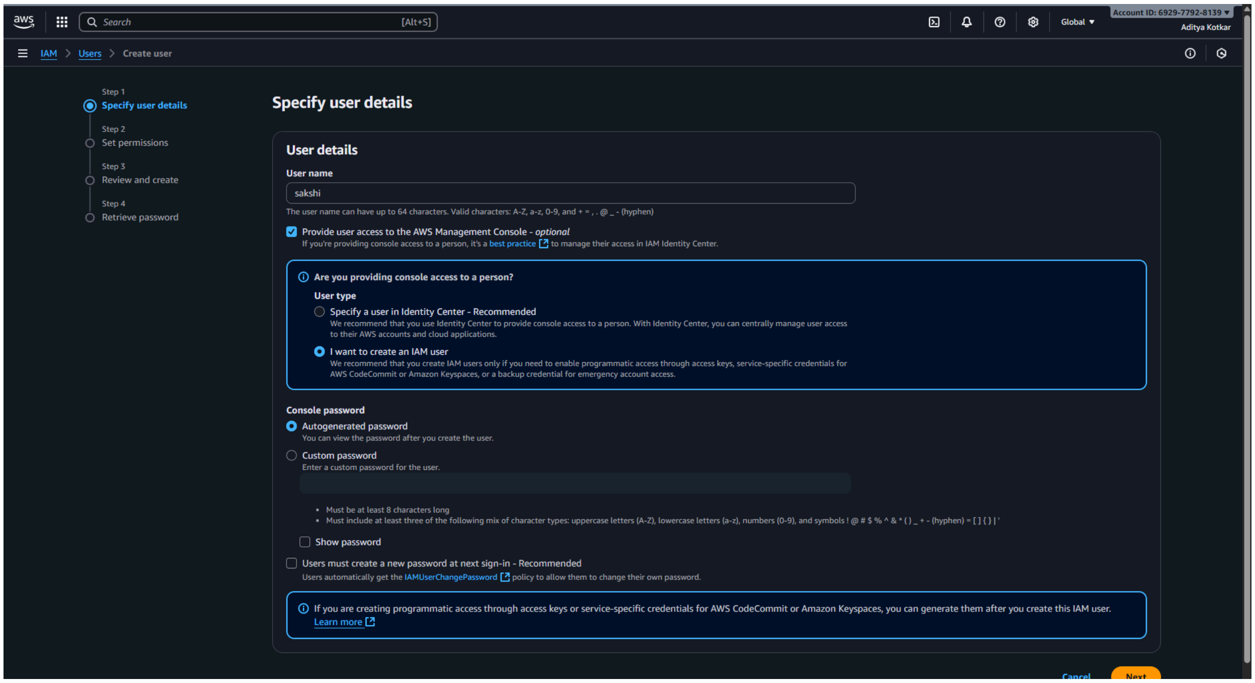
Practical - 3

Name: Sakshi Deshmukh
PRN: 202301040191
Roll no. 158

# Cross Account Role

Creating IAM user in account1



Specify user details

User details

User name: sakshi

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.

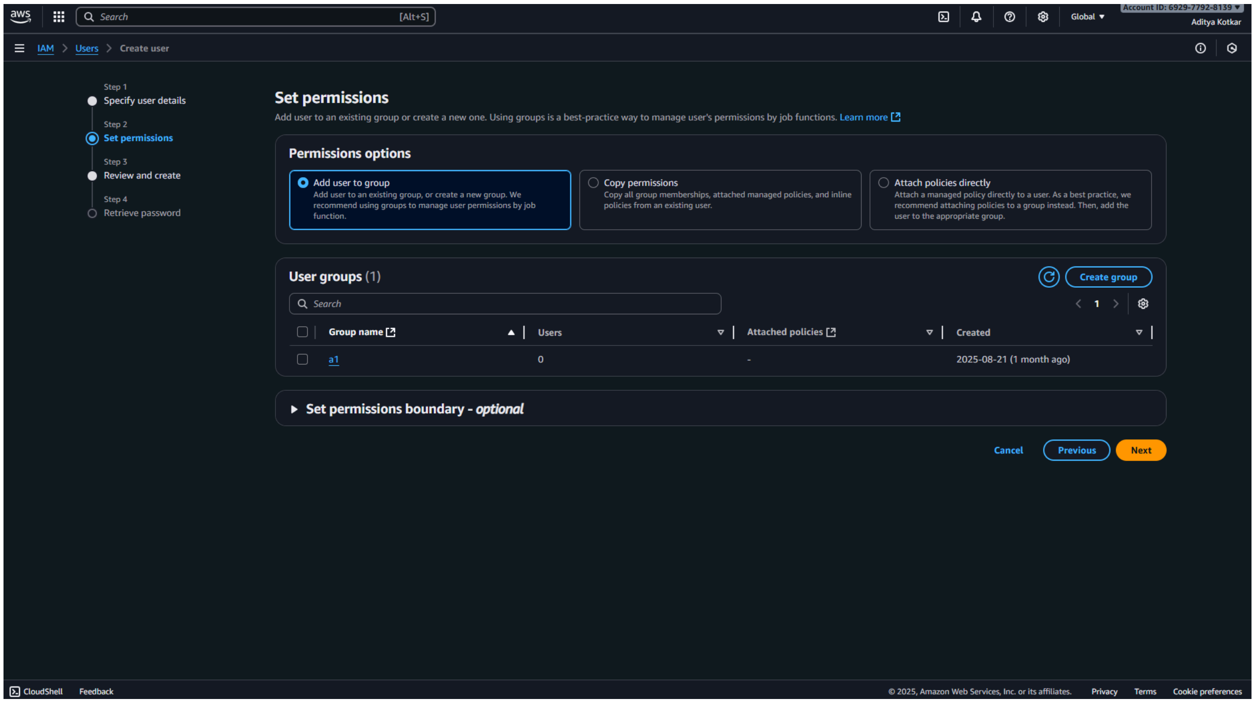
○ Custom password
Enter a custom password for the user.

- 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



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.

