

←→↻us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/create

aws

Search[Alt+S]

IAM>Users>Create user

Step 1Specify user details

Step 2Set permissions

Step 3Review and create

Step 4Retrieve password

Specify user details

User details

User name

karamjot

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☒ Provide user access to the AWS Management Console - optional

If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

Are you providing console access to a person?

User type

☐ Specify a user in Identity Center - Recommended

We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

☒ I want to create an IAM user

We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

☐ Autogenerated password

You can view the password after you create the user.

☒ Custom password

Enter a custom password for the user.

• Must be at least 8 characters long

• Must include at least three of the following mix of characters: lower case letters (a-z), upper case letters (A-Z), numbers (0-9), and symbols ! @ # \$ % ^ & * () _ + = { } | ; ' , . ~ - (hyphen) = ! ! ! ! !

CloudShellFeedback© 2024, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

eu-north-1.console.aws.amazon.com/console/home?region=eu-north-1#

awsSearch [Alt+S]

Stockholm karamjot @ 2111-2555-8466

Verify it's you

Console Home

Info

Recently visited

Info

No recently visited services

Explore one of these commonly visited AWS services.

EC2 S3 RDS Lambda

View all services

Applications (0)

Info

Region: Europe (Stockholm)

eu-north-1 (Current Region) Find applications

< 1 >

Name	Description	Region	Originati.	★ ▲
Access denied to servicecatalog:ListApplications				

Go to myApplications

Welcome to AWS

Getting started with AWS

Learn the fundamentals and find valuable information to

AWS Health

Info

Cost and usage

Info

Current month costs

Access denied

Forecasted month end costs

Cost breakdown

Access denied

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

New: AWS User Notifications quick setup

Enable common notifications for CloudWatch, EC2, and Health using the new quick setup feature in AWS User Notifications.

Done



IAM user sign in ⓘ

Account ID (12 digits) or account alias

211125558466

IAM username

karamjot

Password

.....

☐ Show Password

[Having trouble?](#)

Sign in

Sign in using root user email

[Create a new AWS account](#)

☐ Remember this account

By continuing, you agree to [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

Amazon Lightsail

Lightsail is the easiest way to get started on AWS

Learn more »



Permissions

Entities attached

Policy versions
(5)

Last Accessed

Permissions defined in this policy [Info](#)

Copy

Summary

JSON

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Action": "ec2:*",  
6       "Effect": "Allow",  
7       "Resource": "*"   
8     },  
9     {  
10      "Effect": "Allow",  
11      "Action": "elasticloadbalancing:*",  
12      "Resource": "*"   
13    },  
14    {  
15      "Effect": "Allow",  
16      "Action": "cloudwatch:*",  
17      "Resource": "*"   
18    },  
19    {  
20      "Effect": "Allow",  
21      "Action": "autoscaling:*",  
22      "Resource": "*"   
23    },  
24    {  
25      "Effect": "Allow",  
26      "Action": "iam:CreateServiceLinkedRole",  
27      "Resource": "*",  
28      "Condition": {  
29        "StringEquals": {  
30          "iam:AWSServiceName": [  
31            "autoscaling.amazonaws.com",
```

1 policy added



karamjot

Info

Delete

Summary

ARN
arn:aws:iam::211125558466:user/karamjot

Created
December 26, 2024, 23:14 (UTC+05:30)

Console access
Enabled without MFA

Last console sign-in
Today

Access key 1
Create access key

- Permissions
- Groups
- Tags
- Security credentials
- Last Accessed

Permissions policies (2)



Remove

Add permissions

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type



Search

All types



1



Policy name



Type



Attached via



AmazonEC2FullAccess

AWS managed

Directly



IAMReadOnlyAccess

AWS managed

Directly

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Introducing the new Security Credentials experience
We've redesigned the Security Credentials experience to make it easier to use. [Let us know what you think.](#)

IAM > Security credentials

My security credentials (root user) [Info](#)

The root user has access to all AWS resources in this account, and we recommend following [best practices](#). To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in [AWS General Reference](#).



MFA not activated for root user

The root user for this account does not have multi-factor authentication (MFA) activated. Activate MFA to improve security for this account.

Assign MFA

Account details

Edit account name, email, and password

Select MFA device

Step 2

Set up device

Select MFA device

Specify MFA device name

Device name

Enter a meaningful name to identify this device.

mytable

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

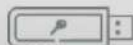
Select MFA device [Info](#)

Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.



Authenticator app

Authenticate using a code generated by an app installed on your mobile device or computer.



Security Key

Authenticate using a code generated by touching a YubiKey or other supported FIDO security key.



Hardware TOTP token

macdLinuxCloudDevOpscliqrwordpressDeveloperHackLabAIOTCiscoosfyf5loadbalancerimpiddhiseo

awsServicesSearch[Alt+S]

IAM > Security credentials > Assign MFA device

Step 1
Select MFA device

Step 2
Set up device

Set up device

Set up your authenticator app

A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

1

Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.
See a list of compatible applications

2

Show QR code

Open your authenticator app, chose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key. Show secret key

Fill in two consecutive codes from your MFA device.

MFA code 1


macdLinuxCloudDevOpscliqrwordpressDeveloperHackLabAIOTciscoosfyf5loadbalancerimpiddhiseo

awsServicesSearch[Alt+S]

1

Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.
[See a list of compatible applications](#)

2



Open your authenticator app, chose **Show QR code on this page**, then use the app to scan the code. Alternatively, you can type a secret key.
[Show secret key](#)

3

Fill in two consecutive codes from your MFA device.

MFA code 1

MFA code 2

Cancel

Previous

Add MFA

aws

Services

Search

[Alt+S]

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
 - Archive rules
 - Analyzers
 - Settings
- Credential report
- Organization activity

AWS account ID

392833926319

Canonical user ID

e78ae569d4b2e675a37fc5c81605436f3c8626290f2d

Multi-factor authentication (MFA) (1)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 1 MFA device. [Learn more](#)

Remove

Resync

Assign MFA device

	Device type	Identifier	Created on
<input type="radio"/>	Virtual	arn:aws:iam::392833926319:mfa/mytable	

Access keys (0)

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys per user. Access keys are inactive if not used for 90 days. [Learn more](#)

Create access key

Access key ID	Created on	Access key last used	Region last used	Service last used
No access keys				

As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials.