

1.1 Ensure that Corporate Login Credentials are Used (Manual)

Profile Applicability:

- Level 1

Description:

Use corporate login credentials instead of personal accounts, such as Gmail accounts.

Rationale:

It is recommended fully-managed corporate Google accounts be used for increased visibility, auditing, and controlling access to Cloud Platform resources. Email accounts based outside of the user's organization, such as personal accounts, should not be used for business purposes.

Impact:

There will be increased overhead as maintaining accounts will now be required. For smaller organizations, this will not be an issue, but will balloon with size.

Audit:

For each Google Cloud Platform project, list the accounts that have been granted access to that project:

From Google Cloud CLI

```
gcloud projects get-iam-policy PROJECT_ID
```

Also list the accounts added on each folder:

```
gcloud resource-manager folders get-iam-policy FOLDER_ID
```

And list your organization's IAM policy:

```
gcloud organizations get-iam-policy ORGANIZATION_ID
```

No email accounts outside the organization domain should be granted permissions in the IAM policies. This excludes Google-owned service accounts.

Remediation:

Follow the documentation and setup corporate login accounts.

Prevention:

To ensure that no email addresses outside the organization can be granted IAM permissions to its Google Cloud projects, folders or organization, turn on the Organization Policy for `Domain Restricted Sharing`. Learn more at:

<https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains>





Default Value:

By default, no email addresses outside the organization's domain have access to its Google Cloud deployments, but any user email account can be added to the IAM policy for Google Cloud Platform projects, folders, or organizations.

References:

1. <https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations#manage-identities>
2. <https://support.google.com/work/android/answer/6371476>
3. <https://cloud.google.com/sdk/gcloud/reference/organizations/get-iam-policy>
4. <https://cloud.google.com/sdk/gcloud/reference/beta/resource-manager/folders/get-iam-policy>
5. <https://cloud.google.com/sdk/gcloud/reference/projects/get-iam-policy>
6. <https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints>
7. <https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 Centralize Account Management Centralize account management through a directory or identity service.			
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.			

1.2 Ensure that Multi-Factor Authentication is 'Enabled' for All Non-Service Accounts (Manual)

Profile Applicability:

- Level 1

Description:

Setup multi-factor authentication for Google Cloud Platform accounts.

Rationale:

Multi-factor authentication requires more than one mechanism to authenticate a user. This secures user logins from attackers exploiting stolen or weak credentials.

Audit:

From Google Cloud Console

For each Google Cloud Platform project, folder, or organization:

1. Identify non-service accounts.
2. Manually verify that multi-factor authentication for each account is set.

Remediation:

From Google Cloud Console

For each Google Cloud Platform project:

1. Identify non-service accounts.
2. Setup multi-factor authentication for each account.

Default Value:

By default, multi-factor authentication is not set.

References:

1. <https://cloud.google.com/solutions/securing-gcp-account-u2f>
2. <https://support.google.com/accounts/answer/185839>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 <u>Require MFA for Externally-Exposed Applications</u> Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v7	16.3 <u>Require Multi-factor Authentication</u> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

1.3 Ensure that Security Key Enforcement is Enabled for All Admin Accounts (Manual)

Profile Applicability:

- Level 2

Description:

Setup Security Key Enforcement for Google Cloud Platform admin accounts.

Rationale:

Google Cloud Platform 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. Ensure that admins use Security Keys to log in instead of weaker second factors like SMS or one-time passwords (OTP). Security Keys are actual physical keys used to access Google Organization Administrator Accounts. They send an encrypted signature rather than a code, ensuring that logins cannot be phished.

Impact:

If an organization administrator loses access to their security key, the user could lose access to their account. For this reason, it is important to set up backup security keys.

Audit:

1. Identify users with Organization Administrator privileges:

```
gcloud organizations get-iam-policy ORGANIZATION_ID
```

Look for members granted the role "roles/resourcemanager.organizationAdmin".

2. Manually verify that Security Key Enforcement has been enabled for each account.

Remediation:

1. Identify users with the Organization Administrator role.
2. Setup Security Key Enforcement for each account. Learn more at: <https://cloud.google.com/security-key/>



Default Value:

By default, Security Key Enforcement is not enabled for Organization Administrators.

References:

1. <https://cloud.google.com/security-key/>
2. https://gsuite.google.com/learn-more/key_for_working_smarter_faster_and_more_securely.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 <u>Require MFA for Externally-Exposed Applications</u> Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.			
v7	16.3 <u>Require Multi-factor Authentication</u> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		