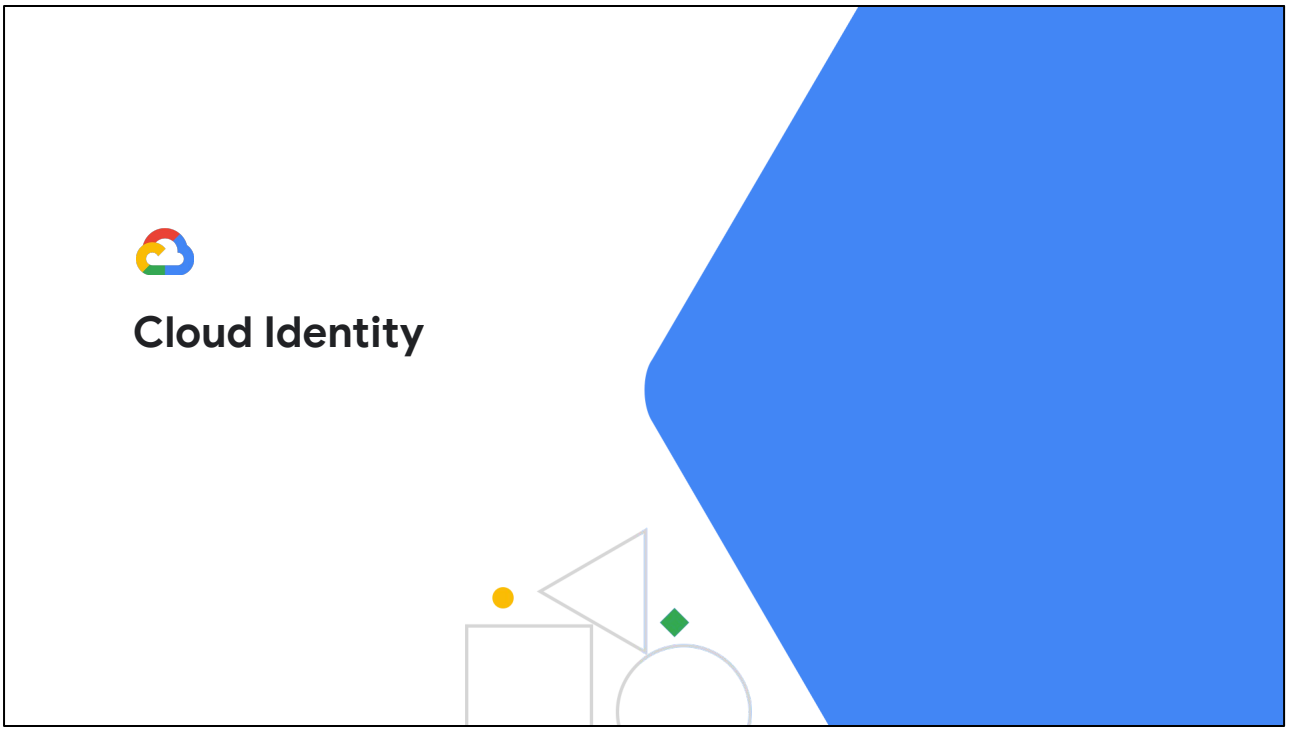


Welcome to the Cloud Identity module, part of the Security in Google Cloud course.

Agenda

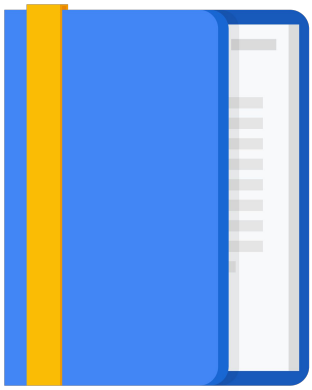
Cloud Identity

Google Cloud Directory Sync

Google authentication versus SAML-based SSO

Authentication Best Practices

Quiz and Module Review



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 and Single Sign On. We will end with some authentication best practices.

Agenda

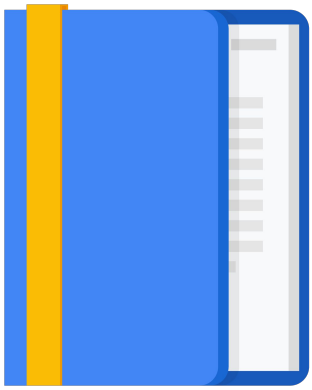
Cloud Identity

Google Cloud Directory Sync

Google authentication versus SAML-based SSO

Authentication Best Practices

Quiz and Module Review

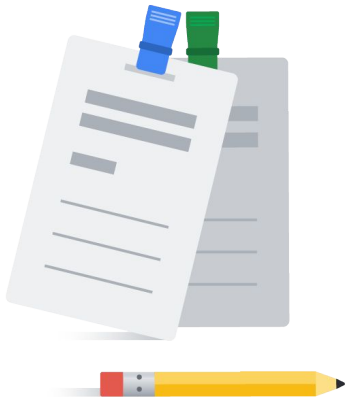


Google Cloud

OK, are you ready? Let's get started with Cloud Identity.

