CITRIX

NetScaler with Unified Gateway

Configuring AWS Console

Contents

Disclaimer (Documentation)

Preface

This section provides an overview about the information included in this guide.

Intended Audience

The information in this guide is intended for the System Administrators.

Document Conventions

The following table lists various conventions used in this guide.

Table 1: Document conventions used in this guide

Convention	Description
Bold	Used for names of interface elements (such as names of fields, panes, windows, menus, buttons, dialog boxes) and what the user specifically selects, clicks, presses, or types.
Note	Used to highlight information that is important.

Overview

The Citrix NetScaler application delivery controller (ADC) helps to load balance, accelerate, optimize, and secure enterprise applications.

AWS Console can be integrated with Identity Provider (IdP) for user authentication. This enable the users to sign in to AWS Console using the same Single Sign On (SSO).

Terminology

An Identity Provider (IdP) provides authentication module to verify users with their corporate network. A Service Provider (SP) supports receiving SSO SAML assertions.

The following table lists various terms that are used alternatively for completing configurations for service providers and identity providers.

Table 2: Terminology used for SP and IdP configurations

Service Provider (SP)	Identity Provider (IdP)
Identity Provider Issuer	Issuer Name
SP Entity ID	Service Provider ID
SP Assertion Consumer Service URL	Assertion Consumer Service URL

Configuring AWS Console for Single Sign-On

AWS Console has SP/IdP initiated flow, which is supported in NetScaler (12.1.).

Before you start, you need the following:

- Admin account for AWS Console
- Admin account for NetScaler

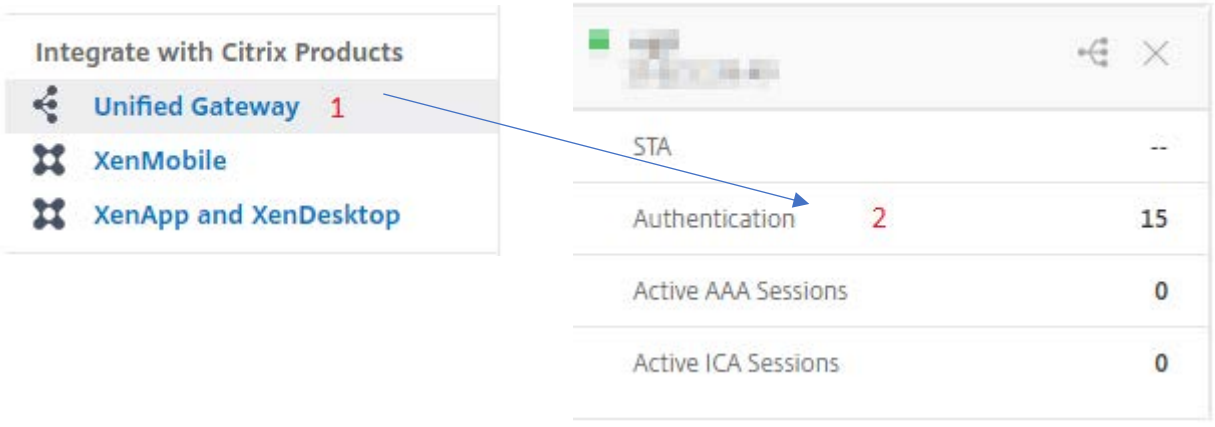
AWS Console Configuration

The AWS Console configuration steps are as follows:

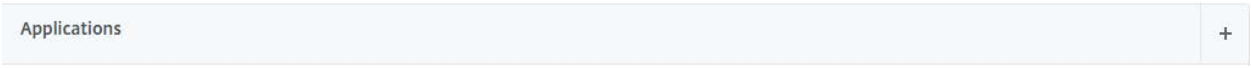
1. Configure AWS Console with the App Catalog.
2. Export AWS Console IdP metadata from NetScaler.
3. Configure IdP into AWS Console.

