This page explains how to control access to devices using Cloud Identity and Access Management (IAM) (https://cloud.google.com/iam/). Access can be granted at the project or registry level. There is no access control at the individual device level. Access is typically granted to a person or a group of users, or to server-side service accounts. (Devices use public/private key authentication; for more details, see the section on device security (/iot/docs/device_security/)).

For example, if you assign a user the role (#roles) of `cloudiot.provisioner` to a device registry IAM policy, that user will be able to add or remove devices but won't be able to modify or delete the registry itself. A role can also be set on a cloud project; it then applies to all registries belonging to that cloud project.

This section focuses on the IAM permissions relevant to Cloud IoT Core and the IAM roles that grant those permissions. For a detailed description of IAM and its features, see the Cloud Identity and Access Management documentation (https://cloud.google.com/iam/). In particular, see the section on managing IAM policies (https://cloud.google.com/iam/docs/granting-changing-revoking-access).

A role is a bundle of permissions (#permissions). For example, `roles/cloudiot.viewer` contains the permissions `cloudiot.registries.get`, `cloudiot.registries.list`, `cloudiot.devices.get`, and `cloudiot.devices.list`. You assign roles to users or groups in order to allow them to perform actions on the registries in your project.

The following table lists the Cloud IoT Core IAM roles, including the permissions associated with each role:

Role	Description	Permissions

Role	Description	Permissions
`roles/cloudiot.viewer`	Read-only access to all Cloud IoT resources	• `cloudiot.registries.get` • `cloudiot.registries.list` • `cloudiot.devices.get` • `cloudiot.devices.list`
`roles/cloudiot.deviceController`	Access to update the configuration of devices, but not to create or delete devices	All of the above, and: • `cloudiot.devices.updateConfig` • `cloudiot.devices.sendCommand`
`roles/cloudiot.provisioner`	Access to create and delete devices from registries, but not to modify the registries	All of the above, and: • `cloudiot.devices.create` • `cloudiot.devices.delete` • `cloudiot.devices.update`
`roles/cloudiot.editor`	Read-write access to all Cloud IoT resources	All of the above, and: • `cloudiot.registries.create` • `cloudiot.registries.delete` • `cloudiot.registries.update`
`roles/cloudiot.admin`	Full control of all Cloud IoT resources and permissions	All of the above, and: • `cloudiot.registries.getIamPolicy` • `cloudiot.registries.setIamPolicy`

An additional role, `roles/cloudiot.serviceAgent`, grants Publisher permission for the relevant Cloud Pub/Sub (/pubsub/docs/access_control#tbl_roles) topics. This role is automatically assigned to a service account that is created when you enable the Google Cloud IoT Core API in a project. In most cases, you won't need to set or manage this role. If you do encounter permission errors related to Cloud Pub/Sub topics, see Troubleshooting (/iot/docs/troubleshooting#im_not_receiving_telemetry_data_on_cloud_pubsub).

For more information about roles, see Understanding Roles (/iam/docs/understanding-roles).

Permissions allow users to perform specific actions on registries or devices in Cloud IoT Core. For example, the `cloudiot.registries.list` permission allows a user to list the registries in your project. You don't directly give users permissions; instead, you assign them roles (#roles), which have one or more permissions bundled within them. You can also create custom roles (/iam/docs/creating-custom-roles).

The following tables list the IAM permissions that are associated with Cloud IoT Core:

Device registry permission name	Description
`cloudiot.registries.create`	Create a new registry in a project.
`cloudiot.registries.delete`	Delete a registry.
`cloudiot.registries.get`	Read registry details, excluding ACLs.
`cloudiot.registries.getIAMPolicy`	Read registry ACLs.
`cloudiot.registries.list`	List the registries in a project.
`cloudiot.registries.setIAMPolicy`	Update registry ACLs.
`cloudiot.registries.update`	Update registry details, excluding ACLs.
`cloudiot.devices.sendCommand`	Send commands (per registry, not per device).

Device permission name	Description
`cloudiot.devices.create`	Add a new device to a registry.
`cloudiot.devices.delete`	Delete a device.
`cloudiot.devices.get`	Read device details, excluding ACLs.
`cloudiot.devices.list`	List devices in a registry.
`cloudiot.devices.update`	Update device details, excluding ACLs.
`cloudiot.devices.updateConfig`	Update the device configuration.
`cloudiot.devices.bindGateway`	Bind a device to a gateway.
`cloudiot.devices.unbindGateway`	Unbind a device from a gateway.

For details on which IAM permissions allow users to run methods on registries and devices, see each method's specific REST reference (/iot/docs/reference/rest/).

You can get and set IAM policies using Cloud Console, the IAM API, or the gcloud tool. For information on how to do so at the project level, see Granting, Changing, and Revoking Access to Project Members (/iam/docs/granting-changing-revoking-access). The rest of this section contains information on IAM management at the device registry level.