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



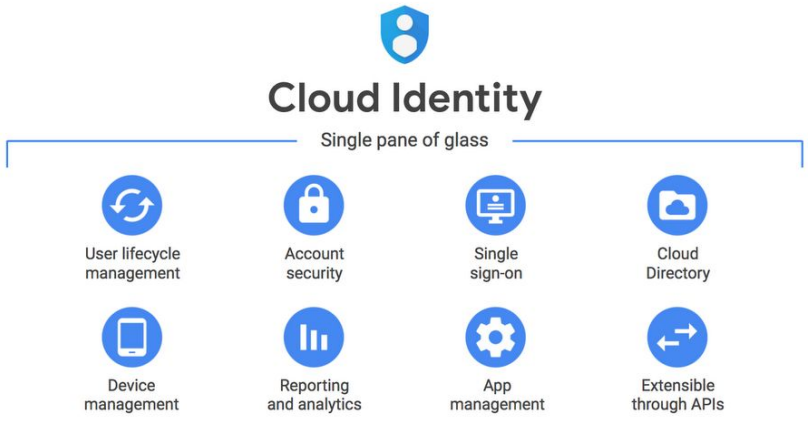
Google Cloud

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.

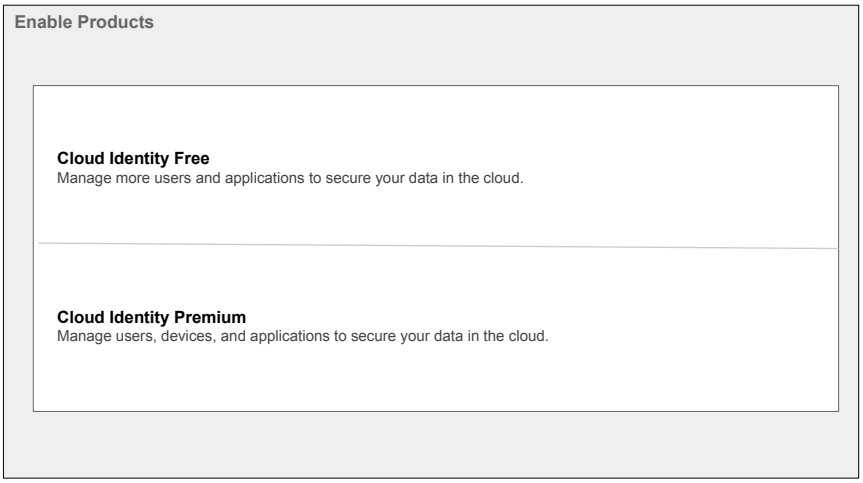
Cloud Identity



Google Cloud

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



Google Cloud

Cloud Identity is available as both a free and a premium edition. 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.

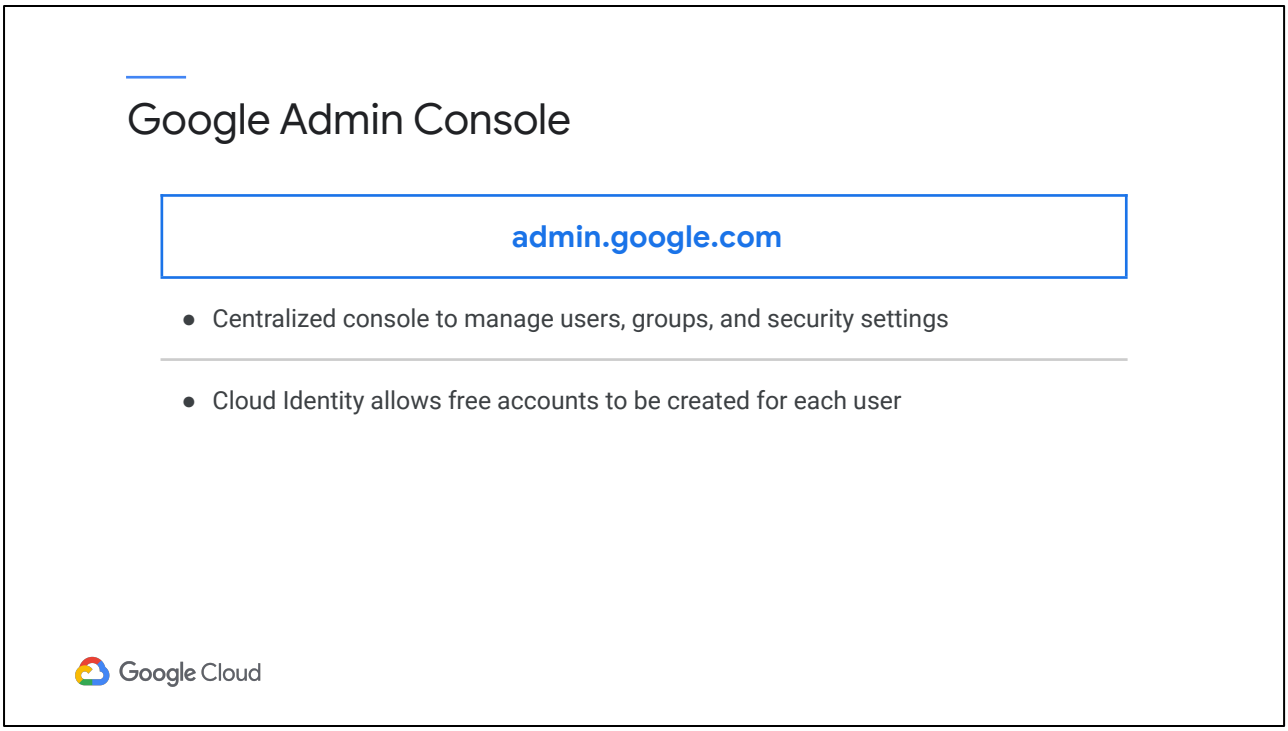
The Cloud Identity Premium edition offers enterprise security, application management, and device management services. These services include automated user provisioning, application allowlisting, and rules for automating mobile device management.

