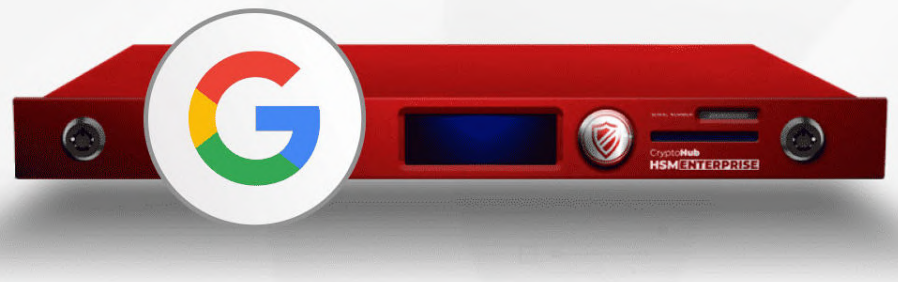


GOOGLE WORKSPACE CLIENT-SIDE ENCRYPTION

Futurex, in collaboration with Google, provides a secure client-side encryption (CSE) solution for Google Workspace. This solution allows enterprises to manage their encryption keys independently, safeguarding sensitive data while meeting compliance standards and data residency requirements.

Essential Features and Benefits

End-to-End Encryption Control

Client-Side Encryption (CSE): Encrypts data before it leaves the user's device, ensuring only you have the decryption keys.

Gmail and Meet Support: Extends robust protection to Gmail and Google Meet, alongside Drive, Docs, Sheets, and Slides.

Native Integration: Operates seamlessly through the Google Workspace web browser—no plugins required.

Simplified S/MIME Certificate Management

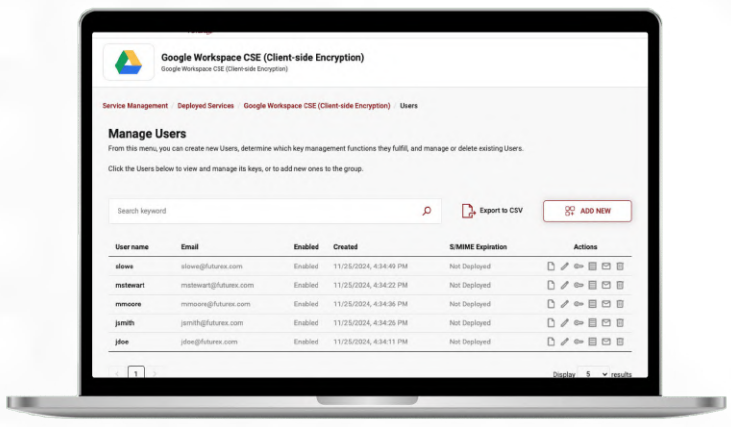
Integrated PKI Functionality: CryptoHub offers native HSM-backed PKI capabilities for Gmail's S/MIME certificates, eliminating the need to work with third-party certificate authorities (CAs).

Streamlined Setup: Enables S/MIME encryption for Gmail without additional tools, ensuring faster adoption and minimal disruption.

Quick and Easy Deployment

Rapid Admin Setup: Configure client-side encryption for your organization in less than a day using the Google Admin Console.

Customizable Policies: Apply encryption settings to specific organizational units to address unique security needs.



Industry-Leading Security

- **FIPS 140-2 Level 3 Validated HSMs:** Ensures the highest level of security for key management and encryption.
- **256-bit AES Encryption:** Delivers robust data protection with automatic monthly key rotation.
- **Flexible Deployment Options:** Available as a cloud-based or on-premises solution to meet infrastructure needs.

Why Choose Futurex For Google Workspace CSE?

Integrated Security Without Complexity:

Futurex's CryptoHub combines HSM-backed encryption and PKI functionality into a single, streamlined solution. This eliminates the need for multiple vendors, simplifies workflows, and accelerates deployment while ensuring your data is secure.

Legislative Compliance and Data Residency

Compliance: Meets strict legislative requirements for data protection, including:

- General Data Protection Regulation (GDPR)
- California Consumer Privacy Act (CCPA)
- Health Insurance Portability and Accountability Act (HIPAA)

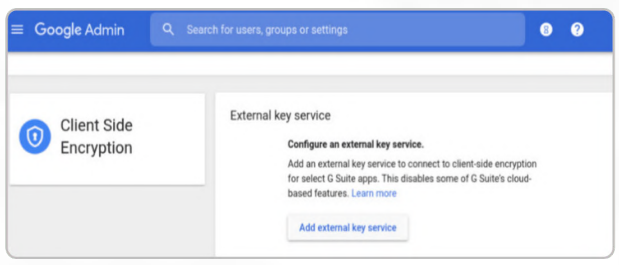
Data Residency: Addresses regulations requiring geographically specific data storage and encryption.

- Data Sovereignty
- Schrems II Ruling Compliance
- Multi-Region Support

Executive Summary

Futurex's Google Workspace Client-Side Encryption (CSE) provides a seamless and powerful solution for securing sensitive data across Gmail, Meet, Drive, Docs, and more. With browser-based deployment and rapid setup, administrators can implement CSE across their organization in under a day.

Google Workspace



How It Works

1. Log into the Google Workspace Admin Console.
2. Add Futurex as your external key service (KACLS).
3. Configure encryption policies for Gmail, Meet, Drive, Docs, Sheets, and Slides.
4. Users can start encrypting their data immediately—no additional software or plugins required.

FUTUREX

For over 40 years, Futurex has been an award-winning leader and innovator in the encryption market, delivering uncompromising enterprise-grade data security solutions. Over 15,000 organizations worldwide trust Futurex to provide groundbreaking hardware security modules, key management servers, and cloud HSM solutions.

Futurex is headquartered outside of San Antonio, Texas, with regional offices worldwide and over a dozen data centers across five continents, and delivers unmatched support for its clients' mission-critical data encryption and key management requirements.

FUTUREX.COM

864 Old Boerne Road,

Bulverde, Texas 78163