Step 1: Configured AWS Console with App Catalog

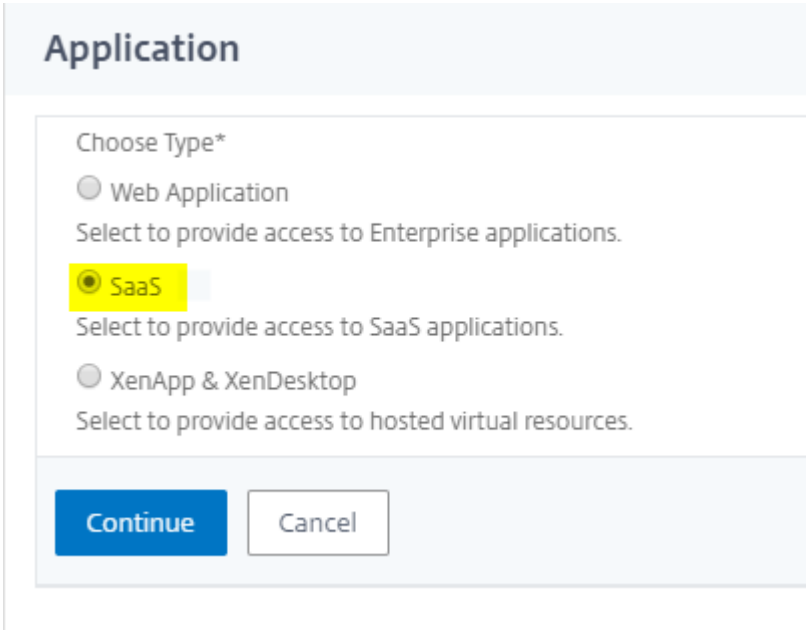
1. Click on **Unified Gateway > Authentication.**



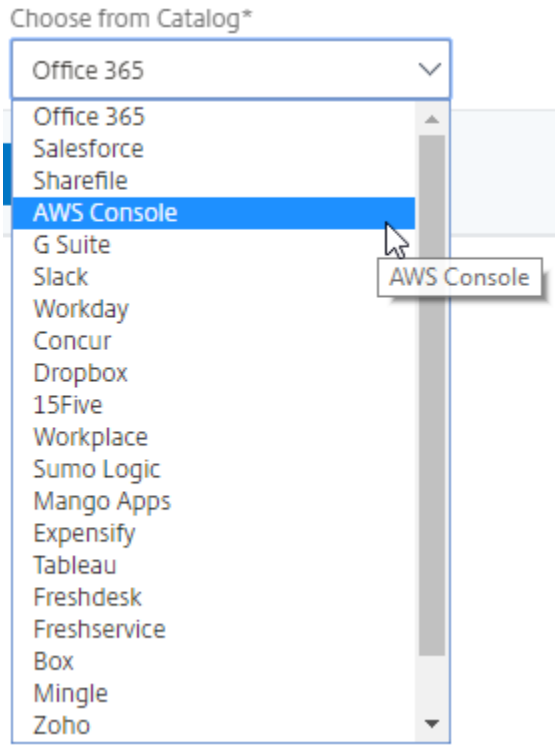
The **Unified Gateway Configuration** screen appears.