Compare Cloud Identity features and editions

https://support.google.com/cloudidentity/answer/7431902

Google Cloud

Visit the URL on this slide for a comparison of features offered by the free and premium editions of Cloud Identity.



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.

Support for Cloud Identity

Cloud Identity can be:

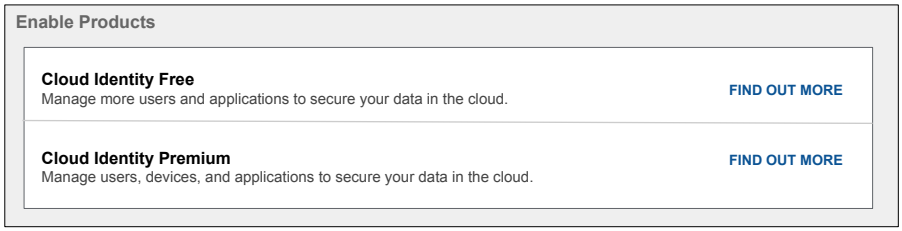
- Used as a standalone service
- Combined with your Google Workspace services

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.

If you are a Google Workspace admin

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



- 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).

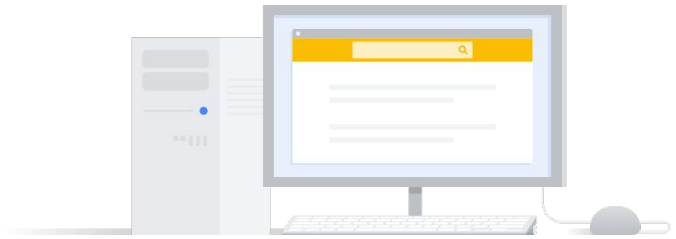
You can create free, non-licensed Cloud Identity accounts for managing users who do not need Google Workspace services.

If you are not using Google Workspace

- Register your domain as a Cloud Identity domain.

  gsuite.google.com/signup/gcpidentity

- Then use the Google Admin console to configure users and groups.



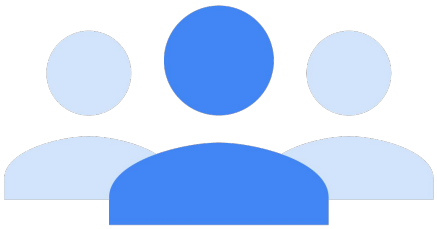
Google Cloud

If you are not using Google Workspace for your domain, you will first need to register your domain with Cloud Identity and verify you are the owner. You can perform these steps at the URL listed on the slide.

Once your domain is registered, the Google Admin Console at admin.google.com is used to manage users, groups, and security settings.

Org Admin

- Organization Administrator IAM role must be assigned to a user or group.
- Organization administrators have central control of all resources.



Google Cloud

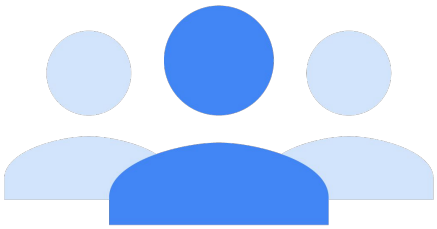
Each Google Workspace or Cloud Identity account is associated with one organization.

Organization administrators have central control of all resources. They can view and manage all of your organization's projects.

When creating the Organization resource, the Google Workspace or Cloud Identity super admin needs to assign the Organization Administrator IAM role to a user or a group.

If you are a Google Cloud Admin

- Assign roles to users or groups in IAM.
  - Can use any Google Workspace or Cloud Identity user or group
  - And any Google accounts and groups (@gmail, @google)



Google Cloud

Consumer accounts, such as personal Gmail accounts or consumer accounts with work email IDs, are unmanaged accounts and are outside of the Google Cloud admin's control.

This can be a security issue if developers in your organization use unmanaged accounts to use Google Cloud resources. To resolve this problem, you can create free Cloud Identity accounts - separate from Google Workspace accounts - to manage these users. You can then manage all of the users across your entire domain from one place by simply assigning roles to users or groups using the Google Cloud Console.

