Securing Access to Google Cloud

Welcome to module 2 of Managing Security in Google Cloud: **Securing Access to Google Cloud**.
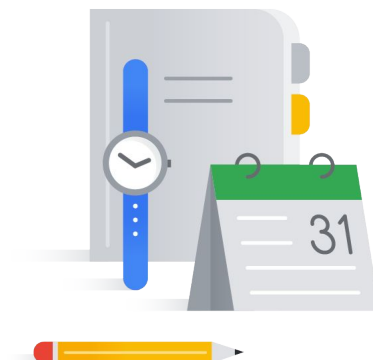
—

Module overview

Cloud Identity

Google Cloud Directory Sync

Managed Microsoft AD

Google authentication versus
SAML-based SSO

Identity Platform

Authentication best practices

Google Cloud

In this module, we will discuss Cloud Identity, a service which makes it easy to manage cloud users, devices, and apps from one console.

We will also discuss a few related features to help reduce the operational overhead of managing Google Cloud users, such as the Google Cloud Directory Sync, Managed Microsoft Active Directory, and Single Sign On.

We will also talk briefly about Identity Platform.

We will end with some authentication best practices.
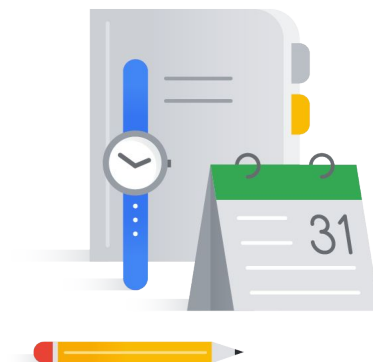
Securing Access to Google Cloud

Cloud Identity

Google Cloud Directory Sync

Managed Microsoft AD

Google authentication versus
SAML-based SSO

Identity Platform

Authentication best practices

Google Cloud

Let's get started with an outline of Google Cloud's approach to security.

High level overview - service comparison

| Service	What it is	Use cases
Cloud Identity	An identity provider (IdP) service that lets you create, manage, and delete identities for authentication purpose. It supports single sign-on, multi factor authentication and mobile device management.	• Cloud-based directory • Authenitcaiton (e.g. SSO) & Authorization • User Lifecycle Management • MFA & Endpoint management
Google Cloud Directory Sync	Synchronize the data in your Google Account with your Microsoft Active Directory or LDAP server.	• Syncs users, aliases, groups, and other data with your Google Account from LDAP of Microsoft AD
Managed Microsoft Active Directory	Extend Microsoft Active Directory on-premises service and configuration to your Google Cloud deployments	• Manage authentication and authorization for AD-dependent apps and servers • Automate AD server maintenance and security configuration
Identity Platform	Add identity and access management functionality to your applications	Customer identity and access management (CIAM) system used for: • Multi-tenant SaaS applications • Mobile and web apps • Games, APIs and more

Google Cloud

Before we dive into the specifics of Cloud Identity, let's take a moment to level set and give you high level view of the services that we'll cover in this module, as well as common uses cases.

- **Cloud Identity** helps you centrally manage identities and provides secure authentication and authorization to applications and devices.
  - Cloud Identity is commonly used as a cloud-based directory, Authenitcaiton (e.g. SSO), Authorization, User Lifecycle Management, Multi-factor authentication, and Endpoint management service.

- **Google Cloud Directory Sync** (or GCDS) lets you synchronize the data in your Google Account with your Microsoft Active Directory or LDAP server.
  - GCDS allows you to sync users, aliases, groups, and other data with your Google Account from LDAP of MS AD.

- **Managed Microsoft Active Directory**
  - Managed Microsoft Active Directory allows you to manage authentication and authorization for AD-dependent apps and servers, as well as Automate AD server maintenance and security configuration amongst other things.

- **Identity Platform** lets you add identity and access management functionality to your applications
  - Identity Platform is a Customer identity and access management

- (CIAM) system commonly used for: multi-tenant SaaS applications, mobile and web apps, games, APIs and more.

