

There are 4 components in IAM

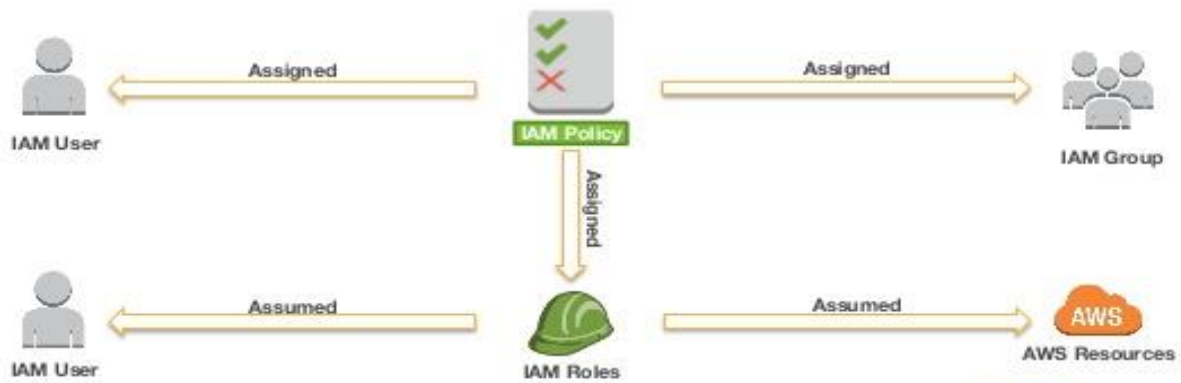
Users

Group

Roles

Policies

AWS IAM Policy Assignment



Step 1: Open IAM in services tab

Services ^

Security, Identity, & Compliance

IAM

Resource Access Manager

Cognito

Secrets Manager

GuardDuty

aws

Services ^

Resource Groups ^

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

Welcome to Identity and Access Management

IAM users sign-in link:

https://550659572743.signin.aws.amazon.com/console

Customize

IAM Resources

Users: 1

Groups: 1

Customer Managed Policies: 0

Roles: 2

Identity Providers: 0

Security Status

3 out of 5 completed

✓

Delete your root access keys

⚠

Activate MFA on your root account

✓

Create individual IAM users

✓

Use groups to assign permissions

⚠

Apply an IAM password policy

You can see the dashboard of IAM and you will see the URL link for IAM users

Step 2 create a user with group attach the policies to group.

Click Add user button

Add userDelete user

Find users by username or access key

☐

User name ▾

Groups

☐

students

Students

Enter Username

Add user

1

2

3

4

5

Set user details

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

User name*

gkaravindkumar

+

Add another user

Select the Access type and password details

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.

- Console password*** ☒ Autogenerated password
☐ Custom password

- Require password reset** ☒ User must create a new password at next sign-in
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

* Required

Cancel

Next: Permissions

Next add a group click “Create group”


Add user

1 2 3 4 5

Set permissions

 Add user to group

 Copy permissions from existing user

 Attach existing policies directly

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Add user to group

Create group Refresh

Q Search		Showing 1 result
Group	Attached policies	
<input type="checkbox"/> Students	AmazonS3ReadOnlyAccess	

Give a group name

Create group

Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions.

[Learn more](#)

Group name

Developer

Create policy

Refresh

Filter policies

Search

Showing 438 results

	Policy name	Type	Used as	Description
<input type="checkbox"/>	AdministratorAccess	Job function	None	Provides full access to AWS services and resources.
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaForBusiness services
<input type="checkbox"/>	AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness resources and access to related A...
<input type="checkbox"/>	AlexaForBusinessGatewayExec	AWS managed	None	Provide gateway execution access to AlexaForBusiness services

Cancel

Create group

Search the related policies in default policies and attach it to the group

Create group

Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions.

[Learn more](#)

Group name

Developer

Create policy

Refresh

Filter policies

ec2full

Showing 1 result

	Policy name	Type	Used as	Description
<input checked="" type="checkbox"/>	AmazonEC2FullAccess	AWS managed	Permissions policy (1)	Provides full access to Amazon EC2 via the AWS Management Console.