Agenda

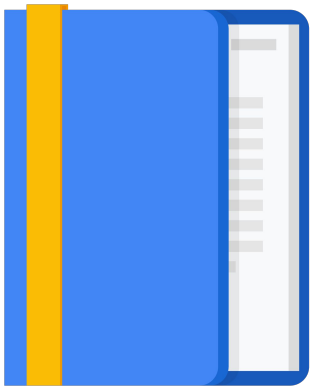
Cloud Identity

Google Cloud Directory Sync

Google authentication versus SAML-based SSO

Authentication Best Practices

Quiz and Module Review



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.

Provisioning users

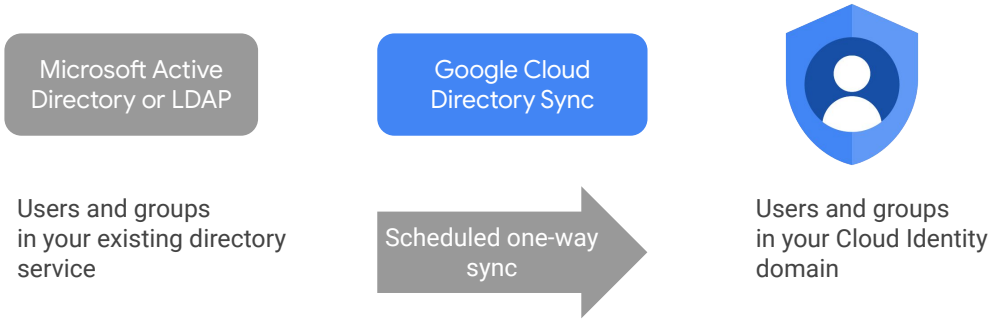
The Admin console allows admins to provisions users manually.

Google Cloud

As mentioned earlier, the Google Admin Console allows admins to provision user accounts manually. This is fine if you only need to add a few users, but it can be tedious and time consuming when many users need to be added.

Managing users manually can also add significant operational overhead. Someone has to manage not only the provisioning of new user accounts, but also the deprovisioning of accounts when users no longer need access.

What if you already have a different corporate directory?



Google Cloud

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 uses, 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

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.

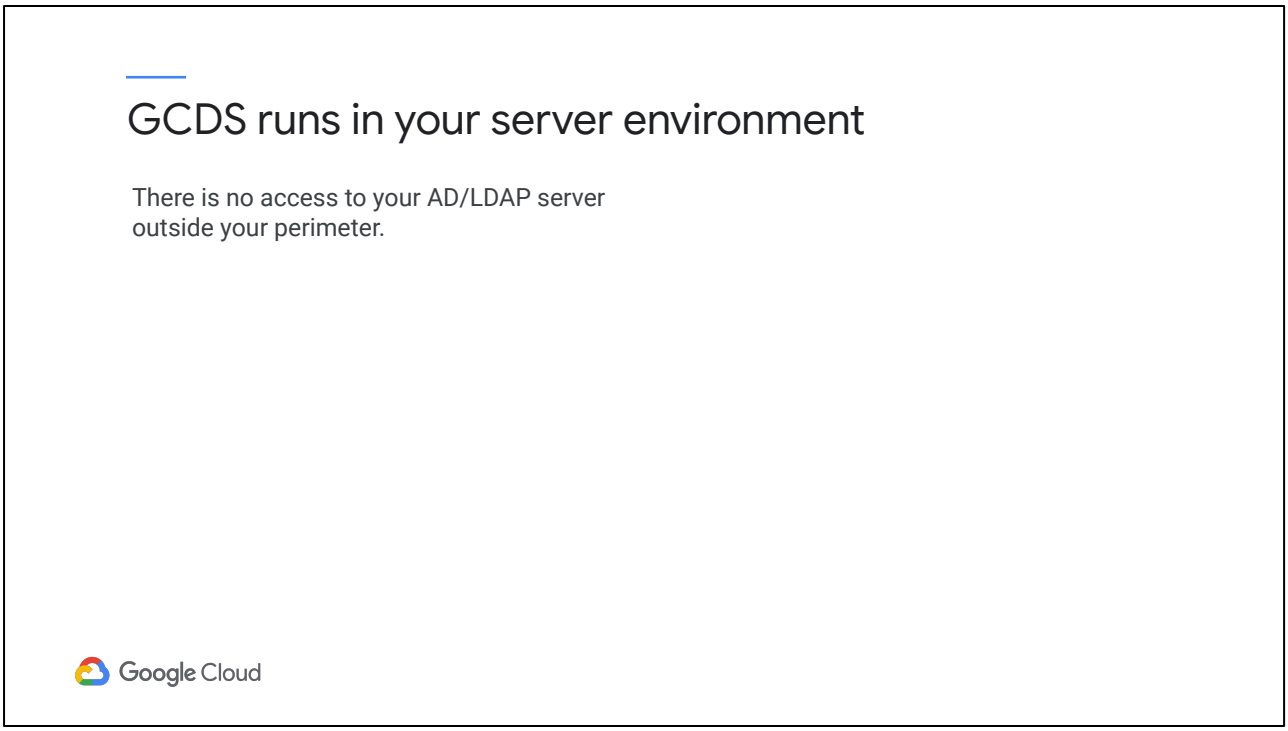
When the synchronization is complete, a report is emailed to the addresses that you specified when configuring GCDS.