Cloud Identity

- An Identity as a Service (IDaaS) solution

- Used for managing users, groups, and domain-wide security settings from a central location

- Tied to a unique DNS domain that is enabled for receiving email

- Up to 600 domains can be associated with your organization's Google account

.com

.info

.edu

.net
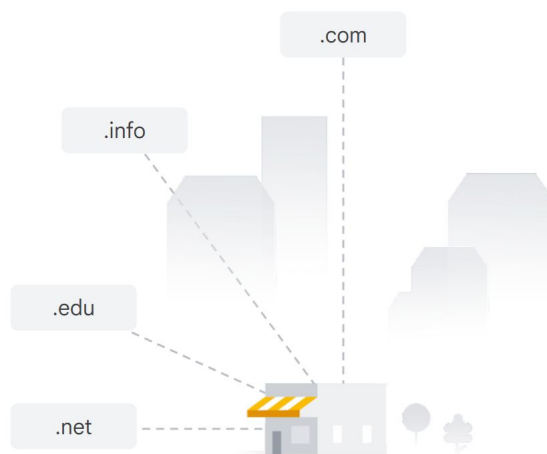
Google Cloud

Now that we have a good overview of the different services that will be discussed, let's dive into Cloud Identity.

Cloud Identity is an Identity as a Service (IDaaS) solution for managing who has appropriate access to your organization's cloud resources and services. It is currently used by hundreds of thousands of business customers to manage millions of users and devices.

Cloud Identity provides a single admin console so users, groups and domain-wide security settings can be managed for your entire organization from a central location.

Cloud Identity can work with any domain name that is able to receive email, so you can use your existing web and email addresses. Your organization **does not** need to use Google Workspace services in order to use Cloud Identity. When you migrate to Cloud Identity, you must verify that you own the domain name, and create an account for each of your users.
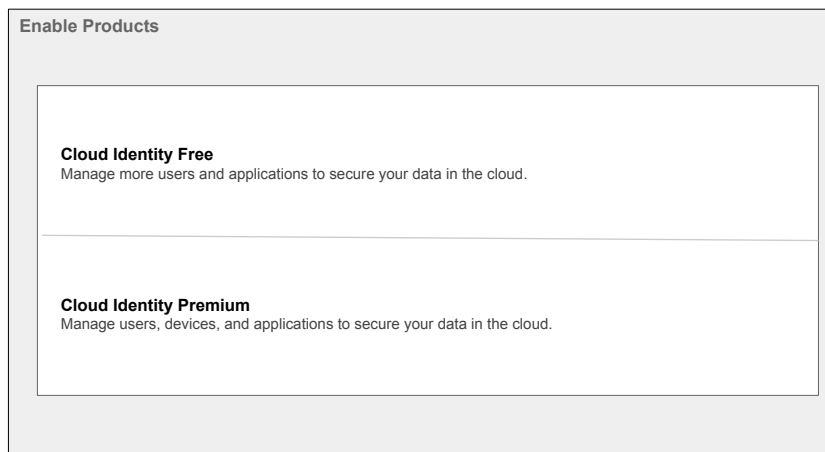
When you sign up for a Cloud Identity domain, the first domain name becomes the primary domain for your organization. Other domains can be added using the Admin Console. You must own each domain and verify your ownership when adding it.You can add up to 600 domains to your organization's Google account.

Cloud Identity
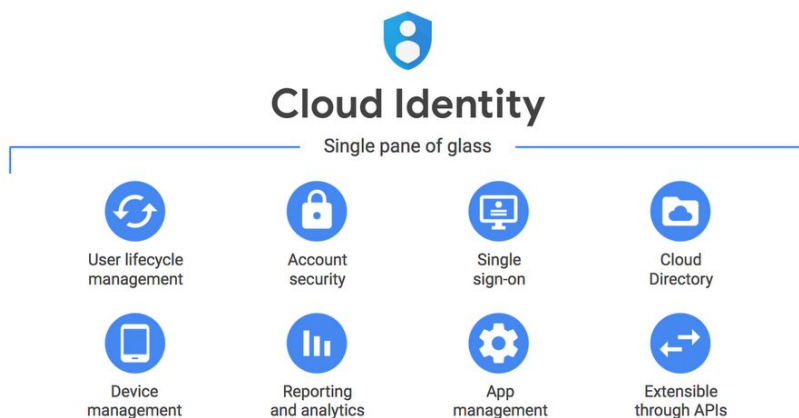
You can then manage all users from the Google Admin Console. The Admin Console provides a central management location or a "single pane of glass" to manage user identities and access permissions across your entire domain. This allows you to easily enforce security policies and roles.

