# Google Cloud

## EKM Integration


# Maximize data privacy and compliance with external key management for Google Cloud by Futurex

### What is Google Cloud External Key Manager (EKM)?

Google Cloud EKM allows you to create, store, and manage keys in a separate environment from encrypted data, using Futurex's FIPS 140-2 Level 3 validated key management technology. With this, you can enhance data privacy, access control, and key provenance and maintain control over your own encryption keys.

Google Cloud

### How is Futurex's Google Cloud EKM solution deployed?

**Futurex On-Premises Hardware**

**VirtuCrypt Cloud**

**Futurex/VirtuCrypt Hybrid**

- **Secure**: FIPS 140-2 Level 3 validated
- **Compliant**: regional data residency, privacy, and sovereignty mandates
- **Resilient**: deploy high-availability configurations with uptimes of 99.999%
- **Scalable**: expands to meet your needs
- **Flexible**: available on-premises, via Futurex's cloud, or as a hybrid model
- **Centralized**: integrates with additional 3rd-party applications for key management

Engineering Campus - 864 Old Boerne Road, Bulverde, Texas 78163 USA - P: +1 (830) 980-9782 TF: (800) 251-5112 - info@futurex.com

## Straightforward setup

### Enable Google Cloud EKM integration

Futurex's solution integrates with all Google Cloud services supported by their KMS.

Google Cloud

1. Log in to KMES Series 3 interface
2. Configure users, keys, and JWT
3. Log in to Google KMS dashboard
4. Create a new key ring
5. Create externally managed keys in Google KMS
6. Test encryption and decryption operations with externally managed keys

## Enterprise-wide data protection

Futurex provides a versatile external key service using fully validated HSM and cloud technology. In addition to solutions for Google Cloud External Key Manager, Futurex's **Key Management Enterprise Server (KMES) Series 3** offers the following functionality:

- Cloud key management
- Data protection
- Public key infrastructure (PKI)
- Certificate authority (CA)
- Code signing
- Vaultless tokenization

## VirtuCrypt Cloud HSM services

**Futurex's VirtuCrypt** cloud grants you access to an innovative set of solutions for encryption, key management, PKI & certificate authority, and much more.

With this service, you can easily create, deploy, and manage virtual HSMs. The VirtuCrypt Intelligence Platform (VIP) provides an intuitive UI with which to centralize cryptographic management across organizational units.

- Automated **provisioning** of cloud HSMs through VirtuCrypt Intelligence Portal
- Easy **migration** from legacy on-premises HSMs to cloud HSMs
- User-controlled **clustering** and high availability
- Services available from **worldwide** data centers
- 99.999%+ **SLA-backed** uptime

FUTUREX

Engineering Campus - 864 Old Boerne Road, Bulverde, Texas 78163 - USA
TF/ (800) 251-5112 P/ +1 (830) 980-9782 info@futurex.com

## Futurex solution details

### Full lifecycle protection

Create, store, and manage keys from a user-friendly centralized platform.

### Encryption key algorithms

Futurex supports 256-bit AES encryption keys for high-assurance data security, with user-defined rotation policies.

### Attribute-based access control

Granular control over key access allows you to control access and set policy based on attributes like geographic location, application, time and date, and more.

### Supported CMEK integration

- Artifact Registry
- BigQuery
- Compute Engine
- Cloud Logging: Log Router
- Cloud Spanner
- Cloud SQL
- Dataflow Appliance and Dataflow Shuffle
- Google Kubernetes Engine: Data on VM disks or Application-layer Secrets
- Pub/Sub
- Secret Manager

*Futurex VirtuCrypt Intelligence Portal (VIP)*

**To learn more about Futurex's solution for Google Cloud EKM integration, or to inquire about a demo, visit [futurex.com](futurex.com)**