One-way synchronization

One-way synchronization; the data in your directory server is never modified or compromised.

Google Cloud

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



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

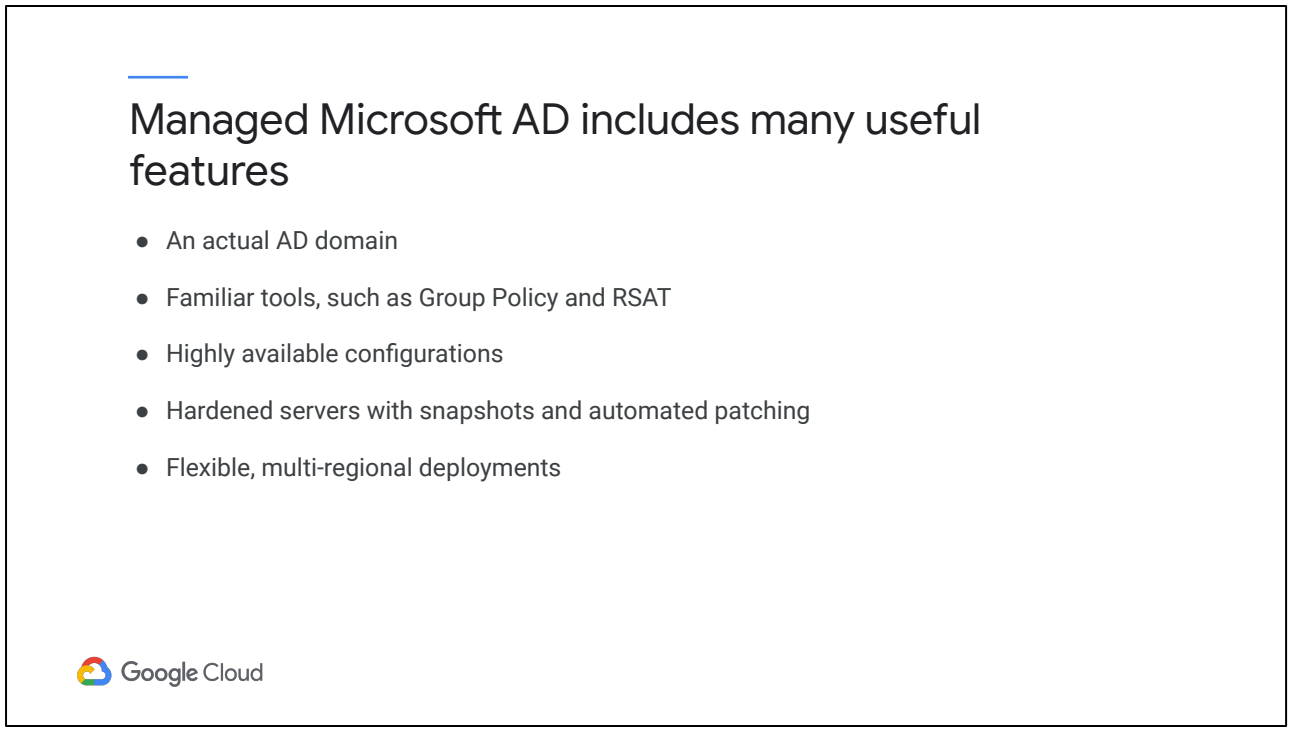
The GCDS auto-provisioning and deprovisioning features reduce possible security risks.

The GCDS auto-provisioning and deprovisioning functions will remove a user's account and deprovisioned 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.

However, 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.

