

MultiFactor SecureAuth® for Google Apps Authentication

SecureAuth® makes Google Apps a secure extension of your enterprise IT environment.

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. An enterprise is able to take full advantage of the benefits of Google Apps hosted model while keeping the control and security benefits of having the applications “in-house”.

Google® has offered enterprises a unique opportunity to reduce the IT cost via the offering of hosted applications, such as messaging, calendaring and document sharing. As with any hosted service, Google Apps introduces a new set of responsibilities associated with a secure establishment of identity to hosted applications.

Google Apps, combined with SecureAuth integrated at the enterprise, is the solution to these security concerns. SecureAuth integrates with the enterprise native directory and then post a secure SAML assertion to Google Apps. (See Diagram #1)

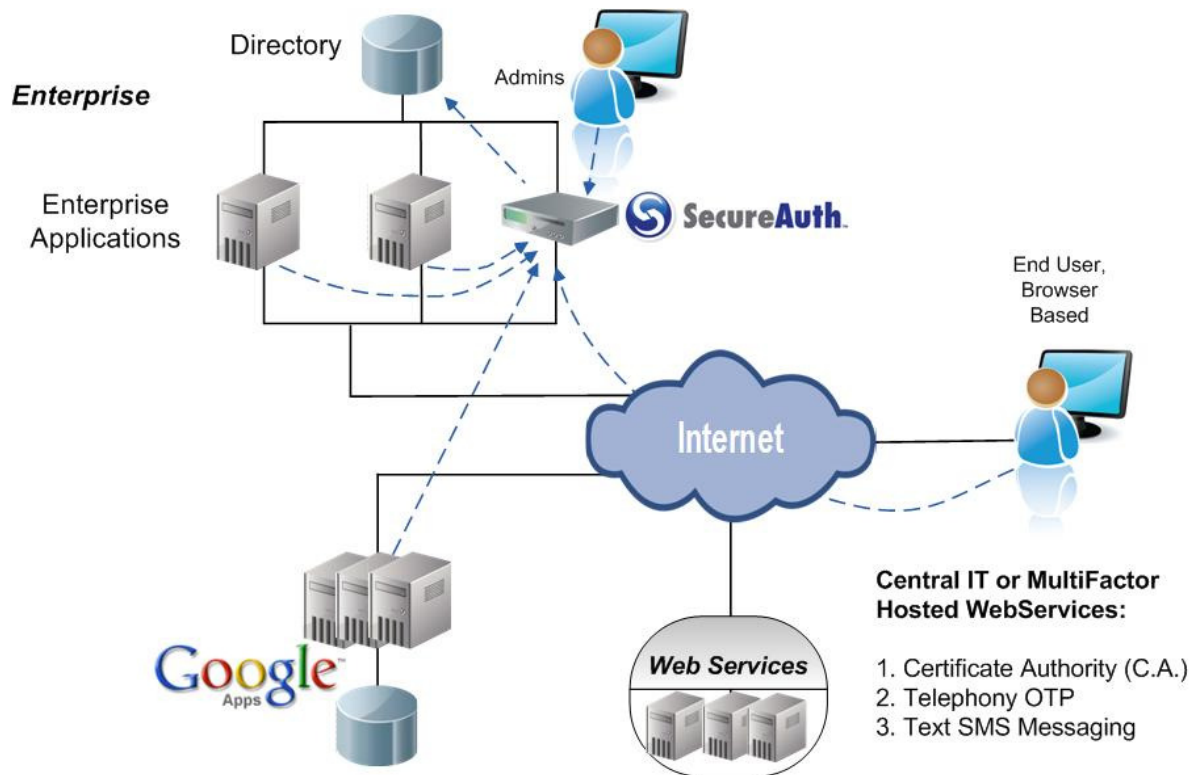


Diagram #1 – MultiFactor SecureAuth Integrates with Enterprise Directory for Google Apps Authentication

SecureAuth® Secures Google Apps® for the Enterprise

Google provides the ABILITY for enterprises to keep their own user credentials and to implement their own authentication – but the choice of the authentication tool – is up to the enterprise.