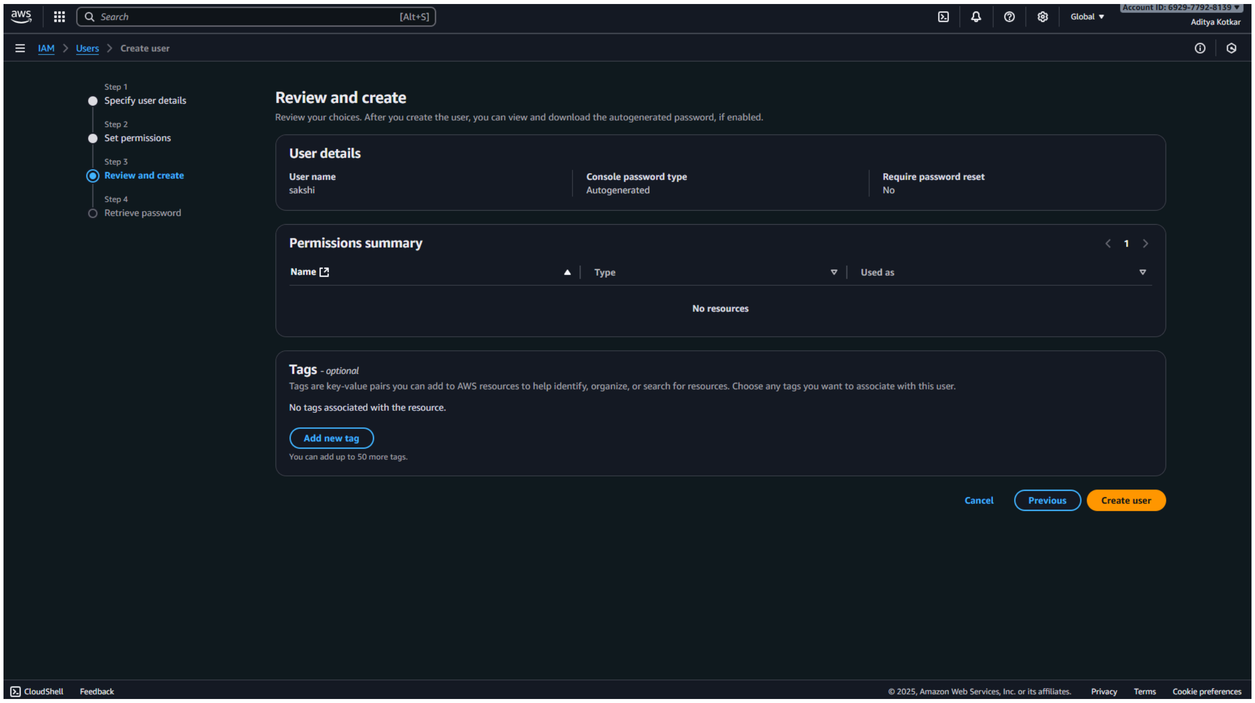
○ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

○ 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
□	a1	0	-	2025-08-21 (1 month ago)

▸ 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	Console password type	Require password reset
sakshi	Autogenerated	No

Permissions summary

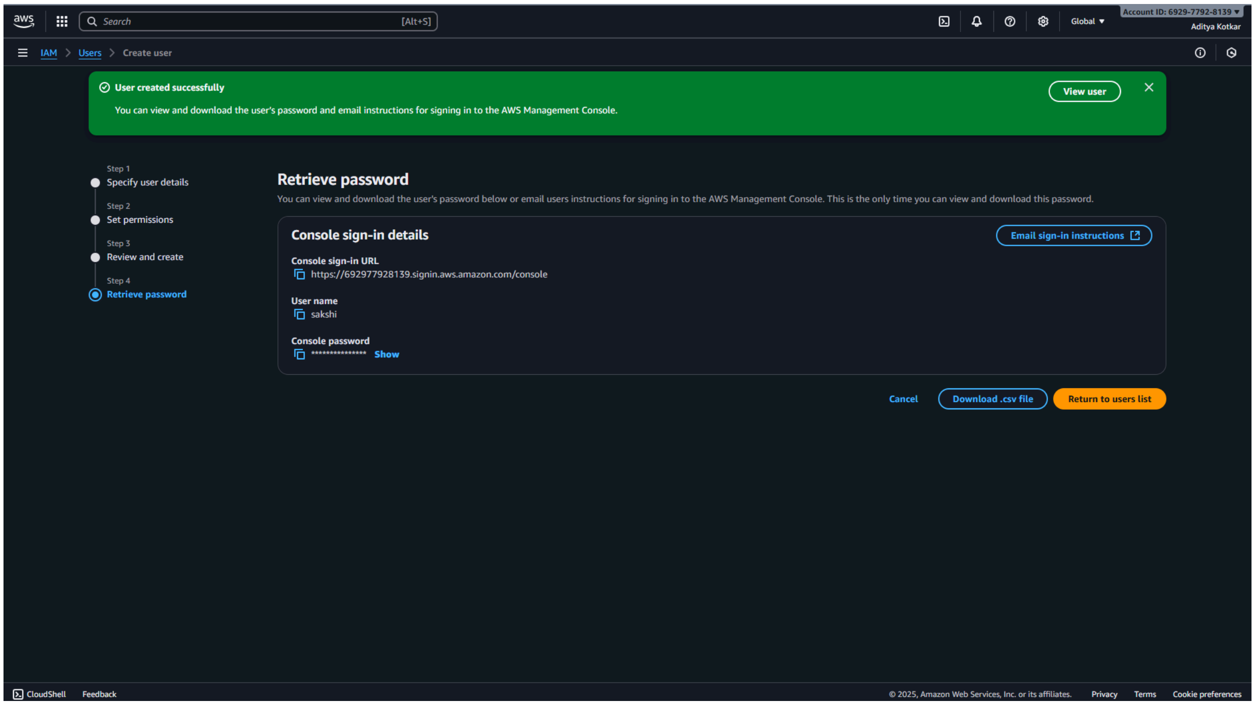
Name	Type	Used as
No resources		

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.

You can add up to 50 more tags.



User created successfully

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.

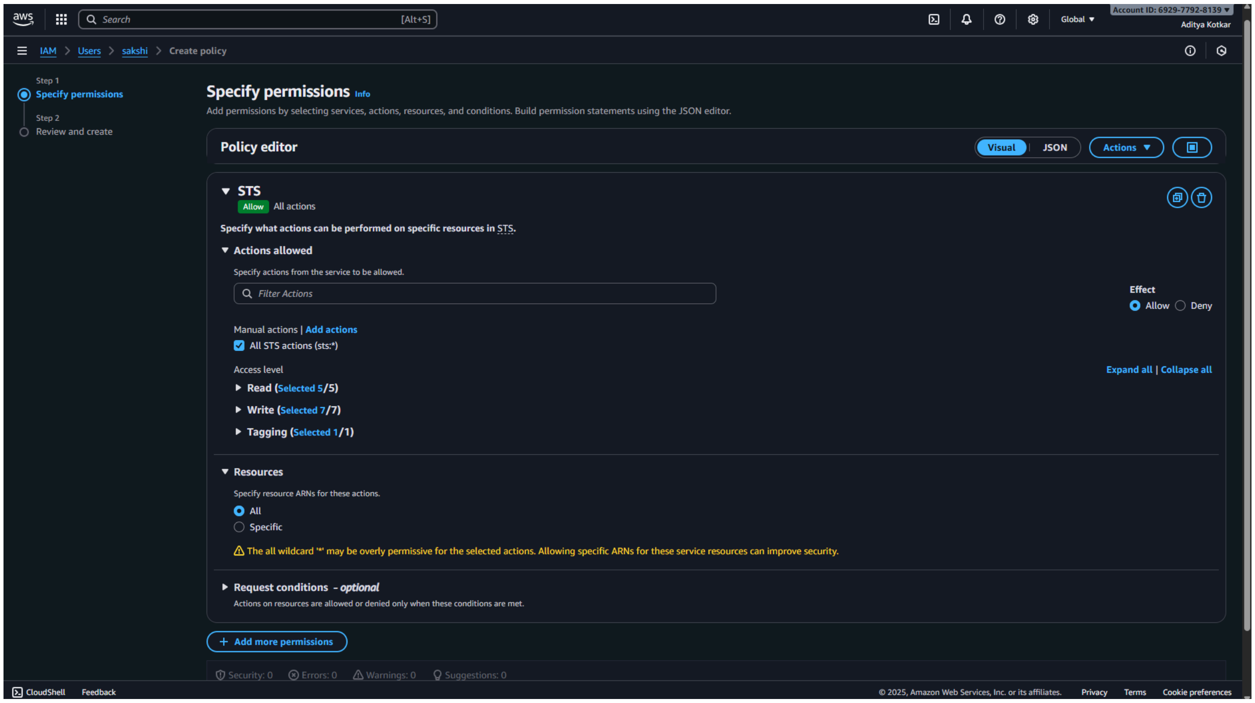
Console sign-in details

Console sign-in URL
https://692977928139.signin.aws.amazon.com/console

User name
sakshi

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

Attaching inline policy directly to created user



aws
Search [Alt+S]
Global ▼
Account ID: 6929-7792-8139 ▼
Aditya Kotkar
IAM > Users > sakshi > Create policy

Step 1
◉ Specify permissions

Step 2
○ Review and create

Specify permissions Info

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

Policy editor

▼ STS
Allow All actions

Specify what actions can be performed on specific resources in STS.

