

Configuring AWS

Users can securely log on to AWS using their enterprise credentials. To configure AWS for SSO through SAML, follow the steps below:



Root user sign in ⓘ

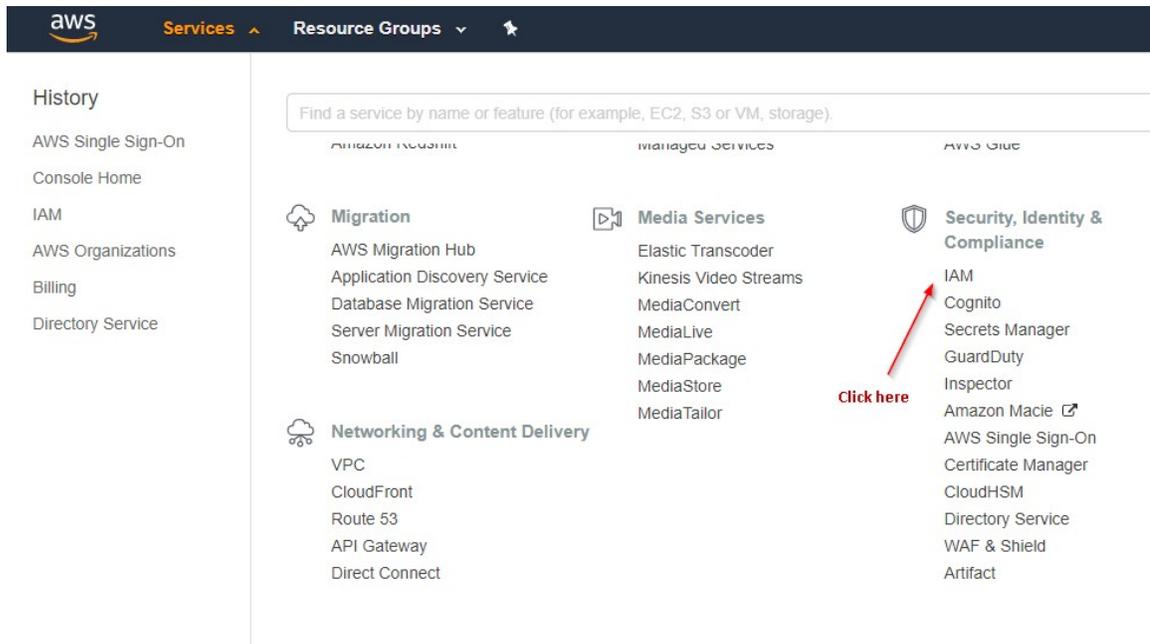
Email:

Password

[Forgot password?](#)

Sign in

1. Login to **AWS Console**.



- From the top panel click on **Services > IAM**.

Dashboard

Groups

Users

Roles

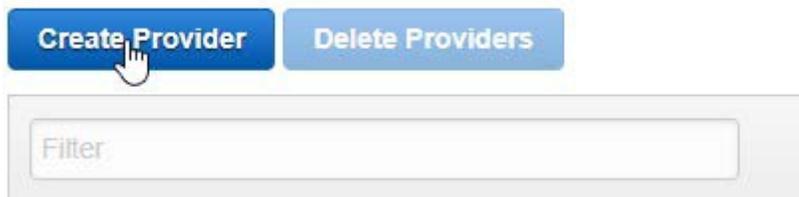
Policies

Identity providers

Account settings

Credential report

- Identity and Access Management page will open > From the left panel select **Identity providers**.



- Click on **Create Provider**.

Configure Provider

Choose a provider type.

Provider Type*

Choose a provider type ▾

SAML

OpenID Connect

- Configure Provider window will open > Select **SAML** from **Provider Type** drop-down.

Provider Type*

SAML ▾

Provider Name*

Netscaler

Maximum 128 characters. Use alphanumeric and '._-' characters.