Cancel

Create group

Attach the user to the respective group

Add user

1


2


3


4

5

Set permissions

Add user to group

Copy permissions from existing user

Attach existing policies directly

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Add user to group

Create group

Refresh

Search

Showing 2 results

Group	Attached policies
<input checked="" type="checkbox"/> Developer	AmazonEC2FullAccess
<input type="checkbox"/> Students	AmazonS3ReadOnlyAccess

Attach Name tag

Add user

1

2

3

4

5

Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. [Learn more](#)

Key	Value (optional)	Remove
<div>Name</div>	<div>aravind</div>	<div>✕</div>
<div>Add new key</div>	<div></div>	

You can add 49 more tags.

Cancel

Previous

Next: Review

Review the details and create user wit group

User details

User name	gkaravindkumar
AWS access type	Programmatic access and AWS Management Console access
Console password type	Autogenerated
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	Developer
Managed policy	IAMUserChangePassword

Tags

The new user will receive the following tag

Key	Value
Name	aravind

The user will be created and it shows the secret key and password only once you should copy it and you can't able to see it again

Add user

1

2

3

4

5

✓

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://550659572743.signin.aws.amazon.com/console>

Download .csv

	User	Access key ID	Secret access key	Password	Email login instructions
▶	✓ gkaravindku...	AKIAYANO6IQDTGHG65HS	***** Show	***** Show	Send email ↗

Add user

1

2

3

4

5

✓

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://550659572743.signin.aws.amazon.com/console>

Download .csv

	User	Access key ID	Secret access key	Password	Email login instructions
▶	✓ gkaravindku...	AKIAYANO6IQDTGHG65HS	Lm1LIINrZRxc5ynBVdHg1kl 0PbteMrtYzXJkP49H Hide	DaIPqe!OMaBN Hide	Send email ↗

Now you User will be shown in the list

Add userDelete user

↺⚙️❓

Find users by username or access key

Showing 2 results

<input type="checkbox"/>	User name ▾	Groups	Access key age	Password age	Last activity	MFA
<input type="checkbox"/>	gkaravindkumar	Developer	None	Today	None	Not enabled
<input type="checkbox"/>	students	Students	None	11 days	2 days	Not enabled

Step3: Check the user by login the console



Account ID or alias

IAM user name

Password

Sign In

[Sign-in using root account credentials](#)

[Forgot password?](#)

