

[AI & Machine Learning Products](https://cloud.google.com/products/machine-learning/) (<https://cloud.google.com/products/machine-learning/>)

[AI Platform](https://cloud.google.com/ml-engine/) (<https://cloud.google.com/ml-engine/>)

[Documentation](https://cloud.google.com/ml-engine/docs/) (<https://cloud.google.com/ml-engine/docs/>) [Guides](#)

# Access control

AI Platform uses [Identity and Access Management \(IAM\)](https://cloud.google.com/iam/) (<https://cloud.google.com/iam/>) to manage access to resources. To grant access to a resource, assign one or more [roles](https://cloud.google.com/iam/docs/understanding-roles) (<https://cloud.google.com/iam/docs/understanding-roles>) to a user, group, or [service account](https://cloud.google.com/iam/docs/overview#service_account) ([https://cloud.google.com/iam/docs/overview#service\\_account](https://cloud.google.com/iam/docs/overview#service_account)).

There are three types of IAM roles that can be used in AI Platform:

- [Primitive roles](https://cloud.google.com/iam/docs/understanding-roles#primitive_roles) ([https://cloud.google.com/iam/docs/understanding-roles#primitive\\_roles](https://cloud.google.com/iam/docs/understanding-roles#primitive_roles)) (Owner, Viewer, and Editor) are common to all Google Cloud services.
- [Predefined AI Platform roles](#) ([#predefined\\_roles](#)) give you fine-grained access control to your AI Platform resources at the project and model levels.
- [Custom roles](https://cloud.google.com/iam/docs/understanding-custom-roles) (<https://cloud.google.com/iam/docs/understanding-custom-roles>) enable you to choose a specific set of permissions, create your own role with those permissions, and grant the role to users in your organization.

This guide focuses on predefined AI Platform roles, their typical usage, and associated [permissions](#) ([#permissions\\_and\\_roles](#)).

## Primitive roles

The legacy AI Platform IAM roles are based on the [primitive roles](https://cloud.google.com/iam/docs/understanding-roles#primitive_roles) ([https://cloud.google.com/iam/docs/understanding-roles#primitive\\_roles](https://cloud.google.com/iam/docs/understanding-roles#primitive_roles)) that are common to all GCP services: Owner, Viewer, and Editor.

The legacy project **Editor** role is equivalent to the [AI Platform Admin role](#) ([#admin\\_role](#)).

The legacy project **Viewer** role grants the same permissions as the [AI Platform Viewer role](#) ([#viewer\\_role](#)), plus access to send online prediction requests. The advantage to using the AI Platform Viewer role is that the user gets read-only access to AI Platform resources.

## Predefined roles

Predefined roles grant a set of [related permissions](#) (#permissions\_and\_roles). AI Platform offers predefined roles for your project, and also for individual models, jobs, and operations.

To view a full list of permissions for each role, click on the name of the role.

### Project roles

The AI Platform Admin, Developer, and Viewer roles grant varying levels of access to resources at the project level.

To add, update, or remove these roles in your AI Platform project, see the documentation on [granting, changing, and revoking access to team members](#)

(<https://cloud.google.com/iam/docs/granting-changing-revoking-access>).

Role Title	Role Name	Capabilities
AI Platform Admin	<a href="#">roles/ml.admin</a> (#admin_role)	Full control of AI Platform project, and its jobs, operations, models, and versions.  <b>Note:</b> The primitive project <b>Editor</b> role is equivalent to <code>roles/ml.admin</code> .
AI Platform Developer	<a href="#">roles/ml.developer</a> (#developer_role)	Create training and prediction jobs, models and versions, and send online prediction requests.
AI Platform Viewer	<a href="#">roles/ml.viewer</a> (#viewer_role)	Read-only access to AI Platform resources.

### Model roles

The AI Platform Model Owner and Model User roles grant varying permissions to a particular model resource.

