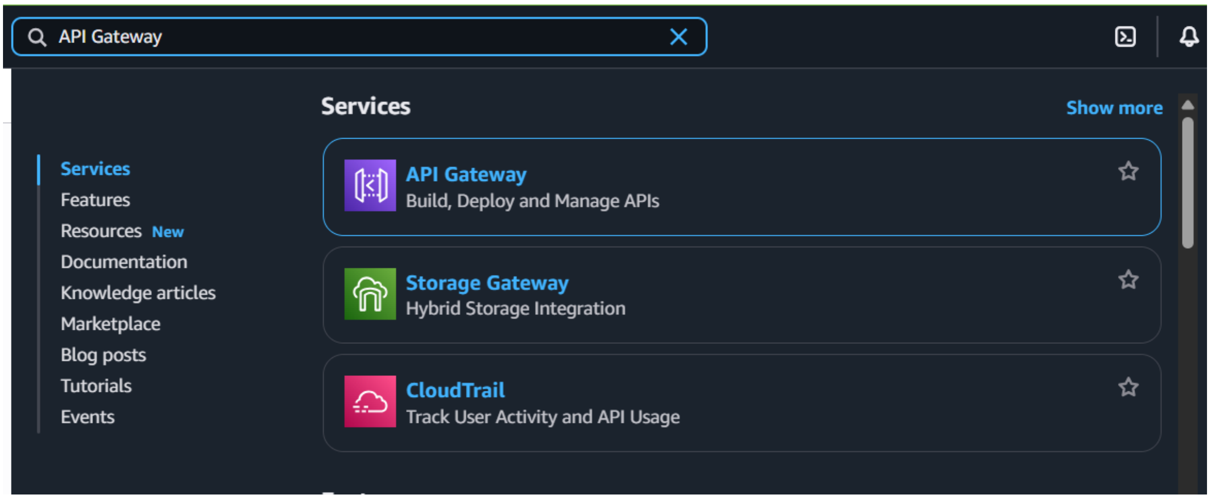
Day 31

“CLOUD SECURITY”

Implementing web application firewalls in AWS:

Steps:

First, we will create a web API in AWS, for which we need to go to API Gateway:

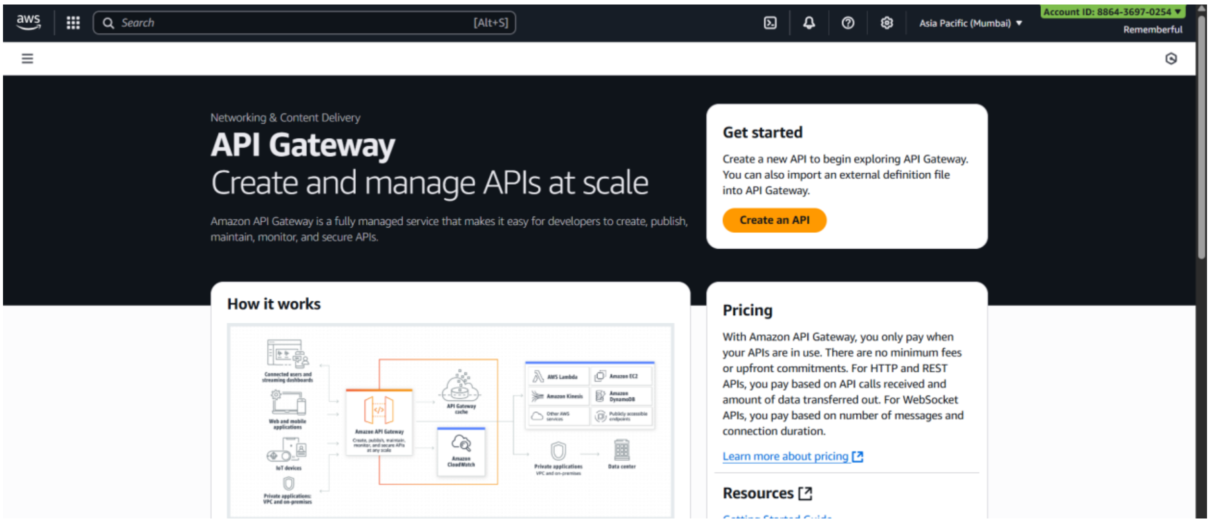


API Gateway
Build, Deploy and Manage APIs

Storage Gateway
Hybrid Storage Integration

CloudTrail
Track User Activity and API Usage

Following window will appear:



Networking & Content Delivery

API Gateway

Create and manage APIs at scale

Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs.

Get started

Create a new API to begin exploring API Gateway. You can also import an external definition file into API Gateway.

Create an API

How it works

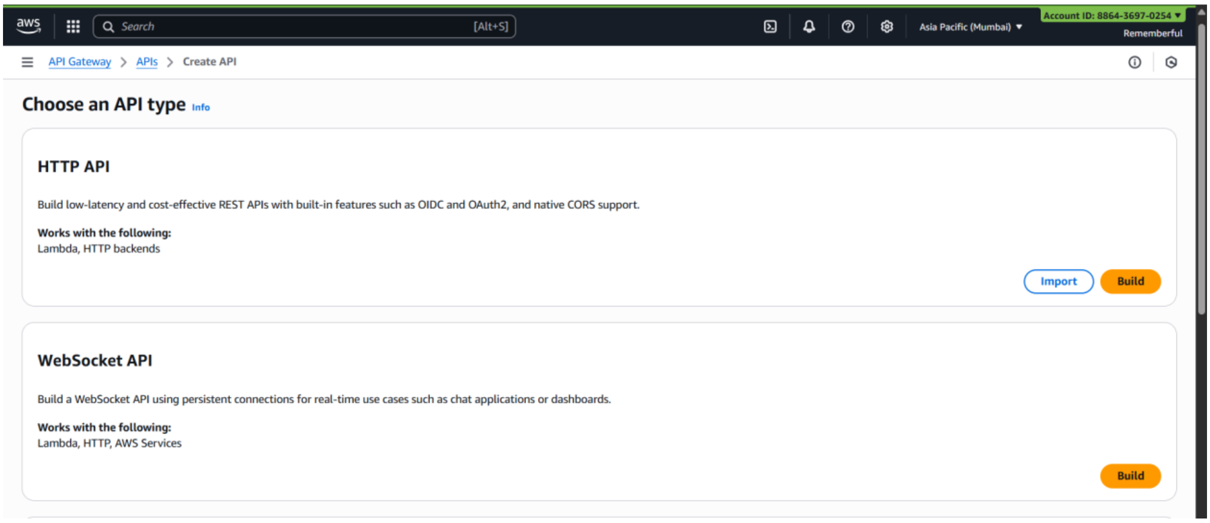
Pricing

With Amazon API Gateway, you only pay when your APIs are in use. There are no minimum fees or upfront commitments. For HTTP and REST APIs, you pay based on API calls received and amount of data transferred out. For WebSocket APIs, you pay based on number of messages and connection duration.

Learn more about pricing

Resources

Click on the “Create an API” button: following window will appear.



Choose an API type Info

HTTP API

Build low-latency and cost-effective REST APIs with built-in features such as OIDC and OAuth2, and native CORS support.

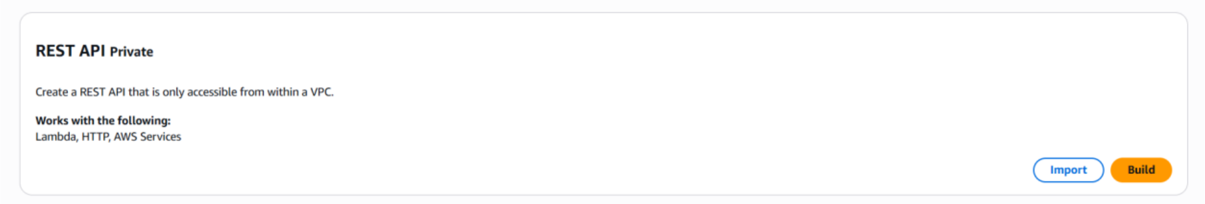
Works with the following:
Lambda, HTTP backends

WebSocket API

Build a WebSocket API using persistent connections for real-time use cases such as chat applications or dashboards.

Works with the following:
Lambda, HTTP, AWS Services

We will create a REST API Private, so scroll down and click on the “Build” button at the REST API private section:

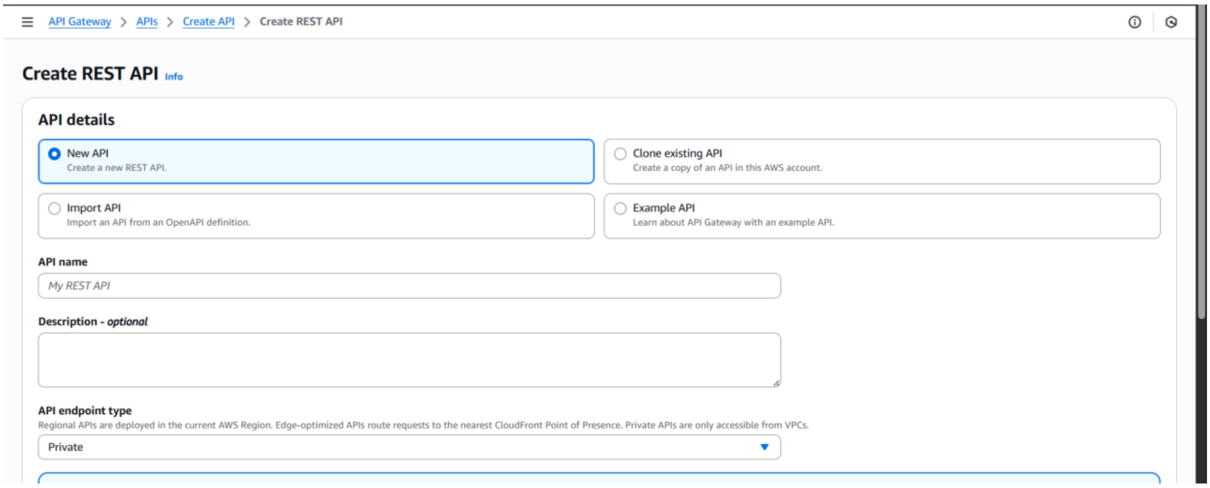


REST API Private

Create a REST API that is only accessible from within a VPC.

Works with the following:
Lambda, HTTP, AWS Services

Following window will appear:



Create REST API Info

API details

● New API
Create a new REST API.

○ Clone existing API
Create a copy of an API in this AWS account.

○ Import API
Import an API from an OpenAPI definition.

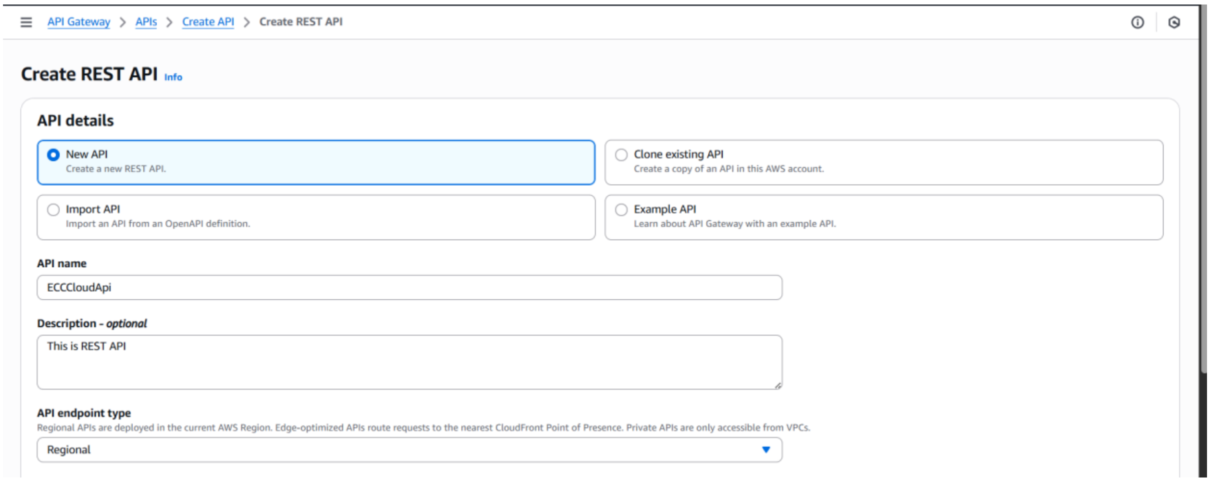
○ Example API
Learn about API Gateway with an example API.

API name
My REST API

Description - *optional*

API endpoint type
Regional APIs are deployed in the current AWS Region. Edge-optimized APIs route requests to the nearest CloudFront Point of Presence. Private APIs are only accessible from VPCs.
Private ▾

Make changes, as shown or as per the requirement:



API Gateway > APIs > Create API > Create REST API

Create REST API Info

API details

● New API
Create a new REST API.

○ Clone existing API
Create a copy of an API in this AWS account.

○ Import API
Import an API from an OpenAPI definition.