Metadata Document*

Choose File

- After selecting Provider Type, two more template will appear.
- Enter Provider Name as **Netscaler** and upload IdP metadata (as shown in **Step 2**) in **Metadata Document**.
- Click on **Next > Create**

Filter			Showing 1 results
<input type="checkbox"/>	Provider Name ↕	Type ↕	Creation Time ↕
<input type="checkbox"/>	NetScaler	SAML	2018-04-04 18:03 UTC+0530

- Provider will be created and will display in the list.

- Dashboard
- Groups
- Users
- Roles**
- Policies
- Identity providers
- Account settings
- Credential report

- Click on **Roles** from the left panel.
- Roles window will open > Click on **Create role**.



AWS service
EC2, Lambda and others



Another AWS account
Belonging to you or 3rd party



Web identity
Cognito or any OpenID provider

1


SAML 2.0 federation
Your corporate directory

Allows users that are federated with SAML 2.0 to assume this role to perform actions in your account. [Learn more](#)

Choose a SAML 2.0 provider

If you're creating a role for API access, choose an Attribute and then type a Value to include in the role. This restricts access to users with the specified attributes.

SAML provider 2

NetScaler Create new provider [↗](#) | Refresh

Allow programmatic access only
3 Allow programmatic and AWS Management Console access

Attribute SAML:aud

Value* https://signin.aws.amazon.com/saml

- Click on **SAML 2.0 federation** > Select **NetScaler** from the SAML provide drop-down.
- Select **Allow programmatic and AWS Management Console access**.

14. Attribute and Value field will generate automatically > Click **Next**.

Filter: Policy type Showing 369 results

	Policy name	Attachments	Description
<input checked="" type="checkbox"/>	AdministratorAccess	0	Provides full access to AWS services and resources.
<input type="checkbox"/>	iam:AttachUserPolicy	1	Provides the ability to attach policies to IAM users.
<input type="checkbox"/>	iam:AttachGroupPolicy	1	Provides the ability to attach policies to IAM groups.
<input type="checkbox"/>	iam:AttachRolePolicy	1	Provides the ability to attach policies to IAM roles.
<input type="checkbox"/>	iam:CreateAccessKey	1	Provides the ability to create an access key for an IAM user.
<input type="checkbox"/>	iam:CreateGroup	1	Provides the ability to create an IAM group.
<input type="checkbox"/>	iam:CreateRole	1	Provides the ability to create an IAM role.
<input type="checkbox"/>	iam:CreateUser	1	Provides the ability to create an IAM user.
<input type="checkbox"/>	iam:DeleteAccessKey	1	Provides the ability to delete an access key for an IAM user.
<input type="checkbox"/>	iam:DeleteGroup	1	Provides the ability to delete an IAM group.
<input type="checkbox"/>	iam:DeleteRole	1	Provides the ability to delete an IAM role.
<input type="checkbox"/>	iam:DeleteUser	1	Provides the ability to delete an IAM user.

15. A list of policy will appear > Select **AdministratorAccess** > Click **Next**.

Role name*

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

Role description

Maximum 1000 characters. Use alphanumeric and '+,.,@,-_' characters.

Trusted entities The identity provider(s)

Policies AdministratorAccess [↗](#)

16. Provide Role name as your choice > Click **Create role**.

Showing 3 results

Role name	Description	Creation time
Administrator		2018-04-04 16:58 UTC+0530

17. Role will appear in the role list > Click on your Role name.

Role ARN	 
Role description	Edit
Instance Profile ARNs	
Path	/
Creation time	2018-04-12 14:54 UTC+0530
Maximum CLI/API session duration	1 hour Edit

18. Copy Role ARN and save it for further use.

Permissions | **Trust relationships** | Access Advisor | Revoke sessions

You can view the trusted entities that can assume the role and the access conditions for the role. [Show policy document](#)

[Edit trust relationship](#)

Trusted entities
The following trusted entities can assume this role.

Trusted entities


 **Copy**

Conditions
The following conditions define how and when trusted entities can assume the role.

Condition	Key	Value
StringEquals	SAML:aud	https://signin.aws.amazon.com/saml

19. Click on **Trust relationships** and copy the IdP ARN from Trusted entities and save it for further use.