INTRODUCING

Google Identity Services for work

Online safety made easy

We all care about keeping our data safe and private. Google Identity brings a new level of intelligence to make security effortless.

Introduction

Millions of businesses and schools rely on Google Apps identity services (IDaaS) every day when they sign in to Google products like Google Drive and Gmail. Google Apps for Work offers core identity services across all editions that make it simple, secure and reliable for users to log in and for administrators to manage usage across the organization. These core features fall into six main areas, where we focus.

- **Single sign-on (SSO)**
- **Provisioning**
- **Directory administration**

- **Multi-factor authentication**
- **Reporting and Analytics**
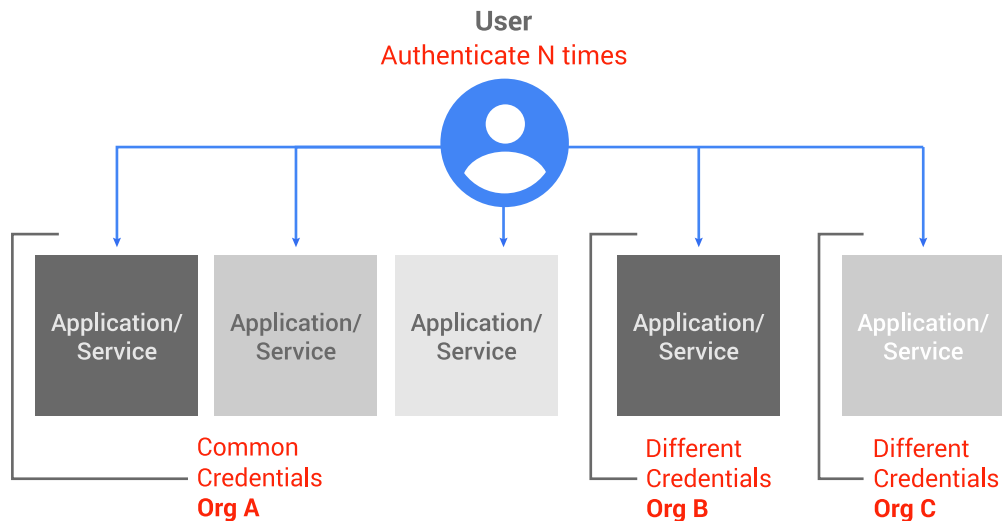- **Endpoint management**

SSO

Provisioning

Endpoint Management

Google Identity

Directory Administration

Reporting & Analytics

Multi-factor Authentication
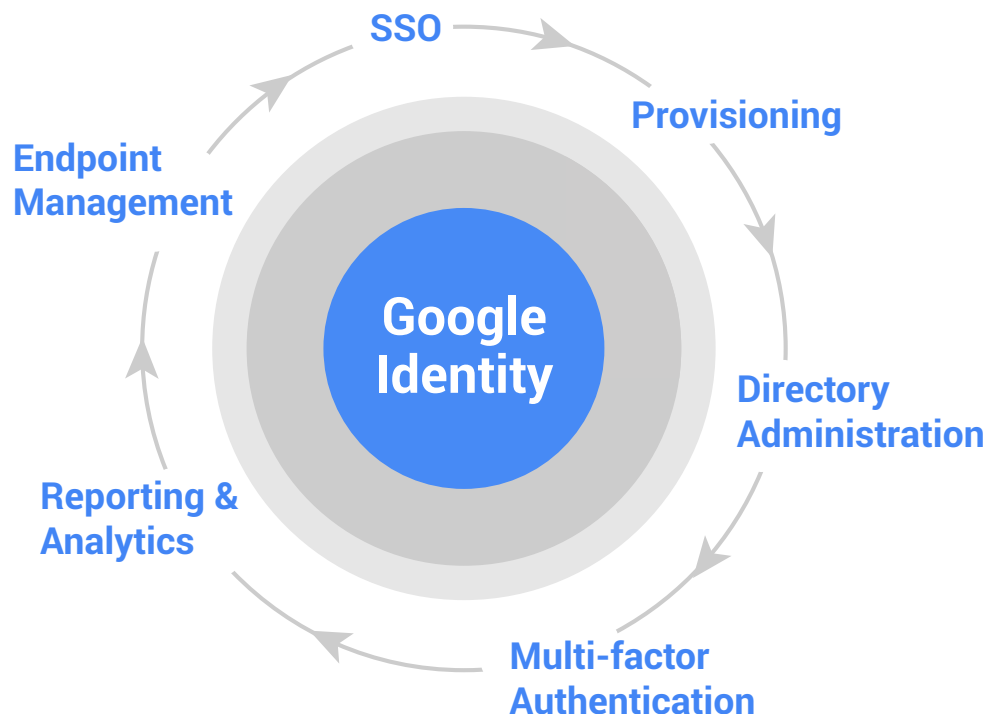
"Google came through for us big time. Google App SAML support is making our Canvas authentication completely seamless for students and staff."

