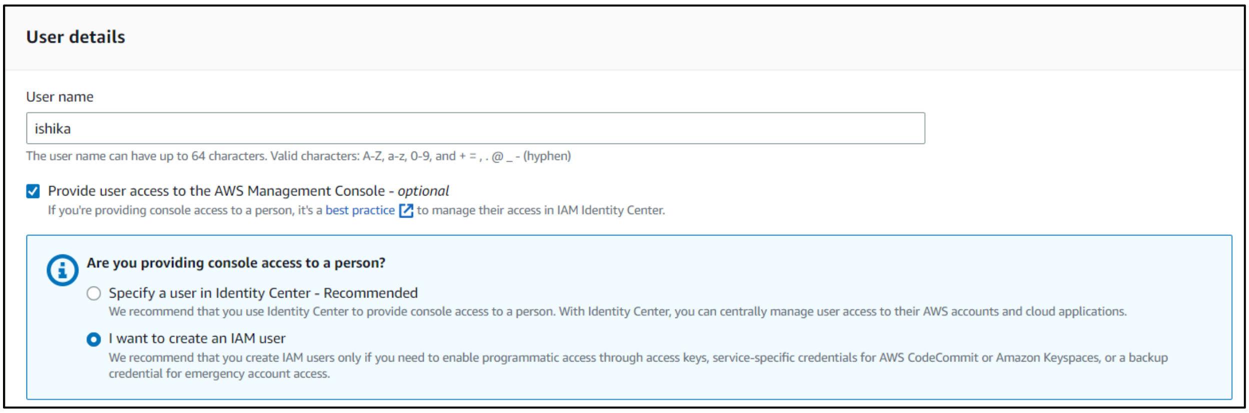


User details

User name

ishika

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?

○ Specify a user in Identity Center - Recommended

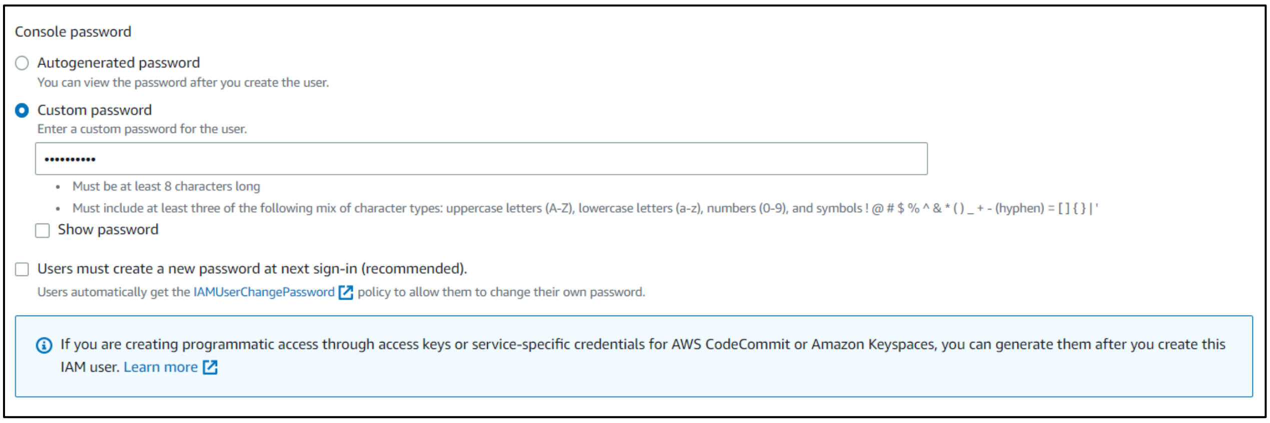
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

● 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.

4. Select the type of access this user will have.

- Select **Enable console access**. This creates a password for the new user.
  - **Custom password** – The user is assigned the password that you type in the box.



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 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).