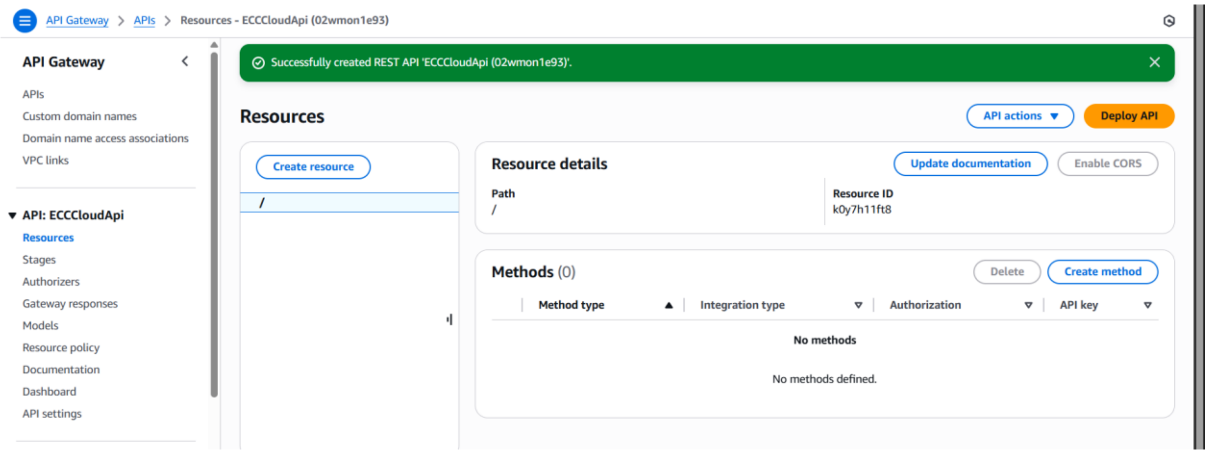
○ Example API
Learn about API Gateway with an example API.

API name
ECCCloudApi

Description - *optional*
This is REST API

API endpoint type
Regional APIs are deployed in the current AWS Region. Edge-optimized APIs route requests to the nearest CloudFront Point of Presence. Private APIs are only accessible from VPCs.
Regional

Following confirmation will occur:



API Gateway > APIs > Resources - ECCCloudApi (02wmon1e93)

Successfully created REST API 'ECCCloudApi (02wmon1e93)'.

Resources

Resource details

Path: /

Resource ID: k0y7h11ft8

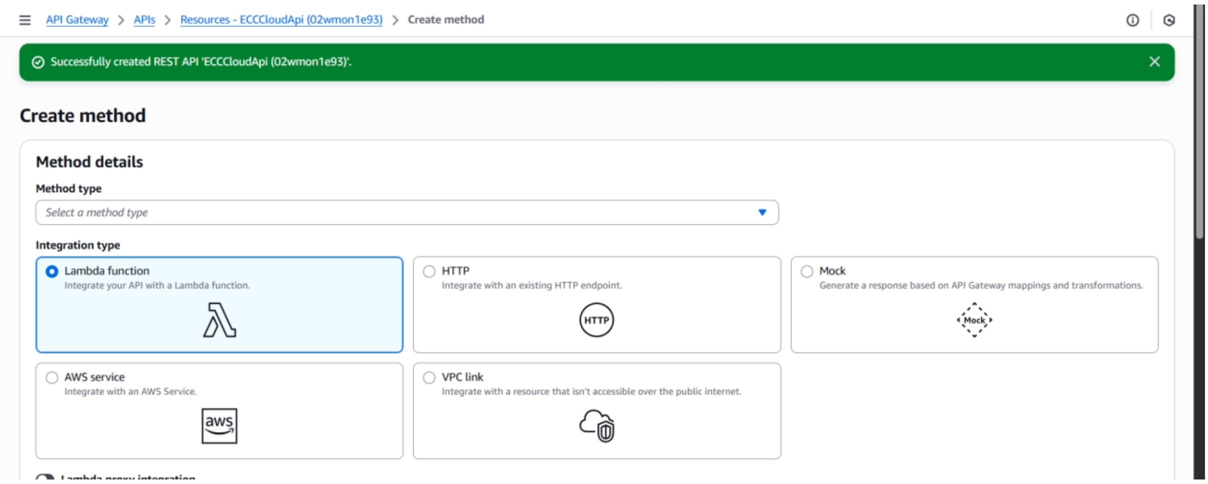
Methods (0)

Method type	Integration type	Authorization	API key

No methods

No methods defined.

Click on the “Create Method” button as shown above:



API Gateway > APIs > Resources - ECCCloudApi (02wmon1e93) > Create method

Successfully created REST API 'ECCCloudApi (02wmon1e93)'.

Create method

Method details

Method type
Select a method type

Integration type

● Lambda function
Integrate your API with a Lambda function.

○ HTTP
Integrate with an existing HTTP endpoint.

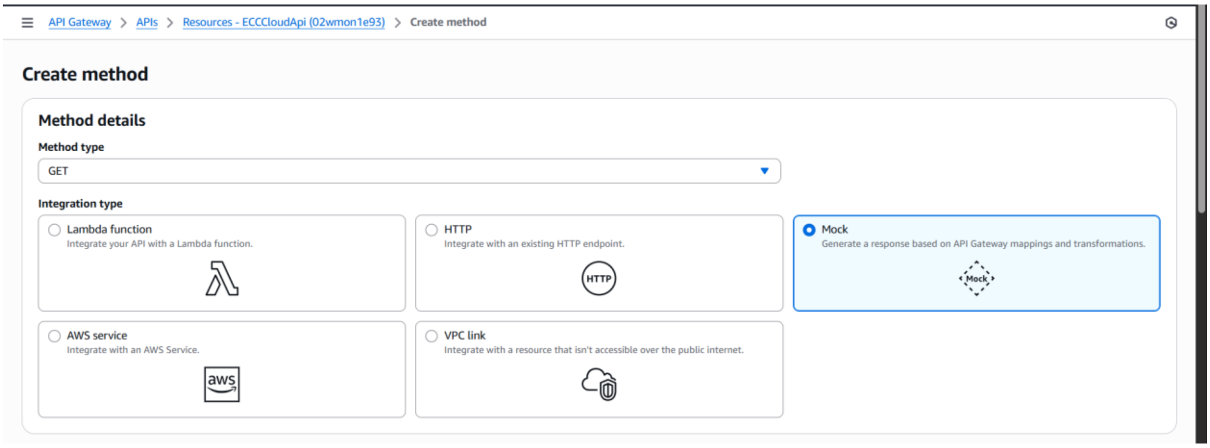
○ Mock
Generate a response based on API Gateway mappings and transformations.

○ AWS service
Integrate with an AWS Service.

○ VPC link
Integrate with a resource that isn't accessible over the public internet.

Lambda proxy integration

Change the options as shown below:


API Gateway > APIs > Resources - ECCCloudApi (02wmon1e93) > Create method
Lambda function
HTTP
AWS service
VPC link
Mock
aws

Create method

Method details

Method type: GET

Integration type:

○ Lambda function
Integrate your API with a Lambda function.

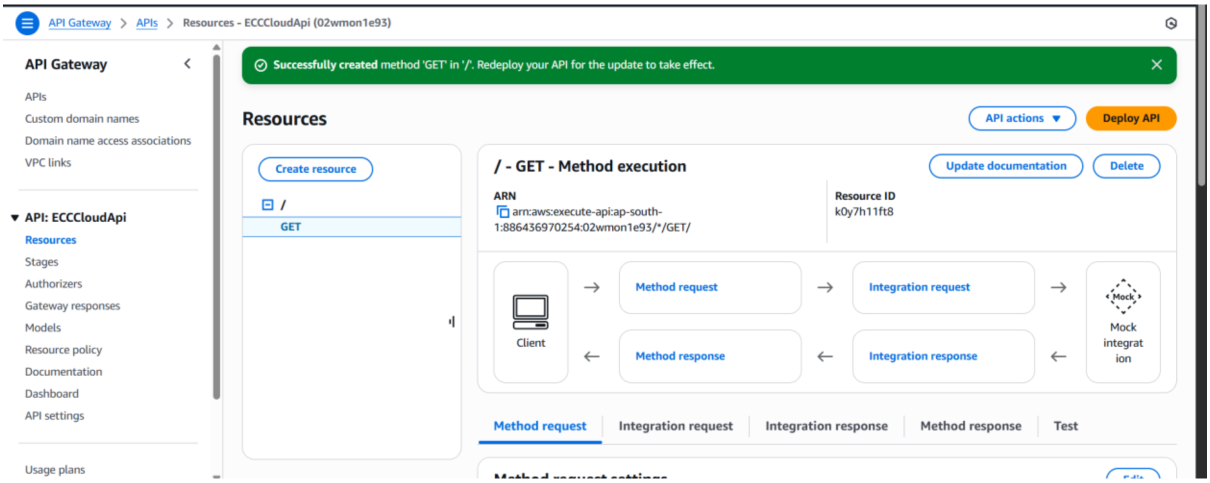
○ HTTP
Integrate with an existing HTTP endpoint.

● Mock
Generate a response based on API Gateway mappings and transformations.

○ AWS service
Integrate with an AWS Service.

○ VPC link
Integrate with a resource that isn't accessible over the public internet.

After this, click on the orange button given below, following confirmation will occur:



Successfully created method 'GET' in '/'. Redeploy your API for the update to take effect.

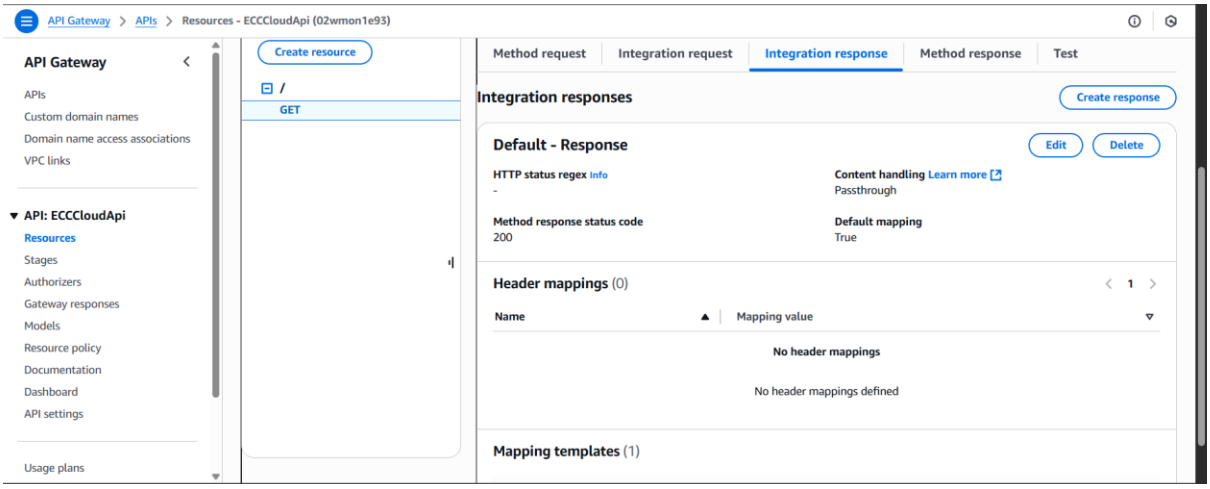
/ - GET - Method execution

ARN: arn:aws:execute-api:ap-south-1:886436970254:02wmon1e93/*/GET/

Resource ID: k0y7h11ft8

Method request settings

Now, click on the “integration responses” section: following option should occur.



Integration responses

Default - Response

HTTP status regex Info: -

Content handling Learn more: Passthrough

Method response status code: 200

Default mapping: True

Header mappings (0)

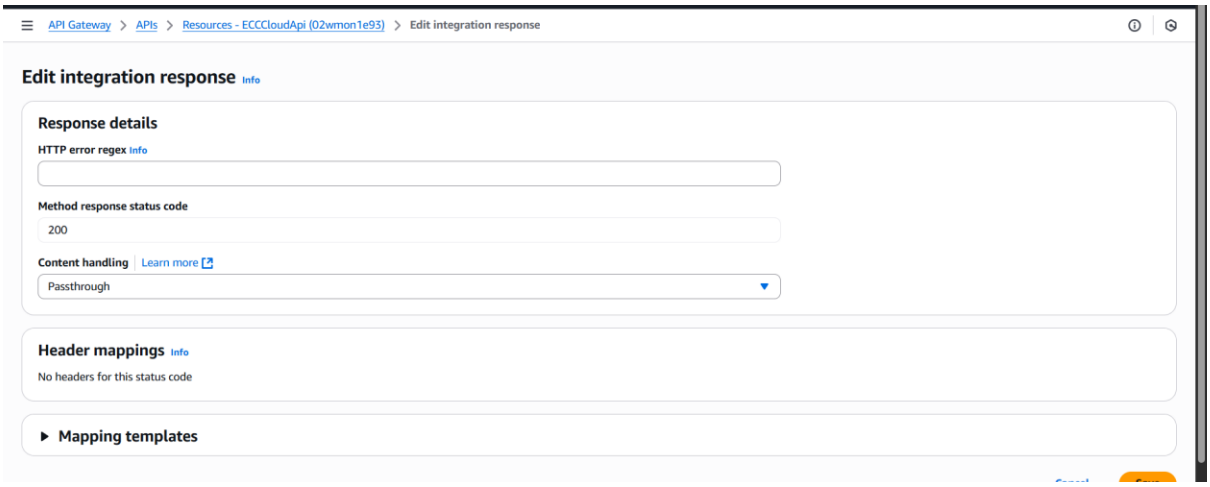
Name	Mapping value

No header mappings

No header mappings defined

Mapping templates (1)

Click on the “edit” button: following window will appears.


