

console.aws.amazon.com/iam/home?region=us-east-1#/users\$new?step=p

aws Services Resource Groups deploy @ fem-dryrun Global Support

Add user

1 2 3 4

▼ Set permissions

Add user to group Copy permissions from existing user Attach existing policies directly

Create policy

Filter policies ▾ Search Showing 359 results

	Policy name ▾	Type	Used as	Description
<input type="checkbox"/>	AdministratorAccess	Job function	Permissions policy (1)	Provides full access to AWS services and re...
<input type="checkbox"/>	AlexaForBusinessD...	AWS managed	None	Provide device setup access to AlexaForBu...
<input type="checkbox"/>	AlexaForBusinessF...	AWS managed	None	Grants full access to AlexaForBusiness reso...
<input type="checkbox"/>	AlexaForBusinessG...	AWS managed	None	Provide gateway execution access to Alexa...
<input type="checkbox"/>	AlexaForBusinessR...	AWS managed	None	Provide read only access to AlexaForBusine...
<input type="checkbox"/>	AmazonAPIGatewa...	AWS managed	None	Provides full access to create/edit/delete A...
<input type="checkbox"/>	AmazonAPIGatewa...	AWS managed	None	Provides full access to invoke APIs in Amaz...
<input type="checkbox"/>	AmazonAPIGatewa...	AWS managed	None	Allows API Gateway to push logs to user's ...

Cancel Previous Next: Review

console.aws.amazon.com/iam/home?region=us-east-1#/users\$new?step=p

aws Services Resource Groups deploy @ fem-dryrun Global Support

Add user

1 2 3 4

▼ Set permissions

 **Create policy**

Attach existing policies directly

Copy permissions from existing user

Add user to group

Filter policies ▾ Search Showing 359 results

	Policy name ▾	Type	Used as	Description
<input type="checkbox"/>	AdministratorAccess	Job function	Permissions policy (1)	Provides full access to AWS services and re...
<input type="checkbox"/>	AlexaForBusinessD...	AWS managed	None	Provide device setup access to AlexaForBu...
<input type="checkbox"/>	AlexaForBusinessF...	AWS managed	None	Grants full access to AlexaForBusiness reso...
<input type="checkbox"/>	AlexaForBusinessG...	AWS managed	None	Provide gateway execution access to Alexa...
<input type="checkbox"/>	AlexaForBusinessR...	AWS managed	None	Provide read only access to AlexaForBusine...
<input type="checkbox"/>	AmazonAPIGatewa...	AWS managed	None	Provides full access to create/edit/delete A...
<input type="checkbox"/>	AmazonAPIGatewa...	AWS managed	None	Provides full access to invoke APIs in Amaz...
<input type="checkbox"/>	AmazonAPIGatewa...	AWS managed	None	Allows API Gateway to push logs to user's ...

Cancel Previous Next: Review

Documentation

Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

[Visual editor](#) [JSON](#) [Import managed policy](#)

[Expand all](#) | [Collapse all](#)

Select a service [Clone](#) | [Remove](#)