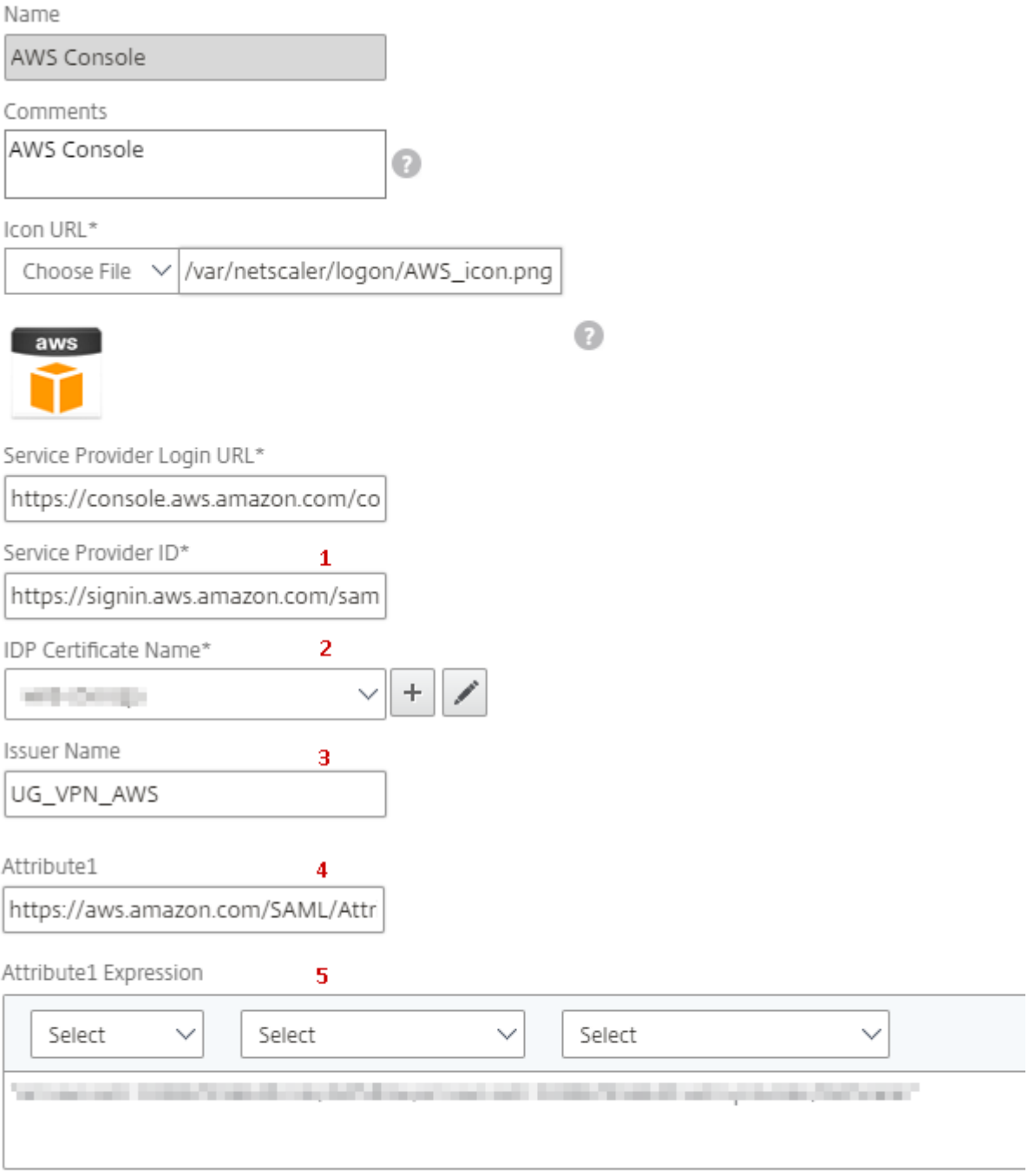
2. Go to **Applications** section. Click on icon. Now, you can see + icon**.** Click on it. The **Application** window appears.



3. Select **SaaS** from the Application type.
4. Select **AWS Console** from the drop-down list.



5. Fill the application template with appropriate values.



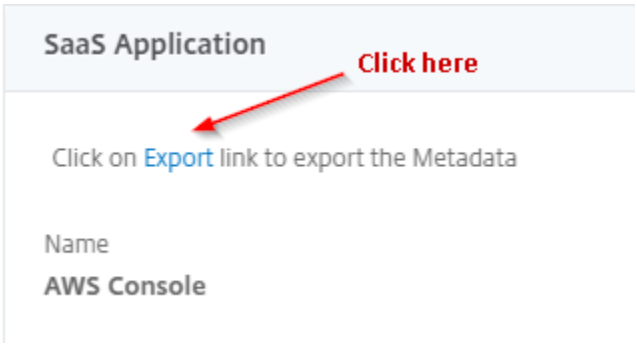
6. You must update the fields in NetScaler with the following values

