

Binary Authorization

Google's BCID (Borg Caller ID)

BCID is an internal tool at Google whose mission is to help ensure that all code running in production is properly reviewed and authorized.

BCID GOAL'S

To ensure that jobs have been “LGTM’d”

BCID’s goals are **Data Protection** and **Change Management**.

Jobs that have access to ***user data***

Internal tool → Customer facing

Binary Authorization



BCID

PROBLEM STATEMENT

How can we ensure that the customer
CI/CD pipeline is used and used
correctly?

Binary Authorization provides deployment control for Google's Container Engine (GKE).

Let's get started on the MVP UX flow.

Security

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Welcome to Binary Authorization

Binary Authorization provides deployment control for Google Kubernetes Engine (GKE). [Learn more](#)



Binary authorization set-up

Define your Binary Authorization policy to restrict the deployment behaviors for this project.

Binary Authorization policy uses previously defined Attestors from the current projects or other projects you have access to.

→ [Configure BinAuthZ policy](#)

→ [Create Attestors](#)

Binary Authorization docs

Learn more about Binary Authorization capabilities and its features.

Check out our quick start Codelab.

→ [View documentation](#)

→ [View Codelab](#)

Security

Binary Authorization

EDIT POLICY

PERMISSIONS

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

POLICY

ATTESTORS

Binary authorization lets you restrict which images can be deployed to a Kubernetes Engine cluster by making sure they pass through the appropriate checkpoints in your deployment workflow. [Learn more](#)

Policy deployment rules

Project default rule

Allow only images that have been approved by all of the following attestors:

- Dev Signer
This is for the dev Signer
- Trusted builder
Centralized secure build pipeline for all production jobs

Cluster-specific rules

Dry run mode

Not enabled

Images exempt from policy

-



Security

Binary Authorization

 [EDIT POLICY](#) [PERMISSIONS](#)

- [Security Command Center](#)
- [Identity-aware proxy](#)
- [Cryptographic keys](#)
- [Binary authorization](#)

[POLICY](#)[ATTESTORS](#)

Binary authorization lets you restrict which images can be deployed to a Kubernetes Engine cluster by making sure they pass through the appropriate checkpoints in your deployment workflow. [Learn more](#)

Policy deployment rules

Project default rule

Allow only images that have been approved by all of the following attestors:

- Dev Signer
This is for the dev Signer
- Trusted builder
Centralized secure build pipeline for all production jobs

Cluster-specific rules

- ClusterFoo

Default: Allow all images

- ClusterBar

Default: Allow all images

- ClusterFB

Attestors required: Dev signer, Prod reviewer

Dry run mode

Not enabled

Images exempt from policy

gcr.io/google-appengine/nodejs*
docker.io/nginx*

Security

Edit policy

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Deployment rules

Applies to this project and all clusters that don't have a cluster-specific rule. When a container image is deployed, a deployment rule will be applied unless the image is exempted as specified in the section below.

Project default rule

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

ADD ATTESTORS

Dry run mode

- Audit log but do not block disallowed images

Cluster-specific rules

Deployment rules for specific clusters. Project default rules won't apply to a cluster if a cluster-specific rule is defined.

Active clusters [3], Cluster rules [0]

Images exempt from deployment rules

Images listed here are exempt from deployment rule checks. Wildcards (*) are allowed in image paths.

Image paths [0]

SAVE POLICY CANCEL

Security

Edit policy

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Deployment rules

Applies to this project and all clusters that don't have a cluster-specific rule. When a container image is deployed, a deployment rule will be applied unless the image is exempted as specified in the section below.

Project default rule

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

ADD ATTESTORS**Dry run mode**

- Audit log but do not block disallowed images

Cluster-specific rules

Deployment rules for specific clusters. Project default rules won't apply to a cluster if a cluster-specific rule is defined.

Active clusters [3], Cluster rules [0]**Images exempt from deployment rules**

Images listed here are exempt from deployment rule checks. Wildcards (*) are allowed in image paths.

Image paths [0]**SAVE POLICY** **CANCEL**

Security

Edit policy

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Deployment rules

Applies to this project and all clusters that don't have a cluster-specific rule. When a container image is deployed, a deployment rule will be applied unless the image is exempted as specified in the section below.

Project default rule

- Allow all images
- Disallow all images
- Allow only images that have been signed by:

[ADD ATTESTORS](#)

Dry run mode

- Audit log but do not block disallow

Cluster-specific rules

Deployment rules for specific clusters

[Active clusters \[3\], Cluster rules \[0\]](#)

Images exempt from deployment rules

Images listed here are exempt from deployment rules

[Image paths \[0\]](#)[SAVE POLICY](#) [CANCEL](#)

Add attestors

Attestors have the authority to make statements about an image. [Learn more](#)

Attestors	Description
<input type="checkbox"/> custom approver	This is a new attester
<input checked="" type="checkbox"/> Trusted Builder	Centralized secure build pipeline for all production jobs
<input type="checkbox"/> QA Signer	Team performs functionality tests and integration tests
<input checked="" type="checkbox"/> Dev Signer	This is for the dev Signer
<input type="checkbox"/> Legal	Legal team reviews for policy violations
<input type="checkbox"/> Prod reviewer	Reviews for production readiness
<input type="checkbox"/> Sec scanner	Security scanner for known vulnerabilities

[+ CREATE NEW ATTESTOR](#)[CANCEL](#) [ADD 2 ATTESTORS](#)

Security

Edit policy

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Deployment rules

Applies to this project and all clusters that don't have a cluster-specific rule. When a container image is deployed, a deployment rule will be applied unless the image is exempted as specified in the section below.

Project default rule

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

Approvers	Description	Action
	Trusted Builder	This is for the Trusted Builder
	Dev Signer	This is for the dev Signer

[ADD ATTESTORS](#)

Dry run mode

- Audit log but do not block disallowed images

Cluster-specific rules

Deployment rules for specific clusters. Project default rules won't apply to a cluster if a cluster-specific rule is defined.

Active clusters [3], Cluster rules [0]



Images exempt from deployment rules

Images listed here are exempt from deployment rule checks. Wildcards (*) are allowed in image paths.

Image paths [0]



[SAVE POLICY](#)

CANCEL

- Cryptographic keys
- Binary authorization

be applied unless the image is exempted as specified in the section below.

Project default rule [?](#)

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

Approvers	Description	
<input checked="" type="checkbox"/> Trusted Builder	This is for the Trusted Builder	'Add' pending
<input checked="" type="checkbox"/> Dev Signer	This is for the dev Signer	'Add' pending

[ADD ATTESTORS](#)

Dry run mode [?](#)

- Audit log but do not block disallowed images

Cluster-specific rules

Deployment rules for specific clusters. Project default rules won't apply to a cluster if a cluster-specific rule is defined.

Filter clusters		
Name	Rule description	
Binary Authorization enabled	<input checked="" type="checkbox"/> ClusterFoo Default: Allow all images	
	<input checked="" type="checkbox"/> ClusterBar Default: Allow all images	
	<input checked="" type="checkbox"/> ClusterFB Default: Allow all images	
No GKE cluster of that name	<input type="checkbox"/> SomeCluster -	
	<input type="checkbox"/> Cluster01 -	
	<input type="checkbox"/> Cluster02 -	
Binary Authorization disabled	<input type="checkbox"/> Cluster03 -	
+ ADD CLUSTER SPECIFIC RULE		

Edit

Delete

Enable in GKE console

Images exempt from deployment rules

Images listed here are exempt from deployment rule checks. Wildcards (*) are allowed in image paths.

Image paths [0]

[SAVE POLICY](#)

[CANCEL](#)

- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Applying this project-level rule will prevent a container image from being deployed if deployment rules can't be applied unless the image is exempted as specified in the section below.

