

Access Cisco Global Launchpad

- Access Hosted Cisco Global Launchpad, on page 1
- Log In to the Cisco Launchpad, on page 5
- Log Out, on page 17

Access Hosted Cisco Global Launchpad

You can access Cisco Global Launchpad with Cisco DNA Portal.

If you are new to Cisco DNA Portal, you must create a Cisco account and a Cisco DNA Portal account. Then you can log in to Cisco DNA Portal to access Cisco Global Launchpad.

If you are familiar with Cisco DNA Portal and have a Cisco account and a Cisco DNA Portal account, you can directly log in to Cisco DNA Portal to access Cisco Global Launchpad.

Create a Cisco Account

To access Cisco Global Launchpad through the Cisco DNA Portal, you first must create a Cisco account.

Step 1 In your browser, enter:

dna.cisco.com

The Cisco DNA Portal login window is displayed.



- Step 2 Click Create a new account.
- Step 3 On the Cisco DNA Portal Welcome window, click Create a Cisco account.
- Step 4 On the Create Account window, complete the required fields and then click Register.
- **Step 5** Verify your account by going to the email that you assigned to your account and clicking Activate Account.

Hi and	
Welcome to Cisco!	
Please click the button to activate your account.	
Activate Account Expires in 7 days.	
After activating your account, you can:	
 Login with your email and password. 	
 Manage your Cisco account profile and request access to and services. 	o Cisco applications
 Become a customer by associating a contract number or account or order services directly through our global net partners. 	bill-to ID to your work of certified
 Become a partner by associating your account with a par register your company as a partner. 	tner company or
• Access supply chain tools and resources.	
Visit help for login, password, and account information. Contact support for help accessing your account.	

Create a Cisco DNA Portal Account

To access Cisco Global Launchpad through the Cisco DNA Portal, you must create a Cisco DNA Portal account.

Before you begin

Make sure that you have a Cisco account. For more information, see Create a Cisco Account, on page 1.

Step 1 In your browser, enter:

dna.cisco.com

The Cisco DNA Portal login window is displayed.



- Step 2 Click Log In With Cisco.
- **Step 3** Enter your Cisco account email in the **Email** field, and click **Next**.
- **Step 4** Enter your Cisco account password in the **Password** field, and click **Log in**.
- **Step 5** On the **Cisco DNA Portal Welcome** window, enter the name of your organization or team in the **Name your account** field. Then click **Continue**.
- Step 6 On the Cisco DNA Portal Confirm CCO Profile window, do the following:
 - a) Verify that the details are correct.
 - b) After reading, acknowledging, and agreeing with the conditions, check the check box.
 - c) Click Create Account.

After successfully creating an account, the Cisco DNA Portal home page is displayed.

Subscribe offers moi Cisco Select an offer b Cis	and maintain your re efficiently with DNA Portal. elow and enjoy your trip with cc DNA Portal.			
fers	Cisco DNA Center Cloud	SAN Insights Discovery	Plun and Play as a Service	pxGrid Cloud
Applications Experience enables Cisco DNA Conter users to integrate with ApX cloud service to collect quality matrices and to emich Cisco DNA Center application databased to get better visibility on the network.	Claco DNA Centre Cloud provides complete, cloud-based lifecycle management of Claco Catalyst \$300, 500, and \$500 Sense Access Privation in Enhanded Wireles Centroller (EVIC) mode. Network administrators can manage three wirel and wireless network infrastructure at the site- leved using a secure cloud sate interface.	SAM Insights Discovery as a Saa's offering on DNAC Cloud. This is much-awaited pre- sales tool for Choos Sales, Account Iwan and check of any schemer SAM Iabics. Silo works for existing Brocade and Cloue SAM Tabrics. SID helps the Close to that the customer has and how Class can help moving forward.	Plag and r. ky as derived Plag and bay as service enables users to securely dy-oriented Catalyst SR family of devices. During onbearding success you can be device. An enablesting system endered the device to be managed by DNA controller.	Disco pakrid Chold enables users to securely share contexts between on-premise Cisco ISE and cloud based applications. It is defined to the secure of the secure data is shared. It is included as part of your Cisco ISE Advantage license.
Subscribe	Subscribe	Subscribe	Subscribe	Subscribe

Log In to the Cisco DNA Portal with Cisco

To access Cisco Global Launchpad through the Cisco DNA Portal, you must log in to the Cisco DNA Portal.

