FUTUREX

Google Workspace

Client-side encryption

Key Lifecycle Management to Protect Data in the Cloud

Client-side encryption: The Next Step Forward in Data Security

Google Workspace Client-side encryption (coming soon to beta) gives enterprises the ability to encrypt their data before sending it to Google's servers. Client-side encryption gives customers direct control of encryption keys and makes customer data indecipherable, placing unprecedented control in the user's hands. Futurex provides the world's most versatile and secure key management service for encrypting data sent to Google Drive, Docs, Sheets, and Slides.

The Benefits of Google Workspace Client-side encryption with Futurex

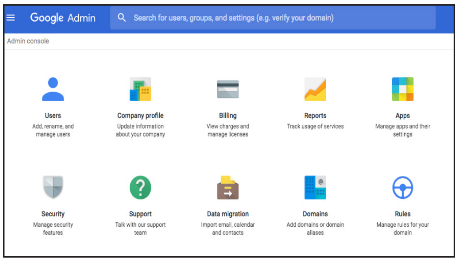
- ✓ FIPS 140-2 Level 3 validated key management service
- ✓ Available on-premises or via the cloud
- ✓ Configurable across organization units
- ✓ Eliminates risk of host-side data leaks
- ✓ Enterprise-wide privacy and security

Drive, Docs, Sheets, and Slides

Straight-Forward Setup

Enable Client-side encryption for Multiple Users via Google Workspace Admin Console

1. Log into admin console
2. Select option to add an external key service (KACLS)
3. Enter the KACLS server address
4. Specify organizational units
5. Configure 3rd party Identity Provider


Google Admin
Search for users, groups, and settings (e.g. verify your domain)
Admin console
Users
Add, rename, and manage users
Company profile
Update information about your company
Billing
View charges and manage licenses
Reports
Track usage of services
Apps
Manage apps and their settings
Security
Manage security features
Support
Talk with our support team
Data migration
Import email, calendar and contacts
Domains
Add domains or domain aliases
Rules
Manage rules for your domain

Enterprise-Wide Data Protection

Futurex provides a versatile external key service using fully validated HSM and cloud technology. In addition to solutions for Google Workspace Client-side encryption, 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

VirtuCrypt, Futurex's cloud HSM and key management platform, is an award-winning provider of enterprise-class cloud security services. VirtuCrypt provides cloud-based access to Futurex's innovative set of solutions for encryption, key management, tokenization, PKI & certificate authority, data protection, remote key loading for POS/ATM/IoT, and much more.

- 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

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

Google Workspace

Futurex Solution Details

- Support for Google Chrome
- 256-bit AES keys with monthly rotation
- FIPS 140-2 Level 3 validated HSM for highest possible security
- Deliverable as 2U network appliance for on-premises use, or via Futurex's VirtuCrypt cloud services

Futurex KMES Series 3 Enterprise

Futurex's natively-integrated HSMs offer streamlined deployment and high security, with no 3rd party relationship management needed.

Futurex VirtuCrypt Intelligenge Portal (VIP)

To learn more about Futurex's solution for Google Workspace Client-side encryption, or to inquire about a demo, visit [futurex.com]