Cloud Identity editions

Enable Products

Cloud Identity Free
Manage more users and applications to secure your data in the cloud.

Cloud Identity Premium
Manage users, devices, and applications to secure your data in the cloud.

Google Cloud

Cloud Identity is available in both free and premium editions. The Cloud Identity Free edition includes core identity and endpoint management services. It provides free, managed Google Accounts to users who don't need Google Workspace Services.

The Cloud Identity Premium edition offers enterprise security, application management, and device management services. These services include automated user provisioning, application allowlisting, and rules for automating mobile device management.

For more information, visit this link for a comparison of features offered by the free and premium editions of Cloud Identity.
- **Link:** support.google.com/cloudidentity/answer/7431902

Google Admin Console

admin.google.com

- Centralized console to manage users, groups, and security settings

---

- Cloud Identity allows free accounts to be created for each user

The Google Admin Console (admin.google.com) is the centralized console for managing users, groups, and security settings.

From the Admin Console, Cloud Identity allows free accounts to be created for users who do not need Google Workspace services. For existing Google Workspace customers the Admin Console provides additional functionality to configure their user's Google Workspace experiences.

Cloud Identity Uses

Cloud Identity can be:

- Used as a standalone service

- Combined with your Google Workspace services
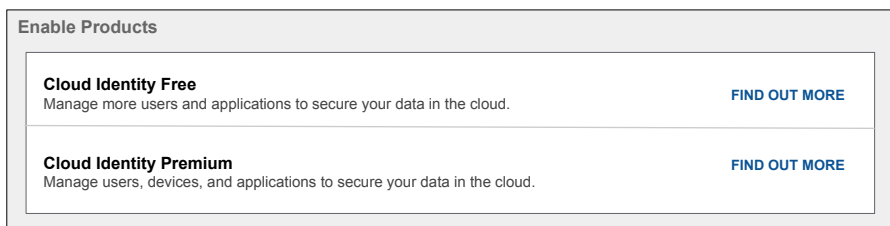
- Used to provision users manually
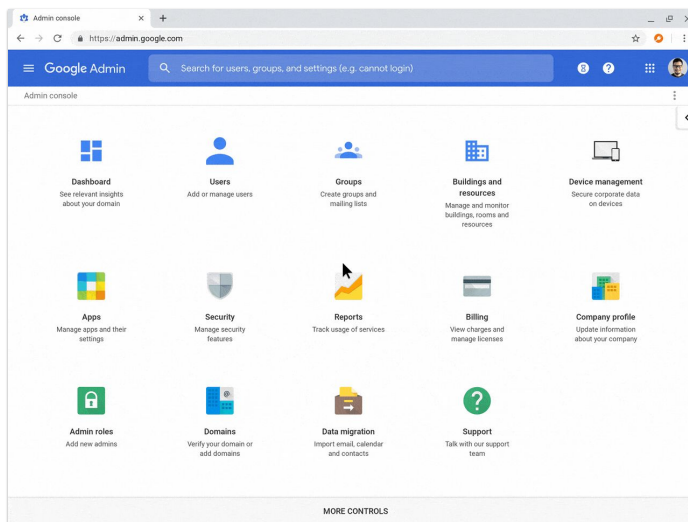
Google Cloud

Cloud Identity can be used as a standalone service for any domain that you own. It can also be combined with your existing Google Workspace subscriptions. In either case, you can manage all users across your entire domain from the Google Admin Console.

As mentioned earlier, the Google Admin Console allows admins to provision user accounts manually. The Google Admin Console allows you to upload individual accounts as well as batch enrollments from a spreadsheet.

As you can see, Cloud Identity provides you with a variety of options that allow you to securely manage users in your organization.

If you are a Google Workspace admin

- Sign up for Cloud Identity from the **Billing** section of the Google Admin console.