▼ Actions allowed

Specify actions from the service to be allowed.

Effect
● Allow ○ Deny

Manual actions | Add actions
☑ All STS actions (sts:*)

Access level

▶ Read (Selected 5/5)
▶ Write (Selected 7/7)
▶ Tagging (Selected 1/1)

▼ Resources

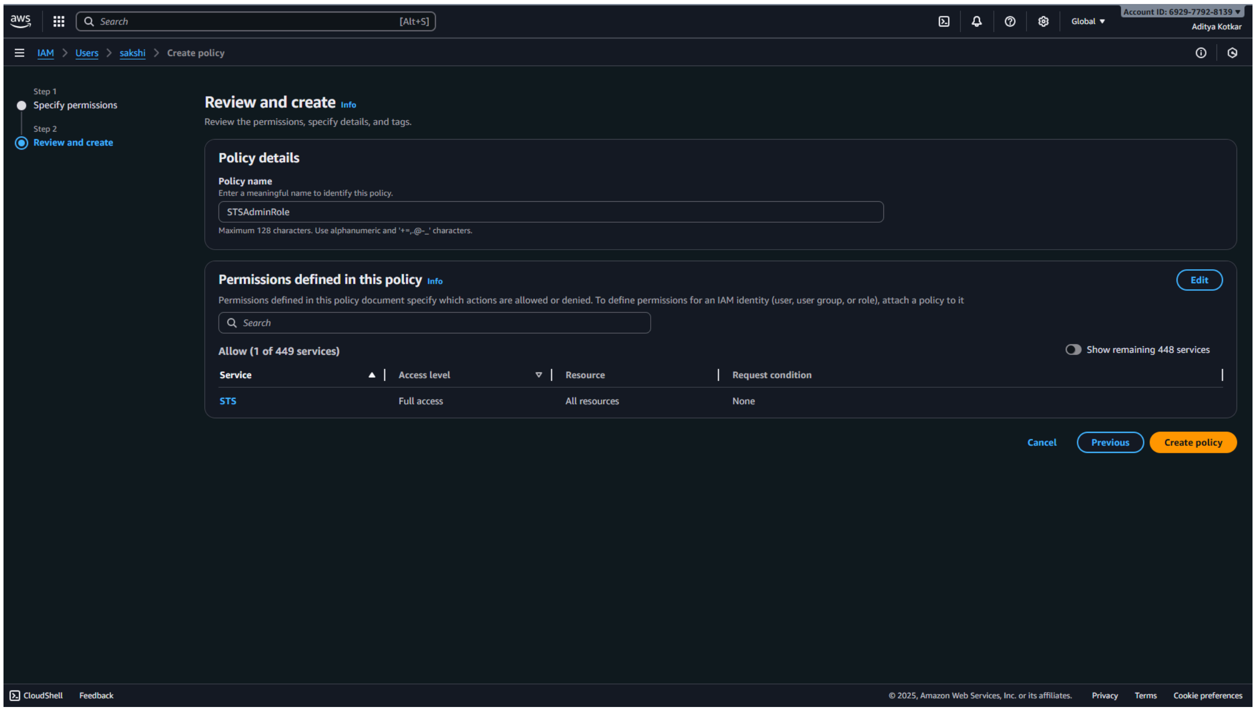
Specify resource ARNs for these actions.
● All
○ Specific

⚠ 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.

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0



Review and create Info

Review the permissions, specify details, and tags.

Policy details

Policy name

Enter a meaningful name to identify this policy.

STSAdminRole

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

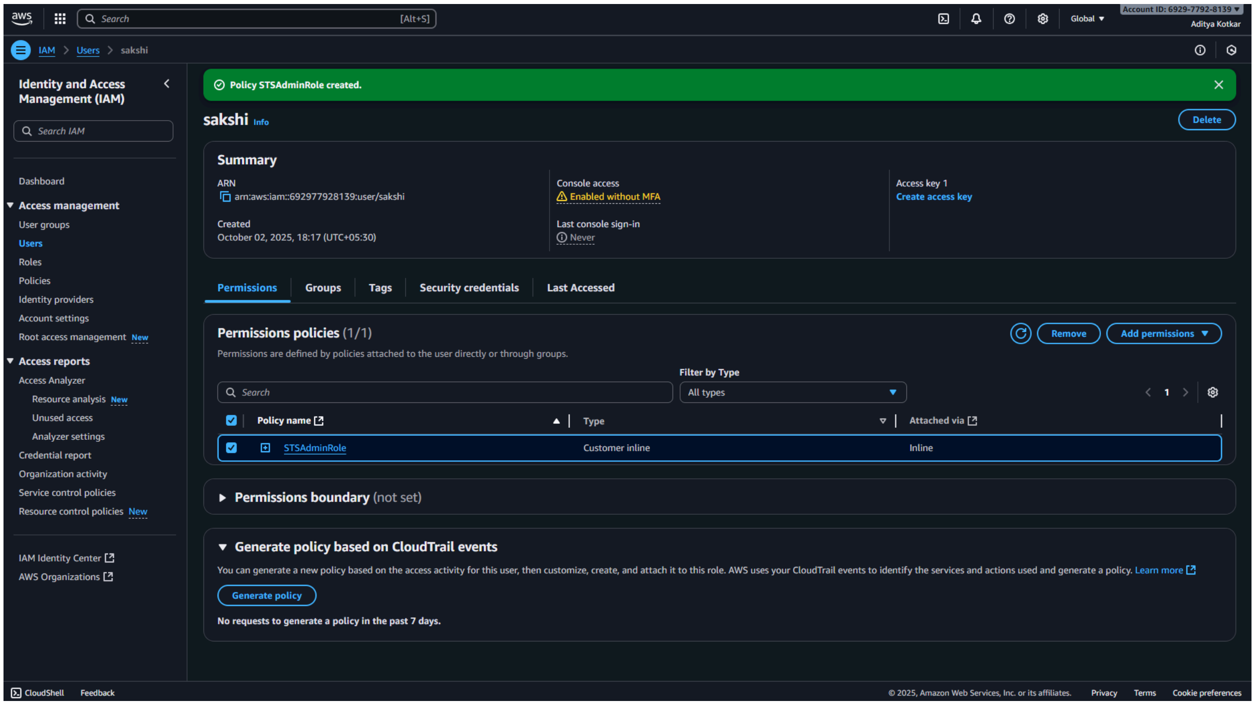
Permissions defined in this policy Info

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 449 services)

Show remaining 448 services

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



Policy STSAdminRole created.

sakshi Info

Summary

ARN
arn:aws:iam::692977928139:user/sakshi

Created
October 02, 2025, 18:17 (UTC+05:30)