It ask for password change if you selected this option while creating



You must change your password to continue

AWS account 550659572743

IAM user name gkaravindkumar

Old password ••••••••

New password ••••••••

Retype new password ••••••••

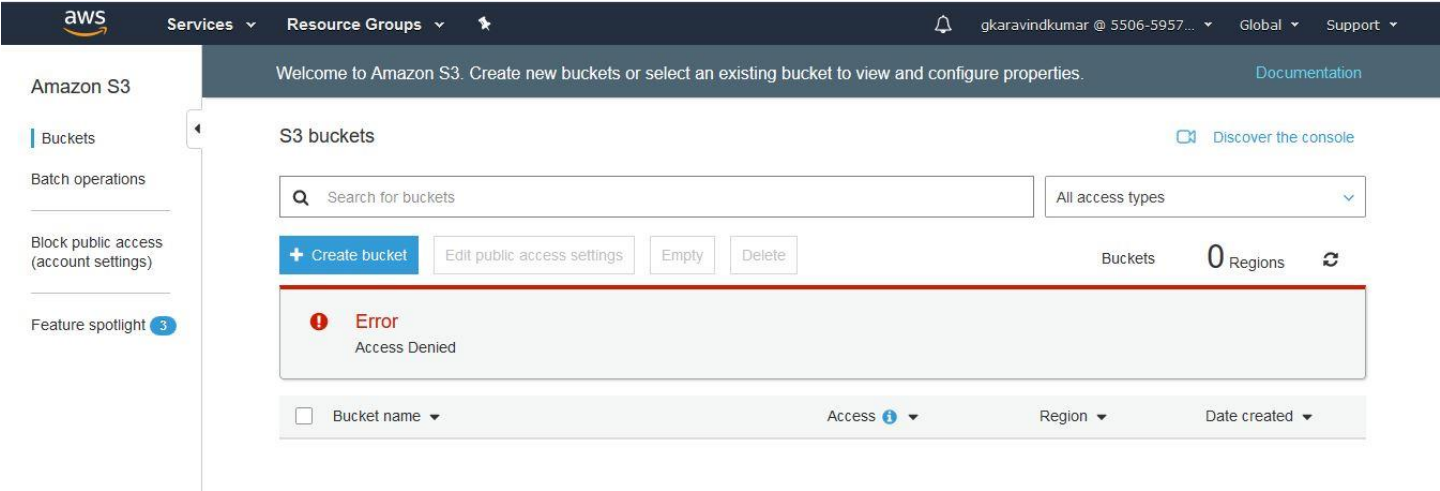
Confirm password change

[Sign-in using root account credentials](#)

English ▾

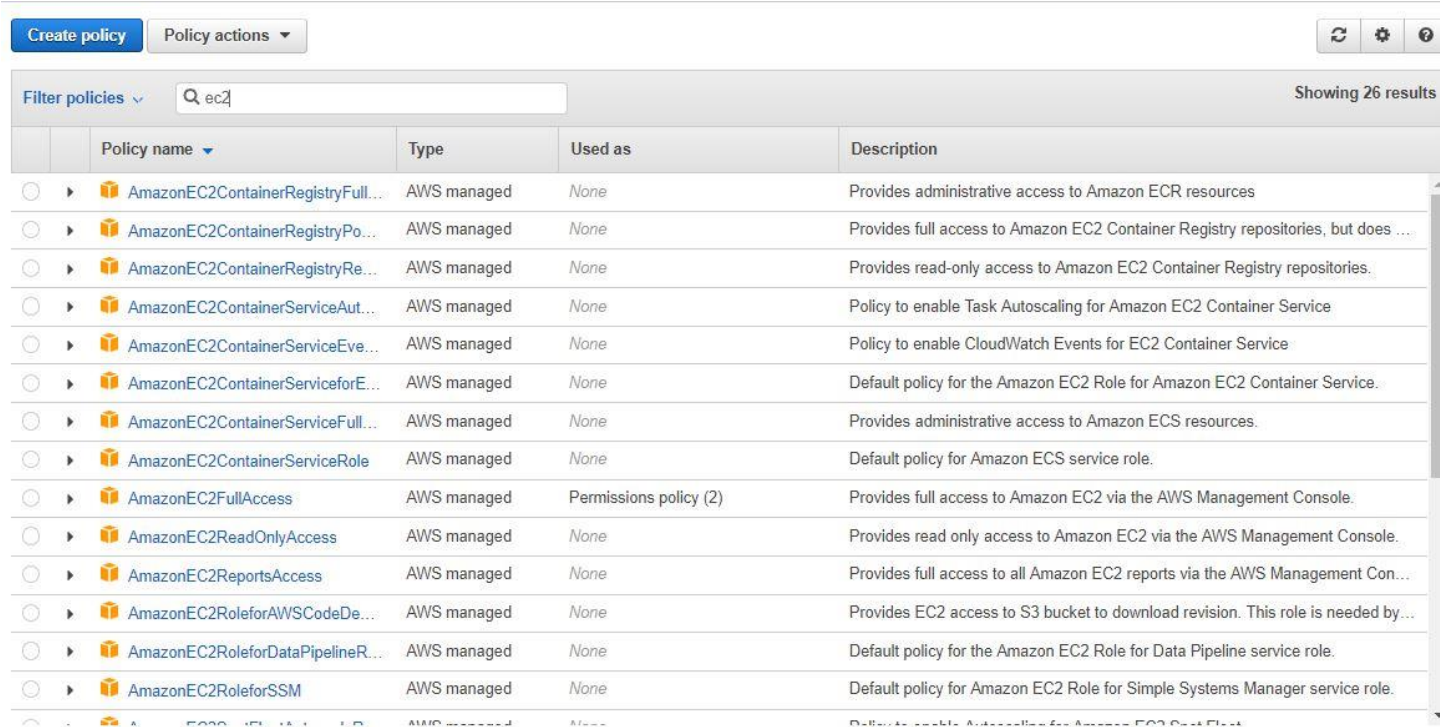
[Terms of Use](#) [Privacy Policy](#) © 1996-2019, Amazon Web Services, Inc. or its affiliates.