Enable Products

Cloud Identity Free
Manage more users and applications to secure your data in the cloud.   FIND OUT MORE

Cloud Identity Premium
Manage users, devices, and applications to secure your data in the cloud.   FIND OUT MORE

- You can create free Cloud Identity accounts for users who don't need Google Workspace.

Google Cloud

If you are a Google Workspace admin, sign up for Cloud Identity from the Billing section of the Google Admin Console.

Google Workspace licenses are required only for users who need Google Workspace services, such as Gmail, Google Drive, etc.

You can create free, non-licensed Cloud Identity accounts for managing users who do not need Google Workspace services.

Securing Access to Google Cloud
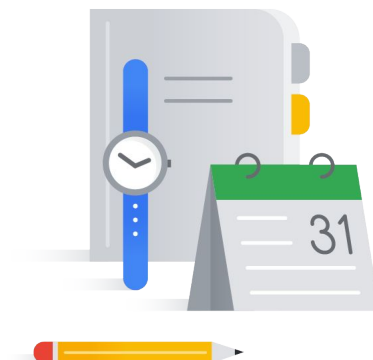
Cloud Identity

Google Cloud Directory Sync

Managed Microsoft AD

Google authentication versus
SAML-based SSO

Identity Platform

Authentication best practices

Google Cloud

As you have seen, Cloud Identity provides a central console to manage all users and groups across your entire domain. The Google Cloud Directory Sync can help simplify provisioning and deprovisioning user accounts.

What if you already have a different corporate directory?

On-prem directory as source of truth
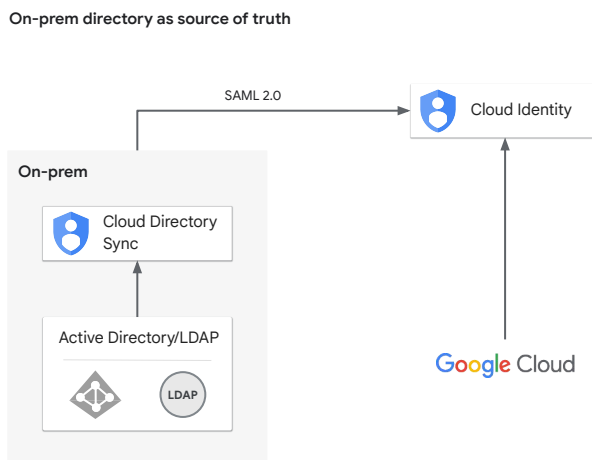
Most organizations already have a Microsoft Active Directory or LDAP service containing user and group information.

The Google Cloud Directory Sync tool can synchronizes Google Workspace accounts to match the data in an existing Active Directory or LDAP. Your Google users, groups, and shared contacts are synchronized to match the information in your Active Directory/LDAP server.

How Google Cloud Directory Sync works

1 Data is exported from your LDAP server or Active Directory.

2 GCDS connects to the Google domain and generates a list of Google users, groups, and shared contacts that you specify.

3 GCDS compares these lists and updates your Google domain to match the data.

4 When the synchronization is complete, a report is emailed.
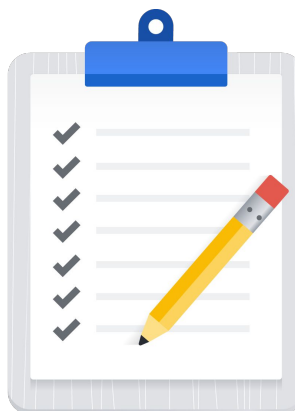
Google Cloud

As mentioned previously, GCDS allows you to synchronize the data in your Google Account with your Microsoft Active Directory or LDAP server.

The Google Cloud Directory Sync, or GCDS, process occurs in 4 steps.

First, data is exported as a list from your LDAP server or Active Directory. You set up rules to specify how and when this list is generated.

The GCDS then connects to your Google domain and generates a list of existing Google users, groups, and shared contacts that you specify.

GCDS compares the list exported from your Active Directory/LDAP with the generated Google users list and updates your Google domain to match the data.

When the synchronization is complete, a report is emailed to the addresses that you specified when configuring GCDS.

