeper Security Workflow application for ServiceNow. The integration empowers enterprise administrators and security teams to manage Keeper Vault operations directly within ServiceNow's IntegrationHub, Flow Designer and Service Catalog portal, creating a governed, self-service experience for privileged access requests without requiring users to leave their existing IT workflows.

As enterprise environments grow in complexity, security teams face mounting pressure to provide controlled, auditable access to privileged credentials and sensitive records, while keeping friction low for end users. Manual processes for requesting and granting vault access create delays, compliance gaps and inconsistent enforcement. The Keeper Security Workflow integration eliminates that friction by embedding Keeper's privileged access controls natively into the ServiceNow platform, where IT and security teams already operate.

Available now on the [ServiceNow Store](#), the application leverages the Keeper Commander Command-Line Interface (CLI) running in service mode on a ServiceNow MID Server to deliver a full suite of governed vault operations, including:

- **Access Request Management:** End users can request access to specific Keeper Vault records or folders through the ServiceNow Service Catalog. Requests route automatically to designated approval groups, and upon approval, records are shared directly to the requesting user with a full audit trail throughout.
- **Endpoint Privilege Management (EPM) Approvals:** EPM requests raised from endpoint devices automatically generate Security Incident Response tickets in ServiceNow. Administrators can approve or deny requests within the platform, and incident tickets are closed with appropriate comments upon resolution.
- **Secure Record Creation:** Administrators and fulfillment teams can store new credentials,

including database credentials, login records, server credentials, SSH keys, software licences, secure notes and membership records, directly in the Keeper Vault within ServiceNow.

- Record and Folder Search: Security teams can search Keeper Vault records and folders by name or UID from within the ServiceNow task interface, enabling rapid fulfillment of access requests.
- One-Time Share Capabilities: Administrators can generate and deliver time-limited, one-time record shares to users without granting permanent vault access.

The integration's guided setup walks administrators through MID Server configuration, Keeper Commander CLI installation, service mode activation and approval group assignment, requiring no custom code.

"This integration reflects how we think about enterprise deployments: meet organisations inside their existing platforms and make security frictionless without making it permissive," said Craig Lurey, CTO and Co-founder of Keeper Security. "The Keeper Commander CLI running in service mode on the MID Server gives ServiceNow a direct, secure channel into the Keeper Vault, enabling real automation without compromising our zero-knowledge architecture."

The Keeper Security Workflow application for ServiceNow is available now on the ServiceNow Store. For more information or to access setup documentation, visit [KeeperSecurity.com](https://www.keepersecurity.com) or the [Keeper documentation portal](#).

###

About Keeper Security

Keeper Security is the leading zero-trust and zero-knowledge identity security solution, trusted by millions of people and thousands of organisations globally. KeeperPAM® is Keeper's privileged access management platform that unifies password and passkey management, secrets management, privileged session management and endpoint privilege management in a single cloud-native platform, protected with quantum-resistant encryption. KeeperAI delivers real-time, AI-native threat detection across every privileged session. As AI agents proliferate and identity becomes the defining attack surface, Keeper governs access for humans, machines, non-human identities and AI agents, serving as the unified control plane for access, compliance and visibility across the enterprise. For more information, visit [KeeperSecurity.com](https://www.keepersecurity.com).

Learn more: <https://www.keepersecurity.com/>

Media Contact

Beth Smith

Senior Account Director - Eskenzi PR

beth@eskenzipr.com

Visit us on social media:

[LinkedIn](#)

[Instagram](#)

[Facebook](#)

[YouTube](#)

[TikTok](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/913638666>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.