You can share models with individuals or services by [granting them the Model User role](#) (<https://cloud.google.com/ml-engine/docs/sharing-models>).

Role Title	Role Name	Capabilities
------------	-----------	--------------

Role Title	Role Name	Capabilities
AI Platform Model Owner	<a href="#">roles/ml.modelOwner</a> (#model_owner_role)	Full access to the model and its versions. This role is automatically granted to the user who creates the model.
AI Platform Model User	<a href="#">roles/ml.modelUser</a> (#model_user_role)	Permissions to read the model and its versions, and use them for prediction. Granting this role makes it easy to share specific models.

## Job and operation roles

Similar to the Model Owner role, there are owner roles at the job and operation resource levels that are assigned automatically to the user who creates the job or operation. These roles allow the user full control of any job or operation they create. For more information, see the [permissions for job and operation roles](#) (#job\_owner\_role).

## Permissions and roles

Refer to this section for a full list of permissions that are granted with each AI Platform predefined role. If these predefined roles do not meet your needs, use this section as a reference for creating your own [custom roles](https://cloud.google.com/iam/docs/understanding-custom-roles) (https://cloud.google.com/iam/docs/understanding-custom-roles).

## Admin role

Role Name	Description	Permissions
-----------	-------------	-------------

Role Name	Description	Permissions
<code>roles/ml.AI Platform Admin admin</code>	<p>Full access to your AI Platform project, and its jobs, operations, models, and versions.</p> <p><b>Note:</b> Migrating to this role from the primitive project <b>Editor</b> role is fairly simple. If you previously used the primitive <b>Editor</b> role assigned at the project level, you can use this <code>roles/ml.admin</code> role to grant exactly the same set of permissions to the user.</p>	<ul style="list-style-type: none"> <li>• <code>resourcemanager.projects.get</code></li> <li>• <code>ml.projects.getConfig</code></li> <li>• <code>ml.jobs.create</code></li> <li>• <code>ml.jobs.list</code></li> <li>• <code>ml.jobs.get</code></li> <li>• <code>ml.jobs.getIamPolicy</code></li> <li>• <code>ml.jobs.setIamPolicy</code></li> <li>• <code>ml.jobs.cancel</code></li> <li>• <code>ml.operations.list</code></li> <li>• <code>ml.operations.get</code></li> <li>• <code>ml.operations.cancel</code></li> <li>• <code>ml.models.create</code></li> <li>• <code>ml.models.list</code></li> <li>• <code>ml.models.get</code></li> <li>• <code>ml.models.setIamPolicy</code></li> <li>• <code>ml.models.getIamPolicy</code></li> <li>• <code>ml.models.predict</code></li> <li>• <code>ml.models.delete</code></li> <li>• <code>ml.models.update</code></li> <li>• <code>ml.versions.create</code></li> <li>• <code>ml.versions.list</code></li> <li>• <code>ml.versions.get</code></li> <li>• <code>ml.versions.predict</code></li> <li>• <code>ml.versions.delete</code></li> </ul>

## Developer role

Role Name	Description	Permissions
-----------	-------------	-------------

Role Name	Description	Permissions
roles/ml-developer	<p>Access to create training and prediction jobs, models and developer versions, and send online prediction requests.</p> <p><b>Note:</b> A developer receives <code>ml.jobs.cancel</code> and <code>ml.jobs.update</code> permissions on all jobs they create, because creating a job automatically grants them the <a href="#">AI Platform Job Owner role</a>. (#job_owner)</p> <p><b>Recommendation:</b> Grant the developer read-only access to the <a href="#">AI Platform logs</a> (<a href="https://cloud.google.com/logging/docs/access-control">https://cloud.google.com/logging/docs/access-control</a>) for <a href="#">troubleshooting purposes</a> (<a href="https://cloud.google.com/ml-engine/docs/troubleshooting#using_job_logs">https://cloud.google.com/ml-engine/docs/troubleshooting#using_job_logs</a>)</p>	<ul style="list-style-type: none"> <li>• <code>resourcemanager.projects.get</code></li> <li>• <code>ml.projects.getConfig</code></li> <li>• <code>ml.jobs.create</code></li> <li>• <code>ml.jobs.list</code></li> <li>• <code>ml.jobs.get</code></li> <li>• <code>ml.jobs.getIamPolicy</code></li> <li>• <code>ml.operations.list</code></li> <li>• <code>ml.operations.get</code></li> <li>• <code>ml.models.create</code></li> <li>• <code>ml.models.list</code></li> <li>• <code>ml.models.get</code></li> <li>• <code>ml.models.getIamPolicy</code></li> <li>• <code>ml.models.predict</code></li> <li>• <code>ml.versions.list</code></li> <li>• <code>ml.versions.get</code></li> <li>• <code>ml.versions.predict</code></li> </ul>

## Viewer role

Role Name	Description	Permissions
-----------	-------------	-------------

Role Name	Description	Permissions
<code>roles/ml.viewer</code>	<p>Read-only access to AI Platform resources on a particular project.</p> <p><b>Note:</b> The legacy project <b>Viewer</b> role grants a user the same permissions as the <code>roles/ml.viewer</code> role, plus access to send online prediction requests.</p>	<ul style="list-style-type: none"> <li><code>resourcemanager.projects.get</code></li> <li><code>ml.projects.getConfig</code></li> <li><code>ml.jobs.list</code></li> <li><code>ml.jobs.get</code></li> <li><code>ml.operations.list</code></li> <li><code>ml.operations.get</code></li> <li><code>ml.models.list</code></li> <li><code>ml.models.get</code></li> <li><code>ml.versions.list</code></li> <li><code>ml.versions.get</code></li> </ul>

## Model Owner role

Role Name	Description	Permissions
<code>roles/ml.modelOwner</code>	<p>Full access to the model and its versions. This role is automatically granted to the user who creates the model.</p>	<ul style="list-style-type: none"> <li><code>ml.models.get</code></li> <li><code>ml.models.setIamPolicy</code></li> <li><code>ml.models.getIamPolicy</code></li> <li><code>ml.models.predict</code></li> <li><code>ml.models.delete</code></li> <li><code>ml.models.update</code></li> <li><code>ml.versions.create</code></li> <li><code>ml.versions.list</code></li> <li><code>ml.versions.get</code></li> <li><code>ml.versions.predict</code></li> <li><code>ml.versions.delete</code></li> </ul>

## Model User role

Role Name	Description	Permissions
<code>roles/ml.modelUser</code>	Permissions to read the model and its versions, and to use them for prediction.	<ul style="list-style-type: none"> <li><code>ml.models.get</code></li> <li><code>ml.models.predict</code></li> <li><code>ml.versions.list</code></li> <li><code>ml.versions.get</code></li> <li><code>ml.versions.predict</code></li> </ul>

## Job Owner role

Role Name	Description	Permissions
<code>roles/ml.jobOwner</code>	<p>Full access to all permissions for a particular job resource. The Job Owner role is granted automatically to the user who creates that job.</p> <p>For example, a user who has the AI Platform Developer role on a project can create jobs, list all jobs, and get all jobs in a given project. The Developer has access to cancel only the job(s) they have created.</p>	<ul style="list-style-type: none"> <li><code>ml.jobs.get</code></li> <li><code>ml.jobs.getIamPolicy</code></li> <li><code>ml.jobs.cancel</code></li> </ul>

## Operation Owner role

Role Name	Description	Permissions
<code>roles/ml.operationOwner</code>	Full access to all permissions for a particular operation resource. The Operation Owner role is granted to the user automatically on any operations that the user indirectly creates when creating a version or a model, so that the user always can get and cancel their own operations.	<ul style="list-style-type: none"> <li><code>ml.operations.get</code></li> <li><code>ml.operations.cancel</code></li> </ul>