Console access
⚠ Enabled without MFA

Last console sign-in
Never

Access key 1
Create access key

Permissions policies (1/1)

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

Filter by Type
All types

☑	Policy name	Type	Attached via
☑	STSAdminRole	Customer inline	Inline

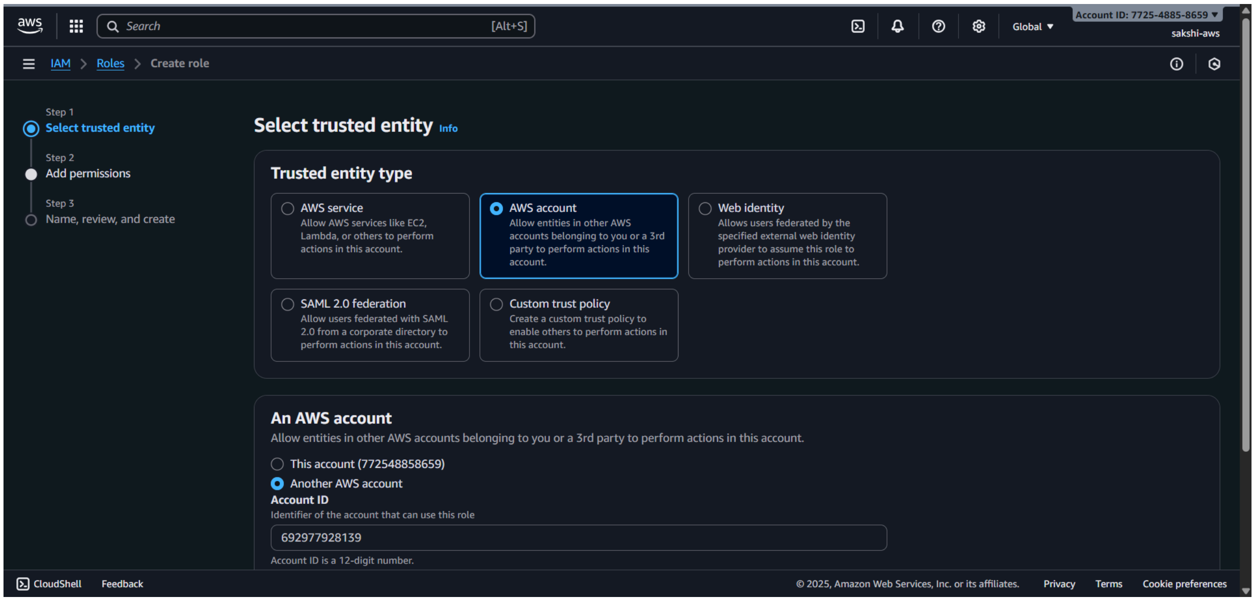
Permissions boundary (not set)

Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more

No requests to generate a policy in the past 7 days.

Creating new role in account2


aws
Search
[Alt+S]
Global
Account ID: 7725-4885-8659
sakshi-aws
IAM > Roles > Create role
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity Info

Trusted entity type

○ AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

● AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

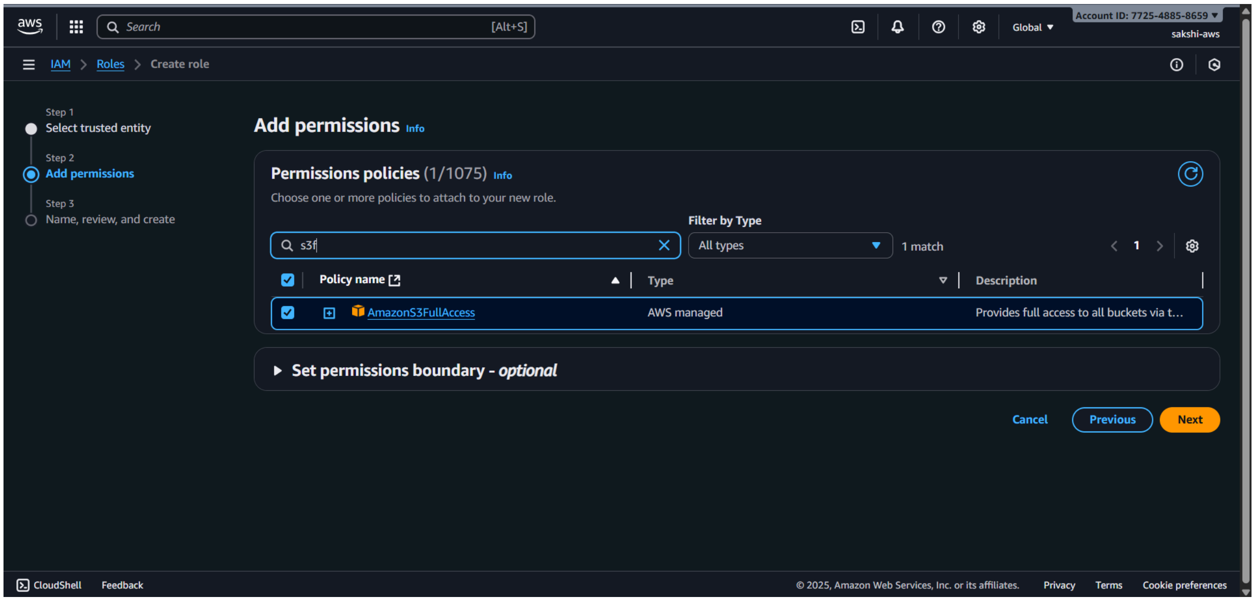
An AWS account

Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ This account (772548858659)
● Another AWS account

Account ID
Identifier of the account that can use this role
692977928139
Account ID is a 12-digit number.

Adding s3 full access permissions


aws
Search
[Alt+S]
Global
Account ID: 7725-4885-8659
sakshi-aws
IAM > Roles > Create role
Cancel
Previous
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Add permissions Info

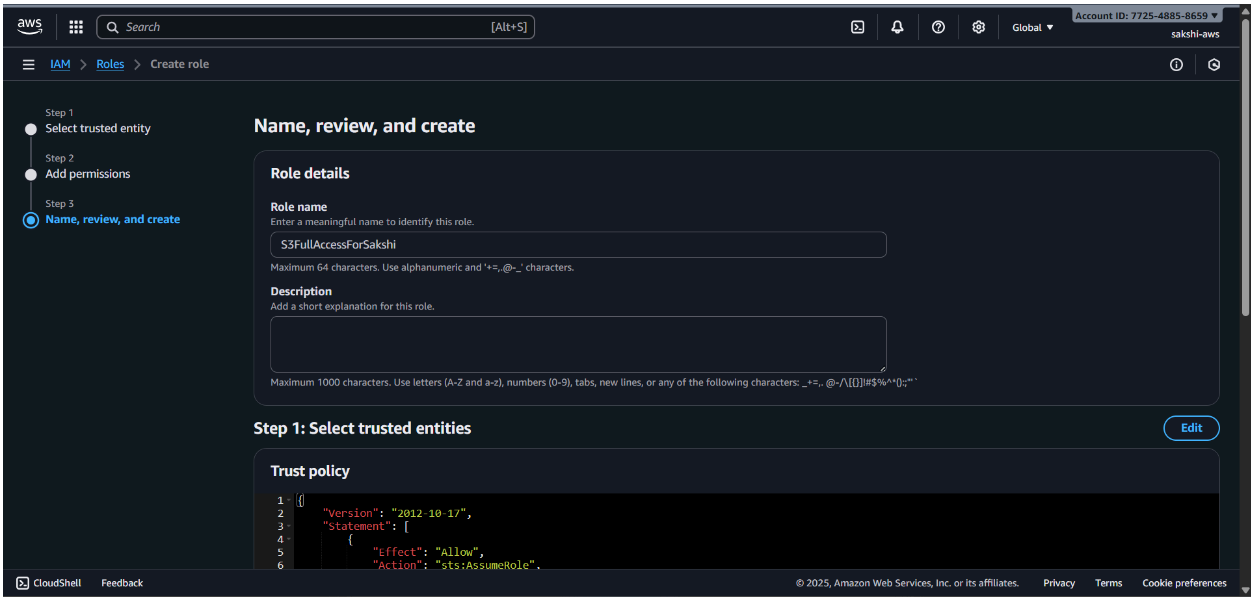
Permissions policies (1/1075) Info

Choose one or more policies to attach to your new role.