API Gateway > APIs > Resources - ECCCloudApi (02wmon1e93) > Edit integration response
Info
Cancel
Save

Edit integration response

Response details

HTTP error regex

Method response status code: 200

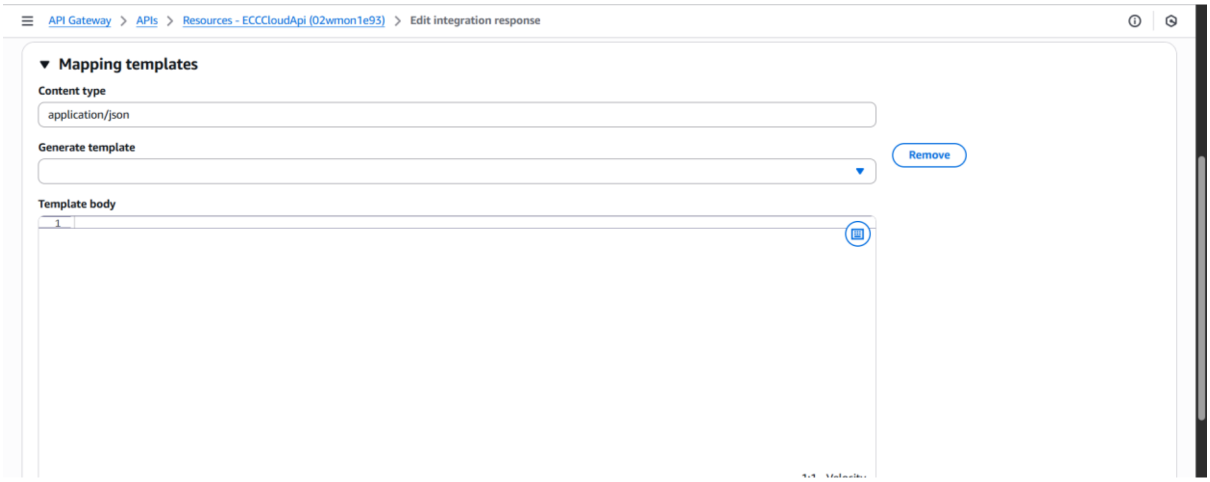
Content handling: Passthrough

Header mappings

No headers for this status code

Mapping templates

Click on the “Mapping Templates” option:


API Gateway > APIs > Resources - ECCCloudApi (02wmon1e93) > Edit integration response
Remove
1:1 Velocity

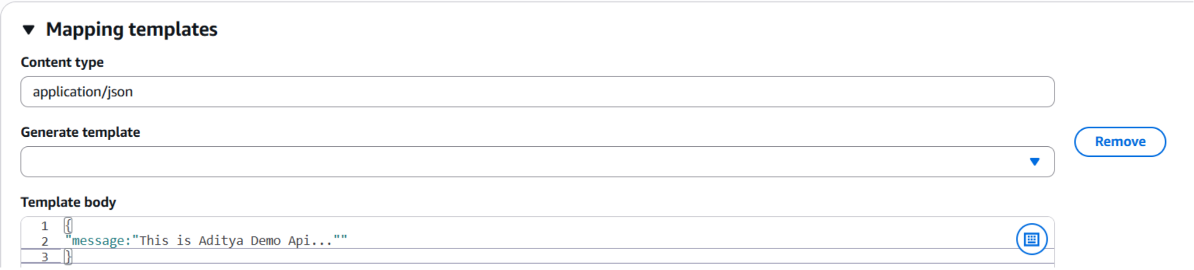
Mapping templates

Content type: application/json

Generate template

Template body

Type the following as shown:



Mapping templates

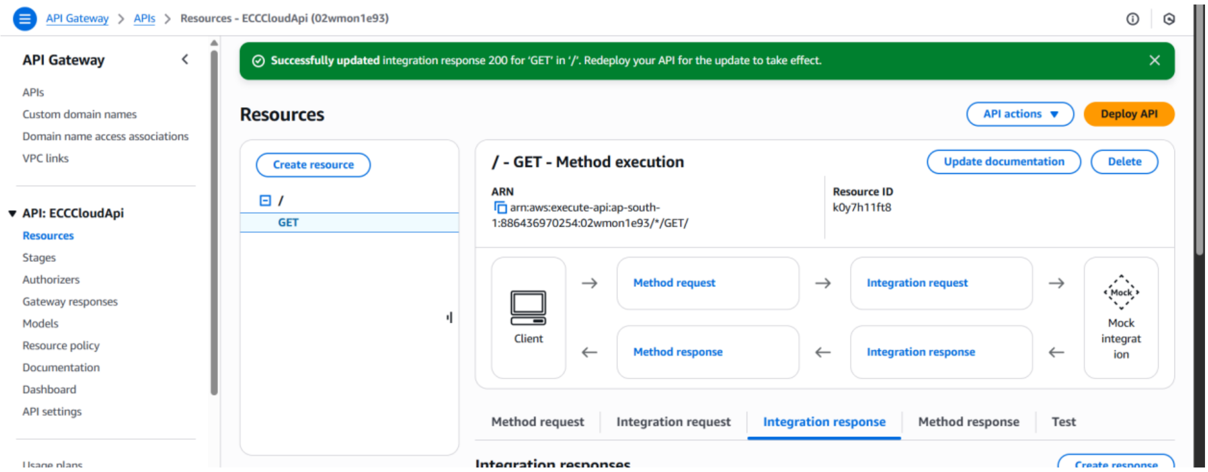
Content type: application/json

Generate template

Template body

```
{
"message:"This is Aditya Demo Api...""
}
```

Following confirmation will occur:



Successfully updated integration response 200 for 'GET' in '/'. Redeploy your API for the update to take effect.

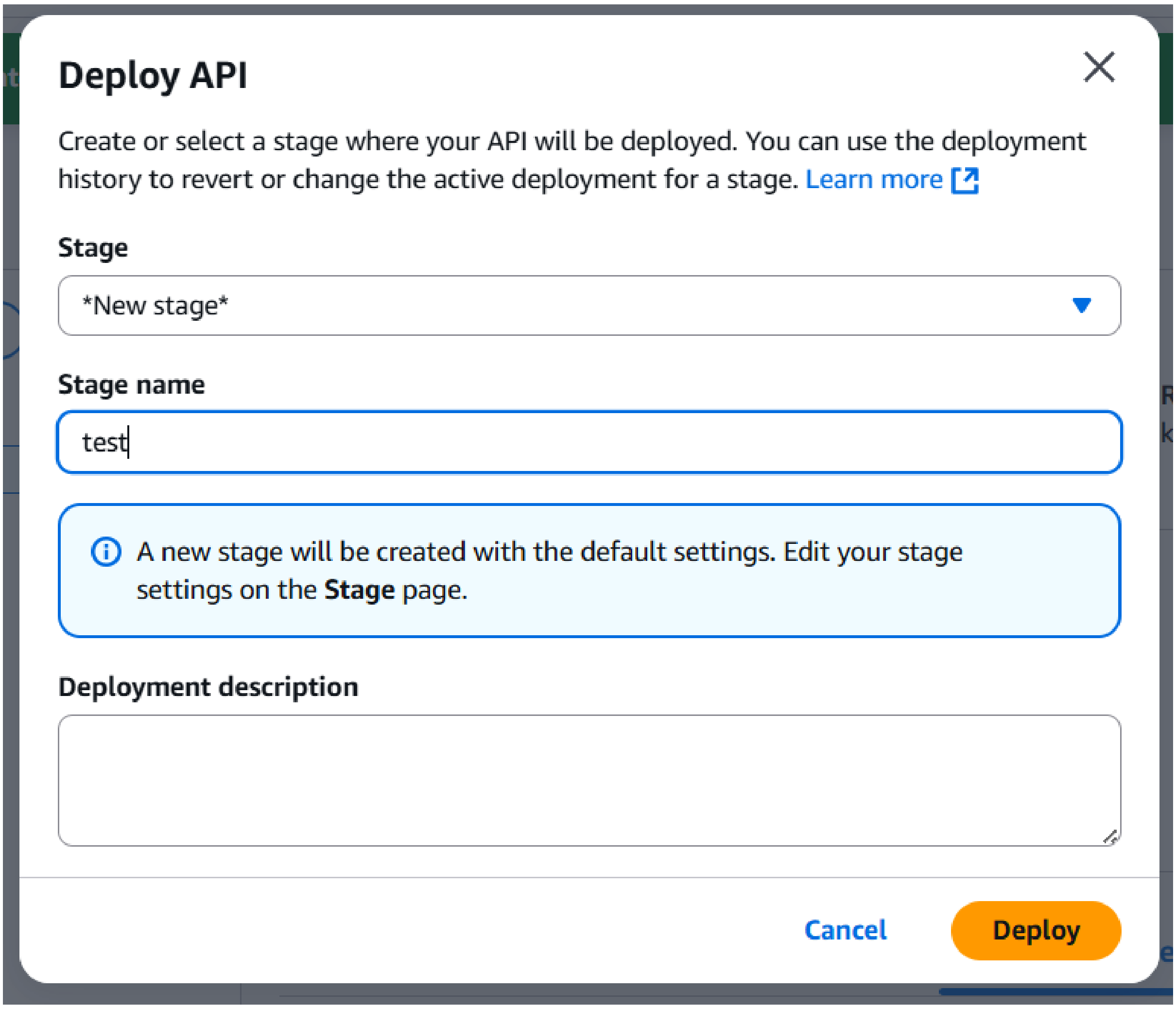
/ - GET - Method execution

ARN
arn:aws:execute-api:ap-south-1:886436970254:02wmon1e93/*/GET/

Resource ID
k0y7h11ft8

Integration responses

Click on the "Deploy API" button, and then select the stage as "New Stage": then click on deploy



Deploy API

Create or select a stage where your API will be deployed. You can use the deployment history to revert or change the active deployment for a stage. Learn more

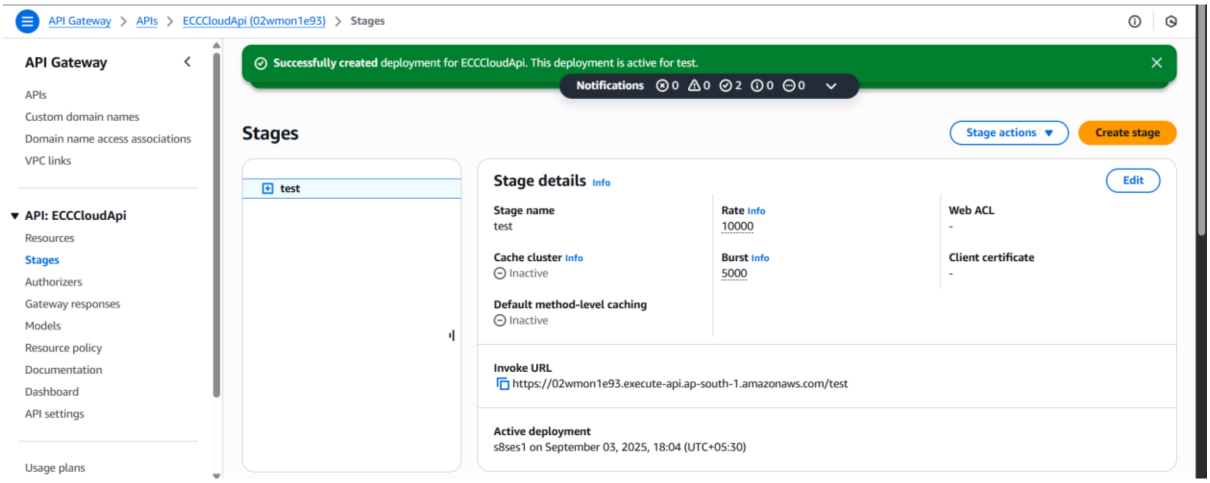
Stage: *New stage*

Stage name: test

A new stage will be created with the default settings. Edit your stage settings on the **Stage** page.

Deployment description:

Following confirmation will occur:



Successfully created deployment for ECCCloudApi. This deployment is active for test.

Stages

test

Stage details Info

Stage name
test

Rate Info
10000

Web ACL
-

Cache cluster Info
Inactive

Burst Info
5000

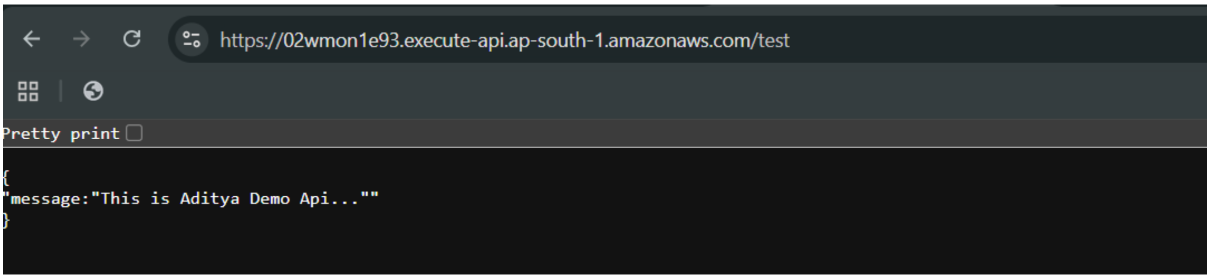
Client certificate
-

Default method-level caching
Inactive

Invoke URL
https://02wmon1e93.execute-api.ap-south-1.amazonaws.com/test

Active deployment
s8ses1 on September 03, 2025, 18:04 (UTC+05:30)

Now, paste the invoke URL which is shown there in new tab: it will show something like this.

