SafeStack

QUICK GUIDE

How to secure administrative access to the cloud

SafeStack

How to secure administrative access to the cloud

Quick guide

What is the purpose of this guide?

This guide is designed to help you secure administrative access to your cloud environment, whether you use Google Cloud Platform (GCP), Microsoft Azure, or Amazon Web Services (AWS). It's not intended to provide detailed instructions of every single security service available — instead, it covers common best practices and what they look like in each of the three major cloud service providers.

Why did you make this guide?

We made it because it can be a bit confusing to understand the different security features between the various cloud providers. We spent a lot of time researching the big three cloud providers, and want to share some of that information in a lightweight way.

We intend for this guide to be a useful resource for organizations embracing the cloud, and particularly those who are taking a hybrid-cloud or multi-cloud approach.

Where can I get more information?

The information collected here is from a number of sources, including the Center for Internet Security (CIS) and the cloud providers themselves; Amazon, Google, and Microsoft.

- Foundational Cloud Security with CIS Benchmarks
- CIS Benchmarks
- Google Cloud Best Practices
- Google Cloud Security Checklist
- AWS Identity Management
- Azure Identity Management

Choose your cloud provider to get started

All cloud providers

aws

Securing admin access to all clouds checklist

Are you maintaining an inventory of all admin accounts? □ Yes

Automated tools should be used to inventory all administrative accounts to ensure that only authorised individuals have elevated privileges.

Are dedicated admin accounts used? □ Yes

Dedicated, or secondary, accounts should be used for administrative tasks.

Is MFA enforced for all admin access? □ Yes

Multi-factor authentication and encrypted channels should be used for all administrative account access.

Are you logging and alerting on changes to admin group membership? □ Yes

The admins should be notified when changes are made to the admin groups.

Are you logging and alerting on unsuccessful admin account login? □ Yes

Unsuccessful logins to administrative accounts to raise an alert for further investigation.

Are you centrally logging admin activities? □ Yes

Logs should be aggregated to a central log management system for monitoring, alerting and analysis.

Are logs analysed by a security tool? □ Yes

Use of a Security Information and Event Management (SIEM) tool, or log analytics tool, can help correlate and identify potential abuse.

Are you reviewing logs regularly? □ Yes

Logs should be reviewed periodically for anomalies or abnormal events.

Are you tuning your SIEM or log analytics platform? □ Yes

These systems should be tuned to decrease event noise, and to help better identify actionable events.

Do you have a process for revoking admin access? □ Yes

Establishing and using automated processes for account revocation upon termination or change of responsibilities reduces the change of misuse.

Are you disabling dormant accounts?	□ Yes
Admin accounts should have access tokens or normal access methods disabled after a set period of activity.	
Do admin accounts have an expiration period set?	□ Yes
All admin accounts should have an expiration date configured.	
Are you able to alert on unusual admin account logins?	□ Yes
Alerting when an admin account logs in from an unusual location may help detect abuse.	

SafeStack doesn't intend these checklists to be comprehensive, and we encourage additions and modifications to fit your practice.

SafeStack

GCP admin access security checklist

Are only corporate login credentials used by admins?	□ Yes
It is recommended fully-managed corporate Google accounts be used for increased visibility, auditing, and controlling access to GCP. Email accounts based outside of the user's organization, such as personal accounts, should not be used for business purposes.	
Have you enforced security key MFA for all admin users?	□ Yes
GCP users with Organization Administrator roles have the highest level of privilege in the organization. These accounts should be protected with the strongest form of two-factor authentication: Security Key Enforcement. Security Keys are actual physical keys used to access Google Organization Administrator Accounts.	
Is separation of duties enforced while assigning Service Account related roles to Users?	□ Yes
No user should have Service Account Admin and Service Account User roles assigned at the same time.	
Are API keys rotated periodically?	□ Yes
Once a key is stolen, it has no expiration, meaning it may be used indefinitely unless the project owner revokes or regenerates the key. Rotating API keys will reduce the window of opportunity for an access key that is associated with a compromised or terminated account to be used. API keys should be rotated to ensure that data cannot be accessed with an old key that might have been lost, cracked, or stolen.	
Are Essential Contacts configured for your GCP organisation?	□ Yes
Many Google Cloud services, such as Cloud Billing, send out notifications to share important information with Google Cloud users. By default, these notifications are sent to members with certain Identity and Access Management (IAM) roles. With Essential Contacts, you can customize who receives notifications by providing your own list of contacts.	
Have you set up multiple super admin accounts?	□ Yes
Your organization should have more than one super administrator account, each managed by a separate individual (avoid sharing an admin account). If one account is lost or compromised, another super admin can perform critical tasks while the other account is recovered.	

Are you restricting daily activities to non-super admin accounts? □ Yes

Give each super administrator 2 accounts: Their own super admin account and a separate account for daily activities. Users should only sign in to a super admin account to perform super admin tasks, such as setting up 2-Step Verification (2SV), managing billing and user licenses, or helping another admin recover their account.

Super administrators should use a separate, non-admin account for day-to-day activities.

Have you configured secondary email contacts with super-admin accounts? □ Yes

If you don't often sign in with your primary admin account, you might miss important mandatory service announcements from Google. To make sure you receive these announcements set up a secondary email contact.