Before you begin

Make sure that you have a Cisco account and a Cisco DNA Portal account. For more information, see Create a Cisco Account, on page 1 and Create a Cisco DNA Portal Account, on page 2.

Step 1 In your browser, enter:

dna.cisco.com

The Cisco DNA Portal login window is displayed.



Step 2 Click Log In With Cisco.

- **Step 3** Enter your Cisco account email in the **Email** field, and click **Next**.
- Step 4 Enter your Cisco account password in the Password field, and click Log in.

If you only have one Cisco DNA Portal account, the Cisco DNA Portal home page displays.

Step 5 (Optional) If you have multiple Cisco DNA Portal accounts, choose the account that you want to log in to by clicking the Continue button next to the account.

The Cisco DNA Portal home page is displayed.



Log In to the Cisco Launchpad

The Cisco Global Launchpad supports the following authentication methods:

- Log In Using IAM, on page 6: This method uses the credentials from your Cisco account.
- Log In Using Federated Identity, on page 8: Federated access ensures that an identity provider (IdP), such as your organization, is responsible for user authentication and sending information to Cisco Global Launchpad to help determine the scope of resource access to be granted after login. For the first-time login, the user will have an admin user role, which creates the CiscoDNACenter role. The admin can assign this role to subsequent users. The CiscoDNACenter role has the same permissions as the CiscoDNACenter user group. For details about the permissions granted by this role, see the *Cisco DNA Center on AWS Deployment Guide*.

You can use the saml2aws CLI or the AWS CLI to generate tokens to log in to Cisco Global Launchpad as a federated user. For information, see the following topics:

- Generate Federated User Credentials Using saml2aws, on page 11
- Generate Federated User Credential Using AWS CLI, on page 12



Note

Cisco Global Launchpad does not store your AWS credentials.

Log In Using IAM

This procedure shows you how to log in to Cisco Global Launchpad using identity and access management (IAM). If your company uses MFA, you can choose to log in using this method.



Note Do not open the application in more than one browser tab, in multiple browser windows, or in multiple browser applications at the same time.

Before you begin

Make sure the following requirements are met:

- Your AWS account has the administrator access permission assigned to it.
- Cisco Global Launchpad is installed or you have access to the hosted Cisco Global Launchpad.
- You have your AWS Access Key ID and Secret Access Key on hand.
- If your company uses multi-factor authentication (MFA), MFA needs to be set up in AWS before you log in. For information, see the Enabling a virtual multi-factor authentication (MFA) device (console) topic in the AWS documentation.

Step 1 From a browser window, do one of the following:

• If you installed Cisco Global Launchpad locally, enter the Cisco Global Launchpad URL in the following format:

http://<localhost>:<client-port-number>/valaunchpad

For example:

http://192.0.2.1:90/valaunchpad

• If you are accessing the hosted Cisco Global Launchpad, enter **dna**.**cisco**.**com** and follow the on-screen prompts to log in. (For information, see Log In to the Cisco DNA Portal with Cisco, on page 4.)

From the Cisco DNA Portal home page, click the menu icon and choose VA Launchpad (Beta).



The AWS login window is displayed.

allalla cisco	aws
Global Launchpad	(a) IAM Login (Construction) (Construc
AWS Access	Secret Access Key ①
Enter the AWS details to connect to your AWS account.	Secret Access Key
O teengina accordinas O contralacidater	Use MFA authentication ① Authenticate

- Step 2 Under the AWS logo, click the IAM Login radio button.
- **Step 3** Enter your credentials in the fields.

