Restricting Identities by Domain

The Resource Manager provides a domain restriction constraint that can be used in organization policies (https://cloud.google.com/resource-manager/docs/organization-policy/understanding-policies) to limit resource sharing based on domain. This constraint allows you to restrict the set of identities that are allowed to be used in Cloud Identity and Access Management policies (https://cloud.google.com/iam/docs/).

Organization policies can use this constraint to limit resource sharing to a specified set of one or more G Suite domains, and exceptions can be granted on a per-folder or per-project basis.

The domain restriction constraint is not retroactive. Once a domain restriction is set, this limitation will apply to Cloud IAM policy changes made from that point forward, and not to any previous changes.

For example, consider two related organizations: examplepetstore.com and altostrat.com. You have granted an examplepetstore.com identity an Cloud IAM role in altostrat.com. Later, you decided to restrict identities by domain, and implemented an organization policy with the domain restriction constraint in altostrat.com. In this case, the existing examplepetstore.com identities would not lose access in altostrat.com. From that point, you could only grant Cloud IAM roles to identities from the altostrat.com domain.

The domain restriction constraint is based on the `iam.allowedPolicyMemberDomains` (https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints#available_constraints) list constraint.

Note: The parent organization is not automatically added to the allowed list of a policy when you set the domain restriction constraint. You must add your organization explicitly to maintain access. If the parent organization is not added, and the **Organization Policy Administrator** role grant is then removed from all users, the organization policy would become inaccessible.

When this constraint is set on a G Suite domain, it will affect all identities that are under that domain. This includes user accounts that are managed in the G Suite console and not from

within the Google Cloud Console.

Setting the organization policy

The domain restriction constraint is a type of list constraint (https://cloud.google.com/resource-manager/docs/organization-policy/using-constraints#list-constraint). G Suite customer IDs can be added and removed from the `allowed_values` list of a domain restriction constraint. All domains associated with that G Suite account will be affected by the organization policy.

You must have permission to modify organization policies (https://cloud.google.com/resource-manager/reference/rest/v1/Policy) to set this constraint. For example, the `resourcemanager.organizationAdmin` (https://cloud.google.com/resource-manager/docs/access-control-org) role has permission to set organization policy constraints. Read the Using Constraints (https://cloud.google.com/resource-manager/docs/organization-policy/using-constraints#add-org-policy-admin) page to learn more about managing policies at the organization level.

CONSOLE GCLOUD

To set an organization policy including a domain restriction constraint:

1. Go to the Organization policies page in the Google Cloud Console.
   GO TO THE ORGANIZATION POLICIES PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/IAM-ADMIN
2. Click **Select**.
3. Select the organization you want to set the policy for.
4. Click **Domain Restricted Sharing**.
5. Click the **Edit** button.
6. Under **Applies to**, select **Customize**.
7. Under **Policy values**, select **Custom**.
8. Enter a G Suite customer ID (#retrieving_customer_id) into the **Policy value** text box, then press **Enter**. Multiple IDs can be entered in this way.
9. Click **Save**. A notification will appear to confirm that the policy has been updated.

To learn about using constraints in organization policies, see Using Constraints (https://cloud.google.com/resource-manager/docs/organization-policy/using-constraints#list-constraint).

Example organization policy

The following code snippet shows an organization policy including the domain restriction constraint:

```
resource: "organizations/842463781240"
policy {
  constraint: "constraints/iam.allowedPolicyMemberDomains"
  etag: "\a\005L\252\122\321\946\334"
  list_policy {
  allowed_values: "C03xgje4y"
  allowed_values: "C03g5e3bc"
  allowed_values: "C03t213bc"
  }
}
```

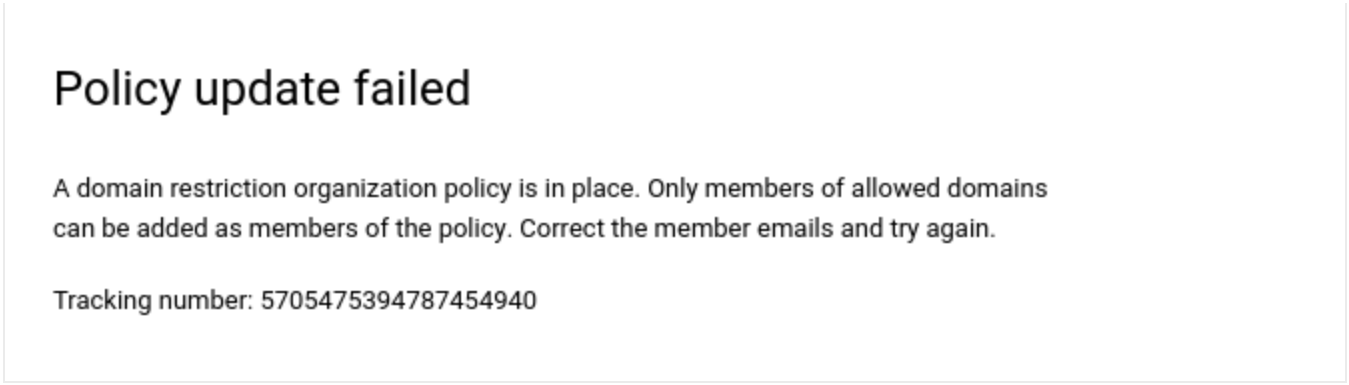
The `allowed_values` are G Suite customer IDs, such as `C03xgje4y`. Only identities belonging to a G Suite domain from the list of `allowed_values` will be allowed on Cloud IAM policies once this organization policy has been applied. G Suite human users and groups must be part of that G Suite domain, and Cloud IAM service accounts must be children of an organization resource associated with the given G Suite domain.

For example, if you created an organization policy with only the customer ID of your company's G Suite, only members from that domain could be added to the Cloud IAM policy from that point forward.

Example error message

When the domain restriction organization constraint is violated by trying to add a member that is not included in the `allowed_values` list, the operation will fail and then an error message will be displayed.

CONSOLE GCLOUD



Retrieving a G Suite customer ID

The G Suite customer ID used by the domain restriction constraint can be obtained in two ways:

GCLOUD API

The gcloud organizations list (https://cloud.google.com/sdk/gcloud/reference/organizations/list) command can be used to see all organizations for which you have the `resourcemanager.organizations.get` permission:

```
gcloud alpha organizations list
```

This command will return the `DISPLAY_NAME`, `ID` (Organization ID), and `DIRECTORY_CUSTOMER_ID`. The G Suite customer ID is the `DIRECTORY_CUSTOMER_ID`.

Restricting subdomains

The domain restriction constraint functions by limiting access to all domains that are associated with a given G Suite customer ID. Every G Suite account has exactly one primary domain, and zero or more secondary domains. All domains that are associated with the G Suite customer ID will be subject to the constraint.

Applying the domain restriction constraint to a resource controls the primary domain and all secondary domains that can access that resource and its descendents in the resource hierarchy.

For examples on common G Suite domain and subdomain combinations, see the table below:

Primary domain	Subdomain	Domain restriction constraint	Is `user@sub.domain.com` allowed?
domain.com	none	Allow: domain.com	No
domain.com	sub.domain.com	Allow: domain.com	Yes
domain.com	sub.domain.com	Allow: sub.domain.com	Yes
sub.domain.com	domain.com	Allow: sub.domain.com	Yes
sub.domain.com	none	Allow: sub.domain.com	Yes

To differentiate domain restriction constraint access between two domains, each domain must be associated with a different G Suite account. Each G Suite account is associated with an organization node, and can have their own organization policies applied. This allows you to associate `domain.com` with one G Suite account, and `sub.domain.com` with another for more granular access control. For more information, see Managing Multiple Organizations (https://cloud.google.com/resource-manager/docs/managing-multiple-orgs).

Troubleshooting known issues

Organization policies are not retroactive. If you need to force a change to your resource hierarchy that would violate an enforced constraint, you can disable the organization policy, make the change, and then enable the organization policy again.

The following sections describe known issues with services that can occur when this constraint is enforced.

Public data sharing

Some Google Cloud products such as BigQuery, Cloud Functions, Cloud Run, Cloud Storage, and Pub/Sub support public data sharing. Enforcing the domain restricted sharing constraint in an organization policy will prevent public data sharing.

To publicly share data, disable (#forcing_access) the domain restricted sharing constraint temporarily for the Project resource where the data you want to share resides. After you share the resource publicly, you can then re-enable the domain restricted sharing constraint.

Cloud Billing export service account

Enabling billing export to a bucket with this constraint enabled will probably fail. Do not use this constraint on buckets used for billing export.

The Cloud Billing export service account email address is: `509219875288-kscf0cheafmf4f6tp1auij5me8qakbin@developer.gserviceaccount.com`

Cloud Composer

Domain restricted sharing for Cloud Composer is currently in Beta. If you have enabled the domain restricted sharing (https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints) policy, you must use the Beta API when creating a Cloud Composer environment. Please refer to Beta Feature Support (https://cloud.google.com/composer/docs/concepts/beta-support) to learn how to deploy a Cloud Composer environment using the Beta API.

Enable storage access logging

If enabled, the domain restriction constraint will block any domain not specifically allowed in the organization policy. This will prevent granting Google service accounts access as well. To set up storage access logging (https://cloud.google.com/storage/docs/access-logs) on a Cloud Storage bucket that has the domain restriction constraint enforced:

1. Remove the organization policy containing the domain restriction constraint.
2. Grant `cloud-storage-analytics@google.com` `WRITE` access to that bucket.
3. Implement the organization policy with the domain restriction constraint again.

Forcing account access

If you need to force account access for a project in violation of domain restrictions:

1. Remove the organization policy containing the domain restriction constraint.
2. Grant account access to the project.
3. Implement the organization policy with the domain restriction constraint again.

Alternatively, you can whitelist a Google Group:

1. Create a Google Group within the allowed domain.
2. Use the G Suite administrator panel to turn off domain restriction for that group.
3. Add the service account to the group.
4. Implement the organization policy with the domain restriction constraint again.
5. Grant access to the Google Group in the Cloud IAM policy.

Last updated January 10, 2020.