Credential Security in Google

This content was last updated in June 2025, and represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

Overview of Credential Security

As highlighted in the latest Google Cloud Threat Horizons Report, the growing number of identities within organizations expands the attack surface, underscoring the critical priority of robust identity protection. At Google, we acknowledge the inherent risks of managing private service account keys, which often have broad permissions and are susceptible to accidental exposure in logs, emails, and public repositories. Compounding these risks, threat actors increasingly target cloud environments by exploiting compromised cloud identities, both human and non-human. We understand the active threat of malicious actors automatically scanning for and rapidly exploiting credentials for activities like crypto mining or resale for hacking. Guided by our shared fate model, we acknowledge that while many customers rely on service account keys in production, and the potential for disruption with automatic disabling, we are committed to providing robust security for your Google Cloud environment. Our aim is to empower you with the necessary tools and capabilities to mitigate the security challenges of potential inadvertent disclosure, offering a strong, multi-layered defense that minimizes risk without disrupting essential operations, ultimately strengthening your overall identity protection posture.

Proactive Protection: Automatic Disabling of Leaked Service Account Keys

Since June 16, 2024, we enhanced our detection service that regularly scanned public repositories for leaked keys and notified customers upon discovery. As of that date, exposed service account keys detected on services including public repositories were automatically disabled by default for both new and existing customers. While customers had the option to opt in to this enhanced service before June 16, we also provided an opt-out for those who wished to retain the previous (less-secure) behavior of notification-only when leaked keys were detected. This automatic disabling of leaked service account keys was implemented as an organization policy update, made possible through close collaboration with secret-scanning programs at public repositories like GitHub and GitLab. For instance, upon detecting a service account key exposed in a public repository, Google Cloud automatically disabled the leaked key.

We ensured all project owners and listed security contacts were notified via email when leaked keys were detected. Subsequently, these keys were automatically disabled, a process that includes generating Cloud Audit Logs events, creating an abuse event in the Abuse Event logs, recording the disable action by the principal gcp-compromised-key-response@system.gserviceaccount.com in the audit logs, and setting the extendedStatus.value field to indicate the location of the leak. This multi-faceted approach underscores the critical importance of maintaining current security contact information to receive these timely security notifications and to be aware of the immediate and comprehensive actions taken to mitigate potential risks.

Enhanced Security Defaults for New Google Cloud Organizations

Ensuring a strong security foundation from the moment of adoption is an essential element of Google Cloud's commitment to our customers. To that end, we've introduced a streamlined onboarding experience for new organizations, automatically applying a more robust set of security best practices right from the start.

Upon successful domain verification, new Google Cloud customers are provisioned with an organization resource. This central element forms the bedrock of their cloud structure, enabling the implementation of consistent and scalable security controls across their entire environment via the Organization Policy Service. With this enhanced default security posture for new organization resources, we proactively mitigate common security risks. A curated collection of organization policies is automatically enforced upon the creation of a new organization, establishing a secure baseline configuration without requiring immediate manual intervention. This enhancement is specifically designed for new customers and will not alter the configurations of existing Google Cloud organizations.

Protecting Google Cloud Environments

To help ensure a more secure Google Cloud environment from the start, Google has implemented stronger default security settings. These automatic protections cover key areas: Identity and Access Management (IAM), Storage, and Essential Contacts.

- **Strengthening Identity and Access Management (IAM) Automatically:** Google has updated the default IAM settings to enforce better security for service accounts and control who can access resources:
- **Service Account Key Creation Disabled by Default:** To reduce the risk of accidentally exposing service account credentials, Google now prevents the automatic creation of long-lasting keys. Google recommends more secure

authentication alternatives for most use cases, allowing service account keys only when absolutely necessary.

- **Restricting Default Service Account Permissions:** When new services are created, their default service accounts will no longer automatically get the broad "Editor" role. Google recommends creating specific service accounts for each application with only the necessary permissions
- **Service Account Key Uploads Prevented:** To further protect against leaked and reused keys, Google has disabled the ability to upload custom service account keys.
- **Access Limited by Domain:** By default, IAM policies now only allow users within an organization's verified domain(s) to access its resources. This helps prevent unauthorized access from external accounts.

Securing Storage by Default

Google Cloud enforces uniform bucket-level access as the new default setting for Cloud Storage. This manages access consistently through IAM policies, disabling the older, more complex system of per-object access controls (ACLs) for simpler and more secure management and auditing.

Ensuring Secure Communication for Essential Notifications

The default setting for Essential Contacts now limits who can receive important platform notifications to users within an organization's verified domain(s). This ensures critical security and operational alerts are sent to the right personnel within the organization's control.

Whats Next

- Restricting Service Account Usage
- Service Account Best Practices
- IAM Best Practices
- Organization Policy Enforcement