Fields in Netscaler	Values
Service Provider ID	https://signin.aws.amazon.com/saml
Signing Certificate Name	IdP certificate needs to be selected
Issuer Name	Issuer name can be filled as per your choice
Attribute1	https://aws.amazon.com/SAML/Attributes/Role
Attribute1 Expression	<Role ARN>,<IdP ARN> : [As shown in step 3]

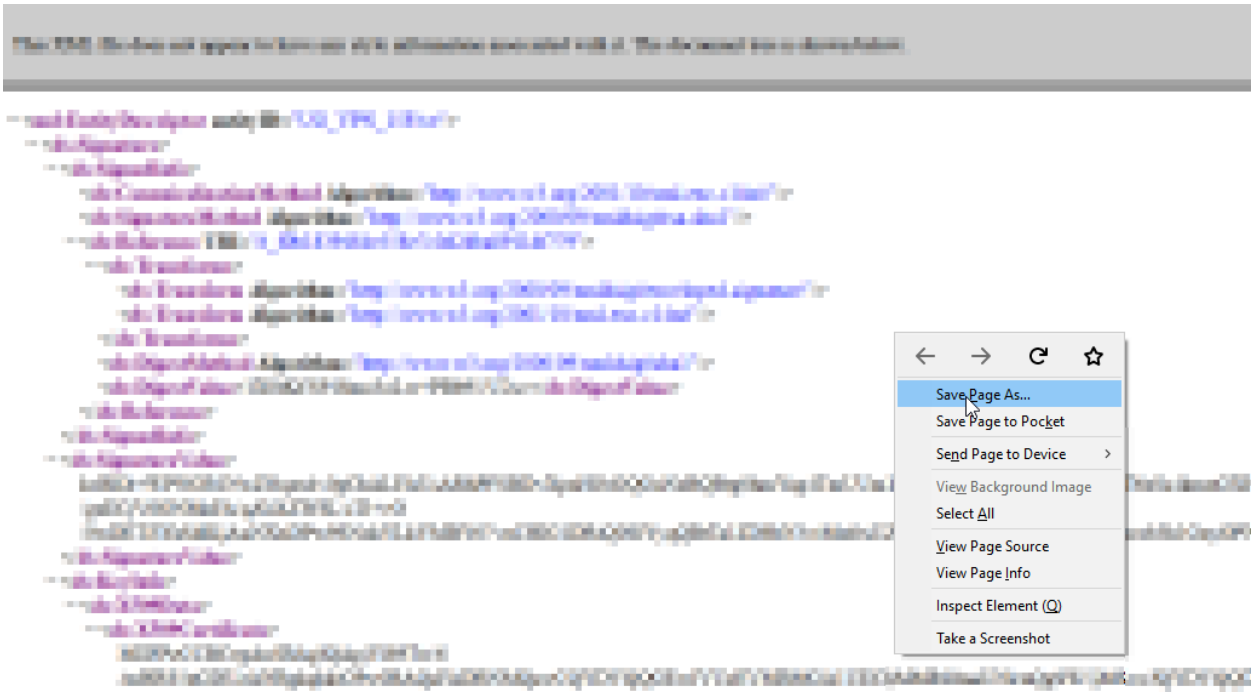
7. After providing the required values, click **Continue.** Click **Done.**

Step 2: Export AWS Console IdP metadata from NetScaler.

1. Click on **Unified Gateway > Authentication.**
2. Scroll down and click on **Mingle** template. The **SaaS Application** window **appears.** Click on **Export** link.

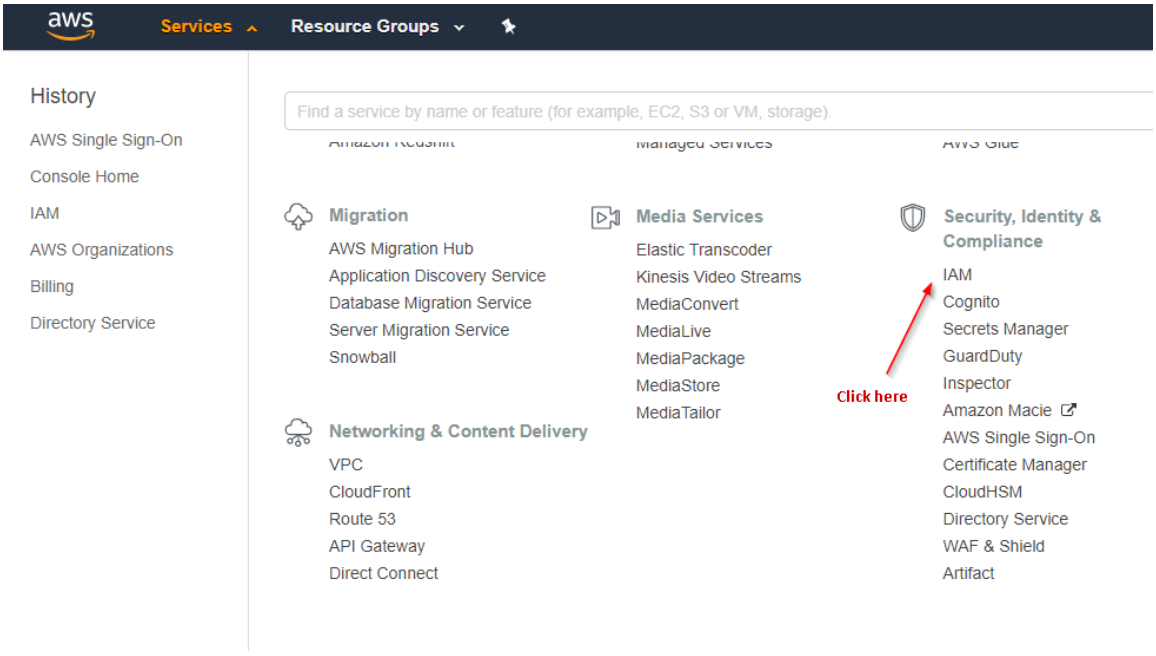


3. **Metadata** will open in a different window. Save the **IdP Metadata** file.

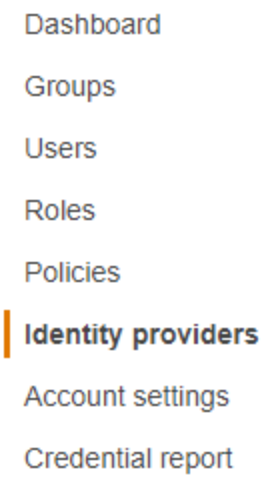


Step 3: Configure Single Sign-On in AWS Console

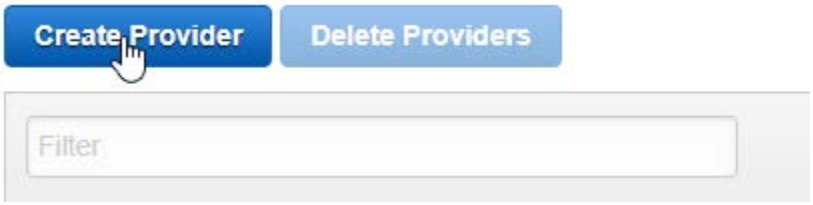
1. Login to **AWS Console**.



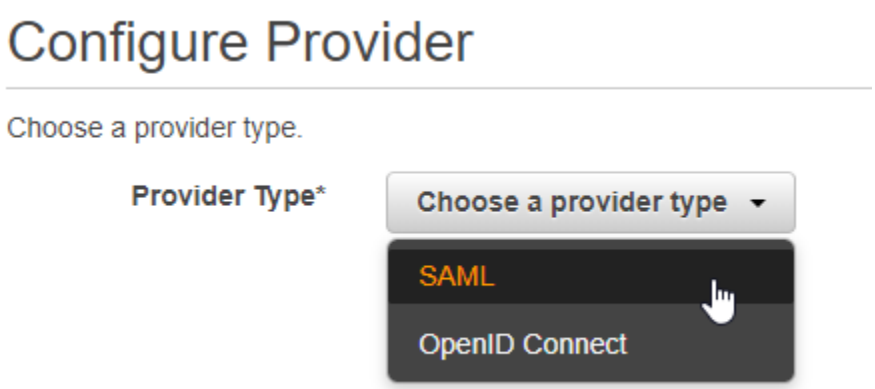
2. From the top panel click on **Services > IAM.**