GCDS allows for one-way synchronization

One-way synchronization; the data in your directory
server is never modified or compromised.
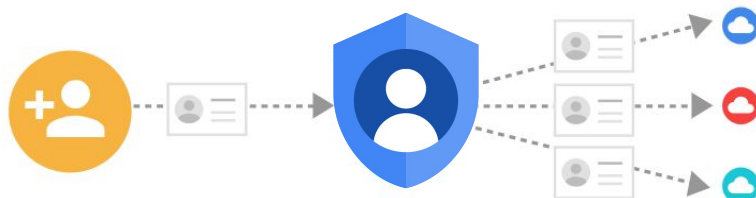
GCDS only performs one-way synchronization. You simply administer users in your
Active Directory/LDAP environment and then periodically update your Google domain.
The data in your directory server is never modified or compromised.

GCDS runs in your server environment

There is no access to your AD/LDAP server
outside your perimeter.

GCDS runs as a utility within your server environment, it does not need to run in the cloud. This means there is no access to your Active Directory or LDAP server needed outside your organization's IT perimeter.

GCDS auto-provisioning and deprovisioning

The GCDS auto-provisioning and deprovisioning features
reduce possible security risks.

The GCDS auto-provisioning and deprovisioning functions will remove a user's
account and deprovision that account from all cloud apps once that user has been
removed from your directory. This means there is no need to rely on a manual
process for this important task, reducing both operational overhead and security risks.
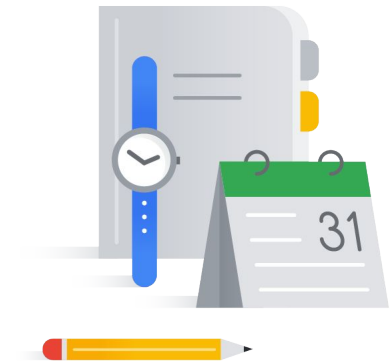
Securing Access to Google Cloud

Cloud Identity

Google Cloud Directory Sync

Managed Microsoft AD

Google authentication versus
SAML-based SSO

Identity Platform
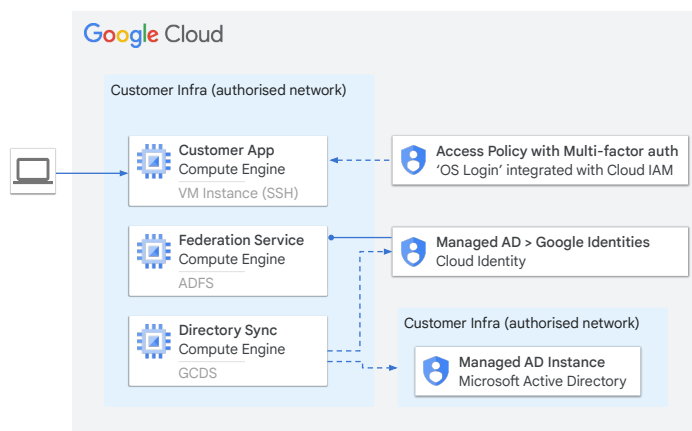
Authentication best practices

Google Cloud

Now let's discuss Managed Microsoft Active Directory.

___

Managed Microsoft AD allows you to manage your cloud-based, AD-dependent workloads

Managed Service for Microsoft Active Directory (Managed Microsoft AD):

- Runs actual Microsoft AD controllers

- Is virtually maintenance-free

- Supports both hybrid cloud and standalone cloud domains

Google Cloud

Customer Infra (authorised network)

Customer App
Compute Engine
VM Instance (SSH)

Access Policy with Multi-factor auth
'OS Login' integrated with Cloud IAM

Federation Service
Compute Engine
ADFS

Managed AD > Google Identities
Cloud Identity

Directory Sync
Compute Engine
GCDS

Customer Infra (authorised network)

Managed AD Instance
Microsoft Active Directory

Google Cloud

If you are already using Microsoft Active Directory on-premises and want that service and configuration to extend to your Google Cloud deployments, you now have the option to use Google's **Managed Service for Microsoft Active Directory**.