For information about how to get an Access Key ID and Secret Access Key, see the AWS Managing access keys topic in the AWS Identity and Access Management User Guide on the AWS website.

- Step 4 (Optional) If your company uses MFA, click the Use MFA authentication check box.
- Step 5 Click Authenticate.

If you are logging in with MFA, choose your MFA device from the drop-down list and enter your MFA passcode. After logging in successfully, the **Dashboard** pane is displayed and the us-east-1 region is selected by default.

Step 6 If you're prompted to update the region version, follow the prompts to complete the update. For more information, see Update a Region.

Global Launchpad	Dashboard	
OS9356112352 >	The following regions have the region setup configured but don't contain any VA pods. Choose which regions you want to remove the region setup from: ev-west-1 ev-west-2 ev-west-3 ev-central-1 ev-south-1 NOTE: The region setup is automatically created when you create a new VA pod. former New Do It Later	
Sign VA Monitoring â₂ User Activities Strings O Help Center		Regions 📕 Pod Failed
	Q. Search Status v	C Refresh + Add VA pod

Step 7 If you encounter any login errors, you need to resolve them and log in again.

Log In Using Federated Identity

This procedure shows you how to log in to Cisco Global Launchpad using a federated identity.

Ŵ

Note Do not open the application in more than one browser tab, in multiple browser windows, or in multiple browser applications at the same time.

Before you begin

Make sure the following requirements are met:

- Your AWS account has the administrator access permission assigned to it. For information, the Cisco DNA Center on AWS Deployment Guide.
- Cisco Global Launchpad is installed or you have access to the hosted Cisco Global Launchpad.
- You have your AWS Account ID, Access Key ID, and Secret Access Key on hand. For information about how to obtain these credentials, see Generate Federated User Credentials Using saml2aws, on page 11 or Generate Federated User Credential Using AWS CLI, on page 12.

Step 1 From a browser window, do one of the following:

• If you installed Cisco Global Launchpad locally, enter the Cisco Global Launchpad URL in the following format:

http://<localhost>:<client-port-number>/valaunchpad

For example:

http://192.0.2.1:90/valaunchpad

• If you are accessing the hosted Cisco Global Launchpad, enter **dna**.**cisco**.**com** and follow the on-screen prompts to log in. (For more information, see Log In to the Cisco DNA Portal with Cisco, on page 4.)

From the Cisco DNA Portal home page, click the menu icon and choose VA Launchpad (Beta).

uludu DNA Portal		Cloud Subscriptions	/ Cisco DNA - Cloud
 ☐ Home ☑ VA Launchpad (Beta) ☑ Workflows △ Users and Accounts 	ibe and maintain your more efficiently with sco DNA Portal. ^{offer below and enjoy your trip with Cisco DNA Portal.}		
	Subscribe	Subscribe	Subscribe

The AWS login window is displayed.



- **Step 2** Under the AWS logo, click the **Federated Login** radio button.
- **Step 3** Enter your credentials in the fields.

For more information, see Generate Federated User Credentials Using saml2aws, on page 11 or Generate Federated User Credential Using AWS CLI, on page 12.

Step 4 Click Authenticate.

After you log in successfully, the **Dashboard** pane is displayed and the us-east-1 region is selected by default.

Step 5 If you're prompted to update the region version, follow the prompts to complete the update. For more information, see Update a Region.



Step 6 If you encounter any login errors, you need to resolve them and log in again. For more information, see the *Cisco DNA Center on AWS Deployment Guide*.

Generate Federated User Credentials Using saml2aws

You can generate temporary AWS credentials using a Command Line Interface (CLI) tool and use the generated credentials to log in to Cisco Global Launchpad.

- **Step 1** From the CLI, install saml2aws. For information, see the detailed instructions on Github.
- **Step 2** Verify the installation by entering **saml2aws**.

If the installation is successful, the following output is displayed:

```
~ % saml2aws
usage: saml2aws [<flags>] <command> [<args> ...]
A command line tool to help with SAML access to the AWS token service.
Flags:
      --help
                               Show context-sensitive help (also try --help-long
                               and --help-man).
      --version
                              Show application version.
     --verbose
                               Enable verbose logging
      --quiet
                               silences logs
 -i, --provider=PROVIDER
                              This flag is obsolete. See:
                               https://github.com/Versent/saml2aws#configuring-i
dp-accounts
     --config=CONFIG
                               Path/filename of saml2aws config file (env:
                               SAML2AWS_CONFIGFILE)
  -a, --idp-account="default"
                              The name of the configured IDP account. (env:
                               SAML2AWS_IDP_ACCOUNT)
      --idp-provider=IDP-PROVIDER
                               The configured IDP provider. (env:
                               SAML2AWS_IDP_PROVIDER)
                               The name of the mfa. (env: SAML2AWS_MFA)
      --mfa=MFA
  -s, --skip-verify
                               Skip verification of server certificate. (env:
```

Step 3 Configure your account.

- a) Enter saml2aws configure.
- b) At the Please choose a provider prompt, use the up- or down-arrow keys to choose a provider or enter the provider name. When done, press Enter.
- c) At the AWS Profile prompt, press Enter to use the default AWS profile.
- d) At the URL prompt, enter the URL of your identity provider (IdP) and press Enter.

Note You can get this information from your IdP.

- e) At the prompts, enter your username and password and press Enter.
- **Step 4** Generate your federated credentials.
 - a) Enter saml2aws login.
 - b) At the prompts, enter your username and password.
 - c) At the prompt, select either the Admin or CiscoDNACenter role and press Enter.

Note Ensure that the tokens created for these roles have a minimum expiry of 180 minutes (3 hours).

Your credentials are generated and stored in ~/aws/credentials.

- **Step 5** Download the credentials by entering saml2aws script.
- **Step 6** Note the values of the following parameters as you will use them to log in to Cisco Global Launchpad as a federated user:
 - AWS_ACCESS_KEY_ID
 - AWS_SECRET_ACCESS_KEY
 - AWS_SESSION_TOKEN
- **Step 7** On the Cisco Global Launchpad login window, select **Federated Login** and enter the generated credentials in the corresponding fields.

، ۱ ۱ ، ۱ ۱ ، CISCO Global Launchpad	MM Login Perferated Login Access Key 10 © Tacess Key 10 ©
AWS Access	Secret Access Key ①
	Secret Access Key
Enter the AWS details to connect to your AWS account.	Session Token
O Managing access keys	Session Token
Cost Calculator	Authenticate

Generate Federated User Credential Using AWS CLI

You can generate temporary AWS credentials using the AWS Command Line Interface (CLI) and use these credentials to log in to Cisco Global Launchpad.

- Step 1 In a browser window, navigate to the AWS Single Sign On (SSO)/Active Directory (AD) window.
- Step 2 In the AWS Single Sign On (SSO)/Active Directory (AD) window, click the AWS Console link.

The following window is displayed.

Select a role:		
 Account: 		
⊖ devops		
- Account:		
O dflyreadonly		
+ Account:		
O dflyreadonly		
🔿 val		
✓ Account:		
⊖ admin		

Step 3 Right-click anywhere in the window, and from the drop-down menu, choose **Inspect Element** or **Inspect** (depending on the browser).

Note You can also press the F12 key to open the Developer Tools panel.