Are you logging out of super admin accounts after completing your tasks? □ Yes

Staying signed in to a super admin account when you aren't doing specific administrative tasks can increase exposure to phishing attacks. Super admins should sign in as needed to do specific tasks and then sign out.

Have you configured recovery options for admin accounts? □ Yes

Admins should add recovery options to their admin account in case they need to recover access.

Have admins enrolled a spare security key? □ Yes

Admins should enroll more than one security key for their admin account and store it in a safe place. If their primary security key is lost or stolen, they can still sign in to their account.

Have admins saved their backup codes ahead of time? □ Yes

If an admin loses their security key or phone (where they receive a 2SV verification code or Google prompt), they can use a backup code to sign in.

Admins should generate and print backup codes in case they're needed. Keep backup codes in a secure location.

SafeStack doesn't intend these checklists to be comprehensive, and we encourage additions and modifications to fit your practice.

SafeStack

Azure admin access security checklist

Have you enabled the 'Restore multi-factor authentication on all remembered devices' configuration? □ Yes

If an account or device is compromised, remembering MFA for trusted devices may affect security.

Hence, it is recommended that users not be allowed to bypass MFA.

Have you configured the 'Number of methods required to reset' account setting to '2' □ Yes

When a user with MFA undergoes self-service password resets this configuration ensures the user's identity is confirmed using two separate methods of identification. Azure AD Privileged Identity Management lets you limit users to only taking on their privileges JIT, and assign roles for a shortened duration with confidence that the privileges are revoked automatically.

Have you enabled the 'Notify users on password resets?' configuration? □ Yes

User notification on password reset is a passive way of confirming password reset activity. It helps the user to recognize unauthorized password reset activities.

Have you enabled the 'Notify all admins when other admins reset their password?' configuration? □ Yes

Administrator accounts are sensitive. Any password reset activity notification, when sent to all administrators, ensures that all administrators can passively confirm if such a reset is a common pattern within their group.

Have you configured Security Defaults on Azure Active Directory? □ Yes

Security defaults provide secure default settings that Microsoft manages on behalf of organizations to keep customers safe until they are ready to manage their own identity security settings.

Have you implemented "just in time" (JIT) access for privileged usage? □ Yes

Azure AD Privileged Identity Management lets you limit users to only taking on their privileges JIT, and assign roles for a shortened duration with confidence that the privileges are revoked automatically.

Have you defined at least two emergency access accounts? □ Yes

Emergency access accounts help organizations restrict privileged access in an existing Azure Active Directory environment. These accounts are highly privileged and are not assigned to specific individuals. Emergency access accounts are limited to scenarios where normal administrative accounts can’t be used.

Have you defined a "break glass" process?	□ Yes
In case you need to gain administrative access during an emergency, you can configure “break glass” access.	
Are critical admin tasks performed from dedicated workstations?	□ Yes
This will protect your admin accounts from attack vectors that use browsing and email and significantly lower your risk of a major incident.	

SafeStack doesn’t intend these checklists to be comprehensive, and we encourage additions and modifications to fit your practice.

SafeStack

AWS admin access security checklist

Have you removed access keys from your ‘root’ accounts? □ Yes

Removing access keys associated with the 'root' user account limits ways by which the account can be compromised. Additionally, removing the 'root' access keys encourages the creation and use of role based accounts that are least privileged.

Is hardware MFA is enabled for 'root' accounts? □ Yes

Hardware MFA devices are more secure than virtual MFAs, such as One-Time Passwords (OTP), or SMS verification methods.

Are you restricting the use of ‘root’ accounts? □ Yes

The 'root’ account has unrestricted access to and control over all account resources. Use of it is inconsistent with the principles of least privilege and separation of duties, and can lead to unnecessary harm due to error or account compromise.

Are you creating new IAM admin users without access keys? □ Yes

Requiring the additional steps be taken by the user for programmatic access after their profile has been created will give a stronger indication of intent that access keys are necessary for their work.

Do IAM user accounts only have one active access key? □ Yes

Access keys are long-term credentials for IAM users. One of the best ways to protect your account is to not allow users to have multiple access keys.

Are access keys rotated periodically? □ Yes

Rotating access keys will reduce the window of opportunity for an access key that is associated with a compromised or terminated account to be used.

Access keys should be rotated to ensure that data cannot be accessed with an old key which might have been lost, cracked, or stolen.

Are admin accounts given permissions via group membership only? □ Yes

Assigning IAM policy only through groups unifies permissions management to a single, flexible layer consistent with organizational functional roles. By unifying permissions management, the likelihood of excessive permissions is reduced.

Are IAM users managed centrally via identity federation or AWS Organizations for multi-account environments? □ Yes

Centralizing IAM user management to a single identity store reduces complexity and thus the likelihood of access management errors.

About SafeStack

SafeStack Academy is a community-centric online training platform that takes a flexible, people-focused approach to ongoing cyber security education at a time when it's never been more needed.

By teaching software development teams to weave in security from idea to maintenance, as well as providing cyber security and privacy awareness training for the wider workforce, SafeStack Academy's training programmes offer a comprehensive way of protecting people, systems, and data in an ever-changing world.

learn.safestack.io hello@safestack.io