Managed Microsoft AD uses actual Microsoft Active Directory controllers, so your work will not be interrupted by the need to resolve application incompatibilities. Because it is a managed service, Google will take care of most routine maintenance needs. This management includes providing a highly available, secured deployment configuration, plus automated system patching and maintenance of appropriate firewall rules.

Managed Microsoft AD allows you to choose how your on-premises and cloud domains and workloads interact. For example, you can run each as a standalone domain, or you can connect your cloud domain with your on-premises domain.

This image highlights a sample architecture that uses Managed Microsoft AD. Check out the video link in the speaker notes for a Managed Microsoft AD deep dive:
- **Link:** youtube.com/watch?v=WnKH49Tp9oI&t=1250s

Managed Microsoft AD includes many useful features

- An actual AD domain

- Familiar tools, such as Group Policy and RSAT

- Highly available configurations

- Hardened servers with snapshots and automated patching

- Flexible, multi-regional deployments

Google Cloud

Managed Service for Microsoft Active Directory offers many useful and familiar features. As already mentioned, it uses actual Active Directory domains, which in addition to ensuring compatibility with your applications, can also be integrated with Cloud DNS to allow domain discovery for VMs. If you already use Group Policies and Remote Server Administration Tools (RSAT) in your on-premises network, your IT department will be able to continue to use these familiar tools to manage your cloud-based Active Directory domains.

Note that a key difference between GCDS and Managed Microsoft AD is that GCDS *syncs* to Google from on-premises AD, while Managed Microsoft AD is a hardened Google Cloud service running *actual* Microsoft AD.

Managed Microsoft AD runs on hardened, highly available servers and includes the ability to take snapshots to aid in recovery.

With its multi-regional Infrastructure, Managed Microsoft AD gives your apps and VMs access to your domain over a low-latency Virtual Private Cloud, and additional regions can be added as needed to increase your workload capacity.
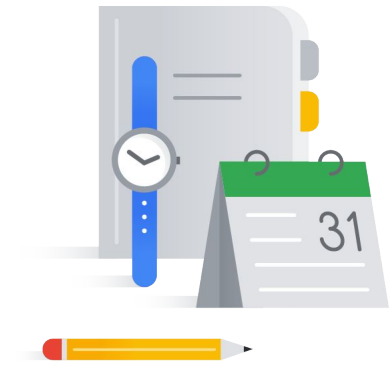
Securing Access to Google Cloud

Cloud Identity

Google Cloud Directory Sync

Managed Microsoft AD

Google authentication versus
SAML-based SSO

Identity Platform

Authentication best practices

Google Cloud

Next, let's discuss the two types of authentication which are supported by Google
Cloud.

User account authentication

Two primary ways to handle Google user account authentication:

- Google authentication
  - Primary mechanism for signing in to Google Cloud

- Single Sign-On (SSO) authentication

Google Cloud
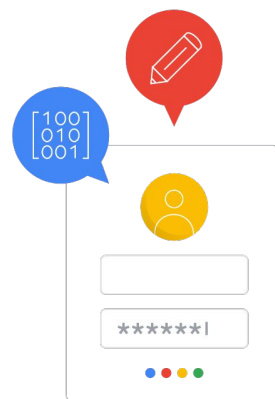
Up until now, we've focused on the various services available for managing users. We'll now focus on two different ways that Google handles user account authentication: Google authentication and Single Sign-On (SSO) authentication. The two authentication mechanisms are mutually exclusive. They cannot be combined, except within super admin accounts.

Google Authentication is the primary mechanism for signing in to Google Cloud. Using this method, a Google password is stored within Google's infrastructure. You can specify the minimum and maximum number of characters (within guidelines) and monitor the length and relative strength of your users' passwords.

Google also supports SAML 2.0 and and OpenID-compliant Single Sign On systems. Using this method Google operates as the service provider and your SSO system operates as the identity provider. This means you can use your own authentication mechanism, and manage your own credentials. This method will also work with hundreds of applications, straight out of the box.

SSO configuration requires 3 links and a certificate

☑ **Setup SSO with third party identity provider**

To setup third party as your identity provider, please provide the information below. ❓

Sign-in page URL

https://sso.your-domain.com/auth

URL for signing in to your system and G Suite

Sign-out page URL

https://sso.your-domain.com/logout

URL for redirecting users to when they sign out

Change password URL

https://sso.your-domain.com/info

URL to let users change their password in your system; when defined here, this is
Shown even when Single Sign-on is not enabled.