Service Choose a service

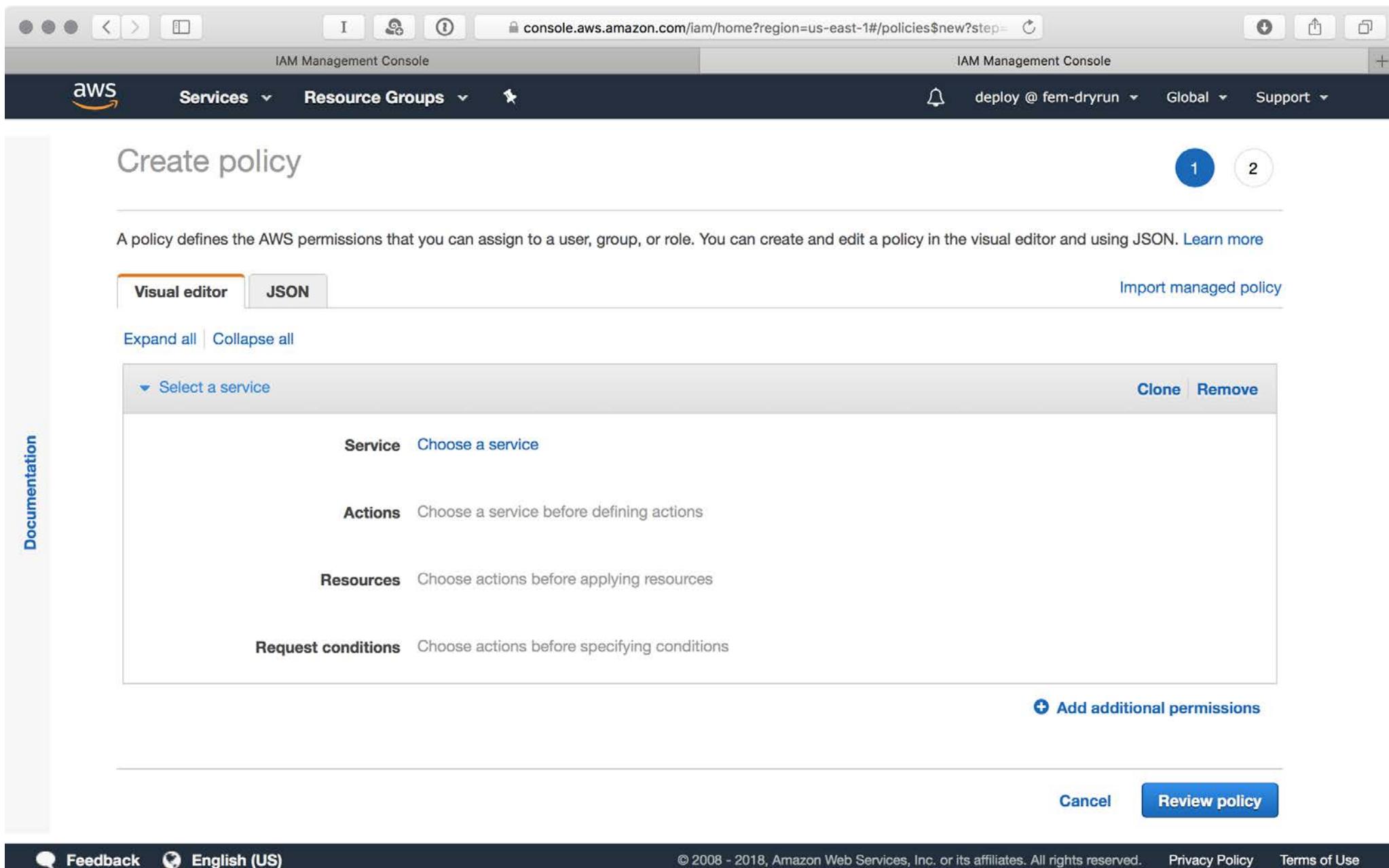
Actions Choose a service before defining actions

Resources Choose actions before applying resources

Request conditions Choose actions before specifying conditions

[+ Add additional permissions](#)

[Cancel](#) [Review policy](#)



Documentation

IAM Management Console

console.aws.amazon.com/iam/home?region=us-east-1#/policies\$new?step=

SIMPLY TESTED

AWS Services Resource Groups

aws deploy @ fem-dryrun Global Support

Service

Actions Specify the actions allowed in S3 [?](#)

close

Filter actions

Manual actions [\(add actions\)](#)

All S3 actions (s3:*)

Access level

List

Read

Write (30 selected)

Permissions management

Switch to deny permissions [i](#)

Expand all | Collapse all

Resources You chose actions that require the **bucket** resource type.
You chose actions that require the **object** resource type.

Request conditions Specify request conditions (optional)

[+ Add additional permissions](#)

Cancel Review policy

Documentation

IAM Management Console

console.aws.amazon.com/iam/home?region=us-east-1#/policies\$new?step=

AWS Services Resource Groups

Global Support

DeletedBucket DeleteBucketNotification PutObject
DeleteBucketWebsite PutBucketRequestPayment PutObjectTagging
DeleteObject PutBucketTagging PutObjectVersionTagging
DeleteObjectTagging PutBucketVersioning PutReplicationConfiguration
DeleteObjectVersion PutBucketWebsite ReplicateDelete
DeleteObjectVersionTagging PutEncryptionConfiguration ReplicateObject
PutAccelerateConfiguration PutInventoryConfiguration ReplicateTags
PutAnalyticsConfiguration PutIpConfiguration RestoreObject

Resources Specific All resources

bucket You chose actions that require the **bucket** resource type. Any
Add ARN to restrict access

object You chose actions that require the **object** resource type. Any
Add ARN to restrict access

Request conditions Specify request conditions (optional)