## Permissions needed for training and prediction

For convenience, this table summarizes the permissions that are specifically required for training and prediction:

Task	Required Permission(s)
Training	<ul style="list-style-type: none"> <li><code>ml.jobs.create</code></li> </ul>
Batch prediction	<ul style="list-style-type: none"> <li><code>ml.jobs.create</code></li> <li><code>ml.models.predict*</code></li> <li><code>ml.versions.predict*</code></li> </ul> <p><b>Note:</b> You can create a batch prediction job without a deployed version by specifying the location of a model saved in Google Cloud Storage. This type of batch prediction job requires only the <code>ml.jobs.create</code> permission.</p> <p>To create a batch prediction job that uses a deployed version, you will also need either <code>ml.models.predict</code> or <code>ml.versions.predict</code>, but not both.</p>
Online prediction	<ul style="list-style-type: none"> <li><code>ml.models.predict</code></li> <li><code>ml.versions.predict</code></li> </ul>

## Permissions required for methods

For convenience, this section lists the permissions required to call each method in AI Platform:

Method	Required Permission(s)
<a href="https://cloud.google.com/ml-engine/reference/rest/v1/projects/getConfig">projects.getConfig</a> (https://cloud.google.com/ml-engine/reference/rest/v1/projects/getConfig)	<code>ml.projects.getConfig</code>
<a href="https://cloud.google.com/ml-engine/reference/rest/v1/projects.jobs/cancel">projects.jobs.cancel</a> (https://cloud.google.com/ml-engine/reference/rest/v1/projects.jobs/cancel)	<code>ml.jobs.cancel</code>
<a href="https://cloud.google.com/ml-engine/reference/rest/v1/projects.jobs/create">projects.jobs.create</a> (https://cloud.google.com/ml-engine/reference/rest/v1/projects.jobs/create)	<code>ml.jobs.create</code>  <b>Note:</b> To create a batch prediction job that uses a deployed version, you will also need either <code>ml.models.predict</code> or <code>ml.versions.predict</code> , but not both.
<a href="https://cloud.google.com/ml-engine/reference/rest/v1/projects.jobs/get">projects.jobs.get</a> (https://cloud.google.com/ml-engine/reference/rest/v1/projects.jobs/get)	<code>ml.jobs.get</code>



<u>projects.jobs.list</u> ( <a href="https://cloud.google.com/ml-engine/reference/rest/v1/projects.jobs/list">https://cloud.google.com/ml-engine/reference/rest/v1/projects.jobs/list</a> )	<b>ml.jobs.list</b>
<u>projects.models.create</u> ( <a href="https://cloud.google.com/ml-engine/reference/rest/v1/projects.models/create">https://cloud.google.com/ml-engine/reference/rest/v1/projects.models/create</a> )	<b>ml.models.create</b>
<u>projects.models.delete</u> ( <a href="https://cloud.google.com/ml-engine/reference/rest/v1/projects.models/delete">https://cloud.google.com/ml-engine/reference/rest/v1/projects.models/delete</a> )	<b>ml.models.delete</b>
<u>projects.models.get</u> ( <a href="https://cloud.google.com/ml-engine/reference/rest/v1/projects.models/get">https://cloud.google.com/ml-engine/reference/rest/v1/projects.models/get</a> )	<b>ml.models.get</b>
<u>projects.models.list</u> ( <a href="https://cloud.google.com/ml-engine/reference/rest/v1/projects.models/list">https://cloud.google.com/ml-engine/reference/rest/v1/projects.models/list</a> )	<b>ml.models.list</b>
<u>projects.models.versions.create</u> ( <a href="https://cloud.google.com/ml-engine/reference/rest/v1/projects.models.versions/create">https://cloud.google.com/ml-engine/reference/rest/v1/projects.models.versions/create</a> )	<b>ml.versions.create</b>
<u>projects.models.versions.delete</u> ( <a href="https://cloud.google.com/ml-engine/reference/rest/v1/projects.models.versions/delete">https://cloud.google.com/ml-engine/reference/rest/v1/projects.models.versions/delete</a> )	<b>ml.versions.delete</b>
<u>projects.models.versions.get</u> ( <a href="https://cloud.google.com/ml-engine/reference/rest/v1/projects.models.versions/get">https://cloud.google.com/ml-engine/reference/rest/v1/projects.models.versions/get</a> )	<b>ml.versions.get</b>
<u>projects.models.versions.list</u> ( <a href="https://cloud.google.com/ml-engine/reference/rest/v1/projects.models.versions/list">https://cloud.google.com/ml-engine/reference/rest/v1/projects.models.versions/list</a> )	<b>ml.versions.list</b>
<u>projects.models.versions.setDefault</u> ( <a href="https://cloud.google.com/ml-engine/reference/rest/v1/projects.models.versions/setDefault">https://cloud.google.com/ml-engine/reference/rest/v1/projects.models.versions/setDefault</a> )	<b>ml.models.update</b>
<u>projects.operations.cancel</u> ( <a href="https://cloud.google.com/ml-engine/reference/rest/v1/projects.operations/cancel">https://cloud.google.com/ml-engine/reference/rest/v1/projects.operations/cancel</a> )	<b>ml.operations.cancel</b>
<u>projects.operations.get</u> ( <a href="https://cloud.google.com/ml-engine/reference/rest/v1/projects.operations/get">https://cloud.google.com/ml-engine/reference/rest/v1/projects.operations/get</a> )	<b>ml.operations.get</b>

