



SecureAuth integrates Google Apps into a 2-Factor SSO solution for the enterprise:

Easier on the end-user

- User Self-Provisioning for 2-Factor authentication
- No tokens
- Single Sign-On to hosted applications

Less expensive

- A fraction of the cost of hard tokens
- No Password to synch

Enterprise Friendly

- Users stored/managed from local directory
- SecureAuth can also provision users.
- User Password Reset
- User Profile Management
- FFIEC, HIPPA, PCI compliant

SecureAuth provides an authentication solution that enables enterprises to retain control and use of their own data store.

SecureAuth® allows enterprises to integrate Google Apps applications, including, Gmail, securely into an enterprise's framework of applications and services.

By using your existing user data store to validate user credentials, SecureAuth avoids replication of sensitive user data outside the enterprise, while maintaining control inside of it. An enterprise is able to take full advantage of the benefits provided by a Google Apps hosted model, but keep the control and security benefits of having an "in-house" hosted application.

Google® has offered enterprises a unique opportunity to reduce IT cost via hosted applications such as messaging, calendaring and document sharing.

SecureAuth Advantages for End-Users:

- Nothing for end-users to Carry
- Securely access from anywhere, including Kiosks or public computers
- Flexible authentication: SMS, Telephony, E-mail, PIN, Certificate
- Single Sign-on between Google Apps and hosted applications

SecureAuth Advantages for Enterprises:

- (1) Uses existing User Data Store, no syncing
- No credential to ship/manage
- More secure than tokens and other solutions
- No end-user training
- Help facility to manage users

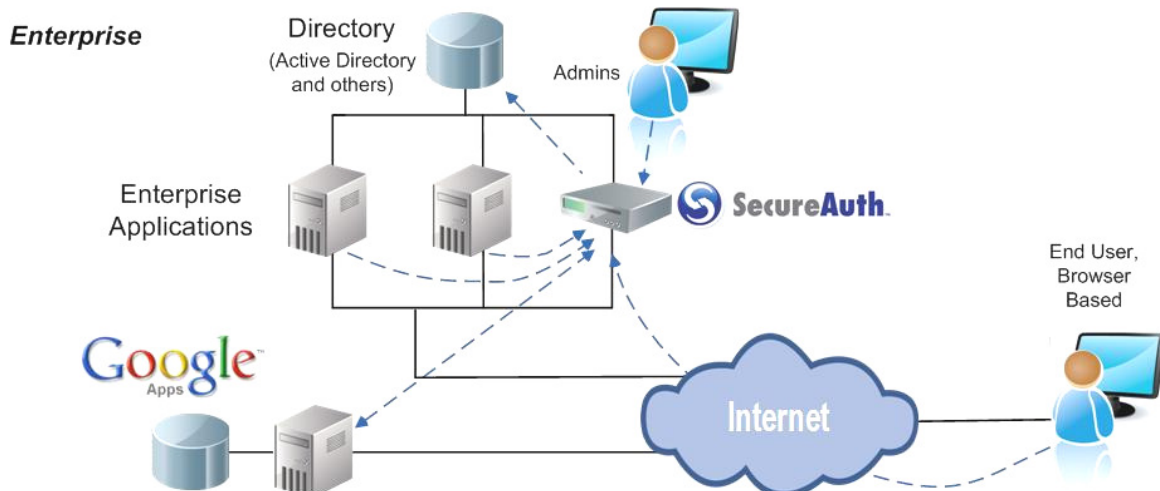


Figure #1: SecureAuth makes Google Apps part of the enterprise application infrastructure.