onelogin

WHITEPAPER

Top 13 Ways to Strengthen Google Apps Security and Compliance

www.onelogin.com • 150 Spear Street, Suite 1400, San Francisco, CA 94015 • 855.426.7227

Executive Summary

As a collaboration suite, Google Apps contains some of the most sensitive business data of any IT system. Everything from emails, contracts, product designs, customer lists and more can be accessed from anywhere. To avoid security issues, Google Apps administrators must take the proper steps to secure their data.

Seven key security customizations are available to domain administrators within Google Apps. These fall largely into two categories: those native to Google Apps and those open to Google Apps Marketplace apps and beyond. Customizations in the first category - such as Google Apps data encryption, secure mail transfer, and archived search - offer clear and direct benefits to the business. Those in the second category - like 2-factor authentication, single sign-on, and security policies - are more challenging to incorporate without first centralizing access control through identity and access management (IAM).

> Google Apps is unlikely to be the only cloud-based solution used by your business, so its important to apply consistent security policies across your entire cloud application porfolio.

By adopting a cloud-based IAM solution such as OneLogin, manual sign-ins on an app-by-app basis become a thing of the past. Centralized authentication through OneLogin enables users to automatically gain access to applications using a secure single sign-on protocol such as SAML. As a result, IT staff can enforce the same access policies across all applications (not just apps in the Google Apps Marketplace), and record a complete audit trail of all authentication and sign-in activity.

Giving IT centralized control and a solid body of security and administrative options beyond what's available within Google Apps increases cloud app security and compliance, and at the same time boosts productivity across both end users and IT. IT administrators can quickly integrate with existing user stores like Active Directory, provision and deprovision applications, and provide users with a seamless single sign-on experiene across desktops, laptops and mobile. End users enjoy one click access to all their apps and IT isn't burdened with the dreaded influx of helpdesk tickets for passwords resets. Everyone wins.

Seven Key Google Apps Security Customizations

Securing the sensitive data contained inside Google Apps is of paramount importance to every Google Apps administrator. These first three Google Apps customizations are native to Google Apps and can be effectively enabled with or without an identity and access management system like OneLogin.

1. Secure Browser Connections (HTTPS)

Google Apps for Business and Google Apps for Education offer domain administrators the ability to force all users in their domain to use Hypertext Transfer Protocol Secure (HTTPS) for services such as Gmail, Docs, Calendar, Sites, etc. Information sent via HTTPS is encrypted from the time it leaves the Google app until it is received by the recipient's computer.

Learn More in the Following Google Support Articles

Setting Up SSL Connections
Setting Up SSL on Custom Domains

2. Policy-enforced Secure Mail Transfer (TLS for SMTP)

With policy-enforced Transfer Layer Security (TLS) for Simple Mail Transfer Protocol (SMTP), administrators can set up policies designed to support the secure sending and receiving of email between specific domains. For example, you could specify that all external mail sent by accounting team members to the company's bank must be secured with TLS, or deferred if TLS is not possible. Similarly, you could mandate a secure TLS connection between the company's domain and outside legal counsel, auditors, or other third parties with which employees may exchange sensitive communications.

Learn More in the Following Google Support Articles

How Policy Enforced TLS Works
Setting up TLS
Setting up Outbound TLS

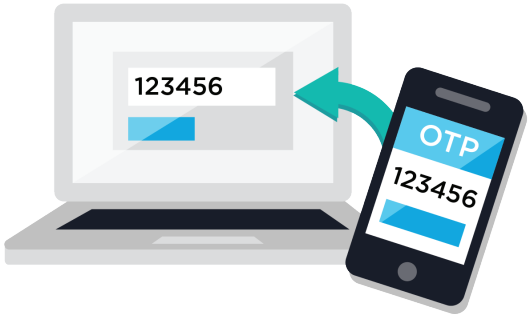
3. Archive Search

By implementing Google Message Discovery, powered by Postini, organizations can create a centralized email repository that enables searching across the archive to locate and export specific messages in support of compliance and eDiscovery requirements. Message Discovery saves and indexes all messages based on customer-defined retention policies, allowing the organization to identify, retain, search, and export relevant messages to share as required with third parties.

Learn More in These Google Support Articles

Setting Up Archive Search
If You're Integrated With Postini, You Might Want to Read This Complete Guide on Message Discovery

The following four Google Apps customizations deliver the best results when deployed within the context of an Identity and Access Management solution like OneLogin, which we explain below in the six ways to strengthen app security and compliance even further with OneLogin.



