



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.

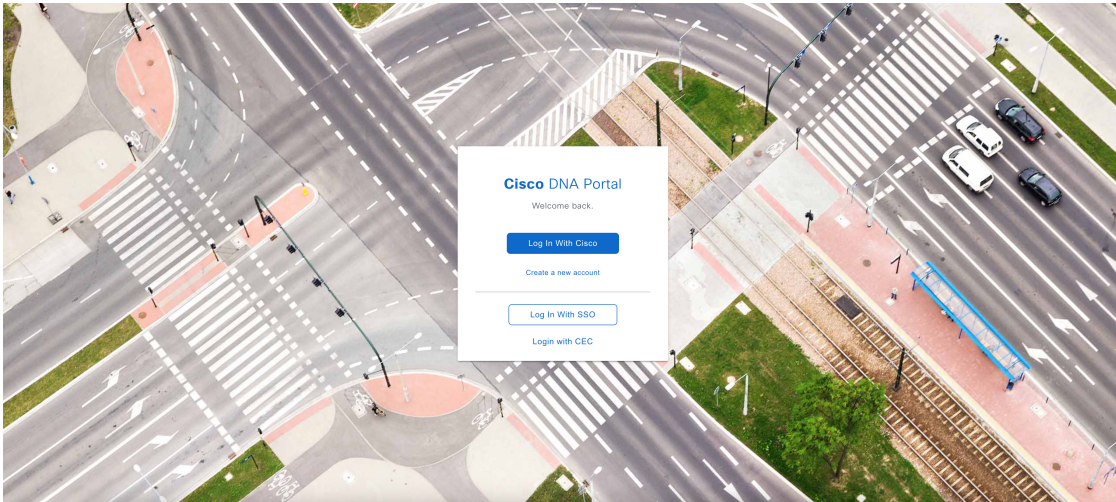
Create a Cisco Account

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 _____,

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 Cisco applications and services.
- [Become a customer](#) by associating a contract number or bill-to ID to your account or [order services](#) directly through our global network of certified partners.
- [Become a partner](#) by associating your account with a partner company or [register your company](#) as a partner.
 - 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

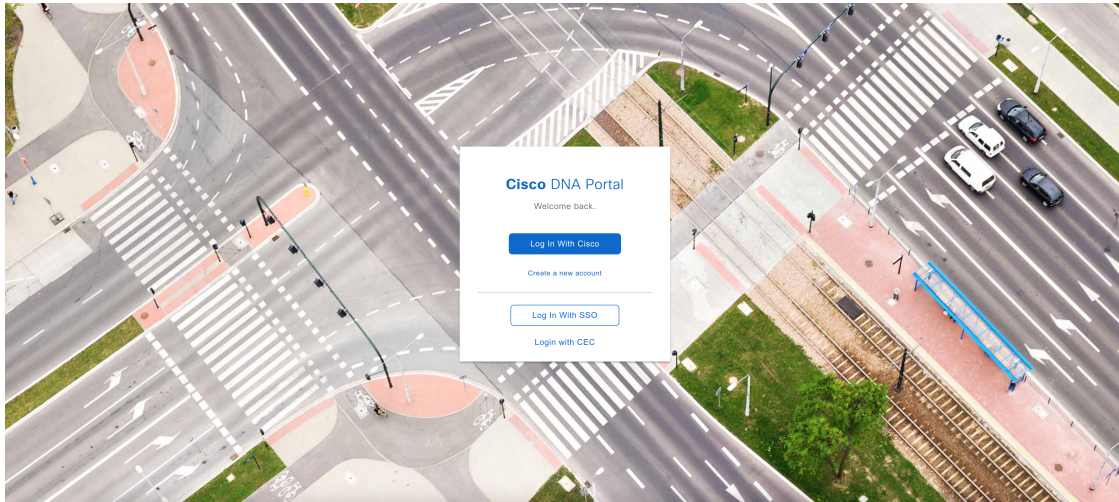
Make sure that you have a Cisco account. For more information, see [Create a Cisco Account, on page 1](#).

