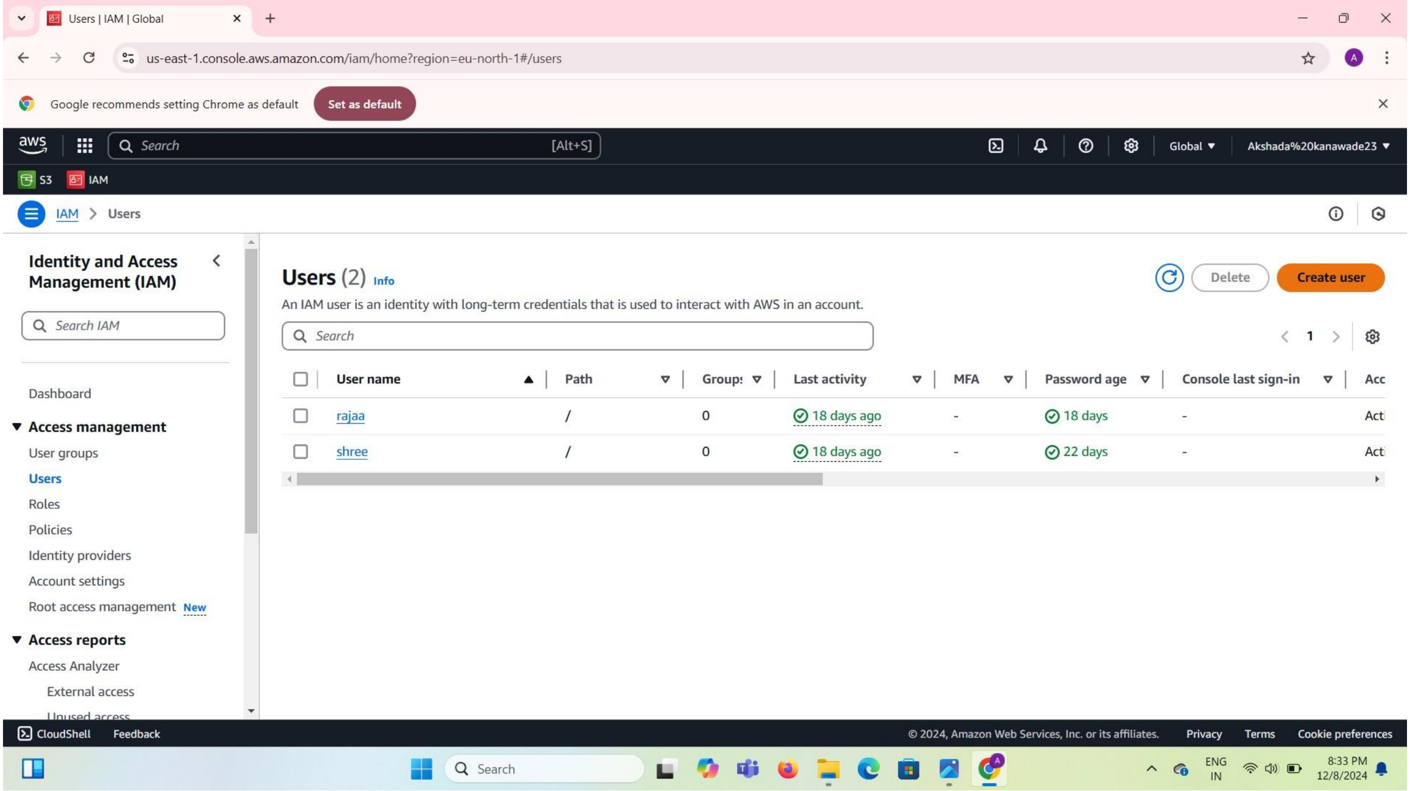
<u>**Akshada Anil Kanawade**</u>

AWS Tasks On IAM Service.

Task 1 :- " Create User And Attach the S3 Permission For One Hour Only."

---

1 . Create A User In IAM Service.