Search: s3f
Filter by Type: All types
1 match

☑	Policy name	Type	Description
☑	AmazonS3FullAccess	AWS managed	Provides full access to all buckets via t...

▸ Set permissions boundary - *optional*


aws
Search
[Alt+S]
Global ▾
Account ID: 7725-4885-8659 ▾
sakshi-aws
IAM > Roles > Create role
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.

S3FullAccessForSakshi

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

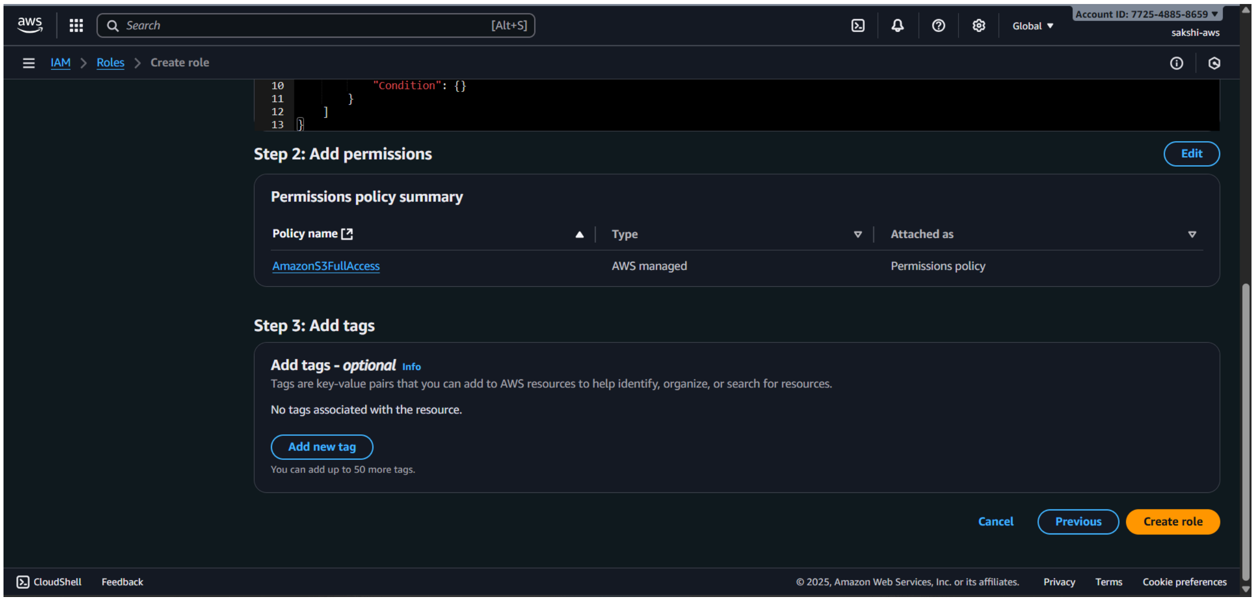
Description
Add a short explanation for this role.

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=,. @-/\[{}]!#$%^*();:"'`

Step 1: Select trusted entities

Trust policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
```


aws
Search
[Alt+S]
Global ▾
Account ID: 7725-4885-8659 ▾
sakshi-aws
IAM > Roles > Create role
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

```
            "Condition": {}
        }
    ]
}
```

Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
AmazonS3FullAccess	AWS managed	Permissions policy

Step 3: Add tags

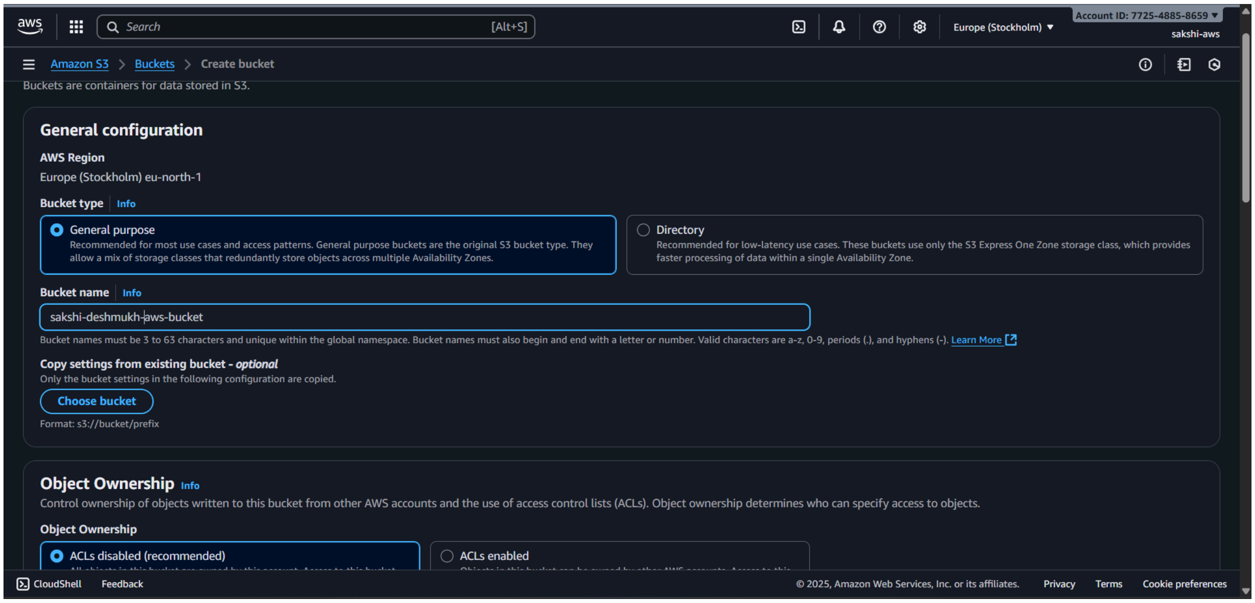
Add tags - *optional* Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

You can add up to 50 more tags.

Creating s3 bucket in account2



aws
Search [Alt+S]
Europe (Stockholm) ▼
Account ID: 7725-4885-8659 ▼
sakshi-aws
Amazon S3 > Buckets > Create bucket

Buckets are containers for data stored in S3.

General configuration

AWS Region
Europe (Stockholm) eu-north-1

Bucket type Info

● General purpose
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

○ Directory
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name Info

sakshi-deshmukh-aws-bucket

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). Learn More

Copy settings from existing bucket - *optional*
Only the bucket settings in the following configuration are copied.

Format: s3://bucket/prefix

Object Ownership Info

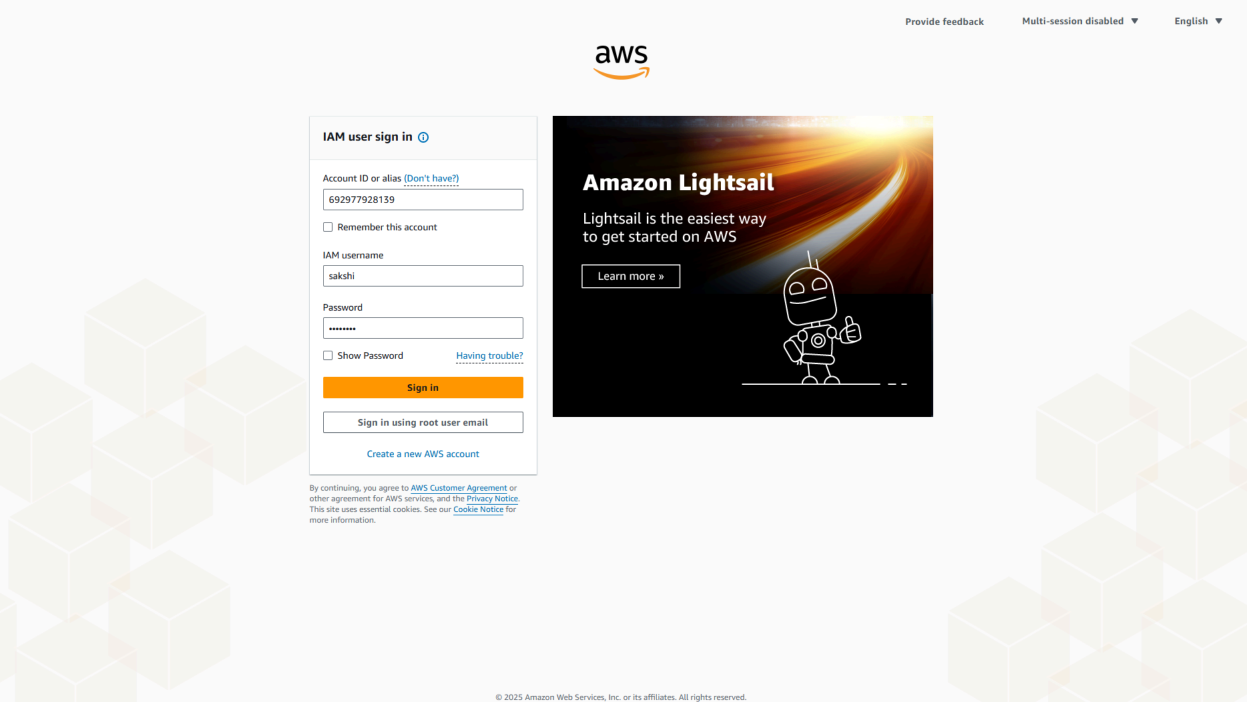
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

Object Ownership

● ACLs disabled (recommended)

○ ACLs enabled

Login to iam user of account1



IAM user sign in

Account ID or alias (Don't have?)
692977928139

□ Remember this account

IAM username
sakshi

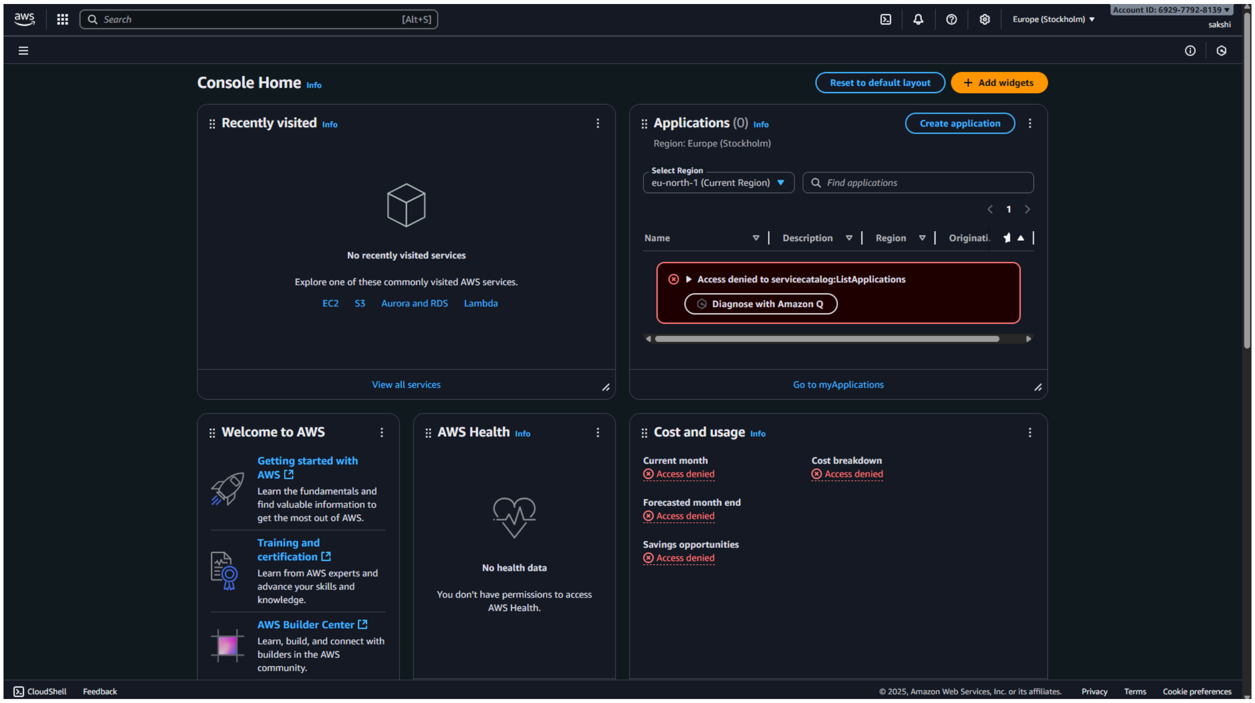
Password
•••••••••

□ Show Password Having trouble?

Sign in
Sign in using root user email
Create a new AWS account
Amazon Lightsail
Lightsail is the easiest way to get started on AWS
Learn more »

By continuing, you agree to AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.

© 2025 Amazon Web Services, Inc. or its affiliates. All rights reserved.



Console Home Info

Recently visited Info

No recently visited services

Explore one of these commonly visited AWS services.

EC2 S3 Aurora and RDS Lambda

View all services

Applications (0) Info

Region: Europe (Stockholm)

Select Region: eu-north-1 (Current Region)

Find applications

Name | Description | Region | Originati…

Access denied to servicecatalog:ListApplications

Diagnose with Amazon Q

Go to myApplications