Add additional permissions

Cancel **Review policy**

This screenshot shows the AWS IAM Policy Editor interface. At the top, there's a navigation bar with tabs for 'Services' and 'Resource Groups'. Below the navigation is a grid of AWS actions categorized by namespace. The 'S3' namespace actions include: DeletedBucket, DeleteBucketNotification, PutObject, DeleteBucketWebsite, PutBucketRequestPayment, PutObjectTagging, DeleteObject, PutBucketTagging, PutObjectVersionTagging, DeleteObjectTagging, PutBucketVersioning, PutReplicationConfiguration, DeleteObjectVersion, PutBucketWebsite, ReplicateDelete, DeleteObjectVersionTagging, PutEncryptionConfiguration, ReplicateObject, PutAccelerateConfiguration, PutInventoryConfiguration, ReplicateTags, PutAnalyticsConfiguration, PutIpConfiguration, and RestoreObject. The 'Resources' section allows specifying specific or all resources. Under the 'bucket' resource type, it notes choosing actions requiring the bucket resource type and provides an option to add an ARN to restrict access. Similarly, for the 'object' resource type, it notes choosing actions requiring the object resource type and provides an option to add an ARN to restrict access. A 'Request conditions' section is present for specifying optional request conditions. At the bottom, there are 'Cancel' and 'Review policy' buttons, with the 'Review policy' button being highlighted.

IAM Management Console

console.aws.amazon.com/iam/home?region=us-east-1#/policies\$new?step=

IAM Management Console

aws Services Resource Groups

Add ARN(s)

Amazon Resource Names (ARNs) uniquely identify AWS resources. Resources are unique to each service. [Learn more](#)

Specify ARN for bucket

List ARNs manually

arn:aws:s3:::mysuperfunwebsite.com

Bucket name

mysuperfunwebsite.com

Any

Any

Any

Cancel Add

Request conditions Specify request conditions (optional)

+ Add additional permissions

Cancel Review policy

Feedback English (US)

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Documentation

I console.aws.amazon.com/iam/home?region=us-east-1#/policies\$new?step=1

IAM Management Console

aws Services Resource Groups

DeletedBucket PutBucketNotification PutObject
DeleteBucketWebsite PutBucketRequestPayment PutObjectTagging
DeleteObject PutBucketTagging PutObjectVersionTagging
DeleteObjectTagging PutBucketVersioning PutReplicationConfiguration
DeleteObjectVersion PutBucketWebsite ReplicateDelete
DeleteObjectVersionTagging PutEncryptionConfiguration ReplicateObject
PutAccelerateConfiguration PutInventoryConfiguration ReplicateTags
PutAnalyticsConfiguration PutIpConfiguration RestoreObject

Resources Specific All resources

close

bucket **EDIT** Any

Add ARN to restrict access

object You chose actions that require the **object** resource type. Any

Add ARN to restrict access

Request conditions Specify request conditions (optional)

+ Add additional permissions

Cancel **Review policy**

IAM Management Console

console.aws.amazon.com/iam/home?region=us-east-1#/policies\$new?step=

IAM Management Console

aws Services Resource Groups

deploy @ fem-dryrun Global Support

DeleteBucketWebsite PutBucketRequestPayment PutObjectTagging
DeleteObject PutBucketTagging PutObjectVersionTagging
DeleteObjectTagging PutBucketVersioning PutReplicationConfiguration
DeleteObjectVersion PutBucketWebsite ReplicateDelete
DeleteObjectVersionTagging PutEncryptionConfiguration ReplicateObject
PutAccelerateConfiguration PutInventoryConfiguration ReplicateTags
PutAnalyticsConfiguration PutIpConfiguration RestoreObject

Resources Specific All resources

close

bucket  Any
arn:aws:s3:::mysuperfunwebsite.com

Add ARN to restrict access

object  Any
You chose actions that require the **object** resource type.
Add ARN to restrict access

Request conditions Specify request conditions (optional)

+ Add additional permissions

Cancel Review policy



Documentation

Add ARN to restrict access

object You chose actions that require the **object** resource type. Any Add ARN to restrict access

Request conditions Specify request conditions (optional)

▼ Select a service Clone | Remove

Service **Select a service below** Enter service manually
close

CloudFront

Actions Choose a service before defining actions

Resources Choose actions before applying resources

Request conditions Choose actions before specifying conditions

+ Add additional permissions

Documentation

IAM Management Console

console.aws.amazon.com/iam/home?region=us-east-1#/policies\$new?step=

AWS Services Resource Groups

deploy @ fem-dryrun Global Support

CloudFront (1 action)

Service CloudFront

Actions Specify the actions allowed in CloudFront [?](#)

close

Filter actions

Manual actions (add actions)

All CloudFront actions (cloudfront:*)

Access level

List

Read

Write (1 selected)

CreateCloudFrontOriginAcc... [?](#) CreateStreamingDistributio... [?](#) UntagResource [?](#)

CreateDistribution [?](#) DeleteCloudFrontOriginAcc... [?](#) UpdateCloudFrontOriginAc... [?](#)

CreateDistributionWithTags [?](#) DeleteDistribution [?](#) UpdateDistribution [?](#)

CreateInvalidation [?](#) DeleteStreamingDistribution [?](#) UpdateStreamingDistribution [?](#)

CreateStreamingDistribution [?](#) TagResource [?](#)

Resources All resources have been selected for you because this service does not allow you to choose specific resources.