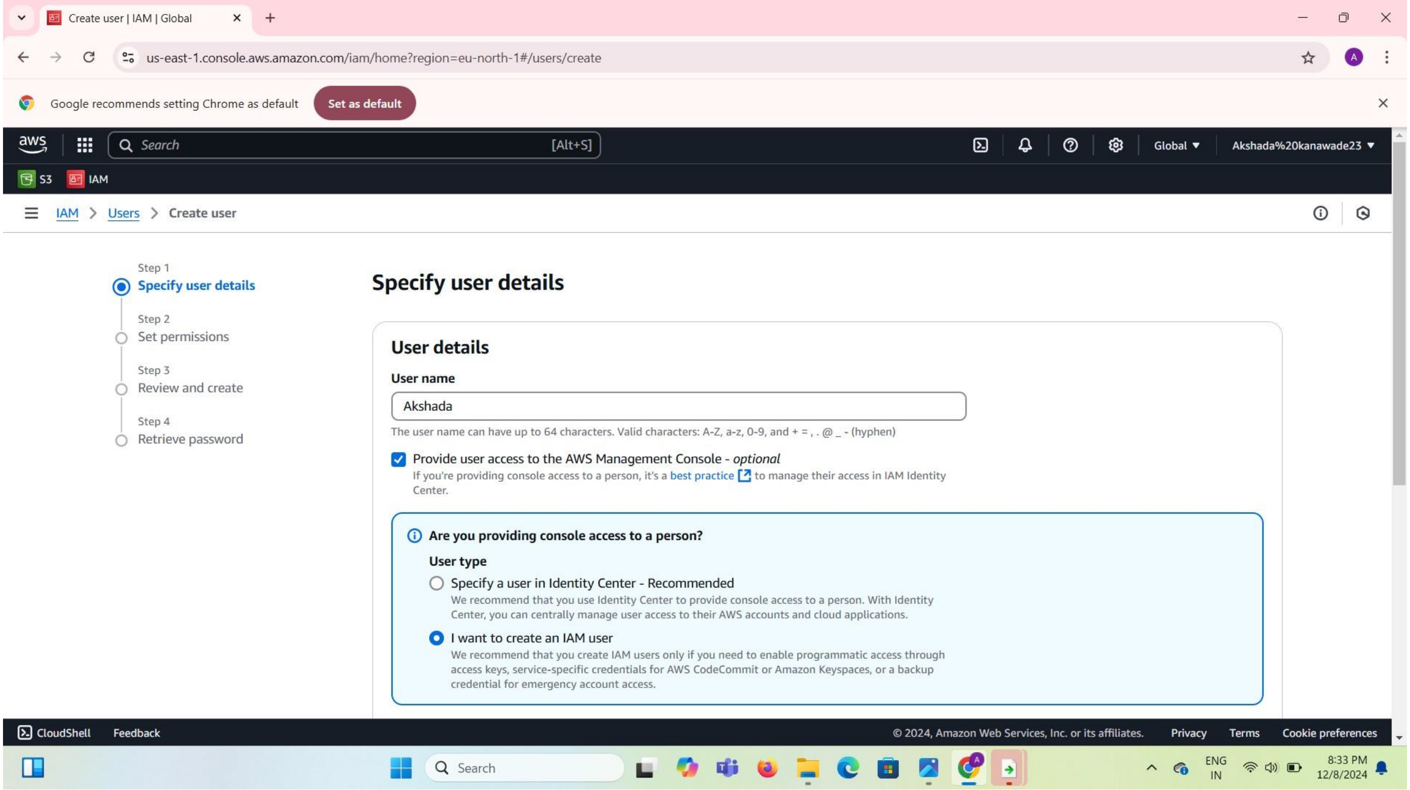


Users (2) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in	Acc
rajaa	/	0	18 days ago	-	18 days	-	Act
shree	/	0	18 days ago	-	22 days	-	Act

2. Enter New User Name.



Create user | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/create
Google recommends setting Chrome as default
Set as default
Search
[Alt+S]
Global
Akshada%20kanawade23
S3
IAM
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
8:33 PM
12/8/2024

Specify user details

User details

User name: Akshada

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

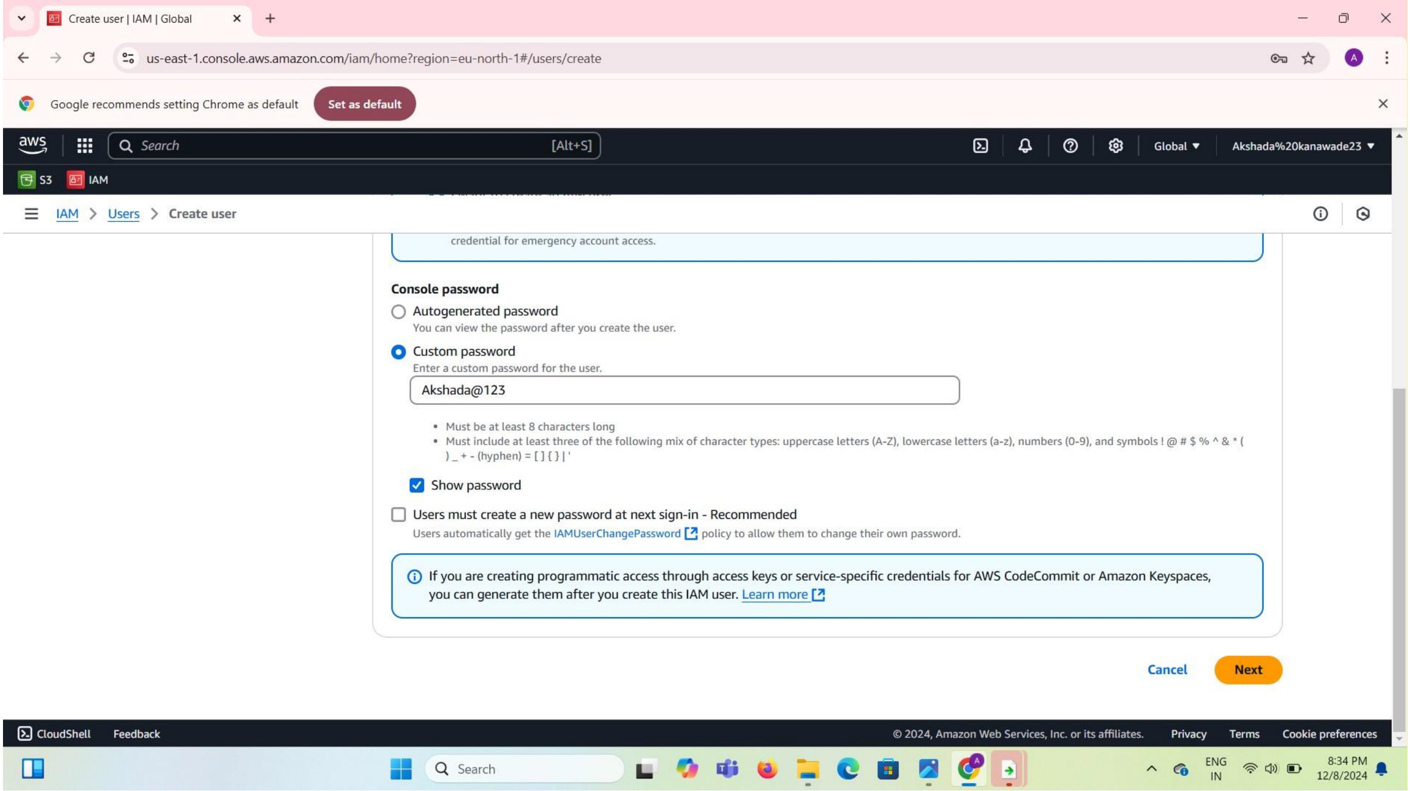
○ Specify a user in Identity Center - Recommended

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.

