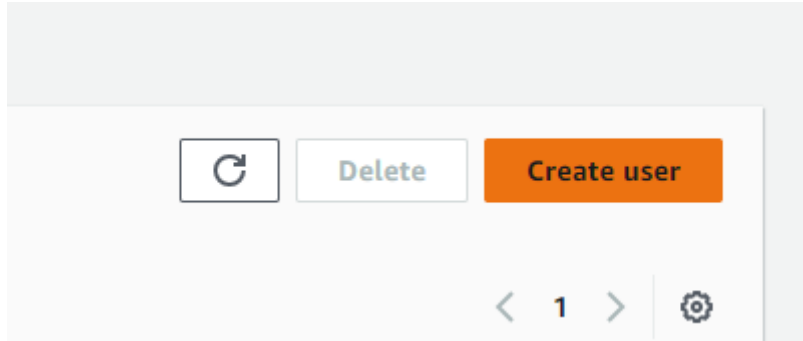


IAM USER

SHARMEEN SHAIKH A106



IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Specify user details

User details

User name

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.

i If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keys

Specify user details

User details

User name

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.

i If you are creating programmatic access through access keys or service-specific credentials for AWS Co

User details

User name

sharryuser

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.

Next

[IAM](#) > [Users](#) > Create user

Step 1

[Specify user details](#)

Step 2

Set permissions

Step 3

Review and create

Step 4

Retrieve password

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user

Permissions options

☒ Add user to group

Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ Copy permission

Copy all group me
policies from an ex



Get started with groups

Create a group and select policies to attach to the group. We recommend using groups to m

► **Set permissions boundary - optional**


Review and create

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

User details

User name sharryuser	Console password type Autogenerated	Require password reset Yes
-------------------------	--	-------------------------------

Permissions summary

Name 	Type	Used as
IAMUserChangePassword	AWS managed	Permissions policy

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

✔ User created successfully

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

[IAM](#) > [Users](#) > Create user

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

Console sign-in details


Console sign-in URL

 <https://796329916611.signin.aws.amazon.com/console>

User name

 sharryuser

Console password

 ***** [Show](#)

Copy url given

Go to incognito and paste url

Copy username and password



Sign in as IAM user

Account ID (12 digits) or account alias

796329916611

IAM user name

sharryuser

Password

.....

☐ Remember this account

Sign in

[Sign in using root user email](#)

[Forgot password?](#)

AWS account 796329916611

IAM user name sharryuser

Old password

New password

Retype new password

Confirm password change

[Sign in using root user email](#)

Now go back to prev tab

Users->continue

Click on the username

A new window opens

[IAM](#) > [Users](#) > sharryuser

sharryuser

Info

Summary

ARN

arn:aws:iam::796329916611:user/sharryuser

Created

March 14, 2024, 08:21 (UTC+05:30)

Console access

Enabled without MFA

Last console sign-in

Today

Access key 1

Create access key

Permissions

Groups

Tags

Security credentials

Access Advisor

Permissions policies (1)

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

Search

Filter by Type

All types

	Policy name	Type	Attached via
<input type="checkbox"/>	IAMUserChangePassword	AWS managed	Directly

Policies (1/1176)

Info

A policy is an object in AWS that defines permissions.

Search S3

Filter by Type

All types

12 matches

	Policy name	Type	Used as	Description
<input type="radio"/>	AmazonDMSRedshiftS3Role	AWS managed	None	Provides access to manage S3 settings fo...
<input checked="" type="radio"/>	AmazonS3FullAccess	AWS managed	None	Provides full access to all buckets via the ...
<input type="radio"/>	AmazonS3ObjectLambdaExecutionRolePo...	AWS managed	None	Provides AWS Lambda functions permissi...

Specify permissions [Info](#)

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

▼ **S3**
Allow All actions

Specify what actions can be performed on specific resources in **S3**.

▼ Actions allowed

Specify actions from the service to be allowed.