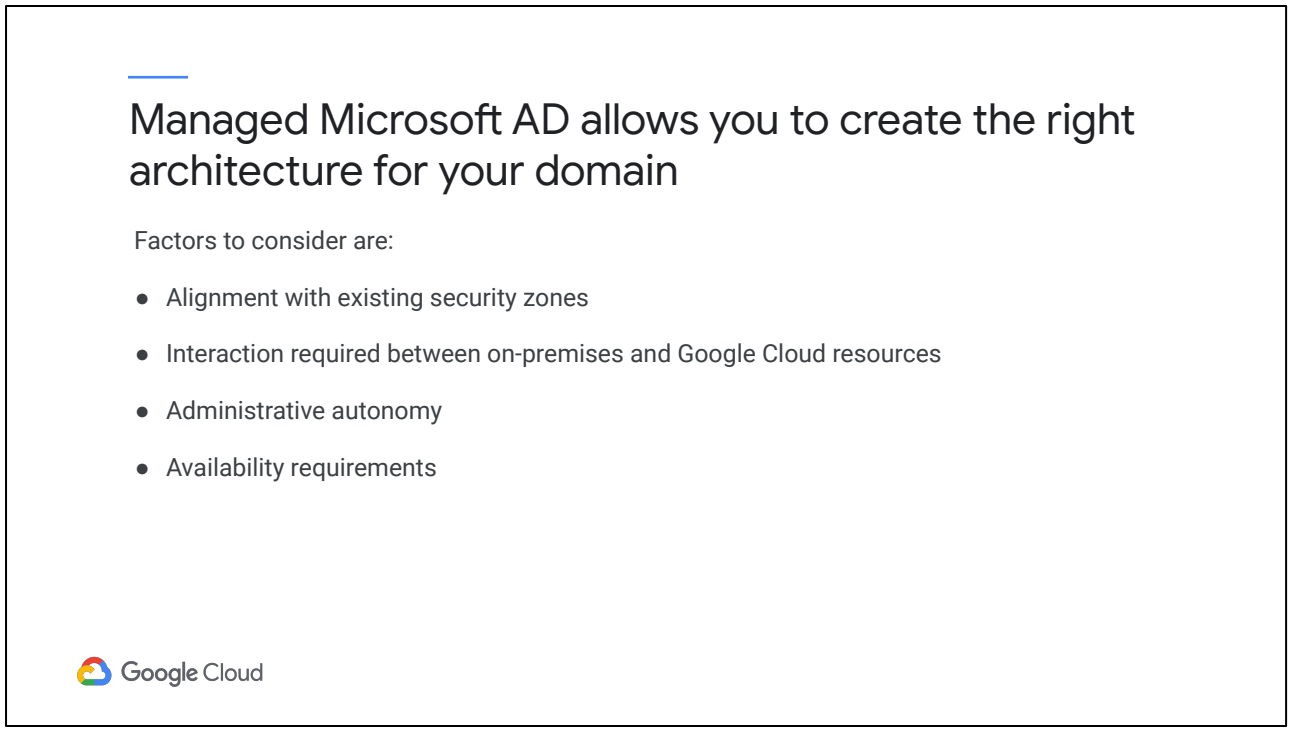
Managed Microsoft AD allows you to choose how your on-premises and cloud domains and workloads interact. For example, you can run each as a standalone domain, or you can connect your cloud domain with your on-premises domain.



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.

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.



In a typical Microsoft Active Directory on-premises environment, networks are often segmented into several “security zones.” These security zones are based on the interactions required to securely run applications and move data between applications. How they are set up outlines the trust boundaries between machines and traffic on your network.

Trust boundaries are also another way to contain the impact of a malicious attack. Attacks will continue across machines until they reach a trust boundary they cannot cross, which means that if one machine in a security zone has become infected, *all* machines in that zone must also be assumed to be compromised.

When you plan a deployment to Google Cloud that requires the use of Active Directory, you must decide between two options: to extend an existing on-premises security zone into Google Cloud, or to create a new security zone (or zones) for your cloud resources.

The expectation that a malicious attack will attempt to cross trust boundaries has implications for the architectural requirements of your hybrid network: this is why the Zero Trust model is the preferred networking model for Google Cloud. Zero Trust means that each machine in the network is treated as a separate entity, with its own Security Zone, and all the network and firewall scrutiny that goes along with that assumption.

Interaction between users and resources, both on-premises and in the cloud, can be

categorized as either “light,” “moderate,” or “heavy.” If all you need, for example, are an additional set of servers that can accept logins from your organization’s internal administrators, then your interaction would be considered light.

- One way to handle this level of interaction is to create two two separate Active Directory forests that don't share a trust relationship. However, that would also require duplicating information in the cloud forest, which could result in the duplicated data not being updated in a timely manner.
- A scenario that is less likely to result in out-of-date information is to create two separate Active Directory forests. Instead of maintaining duplicate records on each side, allow them to communicate with a cross-forest trust.

If your internal administrators also need to access to file shares, or your applications require the ability to authenticate and communicate across trust boundaries, then your interaction would be considered moderate. In this scenario, it is also recommended to use separate Active Directory forests with a cross-forest trust, because Kerberos and other common authentication protocols often cannot authenticate across forests on their own.

An example of heavy interaction might include the use of Virtual Desktop Infrastructure environments, which requires a near constant flow of information between on-premises resources and resources deployed on Google Cloud.

When resources across environments are closely coupled, the overhead of constant communication between separate forests may be prohibitive, so in this case, it is recommended to use a single Active Directory forest and share it across environments.

If the type of workloads you will be running on-premises and in the cloud differ significantly, or for other reasons have different teams administering them, you may wish to grant your teams administrative autonomy. One way to do that in Active Directory is to grant teams the authority to manage resources by using delegated administration. If your need for administrative coordination between teams is too great for delegated administration to handle, you can grant autonomy using separate domains.

The final factor to consider when you extend your Active Directory to Google Cloud is how your proposed architecture will affect resource availability.

For each domain in an Active Directory forest, the domain controller serves as the identity provider for users in that domain; therefore, interacting with a greater number of domain controllers can result in a corresponding decrease in the availability of your resources. Requiring interaction with multiple domains also increases the chance that an outage will impact the availability of your resources.

