

[illegible]

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 character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # \$ % ^ & * () _ + - (hyphen) = [] { } | ' "

☐ Show password

☒ Users must create a new password at next sign-in - Recommended

Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

i If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Cancel

Next

User created successfully

View user

×

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Step 1

[Specify user details](#)

Step 2

[Set permissions](#)

Step 3

[Review and create](#)

Step 4

Retrieve password

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

Email sign-in instructions

Console sign-in URL

https://891377195615.signin.aws.amazon.com/console

User name

induja

Console password

***** Show

Cancel

Download .csv file

Return to users list

travel_application user group created.

View group

×

IAM > User groups

User groups (1) info

↻

Delete

Create group

User groups (1) Info

Refresh

Delete

Create group

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Search

< 1 >

⚙

☐

Group name

▲

Users

▼

Permissions

▼

Creation time

▼

☐

[travel_application](#)

1

⚠ Not defined

Now

✔ developer user group created.

View group

ⓘ

⌵

[IAM](#) > User groups

User groups (1) Info

Refresh

Delete

Create group

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Search

< 1 >

⚙

☐

Group name

▲

Users

▼

Permissions

▼

Creation time

▼

☐

[developer](#)

1

✔ Defined

Now

Role name

Enter a meaningful name to identify this role.

developer

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

Description

Add a short explanation for this role.

Allows EC2 instances to call AWS services on your behalf.

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

Step 1: Select trusted entities

Edit

Trust policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": [  
7         "sts:AssumeRole"
```

© 2021 Amazon Web Services, Inc. or its affiliates. Privacy | Terms | Feedback

✓ Role developer created.

View role



by entities that you trust.

Search



1



Role name



Trusted entities

Roles Anywhere [Info](#)

Manage

Authenticate your non AWS workloads and securely provide access to AWS services.



Access AWS from your non AWS workloads

Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.



X.509 Standard

Use your own existing PKI infrastructure or use [AWS Certificate Manager Private Certificate Authority](#) to authenticate identities.



Temporary credentials

Use temporary credentials with ease and benefit from the enhanced security they provide.