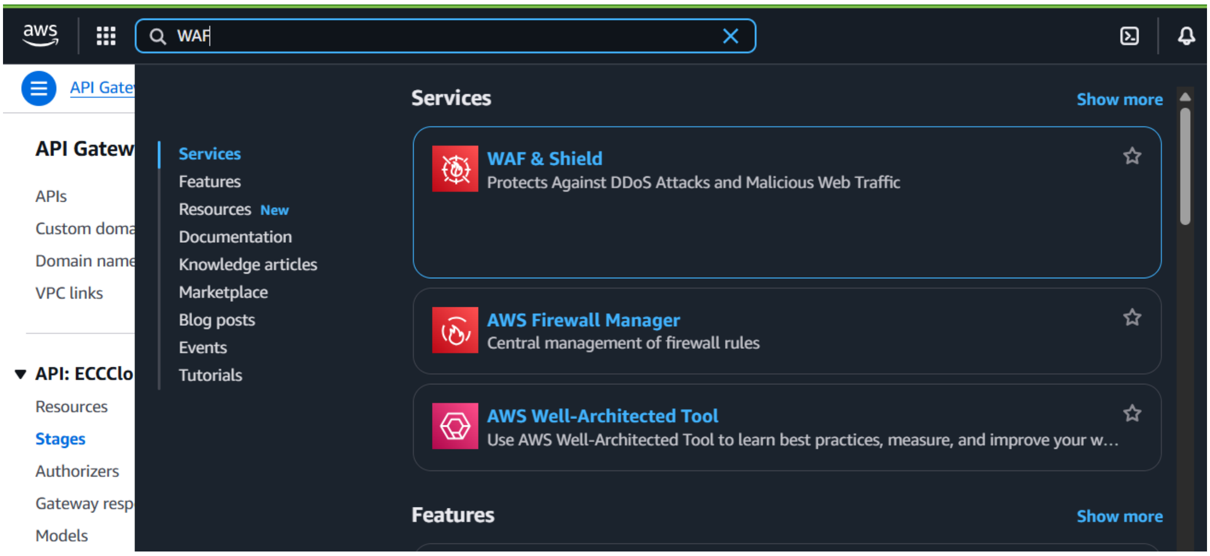


https://02wmon1e93.execute-api.ap-south-1.amazonaws.com/test

Pretty print □

```
{
"message:"This is Aditya Demo Api...""
}
```

So, API is ready, now we will be protecting this API from the specified IP with WAF:



Services

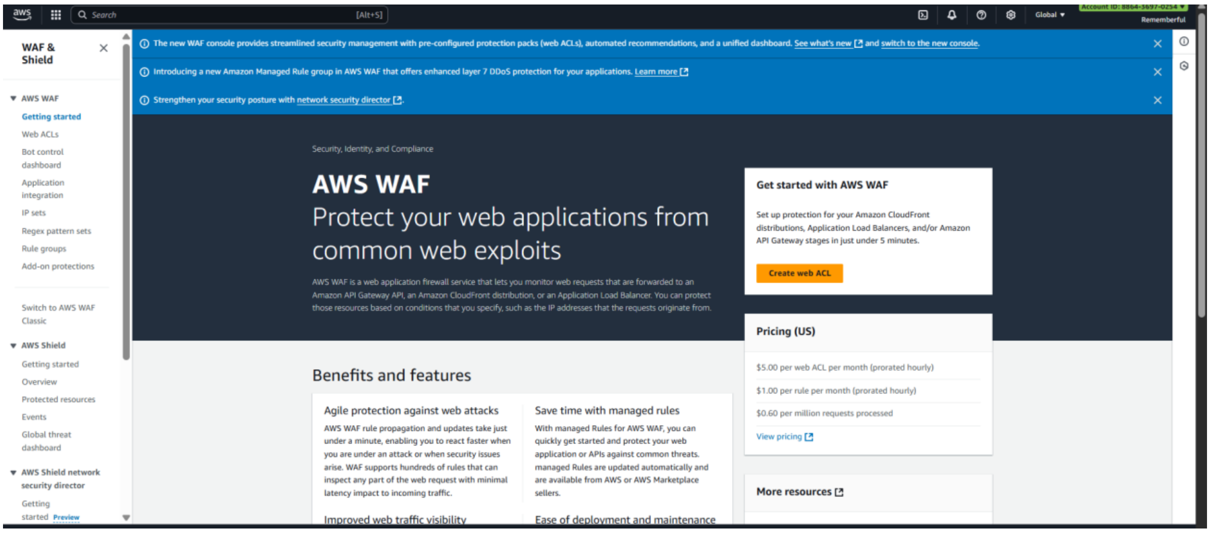
WAF & Shield
Protects Against DDoS Attacks and Malicious Web Traffic

AWS Firewall Manager
Central management of firewall rules

AWS Well-Architected Tool
Use AWS Well-Architected Tool to learn best practices, measure, and improve your w...

Features

Following window will appear:



The new WAF console provides streamlined security management with pre-configured protection packs (web ACLs), automated recommendations, and a unified dashboard. See what's new and switch to the new console.

Introducing a new Amazon Managed Rule group in AWS WAF that offers enhanced layer 7 DDoS protection for your applications. Learn more

Strengthen your security posture with network security director.

Security, Identity, and Compliance

AWS WAF

Protect your web applications from common web exploits

AWS WAF is a web application firewall service that lets you monitor web requests that are forwarded to an Amazon API Gateway API, an Amazon CloudFront distribution, or an Application Load Balancer. You can protect those resources based on conditions that you specify, such as the IP addresses that the requests originate from.

Get started with AWS WAF

Set up protection for your Amazon CloudFront distributions, Application Load Balancers, and/or Amazon API Gateway stages in just under 5 minutes.

Create web ACL

Pricing (US)

$5.00 per web ACL per month (prorated hourly)

$1.00 per rule per month (prorated hourly)

$0.60 per million requests processed

View pricing

More resources

Benefits and features

Agile protection against web attacks

AWS WAF rule propagation and updates take just under a minute, enabling you to react faster when you are under an attack or when security issues arise. WAF supports hundreds of rules that can inspect any part of the web request with minimal latency impact to incoming traffic.

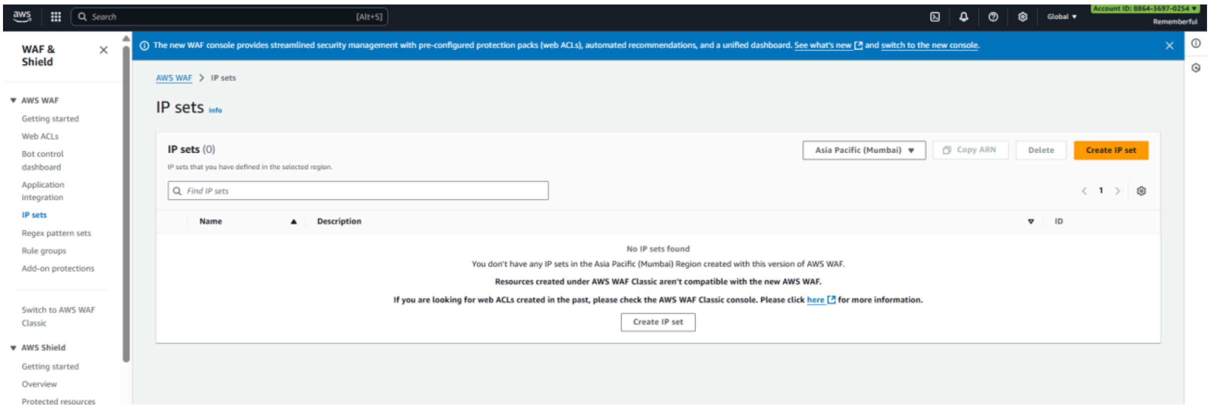
Save time with managed rules

With managed Rules for AWS WAF, you can quickly get started and protect your web application or APIs against common threats. managed Rules are updated automatically and are available from AWS or AWS Marketplace sellers.

Improved web traffic visibility

Ease of deployment and maintenance

Click on the “IP sets” from the left pane:



The new WAF console provides streamlined security management with pre-configured protection packs (web ACLs), automated recommendations, and a unified dashboard. See what's new and switch to the new console.

AWS WAF > IP sets

IP sets Info

IP sets (0)

IP sets that you have defined in the selected region.

Asia Pacific (Mumbai) ▼ | Copy ARN | Delete | Create IP set

Find IP sets

Name	Description	ID

No IP sets found

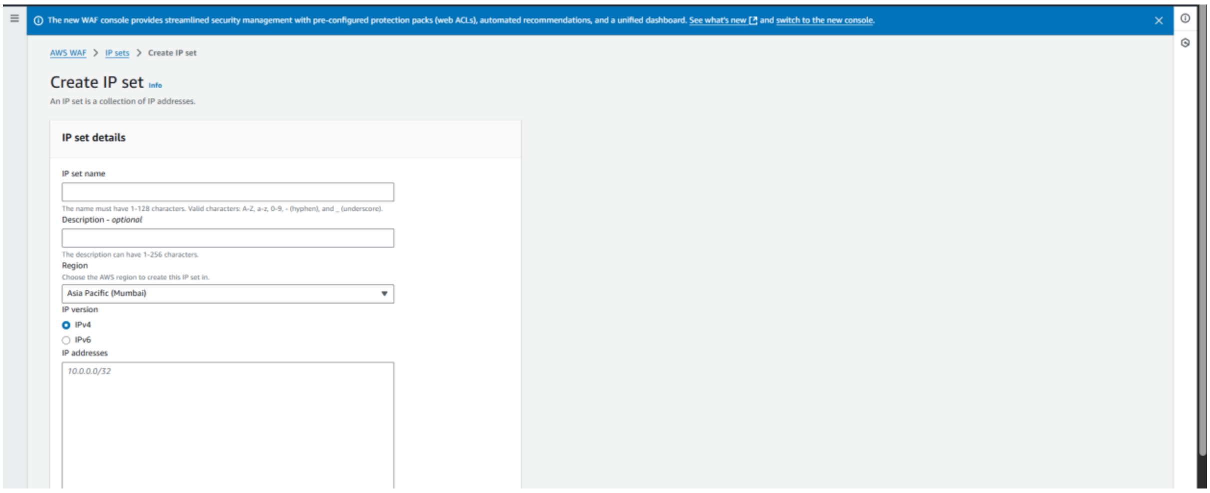
You don't have any IP sets in the Asia Pacific (Mumbai) Region created with this version of AWS WAF.

Resources created under AWS WAF Classic aren't compatible with the new AWS WAF.

If you are looking for web ACLs created in the past, please check the AWS WAF Classic console. Please click here for more information.

Create IP set

Click on the “Create IP Set” button: following page occurs.



The new WAF console provides streamlined security management with pre-configured protection packs (web ACLs), automated recommendations, and a unified dashboard. See what's new and switch to the new console.

AWS WAF > IP sets > Create IP set

Create IP set Info

An IP set is a collection of IP addresses.

IP set details

IP set name

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

Description - *optional*

The description can have 1-256 characters.

Region

Choose the AWS region to create this IP set in.

Asia Pacific (Mumbai)

IP version

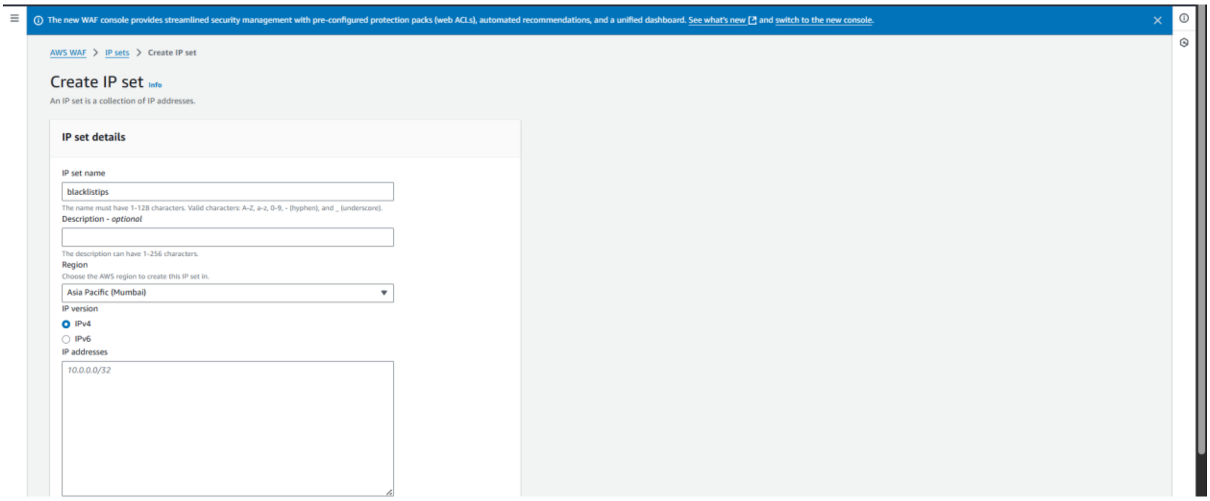
● IPv4

○ IPv6

IP addresses

10.0.0.0/32

Specify the name of your choice:



The new WAF console provides streamlined security management with pre-configured protection packs (web ACLs), automated recommendations, and a unified dashboard. See what's new and switch to the new console.

AWS WAF > IP sets > Create IP set

Create IP set Info

An IP set is a collection of IP addresses.

IP set details

IP set name: blacklistips

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

Description - *optional*

The description can have 1-256 characters.

Region

Choose the AWS region to create this IP set in.