Welcome to AWS

Getting started with AWS
Learn the fundamentals and find valuable information to get the most out of AWS.

Training and certification
Learn from AWS experts and advance your skills and knowledge.

AWS Builder Center
Learn, build, and connect with builders in the AWS community.

AWS Health Info

No health data

You don't have permissions to access AWS Health.

Cost and usage Info

Current month: Access denied

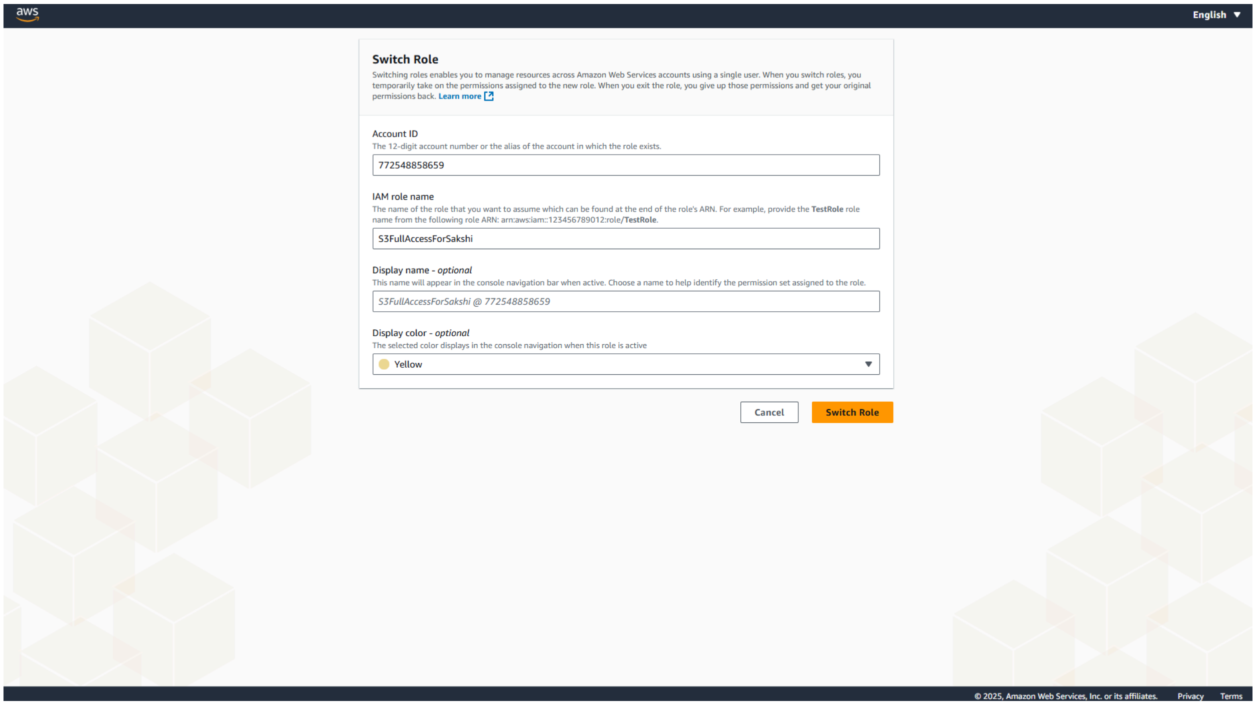
Cost breakdown: Access denied

Forecasted month end: Access denied

Savings opportunities: Access denied

© 2025, Amazon Web Services, Inc. or its affiliates.

Switching role to account2’s role



Switch Role

Switching roles enables you to manage resources across Amazon Web Services accounts using a single user. When you switch roles, you temporarily take on the permissions assigned to the new role. When you exit the role, you give up those permissions and get your original permissions back. Learn more

Account ID
The 12-digit account number or the alias of the account in which the role exists.
772548858659

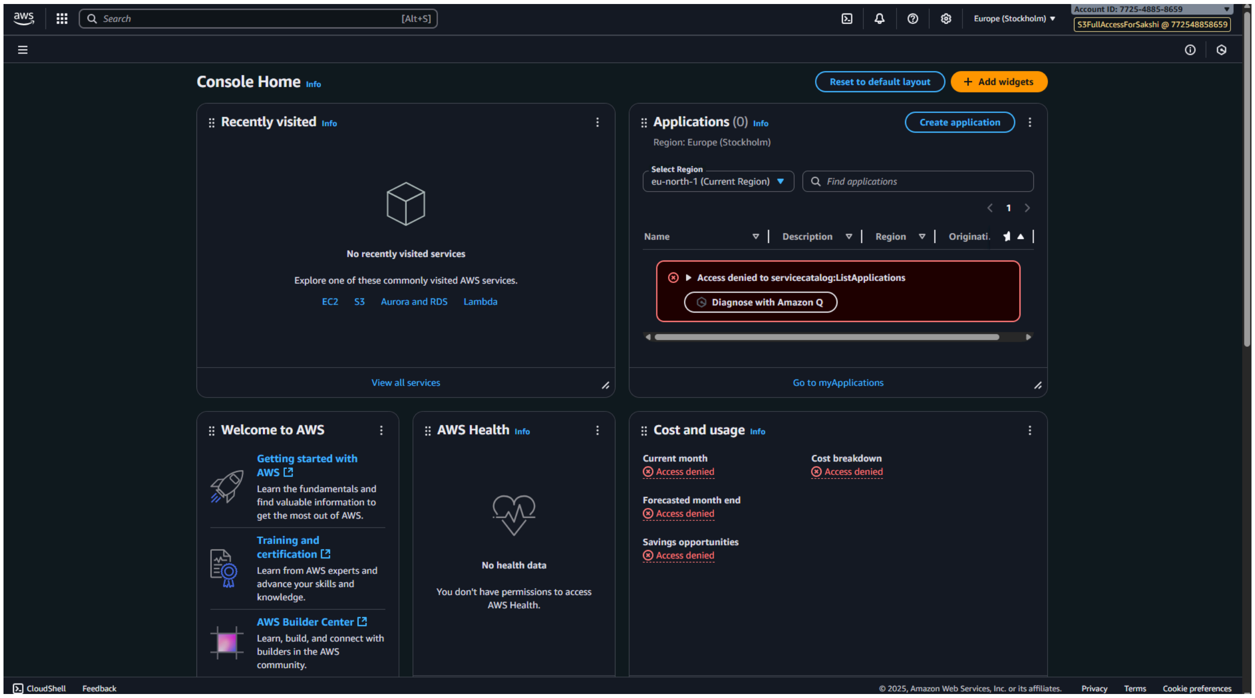
IAM role name
The name of the role that you want to assume which can be found at the end of the role's ARN. For example, provide the **TestRole** role name from the following role ARN: arn:aws:iam::123456789012:role/**TestRole**.
S3FullAccessForSakshi

Display name - *optional*
This name will appear in the console navigation bar when active. Choose a name to help identify the permission set assigned to the role.
S3FullAccessForSakshi @ 772548858659

Display color - *optional*
The selected color displays in the console navigation when this role is active
Yellow ▼

Cancel | Switch Role

© 2025, Amazon Web Services, Inc. or its affiliates.



Account ID: 7725-4885-8659

S3FullAccessForSakshi @ 772548858659

Europe (Stockholm)

Console Home

Reset to default layout | Add widgets

Recently visited

No recently visited services

Explore one of these commonly visited AWS services.

EC2 S3 Aurora and RDS Lambda

View all services

Applications (0)

Region: Europe (Stockholm)

Select Region: eu-north-1 (Current Region)

