AWS TASK :- To provide access to external users using JumpCloud as the Identity Provider (IdP) and AWS as the service provider you'll need to set up the necessary configurations both in JumpCloud and AWS IAM (Identity and Access Management). Below are the general steps you would follow:

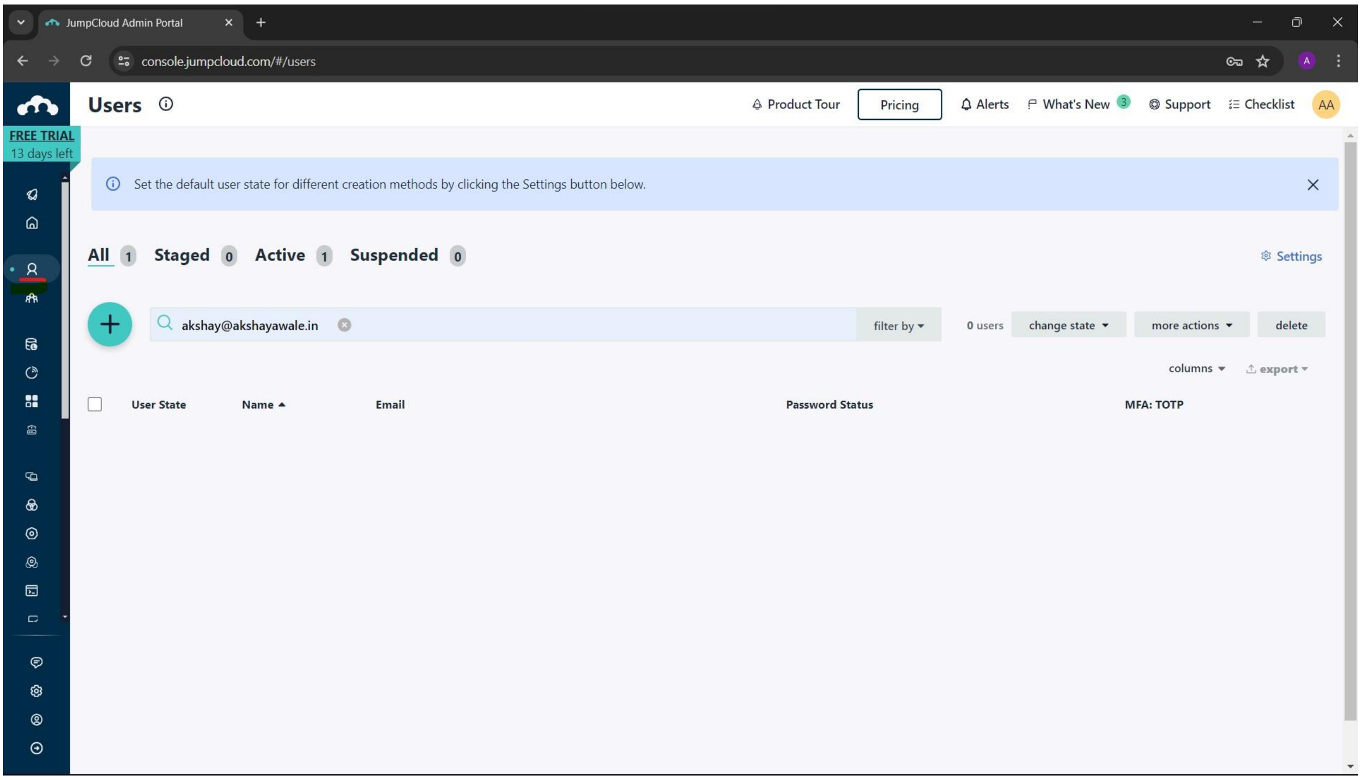
Setup in JumpCloud:

Create a JumpCloud Directory:

If you haven't already, create a JumpCloud Directory where you'll manage your users.

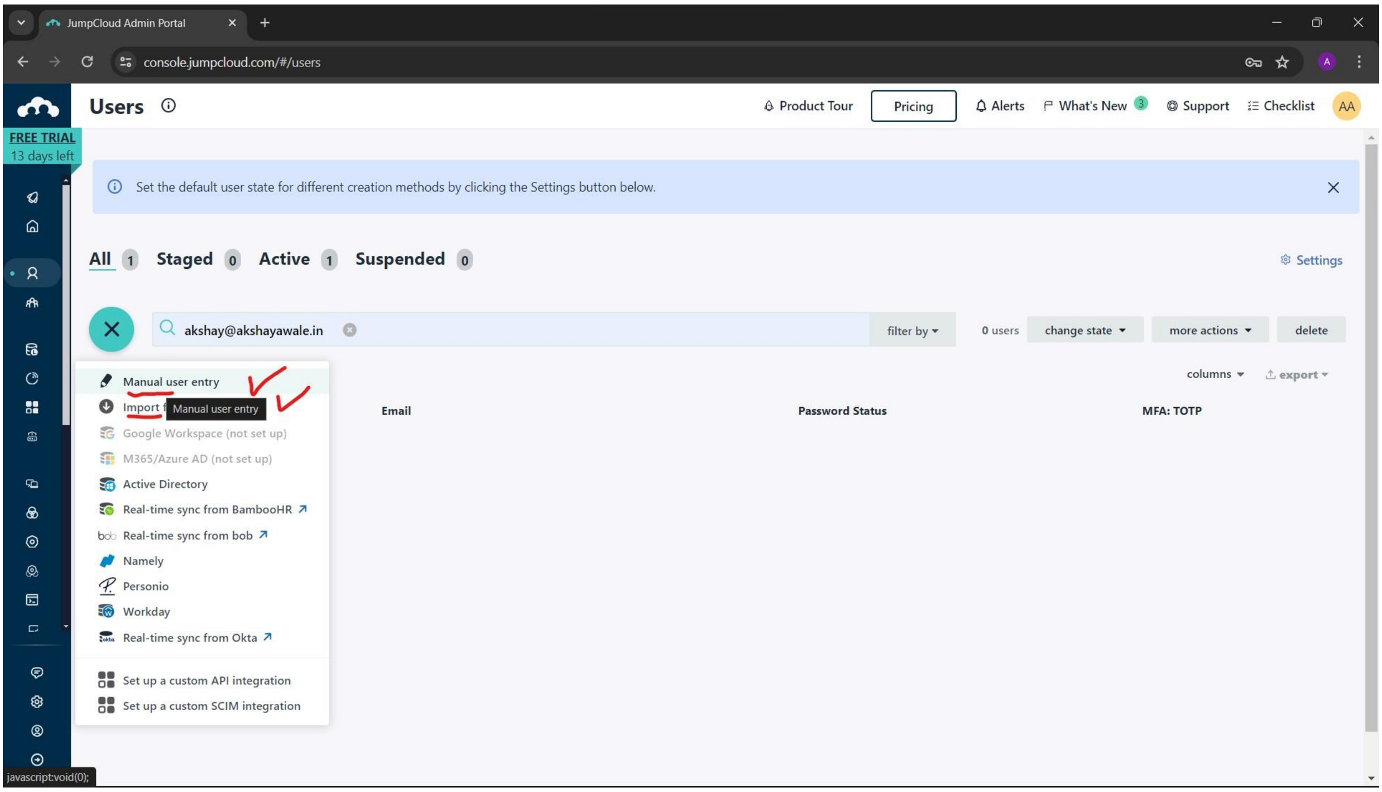
Add External Users to JumpCloud:

Invite and add external users to your JumpCloud directory.