Check the permissions of the user it dot have rights to other services except EC2.



Policies

Step 4:Create a new policy and attaching it to a group. Goto policies > create Policy



You can use JASON script if you have or create policy in UI.

Create policy

12

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](#)

This policy validation failed and might have errors converting to Visual editor : Could not parse the policy: Statement is empty! For more information about the IAM policy grammar, see [AWS IAM Policies](#)

Visual editorJSON

Import managed policy

Expand all | Collapse all

▼ Select a service

CloneRemove

▶ 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

Select the service

Visual editorJSON

Import managed policy

Expand all | Collapse all

▼ Select a service

CloneRemove

▼ Service

Select a service below

close

Q ec2

EC2

EC2 Auto Scaling

EC2 Messages

Enter service manually

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

Choose the Action

► Service EC2

► Actions List

DescribeAccountAttributes	DescribeImportImageTasks	DescribeSpotFleetRequestHistory
DescribeAddresses	DescribeImportSnapshotTasks	DescribeSpotFleetRequests
DescribeAggregateIdFormat	DescribeInstanceAttribute	DescribeSpotInstanceRequests
DescribeAvailabilityZones	DescribeInstanceCreditSpecifications	DescribeSpotPriceHistory
DescribeBundleTasks	DescribeInstances	DescribeStateSecurityGroups
DescribeByoipCidrs	DescribeInstanceStatus	DescribeSubnets
DescribeCapacityReservations	DescribeInternetGateways	DescribeTransitGatewayAttachments
DescribeClassicLinkInstances	DescribeKeyPairs	DescribeTransitGatewayRouteTables
DescribeClientVpnAuthorizationRules	DescribeLaunchTemplates	DescribeTransitGateways
DescribeClientVpnConnections	DescribeLaunchTemplateVersions	DescribeTransitGatewayVpcAttachments
DescribeClientVpnEndpoints	DescribeMovingAddresses	DescribeVolumeAttribute
DescribeClientVpnRoutes	DescribeNatGateways	DescribeVolumes
DescribeClientVpnTargetNetworks	DescribeNetworkAcls	DescribeVolumeStatus
DescribeConversionTasks	DescribeNetworkInterfaceAttribute	DescribeVpcAttribute
DescribeCustomerGateways	DescribeNetworkInterfacePermissions	DescribeVpcClassicLink
DescribeDhcpOptions	DescribeNetworkInterfaces	DescribeVpcClassicLinkDnsSupport
DescribeEgressOnlyInternetGateways	DescribePlacementGroups	DescribeVpcEndpointConnectionNotifications
DescribeExportTasks	DescribePrefixLists	DescribeVpcEndpointConnections
DescribeFleetHistory	DescribePrincipalIdFormat	DescribeVpcEndpoints
DescribeFleetInstances	DescribePublicIpv4Pools	DescribeVpcEndpointServiceConfigurations
DescribeFleets	DescribeRegions	DescribeVpcEndpointServicePermissions
DescribeFlowLogs	DescribeReservedInstances	DescribeVpcEndpointServices
DescribeFpgaImageAttribute	DescribeReservedInstancesListings	DescribeVpcPeeringConnections
DescribeFpgaImages	DescribeReservedInstancesModifications	DescribeVpcs
DescribeHostReservationOfferings	DescribeReservedInstancesOfferings	DescribeVpnGateways
DescribeHostReservations	DescribeRouteTables	ExportClientVpnClientCertificateRevocationList

Set condition

▼ Request conditions

close

☐ MFA required
Requires users to authenticate with an MFA device to perform the specified actions

☐ Source IP
Allow access to the specified actions only when the request comes from the specified IP address range.