Verification certificate

Choose File Certificate.pem **UPLOAD**

The certificate file must contain the public key for Google to verify sign-in requests.

Google Cloud

SSO configuration in Google Cloud is a relatively simple process.

In Google Admin Console (admin.google.com):

- Check the Setup SSO with third party identity provider box
- Provide the required 3 URLs (sign-in, sign-out and password change) and upload your certificate file

Cloud Identity for SSO

Benefits:

● Use their existing credentials to authenticate

● Existing IdP remains the system for authentication

● No need to synchronize passwords to Cloud Identity
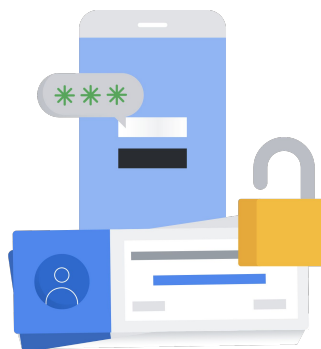
Google Cloud

You can also configure your Cloud Identity account to use single sign-on (SSO).

When you enable SSO, users aren't prompted to enter a password when they try to access Google services. Instead, they are redirected to an external identity provider (IdP) to authenticate.

Using SSO can provide several advantages:

● You enable a better experience for users because they can use their existing credentials to authenticate and don't have to enter credentials as often.
● You ensure that your existing IdP remains the system of record for authenticating users.
● You don't have to synchronize passwords to Cloud Identity or Google Workspace.

For more information check out the link to the documentation in the speaker notes.
● **Link:** cloud.google.com/architecture/identity/single-sign-on

Securing Access to Google Cloud

Cloud Identity

Google Cloud Directory Sync

Managed Microsoft AD

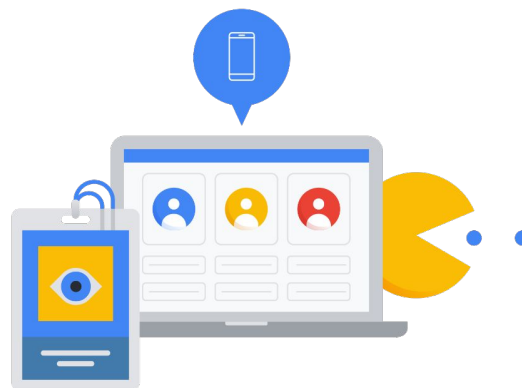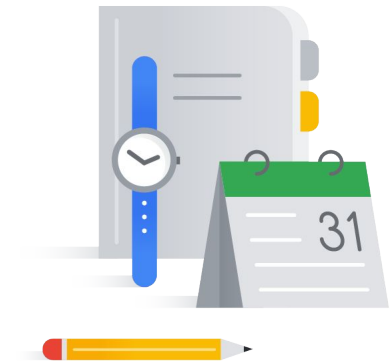Google authentication versus
SAML-based SSO

Identity Platform

Authentication best practices
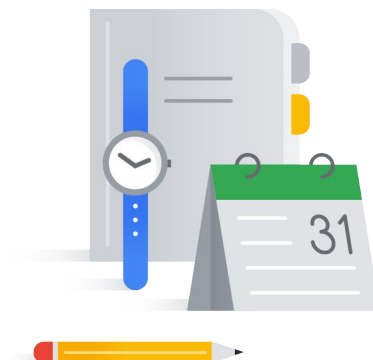
Google Cloud

Now let's talk about Identity Platform.

Identity Platform overview

- Customer identity and access management (CIAM) system
- Used for:
  - Multi-tenant SaaS applications
  - Mobile and web apps
  - Games
  - APIs and more

Google Cloud

Identity Platform is a customer identity and access management (CIAM) system that can help you add identity and access management functionality to your applications, protect user accounts, and scale with confidence.

So, what is a CIAM system? Your Apps may have many registered users. CIAM's allow your users to authenticate themselves using federated identity providers, such as Google, Twitter, Github or Facebook etc.

