Keeper Security Brings Privileged Access Controls to Microsoft Teams With New Keeper Teams App

Keeper Teams App embeds governed, auditable workflows directly into Microsoft Teams, enforcing zero standing privilege and eliminating credential risk

LONDON, LONDON, UNITED KINGDOM, June 25, 2026 /EINPresswire.com/ --
Keeper Security, the leading zero-trust and zero-knowledge identity security and Privileged Access Management (PAM) platform, today announces the availability of the Keeper Teams App, a new integration that brings privileged access request and approval workflows directly into Microsoft Teams. The integration is powered by Keeper Secrets Manager (KSM) and Commander Service Mode, preserving Keeper's zero-knowledge security model while enabling users to manage credential access without switching tools.

When privileged access requests are submitted through email chains, IT tickets or separate portals, security teams lose the visibility that zero-trust enforcement requires. For organisations using Microsoft Teams as their primary collaboration platform, that gap has been structural. The Keeper Teams App closes the loop by embedding governed, auditable access workflows directly in Teams, while keeping all cryptographic operations and credential data within the customer’s preferred environment.

The Keeper Teams App enables users to initiate and approve privileged access actions within Teams, across five core workflows:

- Record and Folder Access Requests: Users can request access to specific vault records or shared folders with justification, custom permissions and time-limited access windows, enforcing zero standing privilege on every request. When a request involves a PAM User record or PAM User folder, approvers reviewing the request see an auto-rotation option enabled by default. Once the time-limited access window expires, credentials automatically rotate on the vault side, ensuring no standing credential footprint survives the session.

- One-Time Share Requests: Users can request a self-destructing share link for a password or secret, with optional editable and bi-directional sharing capabilities.

- Keeper Endpoint Privilege Manager (KEPM) Approvals: Just-in-time elevation requests from

Endpoint Privilege Manager are routed to approvers in real time via a dedicated Teams channel.

- SSO Cloud Device Approvals: Administrators can approve SSO Cloud device requests directly within Teams when the Keeper Automator service is not deployed.

- Self-Service Secret Creation: Users can create new login records with auto-generated passwords directly from Teams. Records are saved to a designated shared folder in the Keeper Vault, including support for Nested Shared Folder (NSF) records. Users can select a Classic or NSF target folder, choose a subfolder and create secrets directly, with the app automatically detecting the correct permission model.

The Teams App is also designed to handle mixed environments. Search results surface whether an item is a Classic shared record or an NSF record, and the approval interface presents the appropriate permission model for each: standard permissions for Classic items and role-based NSF permissions – viewer, share-manager, content-manager or full-manager – for NSF items.

"The weakest point in any access control strategy is the moment a user decides to work around it because the approved process is too cumbersome or slow," said Craig Lurey, CTO and Co-founder, Keeper Security. "By embedding approval workflows directly into Teams, we removed the friction that drives those workarounds, so the secure path and the fast path are one in the same."

The Keeper Teams App is customer-hosted and deployed via Docker alongside Commander Service Mode on the customer's own infrastructure. This design ensures that no credentials or secrets pass through Keeper's cloud, maintaining full end-to-end encryption and zero-knowledge compliance. Configuration is secured and retrieved via KSM, and the streamlined "teams-app-setup" command in Keeper Commander automates the setup process for rapid deployment.

The Teams App extends Keeper's growing ecosystem of workflow integrations. Alongside recently announced integrations with Jira, ServiceNow and Slack, the Teams App reflects Keeper's platform strategy of embedding privileged access governance into the tools where security and IT teams already – operate without surrendering the enforcement, encryption and audit controls that define Keeper's solutions.

The Keeper Teams App is available now for organisations with a Keeper Secrets Manager or KeeperPAM license. Set up documentation is available at docs.keeper.io. For more information on KeeperPAM, visit KeeperSecurity.com.

Bethany Smith
Eskenzi PR
email us here
Visit us on social media:
LinkedIn

Instagram
Facebook
YouTube
TikTok
X