-Tim White, Director of IT, Webb City R-VII School District

Single sign-on (SSO)

Google Apps provides customers a single sign-on service (SSO) that enables their users to leverage Google's strong authentication to access multiple apps using the same credentials. Google Apps currently supports over 1,000 SAML 2.0 and OpenID Connect (OIDC) apps in addition to custom apps that use Google as an identity provider. Users can discover and connect apps through the Google Apps Marketplace (GAM) and administrators can manually connect apps from the Google Apps Admin console.

User
Authenticate N times

Application/ Service   Application/ Service   Application/ Service   Application/ Service   Application/ Service

Common Credentials **Org A**   Different Credentials **Org B**   Different Credentials **Org C**

SSO Security (SAML 2.0)

Google Apps SSO is based on SAML 2.0, an XML standard that allows secure web domains to exchange user authentication and authorization data. For additional security, SSO accepts public keys and certificates generated with either the RSA or DSA algorithm.

OAuth 2.0 and OpenID Connect (OIDC)

Google Apps supports OAuth 2.0 and OIDC, an open protocol for authentication and authorization. This allows customers to configure one SSO for multiple cloud solutions. Users can log on to third-party applications through Google Apps without re-entering their credentials or sharing sensitive password information.

"Google Apps identity services has made single sign-on to services we use every day like Salesforce and Zendesk much easier for end users, who save an hour per month, for our support team, which has seen a 25% reduction in support tickets, and for our IT team, which has experienced 20% time savings."

- Vadim Solovey, Founder & CTO, DoIT International

Provisioning

Users are the core of any identity platform and easily creating those users is important for administrators. Google Apps for Work makes user creation and provisioning easy with the unified Google Apps Admin console and APIs. Organizations moving from Active Directory can use Google Apps Directory Services (GADS) to migrate or sync data. Once a user is provisioned, user details automatically flow throughout Google Apps and are available to third-party apps or custom apps that need user attributes.

For more advanced needs, third-party solutions like Ping Identity can add additional federation and integration into existing cloud or on premise services.

Directory Administration

The Google Apps Admin console makes it easy to manage users. Everything from setting permissions to resetting passwords is in one location so administrators can quickly complete common tasks. Individual Google services and third-party services can be enabled at an individual or organizational unit level. This makes it easy to manage unique app permissions for different departments, like marketing and finance.

For advanced needs, Google's Apps' identity directory provides a user management API to create, retrieve, update and delete users. The user object is extensible and the Admin console/API provides rich search on various core and extensible user attributes so administrators can add and find details that are unique to their needs.

"Google provides business-critical solutions like serving as the central secure access point for cloud apps, while also providing infrastructure for these services like the identity directory. I trust Google to play this foundational role, but wouldn't expect it to meet unique needs that fall between the directory and the login. This is where best-of-breed partners like Ping come in to help us solve complex challenges unique to our business."

-Justin Slaten, Manager, Enterprise Technology & Client Systems at Netflix

Multi-factor Authentication

Google builds security into our structure, technology, operations and approach to customer data. Our robust security infrastructure and systems become the default for each and every Google Apps customer. And beyond these measures, users are actively empowered to enhance and customize their individual security settings to meet their business needs through dashboards and account security wizards. Google Apps also offers administrators full control to configure infrastructure, applications and system integrations in a single dashboard via our Admin console — regardless of the size of the organization. This approach simplifies administration and configuration.

2-step verification

2-step verification adds an extra layer of security to Google Apps accounts by requiring users to enter a verification code in addition to their username and password when they sign in. This can greatly reduce the risk of unauthorized access if a user's password is compromised. Verification codes are delivered on a one-time basis to a user's Android, BlackBerry, iPhone, or other mobile phone. Administrators can choose to turn on 2-step verification for their domain at any time.