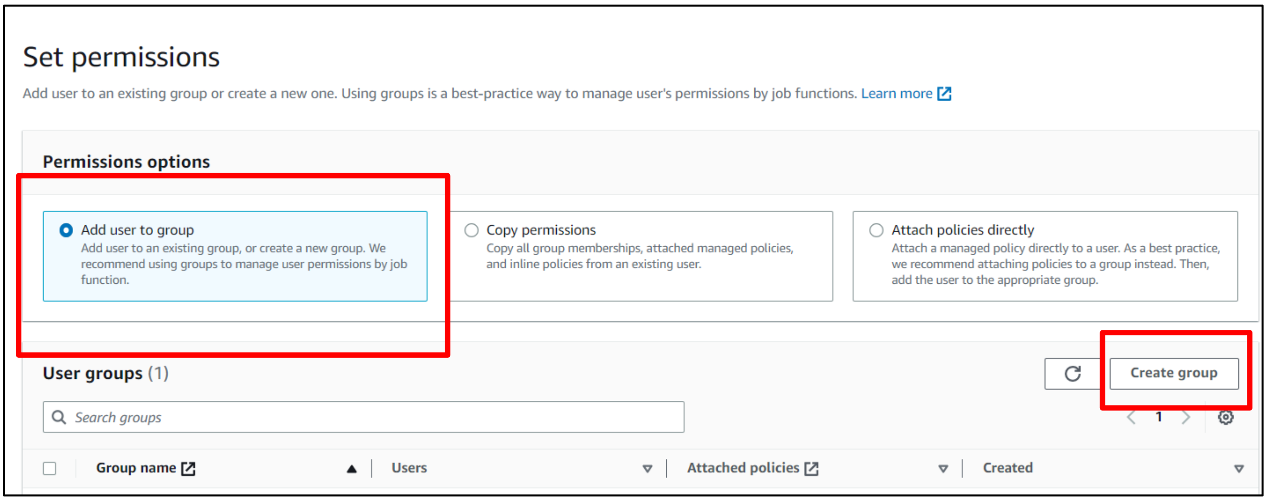
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

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

5. Uncheck Users must create a new password at next sign-in (recommended)

6. Choose **Next.**

7. On the **Set permissions** page, specify how you want to assign permissions to this set of new users. Choose **Add User to Group.**



Set permissions

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

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 permissions

Copy all group memberships, attached managed policies, and inline policies from an existing user.

