>

This guide describes how to use the Security Command Center Security Command Center API to manage security marks. Security marks, or just "marks", are customizable annotations on assets or findings in Security Command Center that allow you to add your own business context to these objects.

Before you can work with security marks, you need to complete the following:

- Set up a service account and SDK (/security-command-center/docs/how-to-programmatic-access)

To add or change security marks, you must have a Cloud Identity and Access Management (Cloud IAM) role that includes permissions for the kind of mark that you want to use:

- Asset marks: **Asset Security Marks Writer**, `securitycenter.assetSecurityMarksWriter`
- Finding marks: **Finding Security Marks Writer**, `securitycenter.findingSecurityMarksWriter`

For more information, see Access control (/security-command-center/docs/access-control) and Using Security Command Center security marks (/security-command-center/docs/how-to-security-marks).

When using the Security Command Center API, adding and updating security marks are the same operation. The example below shows how to add security marks for two key value pairs `(key_a, value_a)` and `(key_b, value_b)`.

The following code uses field masks to ensure that only those values are updated. If field masks aren't provided, all security marks are cleared before adding the given keys and values.

Deleting specific security marks is accomplished in a similar fashion to adding or updating them, specifically calling update with a field mask but without any corresponding value. In the example below, security marks with keys `key_a` and `key_b` are deleted.

The technique to add and update security marks and deleting security marks can be combined into the same request. In the example below, `key_a` is updated while `key_b` is deleted.

Adding, updating, and deleting security marks on findings follows the same process as updating security marks on assets. The only change is the name of the resource used in the API call. Instead of an asset resource, you provide a finding resource name.

For example, to update security marks on a finding, use the following code:

After security marks are set on an asset, they can be used in the filter argument to the `ListAssets` API call. For example, to query for all assets where `key_a = value_a`, use the following code:

After security marks are set on a finding, they can be used in the filter argument to the `ListFindings` API call. For example, to query all assets where `key_a != value_a`, use the following code:

- Learn more about Listing findings (/security-command-center/docs/how-to-api-list-findings) and Listing assets (/security-command-center/docs/how-to-api-list-assets).