Manual actions | [Add actions](#)

☒ All S3 actions (s3:*)

Access level

- ▶ List (Selected 15/15)
- ▶ Read (Selected 60/60)
- ▶ Write (Selected 56/56)
- ▶ Permissions management (Selected 15/15)
- ▶ Tagging (Selected 12/12)

Manual actions | [Add actions](#)

☒ All S3 actions (s3:*)

Access level

- ▶ List (Selected 15/15)
- ▶ Read (Selected 60/60)
- ▶ Write (Selected 56/56)
- ▶ Permissions management (Selected 15/15)
- ▶ Tagging (Selected 12/12)

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

Required permissions not selected.

To grant permissions for the selected resource actions, you must include additional required actions

- s3:CreateJob requires [1 more](#) action.
- s3:PutReplicationConfiguration requires [1 more](#) action.

▼ Resources

Specify resource ARNs for these actions.

- ☒ All
- ☐ Specific

The all wildcard "*" may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.

▶ Request conditions - optional

Actions on resources are allowed or denied only when these conditions are met.

[+ Add more permissions](#)

[IAM](#) > [Policies](#) > Create policy

Step 1
[Specify permissions](#)

Step 2
Review and create

Review and create [Info](#)

Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.

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

Description - optional
Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and "+=, @, _" characters.

Permissions defined in this policy [Info](#)

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

Allow (1 of 404 services)

Service	Access level	Resource	Request condition
S3	Full access	All resources	None

Create policy

Now go back to Previous tab of incognito->click service->S3

Now u can see create bucket service is enabled

NOW FOR ec2->select EC2 full access in policies

Policies (1/1177) [Info](#)

A policy is an object in AWS that defines permissions.

	Policy name	Type	Used as
<input type="radio"/>	AmazonEC2ContainerRegistryFullAccess	AWS managed	None
<input type="radio"/>	AmazonEC2ContainerRegistryPowerUser	AWS managed	None
<input type="radio"/>	AmazonEC2ContainerRegistryReadOnly	AWS managed	None
<input type="radio"/>	AmazonEC2ContainerServiceAutoscaleRole	AWS managed	None
<input type="radio"/>	AmazonEC2ContainerServiceEventsRole	AWS managed	None
<input type="radio"/>	AmazonEC2ContainerServiceforEC2Role	AWS managed	None
<input type="radio"/>	AmazonEC2ContainerServiceRole	AWS managed	None
<input checked="" type="radio"/>	AmazonEC2FullAccess	AWS managed	None

Now create group->go to user groups and create groups

Give a name

In the checklist select EC2f

Now click on the group->verify group is created

The window is visible

[IAM](#) > [User groups](#) > sharrygroup

sharrygroup [Info](#)

Summary

User group name
sharrygroup

Creation time
March 14, 2024, 08:41 (UTC+05:30)

ARN
[Copy](#)

[Users \(1\)](#)

[Permissions](#)

[Access Advisor](#)

Users in this group (1)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

☐ [User name](#)

☐ [sharryuser](#)

Verify policies are attached

[IAM](#) > [Users](#) > sharryuser

sharryuser [Info](#)

Summary

ARN
[Copy](#) `arn:aws:iam::796329916611:user/sharryuser`

Created
March 14, 2024, 08:21 (UTC+05:30)

Console access
[Copy](#) **Enabled without MFA**

Last console sign-in
[Copy](#) **Today**

Access key 1
[Create access key](#)

[Permissions](#)

[Groups \(1\)](#)

[Tags](#)

[Security credentials](#)

[Access Advisor](#)

Permissions policies (3)

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

[Refresh](#) [Remove](#)

Filter by Type
All types

<input type="checkbox"/>	Policy name	Type	Attached via
<input type="checkbox"/>	AmazonEC2FullAccess	AWS managed	Group sharrygroup
<input type="checkbox"/>	AmazonS3FullAccess	AWS managed	Group sharrygroup
<input type="checkbox"/>	IAMUserChangePassword	AWS managed	Directly