



NetScaler with Unified Gateway

Configuring AWS
Console

Contents

- CONTENTS 1
- DISCLAIMER (DOCUMENTATION) 2
- PREFACE 3
- OVERVIEW 4
- CONFIGURING AWS CONSOLE FOR SINGLE SIGN-ON 5

Disclaimer (Documentation)

This document is furnished "AS IS." Citrix Systems, Inc. disclaims all warranties regarding the contents of this document, including, but not limited to, implied warranties of merchantability and fitness for any particular purpose. This document may contain technical or other inaccuracies or typographical errors. Citrix System, Inc. reserves the right to revise the information in this document at any time without notice. This document and the software described in this document constitute confidential information of Citrix Systems, Inc. and its licensors, and are furnished under a license from Citrix Systems, Inc.

Citrix Systems, Inc., the Citrix logo, and Citrix Provisioning Services are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark office and in other countries. All other trademarks and registered trademarks are property of their respective owners.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

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

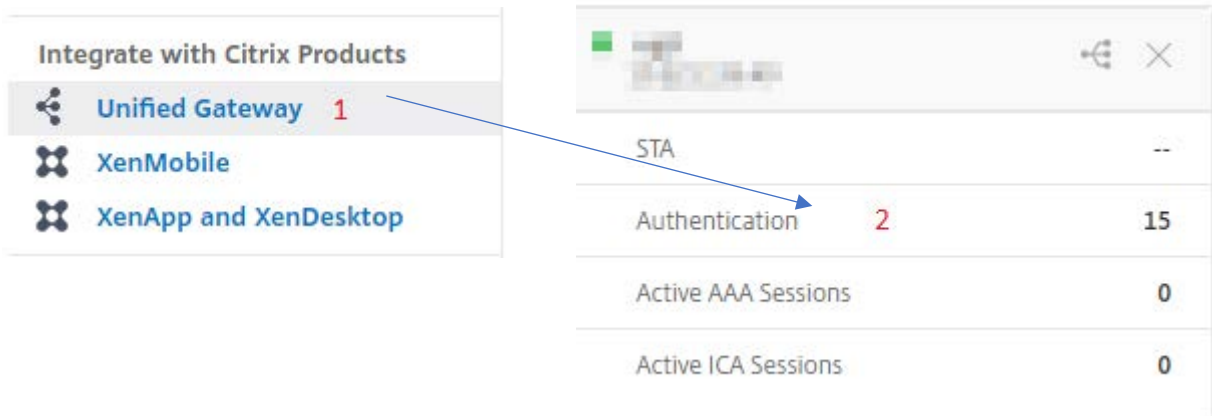
AWS Console Configuration

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.



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

Application

Choose Type*

Web Application
Select to provide access to Enterprise applications.

SaaS
Select to provide access to SaaS applications.

XenApp & XenDesktop
Select to provide access to hosted virtual resources.

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

Choose from Catalog*

Office 365

Office 365

Salesforce

Sharefile

AWS Console

G Suite

Slack

Workday

Concur

Dropbox

15Five

Workplace

Sumo Logic

Mango Apps

Expensify

Tableau

Freshdesk

Freshservice

Box

Mingle

Zoho

AWS Console

5. Fill the application template with appropriate values.

Name

AWS Console

Comments

AWS Console ?

Icon URL*

Choose File /var/netScaler/logon/AWS_icon.png



Service Provider Login URL*

https://console.aws.amazon.com/co

Service Provider ID*

1

https://signin.aws.amazon.com/sam

IDP Certificate Name*

2

Issuer Name

3

UG_VPN_AWS

Attribute1

4

https://aws.amazon.com/SAML/Attr

Attribute1 Expression

5

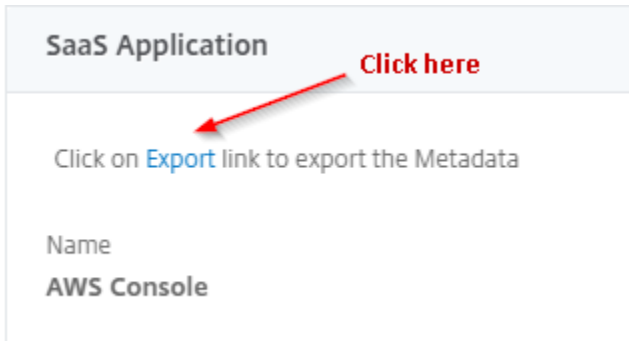
6. You must update the fields in NetScaler with the following values

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]

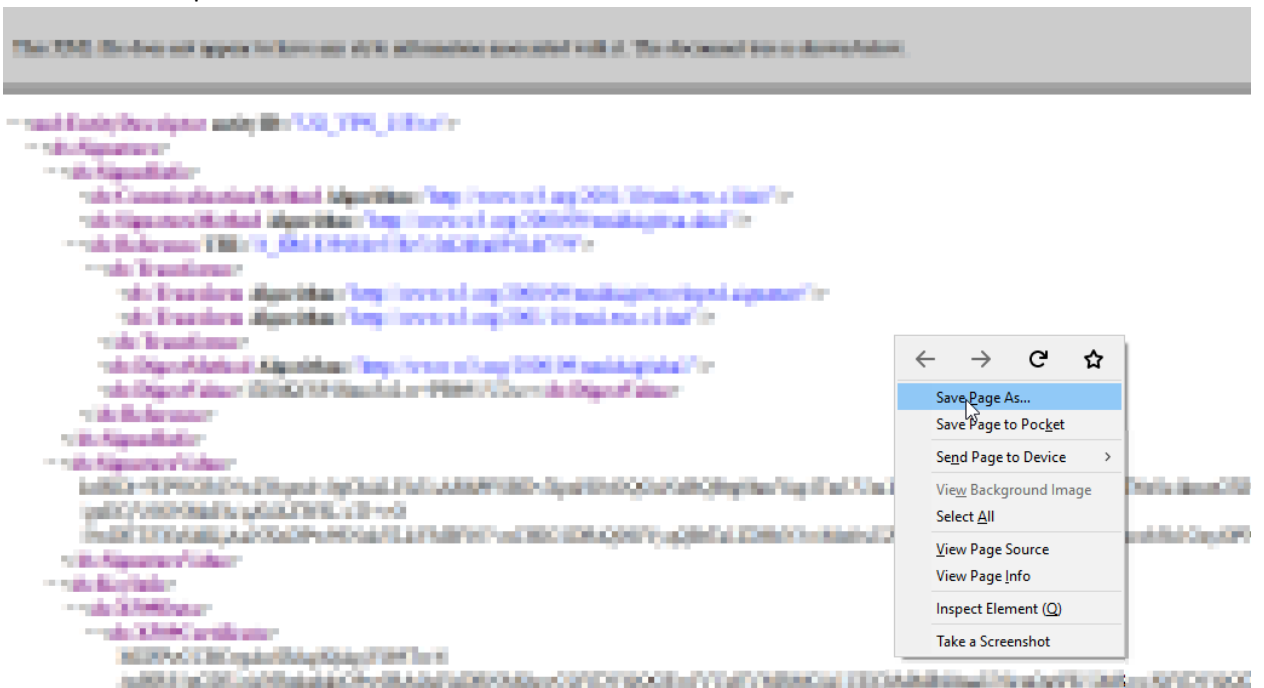
7. After providing the required values, click **Continue**. Click **Done**.

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



Root user sign in ⓘ

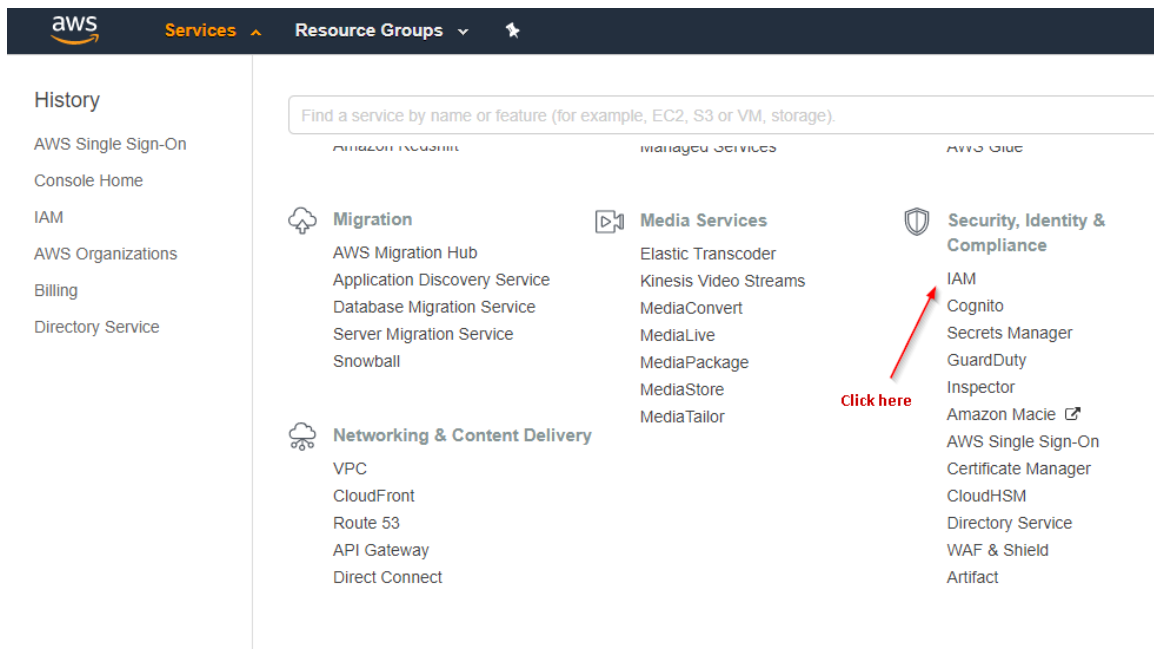
Email:

Password

[Forgot password?](#)

Sign in

1. Login to **AWS Console**.



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

Dashboard

Groups

Users

Roles

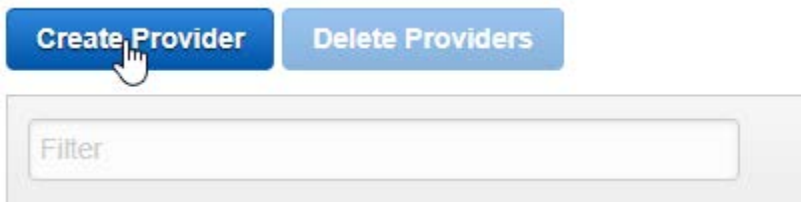
Policies

Identity providers

Account settings

Credential report

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



4. Click on **Create Provider**.

Configure Provider

Choose a provider type.

Provider Type*

Choose a provider type ▾

SAML

OpenID Connect

5. 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 [Create new provider](#) | [Refresh](#)

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










Attribute

Value*

- 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 filed 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:AttachRolePolicy	1	Allows IAM users to attach IAM policies to roles.
<input type="checkbox"/>	 iam:AttachUserPolicy	1	Allows IAM users to attach IAM policies to users.
<input type="checkbox"/>	 iam:CreatePolicyVersion	1	Provides IAM users to create IAM policy versions.
<input type="checkbox"/>	 iam:DeletePolicyVersion	1	Provides IAM users to delete IAM policy versions.
<input type="checkbox"/>	 iam:DeleteRolePolicy	1	Provides IAM users to delete IAM role policies.
<input type="checkbox"/>	 iam:DeleteUserPolicy	1	Provides IAM users to delete IAM user policies.
<input type="checkbox"/>	 iam:DetachRolePolicy	1	Provides IAM users to detach IAM policies from roles.
<input type="checkbox"/>	 iam:DetachUserPolicy	1	Provides IAM users to detach IAM policies from users.

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
<input type="checkbox"/> Administrator Click here		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. [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.