Asia Pacific (Mumbai)

IP version

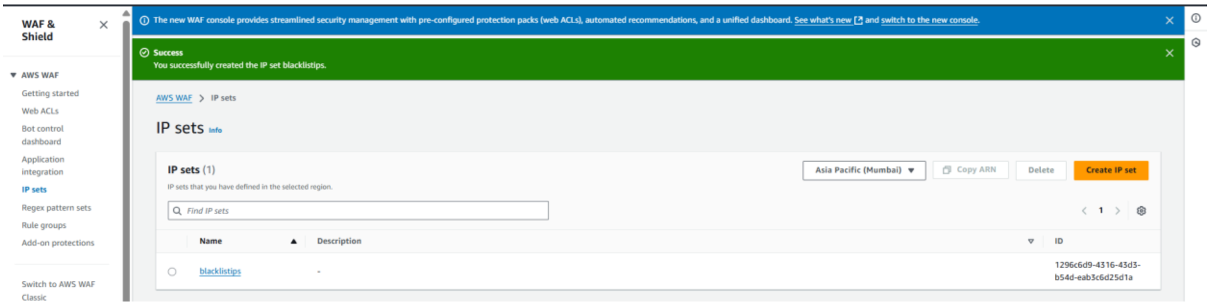
● IPv4

○ IPv6

IP addresses

10.0.0.0/32

Following confirmation will occur:



The new WAF console provides streamlined security management with pre-configured protection packs (web ACLs), automated recommendations, and a unified dashboard. See what's new and switch to the new console.

Success

You successfully created the IP set blacklistips.

AWS WAF > IP sets

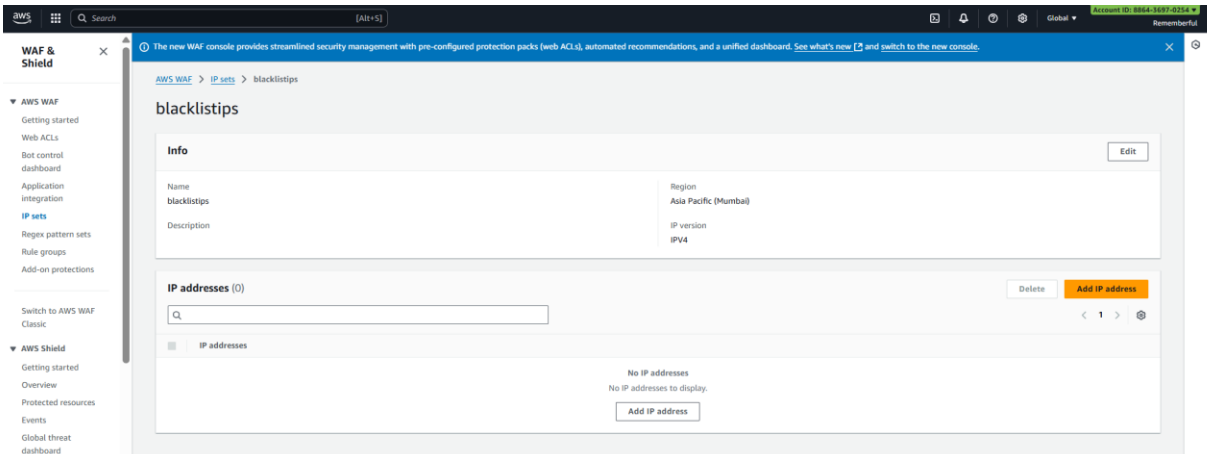
IP sets Info

IP sets (1)

IP sets that you have defined in the selected region.

	Name	Description	ID
○	blacklistips	-	1296c6d9-4316-43d3-b54d-eab3c6d25d1a

Click on the name of it:



The new WAF console provides streamlined security management with pre-configured protection packs (web ACLs), automated recommendations, and a unified dashboard. See what's new and switch to the new console.

AWS WAF > IP sets > blacklistips

blacklistips

Info

Name: blacklistips

Description

Region: Asia Pacific (Mumbai)

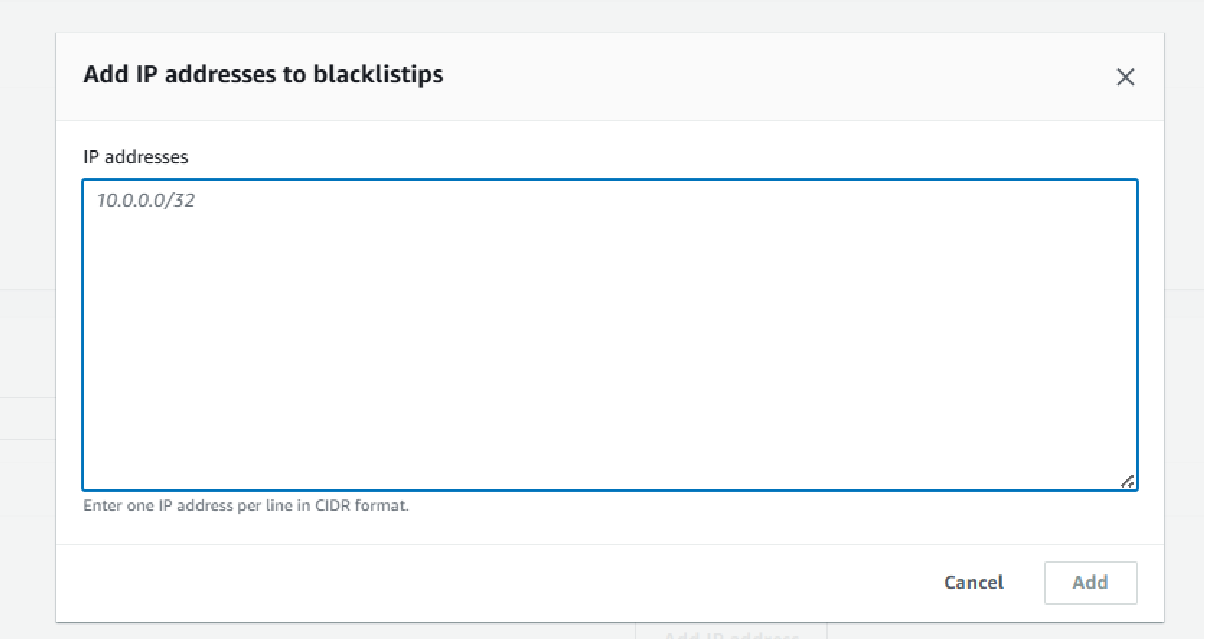
IP version: IPV4

IP addresses (0)

No IP addresses

No IP addresses to display.

Now, click on the “Add IP address” button:



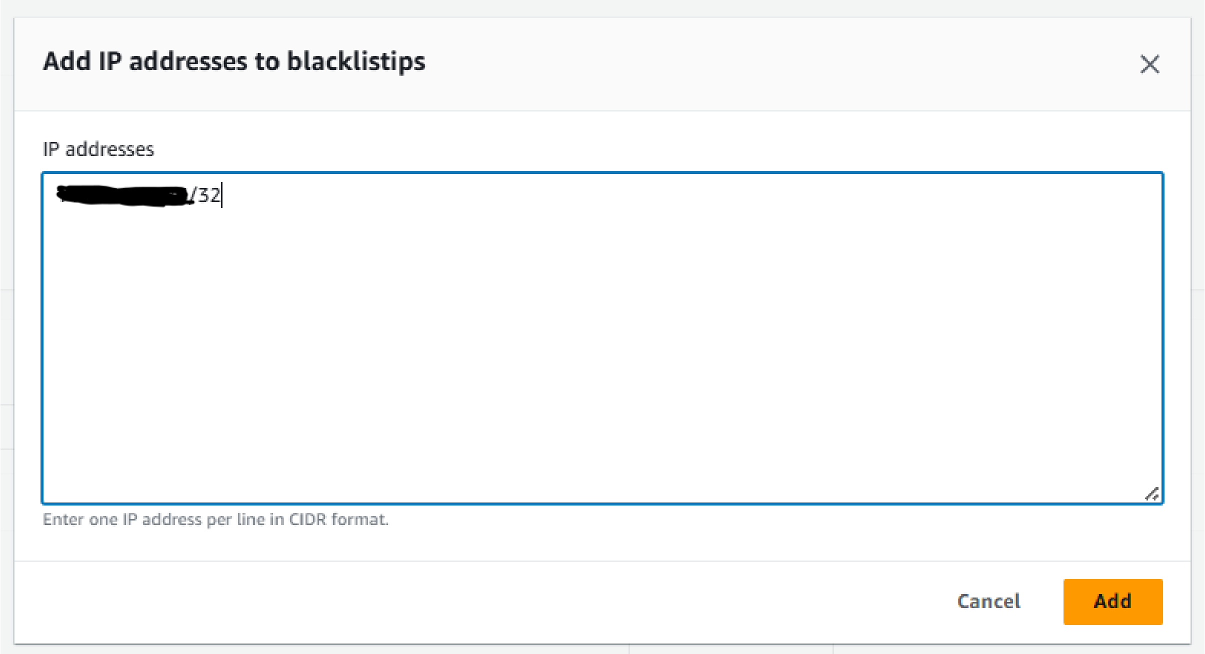
Add IP addresses to blacklistips

IP addresses

10.0.0.0/32

Enter one IP address per line in CIDR format.

Specify the IP: here I did my own public IP.



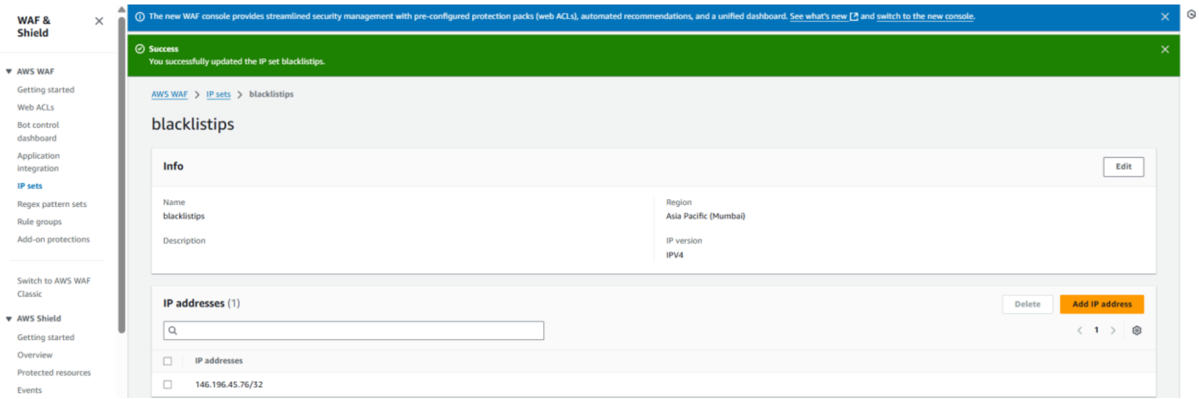
Add IP addresses to blacklistips

IP addresses

[redacted]/32

Enter one IP address per line in CIDR format.

Added:



The new WAF console provides streamlined security management with pre-configured protection packs (web ACLs), automated recommendations, and a unified dashboard. See what's new and switch to the new console.

Success
You successfully updated the IP set blacklistips.

AWS WAF > IP sets > blacklistips

blacklistips

Info

Name: blacklistips

Description:

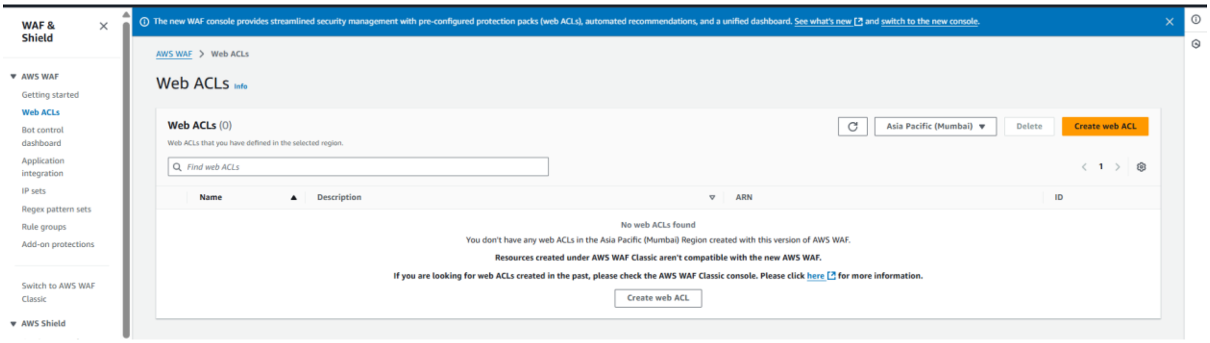
Region: Asia Pacific (Mumbai)

IP version: IPV4

IP addresses (1)

	IP addresses
□	146.196.45.76/32

Now, we will be creating WEB ACL in WAF: click on the “Web ACLs” from the left pane.



The new WAF console provides streamlined security management with pre-configured protection packs (web ACLs), automated recommendations, and a unified dashboard. See what's new and switch to the new console.

AWS WAF > Web ACLs

Web ACLs Info

Web ACLs (0)

Web ACLs that you have defined in the selected region.