3. Enter The Password.


Create user | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/create
Google recommends setting Chrome as default
Set as default
aws
Search
[Alt+S]
Global ▾
Akshada%20kanawade23 ▾
S3
IAM
IAM > Users > Create user

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.

Akshada@123

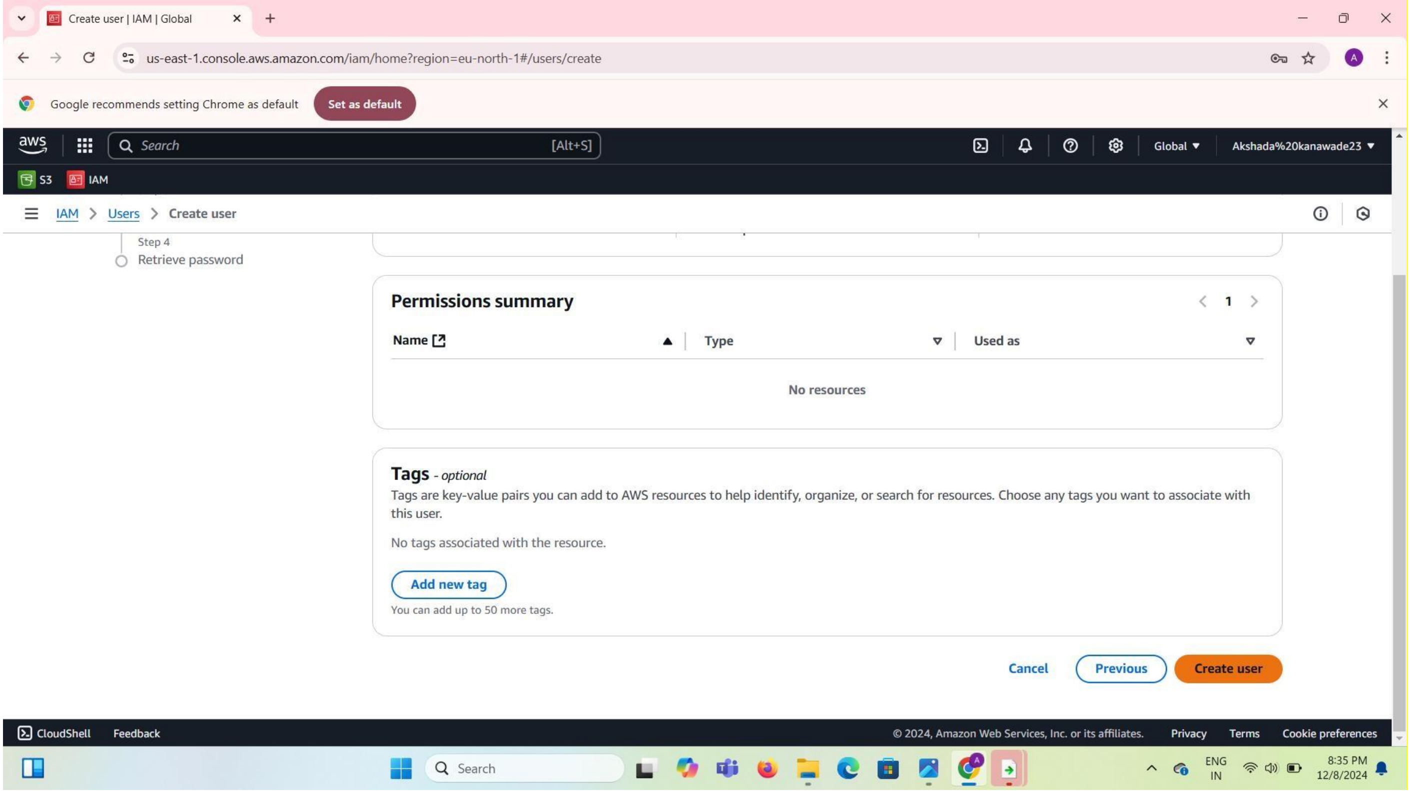
- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

☑ 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

4. Click To Create User


Create user | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/create
Google recommends setting Chrome as default
Set as default
aws
Search
[Alt+S]
Global ▾
Akshada%20kanawade23 ▾
S3
IAM
IAM > Users > Create user
Step 4
Retrieve password

Permissions summary

Name	Type	Used as
No resources		

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.