4. Two-Step Verification

Google Apps includes a two-factor authentication capability called "2–step verification" which can greatly reduce the likelihood of a user account becoming compromised, helping to prevent unauthorized account logins. Two-step verification requires two independent factors for authentication: your password, plus a one-time use code delivered to your cellphone. This additional code is generated on the user's smartphone (iPhone, BlackBerry, or Android device) via an app, or via SMS text message or voice call. All the server-side components are fully integrated into Google Apps.

Learn More in the Following Google Support Articles

2-Step for End-Users
How 2-Step Works

5. Single Sign-On (SSO)

Google Apps offers a Single Sign–On (SSO) service to customers with Google Apps for Business, Google Apps for Education, and Google Apps for ISPs. Google Apps has a SAML–based SSO API that organizations can integrate into their LDAP, or other SSO system and use the authentication mechanism of their choice - certificates, hardware tokens, biometrics, etc.

Learn More in These Google Support Articles

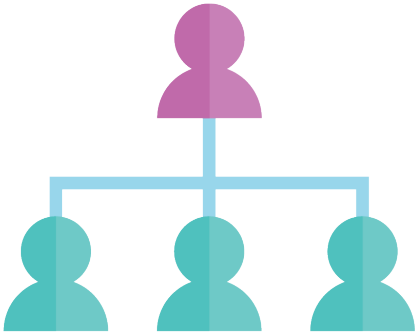
SAML Single Sign-On (SSO) Service for Google Apps
Setting Up SAML for Google Apps with OneLogin

6. Password Length and Strength

Organizations can set password length requirements for their domain users and review password strength indicators to help identify passwords that may meet the length requirement but still not be strong enough. The password strength indicators work in real-time and help administrators to spot passwords that may become less secure over time based on emerging patterns of attack.

Learn More in These Google Support Articles

Managing Passwords in Google Apps
Password Management in OneLogin



7. Administrator–based Single Sign-Out

Administrators can reset users' sign-in cookies to help prevent unauthorized access to their accounts. The process logs that user out of all current browser sessions and requires new authentication the next time that user attempts to access Google Apps. When combined with the base ability for administrators to reset user passwords, this option improves security for cloud apps in case of device theft or loss.

Six Ways to Strengthen App Security & Compliance Even Further with OneLogin

1. Two-factor options and policies that work across all apps, resources and users

Google Authenticator is great for authenticating into Google Apps as well as other apps that integrate with Google Authenticator, but most enterprises will have non-Google applications and other resources that need to be protected. These might include custom web apps, legacy applications, Microsoft access servers and gateways, VPNs, and Unix systems with remote (SSH) or local logins.

The problem with enforcing 2-factor authentication at the application level is that users quickly get annoyed with it. Even if you are using only Google Apps, Dropbox, and Evernote for work, you'll need to use 2-factor authentication three times just to access your apps - and if your session times out, you have to go through the whole process again. The more apps you use, the more annoyed users are going to get.

Additionally, when employees log into an app directly, the business has no control over or record of that access, introducing a potential compliance problem - 2-factor authentication at the application level does not provide the governance and access control over corporate data required for compliance audit trails. With OneLogin, the business can centralize access control and enforce the authentication of all users following the terms of corporate mandated policies.

Centralized IAM also provides choice and flexibility for both end users and IT: IT can, for example, enable or enforce different 2-factor options for different types of users, at the same time giving end users the option to toggle between those options.

2. Leverage existing Active Directory and/or LDAP security models

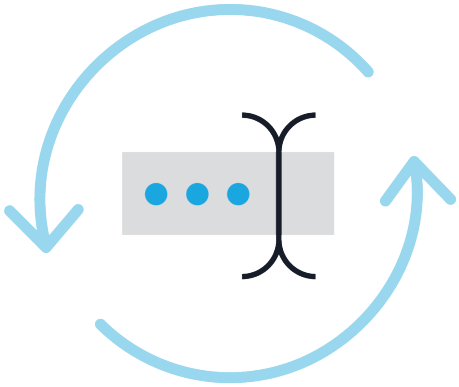
With OneLogin, users' status and roles in the on-premise directory are updated in real-time; creating, updating and suspending of privileges takes effect in OneLogin and connected services immediately. This removes the need to update multiple access lists or wait for a batch program to be completed, closing potential security gaps. This real-time synchronization streamlines administration and provides IT with an effective "kill switch" for users whose access need to be removed immediately. This becomes critical when services such as Google Apps allow back-door access through protocols like IMAP.

By establishing or mapping your existing Active Directory roles and groups to OneLogin, you can quickly grant, modify, or remove access using role-based privileges that are as granular as you want to make them. For example, a business might assign all finance personnel the "Finance" role and also assign the "Equity Accountant" role to two of them to enable them to access the stock options application. If you disable the directory account for one of those two Equity Accountants, the update is made immediately in OneLogin, which then secures access to all applications managed through the IAM portal.

