

Keeper Security Launches Certified Microsoft Power Platform Connector for Secrets Manager

Connector lets teams retrieve and manage credentials at runtime within Azure Logic Apps & Power Automate, eliminating hardcoded secrets from automated workflows



LONDON, UNITED KINGDOM, August 19, 2026 /EINPresswire.com/ -- [Keeper Security](#), the leading zero-trust and zero-knowledge identity security platform, today announces the availability of a certified connector integrating Keeper Secrets Manager with Microsoft Azure Logic Apps. The connector, now published on the [Microsoft Power Platform marketplace](#),

“

The architecture here reflects a principle Keeper holds across the entire platform. Secrets should be decrypted as close to the workload as possible and only when needed.”

Craig Lurey, CTO and Co-founder of Keeper Security

enables enterprise teams to create and retrieve credentials at runtime directly within automated workflows without ever hardcoding sensitive values in flows.

As organisations scale workflow automation across cloud environments, secrets management has become a critical, and frequently overlooked, gap. Hardcoded credentials in automation scripts and workflows represent one of the most persistent and exploitable vulnerabilities in enterprise environments. The Keeper Secrets Manager connector for Azure Logic Apps addresses this directly, giving teams a zero-knowledge, policy-enforced path to

secrets management inside Microsoft Power Platform.

"Workflow automation is only as secure as the secrets powering it, and most organisations are still hardcoding those secrets which creates massive cyber risk," said Darren Guccione, CEO and Co-founder of Keeper Security. "This connector eliminates that exposure by bringing Keeper's zero-knowledge architecture directly into the Microsoft automation layer: secrets stay encrypted in the vault and are retrieved only at the moment they are needed, so there is nothing hardcoded to steal."

The connector operates through a lightweight Python middleware service deployed as an Azure

Function App, communicating with the Keeper Vault via the Keeper Secrets Manager SDK. All secrets remain encrypted under Keeper's zero-knowledge security architecture and are decrypted locally within the customer's Azure environment – never transmitted in plaintext through Keeper's infrastructure.

"The architecture here reflects a principle Keeper holds across the entire platform," said Craig Lurey, CTO and Co-founder of Keeper Security. "Secrets should be decrypted as close to the workload as possible and only when needed. The Azure Function middleware gives customers a deployment model where the Keeper SDK runs inside their own Azure environment, their own key management handles the configuration and plaintext credentials are never in motion across a network boundary they do not control."

Key capabilities of the Keeper Secrets Manager Connector for Azure Logic Apps

- Certified connector: Integrates natively in the Logic App Designer with no custom import required for standard deployments.
- Runtime secrets retrieval: Fetches credentials on demand within any Logic App flow without storing them in the workflow definition.
- One-click deployment: Provisions all required infrastructure – including the Azure Function App, Key Vault and Managed Identity – in minutes using an Azure Resource Manager (ARM) template.
- Dynamic dropdowns: Auto-populates secret and folder pickers in the Logic App designer, reducing configuration error and accelerating deployment.
- Credential creation: Provisions secrets directly from automated workflows, supporting employee onboarding and scheduled compliance audits.

The connector supports five operations, including List Secrets, Get Secret, Create Secret, Update Secret and List Folders, covering workflows from API credential injection and database connection string retrieval to GitHub secret synchronisation and vault compliance auditing. The Keeper Secrets Manager connector for Azure Logic Apps is available now. Full documentation, the middleware repository and deployment instructions are available at docs.keeper.io.

###

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.

Charley Nash

Eskenzi PR

[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/935120311>

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.