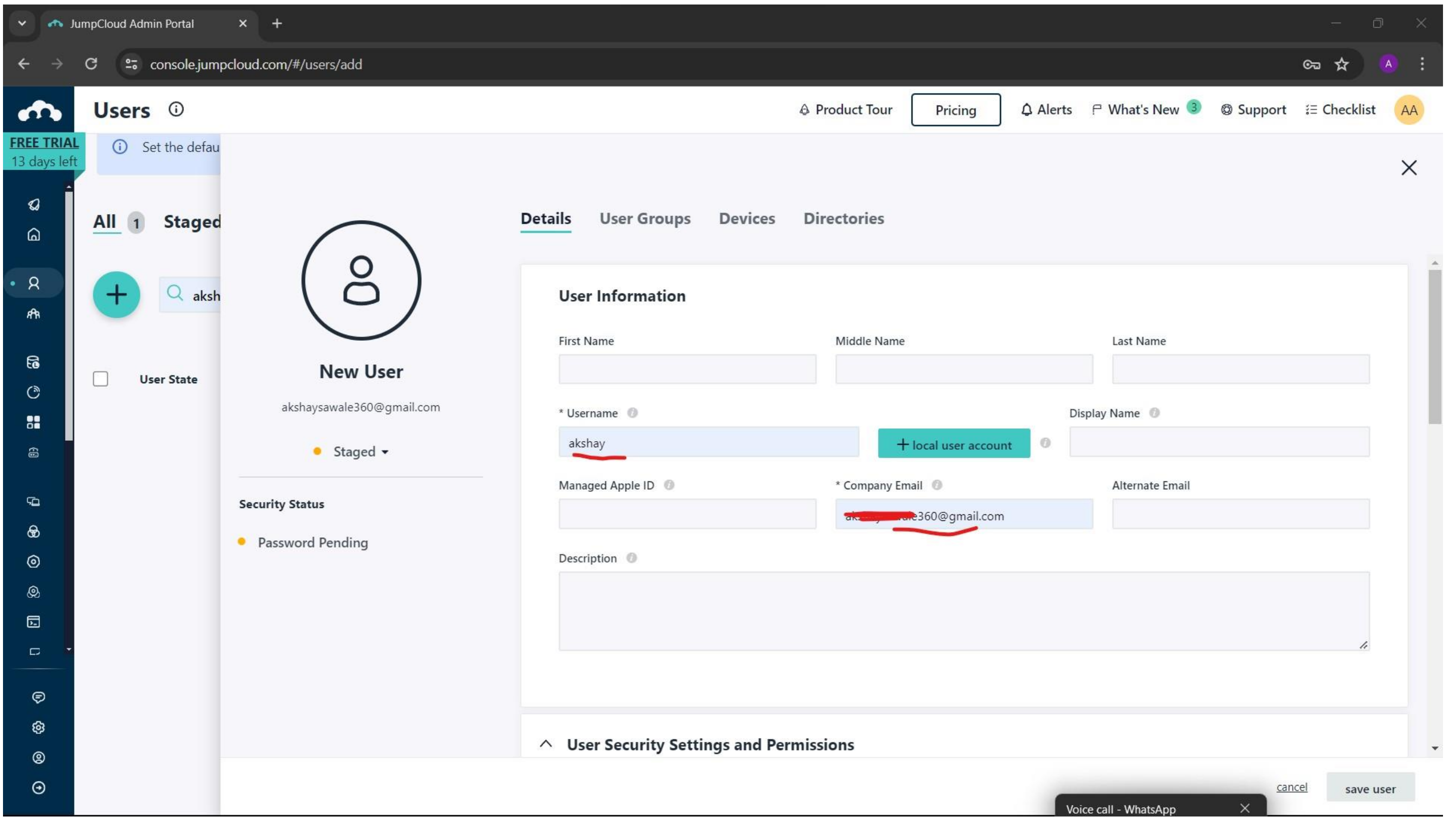
Set the default user state for different creation methods by clicking the Settings button below.

akshay@akshayawale.in



Set the default user state for different creation methods by clicking the Settings button below.

akshay@akshayawale.in



New User

akshaysawale360@gmail.com

● Staged

Security Status

● Password Pending

User Information

First Name	Middle Name	Last Name

* Username		Display Name
akshay	+ local user account	

Managed Apple ID	* Company Email	Alternate Email
	[redacted]360@gmail.com	

Description

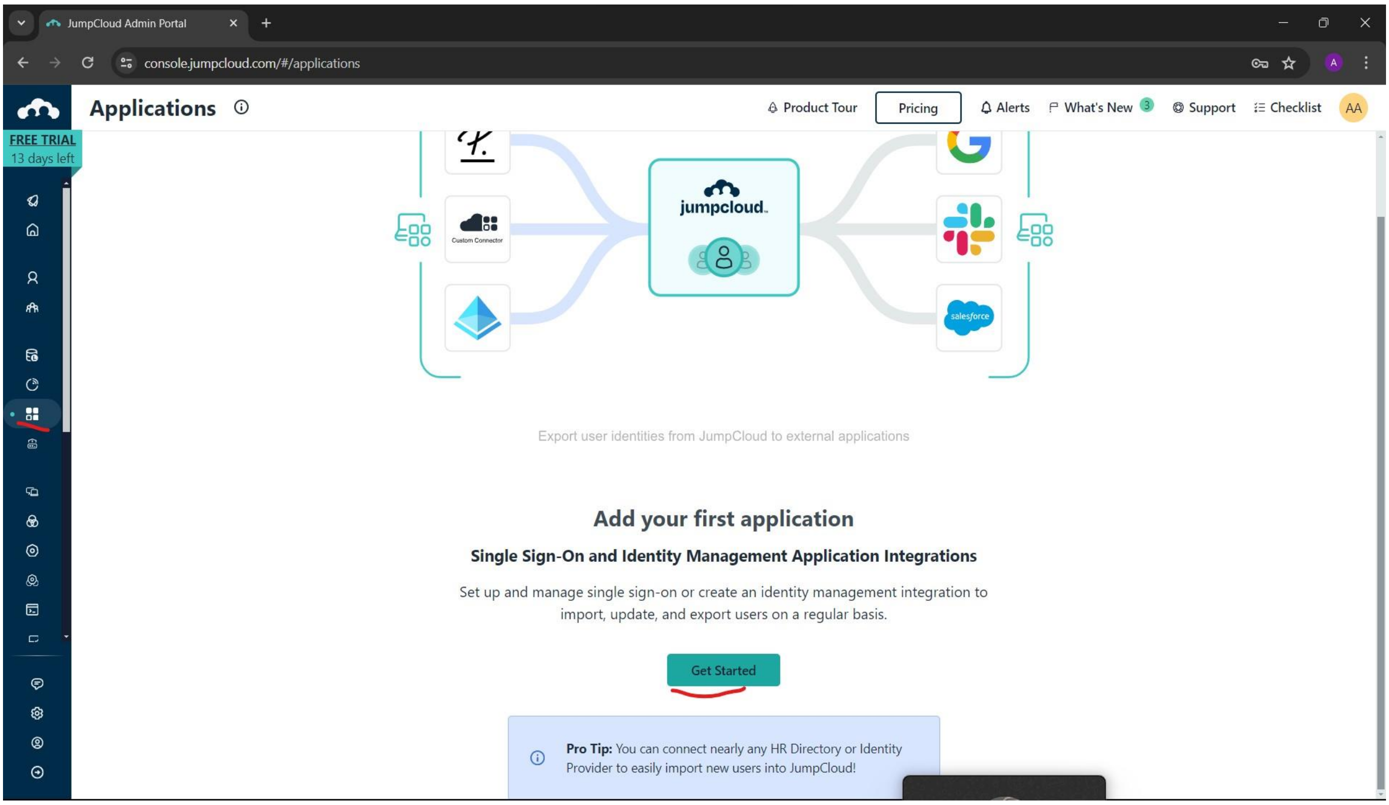
User Security Settings and Permissions

Configure SAML Application:

- Log in to JumpCloud Admin Console. Go to Applications > SAML > Export Metadata Click on the "New Application" button.
- Choose AWS as the application.
- Configure the necessary settings, such as ACS URL, Entity ID, and Attribute Statements.
- Save the configuration.

Assign Users to the AWS Application:

- Go back to Applications > SAML.
- Select the AWS application.
- Assign the external users you want to grant access to.



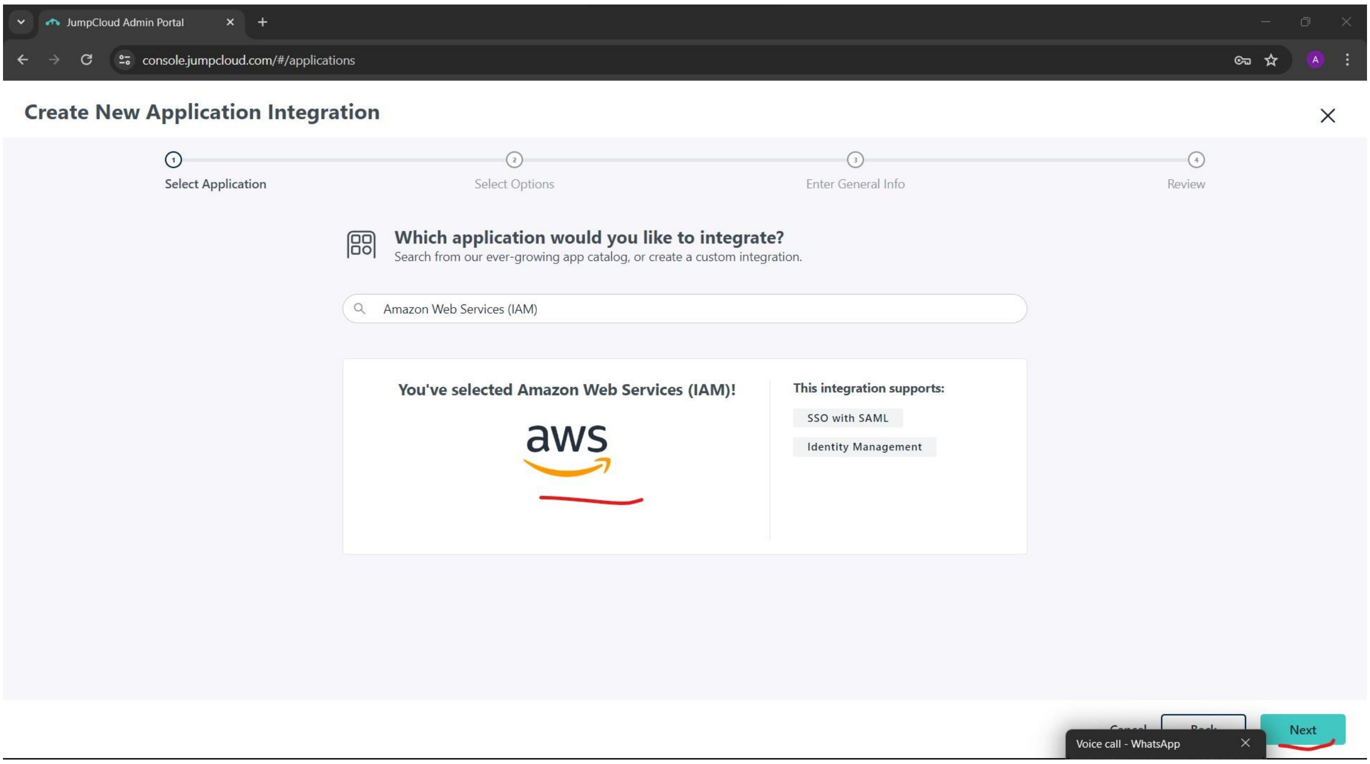
Export user identities from JumpCloud to external applications