Project default rule [?](#)

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

Approvers	Description	
<input checked="" type="checkbox"/> Trusted Builder	This is for the Trusted Builder	'Add' pending
<input checked="" type="checkbox"/> Dev Signer	This is for the dev Signer	'Add' pending

[ADD ATTESTORS](#)

Dry run mode [?](#)

- Audit log but do not block

Cluster-specific rules

Deployment rules for specific clusters

[Filter clusters](#)

Name

ClusterFoo

ClusterBar

ClusterFB

SomeCluster

Cluster01

Cluster02

Cluster03

[+ ADD CLUSTER SPEC](#)

Images exempt from deployment

Images listed here are exempt from deployment rule checks. Wildcards (*) are allowed in image paths.

Image paths [0]

[CANCEL](#) [ADD](#)

[SAVE POLICY](#) [CANCEL](#)

- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Applying this project-level rule will result in a container image being deployed to a deployment target unless it is exempted.

Project default rule [?](#)

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

Approvers	Description	Action
<input checked="" type="checkbox"/> Trusted Builder	This is for the Trusted Builder	'Add' pending
<input checked="" type="checkbox"/> Dev Signer	This is for the dev Signer	'Add' pending

[ADD ATTESTORS](#)

Dry run mode [?](#)

- Audit log but do not block

Cluster-specific rules

Deployment rules for specific clusters

Filter clusters

Name

ClusterFoo

ClusterBar

ClusterFB

SomeCluster

Cluster01

Cluster02

Cluster03

[+ ADD CLUSTER SPEC](#)

Images exempt from deployment

Images listed here are exempt from deployment rule checks. Wildcards (*) are allowed in image paths.

Image paths [0]

[SAVE POLICY](#) [CANCEL](#)

Edit cluster specific rule for ClusterFB

Project default rules [?](#)

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

Filter attestors

Attestors

Attestors	Description
<input type="checkbox"/> custom approver	This is a new attester
<input type="checkbox"/> Trusted Builder	Centralized secure build pipeline for all production jobs
<input type="checkbox"/> QA Signer	Team performs functionality tests and integration tests
<input checked="" type="checkbox"/> Dev Signer	This is for the dev Signer
<input type="checkbox"/> Legal	Legal team reviews for policy violations
<input checked="" type="checkbox"/> Prod reviewer	Reviews for production readiness
<input type="checkbox"/> Sec scanner	Security scanner for known vulnerabilities

[+ CREATE NEW ATTESTOR](#)

Dry run mode [?](#)

- Audit log but do not block disallowed images

[CANCEL](#) [ADD](#)

- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Applies to this project and all clusters that don't have a cluster-specific rule. When a container image is deployed, a deployment rule will be applied unless the image is exempted as specified in the section below.

Project default rule [?](#)

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

Approvers	Description	Add pending	Remove
<input checked="" type="checkbox"/> Trusted Builder	This is for the Trusted Builder	'Add' pending	
<input checked="" type="checkbox"/> Dev Signer	This is for the dev Signer	'Add' pending	

[ADD ATTESTORS](#)

Dry run mode [?](#)

- Audit log but do not block disallowed images

Cluster-specific rules

Deployment rules for specific clusters. Project default rules won't apply to a cluster if a cluster-specific rule is defined.

Filter clusters

Name	Rule description	⋮
<input checked="" type="checkbox"/> ClusterFoo	Default: Allow all images	
<input checked="" type="checkbox"/> ClusterBar	Default: Allow all images	
<input checked="" type="checkbox"/> ClusterFB	Attestors required: Dev signer, Prod reviewer	
⚠ SomeCluster	-	
⚠ Cluster01	-	
❗ Cluster02	-	
❗ Cluster03	-	

[Edit](#)
[Delete](#)
[Enable in GKE console](#)

[+ ADD CLUSTER SPECIFIC RULE](#)

Images exempt from deployment rules

Images listed here are exempt from deployment rule checks. Wildcards (*) are allowed in image paths.

Image paths [0]

[SAVE POLICY](#) [CANCEL](#)

- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Applied to this project and all clusters that don't have a cluster-specific rule. When a container image is deployed, a deployment rule will be applied unless the image is exempted as specified in the section below.