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

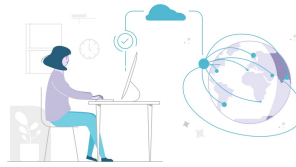
On the **Cisco DNA Portal Confirm CCO Profile** window, do the following:

- Verify that the details are correct.
- After reading, acknowledging, and agreeing with the conditions, check the check box.
- Click **Create Account**.

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

Log In to the Cisco DNA Portal with Cisco

Subscribe and maintain your offers more efficiently with Cisco DNA Portal. Select an offer below and enjoy your trip with Cisco DNA Portal.



Offers

Applications Experience

Application Experience enables Cisco DNA Center users to integrate with AppX cloud service to collect quality metrics and to enrich Cisco DNA Center application dashboards to get better visibility on the network.

[Subscribe](#)

Cisco DNA Center Cloud

Cisco DNA Center Cloud provides complete, cloud-based lifecycle management of Cisco Catalyst 9200, 9300, and 9500 Series Switches and Cisco Catalyst 9100 Series Access Points in Embedded Wireless Controller (EWC) mode. Network administrators can manage their wired and wireless network infrastructure at the site-level using a secure cloud user interface.

[Subscribe](#)
[Learn More](#)

SAN Insights Discovery

SAN Insights Discovery as a SaaS offering on DNAC Cloud. This is a much-awaited pre-sales tool for Cisco Sales, Account team and Partners. It provides a comprehensive health check of any customer SAN fabric. SID works for existing Brocade and Cisco SAN fabrics. SID helps the Cisco team to better understand what the customer has and how Cisco can help moving forward.

[Subscribe](#)
[Learn More](#)

Plug and Play as a Service

Plug and Play as a service enables users to securely day-0 onboard Catalyst 9K family of devices. During onboarding process you can upgrade image and deploy configuration to the device. After onboarding you can redirect the device to be managed by DNA controller.

[Subscribe](#)

pxGrid Cloud

Cisco pxGrid Cloud enables users to securely share context between on-premise Cisco ISE and cloud based applications. It is customizable, ensuring that only relevant data is shared. It is included as part of your Cisco ISE Advantage license.

[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.

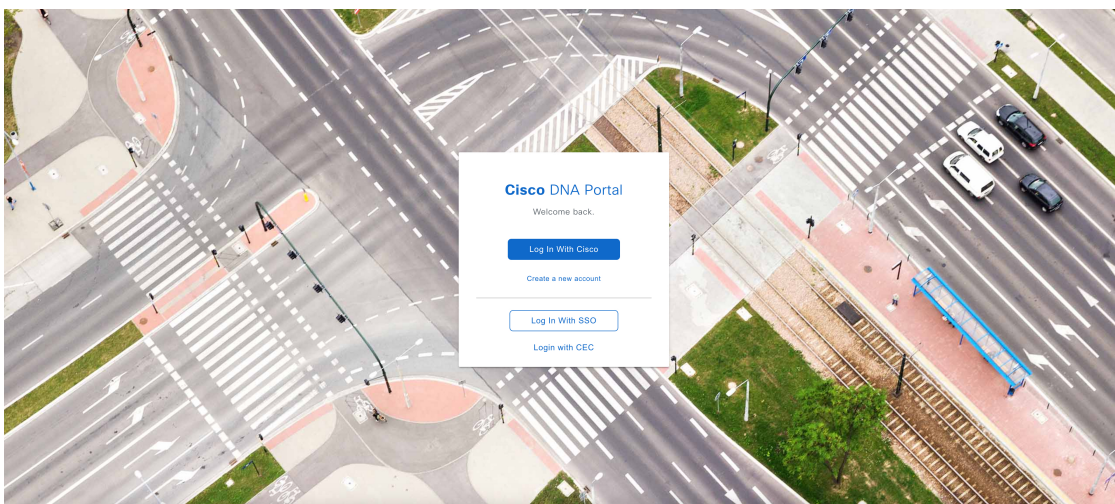
Before you begin

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**.