Taking all of these factors into account can help you align your hybrid network

topology with the availability requirements of your applications and other resources.

Agenda

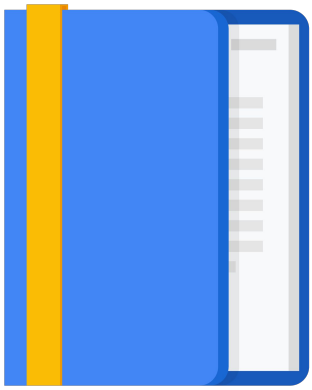
Cloud Identity

Google Cloud Directory Sync

Google authentication versus SAML-based SSO

Authentication Best Practices

Quiz and Module Review



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
- Single Sign-On (SSO) authentication

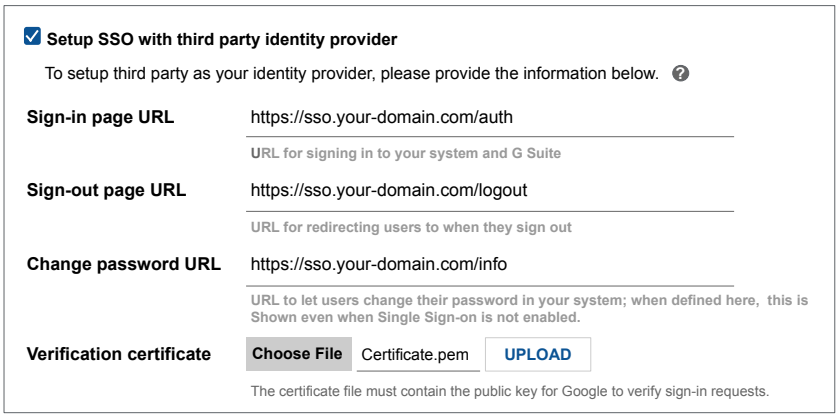
Google Cloud

There are two primary ways to handle Google 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



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

Agenda

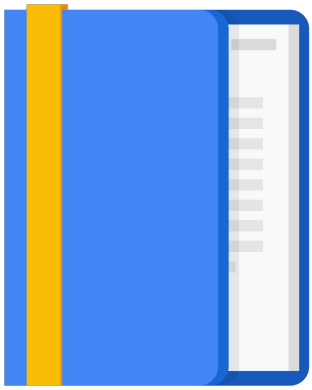
Cloud Identity

Google Cloud Directory Sync

Google authentication versus SAML-based SSO

Authentication Best Practices

Quiz and Module Review



Google Cloud

Finally, let’s take a quick look at some authentication “best practices.”

Manage Google Cloud permissions with groups

- Avoid managing permissions for individual users.
- Best to assign Google Cloud roles to groups instead.

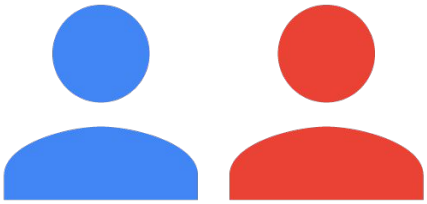
Google Cloud

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.



Google Cloud

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.

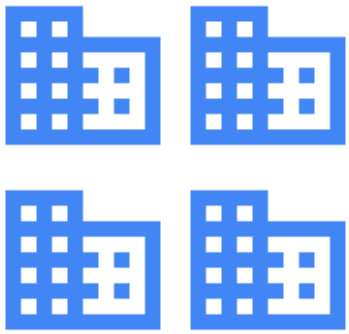
Google Cloud

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.

Multiple domains

- Multiple domains can be associated with your organization's Google account.
- You can add up to 600 domains.



Google Cloud

Multiple domains can be associated with your organization's account.

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.

Agenda

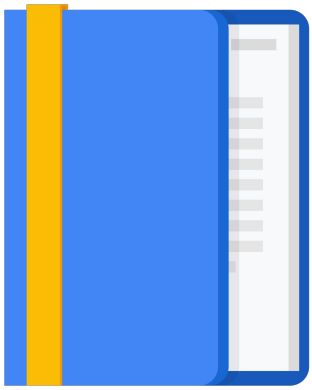
Cloud Identity

Google Cloud Directory Sync

Google authentication versus SAML-based SSO

Authentication Best Practices

Quiz and Module Review



Google Cloud

Quiz #1

Question

Which ONE of the following statements is TRUE for the use of Cloud Identity?

A. Cloud Identity can work with any domain name that is able to receive email.

B. Your organization must use Google Workspace services in order to use Cloud Identity.

C. You cannot use both Cloud Identity and Google Workspace services to manage your users across your domain.

D. A Google Workspace or Cloud Identity account can be associated with more than one Organization.

Quiz #1

Answer

Which ONE of the following statements is TRUE for the use of Cloud Identity?