Project default rule [?](#)

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

Approvers	Description	Add pending	Remove
<input checked="" type="checkbox"/> Trusted Builder	This is for the Trusted Builder	'Add' pending	
<input checked="" type="checkbox"/> Dev Signer	This is for the dev Signer	'Add' pending	

[ADD ATTESTORS](#)

Dry run mode [?](#)

- Audit log but do not block deployment

Cluster-specific rules

Deployment rules for specific clusters

[Filter clusters](#)

Name	Rule	⋮
<input checked="" type="checkbox"/> ClusterFoo	Default: Allow all images	
<input checked="" type="checkbox"/> ClusterBar	Default: Allow all images	
<input checked="" type="checkbox"/> ClusterFB	Attestors required: Dev signer, Prod reviewer	
<input checked="" type="checkbox"/> SomeCluster	-	
<input checked="" type="checkbox"/> Cluster01	-	
<input checked="" type="checkbox"/> Cluster02	-	
<input checked="" type="checkbox"/> Cluster03	-	

[+ ADD CLUSTER SPECIFIC RULE](#)

[CLOSE](#) [REMOVE](#)

Remove deployment rule override for ClusterFB

Removing this override will remove the requirement of having approvers authorize on this cluster and revert back to the default deployment rule which will always allow all images.

Images exempt from deployment rules

Images listed here are exempt from deployment rule checks. Wildcards (*) are allowed in image paths.

Image paths [0]



[SAVE POLICY](#) [CANCEL](#)

- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Applies to this project and all clusters that don't have a cluster-specific rule. When a container image is deployed, a deployment rule will be applied unless the image is exempted as specified in the section below.

Project default rule ⓘ

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

Approvers	Description	Add pending	Remove
	Trusted Builder	This is for the Trusted Builder	'Add' pending
	Dev Signer	This is for the dev Signer	'Add' pending

[ADD ATTESTORS](#)

Dry run mode ⓘ

- Audit log but do not block disallowed images

Cluster-specific rules

Deployment rules for specific clusters. Project default rules won't apply to a cluster if a cluster-specific rule is defined.

Filter clusters	
Name	Rule description
	ClusterFoo Default: Allow all images
	CusterBar Default: Allow all images
	ClusterFB Default: Allow all images
	SomeCluster -
	Cluster01 -
	Cluster02 -
	Cluster03 -

[+ ADD CLUSTER SPECIFIC RULE](#)

Images exempt from deployment rules

Images listed here are exempt from deployment rule checks. Wildcards (*) are allowed in image paths.

Image paths [0]

[SAVE POLICY](#) [CANCEL](#)

- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Applies to this project and all clusters that don't have a cluster-specific rule. When a container image is deployed, a deployment rule will be applied unless the image is exempted as specified in the section below.

Project default rule ⓘ

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

Approvers	Description	'Add' pending	trash
	Trusted Builder	This is for the Trusted Builder	
	Dev Signer	This is for the dev Signer	

[ADD ATTESTORS](#)

Dry run mode ⓘ

- Audit log but do not block disallowed images

Cluster-specific rules

Deployment rules for specific clusters. Project default rules won't apply to a cluster if a cluster-specific rule is defined.

Active clusters [3], Cluster rules [1]

'Add' pending

Images exempt from deployment rules

Images listed here are exempt from deployment rule checks. Wildcards (*) are allowed in image paths.

Image path	^	
gcr.io/google-appengine/nodejs*		
docker.io/nginx*		

[+ ADD IMAGE PATH](#)

[SAVE POLICY](#) [CANCEL](#)

- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Applies to this project and all clusters that don't have a cluster-specific rule. When a container image is deployed, a deployment rule will be applied unless the image is exempted as specified in the section below.

