DATASHEET

Sectigo's Google Workspace Certificate Connector

Enterprises of all sizes are turning to Google Workspace for their comprehensive business support solutions, with Gmail at its center. While Gmail has some built in security capabilities, Security experts will agree that a secure enterprise should be encrypting and signing all emails using S/MIME Certificates.

Google Workspace Enterprise tier includes the capability to activate S/MIME for users, which allows IT Managers to have greater control of email security, providing protection for corporate and user data. Users can encrypt their email content and use certificate-based signatures to assure the senders identity. Using Sectigo Certificate Manager (SCM) enterprises can define policies for certificate creation and manage the certificate lifecycle from request to revocation or renewal. With the Sectigo Google Workplace Certificate Connector, IT Managers can easily deploy certificates directly to their Workspace instance, thus activating hosted S/MIME capabilities for email.

To use Google's hosted S/MIME offering, an IT Manager would enable it in the Google Admin console. The S/MIME certificates are configured and issued via Sectigo Certificate Manager and can then be installed in Google Workspace using the Sectigo Google Workspace Certificate Connector.

This solution provides a seamless workflow for creating certificates in SCM and activating users secure email via Google Workspace.

S/MIME (Secure/Multipurpose Internet Mail Extension) certificates ensure email security, confidentiality, and integrity. Leveraging numerous sophisticated security features, S/MIME email certificates give users the confidence to trust their digital correspondence and avoid many of today's attacks on enterprise email users and infrastructure.

Benefits:

- Enterprises can issue certificates for all users and easily upload them to Google Workspace
- Certificates can be managed by SCM (reissued, revoked, renewed) enabling greater control of secure email in the enterprise
- SCM can store certificates securely in the cloud, ensuring recoverability in case of loss
- S/MIME certificates can be included in an enterprise-wide certificate lifecycle strategy with SCM and Sectigo providing manageability and expertise at every level
- Users can exchange email securely with increased confidence in sender credentials and data integrity

Sectigo's Google Workspace Certificate Connector is another in a series of powerful integration tools that enable enterprises to deploy Sectigo Certificate Manager as an enterprise-wide Certificate Lifecycle Management solution, enabling enterprises to communicate and transact business securely.

For more information on Sectigo's Google Workspace Certificate Connector, S/MIME certificates or certificate management in general please reach out to Sectigo Sales at sales@sectigo.com.

About Sectigo

Sectigo is a leading provider of digital certificates and automated certificate lifecycle management solutions to leading brands globally. As one of the longest-standing and largest Certificate Authorities (CA), Sectigo has over 20 years of experience delivering innovative security solutions to over 700,000 businesses worldwide. Sectigo is the leading certificate lifecycle management provider supporting multiple CA vendors and integrating with the largest software ecosystems in the world.

For more information, visit www.sectigo.com and follow @SectigoHQ.