Name ▲	Description	ARN	ID

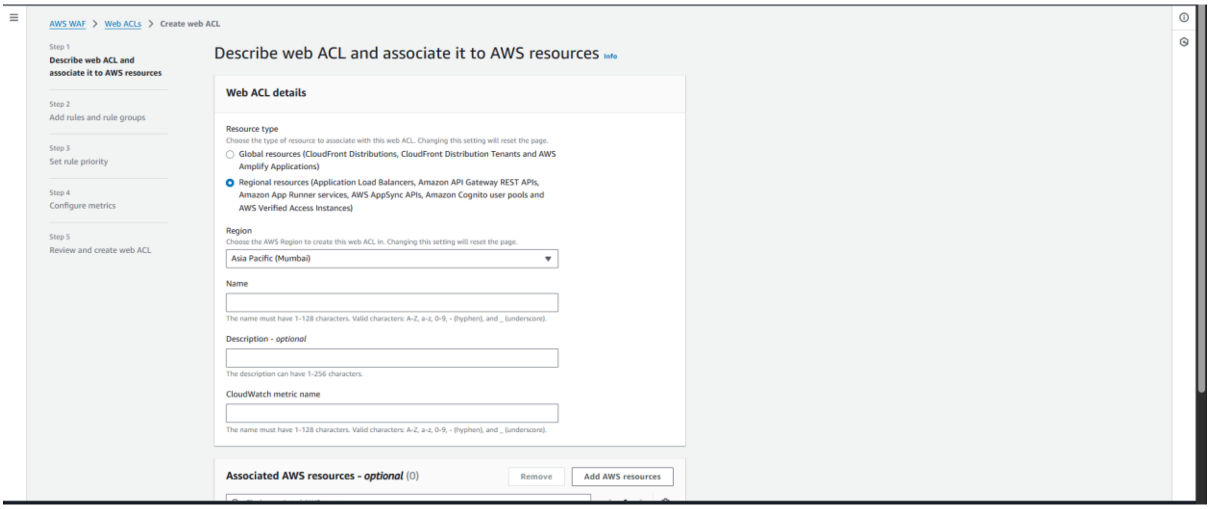
No web ACLs found

You don't have any web ACLs in the Asia Pacific (Mumbai) Region created with this version of AWS WAF.

Resources created under AWS WAF Classic aren't compatible with the new AWS WAF.

If you are looking for web ACLs created in the past, please check the AWS WAF Classic console. Please click here for more information.

Click on the “Create Web ACL” button:



AWS WAF > Web ACLs > Create web ACL

Step 1
Describe web ACL and associate it to AWS resources
Step 2
Add rules and rule groups
Step 3
Set rule priority
Step 4
Configure metrics
Step 5
Review and create web ACL

Describe web ACL and associate it to AWS resources Info

Web ACL details

Resource type

Choose the type of resource to associate with this web ACL. Changing this setting will reset the page.

○ Global resources (CloudFront Distributions, CloudFront Distribution Tenants and AWS Amplify Applications)

● Regional resources (Application Load Balancers, Amazon API Gateway REST APIs, Amazon App Runner services, AWS AppSync APIs, Amazon Cognito user pools and AWS Verified Access Instances)

Region

Choose the AWS Region to create this web ACL in. Changing this setting will reset the page.

Asia Pacific (Mumbai) ▼

Name

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

Description - *optional*

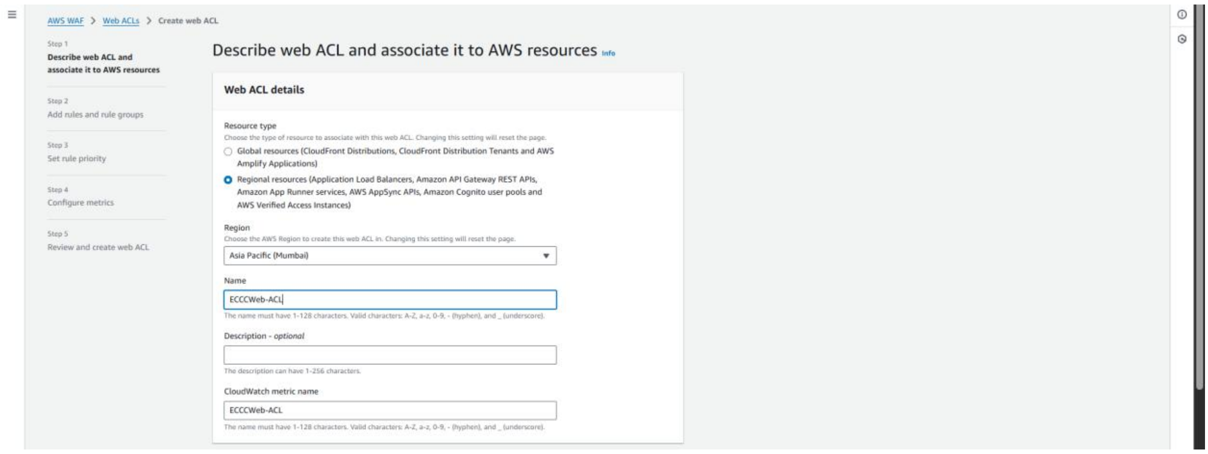
The description can have 1-256 characters.

CloudWatch metric name

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

Associated AWS resources - *optional* (0)

Now, specify it as like this:



AWS WAF > Web ACLs > Create web ACL

Step 1
Describe web ACL and associate it to AWS resources
Step 2
Add rules and rule groups
Step 3
Set rule priority
Step 4
Configure metrics
Step 5
Review and create web ACL

Describe web ACL and associate it to AWS resources Info

Web ACL details

Resource type

Choose the type of resource to associate with this web ACL. Changing this setting will reset the page.

○ Global resources (CloudFront Distributions, CloudFront Distribution Tenants and AWS Amplify Applications)

● Regional resources (Application Load Balancers, Amazon API Gateway REST APIs, Amazon App Runner services, AWS AppSync APIs, Amazon Cognito user pools and AWS Verified Access Instances)

Region

Choose the AWS Region to create this web ACL in. Changing this setting will reset the page.

Asia Pacific (Mumbai) ▼

Name

ECCCWeb-ACL

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

Description - *optional*

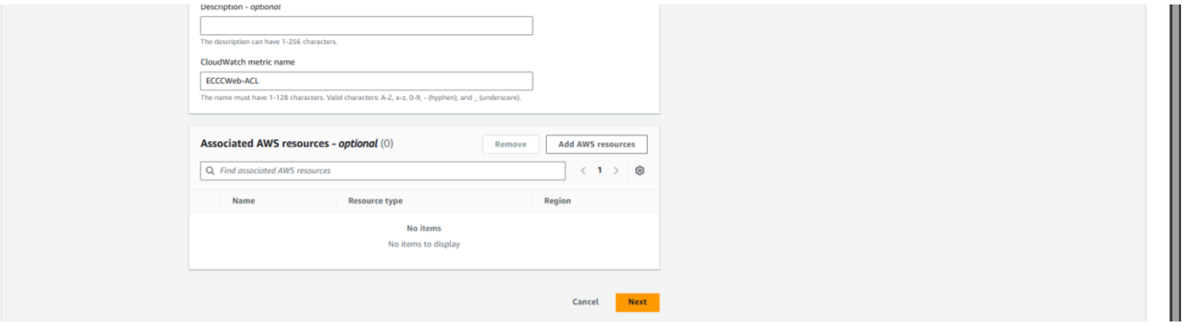
The description can have 1-256 characters.

CloudWatch metric name

ECCCWeb-ACL

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

Now, “Add AWS Resources”:



Description - *optional*

The description can have 1-256 characters.

CloudWatch metric name

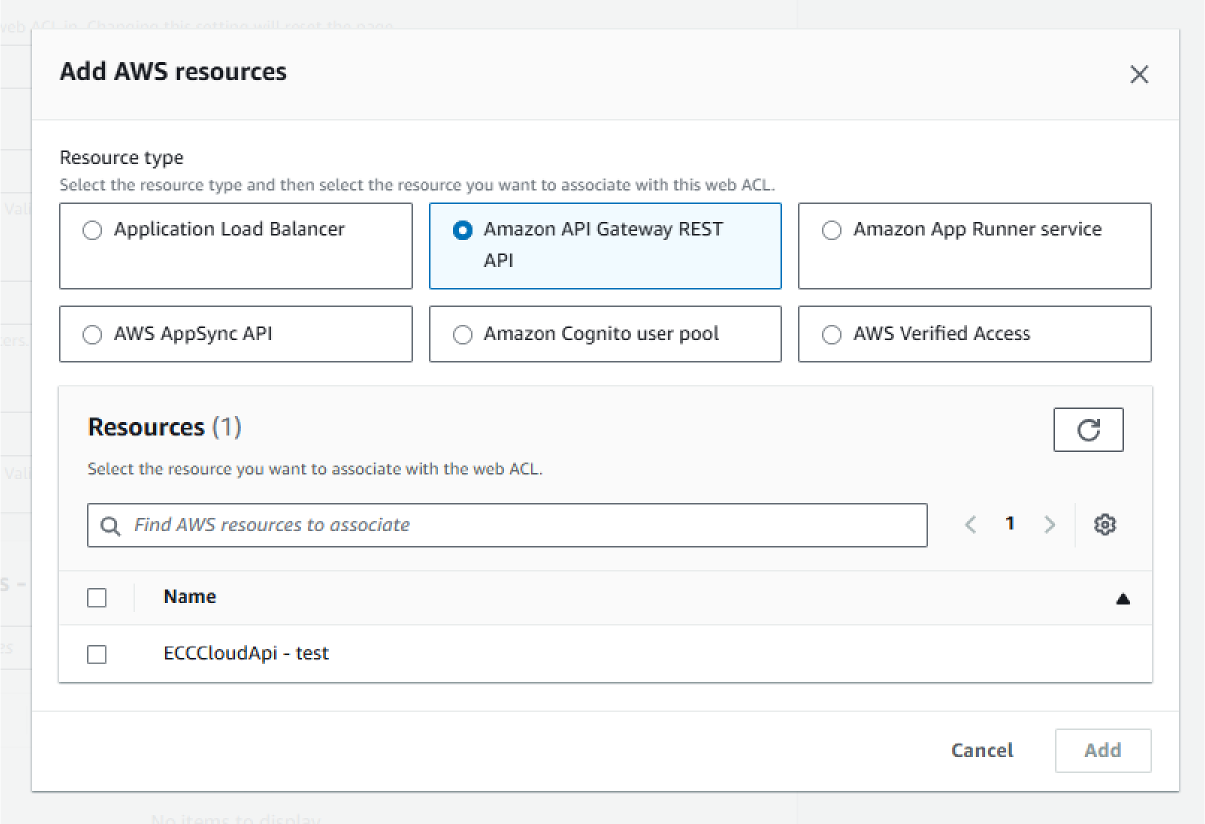
ECCCWeb-ACL

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

Associated AWS resources - *optional* (0)

Name	Resource type	Region
No items No items to display		

Following options occur:



Add AWS resources

Resource type

Select the resource type and then select the resource you want to associate with this web ACL.

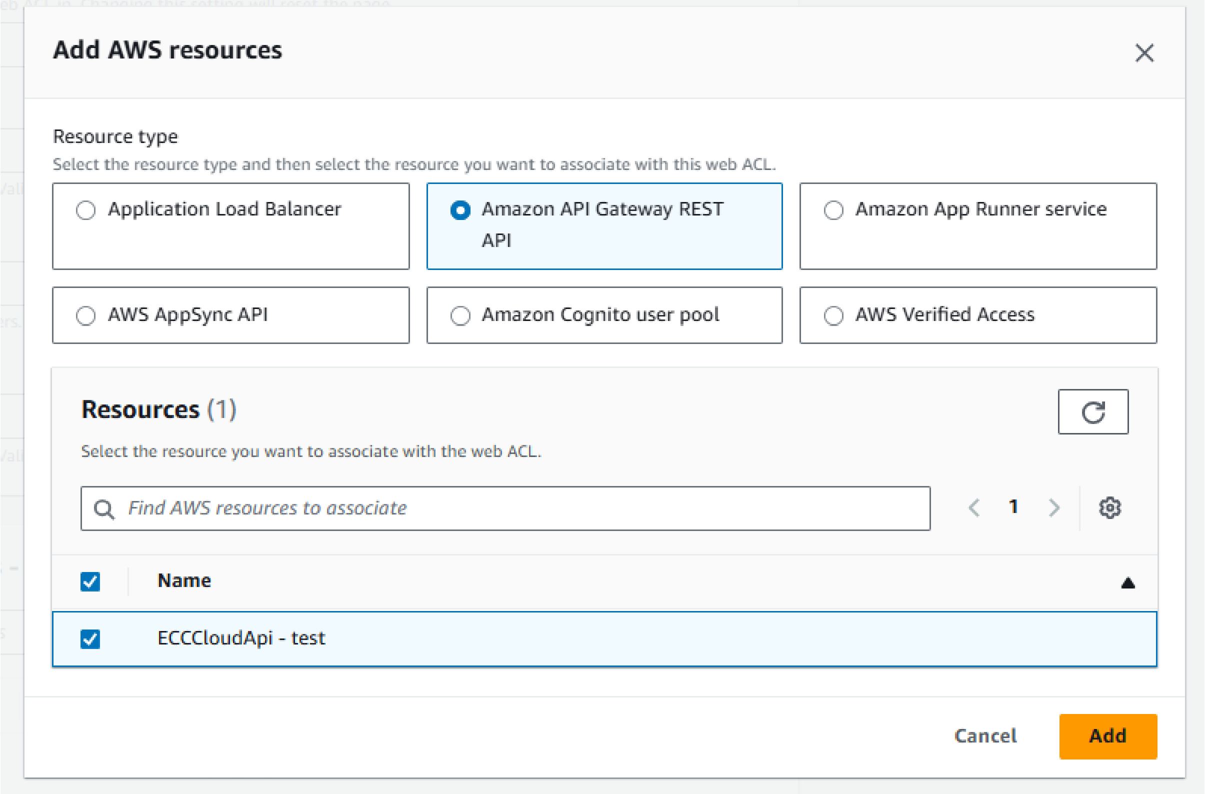
○ Application Load Balancer
● Amazon API Gateway REST API
○ Amazon App Runner service
○ AWS AppSync API
○ Amazon Cognito user pool
○ AWS Verified Access

Resources (1)

Select the resource you want to associate with the web ACL.