Project default rule ⓘ

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

Approvers	Description	'Add' pending	trash
<input checked="" type="checkbox"/> Trusted Builder	This is for the Trusted Builder	'Add' pending	trash
<input checked="" type="checkbox"/> Dev Signer	This is for the dev Signer	'Add' pending	trash

[ADD ATTESTORS](#)

Dry run mode ⓘ

- Audit log but do not block disallowed images

Cluster-specific rules

Deployment rules for specific clusters. Project default rules won't apply to a cluster if a cluster-specific rule is defined.

Active clusters [3], Cluster rules [1]

'Add' pending ▾

Images exempt from deployment rules

Images listed here are exempt from deployment rule checks. Wildcards (*) are allowed in image paths.

Image path	edit	trash
gcr.io/google-appengine/nodejs*	edit	trash
docker.io/nginx*	edit	trash
gcr.io/testlabs/payment@sha256:aba48d60ba4410ec921f9d2e816	edit	trash

[+ ADD IMAGE PATH](#)

[SAVE POLICY](#) [CANCEL](#)

- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Applies to this project and all clusters that don't have a cluster-specific rule. When a container image is deployed, a deployment rule will be applied unless the image is exempted as specified in the section below.

Project default rule ⓘ

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

Approvers	Description	'Add' pending	trash
<input checked="" type="checkbox"/> Trusted Builder	This is for the Trusted Builder	'Add' pending	trash
<input checked="" type="checkbox"/> Dev Signer	This is for the dev Signer	'Add' pending	trash

[ADD ATTESTORS](#)

Dry run mode ⓘ

- Audit log but do not block disallowed images

Cluster-specific rules

Deployment rules for specific clusters. Project default rules won't apply to a cluster if a cluster-specific rule is defined.

Active clusters [3], Cluster rules [1]

'Add' pending ▾

Images exempt from deployment rules

Images listed here are exempt from deployment rule checks. Wildcards (*) are allowed in image paths.

Image path	'Add' pending	trash
gcr.io/google-appengine/nodejs*	'Add' pending	trash
docker.io/nginx*	'Add' pending	trash
gcr.io/testlabs/payment@sha256:aba48d60ba...	'Add' pending	trash

[+ ADD IMAGE PATH](#)

[SAVE POLICY](#) CANCEL

- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Applied to this project and all clusters that don't have a cluster-specific rule. When a container image is deployed, a deployment rule will be applied unless the image is exempted as specified in the section below.

Project default rule [?](#)

- Allow all images
- Disallow all images
- Allow only images that have been approved by all of the following attestors

Approvers	Description	Action
 Trusted Builder	This is for the Trusted Builder	'Add' pending 
 Dev Signer	This is for the dev Signer	'Add' pending 

[ADD ATTESTORS](#)

Dry run mode [?](#)

- Audit log but do not block deployment

Cluster-specific rules

Deployment rules for specific clusters

Active clusters [3], Cluster rules

Images exempt from deployment rule checks

Images listed here are exempt from deployment rule checks. Wildcards (*) are allowed in image paths.

[LEAVE](#) [STAY](#)

Image path

gcr.io/google-appengine/nodejs*	 
docker.io/nginx*	 
gcr.io/testlabs/payment@sha256:aba48d60ba...	'Add' pending  

[+ ADD IMAGE PATH](#)

[SAVE POLICY](#) [CANCEL](#)

Security

Binary Authorization

CREATE ATTESTOR

PERMISSIONS

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

POLICY

ATTESTORS

Attestors have the authority to make statements about an image. [Learn more](#)

Filter attestors

<input type="checkbox"/>	Name	Description	Public Keys	Last Updated
--------------------------	------	-------------	-------------	--------------

Security

Binary Authorization

CREATE ATTESTOR

PERMISSIONS

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

POLICY

ATTESTORS

Attestors have the authority to make statements about an image. [Learn more](#)

Filter attestors

<input type="checkbox"/>	Name	Description	Public Keys	Last Updated	
<input type="checkbox"/>	Trusted Builder	This is for the Trusted Builder	1	April 1, 2018 - 8:00 AM	
<input type="checkbox"/>	Dev Signer	This is for the Dev Signer	1	April 1, 2018 - 8:00 AM	

Security

← Create attester

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Attestors have the authority to make statements about an image. [Learn more](#)

Attestor name

Make sure that your name is easy to identify.