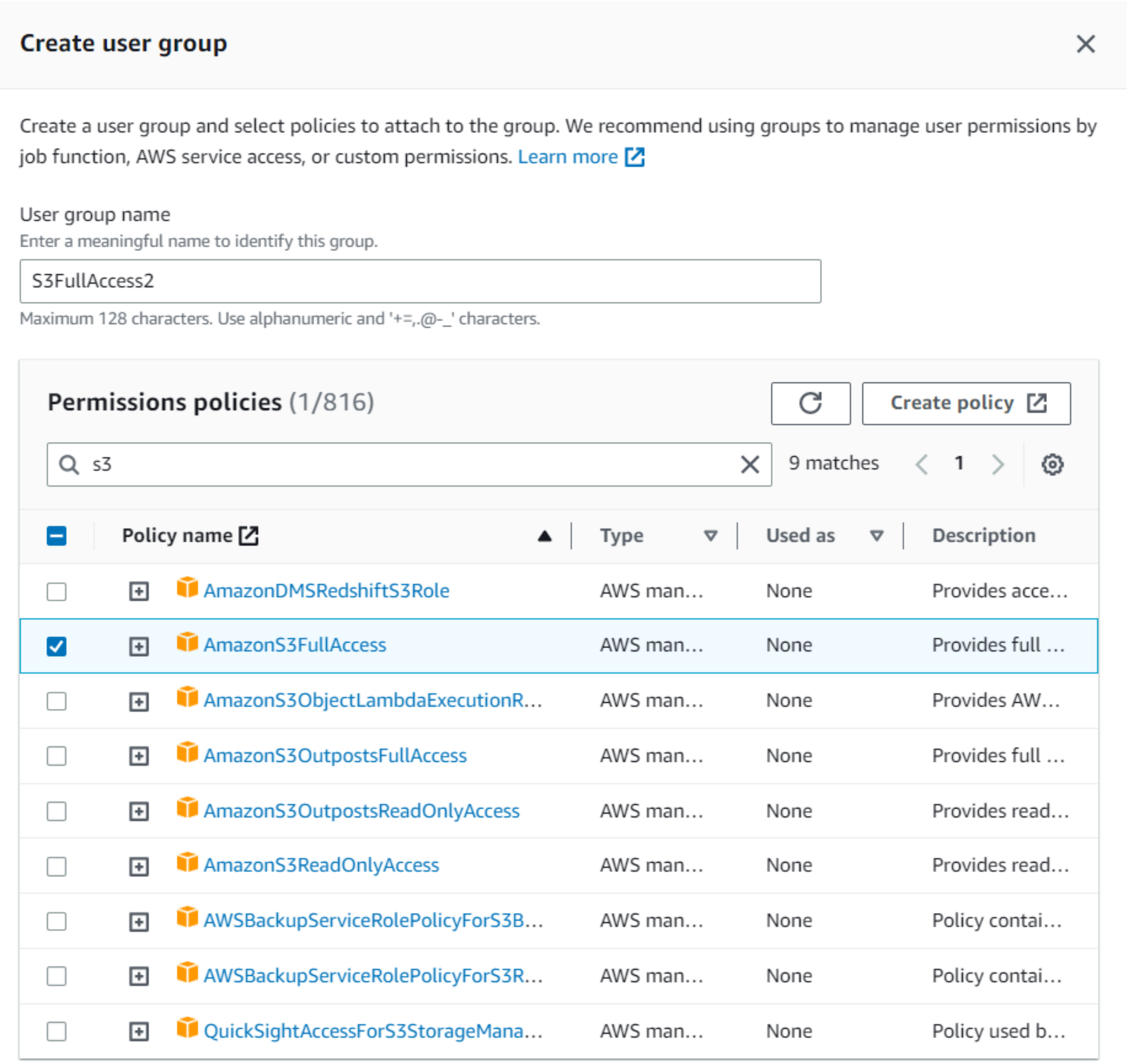
○ Attach policies directly

Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

User groups (1)

□	Group name	Users	Attached policies	Created

- Choose **Create group** to create a new group.
- Give the **User Group Name**
- Give the required **Permission Policies**
- Click Create **User Group**



Create user group

Create a user group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. Learn more

User group name

Enter a meaningful name to identify this group.

S3FullAccess2

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

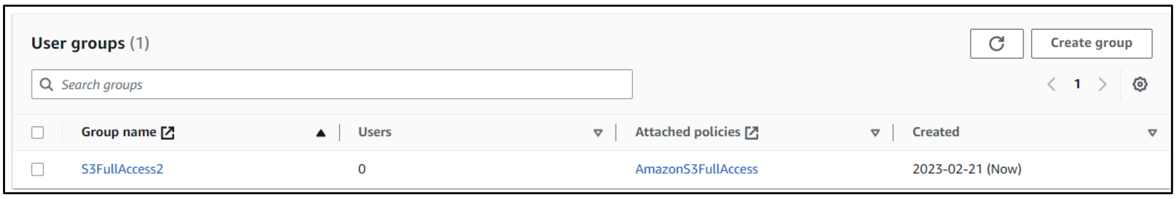
Permissions policies (1/816)

s3

9 matches

	Policy name	Type	Used as	Description
□	AmazonDMSRedshiftS3Role	AWS man…	None	Provides acce…
☑	AmazonS3FullAccess	AWS man…	None	Provides full …
□	AmazonS3ObjectLambdaExecutionR…	AWS man…	None	Provides AW…
□	AmazonS3OutpostsFullAccess	AWS man…	None	Provides full …
□	AmazonS3OutpostsReadOnlyAccess	AWS man…	None	Provides read…
□	AmazonS3ReadOnlyAccess	AWS man…	None	Provides read…
□	AWSBackupServiceRolePolicyForS3B…	AWS man…	None	Policy contai…
□	AWSBackupServiceRolePolicyForS3R…	AWS man…	None	Policy contai…
□	QuickSightAccessForS3StorageMana…	AWS man…	None	Policy used b…

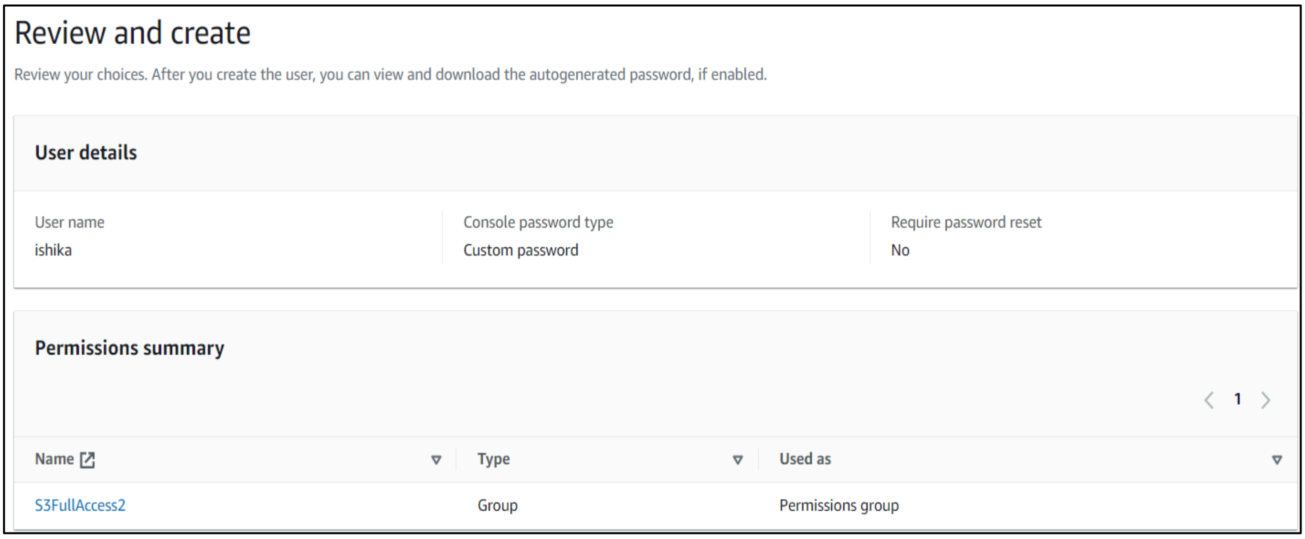
8. Check the Group and Choose **Next**.