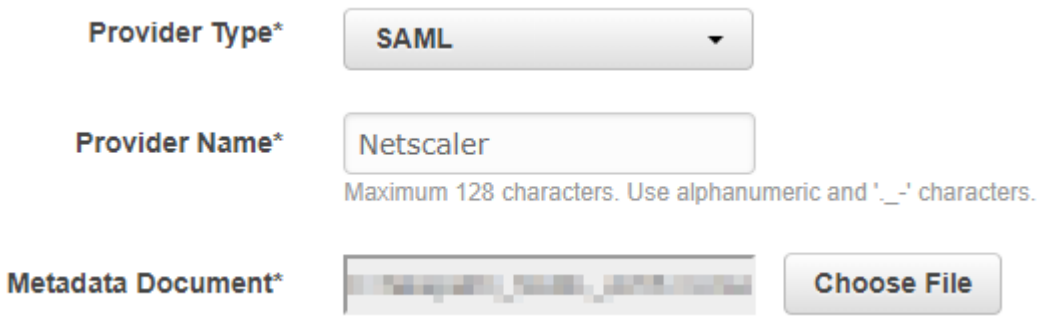
3. Identity and Access Management page will open **>** From the left panel select **Identity providers.**



4. Click on **Create Provider.**

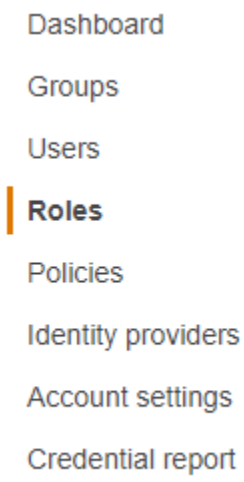


5. Configure Provider window will open **>** Select **SAML** from **Provider Type** drop-down.

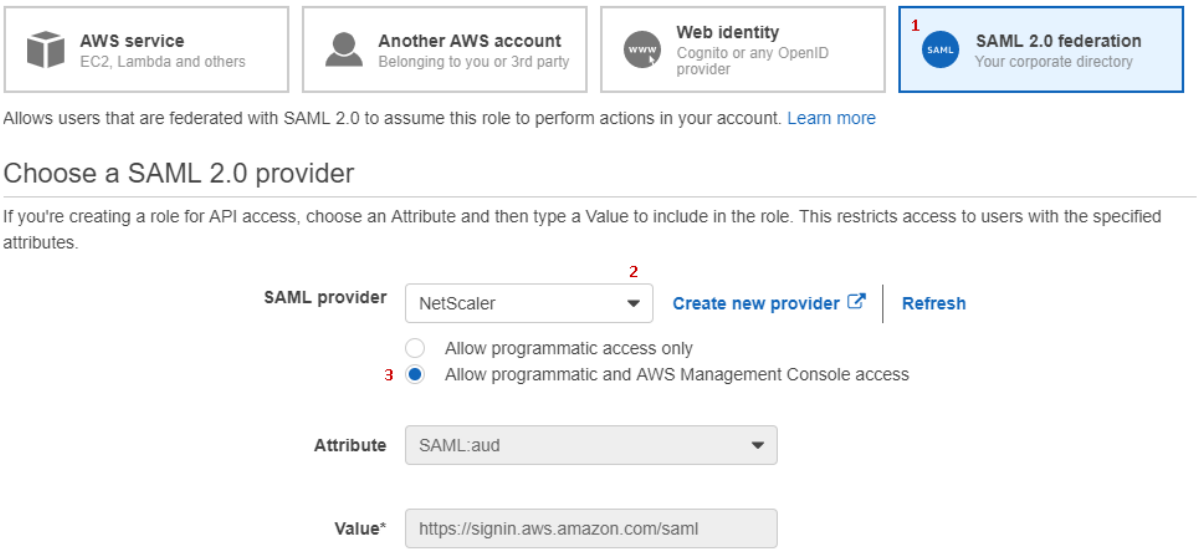


6. After selecting Provider Type, two more template will appear.
7. Enter Provider Name as **Netscaler** and upload IdP metadata (as shown in **Step 2**) in **Metadata Document**.
8. Click on **Next > Create**