Add condition

Edit request condition

✕

Condition key

ec2:Region

▼

Qualifier

For any value in request

▼

Operator

StringEquals

▼

☐ If exists

Value

N. Virginia

+

Add another condition value

Cancel

Save changes

EC2 (107 actions)

CloneRemove

Service

EC2

Actions

Specify the actions allowed in EC2

Switch to deny permissions

close

Filter actions

Manual actions (add actions)

☐ All EC2 actions (ec2:*)

Access level

☒ List (95 selected)

☒ Read (12 selected)

☐ Tagging

☐ Write

Expand allCollapse all

Resources

All resources

Request conditions

ec2:Region (StringEquals N.Virginia)

Add additional permissions

Cancel

Review policy

Review and create Policy

Review policy

Name*

Testpolicy

Use alphanumeric and '+=, @, _' characters. Maximum 128 characters.

Description

Providing access to North Virginia

Maximum 1000 characters. Use alphanumeric and '+=, @, _' characters.

Summary

Filter

Service	Access level	Resource	Request condition
Allow (1 of 177 services) Show remaining 176			
EC2	Full: List, Read	All resources	ec2:Region = N.Virginia

* Required

Cancel

Previous

Create policy

Testpolicy has been created.

Create policy

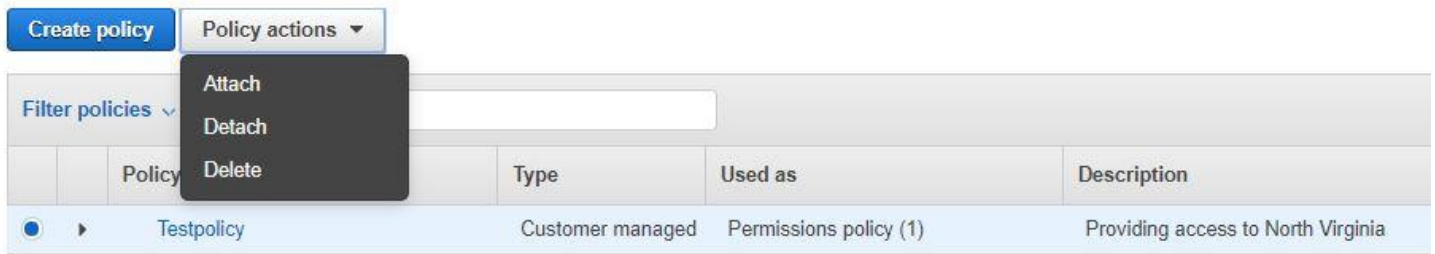
Policy actions

Filter policies

ec2

Showing 26 results

	Policy name	Type	Used as	Description
<input type="radio"/>	AmazonEC2ContainerRegistryFu...	AWS managed	None	Provides administrative access to Amazon ECR resources
<input type="radio"/>	AmazonEC2ContainerRegistryPo...	AWS managed	None	Provides full access to Amazon EC2 Container Registry repositories, but doe...
<input type="radio"/>	AmazonEC2ContainerRegistryR...	AWS managed	None	Provides read-only access to Amazon EC2 Container Registry repositories.



Use “**Attach**” to attach the policy to a group.

Adding MFA to a user

MFA is a additional authentication for user you can add mobile device of user to avoid hacking.

Go to user in the security credentials you find MFA

Users: vipul

User ARN: arn:aws:iam:::user/vipul
Path: /
Creation time: 2017-02-26 22:20 UTC+0530

