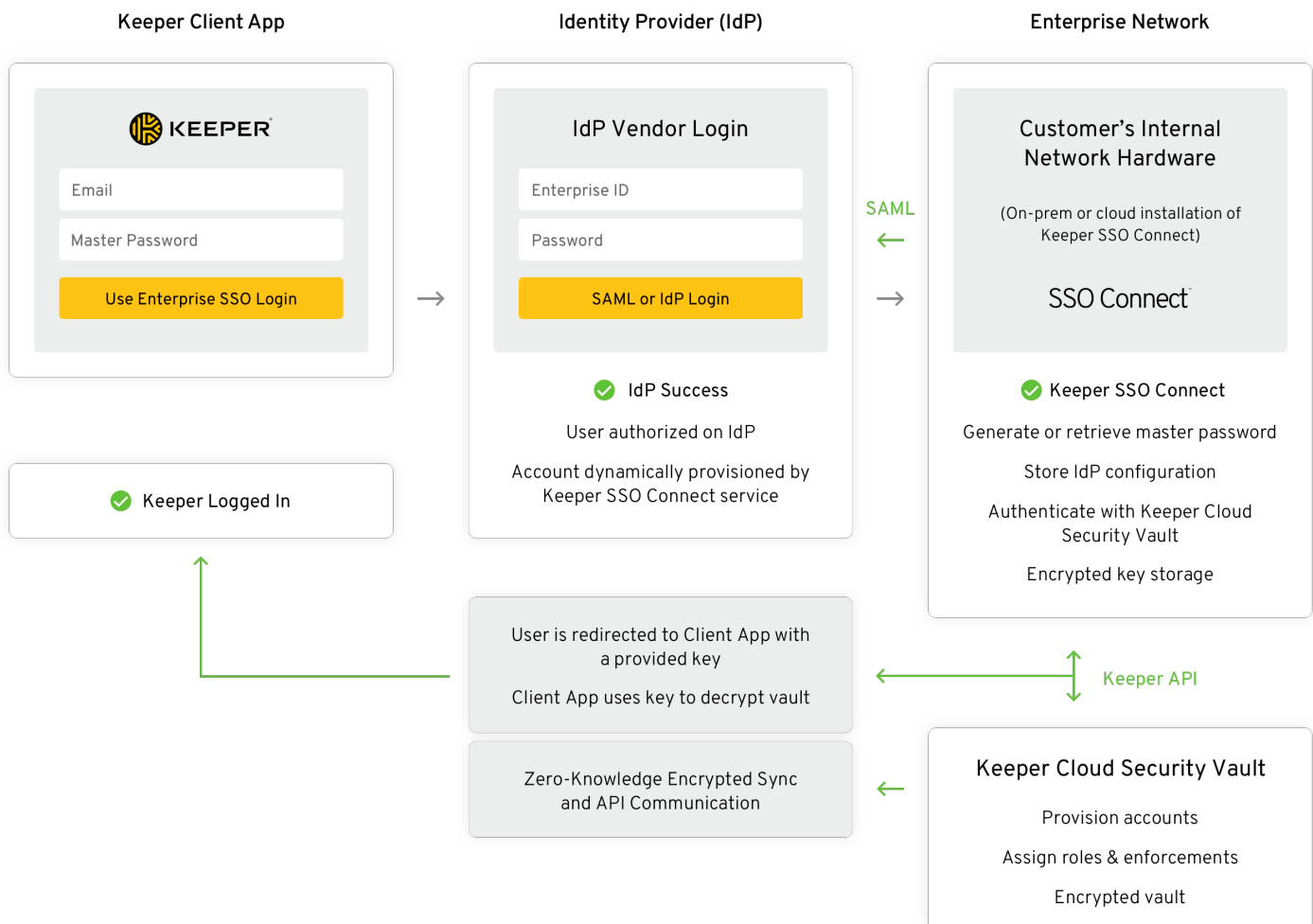


Keeper Security is transforming the way businesses and individuals protect their passwords and sensitive digital assets to significantly reduce cyber theft and increase online productivity. As the leading password manager and digital vault, Keeper helps millions of people and thousands of businesses substantially mitigate the risk of a data breach.

Keeper SSO Connect enables organizations to significantly enhance their Single Sign-On deployments with an integrated zero-knowledge vault which provides advanced password management, sharing and security capabilities. Keeper SSO Connect also provides secure storage, management and sharing of sensitive files, documents, photos and videos.

Product Overview

Keeper SSO Connect is a SAML 2.0 application which leverages Keeper's zero-knowledge security architecture to securely and seamlessly authenticate users into their Keeper Vault and dynamically provision users to the platform. Keeper SSO Connect works with popular SSO IdP platforms such as Okta, OneLogin, Ping Identity, F5 BIG-IP APM, G Suite and Microsoft ADFS/Azure to provide businesses the utmost in authentication flexibility.



Business Value

Many businesses use Single Sign-On (SSO) solutions. Although these solutions offer a unified login experience they lack the flexibility to store a variety of sensitive information beyond a simple username and password record. As an example, these solutions can't accommodate login credentials for native applications, bank account numbers, personal identifiable information, employee census data, customer credentials and confidential images, documents and video files.

Keeper SSO connect enhances any Single Sign-On solution by providing a secure password manager and digital vault solution in a zero-knowledge environment that stores not only a login and password, but also securely stores and encrypts proprietary customer data, access credentials to restricted systems and sensitive documents.

System Requirements

Keeper SSO Connect is a software application that is installed on the enterprise customer's on-premise, private or cloud servers. User encryption keys are generated dynamically by Keeper SSO Connect, encrypted and stored locally on the installed server, providing the customer with full control over the encryption keys that are used to encrypt and decrypt their digital vaults.

The Keeper SSO Connect service application can be installed on a private on-premise or cloud-based server. Windows, Mac OS and Linux operating systems are supported.

Certifications



*Visit keepersecurity.com/security for a complete list of all audit and security certifications.

Who Uses Keeper?

Over 3,000 organizations trust Keeper including Sony, Siemens, Dow, Chipotle and IBM. Feedback and collaboration with our customers helps drive ongoing feature improvement and product innovation to ensure the Keeper solution continues to deliver business value.