Security Key

Security Key is an enhancement for 2-step verification. Google, working with the FIDO Alliance standards organization, developed the Security Key — an actual physical key used to access your Google Account. It sends an encrypted signature rather than a code and helps ensure that your login cannot be phished. Google for Work administrators can easily deploy, monitor and manage the Security Key at scale with new controls in the Admin console with no additional software to install. IT administrators can see where and when employees last used their keys with usage tracking and reports. If Security Keys are lost, administrators can easily revoke access to those keys and provide backup codes so employees can still sign-in and get work done.

Risk-based account profiling

To make accounts even more secure, Google provides additional risk-based account profiling. On detection of suspicious login attempts, a variety of login challenges will be presented automatically, while separately alerting users to the suspicious activity.

Smart Lock

Google is continually advancing security along multiple dimensions and recently introduced Google Smart Lock, a feature which can help employees manage their passwords and protect their devices. Smart Lock is even able to distinguish between passwords for work accounts and personal accounts on personal devices.

Reporting and Analytics

Google Apps administrators have access to security reports that provide vital information on their organization's exposure to data compromise. They can quickly discover which particular users pose security risks by eschewing 2-step verification, installing external apps, or sharing documents indiscriminately. Administrators can also choose to receive alerts when suspicious login activity occurs, indicating a possible security threat.

Google Apps audit and reporting help administrators track important activities. Log-in activity for third-party apps is included so administrators have a complete picture in one place.

> "At ExtraHop, our mantra is 'Security in everything we do.' Enabling Google SAML was very straightforward and lets us effortlessly enforce our security policies, for example, implementing two-factor authentication for third-party SaaS services that don't support advanced security features."
>
> *-Bri Hatch, Director of IT at ExtraHop Networks*

Endpoint Management

Mobile device management (MDM)

Mobile device management in Google Apps eliminates the need for on-premises device or third-party management solutions. Administrators can enforce policies over mobile devices in their organization, encrypt data on devices and perform actions like remotely wiping or locking lost or stolen devices. This type of control helps ensure the security of business data, even if employees choose to work on their personal phones and tablets. MDM in Google Apps works with Android, iOS, Windows Phone and smartphones and tablets using Microsoft Exchange ActiveSync, such as BlackBerry 10

Policy-based Chrome browser security

All of the tools and features in Google Apps are best supported by Google Chrome. Administrators can apply security and usage policies across Windows, OSX, Linux, iOS and Android. Chrome's standard security features include Safe Browsing, sandboxing and managed updates that protect users from malicious sites, viruses, malware and phishing attacks. There are also measures in place to prevent cross-site scripting, which attackers can use to steal private data. Google Apps administrators can deploy Chrome for Work across their organization and customize it to meet their needs. Over 280 policies help administrators control how employees use Chrome across devices. For example, administrators can enable automatic updates to get the latest security fixes, block or allow specific apps and configure support for legacy browsers.

Chrome device management

The Google Apps Admin console applies policy to Chrome devices such as Chromebooks, Chromeboxes and Chromebox for meetings, which are fast, secure and cost-effective computers that run Chrome as an operating system. Administrators can easily manage security and other settings for their organization's Chrome devices from a single place. They can configure Chrome features for their users, set up access to VPNs and WiFi networks, pre-install apps and extensions, restrict sign-in to certain users and more.

FAQ's

What does Google's identity service cost to use?

Google's identity services are included in Google Apps for Work at no additional charge. Google Apps for Work starts at $5/user/month for the basic plan and offers a premium plan at $10/user/month that includes unlimited storage, advanced audit and reporting capabilities and Google Apps Vault for eDiscovery and retention.

How can I learn more about Google Apps security and compliance?

The Google for Work Security and Compliance Whitepaper describes how Google protects your data, meets regulatory and compliance needs, and empowers users and administrators.

Who owns the data I put into Google Apps?

To put it simply, the data that companies, schools and governments agencies put into our systems is theirs, whether it's corporate intellectual property, personal information or a homework assignment, Google does not own that data.

That means three key things:

1. We do not use your information for any other purpose than deliver you the service you pay for. There are no Ads in Google for Work.

2. You have control over your data. We provide you with tools to delete and export your data so that you can take your data with you at any time, use external services in conjunction with Google Apps or stop using our services altogether.

3. We protect your information from third-party requests and government access.

Learn more

Visit get.google.com/smartlock

If you are not already a Google Apps for Work customer, you can start a
free **30-day trial** to try all of the identity services.