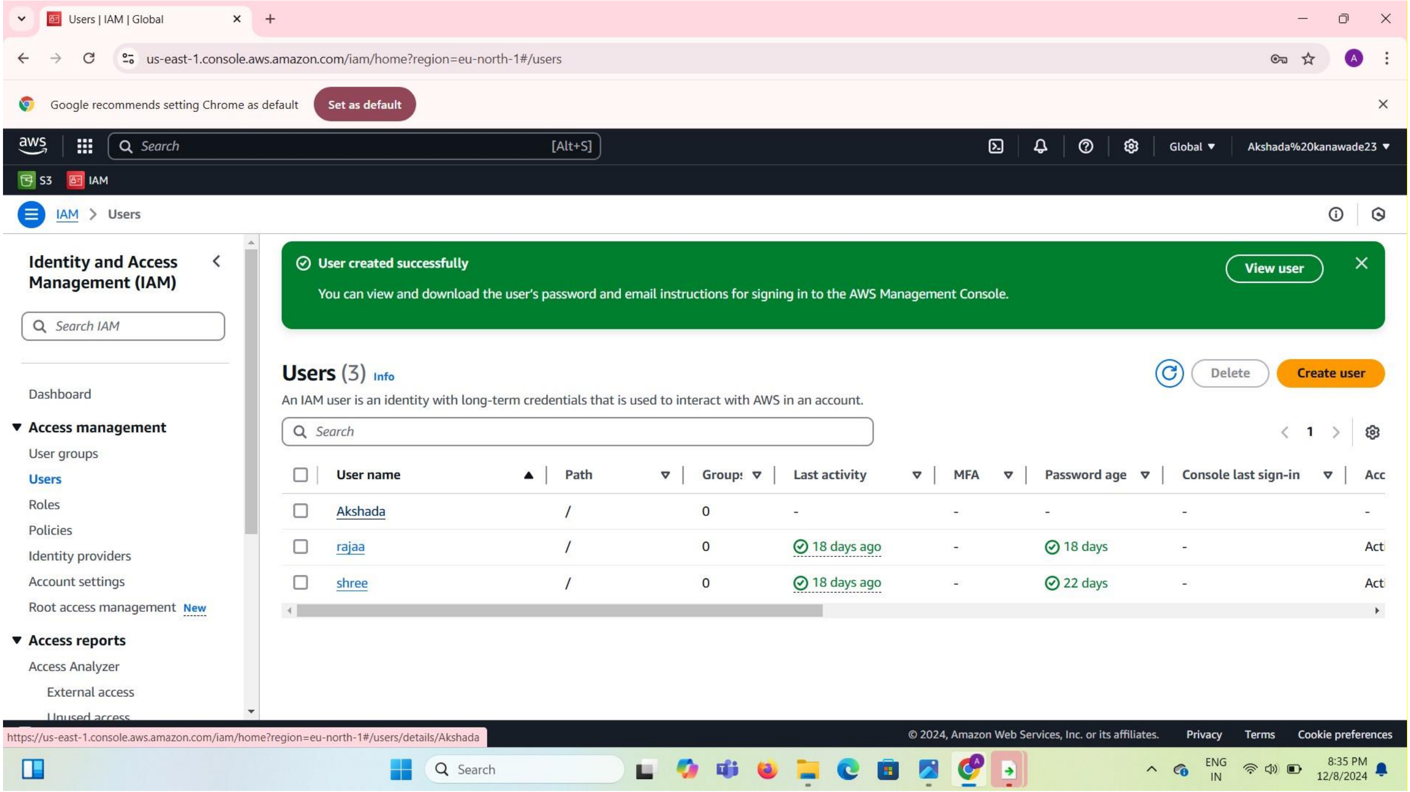
No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel
Previous
Create user
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG
IN
8:35 PM
12/8/2024

5. Your User Is Successfully Created .



User created successfully

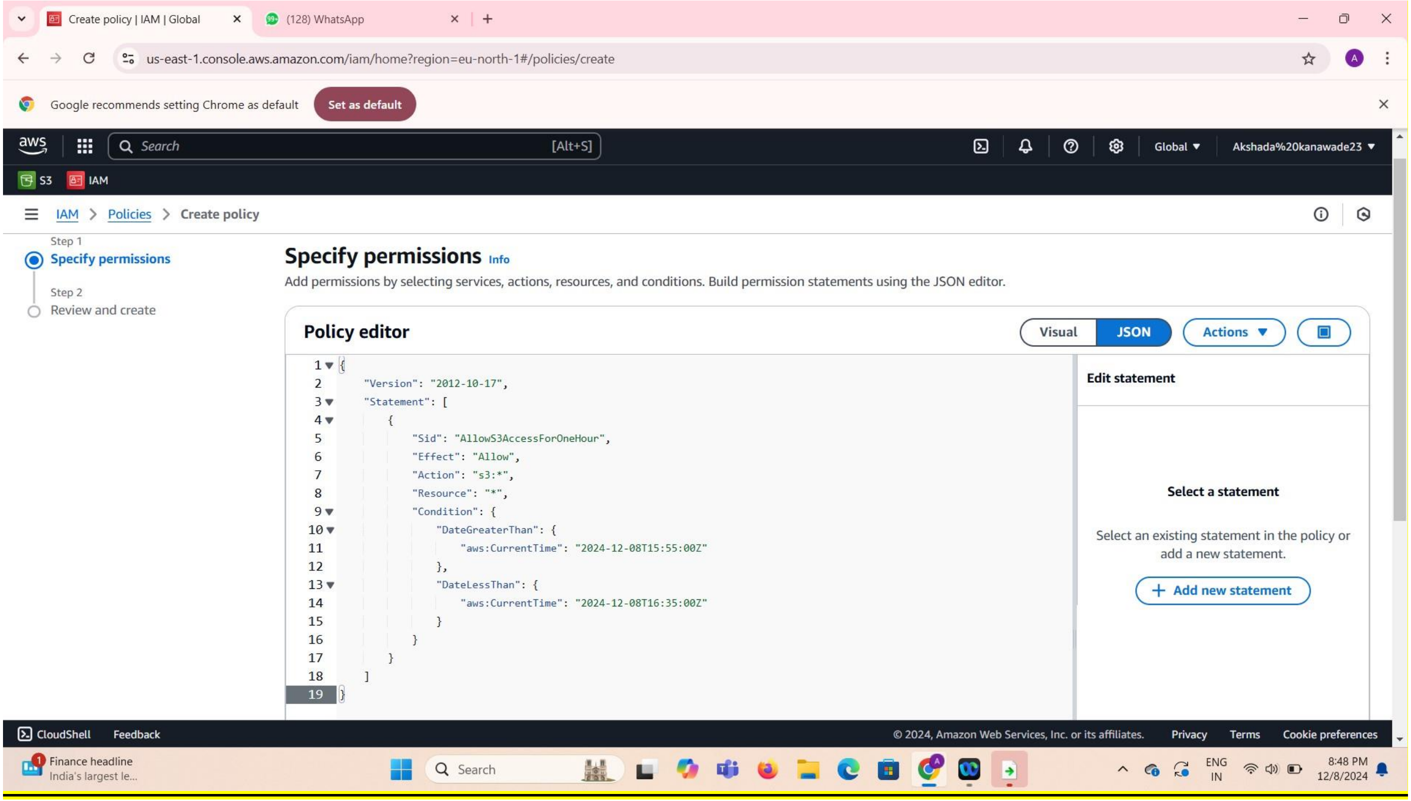
You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Users (3) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