Select "Security credentials" tab

Permissions Groups (0) **Security credentials** Access Advisor

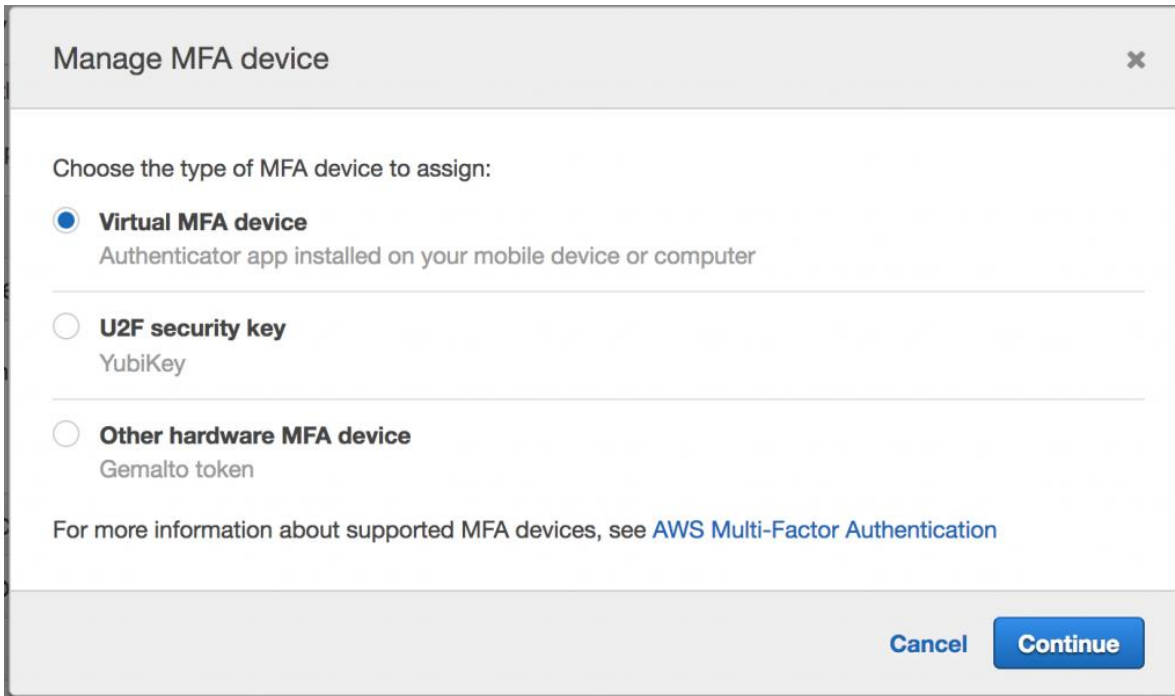
Add permissions Number of attached policies 1

IAMUserChangePassword - AWS Managed policy Add inline policy

Sign-in credentials

Console password	Enabled Manage password
Console login link	https://signin.aws.amazon.com/console
Last login	2018-04-06 10:04 UTC+0300
Assigned MFA device	No
Signing certificates	None

Edit “Assigned MFA device” and select “Virtual MFA device”



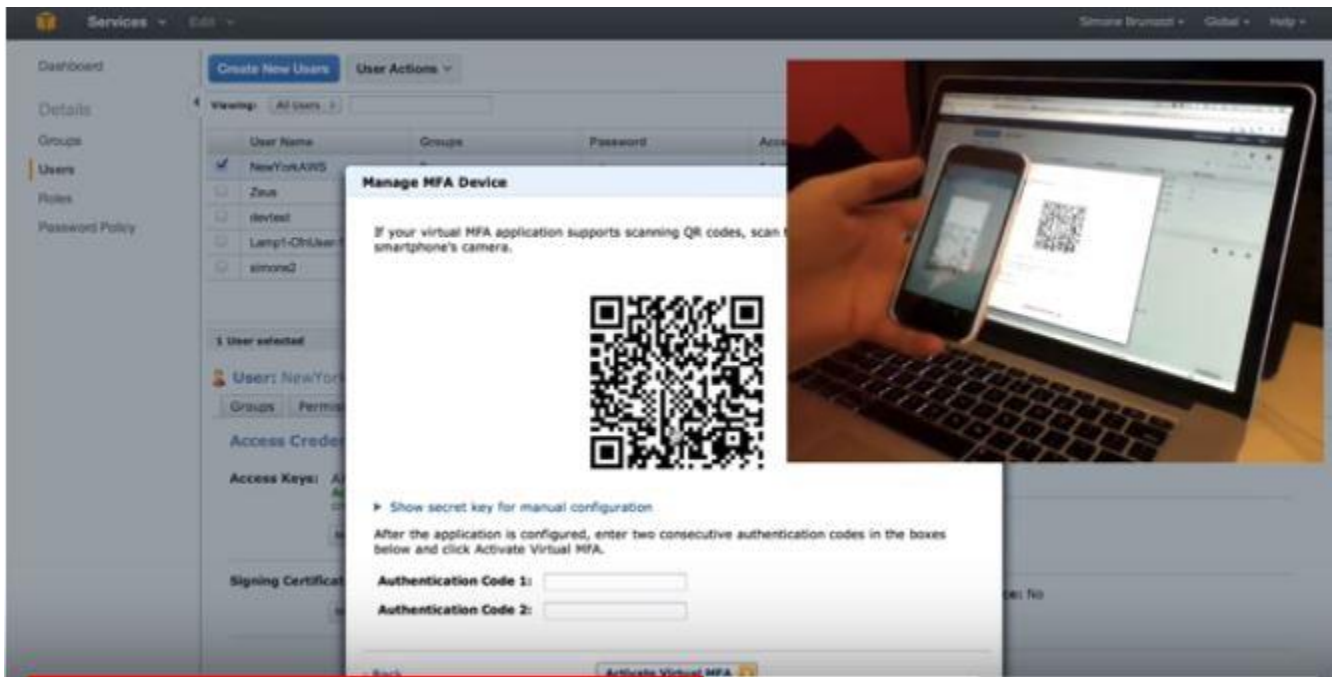
The screenshot shows a 'Manage MFA device' dialog box with a close button (X) in the top right corner. The main heading is 'Manage MFA device'. Below it, the instruction 'Choose the type of MFA device to assign:' is followed by three radio button options:

