# How to Configure SAML 2.0 for AWS Single Sign-on

## Contents

- Supported Features
- <u>Configuration Steps</u>
- Notes

## Supported Features

The Okta/AWS Single Sign-on SAML integration currently supports the following features:

- SP-initiated SSO
- IdP-initiated SSO

For more information on the listed features, visit the Okta Glossary.

# **Configuration Steps**

- 1 Log in to the AWS Management Console.
- 2 Navigate to Security, Identity, & Compliance > AWS Single Sign-On:

Compute	×	Developer Tools	69	Machine Learning	<b>L</b>	Mobile
EC2		CodeStar		Amazon SageMaker		AWS Amplify
Lightsail 🛂		CodeCommit		Amazon CodeGuru		Mobile Hub
ECR		CodeBuild		Amazon Comprehend		AWS AppSync
ECS		CodeDeploy		Amazon Forecast		Device Farm
EKS		CodePipeline		Amazon Fraud Detector		
Lambda		Cloud9		Amazon Kendra	5M2	AR & VR
Batch		X-Ray		Amazon Lex	613	Amazon Sumerian
Elastic Beanstalk				Amazon Machine Learning		Amazon Sumerian
Serverless Application Repository	6	Customer Enablement		Amazon Personalize		
AWS Outposts	0	AWS IQ		Amazon Polly	98) 1	Application Integrat
EC2 Image Builder		Support		Amazon Rekognition		Step Functions
		Managed Services		Amazon Textract		Amazon EventBridge
🕾 Storage		Managed Services		Amazon Transcribe		Amazon MQ
S3				Amazon Translate		Simple Notification Se
EFS	õ	Robotics		AWS DeepLens		Simple Queue Service
FSx		AWS RoboMaker		AWS DeepRacer		SWF
S3 Glacier				Amazon Augmented Al		
Storage Gateway	000	Blockchain			æ	Customer Engageme
AWS Backup		Amazon Managed Blockchain	<b>a</b>	Analytics		Amazon Connect
Амуз Васкир			<u> </u>	Athena		Pinpoint
				EMR		Simple Email Service
Database	đ	Satellite		EMR CloudSearch		Simple email service
RDS		Ground Station				
DynamoDB				Elasticsearch Service	Æ	Business Application
ElastiCache	833	Quantum Technologies		Kinesis		Alexa for Business
Neptune	-0-	Amazon Braket		QuickSight 🖸		Amazon Chime 🛂
Amazon Redshift				Data Pipeline		WorkMail
Amazon QLDB	.191			AWS Data Exchange		
Amazon DocumentDB		Management & Governance		AWS Glue	6	End User Computing
Managed Cassandra Service		AWS Organizations		AWS Lake Formation		WorkSpaces
		CloudWatch		MSK		AppStream 2.0
Migration & Transfer		AWS Auto Scaling				WorkDocs
AWS Migration Hub		CloudFormation	Ū	Security, Identity, & Compliance		WorkLink
		CloudTrail		IAM		
Application Discovery Service Database Migration Service		Config		Resource Access Manager		
-		OpsWorks		Cognito	Ð	Internet of Things
Server Migration Service AWS Transfer for SFTP		Service Catalog		Secrets Manager		IoT Core
Snowball		Systems Manager		GuardDuty		Amazon FreeRTOS
		AWS AppConfig		Inspector		IoT 1-Click
DataSync		Trusted Advisor		Amazon Macie 🔀		IoT Analytics
		Control Tower		AWS Single Sign-On		IoT Device Defender
💭 Networking & Content Delivery		AWS License Manager		Certificate Manager		IoT Device Managemen
VPC		AWS Well-Architected Tool		Key Management Service		IoT Events

#### 3 Click Enable AWS SSO:



Dashboard AWS accounts Applications	Welcome to AWS Single Sign-On     AWS Single Sign-On (SSO) enables you to manage SSO access to your AWS accounts, resources, and cloud applications centrally, for users from your     preferred identity source. Learn more
Users Groups Settings	You successfully enabled AWS SSO To get started, go to the Users page and add your users, or use the Settings page to choose a different identity source. After setting up your identity source, you can manage permissions to your AWS accounts, roles, and cloud applications.
	Recommended setup steps
	Choose your identity source     The identity source is where you administer users and groups, and is the service that authenticates your users.     Manage SSO access to your AWS accounts
	2 Manage SSO access to your AWS accounts Give your users and groups access to specific AWS accounts and roles within your AWS organization.
	3 Manage SSO access to your cloud applications Give your users and groups access to your cloud applications and any SAML 2.0-based custom applications.
	User portal
	The user portal offers a single place to access all their assigned AWS accounts, roles, and applications. User portal URL: https://awsapps.com/start   Customize