This makes the decision for the enterprise a little more complicated. Not only does the enterprise have to find an authentication solution that:

Solves the issues resulting in Web Authentication, including:

- Phishing/Pharming
- KeyLogger
- DNS Attacks
- Man-in-the-Middle Attacks

The enterprise must also find a solution that works in Google’s SAML 2.0 authentication model – that is where the authentication solution:

- Can be exposed to Google Apps as a URL (See Diagram #2)
- Can create a SAML 2.0 assertion for Google Apps to accept (See Diagram #1)

SecureAuth® for Google Apps is this solution.

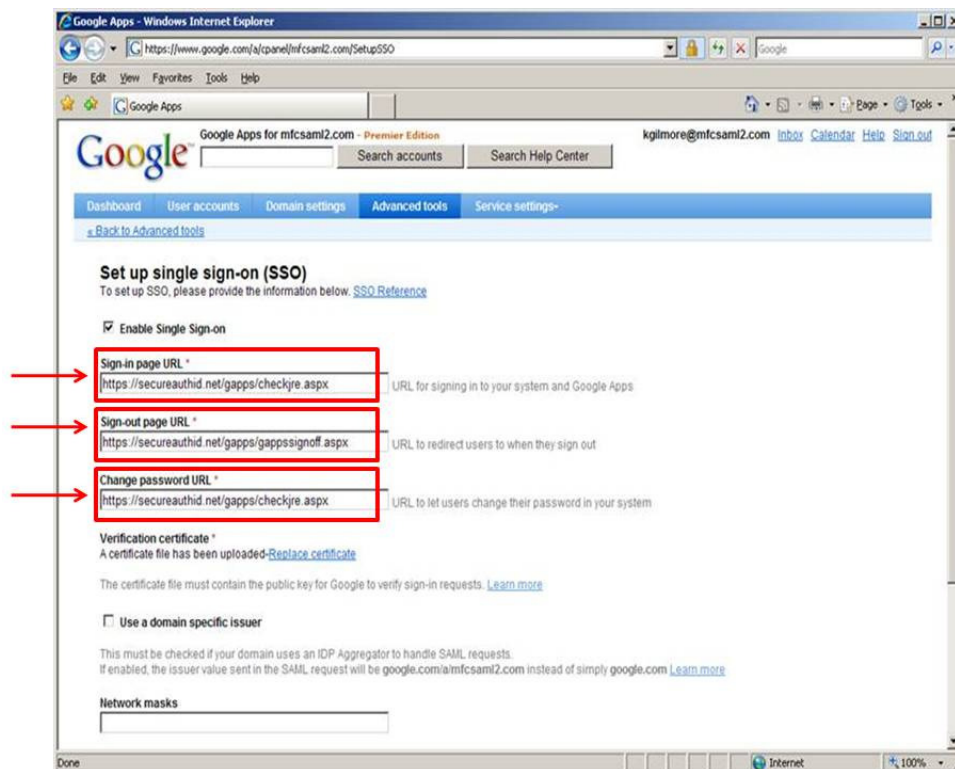


Diagram #2: Configuring Google Apps to Utilize SecureAuth® for Authentication



SecureAuth® provides the enterprise a solution that:

1. Is “Exposed” to Google Apps via a public URL
2. Can create the session ticket need, post authentication to Google Apps
3. Connects to the enterprise’s native user store

This last item is key. Because SecureAuth® connects to the enterprise user store the enterprise has the ability to retain identities “in-house” – and thus put in all the necessary administrative tools and practices in place to meet the relevant regulations (PCI DSS, GLB, FFIEC, etc.) In short, the enterprise keeps the user’s data in place – under “lock and key” – as if the application was in-house.

This is truly the beauty of the federation model and how SecureAuth® integrates. Regulations are pretty much determining that enterprises not only maintain user accounts – but also put in extensive practices to insure their safe keeping. The application itself can be hosted at another site – as long as the enterprise can prove:

1. The identity credential is securely stored
2. The session for the authentication/authorization is secured

Summary:

SecureAuth is the superior 2-Factor authentication solution for Google Apps. SecureAuth integrates with the native directory for the enterprise and then securely transfers a trusted assertion to the Google Apps application. The SecureAuth solution provides seamless SSO to the rest of the enterprise applications as well as secure mechanism for user and help desk identity management.