You can use Identity Platform for multi-tenant SaaS applications, mobile and web apps, games, APIs, and more.

Identity Platform is perfect if you're building a service on Google Cloud—or anywhere else for that matter—and want a Google-grade, easy to use authentication service.

Identity platform supports authentication using passwords, phone numbers, popular federated identity providers like Google, Facebook, Twitter, and any provider that supports SAML or OpenID Connect protocol.

Identity Platform integrates tightly with Google Cloud services, and it leverages industry standards like OAuth 2.0 and OpenID Connect, so it can be easily integrated with your custom backend.

Identity Platform provides Google-grade authentication, advanced user security, and planet-scale infrastructure.

For more information and hands-on practice with this service, search for the *Securing and Integrating Components of your Application* course on your preferred on-demand learning platform.

Securing Access to Google Cloud

Cloud Identity

Google Cloud Directory Sync

Managed Microsoft AD

Google authentication versus
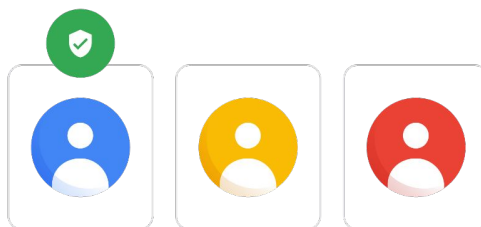SAML-based SSO

Identity Platform

Authentication best practices

Finally, let's look at some authentication best practices.

Manage Google Cloud permissions with groups

- Avoid managing permissions for individual users.
  - Managing individual users adds significant amount of operational overhead.
- Best to assign Google Cloud roles to groups instead.

Google Cloud

As with other identity systems, you should avoid managing permissions for individual users. Managing individual users will add a significant amount of operational overhead. It is much better to assign Google cloud roles to groups and let the Google Workspace/Cloud Identity admins handle group membership.

Group administration is completely handled in Google Admin Console, and users can be added or removed from groups without making any changes in IAM. For high-risk areas, you may want to make an exception to this practice -- assigning roles to individuals directly and foregoing the convenience of group assignment.

Number of Org admins

You should have at least two Organization admins, but not many more.
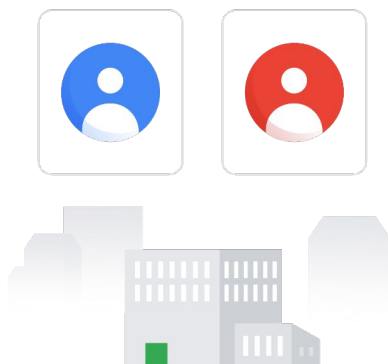
For convenience, you should have at least two Organization admins. This provides redundancy in case one of them is not available for any reason or if an account is lost.

But be careful about adding too many admins to your organization—a general guideline is to add no more than three.

Limit permissions

- Existing users are granted Project Creator and Billing Account Creator roles.

- Remove these permissions to start locking down access at a finer granularity.

Google Cloud

When the organization is first created, all users in your domain are automatically granted Project Creator and Billing Account Creator IAM roles at the organization level. This enables users in your domain to continue creating projects without disruption.

However, Organization Admins should remove these Organization-level permissions and start locking down access at a finer granularity as soon as possible.

Lab Demo

Defining Users with Cloud Identity Console

In this lab demo, you learn how to perform the following tasks:

- Register for a free Google Cloud trial account (only if you do not already have a Google Cloud account)
- Sign up for the free edition of Cloud Identity
- Create your Cloud Identity account and first admin user
- Verify your domain for use with Cloud Identity
- Create Cloud Identity user accounts
- Assign a Cloud Identity user access to a Google Cloud project
- And utilize groups to simplify user management and lower operational overhead

Module review

- Cloud Identity is an Identity as a Service (IDaaS) solution.
  - Tied to a unique DNS domain that is enabled for receiving email.
    - Does not need to be using Google Workspace services like Gmail or Drive.
  - Used for managing users, groups, and domain-wide security settings from a central location.
- Google Cloud Directory Sync tool can synchronizes Google Workspace accounts to match the data in an existing Active Directory or LDAP.

Google Cloud

To wrap up, here's an overview of what we discussed: