Reserving a static external IP address

If a virtual machine (VM) instance requires a fixed external IP address that does not change, you can obtain a static external IP address for that instance by using one of the following options:

- Reserve a new static external IP address (#reserve_new_static) and then assign the address to a new VM instance (#assign_new_instance).

- Promote an existing ephemeral external IP address (#promote_ephemeral_ip) to become a static external IP address.

If you require a static IP address on your internal Compute Engine network, read Reserving a static internal address (/compute/docs/ip-addresses/reserve-static-internal-ip-address) instead.

In Compute Engine, each VM instance can have multiple network interfaces (/compute/docs/create-use-multiple-interfaces). Each interface can have both internal and external IP addresses. Forwarding rules can have external IP addresses for external load balancing or internal addresses for internal load balancing. To learn about IP addresses, read the IP addresses (/compute/docs/ip-addresses) documentation.

Before you begin

- If you want to use the command-line examples in this guide:

    1. Install or update to the latest version of the gcloud command-line tool (/compute/docs/gcloud-compute).

    2. Set a default region and zone (/compute/docs/gcloud-compute#set_default_zone_and_region_in_your_local_client).

- If you want to use the API examples in this guide, set up API access (/compute/docs/api/prereqs).

- Read IP addresses (/compute/docs/ip-addresses).

Reserving a new static external IP address

A static external IP address is an external IP address that is reserved for your project until you decide to release it (#release_ip). If you have an IP address that your customers or users rely on to access your service, you can reserve that IP address so that only your project can use it. It is also possible to promote an ephemeral external IP address (/compute/docs/configure-ip-addresses#promote_ephemeral_ip) to a static external IP address.

You can reserve two types of external IP addresses:

- A regional IP address which can be used by VM instances (/compute/docs/instances) with one or more network interfaces or by Network load balancers (/load-balancing/docs/network) .

- A global IP address which can be used for global load balancers: HTTP(S) (/load-balancing/docs/https), SSL proxy (/load-balancing/docs/ssl), and TCP proxy (/load-balancing/docs/tcp).

Reserve a static external IP address in the `gcloud` command-line tool or through the API. After reserving the address, assign it to an instance during instance creation (#assign_new_instance) or to an existing instance (#IP_assign).

Restrictions

- Only one resource at a time can use a static external IP address.

- There is no way to tell whether an IP address is static or ephemeral after it has been assigned to a resource, except to compare the IP address against the list of static external IP addresses reserved to that project. Use the `addresses list` (/sdk/gcloud/reference/compute/addresses/list) sub-command to see a list of static external IP addresses available to the project.

- Each VM instance can have multiple network interfaces (/compute/docs/create-use-multiple-interfaces), but each interface can have only one external IP address that is either ephemeral or static.

Network interfaces can receive traffic from multiple forwarding rules -balancing/docs/forwarding-rule-concepts), which might serve other external IP addresses. Any number of ex resses can reference a network interface through these forwarding rules, but each network interface can have ternal IP address that translates packets to the interface's internal IP address.

re information about load balancing and forwarding rules, read the load balancing (/load-balancing/docs) entation.

Console**gcloud** (#gcloud)API (#api)

1. In the Cloud Console, go to the **Reserve a static address** page.

   Go to the Reserve a static address page (https://console.cloud.google.com/networking/address

2. Choose a name for the new address.

3. Specify whether this is an `IPv4` or `IPv6` address. `IPv6` addresses can only be global and can only be used with global HTTP(S), SSL proxy, and TCP proxy load balancers.

4. Choose whether this IP address is regional or global. If you are reserving a static IP address for an instance or for a Network load balancer, choose **Regional**. If you are reserving a static IP address for an HTTP(S), SSL proxy, or TCP proxy load balancer, choose **Global**.

5. If this is a regional IP address, select the region to create the address in.

6. Optional. Select a resource to attach the IP.

7. Click **Reserve** to reserve the IP.

Assigning a static external IP address to a new VM instance

When you create a VM instance, it is automatically assigned an ephemeral external IP address. If you don't want an ephemeral external IP address, you can explicitly assign a static external IP address to the instance instead.

Before you can assign a static IP address, you must first reserve the static external IP address erve_new_static).

Console**gcloud** (#gcloud)API (#api)

1. In the Cloud Console, go to the **VM Instances** page.

   Go to the VM Instances page (https://console.cloud.google.com/compute/instances)

2. Click **Create instance**.

3. On the **Create a new instance** page, fill in the properties for your instance.

4. Expand the **Management, security, disks, networking, sole tenancy** section.

5. Click **Networking**.

6. Under **Network interfaces**, click on the default network interface to edit it.

7. Under the **External IP** section, select the static external IP address that you reserved from the drop-down menu.

8. Click **Done** to finish modifying the default network interface.

9. Click **Create** to create the instance.

Changing or assigning an external IP address to an existing instance

You can change or assign an external IP address, either ephemeral or static, to an existing instance by modifying the instance's access configuration.

An instance can have multiple interfaces and each interface can have an external IP address. If the instance already has an external IP address, you must remove that address first by deleting the old access configuration. Then, you can add a new access configuration with the new external IP address.

It is not possible to change the external IP address of a forwarding rule. If you need to update the IP address o̶rding rule, unassign the current IP address and delete and recreate the forwarding rule with the desired IP add̶

Console gcloud (#gcloud)

1. In the Cloud Console, go to the **VM instances** page.

   Go to the VM instances page (https://console.cloud.google.com/compute/instances)

2. Click the name of the instance that you want to assign an external IP to. The instance details page displays.

3. From the instance details page, complete the following steps:

   a. Click **Edit**.

b. Under **Network interfaces**, click the edit button.
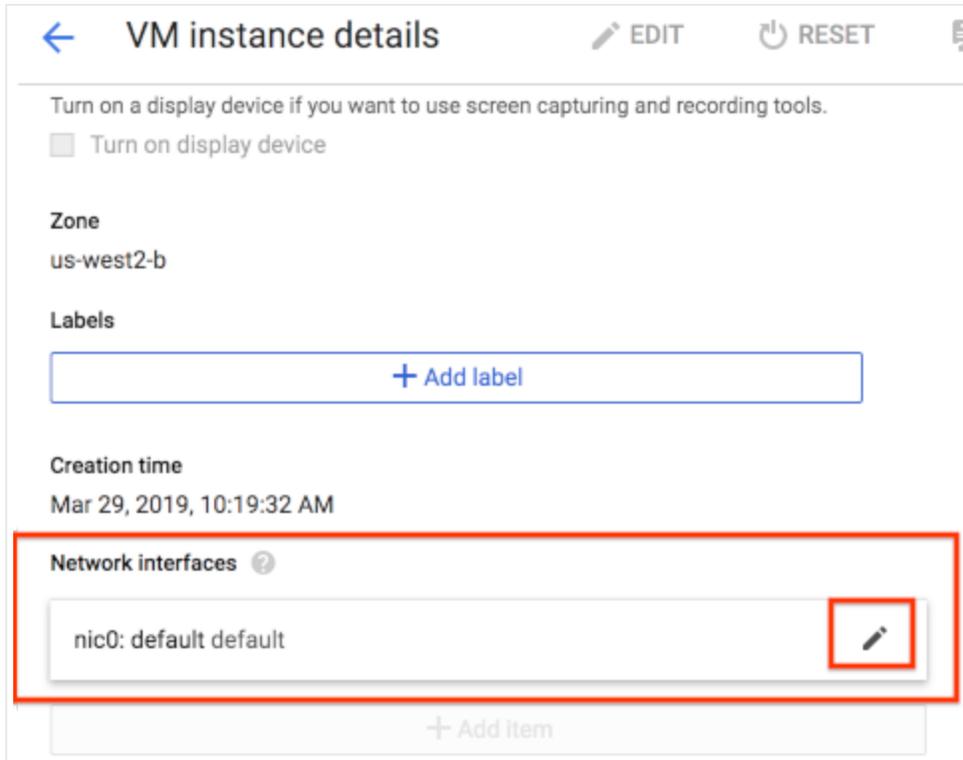
c. Under **External IP**, select either an ephemeral or static external IP address to assign to the instance.
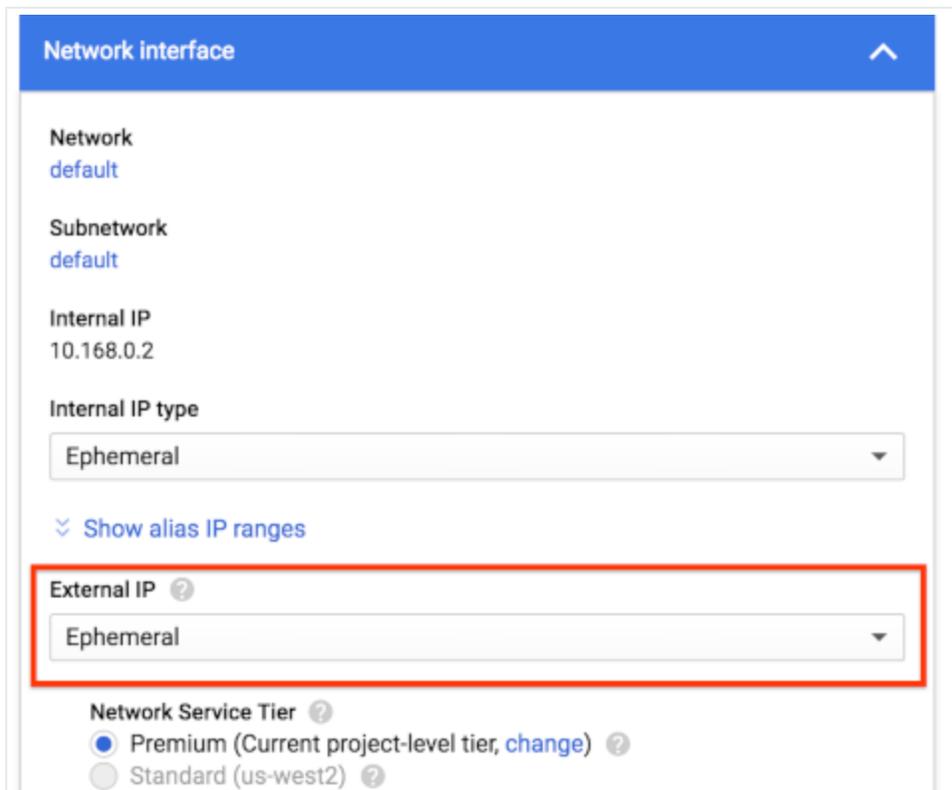
d. Click **Done**.

        e. Click **Save**.

Promoting an ephemeral external IP address

If your instance has an <u>ephemeral external IP address</u>
(/compute/docs/ip-addresses#ephemeraladdress) and you want to permanently assign the IP to
your project, promote the ephemeral external IP address to a static external IP address.
Promoting an ephemeral external IP address to reserved does not cause Google Cloud to drop
packets sent to the instance. This includes packets sent to the instance directly or by means of
a load balancer.

<u>Console</u><u>gcloud</u> (#gcloud)<u>API</u> (#api)

  1. In the Cloud Console, go to the **External IP addresses** page.

     <u>Go to the External IP addresses page</u> (https://console.cloud.google.com/networking/addresses)

  2. In the **Type** column, change the address type to **Static** for the IP address you want to promote.

  3. Provide a name for the new static IP address and click **Reserve**.

The external IP address remains attached to the instance even after it is been promoted to a
static external IP address. If you need to assign the newly promoted static external IP address
to another resource, <u>unassign the static external IP address</u> (#unassign_ip) from the existing
instance.

Listing static external IP addresses

To list static external IP addresses that you have reserved for your project, run `addresses list`
or make a `GET` request to the API.

<u>Console</u><u>gcloud</u> (#gcloud)<u>API</u> (#api)

In the Cloud Console, go to the **External IP addresses** page to see a list of IP addresses for your
project.

Go to the External IP addresses page (https://console.cloud.google.com/networking/addresses)

Describing a static external IP address

To get information about a static external IP address, use the console, the `gcloud` tool, or the API.

[Console](#)[gcloud](#gcloud)[API](#api)

1. In the Cloud Console, go to the **External IP addresses** page.

   Go to the External IP addresses page (https://console.cloud.google.com/networking/addresses)

2. Click the IP address you want to get more information about.

Unassigning a static external IP address

You can unassign a static external IP address by deleting the instance (/compute/docs/instances/deleting-instance) or deleting the access config attached to the instance that is using the address. Unassigning a static external IP address allows you to reassign the static external IP address to another resource.

Unassigning an IP address removes it from the resource but keeps the IP address reserved to your project. You can tell that a static IP address is in use by performing a `gcloud compute addresses list` request:

```
d compute addresses list
```

A response might look similar to the following:

```
                REGION        ADDRESS              STATUS
le-address      REGION        130.211.160.207      RESERVED
```

```
le-address-new    REGION      130.211.114.137      IN_USE
```

In this example, `example-address-new` is currently in use.

To delete an instance's access config and unassign a static external IP address, follow these steps:

1. Get the name of the access config to delete. To get the name, use the `gcloud compute instances describe` command. Replace *INSTANCE_NAME* with the name of the instance.

   ```
   gcloud compute instances describe INSTANCE_NAME
   ```

   The access config appears in the following format:

   ```
   networkInterfaces:
   - accessConfigs:
    - kind: compute#accessConfig
      name: external-nat
      natIP: 130.211.181.55
      type: ONE_TO_ONE_NAT
   ```

   Note: The `name` of your access config might be different than `external-nat`; make sure to check for your own access config name. In some cases, an older version of the access config name, `External NAT`, might be used.

2. Delete the access config.

   Note: Keep in mind that if an instance does not have an access config, it will not be able to access the Internet.

   Use the <u>instances delete-access-config command</u>
   (/sdk/gcloud/reference/compute/instances/delete-access-config):

```
gcloud compute instances delete-access-config INSTANCE_NAME \
        --access-config-name "ACCESS_CONFIG_NAME"
```

Replace the following:

- **INSTANCE_NAME**: The name of the instance.

- **ACCESS_CONFIG_NAME**: The name of the access config to delete. Make sure to include the full name between quotes.

3. Check that your static external IP address is now available and marked as `RESERVED` instead of `IN_USE`.

```
gcloud compute addresses list
```

For example:

```
NAME                REGION      ADDRESS          STATUS
example-address     REGION      130.211.160.207  RESERVED
example-address-new REGION      130.211.114.137  RESERVED
```

Now that your static external IP address is available, you can choose to assign it to another instance (#IP_assign).

Releasing a static external IP address

If you no longer need a static external IP address, you can release the address so that it is returned to the general IP pool for other Compute Engine users.

You can only release a static IP address if it is not being used by another resource.

Consolegcloud (#gcloud)API (#api)

1. In the Cloud Console, go to the **External IP addresses** page.

   [Go to the External IP addresses page](https://console.cloud.google.com/networking/addresses) (https://console.cloud.google.com/networking/addresses)

2. Check the box next to the IP address to release.

3. Click **Release IP address**.

Restricting external IP addresses to specific VM instances

For certain workloads, you might have essential requirements that include security and network restrictions. For example, you might want to restrict external IP address so that only specific VM instances can use them. This option can help to prevent data exfiltration or maintain network isolation. Using an Organization Policy (/resource-manager/docs/organization-policy/overview), you can restrict external IP addresses to specific VM instances with constraints to control use of external IP addresses for your VM instances within an organization or a project.

on: Restricting external IPs to specific instances can prevent existing GKE clusters and Managed Instance Grou dding new instances. If a GKE cluster or a Managed Instance Group is configured to create instances that do al IP addresses, autohealing and autoscaling actions will fail.

The constraint for controlling external IP address on VM instances is:

```
raints/compute.vmExternalIpAccess
```

To use the constraint, you specify a policy with an `allowedList` of VM instances that can have external IP addresses. If no policy is specified, all external IP addresses are allowed for all VM instances. When the policy is in place, only the VM instances that are listed in the `allowedValues` list can be assigned an external IP address, either ephemeral or static, and other Compute Engine VM instances in the organization or project that are not explicitly defined in the policy are prohibited from using external IP addresses.

VMs are identified in the allow and deny lists using the instance's URL:

```
cts/PROJECT_ID/zones/ZONE/instances/INSTANCE_NAME
```

Specifications

- You can only apply this <u>list constraint</u>
  (/resource-manager/docs/organization-policy/understanding-policies#list_policies) to VM
  instances.

- You cannot apply the constraint retroactively. All VM instances that have external IP
  addresses before the policy is enabled will keep their external IP address.

- This constraint accepts either an `allowedList` or a `deniedList` but not both in the same
  policy.

- It is up to the you or an administrator with the right permissions to manage and maintain
  the instance lifecycle and integrity. The constraint only verifies the instance's URL, and it
  does not prevent the white listed VMs from being altered, deleted, or recreated.

Permissions

To set a constraint on either the project or the organization level, you must have been granted
the `orgpolicy.policyAdmin` role on the organization.

Setting the policy constraint on the organization level

To set a constraint for external IP access, you first need your organization ID.

Find your organization ID

<u>Consolegcloud</u> (#gcloud)

You can also find the ID on the <u>Google Cloud Console</u> (https://console.cloud.google.com/):

1. Log in to the <u>Google Cloud Console</u> (https://console.cloud.google.com/).

2. Click the project selector.
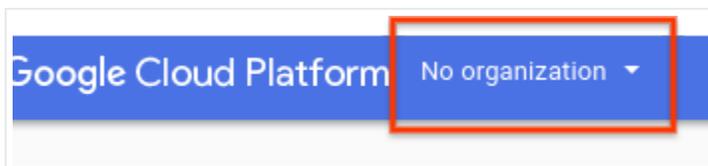
3. Select an organization and look for the organization ID.

Select

| No organization ▾ | ☰ Search projects and folders | | 🗂 | + |

Recent   All

Name	ID
⊞ No organization	0
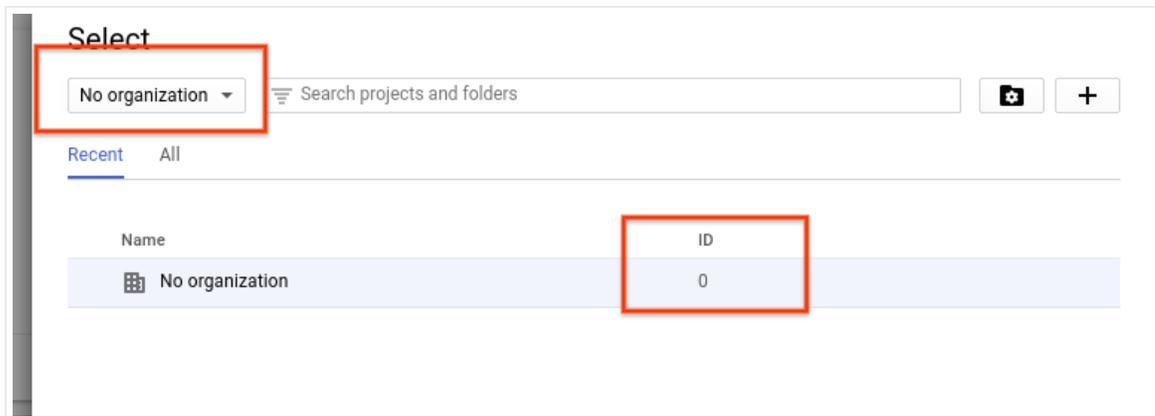
Set your policy constraint

The max length of each string used for each VM instance URL cannot exceed 200 characters.