9. Priovider will be created and will display in the list.

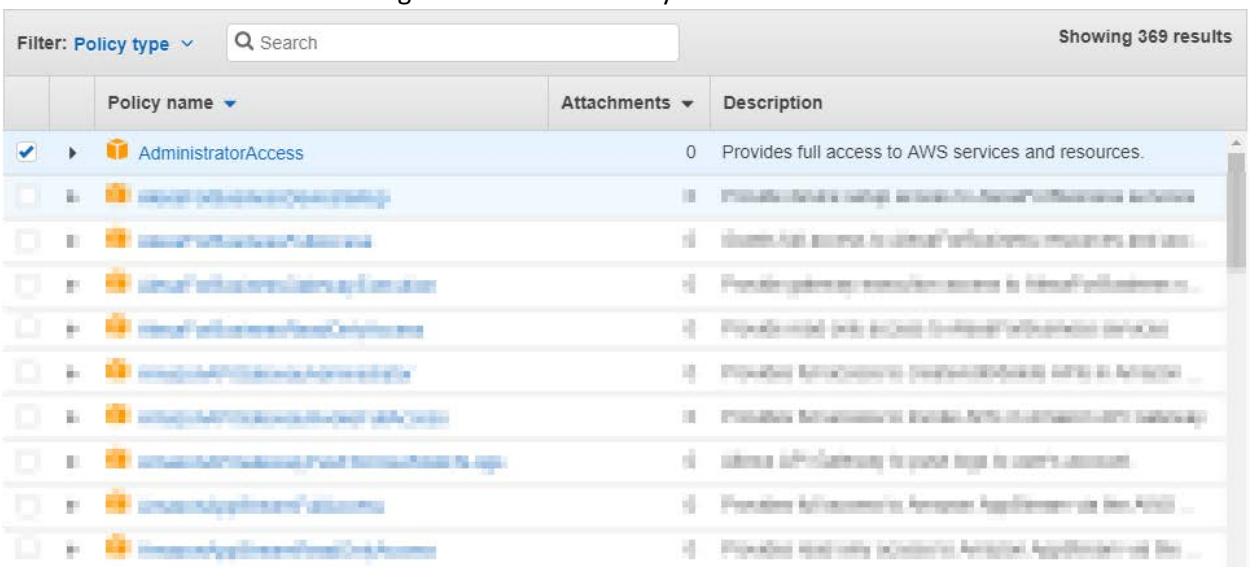


10. Click on **Roles** from the left panel.
11. Roles window will open **>** Click on **Create role.**

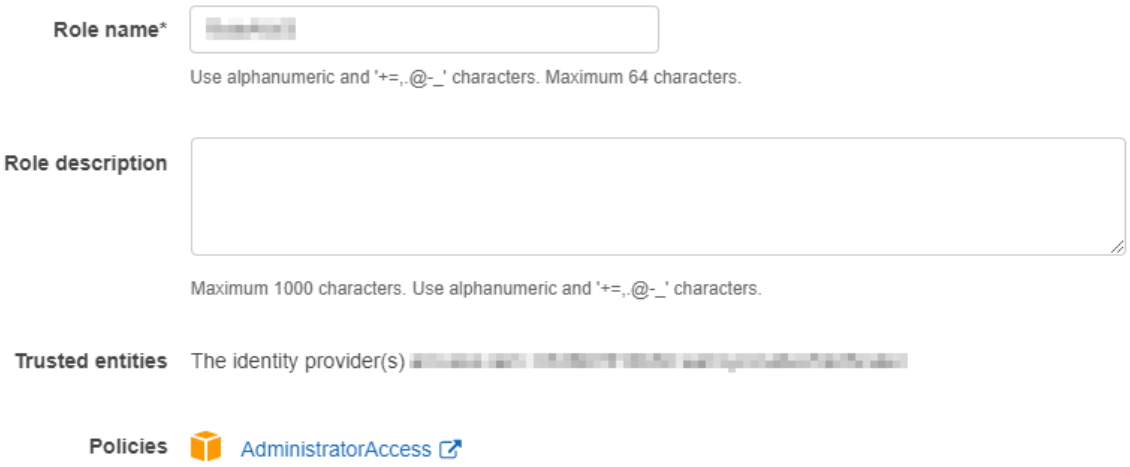


12. Click on **SAML 2.0 federation >** Select **NetScaler** from the SAML provide drop-down.
13. Select **Allow programmatic and AWS Management Console access.**