□	User name	Path	Group:	Last activity	MFA	Password age	Console last sign-in	Acc
□	Akshada	/	0	-	-	-	-	-
□	rajaa	/	0	✓ 18 days ago	-	✓ 18 days	-	Act
□	shree	/	0	✓ 18 days ago	-	✓ 22 days	-	Act

6. Now Create AWS Customer Managed JSON Policy (S3-full-access-1hr) IAM → Policies → Create Policy →JSON.



Specify permissions Info

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

Policy editor

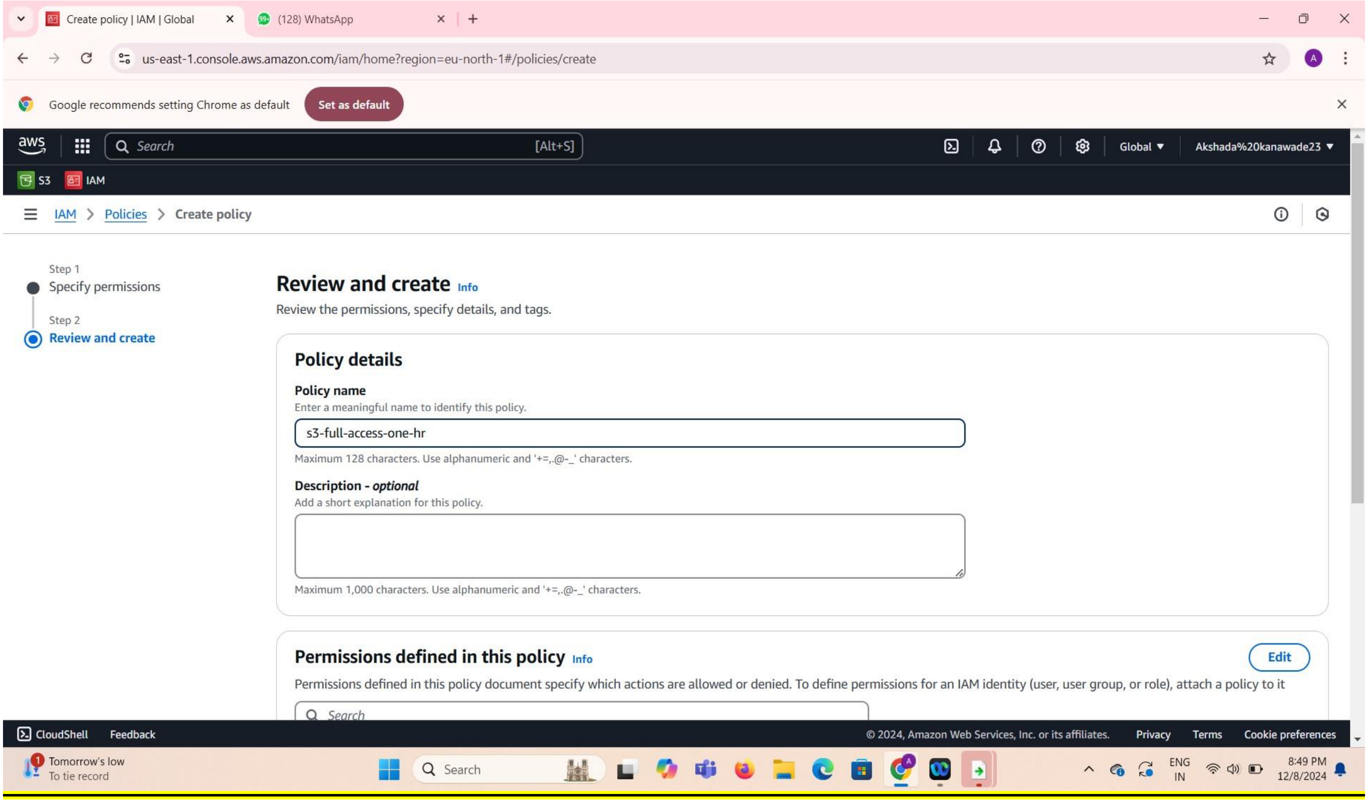
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowS3AccessForOneHour",
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": "*",
            "Condition": {
                "DateGreaterThan": {
                    "aws:CurrentTime": "2024-12-08T15:55:00Z"
                },
                "DateLessThan": {
                    "aws:CurrentTime": "2024-12-08T16:35:00Z"
                }
            }
        }
    ]
}
```

Select a statement

Select an existing statement in the policy or add a new statement.