 Create default analysis note ②

A corresponding note needs to be created in Container Analysis directly prior to creating an attester in Binary Authorization. [Learn more](#)

Container analysis note name ②

Description (Optional)

The description is shown during rule setup to provide additional context for attestors.

PGP public keys ②

Learn more about key generation and how to set one up. [Learn more](#)

Add a PGP public key



Name (optional)

PASTE KEY or UPLOAD KEY

DONE

CANCEL

ADD KEY

CREATE

CANCEL

Security

← Create attester

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Attestors have the authority to make statements about an image. [Learn more](#)

Attector name

QA

Make sure that your name is easy to identify.

 Create default analysis note ②

A corresponding note needs to be created in Container Analysis directly prior to creating an attector in Binary Authorization. [Learn more](#)

Container analysis note name ②

Description (Optional)

This is the QA team

The description is shown during rule setup to provide additional context for attestors.

PGP public keys ②

Learn more about key generation and how to set one up. [Learn more](#)

Add a PGP public key



Name (optional)

Key version 1.0.0

PASTE KEY or UPLOAD KEY

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: BCPG C# v1.6.1.0

IAjwlker83lkjslkjfIakjsldkfjlkjklakjsdlkfjlkallsllsllsllkdfjsf13120893a

DONE

CANCEL

ADD KEY

CREATE

CANCEL

Security

Binary Authorization

CREATE ATTESTOR

PERMISSIONS

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

POLICY

ATTESTORS

Attestors have the authority to make statements about an image. [Learn more](#)

Filter attestors

<input type="checkbox"/>	Name	Description	Public Keys	Last Updated	
<input type="checkbox"/>	QA	This is the QA team	2	April 1, 2018 - 8:00 AM	
<input type="checkbox"/>	Trusted Builder	This is for the Trusted Builder	1	April 1, 2018 - 8:00 AM	
<input type="checkbox"/>	Dev Signer	This is for the Dev Signer	1	April 1, 2018 - 8:00 AM	

 Security["QA" attester](#)

EDIT

DELETE

DISABLE

 Security Command Center

Attestor name

QA

 Identity-aware proxy

Container analysis note name

projects/some_project/notes/some_note

 Cryptographic keys

Description (optional)

This is the QA team

 Binary authorization

Public keys

Name: Key version 1.0.0 ID: 5252E2D910...

Name: legal change ID: 728282D910...

Security

← "QA" attester

EDIT

DELETE

DISABLE

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

Attestor name

QA

Container analysis note name

projects/some_project/notes/some_note

Description (optional)

This is the QA team

Public keys

Name: Key version 1.0.0 — ID: 5252E2D910...

Pending deletion UNDO

Name: legal change

ID: 728282D910...



SAVE CHANGES

CANCEL

■ Security

← “QA” attestor

 EDIT

 DELETE

 DISABLE

- Security Command Center
 - Identity-aware proxy
 - Cryptographic keys
 - Binary authorization

Attestor name [?](#)

QA

Container analysis note name

projects/some_project/notes/some_note

Description (optional) [?](#)

This is the QA team

Public keys

ID: 5252F2D91C

[View Details](#)

-----BEGIN PGP PUBLIC K

IAjwlker83lkjlskjf;lkjlsdkfjjlkjklakjsdlkfjlkallslsllsldkfjsf13120893aoiu7
833nbskksfh19920709833nbskksfh19920709IAjwlker83lkjlskjf;lakjsldkfj

NEXT

CANCEI

Name: legal changes

ID: 728282D910

SAVE CHANGES

CANCELLATION

Security

Binary Authorization

CREATE ATTESTOR

PERMISSIONS

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

POLICY

ATTESTORS

Attestors have the authority to make statements about an image. [Learn more](#)