Add your first application

Single Sign-On and Identity Management Application Integrations

Set up and manage single sign-on or create an identity management integration to import, update, and export users on a regular basis.

Pro Tip: You can connect nearly any HR Directory or Identity Provider to easily import new users into JumpCloud!



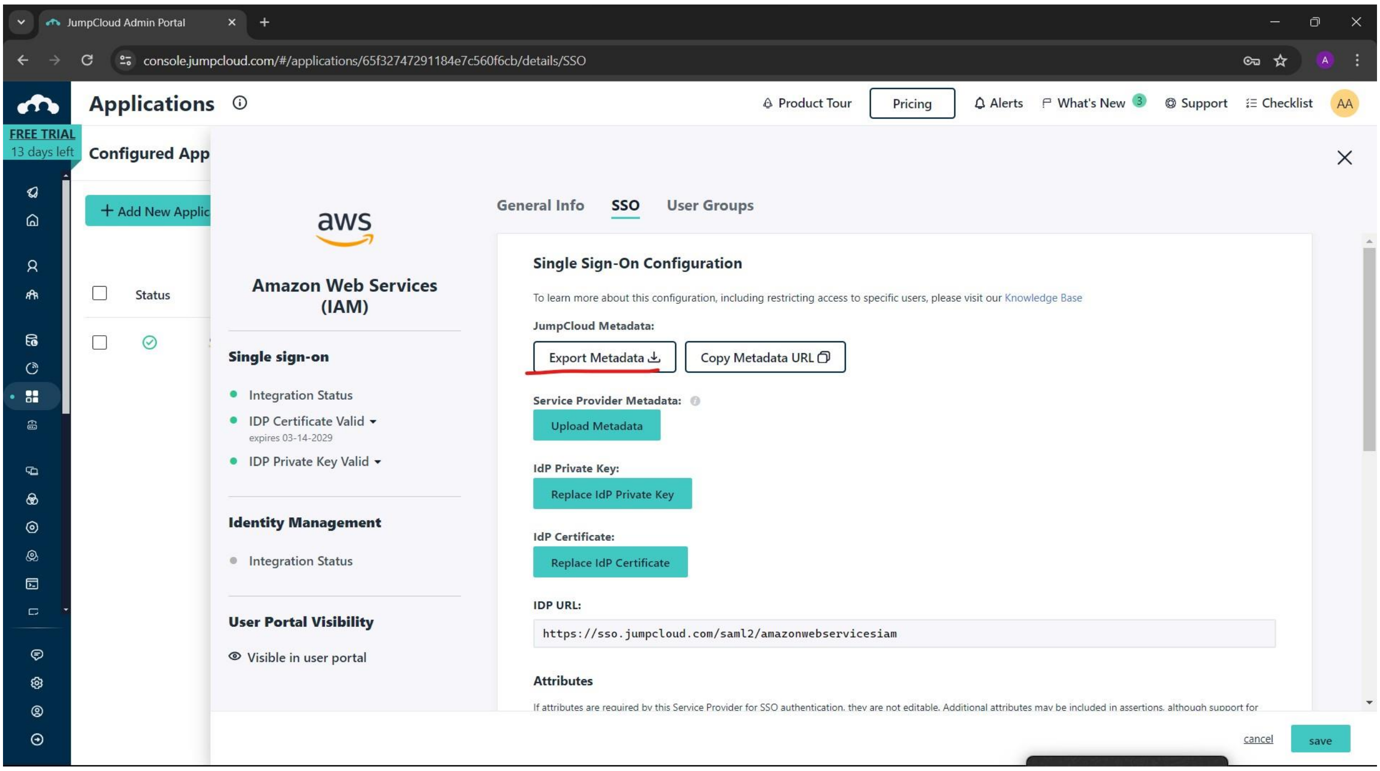
Create New Application Integration

Which application would you like to integrate?
Search from our ever-growing app catalog, or create a custom integration.

Amazon Web Services (IAM)

You've selected Amazon Web Services (IAM)!

This integration supports:
- SSO with SAML
- Identity Management



Amazon Web Services (IAM)

Single sign-on

- Integration Status
- IDP Certificate Valid
  expires 03-14-2029
- IDP Private Key Valid

Identity Management

- Integration Status

User Portal Visibility

Visible in user portal

Single Sign-On Configuration

To learn more about this configuration, including restricting access to specific users, please visit our Knowledge Base

JumpCloud Metadata:

Service Provider Metadata:

IdP Private Key:

IdP Certificate:

IDP URL:

`https://sso.jumpcloud.com/saml2/amazonwebservicesiam`

Attributes

If attributes are required by this Service Provider for SSO authentication, they are not editable. Additional attributes may be included in assertions, although support for

Setup in AWS IAM:

Create an IAM Role:

- Log in to the AWS Management Console.
- Go to IAM.
- Create a new IAM role for SAML 2.0 federation.
- Upload Metadata you downloaded
- Define the trust relationship to include JumpCloud as the trusted entity.

Configure the Role's Permissions:

- Define the permissions that external users will have when assuming this role. This could involve attaching policies or creating custom policies that define the permissions users will have.

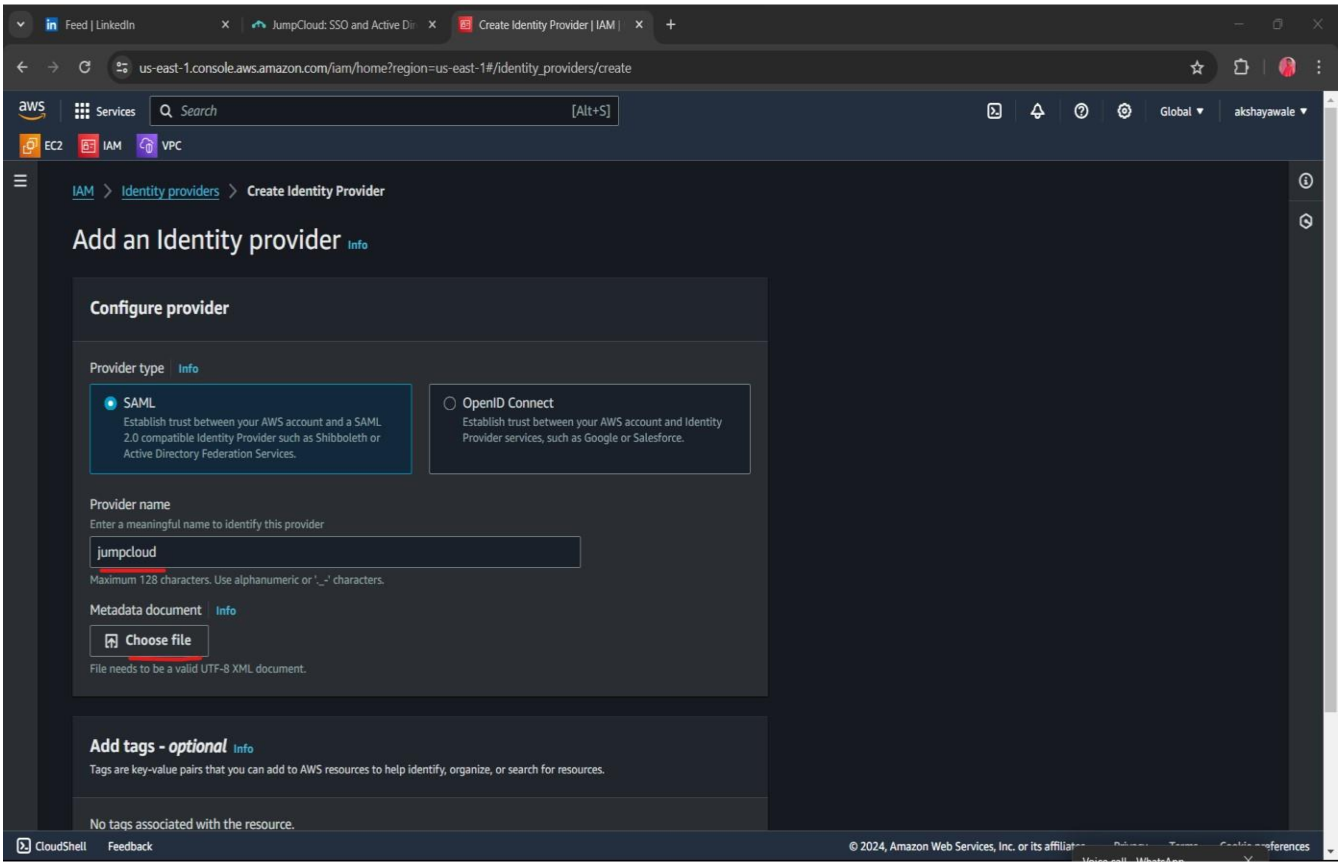
Configure Attribute Mapping:

- Map the SAML attributes sent by JumpCloud to the corresponding IAM role attributes.
- For example, you might map the NameID or email attribute to the AWS:username or AWS:email role attribute.

Provide the ARN of the IAM Role to JumpCloud:

The arn format should be :- <>,IdentityProviderArn,RoleArn<>

- After creating the IAM role, copy its ARN (Amazon Resource Name).
- Go back to JumpCloud's AWS SAML configuration.
- Paste the ARN into the appropriate field.


Feed | LinkedIn
JumpCloud: SSO and Active Di
Create Identity Provider | IAM |
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/identity_providers/create
Services
Search
[Alt+S]
Global ▼
akshayawale ▼
EC2
IAM
VPC
CloudShell
Feedback

IAM > Identity providers > Create Identity Provider

Add an Identity provider Info

Configure provider

Provider type Info

● SAML
Establish trust between your AWS account and a SAML 2.0 compatible Identity Provider such as Shibboleth or Active Directory Federation Services.

○ OpenID Connect
Establish trust between your AWS account and Identity Provider services, such as Google or Salesforce.

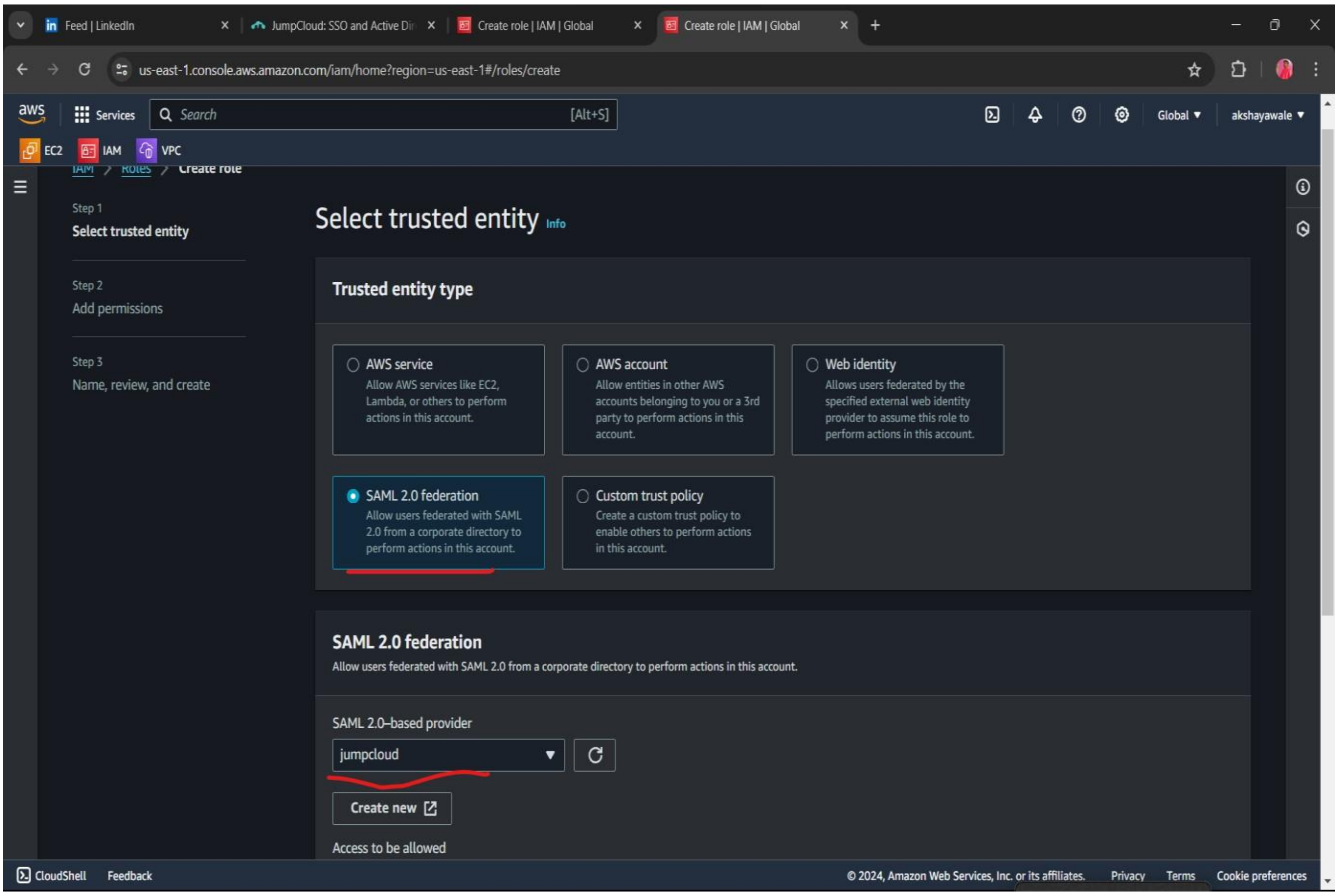
Provider name
Enter a meaningful name to identify this provider
jumpcloud
Maximum 128 characters. Use alphanumeric or '_-' characters.

Metadata document Info
Choose file
File needs to be a valid UTF-8 XML document.

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.

© 2024, Amazon Web Services, Inc. or its affiliat


Feed | LinkedIn
JumpCloud: SSO and Active Di
Create role | IAM | Global
Create role | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/create
Services
Search
[Alt+S]
Global ▼
akshayawale ▼
EC2
IAM
VPC
CloudShell
Feedback
Privacy
Terms
Cookie preferences

IAM > Roles > Create role

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.

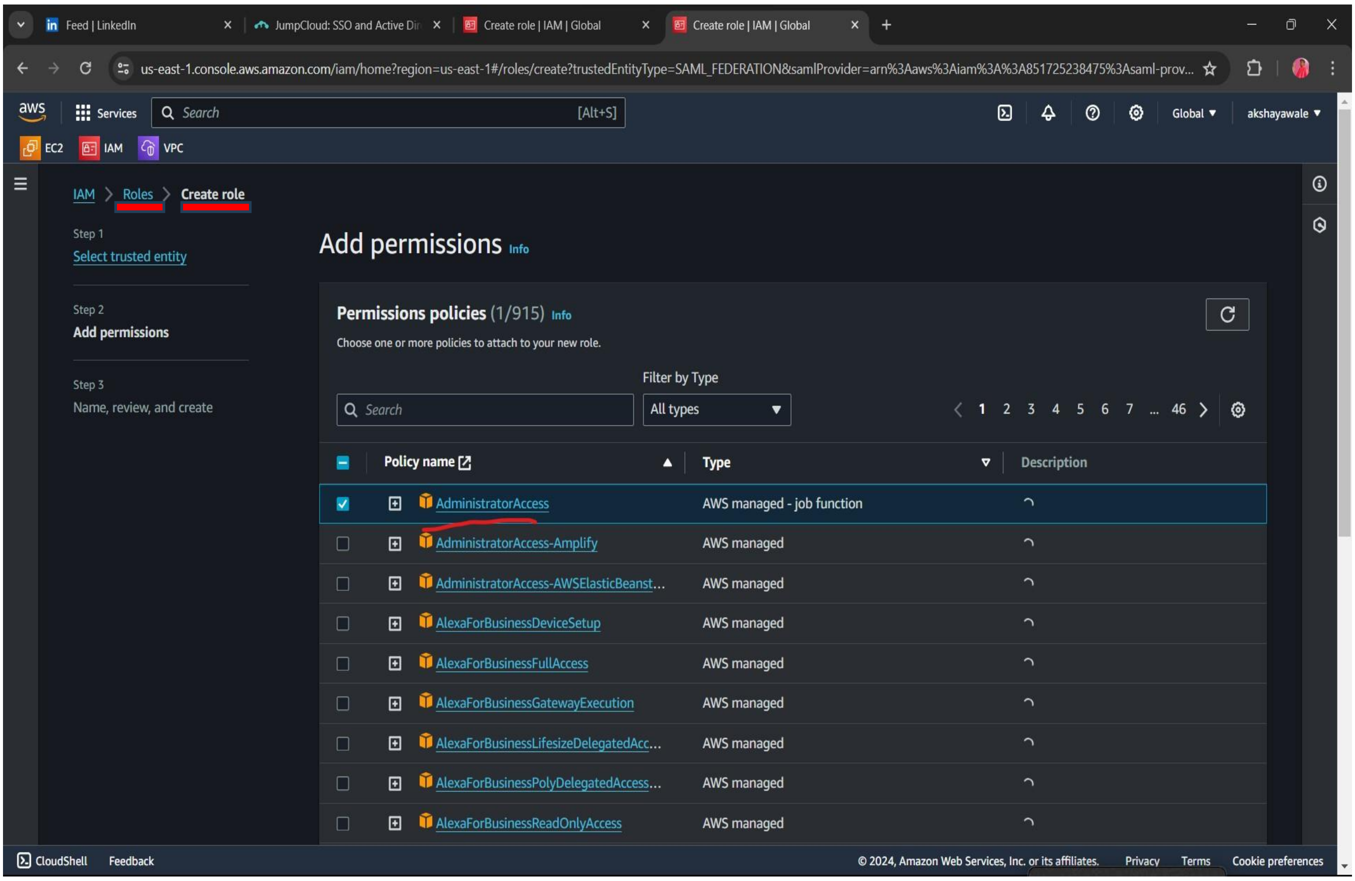
○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

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

SAML 2.0–based provider
jumpcloud ▼
Create new

Access to be allowed

© 2024, Amazon Web Services, Inc. or its affiliates.



us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/create?trustedEntityType=SAML_FEDERATION&samlProvider=arn%3Aaws%3Aiam%3A%3A851725238475%3Asaml-prov...

IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

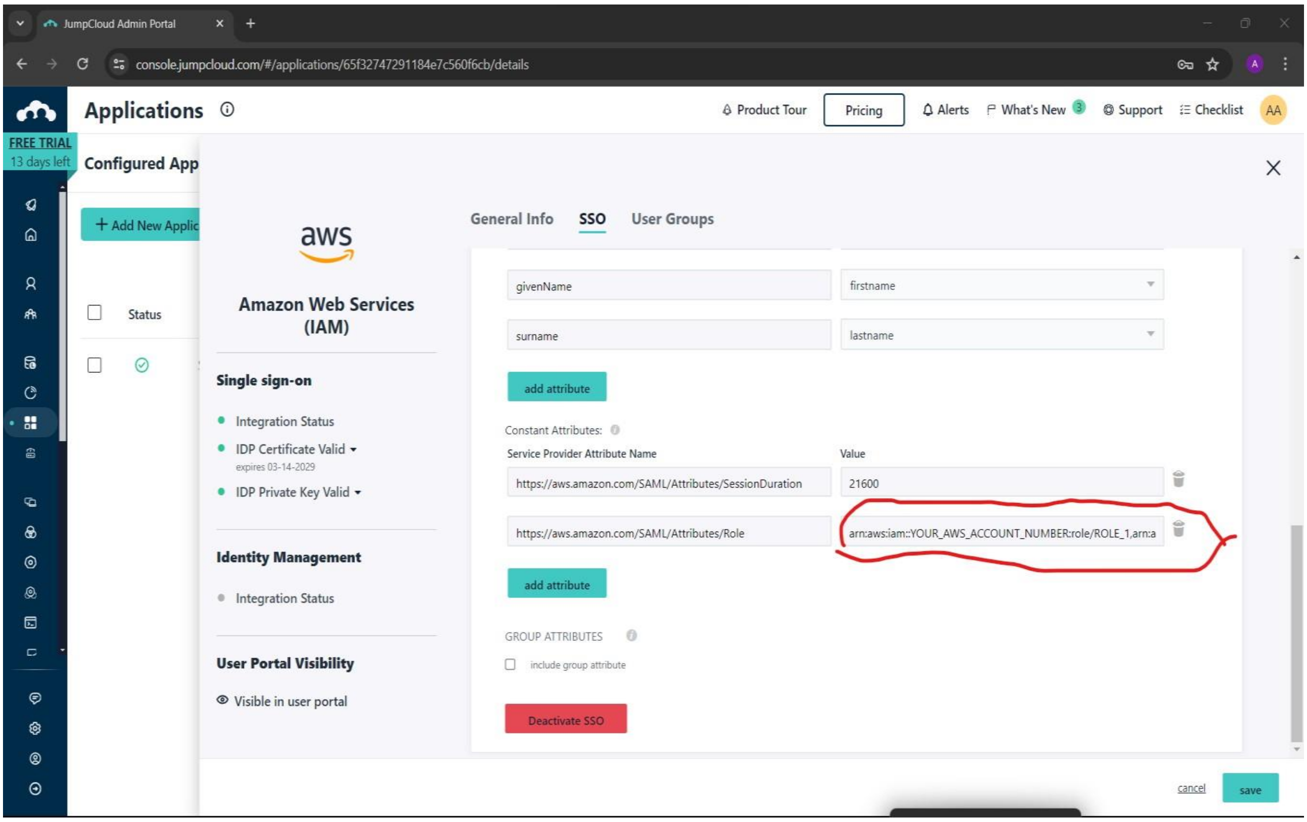
Add permissions Info

Permissions policies (1/915) Info

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

Filter by Type: All types

	Policy name	Type	Description
☑	AdministratorAccess	AWS managed - job function	
□	AdministratorAccess-Amplify	AWS managed	
□	AdministratorAccess-AWSElasticBeanst...	AWS managed	
□	AlexaForBusinessDeviceSetup	AWS managed	
□	AlexaForBusinessFullAccess	AWS managed	
□	AlexaForBusinessGatewayExecution	AWS managed	
□	AlexaForBusinessLifesizeDelegatedAcc...	AWS managed	
□	AlexaForBusinessPolyDelegatedAccess...	AWS managed	
□	AlexaForBusinessReadOnlyAccess	AWS managed	



console.jumpcloud.com/#/applications/65f32747291184e7c560f6cb/details

Applications

Amazon Web Services (IAM)

Single sign-on
- Integration Status
- IDP Certificate Valid
  expires 03-14-2029
- IDP Private Key Valid

Identity Management
- Integration Status

User Portal Visibility
Visible in user portal

General Info | **SSO** | User Groups

givenName	firstname
surname	lastname

add attribute

Constant Attributes:

Service Provider Attribute Name	Value
https://aws.amazon.com/SAML/Attributes/SessionDuration	21600
https://aws.amazon.com/SAML/Attributes/Role	arn:aws:iam::YOUR_AWS_ACCOUNT_NUMBER:role/ROLE_1,arn:a

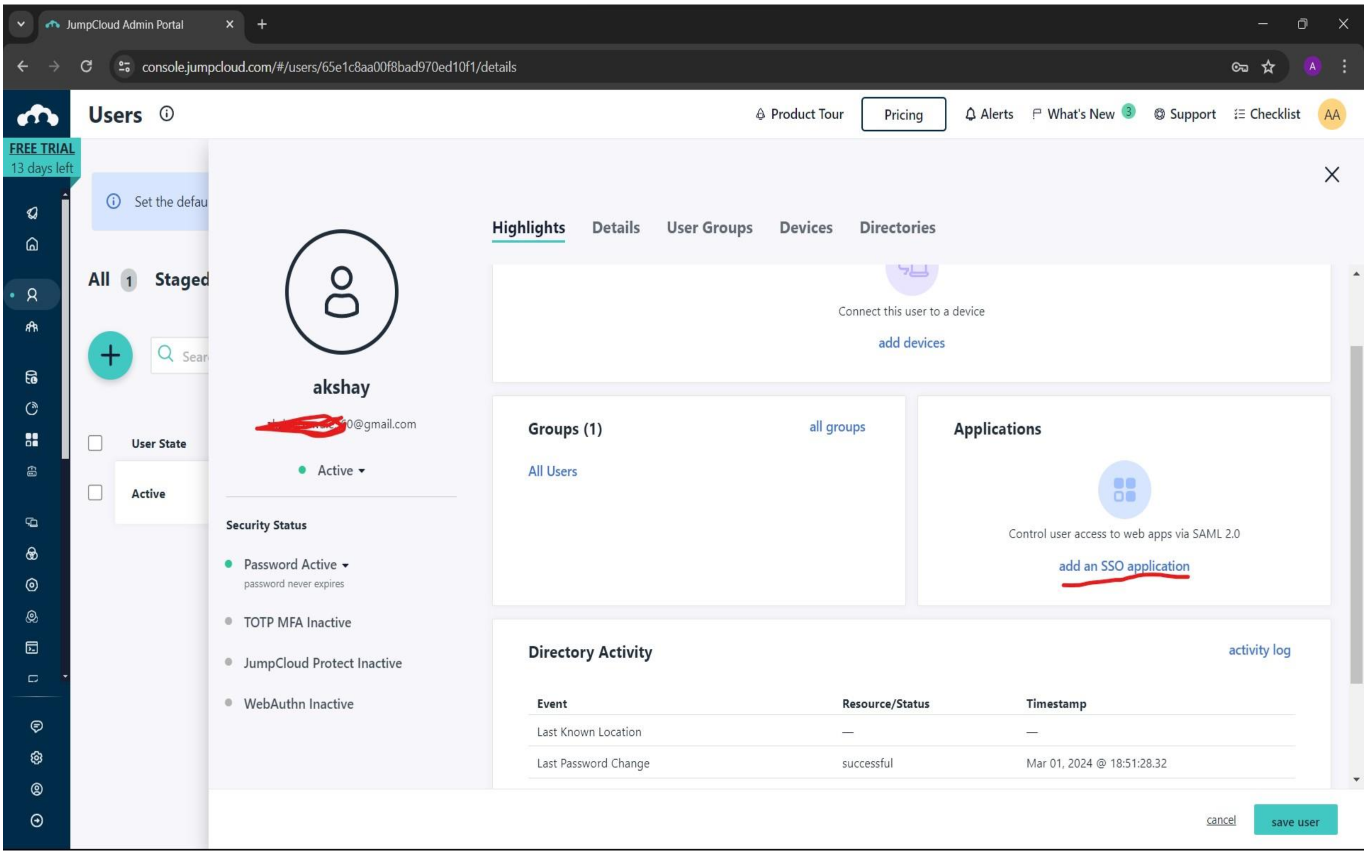
add attribute

GROUP ATTRIBUTES

□ include group attribute

Deactivate SSO

cancel save



JumpCloud Admin Portal

console.jumpcloud.com/#/users/65e1c8aa00f8bad970ed10f1/details

Users

Product Tour | Pricing | Alerts | What's New 3 | Support | Checklist | AA

FREE TRIAL
13 days left

Set the defau

All 1 Staged

Sear

User State

Active

akshay

[redacted]0@gmail.com

● Active

Security Status

- Password Active
  password never expires
- TOTP MFA Inactive
- JumpCloud Protect Inactive
- WebAuthn Inactive

Highlights | Details | User Groups | Devices | Directories

Connect this user to a device

add devices

Groups (1) — all groups

All Users

Applications

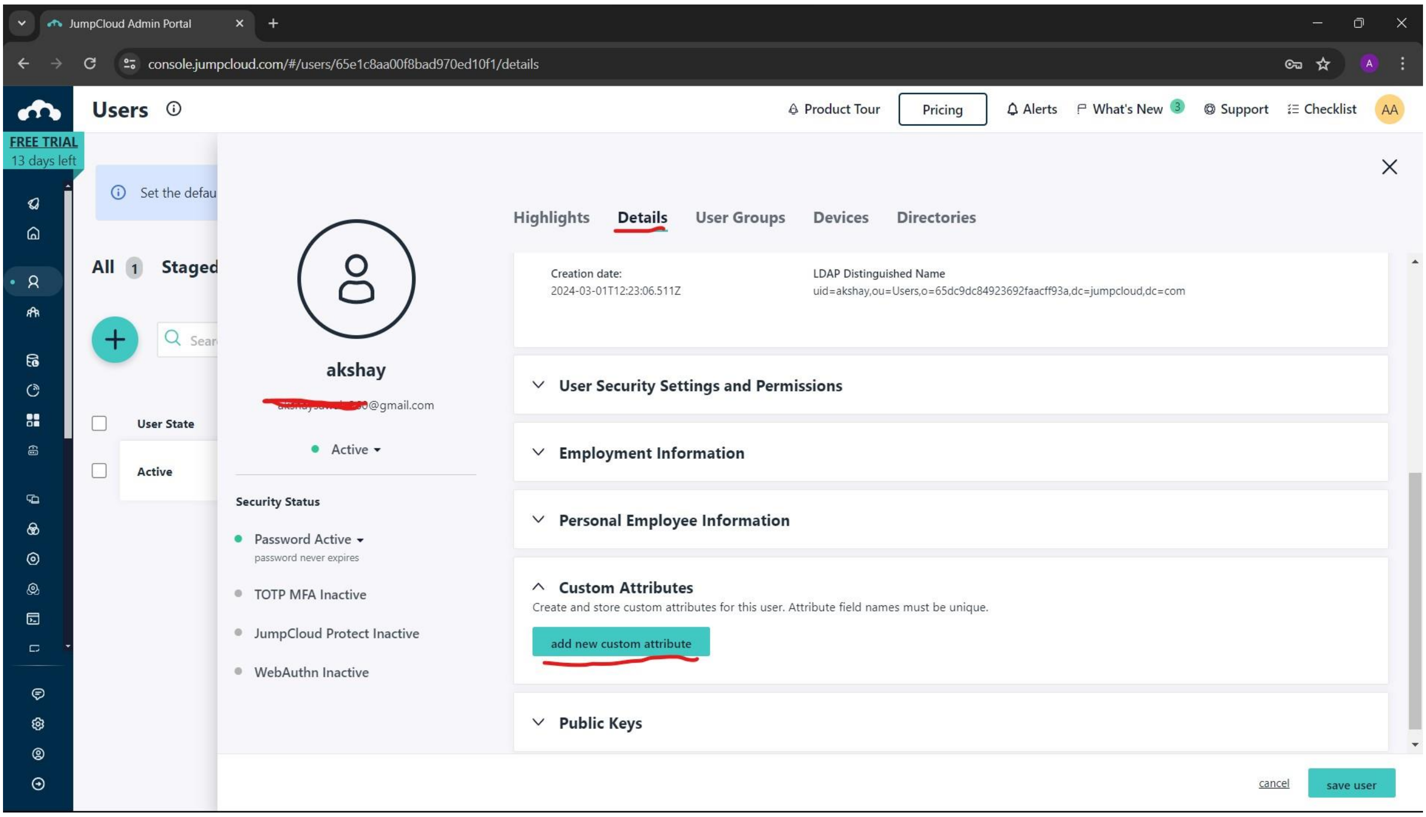
Control user access to web apps via SAML 2.0

add an SSO application

Directory Activity — activity log

Event	Resource/Status	Timestamp
Last Known Location	—	—
Last Password Change	successful	Mar 01, 2024 @ 18:51:28.32

cancel | save user



JumpCloud Admin Portal

console.jumpcloud.com/#/users/65e1c8aa00f8bad970ed10f1/details

Users

Product Tour | Pricing | Alerts | What's New 3 | Support | Checklist | AA

FREE TRIAL
13 days left

Set the defau

All 1 Staged

Sear

User State

Active

akshay

[redacted]0@gmail.com

● Active

Security Status

- Password Active
  password never expires
- TOTP MFA Inactive
- JumpCloud Protect Inactive
- WebAuthn Inactive

Highlights | Details | User Groups | Devices | Directories

Creation date:
2024-03-01T12:23:06.511Z

LDAP Distinguished Name
uid=akshay,ou=Users,o=65dc9dc84923692faacff93a,dc=jumpcloud,dc=com

User Security Settings and Permissions

Employment Information

Personal Employee Information

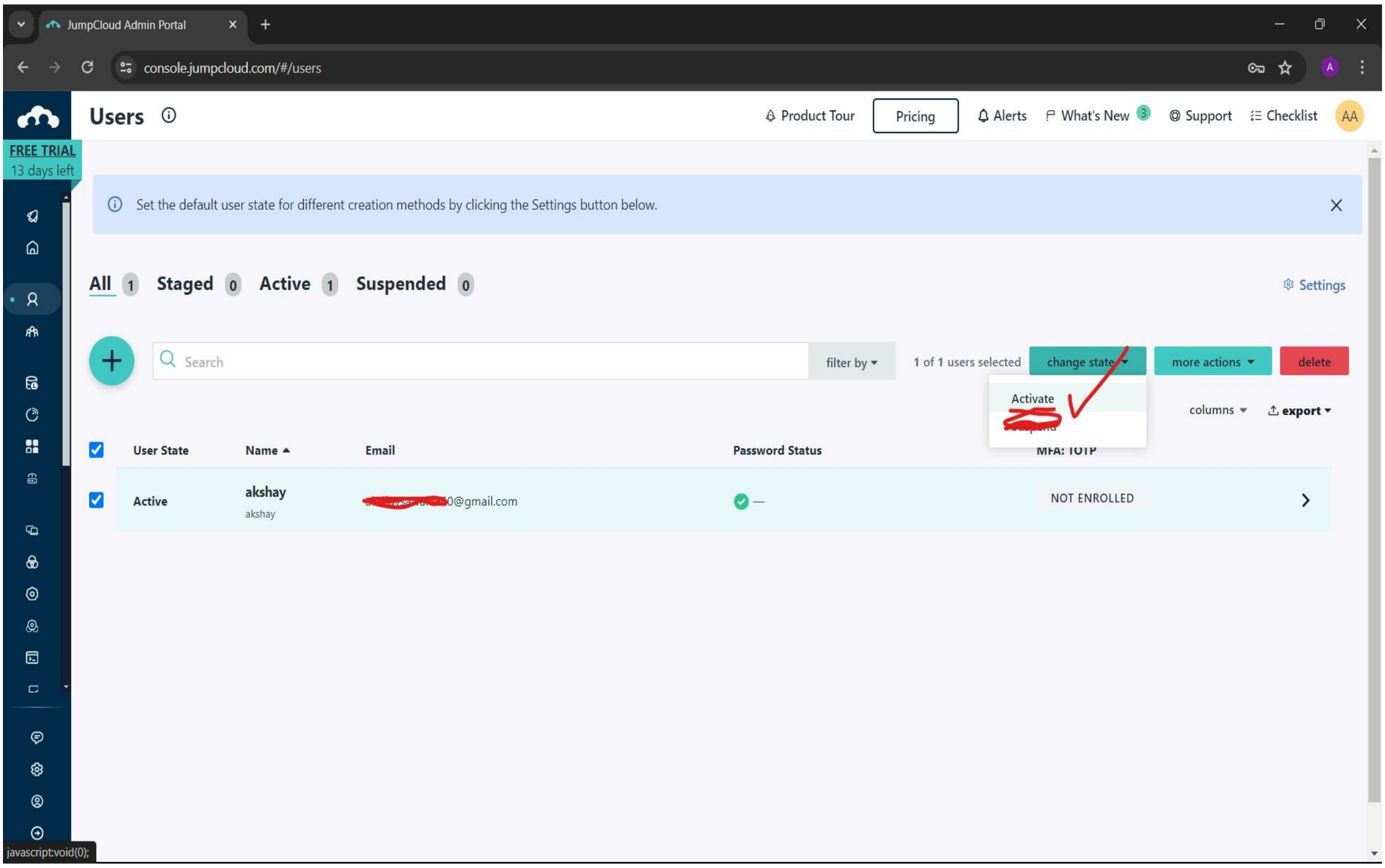
Custom Attributes

Create and store custom attributes for this user. Attribute field names must be unique.

add new custom attribute

Public Keys

cancel | save user



Users

Set the default user state for different creation methods by clicking the Settings button below.

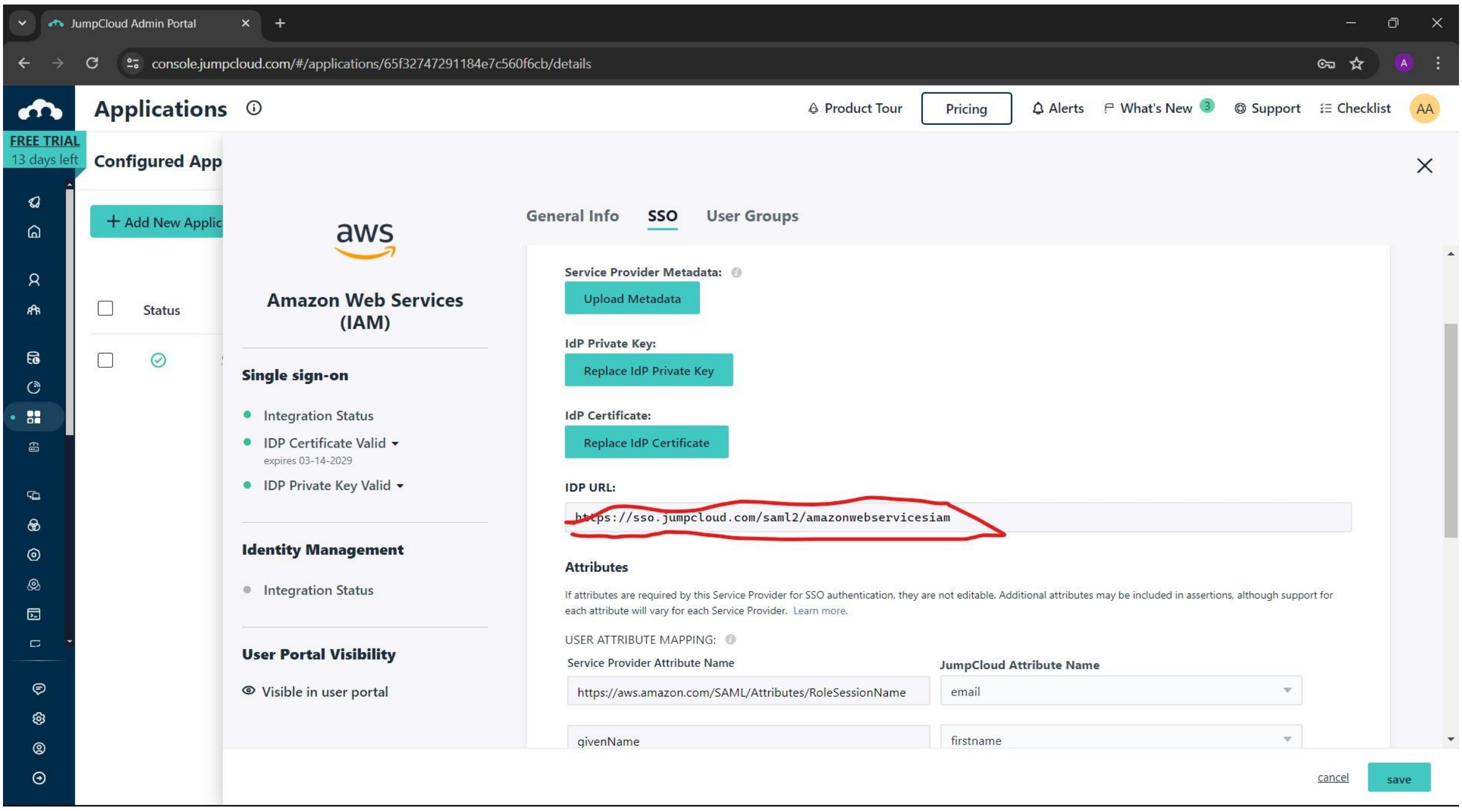
All 1 Staged 0 Active 1 Suspended 0 Settings

Search filter by ▾ 1 of 1 users selected change state ▾ more actions ▾ delete

Activate ✓
~~Suspend~~

columns ▾ export ▾

☑	User State	Name ▲	Email	Password Status	MFA: TOTP
☑	Active	akshay akshay	[redacted]@gmail.com	✓ —	NOT ENROLLED



Applications

General Info SSO User Groups

Amazon Web Services (IAM)

Single sign-on

- Integration Status
- IDP Certificate Valid ▾ expires 03-14-2029
- IDP Private Key Valid ▾

Identity Management

- Integration Status

User Portal Visibility

Visible in user portal

Service Provider Metadata: Upload Metadata

IdP Private Key: Replace IdP Private Key

IdP Certificate: Replace IdP Certificate

IDP URL:

```
https://sso.jumpcloud.com/saml2/amazonwebservicesiam
```

Attributes

If attributes are required by this Service Provider for SSO authentication, they are not editable. Additional attributes may be included in assertions, although support for each attribute will vary for each Service Provider. Learn more.

USER ATTRIBUTE MAPPING:

Service Provider Attribute Name	JumpCloud Attribute Name
https://aws.amazon.com/SAML/Attributes/RoleSessionName	email ▾
givenName	firstname ▾

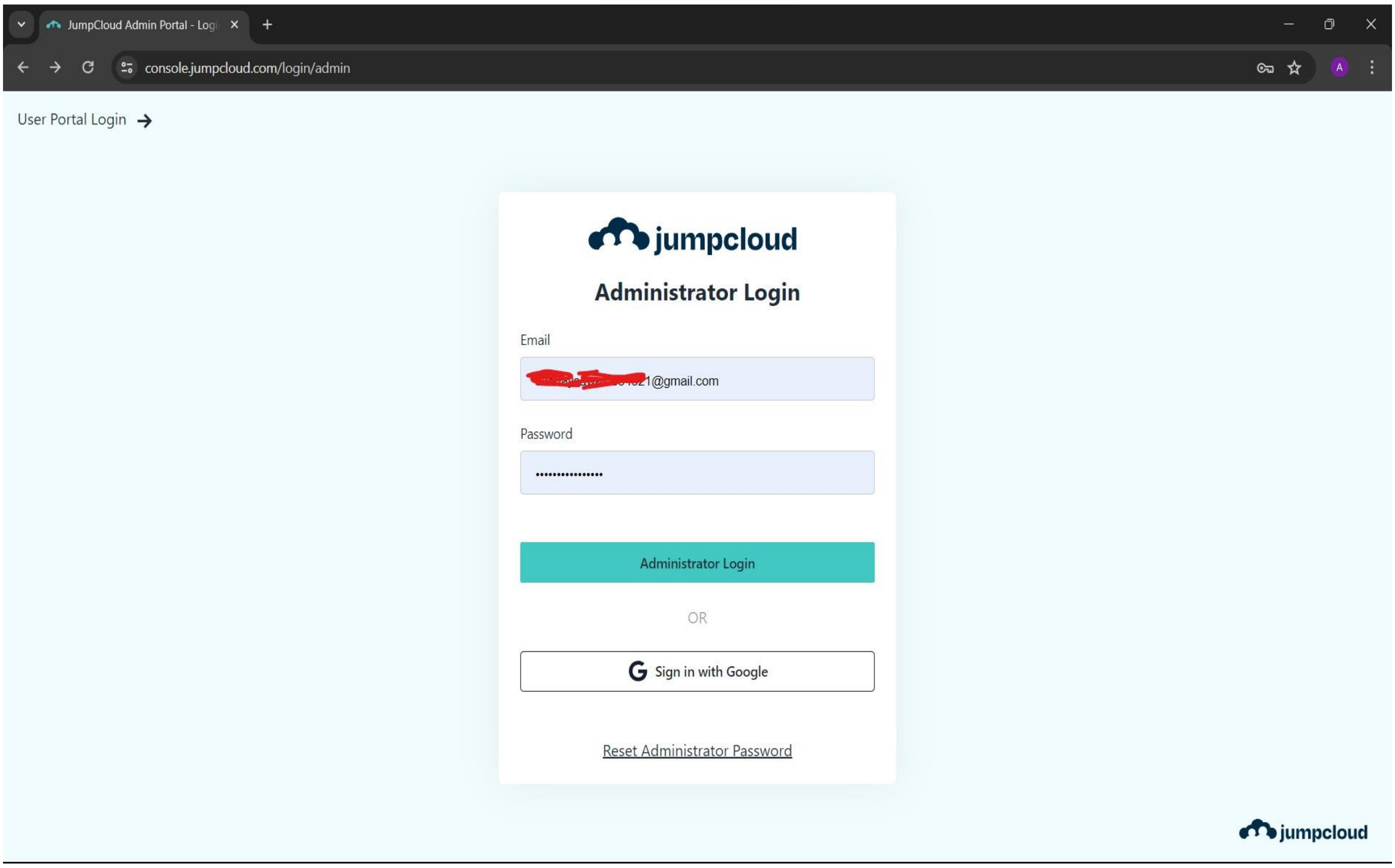
cancel save

Testing:

Test Access to Resources:

- After successful authentication, ensure that users have the appropriate permissions within AWS based on the IAM role assigned to them.
- Go to application and go to sso now you will get idp url copy and paste it in the browser
- Use the user credentials and login
- Click on application and now you will be redirected to aws console

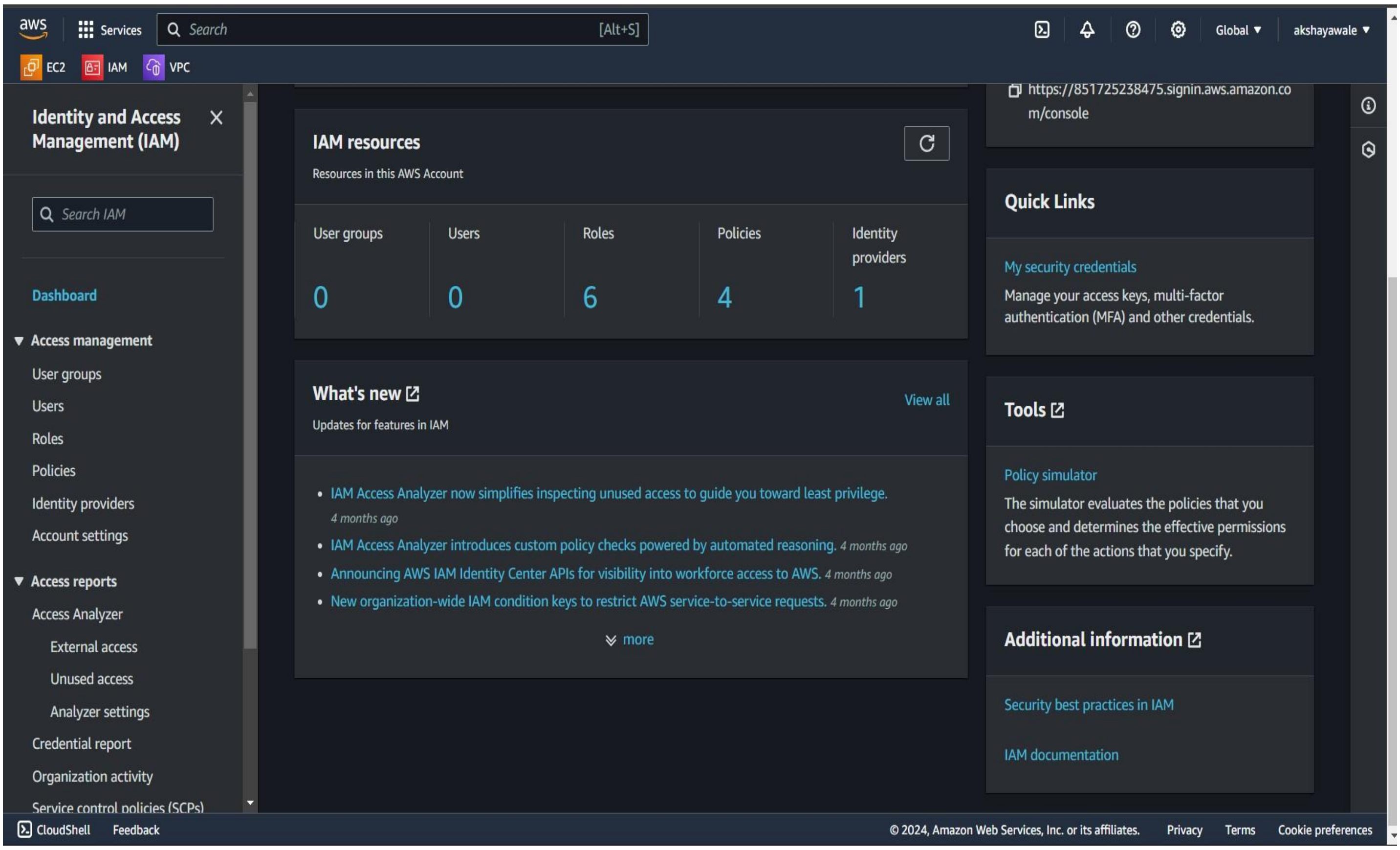
By following these steps, you should be able to set up access for external users to AWS using JumpCloud as the Identity Provider and AWS IAM roles for access control. Remember to follow best practices for security and regularly review and update your configurations as needed.



console.jumpcloud.com/login/admin

Email: [redacted]1@gmail.com

Password: ••••••••••••••••



https://851725238475.signin.aws.amazon.com/console

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
0	0	6	4	1

What's new

Updates for features in IAM

- IAM Access Analyzer now simplifies inspecting unused access to guide you toward least privilege. *4 months ago*
- IAM Access Analyzer introduces custom policy checks powered by automated reasoning. *4 months ago*
- Announcing AWS IAM Identity Center APIs for visibility into workforce access to AWS. *4 months ago*
- New organization-wide IAM condition keys to restrict AWS service-to-service requests. *4 months ago*

Quick Links

My security credentials

Manage your access keys, multi-factor authentication (MFA) and other credentials.

Tools

Policy simulator

The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.

Additional information

Security best practices in IAM

IAM documentation

© 2024, Amazon Web Services, Inc. or its affiliates.