3. Reduce the risk of phishing and spear phishing

The most effective way to protect your organization against phishing is to eliminate what the criminals are targeting: passwords. The SAML single sign-on standard supported by most leading cloud applications uses digital signatures to establish trust between the identity provider and the application, obviating the need for passwords. As a result, users need to remember only one set of credentials – those for the single sign-on portal - which also becomes the single, familiar place they go to to access their applications.

For those apps that don't support a standard like SAML, you can use OneLogin's Password Vaulting, which enables you to securely share logins for those applications -which might include Twitter, FedEx, or SurveyMonkey - without disclosing the password. End users can't be phished because they don't know what the underlying passwords are, and authorized access is simplicity itself: they simply click on an icon in the OneLogin portal to be authenticated directly into the app.

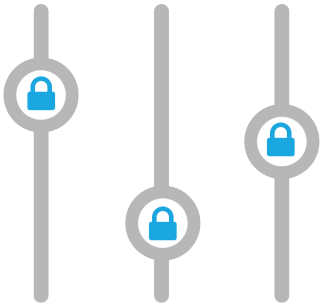


4. Enforce company-wide password policies, synchronize passwords, and force resets

OneLogin makes it easy to enforce company-wide password policies for password strength, expiration, and reuse. Most companies require regular password changes, but managing those changes can be an error-prone and time-consuming task.

When your organization systematically changes passwords for Active Directory, it's important that these changes extend to your single sign-on portal and web apps. OneLogin provides a frictionless way to synchronize password changes across Active Directory, your OneLogin portal, and those web applications secured with OneLogin.

By the same token, administrators can force password resets on individuals or groups of users. Remember the Heartbleed security vulnerability? Many IT admins needed to force a password change for all users, but there was no easy way to achieve this through Google Apps.



5. Flexible administrative controls increase security and compliance

In terms of administrative access enforcement, OneLogin administrators can restrict access to target applications based on IP addresses, set session time-outs, create or require additional authentication from unknown browsers and access from outside the corporate network -- all of which can be assigned on a per-user, per-group, or global basis.

OneLogin also gives administrators the ability to separate Google App administration from user management. For example, administrators can assign security policies to specific users independent of granting them access to their apps. Role-based access to applications can be combined with notifications to alert an administrator to a segregation of duties violation, which occurs when an individual should not have access to sets of apps that have been segregated by roles, as defined by the administrator.

6. Hassle-free compliance reporting and detective controls

OneLogin provides a range of reports that can help you actively or periodically monitor what your users are doing in the OneLogin portal and, by extension, the apps being managed by OneLogin. For example, the quarterly OneLogin roles report review helps to identify a user with access to an additional application that should have been removed the previous month. After updating this user's access, you can review the logs to confirm that they did not access the application during that time.

If you work for a public company, you know that Sarbanes-Oxley compliance auditors will request a lot of documentation, including several access control lists as well as evidence that access was granted appropriately for those in scope. Instead of chasing down multiple access lists or trying to prove that the list of new users is complete and accurate, you will greatly reduce the level of effort and documentation needed for a SOX audit if you are using OneLogin as your central point of access management and authentication. For example, you can provide auditors with a OneLogin portal log showing the users added to it during the audit period for their access testing population, along with OneLogin's list of active and disabled users for their testing evidence.

By combining an IAM solution like OneLogin with the built-in security measures of the apps themselves, it is possible to create a user-friendly, yet secure environment that meets compliance requirements and protects data, applications, and the business itself.

ABOUT ONELOGIN

OneLogin is the innovator in enterprise identity management and provides the industry's fastest, easiest and most secure solution for managing internal and external users across all devices and applications.

The only Challenger in Gartner's IDaaS MQ, considered a "Major Player" in IAM by IDC, and Ranked #1 in Network World Magazine's review of SSO tools, OneLogin's cloud identity management platform provides secure single sign-on, multi-factor authentication, integration with common directory infrastructures such as Active Directory and LDAP, user provisioning and more. OneLogin is SAML-enabled and pre-integrated with thousands of applications commonly used by today's enterprises, including Microsoft Office 365, Asure Software, BMC Remedyforce, Coupa, Box, Clarizen, DocuSign, Dropbox, Egnyte, EMC Syncplicity, EchoSign, Google Apps, Jive, Innotas, LotusLive, NetSuite, Oracle CRM On-Demand, Parature, Salesforce.com, SuccessFactors, WebEx, Workday, Yammer, ServiceNow, Zscaler and Zendesk. OneLogin, Inc. is backed by CRV and The Social+Capital Partnership.

onelogin

www.onelogin.com | 150 Spear Street, Suite 1400, San Francisco, CA 94105 | 855.426.7227