Filter attestors

<input type="checkbox"/>	Name	Description	Public Keys	Last Updated	
<input type="checkbox"/>	QA	This is the QA team	2	April 1, 2018 - 8:00 AM	
<input type="checkbox"/>	Trusted Builder	This is for the Trusted Builder	1	April 1, 2018 - 8:00 AM	
<input type="checkbox"/>	Dev Signer	This is for the Dev Signer	1	April 1, 2018 - 8:00 AM	 Edit Disable Delete

Security

Binary Authorization

CREATE ATTESTOR

PERMISSIONS

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

POLICY

ATTESTORS

Attestors have the authority to make statements about an image. [Learn more](#)

Filter attestors

<input type="checkbox"/>	Name	Description	Public Keys	Last Updated	
<input type="checkbox"/>	QA	This is the QA team	2	April 1, 2018 - 8:00 AM	
<input type="checkbox"/>	Trusted Builder	This is for the Trusted Builder	1	April 1, 2018 - 8:00 AM	
<input type="checkbox"/>	Dev Signer			April 1, 2018 - 8:00 AM	

Disable "Dev Signer" attestor

 Disabling this attestor will affect your policy if it's part of your deployment rule

Are you sure you want to disable?

[CLOSE](#) [YES, DISABLE](#)

Security

Binary Authorization

CREATE ATTESTOR

PERMISSIONS

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

POLICY

ATTESTORS

Attestors have the authority to make statements about an image. [Learn more](#)

Filter attestors

<input type="checkbox"/>	Name	Description	Public Keys	Last Updated	
<input type="checkbox"/>	QA	This is the QA team	2	April 1, 2018 - 8:00 AM	
<input type="checkbox"/>	Trusted Builder	This is for the Trusted Builder	1	April 1, 2018 - 8:00 AM	
<input type="checkbox"/>	Dev Signer	This is for the Dev Signer	1	April 1, 2018 - 8:00 AM	

Security

Binary Authorization

CREATE ATTESTOR

PERMISSIONS

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

POLICY

ATTESTORS

Attestors have the authority to make statements about an image. [Learn more](#)

Filter attestors

X | C |

<input type="checkbox"/>	Name	Description	Public Keys	Last Updated	
<input type="checkbox"/>	QA	This is the QA team	2	April 1, 2018 - 8:00 AM	
<input type="checkbox"/>	Trusted Builder	This is for the Trusted Builder	1	April 1, 2018 - 8:00 AM	
<input type="checkbox"/>	Dev Signer	This is for the Dev Signer	1	April 1, 2018 - 8:00 AM	

- [Edit](#)
- [Enable](#)
- [Delete](#)

Security

Binary Authorization

CREATE ATTESTOR

PERMISSIONS

Security Command Center

POLICY

ATTESTORS

Identity-aware proxy

Cryptographic keys

Binary authorization

Filter attestors

<input type="checkbox"/>	Name	Description	Public Keys	Last Updated	
<input type="checkbox"/>	QA	This is the QA team	2	April 1, 2018 - 8:00 AM	
<input type="checkbox"/>	Trusted Builder			18 - 8:00 AM	
<input type="checkbox"/>	Dev Signer			18 - 8:00 AM	

Delete "Dev Signer" approver

 Deleting this approver may potentially affect your policy.

Deleting "Dev Signer" is permanent. Consider disabling this approver as an alternative.

CLOSE

DELETE

Security

Binary Authorization

CREATE ATTESTOR

PERMISSIONS

- Security Command Center
- Identity-aware proxy
- Cryptographic keys
- Binary authorization

POLICY

ATTESTORS

Attestors have the authority to make statements about an image. [Learn more](#)

Filter attestors

<input type="checkbox"/>	Name	Description	Public Keys	Last Updated	
<input type="checkbox"/>	QA	This is the QA team	2	April 1, 2018 - 8:00 AM	
<input type="checkbox"/>	Trusted Builder	This is for the Trusted Builder	1	April 1, 2018 - 8:00 AM	