+ Add new statement

7. Specify Policy Name, Then Click On Create Policy.



Review and create Info

Review the permissions, specify details, and tags.

Policy details

Policy name

Enter a meaningful name to identify this policy.

s3-full-access-one-hr

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

Description - *optional*

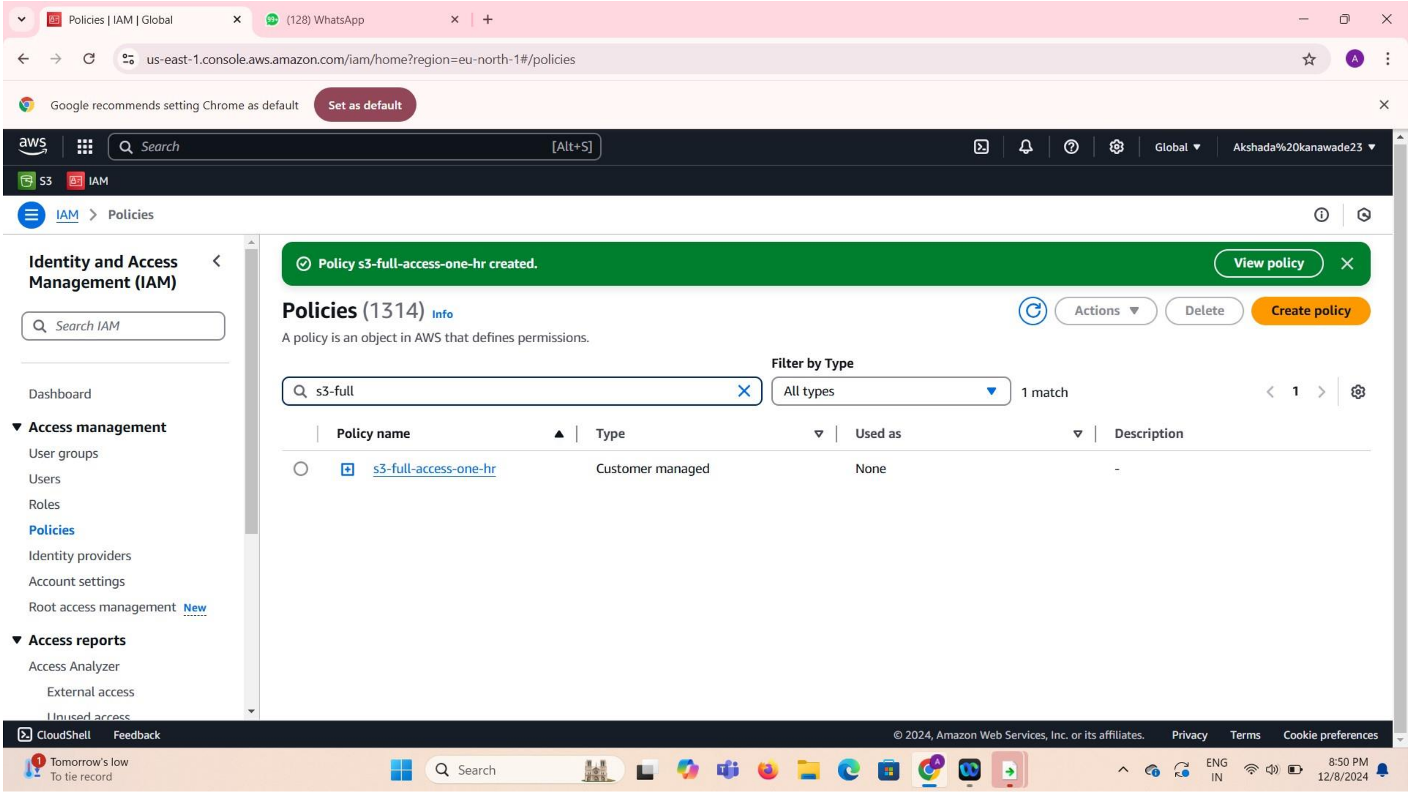
Add a short explanation for this policy.

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

8. Policy Created Successfully.



Policy s3-full-access-one-hr created.

Policies (1314) Info

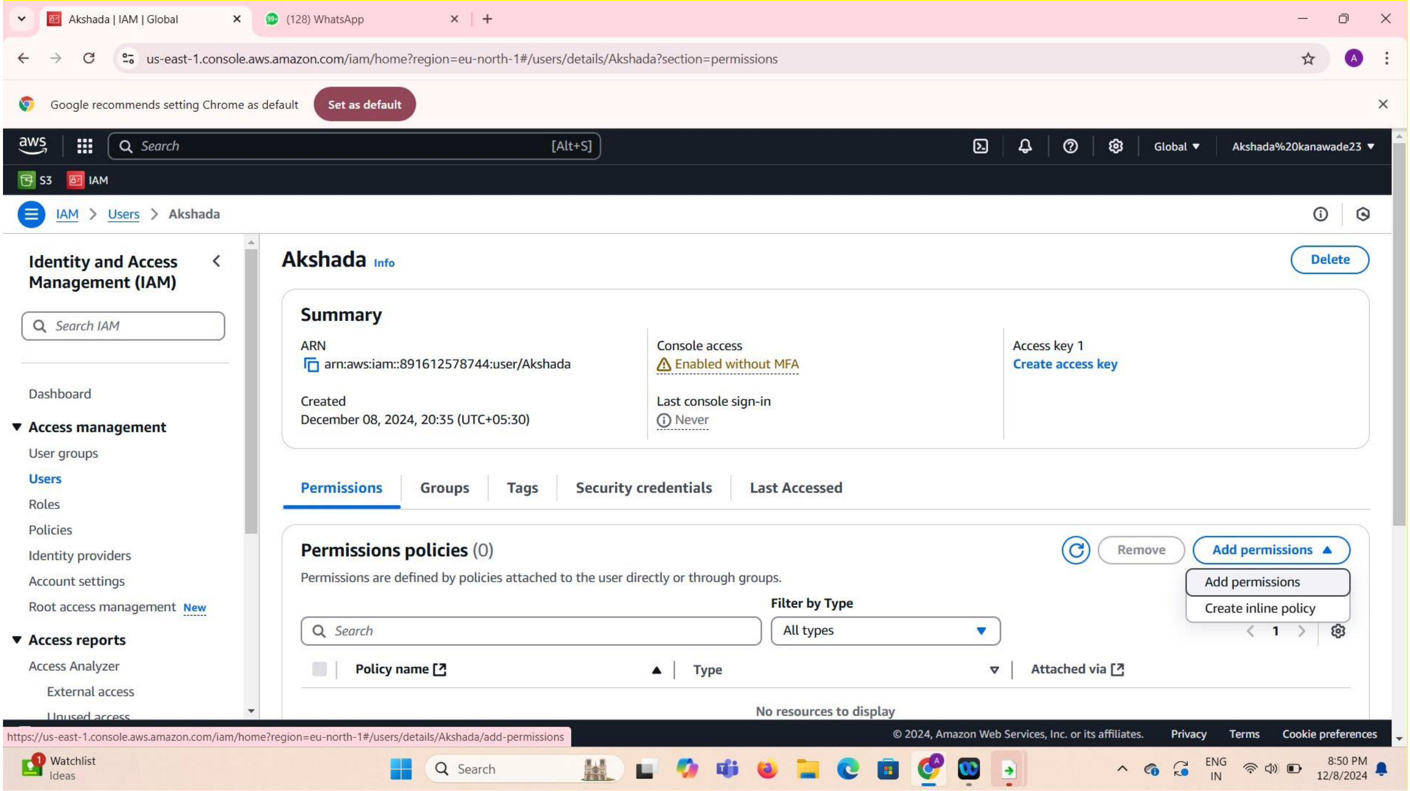
A policy is an object in AWS that defines permissions.

Filter by Type: All types

s3-full — 1 match

	Policy name ▲	Type	Used as	Description
○	s3-full-access-one-hr	Customer managed	None	-

9. To Attached Policy To User , Go to User → Select User → Permission → Add Permission.