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

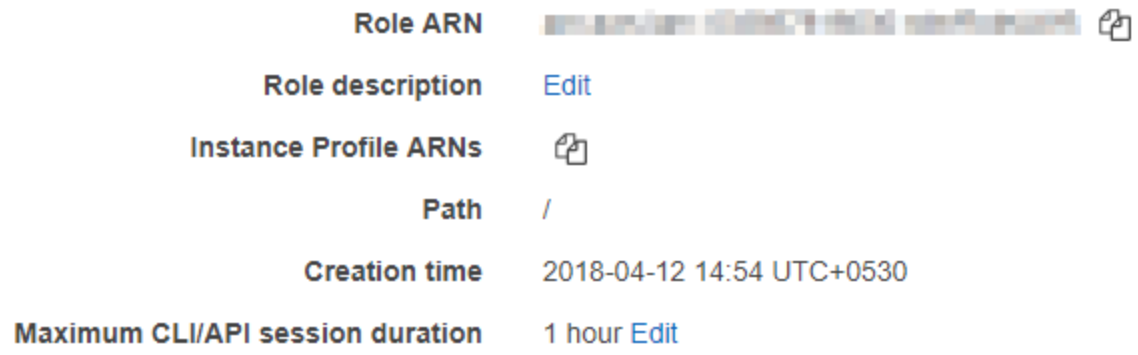


15. A list of policy will appear **>** Select **AdministratorAccess >** Click **Next.**

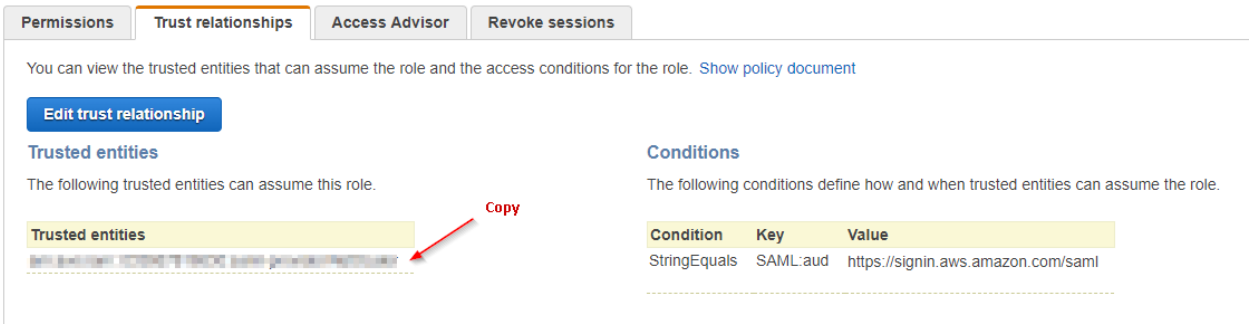


16. Provide Role name as your choice **>** Click **Create role.**

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



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



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