- ☒ **Virtual MFA device**
Authenticator app installed on your mobile device or computer
- ☐ **U2F security key**
YubiKey
- ☐ **Other hardware MFA device**
Gemalto token

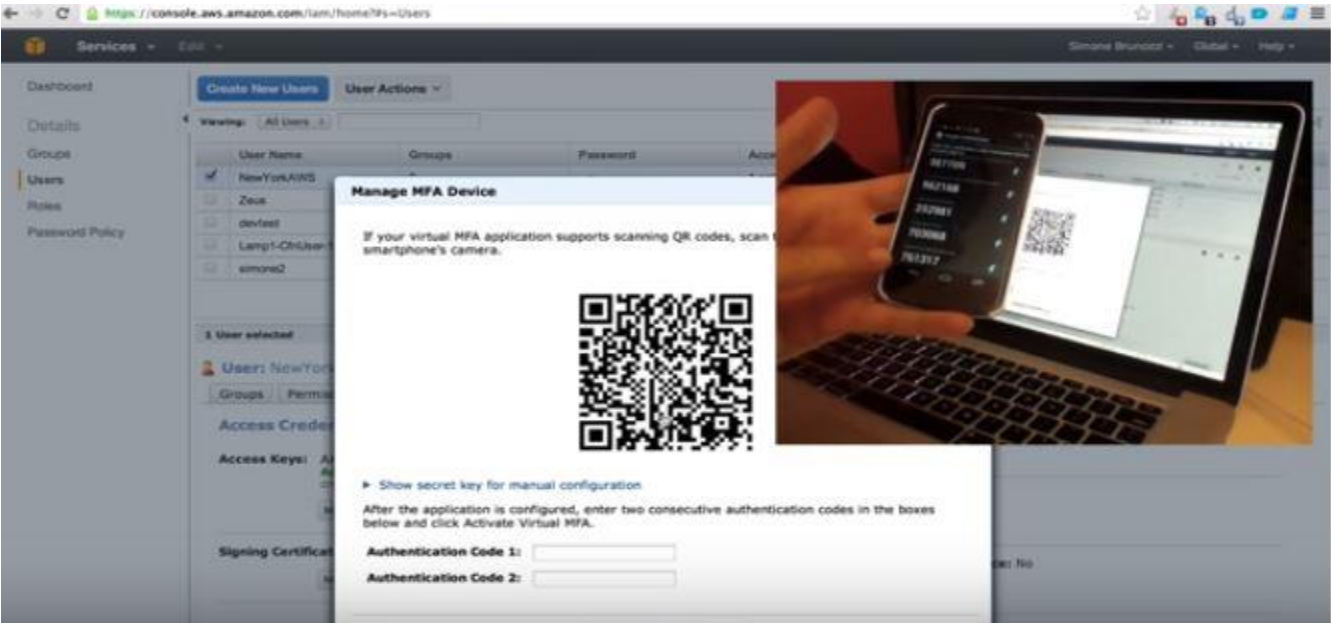
Below the options, a link states: 'For more information about supported MFA devices, see [AWS Multi-Factor Authentication](#)'. At the bottom right, there are 'Cancel' and 'Continue' buttons.