The Developer Tools panel is displayed, similar to the following window.

aws		🖟 🔂 Elements Console Sources Network » 📮1 🌣 :
und a		🥌 🔕 🦞 Q, 🗌 Preserve log 🗌 Disable cache Nic throttling 💌 🐾 🛛
		Do not clear log on page reload / navigation
	Select a role:	Filor Hide data UFLs
	 Account: 	Has blocked cookies. Blocked Requests 3rd-party requests
	() devons	Use large request rows Group by frame
	() the	2 Show overview Capture screenshots
	 Account: 	2000 ma 4000 ma 8000 ma 10000 ma 10000 ma 12000 ma 14000 ma
	O dflyreadonly	
	• Account:	Name Sta Type Initiator Size Ti Waterfall 4
	O dtlyreadonty	
	🔿 val	
	✓ Account:	
	🔘 admin	
	Sign in	
	English v	
	Terms of Line Privacy Policy © 1996-2003, Arrazon Web Services, Inc. or its affliates.	
		D / 10 requests 0 B / 13.7 kB transferred 0 B / 130 kB resources
] Console What's New ×
		Highlights from the Chrome 110 update
		Recorder panel updates View and highlight the code of your user frow instantly, and more.
		Improved syntax higlights new

- **Step 4** In the **Developer Tools** panel, click the **Network** tab and check the **Preserve Log** check box. (This option can be found on the tool panel, right beside the Magnifying Glass icon.)
- Step 5 In the AWS Console, click Sign In.
- **Step 6** In the **Developer Tools** panel, filter the required API calls by entering **saml** in the **Filter** field.

aws III Services	Q. Search	[Option+S] 🗗 🗘 🕐 Tokyo 🕶 💻	•	G E	Elements Co	nsole Netw	ork »	cache 1	01		* : ×
🔝 Lambda 🛛 🔯 CloudFo	mation 📈 EC2			± ±		nerve ng 1 c) cosesie	Gaurie	10 11101	- M	·• •
	Console Home Info	Reset to default layout + Add widge	*	sami All Fetc	N/XHR JS CSS k	Invert Invert	Hide da	ta URLs WS Wat	sm Mai	nifest Oth	ar
	Recently visited Info			Use la	locked cookies	Nocked Reque	sts 🗌 3	rd-party r	equests ame		
				Show	overview		00	spture scr	eenshot	5	
	CloudWatch	VPC		2000 r	ns 4000 ms	6000 ms 8	000 ms	10000 mm	12	000 ms	14000 ms
	CloudFormation	EC2 Image Builder					ALTERNA.				
	S3	A Lambda		Namo		Status	Туре	Initiator	S 1	ime Wate	rfall A
	AWS Organizations	Amazon EventBridge		🗐 sami		302	doc	Other	4		
	Systems Manager				nothe Steldan www.	mazon.com/kam					
	IAM Identity Center (successor to AWS Single	-									
	2 EC2										
	Viev	v all services									
	Welcome to AWS	# AWS Health Info									
	Getting started with AWS C Learn the fundamentals and find valuable information to get the most out of AWS.										
	Training and certification	-									

Step 7 Click the API request named **saml**.

Step 8 Click the Payload tab.

The saml API response is displayed under the Form Data tab.

aws III Services Q. Search	[Option+5] 🕨 🗘 🗇 Tokyo 🕶	😯 🔂 Elements Console Network » 💽 1 🛦 1 📮 1 🌣 🚦 🗙
Kamibda 📓 CloudFormation 📓 EC2	and the second	Q Q Q Preserve log Disable cache No throttling * %
Console Home Infe	Reset to default layout + Add widgets	semi faction factor
Recently visited Into	1	Use targe request rows Group by frame
CloudWatch CloudFormation S 53 AVIS Organizations S Systems Manager	VPC EC2 Image Builder Lambca Amazon EventBridge	1000 of the first fill 2000 m
MM Identity Center (successor to AWS Single EC2	I. services	The series is a series and the series and the series of the series and the series of t
Welcome to AWS :	AWS Health Info :	2/TOROUGHINGTO 2/YE RESUME 22/YE CASED (TOTALING SUCCESSION AND AND AND AND AND AND AND AND AND AN
Getting started with AWS [2] Learn the fundamentals and find valuable	Open issues O Past 7 days	341221+X2-wkke/c280/011+Y280/014+C2014011+Y280/014+C20140120411c2414 (c) 448 DMMU2 nbm?bbx3117m1532/04424532/04424532/044245320482420422716325927921630040 3h156642a4c11140274063244421444044546404424544042516452597271630040 vbx31/0402/2016/044444444444444444444444444444444444
Training and certification [2]	Scheduled changes 4 Upcoming and past 7 days	TAVEGISLAVI AVYSI JAHTALI SI VP JAKES PERMANERI OM AZZRADZO JAKONE polici MPS Josebno SI VIZICALI, na z la kry z vytyka kr. z ANJ, hrvatska v Azdrov Silvy ZZPE czestwi Juži z Jak Police SI Jakone SI Vetra Jakone SI Vetra Torolow VIEL V ENIX ZZPI MPK CE I kr. accolarate Zzenicke Z Polici Torolow VIEL V ENIX ZZPI MPK CE I kr. accolarate Zzenicke Z Polici SI Vetra ZZPI VETRI ZZPI MPK CE I kr. accolarate Zzenicke Z Polici SI Vetra ZZPI VETRI ZZPI VETRI ZZPI VETRI ZZPI ZZPI ZZPI ZZPI ZZPI ZZPI ZZPI ZZ
Feedback Language	Others not Rentificant 0 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Coolide prefe	ances 1/223 requests to an

Step 9 Copy the value of the SAML response.

Note Be sure to copy the entire value, but do not copy the SAMLResponse field name.

Step 10 Navigate to your AWS Console, choose IAM > Access Management > Identity Providers, and select your IdP.

Identity and Access X Management (IAM)	IAM > Identity providers		
Q, Search IAM Dashboard	Have you consider AWS IAM Identity O users with single si create and manage identity provider. L	red using AWS IAM Identity Center? Center ^[2] makes it easy to centrally manage aci ign-on access to all their assigned accounts fro e user identities in IAM Identity Center or easily .earn more ^[2]	cess to multiple AWS accounts and provide m one place. With IAM Identity Center, you can v connect to your existing SAML 2.0 compatible
Access management Jser groups Jsers	Identity providers (Use an identity provider (k grant the user identities pe	1/5) Into dP) to manage your user identities outside of Al ermissions to use AWS resources in your accou	Delete Add provider WS, but unt.
Roles	Q. Filter Identity provide	ers by property or provider name and press ente	er (1 > ()
Policies			
dentity providers	Provider	✓ Type	✓ Creation time
ccount settings	O idp1	SAML	21 days ago
access reports	O DNACADES	SAML	10 days ago
Access analyzer	0 ide001	SAMI	18 days ago
Archive rules			10 days ago
Analyzers	O cloudsso.cisco.co	om SAML	7 months ago
Settings	O RAMANTECH	SAML	4 months ago
Credential report			
organization activity			
service control policies (SCPs)			
Related consoles			

- **Step 11** Obtain the following details for your IdP:
 - Role assigned to the IdP
 - Amazon Resource Name (ARN) of the IdP

Step 12 From the AWS CLI, enter the following command:

aws sts assume-role-with-saml --role-arn <Role-Arn> --principal-arn <IDP-Arn> --saml-assertion <SAML response>

The variables in this command refer to the values obtained earlier, as follows:

- <Role-Arn>: Role assigned to the IdP, obtained in Step 11.
- <IDP-Arn>: Amazon Resource Name (ARN) of the IdP, obtained in Step 11.
- <SAML response>: Value of the SAML response, obtained in Step 9.