us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/details/Akshada?section=permissions

IAM > Users > Akshada

Akshada Info

Summary

ARN
arn:aws:iam::891612578744:user/Akshada

Console access
⚠ Enabled without MFA

Access key 1
Create access key

Created
December 08, 2024, 20:35 (UTC+05:30)

Last console sign-in
ⓘ Never

Permissions policies (0)

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

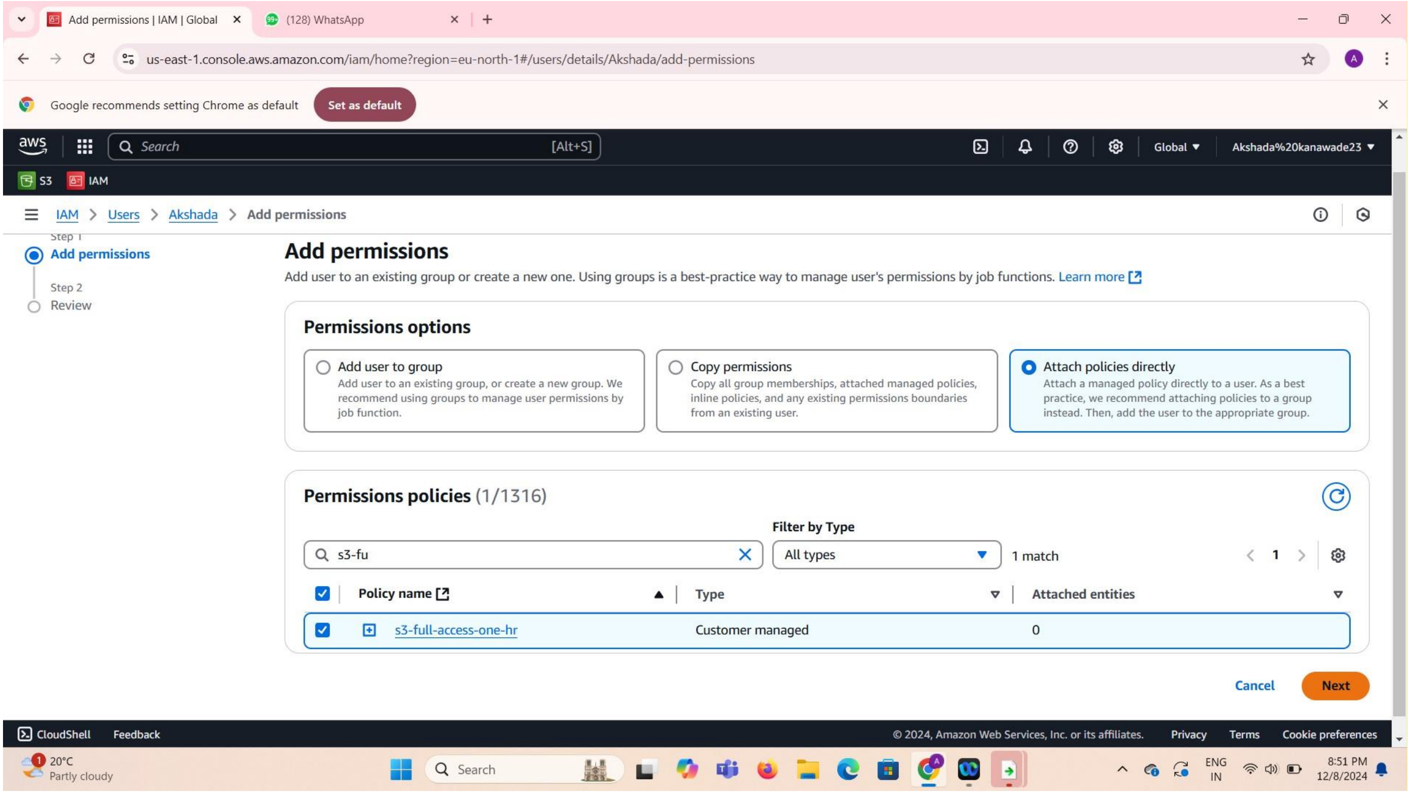
Filter by Type: All types

☐	Policy name	Type	Attached via

No resources to display

https://us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/details/Akshada/add-permissions

10. Then , Attach Policies Directly → Select Policy → Next → Attach Policy.



us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/details/Akshada/add-permissions

IAM > Users > Akshada > Add permissions

Step 1
Add permissions

Step 2
Review