Console gcloud (#gcloud) API (#api)

1. Go to the **Organizational Policies** page.

   Go to the Organizational Policies page (https://console.cloud.google.com/iam-admin/orgpolicies

2. If necessary, choose the desired organization from the project dropdown menu.

3. Click **Define Allowed External IPs for VM instances**.

4. Click **Edit** to edit the external IP policy. If you can't access the **Edit** tool, you do not have the correct permissions (#permissions).

5. Select **CPU platform and GPU** to set specific the org policy for specific VM instances.

   Replace the parent's policy and use the constraint defau

   ◉ Customize ❓
   Merge with or replace the parent's policy

   Policy enforcement ❓
   ● Merge with parent ❓
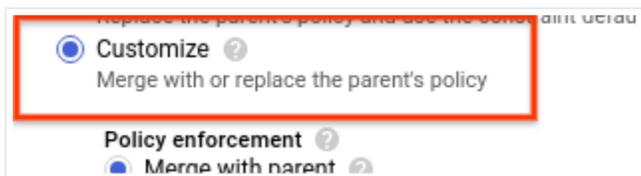
6. Choose the desired **Policy enforcement** and **Policy type**.

7. Under **Policy values**, select **Custom**.

8. Enter a partial URL to a VM instance and hit enter. Continue entering VM instances as desired.

> ⚠ To make sure your custom value works, test your policy after it's
> created. Learn more.

projects/myproject/zones/us-central1-a/example-vm-instance|

9. Click **Save** to save your changes.

Setting the policy at the project level

Setting a policy at the project level overrides the policy at the organization level. For example, if the organization level has `example-vm-1` on the `allowedValues` list but the policy at the project level has the same VM on the `deniedValues` list, the VM instance would not be allowed to have an external IP addresses.

Console gcloud (#gcloud) API (#api)

Follow the same process documented under Setting a policy constraint on the organization level (#setorgpolicy) but choose your desired project from the project selector instead of the organization.
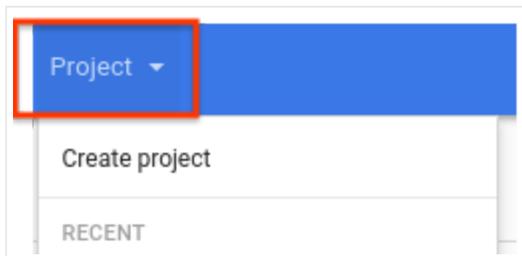
Best practices

- Google recommends that you avoid using the `deniedValues` list with this constraint. If you define values in the `deniedValues` list, it means only the VM instances in the `deniedValues` list are restricted from using external IP addresses. This could be a security concern if you want control over exactly which instances can have external IP addresses. If you want to remove certain instances from the `allowedValues` list, update the existing policy to remove the instances from the `allowedList` rather than putting the instances into the `deniedValues` list at a lower hierarchy.

- If you want to set a policy over a large part of the resource hierarchy but exempt certain projects, you should restore the default policy using the `setOrgPolicy` method by specifying the <u>restoreDefault</u> (/resource-manager/reference/rest/v1/Policy#RestoreDefault) object to allow all VMs in the projects to be associated with external IP addresses. The policies currently in place for projects will not be affected by this default setting.

- Use this org policy together with IAM roles to better control your environment. This policy only applies to VM instances but if you want to better control and restrict external IP addresses on network devices, you can grant the `compute.networkAdmin` role to the appropriate parties.

- Any services and products that are running on Compute Engine within the organization or project with the policy enabled are subject to this org policy. Specifically, services such as Google Kubernetes Engine, Dataflow, Dataproc, and Cloud SQL are affected by this policy. If this is an issue, Google recommends setting up other services and products in a different project that does not have the organization policy applied, and use <u>Cross-Project Networking</u> (/compute/docs/xpn) if needed.

What's next

- Learn more about <u>IP addresses</u> (/compute/docs/ip-addresses).

- Learn more about <u>networks and firewalls</u> (/compute/docs/networks-and-firewalls).

- Learn how to <u>address VM instances using internal DNS</u> (/compute/docs/internal-dns).

- Review <u>VPC pricing</u> (/vpc/network-pricing#vpc-pricing).