#### 5 Under Identity source, select Change:

Dashboard	AWS SSO > Settings		
AWS accounts	Settings		
Applications			
Users	Identity source		
Groups	Your identity source is where you administer your users and groups, and where AWS SSO authenticates your users. You can choose between AWS SSO, SAML 2.0-compatible identity provider (IdP), or Active Directory (AD). Learn more		
Settings	Identity source AWS SSO   Change		
	Authentication AWS SSO		
	Provisioning 🕢 AWS SSO		
	User portal		
	The user portal is a central place where your users can see and access their assigned AWS accounts, roles, and applications. Share this URL with your users to get them started with AWS SSO.		
	User portal URL https://c awsapps.com/start		
	Customize		
	Multifactor authentication		
	Define the behavior you want to enforce to secure user portal access with multi-factor authentication. You register multi-factor authentication devices for users through the Users page. Learn more		
	Prompt users for multi-factor authentication (MFA) Only when their sign-in context changes (context-aware)		
	When prompted for a MFA code Users can authenticate with an app on their device		
	If user does not have a registered MFA device Allow them to sign in		
	Who can manage MFA devices Users and administrators can add and manage MFA devices		
	Configure		
	AWS SSO-integrated applications		
	Enable AWS SSO for use with AWS SSO integrated applications that authenticate with and can access user and group information from AWS SSO. Learn more		
	Status Enabled in member accounts		

- 6 Enter the following:
  - Select External identity provider.
  - Click Show individual metadata values.

Change identity source 1 2				
Choose where your identities are sourced Choose directory Review				
Your identity source is the place where you administer and authenticate identities. You use AWS SSO to manage permissions for identities from your identity source to access AWS accounts, roles, and applications. Learn more				
<ul> <li>AWS SSO</li> <li>You will administer all users, groups, credentials, and multi-factor authentication assignments in AWS SSO. Users sign in through the AWS SSO user portage</li> </ul>	tal.			
Active Directory You will administer all users, groups, and credentials in AWS Managed Microsoft AD, or you can connect AWS SSO to your existing Active Directory using AWS Managed Microsoft AD or AD Connector. Users sign in through the AWS user portal.				
External identity provider You will administer all users, groups, credentials, and multi-factor authentication in an external identity provider (IdP). Users sign in through your IdP sign-in page to access the AWS SSO user portal, assigned accounts, roles, and applications.				
Configure external identity provider AWS SSO works as a SAML 2.0 compliant service provider to your external identity provider (IdP). To configure your IdP as your AWS SSO identity source you must establish a SAML trust relationship by exchanging meta data between your IdP and AWS SSO. While AWS SSO will use your IdP to authenticate users, the users must first be provisioned into AWS SSO before you can assign permissions to AWS accounts and resources. You can either provision use manually from the Users page, or by using the automatic provisioning option in the Settings page after you complete this wizard. Learn more Service provider metadata	te			
Your IdP requires the following AWS SSO certificate and metadata details to trust AWS SSO as a service provider. You may copy and paste, or type this information into your IdP's service provider configuration interface, or you may download the AWS SSO metadata file and upload it into your IdP.				
AWS SSO SAML metadata Download metadata file				
Show individual metadata values				
Identity provider metatdata				
AWS requires specific metadata provided by your IdP to establish trust. You may copy and paste from your IdP, type the metadata in manually, or upload metadata exchange file that you download from your IdP.	a			
IdP SAML metadata* Browse				
If you don't have a metadata file, you can manually type your metadata values				
Cancel Next: Revie	ew			

- Make a copy of the AWS SSO Sign-in URL, AWS SSO ACS URL, and AWS SSO issuer URL values. These values will be used later on.
- IdP SAML metadata: Save the following file as metadata.xml, then upload it into AWS.

Individual data will be generated here

• Click Next: Review.

**Important**: Changing your source to or from Active Directory removes all existing user and group assignments. You must manually reapply assignments after you have successfully changed your source.