Add 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, inline policies, and any existing permissions boundaries 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.

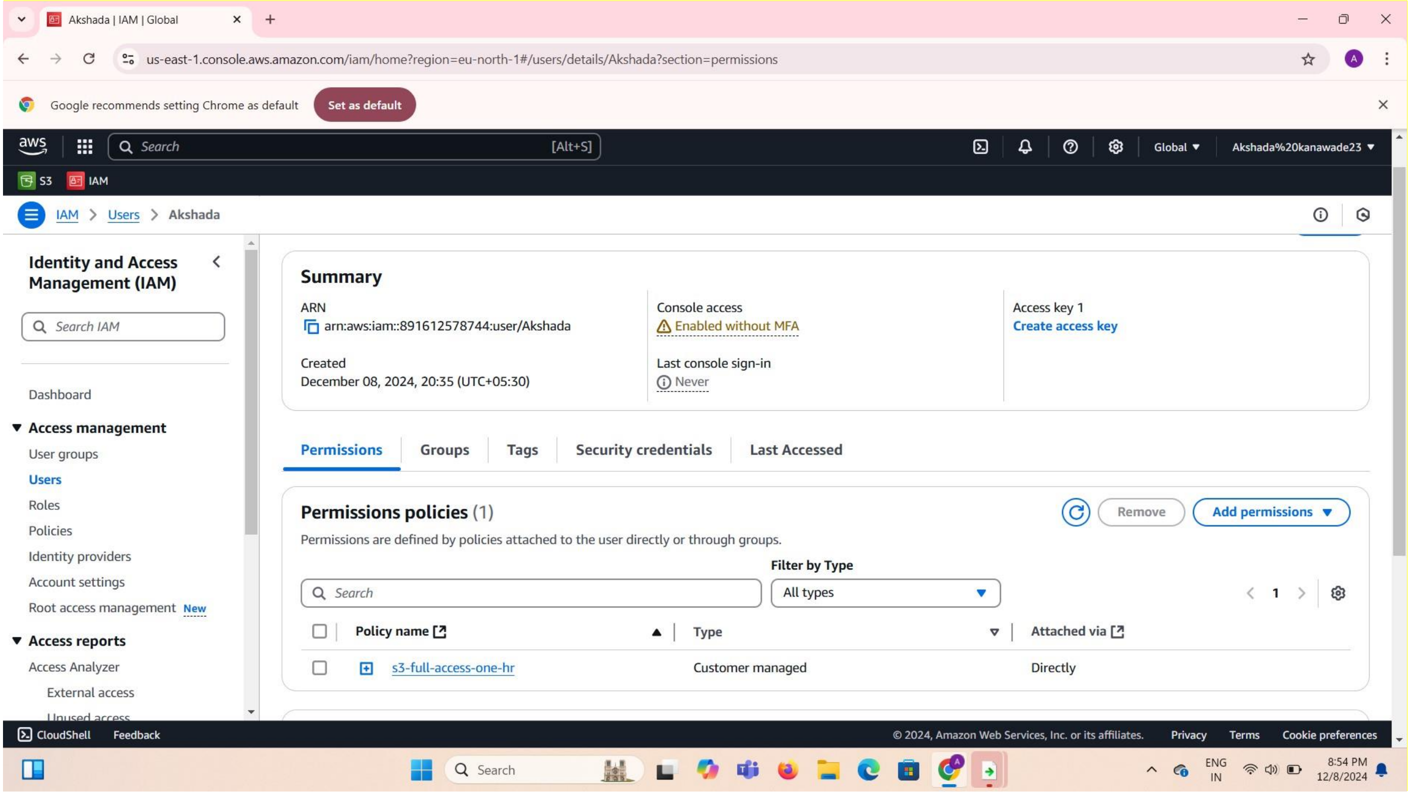
Permissions policies (1/1316)

Filter by Type: All types

Search: s3-fu — 1 match

☑	Policy name	Type	Attached entities
☑	s3-full-access-one-hr	Customer managed	0

11. S3-full-access-one-hr Policy is Attached To The User.



us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/details/Akshada?section=permissions

IAM > Users > Akshada

Summary

ARN: arn:aws:iam::891612578744:user/Akshada

Console access: Enabled without MFA

Access key 1: Create access key

Created: December 08, 2024, 20:35 (UTC+05:30)

Last console sign-in: Never

Permissions | Groups | Tags | Security credentials | Last Accessed

Permissions policies (1)

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

Filter by Type: All types

Policy name	Type	Attached via
s3-full-access-one-hr	Customer managed	Directly

THANK YOU !!