□	Name
□	ECCCloudApi - test

Click on the:



Add AWS resources

Resource type

Select the resource type and then select the resource you want to associate with this web ACL.

○ Application Load Balancer
● Amazon API Gateway REST API
○ Amazon App Runner service
○ AWS AppSync API
○ Amazon Cognito user pool
○ AWS Verified Access

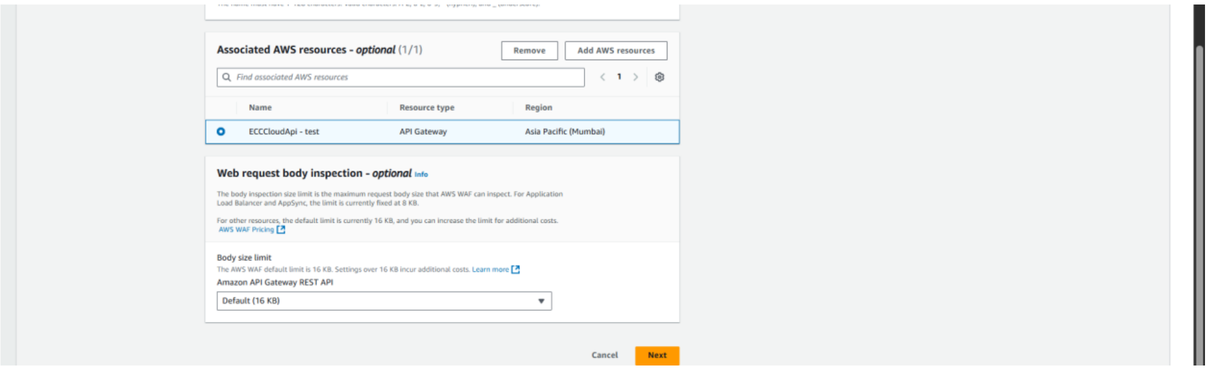
Resources (1)

Select the resource you want to associate with the web ACL.

Find AWS resources to associate

☑	Name
☑	ECCCloudApi - test

Following things shown:



Associated AWS resources - *optional* (1/1)

Find associated AWS resources

	Name	Resource type	Region
●	ECCCloudApi - test	API Gateway	Asia Pacific (Mumbai)

Web request body inspection - *optional* Info

The body inspection size limit is the maximum request body size that AWS WAF can inspect. For Application Load Balancer and AppSync, the limit is currently fixed at 8 KB.

For other resources, the default limit is currently 16 KB, and you can increase the limit for additional costs. AWS WAF Pricing

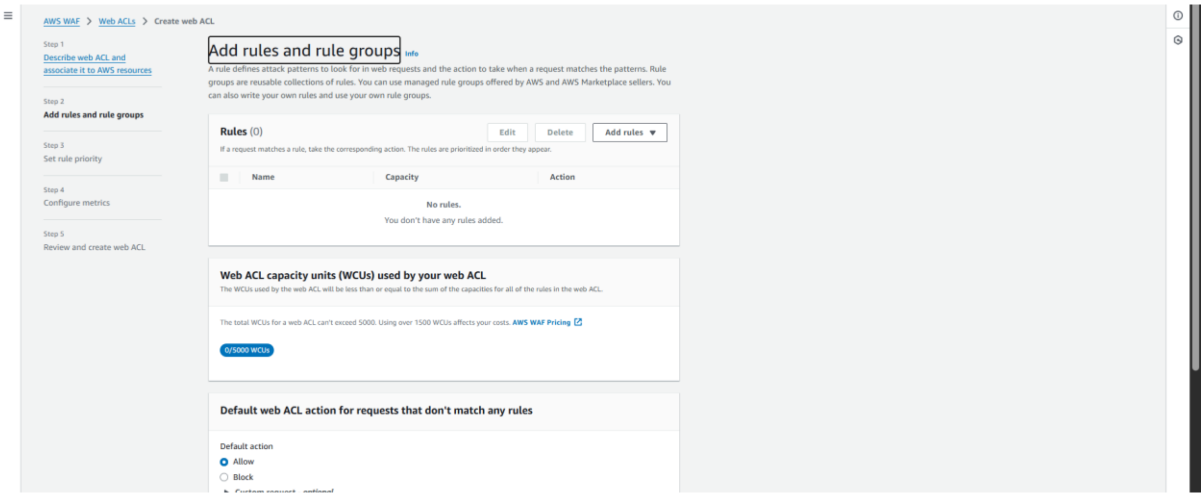
Body size limit

The AWS WAF default limit is 16 KB. Settings over 16 KB incur additional costs. Learn more

Amazon API Gateway REST API

Default (16 KB)

Following screen will appear:



AWS WAF > Web ACLs > Create web ACL
Step 1
Describe web ACL and associate it to AWS resources
Step 2
Add rules and rule groups
Step 3
Set rule priority
Step 4
Configure metrics
Step 5
Review and create web ACL
Info
Edit
Delete
Add rules ▼
Name
Capacity
Action
0/5000 WCUs
AWS WAF Pricing

Add rules and rule groups

A rule defines attack patterns to look for in web requests and the action to take when a request matches the patterns. Rule groups are reusable collections of rules. You can use managed rule groups offered by AWS and AWS Marketplace sellers. You can also write your own rules and use your own rule groups.

Rules (0)

If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

No rules.

You don't have any rules added.

Web ACL capacity units (WCUs) used by your web ACL

The WCUs used by the web ACL will be less than or equal to the sum of the capacities for all of the rules in the web ACL.

The total WCUs for a web ACL can't exceed 5000. Using over 1500 WCUs affects your costs.

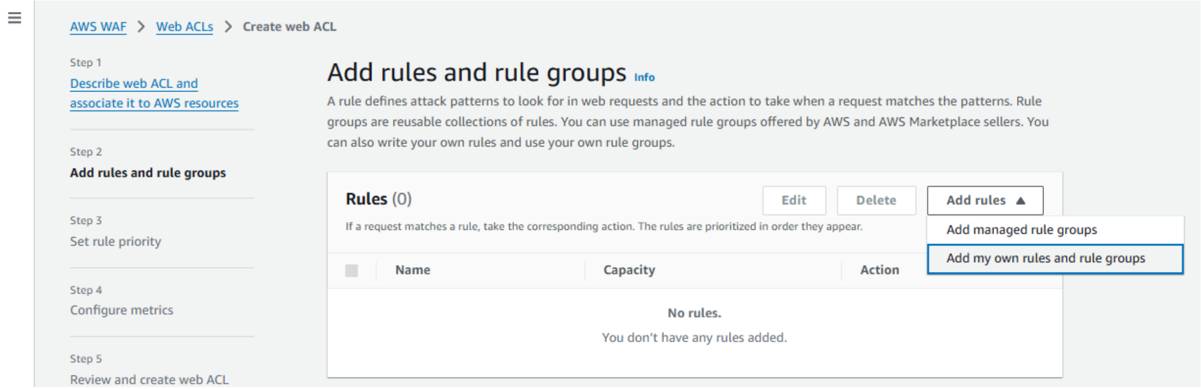
Default web ACL action for requests that don't match any rules

Default action

● Allow

○ Block

Click on the “Add rules”, click on the “Add my own rules and rule groups”:



AWS WAF > Web ACLs > Create web ACL
Step 1
Describe web ACL and associate it to AWS resources
Step 2
Add rules and rule groups
Step 3
Set rule priority
Step 4
Configure metrics
Step 5
Review and create web ACL
Info
Edit
Delete
Add rules ▲
Add managed rule groups
Add my own rules and rule groups
Name
Capacity
Action

Add rules and rule groups

A rule defines attack patterns to look for in web requests and the action to take when a request matches the patterns. Rule groups are reusable collections of rules. You can use managed rule groups offered by AWS and AWS Marketplace sellers. You can also write your own rules and use your own rule groups.

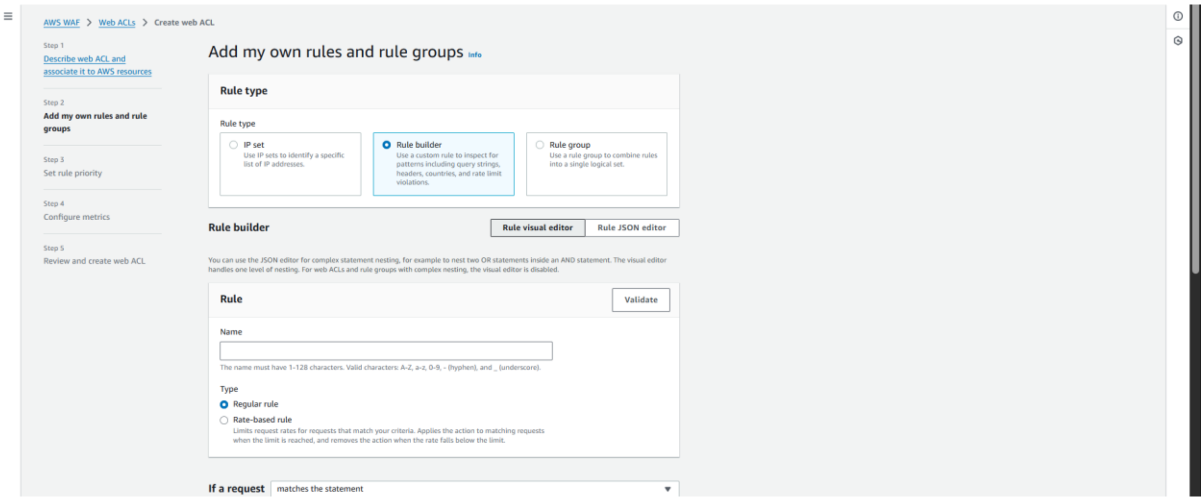
Rules (0)

If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

No rules.

You don't have any rules added.

Following screen appears:



AWS WAF > Web ACLs > Create web ACL
Step 1
Describe web ACL and associate it to AWS resources
Step 2
Add my own rules and rule groups
Step 3
Set rule priority
Step 4
Configure metrics
Step 5
Review and create web ACL
Info
Rule visual editor
Rule JSON editor
Validate

Add my own rules and rule groups

Rule type

Rule type

○ IP set
Use IP sets to identify a specific list of IP addresses.

● Rule builder
Use a custom rule to inspect for patterns including query strings, headers, countries, and rate limit violations.

○ Rule group
Use a rule group to combine rules into a single logical set.

Rule builder

You can use the JSON editor for complex statement nesting, for example to nest two OR statements inside an AND statement. The visual editor handles one level of nesting. For web ACLs and rule groups with complex nesting, the visual editor is disabled.

Rule

Name

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

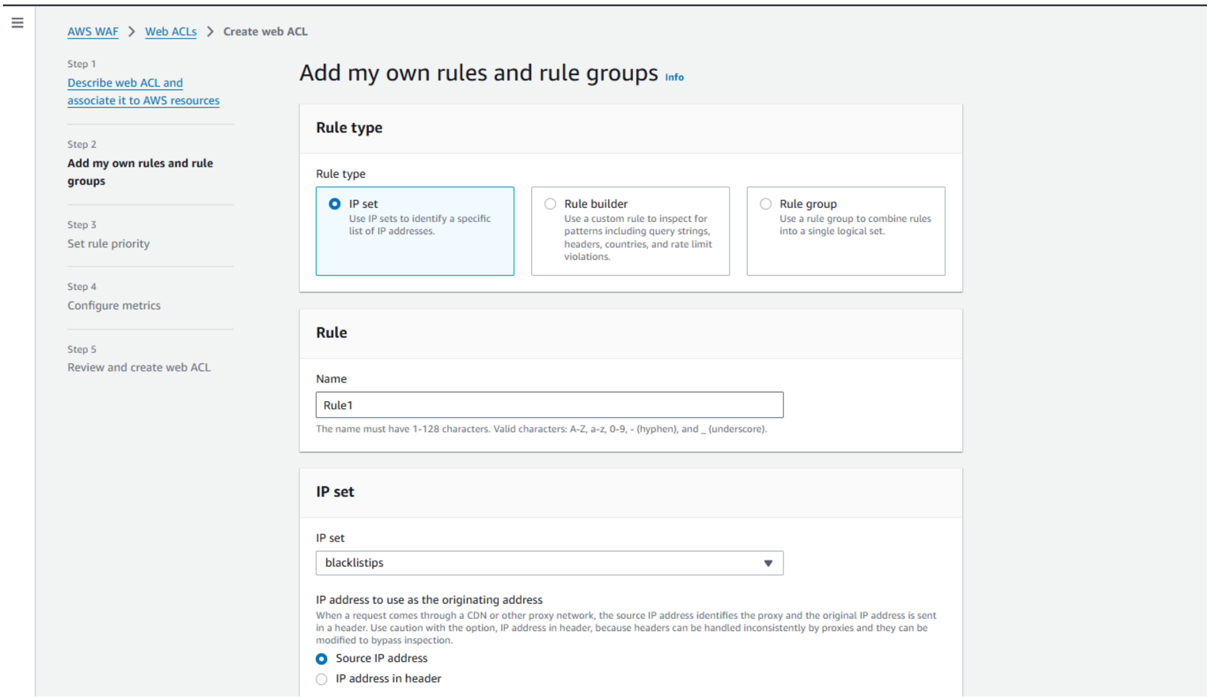
Type

● Regular rule

○ Rate-based rule
Limits request rates for requests that match your criteria. Applies the action to matching requests when the limit is reached, and removes the action when the rate falls below the limit.