Documentation

IAM Management Console

console.aws.amazon.com/iam/home?region=us-east-1#/policies\$new?step=

AWS Services Resource Groups

deploy @ fem-dryrun Global Support

All CloudFront actions (cloudfront:*)

Access level

Expand all | Collapse all

List

Read

Write (1 selected)

CreateCloudFrontOriginAcc... ? CreateStreamingDistributio... ? UntagResource ?

CreateDistribution ? DeleteCloudFrontOriginAcc... ? UpdateCloudFrontOriginAc... ?

CreateDistributionWithTags ? DeleteDistribution ? UpdateDistribution ?

CreateInvalidation ? DeleteStreamingDistribution ? UpdateStreamingDistribution ?

CreateStreamingDistribution ? TagResource ?

Resources All resources have been selected for you because this service does not allow you to choose specific resources.

Request conditions Specify request conditions (optional)

+ Add additional permissions

Cancel Review policy



A screenshot of the AWS IAM 'Add user' wizard. The top navigation bar shows 'Services', 'Resource Groups', and 'Global'. The main title is 'Add user'. Below it, 'Set user details' is displayed. A red arrow points from the 'User name*' field, which contains 'travis'. At the bottom of this section is a blue 'Add another user' button. The status bar at the bottom right shows 'deploy @ fem-dryrun'.

Add user

1

2

3

4

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

travis

[+ Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type*



Programmatic access

Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.



AWS Management Console access

Enables a **password** that allows users to sign-in to the AWS Management Console.

* Required

[Cancel](#)

[Next: Permissions](#)

IAM Management Console

console.aws.amazon.com/iam/home?region=us-east-1#/users\$new?step=pe

IAM Management Console

aws Services Resource Groups

deploy @ fem-dryrun Global Support

Add user

1 2 3 4

▼ Set permissions

Add user to group Copy permissions from existing user Attach existing policies directly

Create policy

Filter policies CID Showing 1 result

	Policy name	Type	Used as	Description
<input checked="" type="checkbox"/>	CIDDeploy	Customer managed	None	

Cancel Previous Next: Review

Feedback English (US)

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

The screenshot shows the AWS IAM Management Console with the URL `console.aws.amazon.com/iam/home?region=us-east-1#/users$new?step=re`. The top navigation bar includes the AWS logo, 'Services' dropdown, 'Resource Groups' dropdown, a bell icon for notifications, and links for 'deploy @ fem-dryrun', 'Global', and 'Support'. Below the navigation is a breadcrumb trail: 'Add user' > 'Review'.

Add user

1 2 3 4

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	travis
AWS access type	Programmatic access - with an access key
Permissions boundary	Permissions boundary is not set

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	CI Deploy

Cancel

Previous

Create user

The screenshot shows the AWS IAM Management Console interface. At the top, there's a navigation bar with tabs for 'Services', 'Resource Groups', and a bell icon for notifications. Below the navigation bar, the main title is 'Add user'. To the right of the title, there are four numbered steps: 1, 2, 3, and 4, where step 4 is highlighted with a blue background. A success message box is displayed, containing a green checkmark icon and the word 'Success'. It states: 'You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.' Below this message, a link provides the sign-in URL: 'Users with AWS Management Console access can sign-in at: <https://fem-dryrun.signin.aws.amazon.com/console>'. At the bottom left, there's a 'Download .csv' button. On the right, a table lists the newly created user 'travis' with their Access key ID (AKIAIBJ6O76NJJYDMEWA) and Secret access key (represented by a series of asterisks). A 'Show' link is provided for the secret key. At the very bottom right, there's a 'Close' button.

Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://fem-dryrun.signin.aws.amazon.com/console>

Download .csv

	User	Access key ID	Secret access key
	travis	AKIAIBJ6O76NJJYDMEWA	***** Show

Close

Feedback

English (US)

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

[Privacy Policy](#)

[Terms of Use](#)