External identity provider		
	entials, and multi-factor authentication in an external identity prov	ider (IdP). Users sign in through your IdP sian-in
	assigned accounts, roles, and applications.	
Configure external identity	provider	
you must establish a SAML trust relations users, the users must first be provisioned	It service provider to your external identity provider (IdP). To config hip by exchanging meta data between your IdP and AWS SSO. W into AWS SSO before you can assign permissions to AWS accou g the automatic provisioning option in the Settings page after you	Thile AWS SSO will use your IdP to authenticate nts and resources. You can either provision users
Service provider metadata		
	certificate and metadata details to trust AWS SSO as a service pr er configuration interface, or you may download the AWS SSO me	
AWS SSO SAML metadata	Download metadata file	
AWS SSO Sign-in URL	https:// .awsapps.com/start	42
AWS SSO ACS URL	https://us-east-2.signin.aws.amazon.com/platform/saml/acs.	ළු
AWS SSO issuer URL	https://us-east-2.signin.aws.amazon.com/platform/saml/	43
	Hide individual metadata values	
Identity provider metatdata		
AWS requires specific metadata provideo metadata exchange file that you downloa	by your IdP to establish trust. You may copy and paste from your d from your IdP.	IdP, type the metadata in manually, or upload a
IdP SAML metadata*	metadata_amazon_aws_sso.xml Browse	
	If you don't have a metadata file, you can manually type your me	tadata values
		Cancel Next: Review

7 Review the list of changes. Once you are ready to proceed, type **CONFIRM**, then click Change identity source.

## Change identity source

# Choose directory Review

### Review and confirm

#### A Review list of changes

You are changing your source of identity to use an external identity provider. Please review the list of changes

- · You must complete the SAML federation between AWS SSO and your IdP for your users to be able to federation in.
- AWS SSO will preserve your existing users and assignments.
- Existing users in AWS SSO that are not in IdP will be retained in AWS SSO, but will be unable to sign in to AWS SSO. You may add these
  users in the IdP or may remove the user from AWS SSO.
- · Users from IdP that do not exist in AWS SSO will be provisioned in AWS SSO.
- You must configure provisioning via SCIM to auto provision your users from IdP to AWS SSO. Alternatively, you may manually provision
  users in AWS SSO without SCIM.
- With SCIM enabled, Your IdP will be authoritative source of identity. You may only provision new user or edit existing user attributes in your IdP.
- All existing MFA configurations will be deleted when customer switches from AWS SSO to IdP. MFA policy controls will be managed on IdP.
- With SCIM disabled, you can provision new users and/or edit existing users in AWS SSO. User Email Id must match in AWS SSO and your IdP in order for user to be able to sign in to AWS SSO.

Type "CONFIRM" to confirm changing the identity source

CONFIRM		
	Cancel	Previous Change identity source

- 8 In Okta select the Sign On tab for the AWS Single Sign-On SAML app, then click Edit:
  - Enter your AWS SSO ACS URL and AWS SSO issuer URL values you made a copy of in step 6 into the corresponding fields.
  - Application username format: Select one of the options from the dropdown menu.

Note: All users in AWS SSO require a unique username, so the mapped value should be unique within your organization.

Click Save:

Seneral	Sign On	Mobile	Import	Assignments
Settings				Can
The sign on metho	ods require add	itional configu	ration in the 3	o and manages their credentials for an application. Some sign d party application. lie mapping. <b>Configure profile mapping</b>
0 S	AML 2.0 is the o	only sign-on op	otion currently	supported for this application.
⊛ SAJ	ML 2.0			
	Default Relay S	tate	All IDP-in	tieted requests will include this ReleyState.
	Disable Force A	Authentication		ampt user to re-authenticate.
⊜	View Set.	p Instructions		nplete the setup instructions. this application supports dynamic configuration.
	CED SIGN-ON		'S Single Sign-	on proprietary sign-on option or general setting.
AWS SS	D ACS URL		Enter y	/us-east-2.signin.aws.amazon.com/platform/samt our AWS SSO ACS URL. Refer to the Setup Instructions above in this value.
AWS SS	D issuer URL			//us-east-2.signin.aws.amazon.com/platform/sami/acs
				our AWS SSO issuer URL. Refer to the Setup Instructions abov in this value.
CREDEN	ITIALS DETAIL	S		

9 Done!

## SP-initiated SSO

Go to the AWS SSO Sign-in URL you made a copy of in step 6.