A. Cloud Identity can work with any domain name that is able to receive email.

B. Your organization must use Google Workspace services in order to use Cloud Identity.

C. You cannot use both Cloud Identity and Google Workspace services to manage your users across your domain.

D. A Google Workspace or Cloud Identity account can be associated with more than one Organization.

Google Cloud

A. You do not have to use Google Workspace services to use the Cloud Identity Free edition.

Quiz #2

Question

The main purpose of Google Cloud Directory Sync is to: (choose ONE option below)

A. Help simplify provisioning and de-provisioning user accounts.

B. Completely replace an Active Directory or LDAP service.

C. Enable two-way data synchronization between Google Cloud and AD/LDAP accounts.

Quiz #2

Answer

The main purpose of Google Cloud Directory Sync is to: (choose ONE option below)

A. Help simplify provisioning and de-provisioning user accounts.

B. Completely replace an Active Directory or LDAP service.

C. Enable two-way data synchronization between Google Cloud and AD/LDAP accounts.

Google Cloud

A. Managing user accounts manually can be tedious and time-consuming when an organization has many users.

Quiz #3

Question

Which TWO of the following are considered authentication "best practices?"

A. Requiring 2-Step Verification (2SV) is only recommended for super-admin accounts.

B. You should have no more than three Organization admins.

C. Avoid managing permissions on an individual user basis where possible.

D. Organization Admins should never remove the default Organization-level permissions from users after account creation.

Quiz #3

Answer

Which TWO of the following are considered authentication "best practices?"

A. Requiring 2-Step Verification (2SV) is only recommended for super-admin accounts.

B. You should have no more than three Organization admins.

C. Avoid managing permissions on an individual user basis where possible.

D. Organization Admins should never remove the default Organization-level permissions from users after account creation.

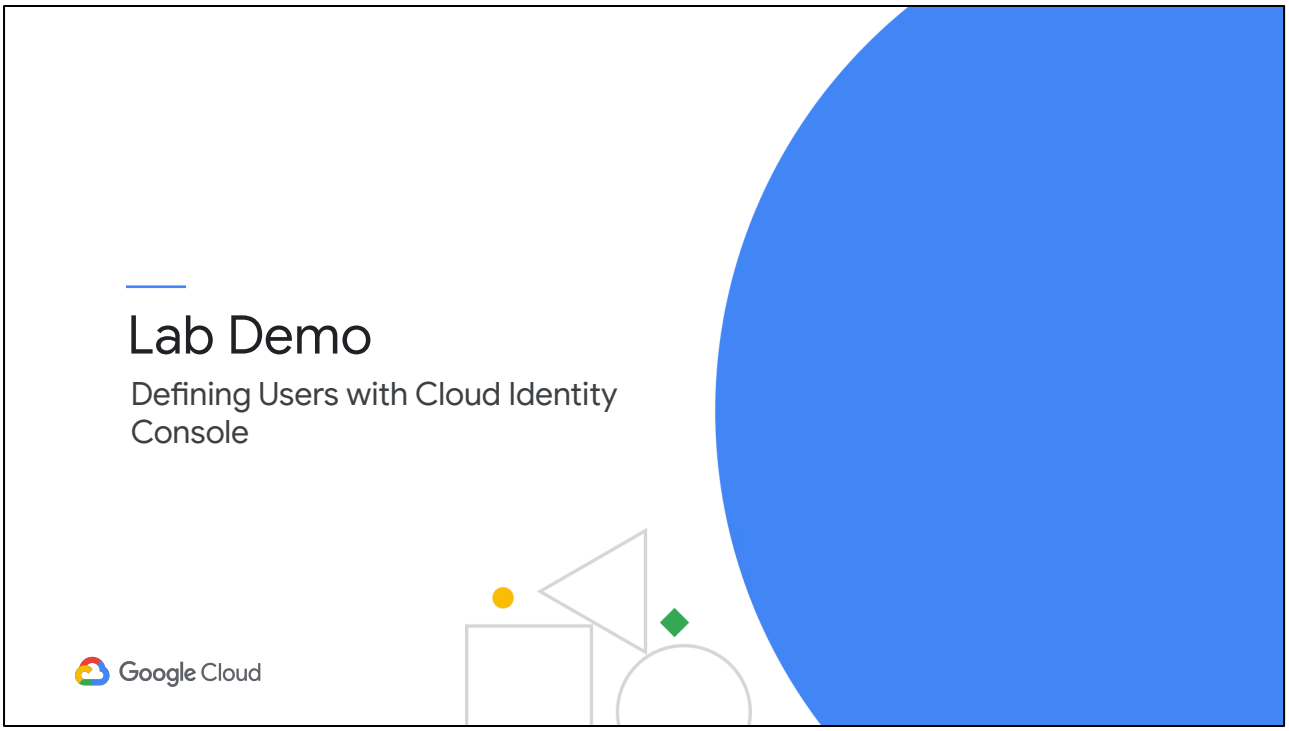
Google Cloud

B. Too many admins can create additional risk as well - the general advice is no more than three admins per organization.

C. Assigning users to groups and giving the group role-based permissions is much easier to manage.

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.
- Avoid managing permissions for individual users.
  - Best to assign Google Cloud roles to groups.
- You should have at least two Organization admins, but not many more.



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
- Utilize groups to simplify user management and lower operational overhead


Google Cloud