For example:

```
aws sts assume-role-with-saml --role-arn
arn:aws:iam::059356109852:role/ADFS-AWS-ADMIN --principal-arn
arn:aws:iam::059356109852:saml-provider/cloudsso.cisco.com --saml-
assertion
MIIC6jCCAdKqAwIBAqIQPP5He1K6QoZPQrIuPjzCUTANBqkqhkiG9w0BAQsFADAxMS8wLQY
DVQDEyZBREZTIFNpZ25pbmcgLSBFQzJBTUFaLU1IMUYzQ0Quc3NvLmNvbTAeFw0yMzAyMDY
wNTUyNDJaFw0yNDAyMDYwNTUNDJaMDExLzAtBgNVBAMTJkFER1MgU21nbm1uZyAtIEVDMkF
NQVotTUqxRjNDRC5zc28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsl
Sx/rQJ/wA0J6ZRBbgYkfE7TMPsnOTqX0C+dh+yQ30+X9xqRDPVKuSDHrv72bsGwk/
2VRdb38xdVueuFYRavyVPzjsSF95fkjC3qFDN+R5Dk1Cnba7GT6i+HGfacEpL8Vqd3jzNgh
guskMlOrHDHKDv5ksNMxppHIDPlVhyRCdKEtP1PG5gBftoKvBZX+RxYcTaVUK/
NrMfkWmklyQTNRmpUDj+NAwGGjr4byjH8hUu59cFJetatzJo8qxuWWtPBtd+ESs/
DVR5dpilfyEBi4Dc22X91kOShJpeDu08EGfR605/nmRErlyy/p5f2sPKM0/
ix+XlQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA7kt4HeU/
zohOSDnnfmXYpYi8WrJFxMvTS6CjwE8eYZ6BwByEI4PjxcjPOu+sVNXrtBzJUwyPM+LKKMs
zYn5VQ/skrwc1jW5P4msUMj4/J5K4vuYcKbJS4VyASKVZmWUWC23WhpC3U8ft6F7Jynp/
omrEh6Xrc4f4SqFdvIz35h2Sd/
HbcDp+sHZzm4TgnA2XuSuvv0NJPf2VsRHMCMSn3eBTQfbbD5naLEpitjU8Zy5qW+Ic8Up51
ATNzPP+kmaQY6SxPLeuAarrnp4vDrD7hpzhneRfWX8h9v/Fg+w1nOsEeD1FYyLRoc
```

Output similar to the following output is displayed:

```
{
"Credentials": {
"AccessKeyId": "xxxx",
"SecretAccessKey": "xxxxx,
"Expiration": "2023-03-10T18:07:15+00:00"
},
"AssumedRoleUser": {
"AssumedRoleId": "xxx:user@sso.com",
"Arn":"arn:aws:sts::059356109852:assumed-role/ADFS-AWS-ADMIN/user@sso.com"
},
"Subject": "SSO\\USER",
"SubjectType": "transient",
"Issuer": "http://EC2AMAZ-MH1F3CD.sso.com/adfs/services/trust",
"Audience": "https://signin.aws.amazon.com/saml",
"NameQualifier": "POIUYTRFVNMKJGFKJHJJHJCYLQCePSAZg="
}
```

- **Step 13** Note the values of the following generated credentials:
 - AccessKeyId
 - SecretAccessKey
 - SessionToken
- **Step 14** On the Cisco Global Launchpad login window, select **Federated Login** and enter the generated credentials from Step 13 in the corresponding fields.



Log Out

Depending on how you accessed your Cisco Global Launchpad account, you either need to log out of only Cisco Global Launchpad or both Cisco Global Launchpad and Cisco DNA Portal.

- **Step 1** To log out of Cisco Global Launchpad, do the following:
 - **a.** In the left navigation pane, click the log out icon $(\stackrel{[]}{\vdash})$.
 - b. In the Confirmation dialog box, click Log Out.

Your progress is automatically saved when you log out.

- **Step 2** (Optional) If you accessed Cisco Global Launchpad through Cisco DNA Portal, you must also log out of Cisco DNA Portal. Do the following:
 - a) In the upper-right corner of the Cisco DNA Portal GUI, click your displayed username.
 - b) Click Log Out.

I