If a request: matches the statement ▼

Make following changes:



AWS WAF > Web ACLs > Create web ACL

Step 1
Describe web ACL and associate it to AWS resources

Step 2
Add my own rules and rule groups

Step 3
Set rule priority

Step 4
Configure metrics

Step 5
Review and create web ACL

Add my own rules and rule groups Info

Rule type

Rule type

● IP set
Use IP sets to identify a specific list of IP addresses.

○ Rule builder
Use a custom rule to inspect for patterns including query strings, headers, countries, and rate limit violations.

○ Rule group
Use a rule group to combine rules into a single logical set.

Rule

Name

Rule1

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

IP set

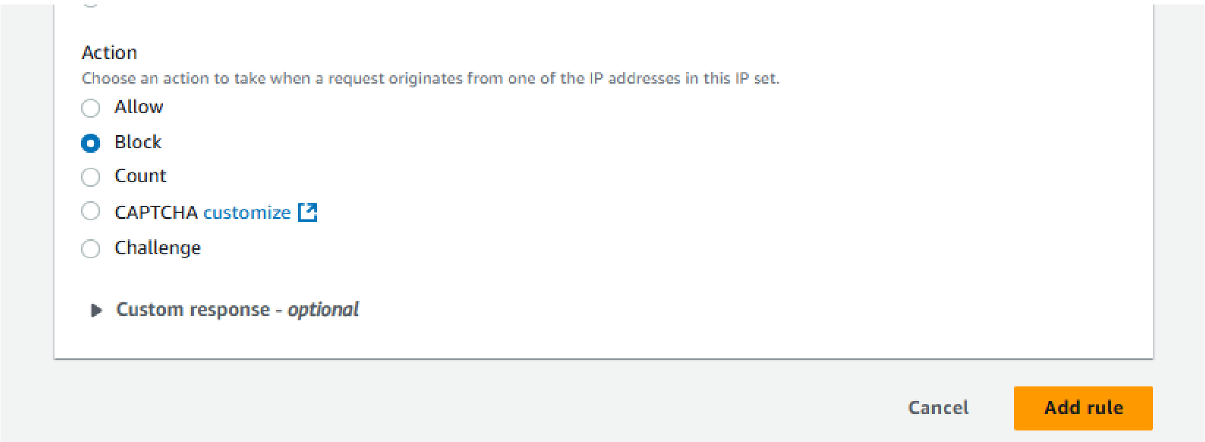
IP set

blacklistips ▼

IP address to use as the originating address
When a request comes through a CDN or other proxy network, the source IP address identifies the proxy and the original IP address is sent in a header. Use caution with the option, IP address in header, because headers can be handled inconsistently by proxies and they can be modified to bypass inspection.

● Source IP address
○ IP address in header

Also, ensure:

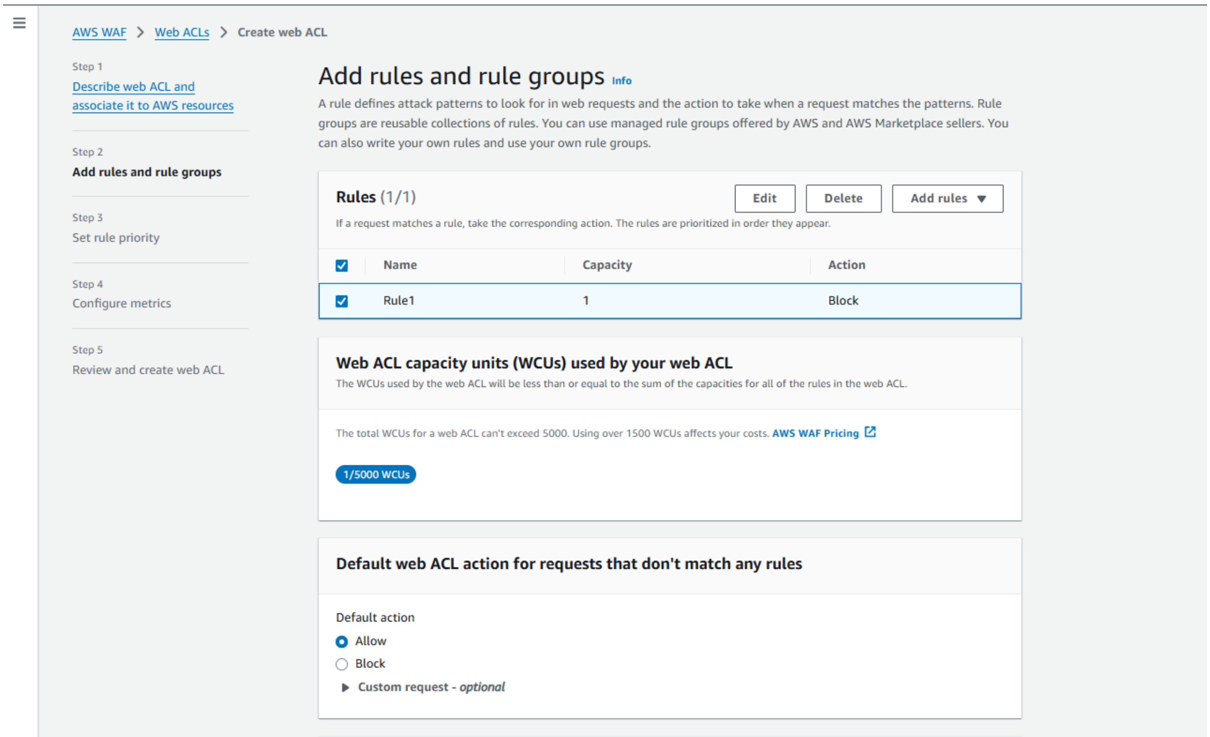


Action
Choose an action to take when a request originates from one of the IP addresses in this IP set.

○ Allow
● Block
○ Count
○ CAPTCHA customize
○ Challenge

▶ Custom response - *optional*

Click on “add rule” button:



AWS WAF > Web ACLs > Create web ACL

Step 1
Describe web ACL and associate it to AWS resources

Step 2
Add rules and rule groups

Step 3
Set rule priority

Step 4
Configure metrics

Step 5
Review and create web ACL

Add rules and rule groups Info

A rule defines attack patterns to look for in web requests and the action to take when a request matches the patterns. Rule groups are reusable collections of rules. You can use managed rule groups offered by AWS and AWS Marketplace sellers. You can also write your own rules and use your own rule groups.

Rules (1/1)

If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

☑	Name	Capacity	Action
☑	Rule1	1	Block

Web ACL capacity units (WCUs) used by your web ACL

The WCUs used by the web ACL will be less than or equal to the sum of the capacities for all of the rules in the web ACL.

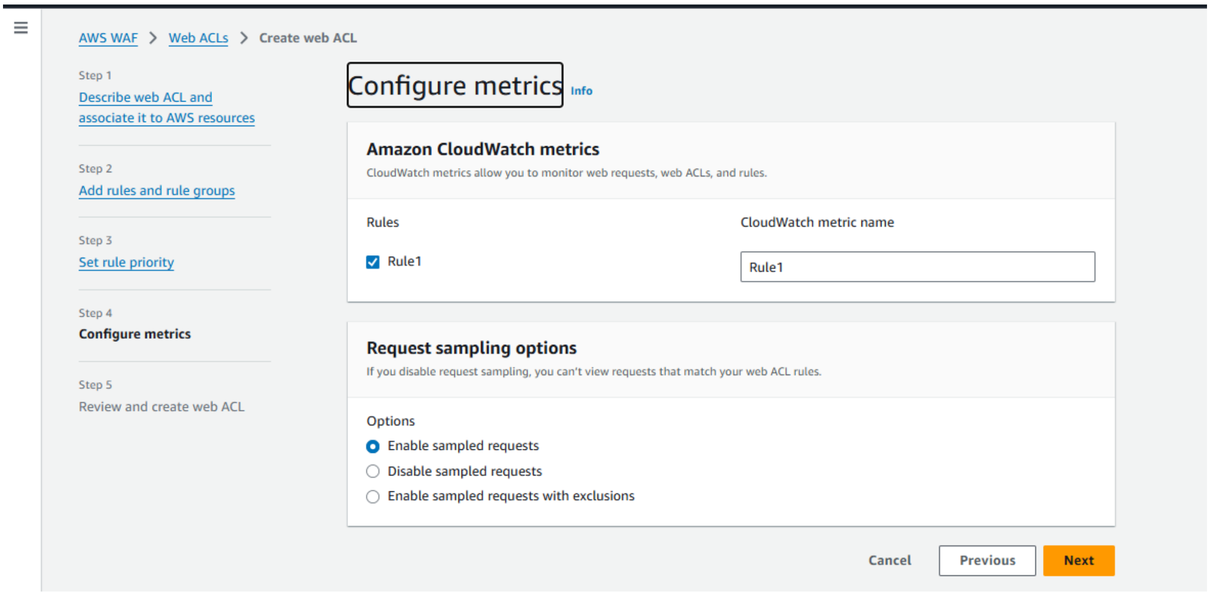
The total WCUs for a web ACL can't exceed 5000. Using over 1500 WCUs affects your costs. **AWS WAF Pricing**

1/5000 WCUs

Default web ACL action for requests that don't match any rules

Default action
● Allow
○ Block
▶ Custom request - *optional*

Click on the “next” button:



AWS WAF > Web ACLs > Create web ACL

Step 1
Describe web ACL and associate it to AWS resources

Step 2
Add rules and rule groups

Step 3
Set rule priority

Step 4
Configure metrics

Step 5
Review and create web ACL

Configure metrics Info

Amazon CloudWatch metrics

CloudWatch metrics allow you to monitor web requests, web ACLs, and rules.

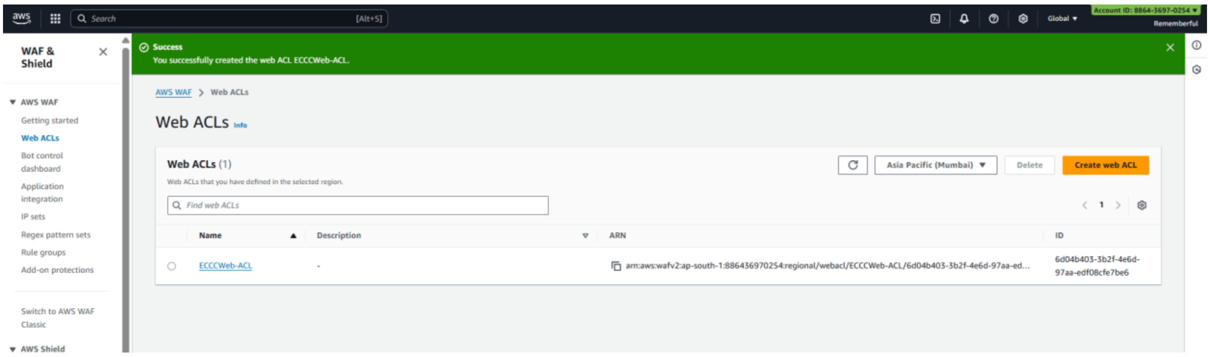
Rules	CloudWatch metric name
☑ Rule1	Rule1

Request sampling options

If you disable request sampling, you can't view requests that match your web ACL rules.

Options
● Enable sampled requests
○ Disable sampled requests
○ Enable sampled requests with exclusions

Following confirmation will occur:



Success
You successfully created the web ACL ECCCWeb-ACL.

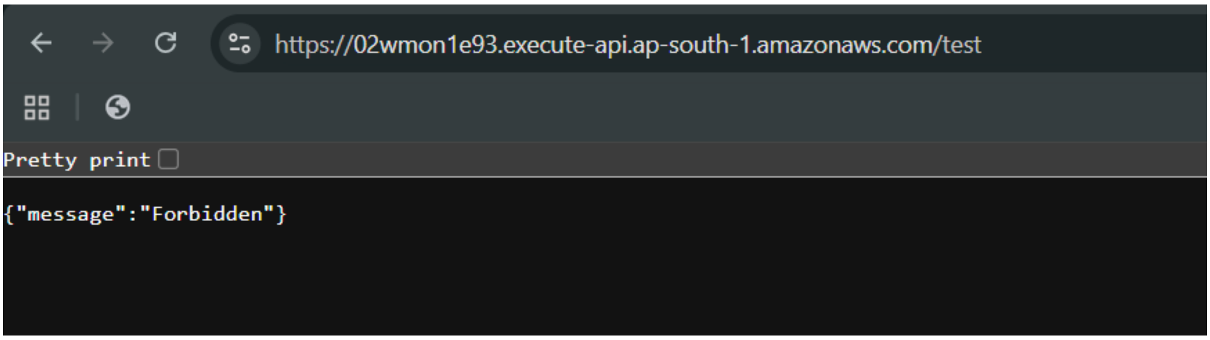
Web ACLs

Web ACLs (1)

Web ACLs that you have defined in the selected region.

	Name	Description	ARN	ID
○	ECCCWeb-ACL	-	arn:aws:wafv2:ap-south-1:886436970254:regional/webacl/ECCCWeb-ACL/6d04b403-3b2f-4e6d-97aa-ed...	6d04b403-3b2f-4e6d-97aa-edf08cfe7be6

Reopen the Invoke URL: clearly it worked.



https://02wmon1e93.execute-api.ap-south-1.amazonaws.com/test

```
{"message":"Forbidden"}
```

--The End--