

Create a fully Managed IAM account:

Go to www.aws.amazon.com;

Open IAM to create an account

Welcome to Identity and Access Management

IAM users sign-in link:

<https://514602770466.signin.aws.amazon.com/console> [Customize](#) | [Copy Link](#)

IAM Resources

Users: 0 Roles: 0

Groups: 0 Identity Providers: 0

Customer Managed Policies: 0

Security Status

2 out of 5 complete.

✓

Delete your root access keys

▼

✓

Activate MFA on your root account

▼

⚠

Create individual IAM users

▲

Create IAM users and give them only the permissions they need. Do not use your AWS root account for day-to-day interaction with AWS, because the root account provides unrestricted access to your AWS resources. [Learn More](#)

Manage Users

⚠

Use groups to assign permissions

▼

⚠

Apply an IAM password policy

▼

Add userDelete user

Find users by username or access key

Show

<input type="checkbox"/>	User name ▼	Groups	Access key age	Password age	Last activity
There are no IAM users. Learn more					

We have complete all those 5 as shown in above.

Set user details

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

User name* S3

+ 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.

Console password* ☐ Autogenerated password
☒ Custom password
.....
☐ Show 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.

Set permissions for S3



Add user to group



Copy permissions from existing user







Attach existing policies directly

Attach one or more existing policies directly to the user or create a new policy. [Learn more](#)

Create policy Refresh

Filter: Policy type Q s3 Showing 4 results

	Policy name	Type	Attachments	Description
<input type="checkbox"/>	 AmazonDMSRedshiftS3Role	AWS managed	0	Provides access to manage S3 settings for Redshift endpoints for DMS.
<input checked="" type="checkbox"/>	 AmazonS3FullAccess	AWS managed	0	Provides full access to all buckets via the AWS Management Console.
<input type="checkbox"/>	 AmazonS3ReadOnlyAccess	AWS managed	0	Provides read only access to all buckets via the AWS Management Console.
<input type="checkbox"/>	 QuickSightAccessForS3StorageMa...	AWS managed	0	Policy used by QuickSight team to access customer data produced by S3 Storage ...

We have to provide these all details to proceed further.

Add user



Review

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

User details

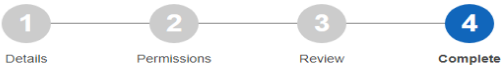
User name	S3
AWS access type	AWS Management Console access - with a password
Console password type	Custom
Require password reset	Yes

Permissions summary

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

Type	Name
Managed policy	AmazonS3FullAccess
Managed policy	IAMUserChangePassword

Add user



✓

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://514602770466.signin.aws.amazon.com/console>

Download .csv

	User	Email login instructions
▶	✓ S3	Send email

Add userDelete user

Close

Find users by username or access key

Showing 1 result

<input type="checkbox"/>	User name ▼	Groups	Access key age	Password age	Last activity	MFA
<input type="checkbox"/>	S3	None	None	Today	None	Not enabled

So first user was created successfully.

Welcome to Identity and Access Management

IAM users sign-in link:

<https://514602770466.signin.aws.amazon.com/console>

[Customize](#) | [Copy Link](#)

IAM Resources

Users: 1

Roles: 0

Groups: 0

Identity Providers: 0

Customer Managed Policies: 0

Security Status

3 out of 5 complete.

<input checked="" type="checkbox"/>	Delete your root access keys	▼
<input checked="" type="checkbox"/>	Activate MFA on your root account	▼
<input checked="" type="checkbox"/>	Create individual IAM users	▼
<input type="checkbox"/>	Use groups to assign permissions	▲
Use IAM groups to assign permissions to your IAM users to simplify managing and auditing permissions in your account. Learn More		
Manage Groups		
<input type="checkbox"/>	Apply an IAM password policy	▼

Set Group Name

Specify a group name. Group names can be edited any time.





Group Name:

Example: Developers or ProjectAlpha
Maximum 128 characters

Filter: Policy Type

Filter

Showing 264 results

		Policy Name	Attached Entities	Creation Time	Edited Time
<input checked="" type="checkbox"/>		AmazonS3FullAccess	1	2015-02-07 00:10 UTC+0530	2015-02-07 00:10 UTC+0530
<input type="checkbox"/>		IAMUserChangePassword	1	2016-11-15 05:55 UTC+0530	2016-11-16 04:48 UTC+0530
<input type="checkbox"/>		AdministratorAccess	0	2015-02-07 00:09 UTC+0530	2015-02-07 00:09 UTC+0530
<input type="checkbox"/>		AmazonAPIGatewayAdministra	0	2015-07-09 23:04 UTC+0530	2015-07-09 23:04 UTC+0530

Filter

Showing 1 results

	Group Name	Users	Inline Policy	Creation Time
<input type="checkbox"/>	acadgroup	0		2017-08-05 10:08 UTC+0530

After these all steps, we have to proceed with account settings to set the password policy.

Minimum password length:

- ☐ Require at least one uppercase letter ⓘ
- ☒ Require at least one lowercase letter ⓘ
- ☐ Require at least one number ⓘ
- ☐ Require at least one non-alphanumeric character ⓘ
- ☒ Allow users to change their own password ⓘ
- ☒ Enable password expiration ⓘ
Password expiration period (in days):
- ☒ Prevent password reuse ⓘ
Number of passwords to remember:
- ☐ Password expiration requires administrator reset ⓘ

Apply password policy

Delete password policy

Security Status

 5 out of 5 complete.

<input checked="" type="checkbox"/>	Delete your root access keys	▼
<input checked="" type="checkbox"/>	Activate MFA on your root account	▼
<input checked="" type="checkbox"/>	Create individual IAM users	▼
<input checked="" type="checkbox"/>	Use groups to assign permissions	▼
<input checked="" type="checkbox"/>	Apply an IAM password policy	▼

Fully managed IAM account Created.