User groups (1)

□	Group name	Users	Attached policies	Created
□	S3FullAccess2	0	AmazonS3FullAccess	2023-02-21 (Now)

9. On the **Review and create** page, after reviewing choose **Create user**.



Review and create

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

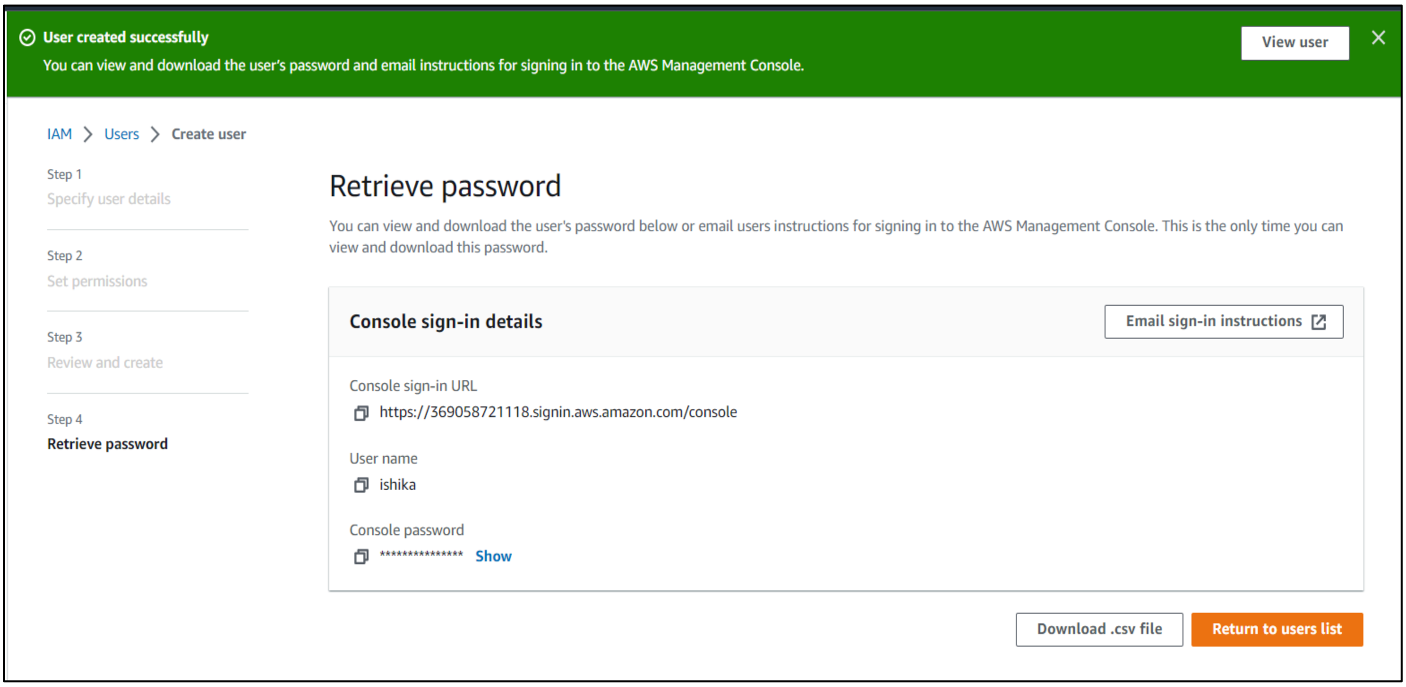
User details

User name	Console password type	Require password reset
ishika	Custom password	No

Permissions summary

Name	Type	Used as
S3FullAccess2	Group	Permissions group

10. To save the password, choose **Download .csv** and then save the file to a safe location.



User created successfully

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

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

Console sign-in URL
https://369058721118.signin.aws.amazon.com/console

User name
ishika

Console password
*************** Show

11. Provide the user with their **credentials**.

12. **New IAM User** is being created with **S3 Full Access**.