Install Google Authenticator in your mobile.

You will get a QR code scan using mobile.



Once your code get scanned you will be getting code in your app enter that code your device will be added and you will be geetting this code automatically.



Then your code will be keep on changing user the current code to login while it through MFA authentication.


ROLES:


Create a role and Assign it to a EC2 instance Go to Roles and select service you are going to assign


Create role


1234

Select type of trusted entity

 **AWS service**
EC2, Lambda and others

 **Another AWS account**
Belonging to you or 3rd party

 **Web identity**
Cognito or any OpenID provider

 **SAML 2.0 federation**
Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose the service that will use this role

EC2
Allows EC2 instances to call AWS services on your behalf.

Lambda
Allows Lambda functions to call AWS services on your behalf.

API Gateway	CodeDeploy	EKS	Kinesis	S3
AWS Backup	Comprehend	EMR	Lambda	SMS
AWS Support	Config	ElastiCache	Lex	SNS
Amplify	Connect	Elastic Beanstalk	License Manager	SWF
AppSync	DMS	Elastic Container Service	Machine Learning	SageMaker
Application Auto Scaling	Data Lifecycle Manager	Elastic Transcoder	Macie	Security Hub
Application Discovery Service	Data Pipeline	ElasticLoadBalancing	MediaConvert	Service Catalog

* Required

CancelNext: Permissions

Next Add permission to the selected service

Create role

1234

▼ Attach permissions policies

Choose one or more policies to attach to your new role.


Create policy

↺

Filter policies ▼

Q s3full

Showing 1 result

	Policy name ▼	Used as	Description
<input checked="" type="checkbox"/>	▶  AmazonS3FullAccess	None	Provides full access to all buckets via the...

▶ Set permissions boundary

* Required

CancelPreviousNext: Tags

Next Add tags

Create role

1234

Add tags (optional)

IAM tags are key-value pairs you can add to your role. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this role. [Learn more](#)

Key	Value (optional)	Remove
<input type="text" value="name"/>	<input type="text" value="full s3 "/>	✕
<input type="text" value="Add new key"/>	<input type="text"/>	

You can add 49 more tags.

Review the Role and create role

Review

Provide the required information below and review this role before you create it.

Role name*

s3_test

Use alphanumeric and '+=, @-_' characters. Maximum 64 characters.

Role description



Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and '+=, @-_' characters.

Trusted entities

AWS service: ec2.amazonaws.com

Policies

 AmazonS3FullAccess 

Permissions boundary

Permissions boundary is not set

The new role will receive the following tag

Key	Value
name	full s3

* Required

Cancel

Previous

Create role

Assign a Role to the EC2 instance

Filter by tags and attributes or search by keyword

	Name	Instance ID	Instance Type	Availability
<input checked="" type="checkbox"/>		d7b351d	t2.micro	us-east-1d
<input type="checkbox"/>		ed148	t2.micro	us-east-1d

Connect

Get Windows Password

Create Template From Instance

Launch More Like This

Instance State

Instance Settings

Image

Networking

CloudWatch Monitoring

Add/Edit Tags

Attach to Auto Scaling Group

Attach/Replace IAM Role

Change Instance Type

Change Termination Protection

View/Change User Data

Change Shutdown Behavior

Change T2/T3 Unlimited

Get System Log

Get Instance Screenshot

Modify Instance Placement

Modify Capacity Reservation Settings

Instance: i-02aac0ba44d7b351d (Ansible)

Description

Status Checks

More

Instance ID	i-02aac0ba44d7b351d
Instance state	stopped
Instance type	t2.micro
Elastic IPs	

Attach/Replace IAM Role

Select an IAM role to attach to your instance. If you don't have any IAM roles, choose Create new IAM role to create a role in the IAM console. If an IAM role is already attached to your instance, the IAM role you choose will replace the existing role.

Instance ID i-02aac0ba44d7b351d (Ansible)  

IAM role* EC2_S3  [Create new IAM role](#) 

* Required

 Filter by attributes

Profile Name

No Role

ec2

EC2_S3

Cancel

Apply

Now this EC2 instance have full access to S3 bucket.

Try by creating different Roles

----- END of the Document -----