Find applications

Name	Description	Region	Originati...

Access denied to servicecatalog:ListApplications

Diagnose with Amazon Q

Go to myApplications

Welcome to AWS

Getting started with AWS
Learn the fundamentals and find valuable information to get the most out of AWS.

Training and certification
Learn from AWS experts and advance your skills and knowledge.

AWS Builder Center
Learn, build, and connect with builders in the AWS community.

AWS Health

No health data

You don't have permissions to access AWS Health.

Cost and usage

Current month: Access denied

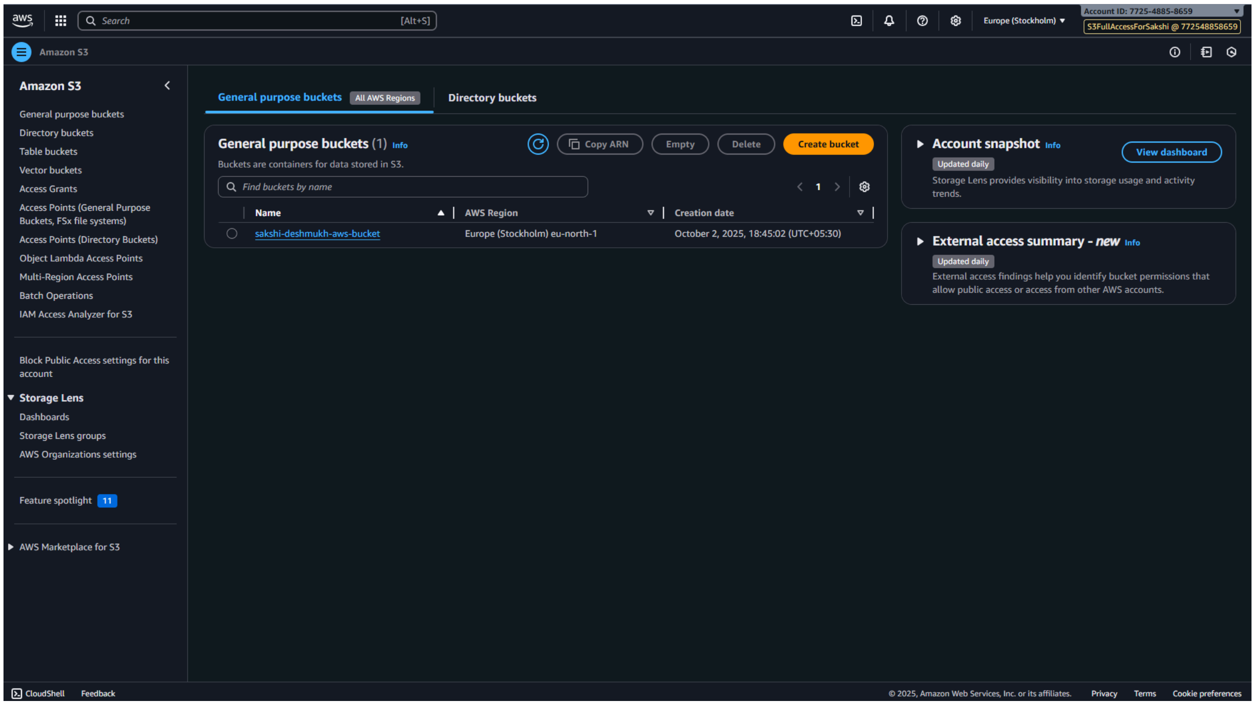
Cost breakdown: Access denied

Forecasted month end: Access denied

Savings opportunities: Access denied

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Bucket was successfully accessed



Account ID: 7725-4885-8659

S3FullAccessForSakshi @ 772548858659

Europe (Stockholm)

Amazon S3

Amazon S3

- General purpose buckets
- Directory buckets
- Table buckets
- Vector buckets
- Access Grants
- Access Points (General Purpose Buckets, FSx file systems)
- Access Points (Directory Buckets)
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3
- Block Public Access settings for this account
- Storage Lens
  - Dashboards
  - Storage Lens groups
  - AWS Organizations settings
- Feature spotlight 11
- AWS Marketplace for S3

General purpose buckets (All AWS Regions) | Directory buckets

General purpose buckets (1)

Buckets are containers for data stored in S3.

Copy ARN | Empty | Delete | Create bucket

Find buckets by name

Name	AWS Region	Creation date
sakshi-deshmukh-aws-bucket	Europe (Stockholm) eu-north-1	October 2, 2025, 18:45:02 (UTC+05:30)

Account snapshot

Updated daily

Storage Lens provides visibility into storage usage and activity trends.

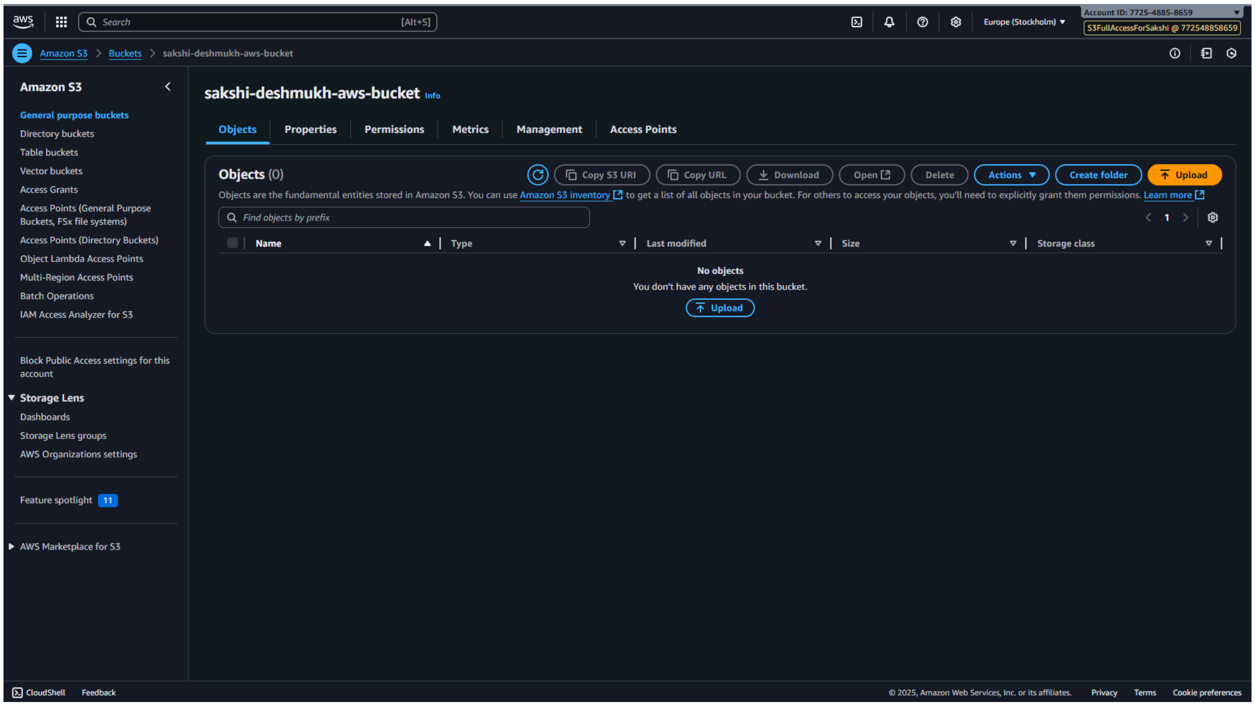
View dashboard

External access summary - new

Updated daily

External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



sakshi-deshmukh-aws-bucket

Objects (0)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

□	Name	Type	Last modified	Size	Storage class

No objects

You don't have any objects in this bucket.