Super Administrator Account Best Practices

To configure your Google Cloud Organization resource, you need to use a G Suite or Cloud Identity super admin account. Super admin accounts have irrevocable administrative permissions that we do not recommended using in the day-to-day administration of your organization. This page describes best practices for using your G Suite or Cloud Identity super admin accounts with your Google Cloud organization.

Account types

A G Suite super admin account has a set of administrative capabilities that includes Cloud Identity. This provides a single set of identity management controls for use across all Google services, such as Docs, Sheets, Google Cloud, and so forth.

A Cloud Identity account only provides authentication and identity management functionality, independent of G Suite.

Create a super admin email address

Create a new email address that is not specific to a particular user as the G Suite or Cloud Identity super admin account. This account should be further secured with multi-factor authentication, and could be used as an emergency recovery tool.

Designate organization admins

After you have acquired a new organization, you designate one or more organization administrators (https://cloud.google.com/resource-manager/docs/creating-managing-organization#adding_an_organization_admin). This role has a smaller set of permissions that are designed to manage your day to day organization operations.

You should also create a private Google Cloud administrator group in your G Suite or Cloud Identity super admin account. Add your organization administrator users to this group, but not your super admin user. Grant this group the Organization Administrator Cloud IAM role or a limited subset of the role's permissions.

We recommend keeping your super admin account separate from your organization administrator group. The super admin has irrevocable organization administrator privileges and can grant that role, but removing it can discourage using the super admin account for daily administration of your organization.

For information about managing access control for your organization using Cloud Identity and Access Management policies, see Access Control for Organizations using IAM (https://cloud.google.com/resource-manager/docs/access-control-org).

Set appropriate roles

G Suite and Cloud Identity has administrative roles that are not as permissive as the super admin role. We recommend following the principle of least privilege by granting users the minimum set of permissions they need to manage users and groups.

Discourage super admin account usage

The G Suite and Cloud Identity super admin account has a powerful set of permissions that are not necessary for use in the daily administration of your organization. You should implement policies that will secure your super admin accounts and make users less likely to attempt to use them for day-to-day operations, such as:

- Enforce multi-factor authentication (https://cloud.google.com/identity/solutions/enforce-mfa) on your super admin accounts as well as all accounts that have elevated privileges.
- Use a security key or other physical authentication device to enforce two-step verification.
- For the initial super admin account, ensure that the security key is kept in a safe place, preferably at your physical location.
- Give super admins a separate account that requires a separate login. For example, user alice@example.com could have a super admin account alice-admin@example.com.

    - If you are synchronizing with a third-party identity protocol, ensure you apply the same suspension policy to Cloud Identity and the corresponding third-party identity.
- If you have a G Suite enterprise or business account or a Cloud Identity premium account, you can enforce a short sign-in (https://support.google.com/a/answer/7576830?hl=en) period for any super admin accounts.
- Follow the guidance in the Security best practice patterns for administrator accounts (https://support.google.com/a/answer/9011373?hl=en).

API call alerts

Use Stackdriver to set up alerts (https://www.youtube.com/watch?v=LdGqmnoowc8) that will notify you when a `SetIamPolicy()` (https://cloud.google.com/resource-manager/reference/rest/v1/projects/setIamPolicy) API call is made. This will send an alert when anyone modifies any Cloud IAM policy.

Account recovery process

Ensure that the organization administrators are familiar with the super admin account recovery process (https://support.google.com/a/answer/33561?hl=en). This process will help you recover your account in the event that super admin credentials are lost or compromised.

Multiple organizations

We recommend using folders (https://cloud.google.com/resource-manager/docs/creating-managing-folders) to manage parts of your organization that you want to manage separately. If you want to use multiple organization resources instead, you will need multiple G Suite or Cloud Identity accounts. For information about the implications of using multiple G Suite and Cloud Identity, see Managing Multiple Organizations (https://cloud.google.com/resource-manager/docs/managing-multiple-orgs).

Except as otherwise noted, the content of this page is licensed under the Creative Commons Attribution 4.0 License (https://creativecommons.org/licenses/by/4.0/), and code samples are licensed under the Apache 2.0 License

(https://www.apache.org/licenses/LICENSE-2.0). *For details, see our Site Policies* (https://developers.google.com/terms/site-policies). *Java is a registered trademark of Oracle and/or its affiliates.*

Last updated November 19, 2019.