[projects.operations.list](https://cloud.google.com/ml-engine/reference/rest/v1/projects.operations/list)

(<https://cloud.google.com/ml-engine/reference/rest/v1/projects.operations/list>)

**ml.operations.list**

## Permissions required for storage

When you deploy your trained model on AI Platform to get predictions, you upload your saved model files to Cloud Storage. Within the [Cloud Storage bucket](https://cloud.google.com/storage/docs/key-terms#buckets)

(<https://cloud.google.com/storage/docs/key-terms#buckets>), your model files are *objects* (<https://cloud.google.com/storage/docs/key-terms#objects>). You must ensure that your AI Platform service account can access the files for your trained model in your Cloud Storage bucket.

Grant your AI Platform service account a [Cloud Storage IAM role](https://cloud.google.com/storage/docs/access-control/iam-roles)

(<https://cloud.google.com/storage/docs/access-control/iam-roles>) that includes the following permissions at minimum:

Task	Required Permission(s)	Explanation
Predictionstorage.buckets.list		Allows your AI Platform project to find model files in your Cloud Storage bucket.
Predictionstorage.objects.get		Allows your AI Platform project to read your model files in your Cloud Storage bucket.

See [how to configure Cloud Storage permissions for AI Platform](https://cloud.google.com/ml-engine/docs/working-with-cloud-storage)

(<https://cloud.google.com/ml-engine/docs/working-with-cloud-storage>).

## What's next

- [Learn more about Cloud IAM](https://cloud.google.com/iam/) (<https://cloud.google.com/iam/>).
- [Get an overview of AI Platform](https://cloud.google.com/ml-engine/docs/technical-overview) (<https://cloud.google.com/ml-engine/docs/technical-overview>).

*Except as otherwise noted, the content of this page is licensed under the [Creative Commons Attribution 4.0 License](https://creativecommons.org/licenses/by/4.0/) (<https://creativecommons.org/licenses/by/4.0/>), and code samples are licensed under the [Apache 2.0 License](https://www.apache.org/licenses/LICENSE-2.0)*

(<https://www.apache.org/licenses/LICENSE-2.0>). For details, see our [Site Policies](#) (<https://developers.google.com/terms/site-policies>). Java is a registered trademark of Oracle and/or its affiliates.

*Last updated December 4, 2019.*