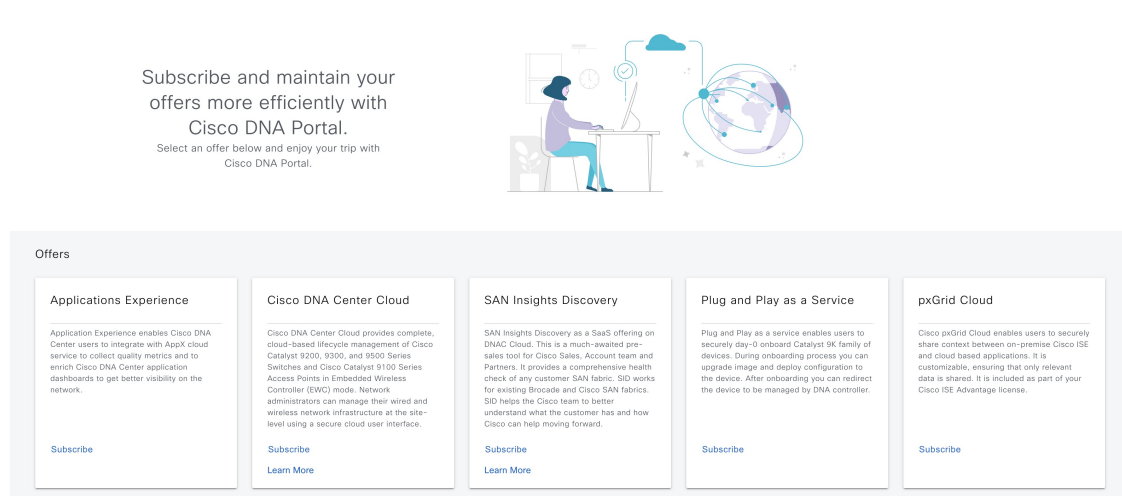
Step 3 Enter your Cisco account email in the **Email** field, and click **Next**.

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.



Subscribe and maintain your offers more efficiently with Cisco DNA Portal. Select an offer below and enjoy your trip with Cisco DNA Portal.

Offers

Applications Experience	Cisco DNA Center Cloud	SAN Insights Discovery	Plug and Play as a Service	pxGrid Cloud
Application Experience enables Cisco DNA Center users to integrate with AppX cloud service to collect quality metrics and to enrich Cisco DNA Center application dashboards to get better visibility on the network.	Cisco DNA Center Cloud provides complete, cloud-based lifecycle management of Cisco Catalyst 9200, 9300, and 9500 Series Switches and Cisco Catalyst 9100 Series Access Points in Embedded Wireless Controller (EWC) mode. Network administrators can manage their wired and wireless network infrastructure at the site-level using a secure cloud user interface.	SAN Insights Discovery as a SaaS offering on DNAC Cloud. This is a much-awaited pre-sales tool for Cisco Sales, Account team and Partners. It provides a comprehensive health check of any customer SAN fabric. SID works for existing Brocade and Cisco SAN fabrics. SID helps the Cisco team to better understand what the customer has and how Cisco can help moving forward.	Plug and Play as a service enables users to securely day-0 onboard Catalyst 9K family of devices. During onboarding process you can upgrade image and deploy configuration to the device. After onboarding you can redirect the device to be managed by DNA controller.	Cisco pxGrid Cloud enables users to securely share context between on-premise Cisco ISE and cloud based applications. It is customizable, ensuring that only relevant data is shared. It is included as part of your Cisco ISE Advantage license.
Subscribe	Subscribe Learn More	Subscribe Learn More	Subscribe	Subscribe

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:

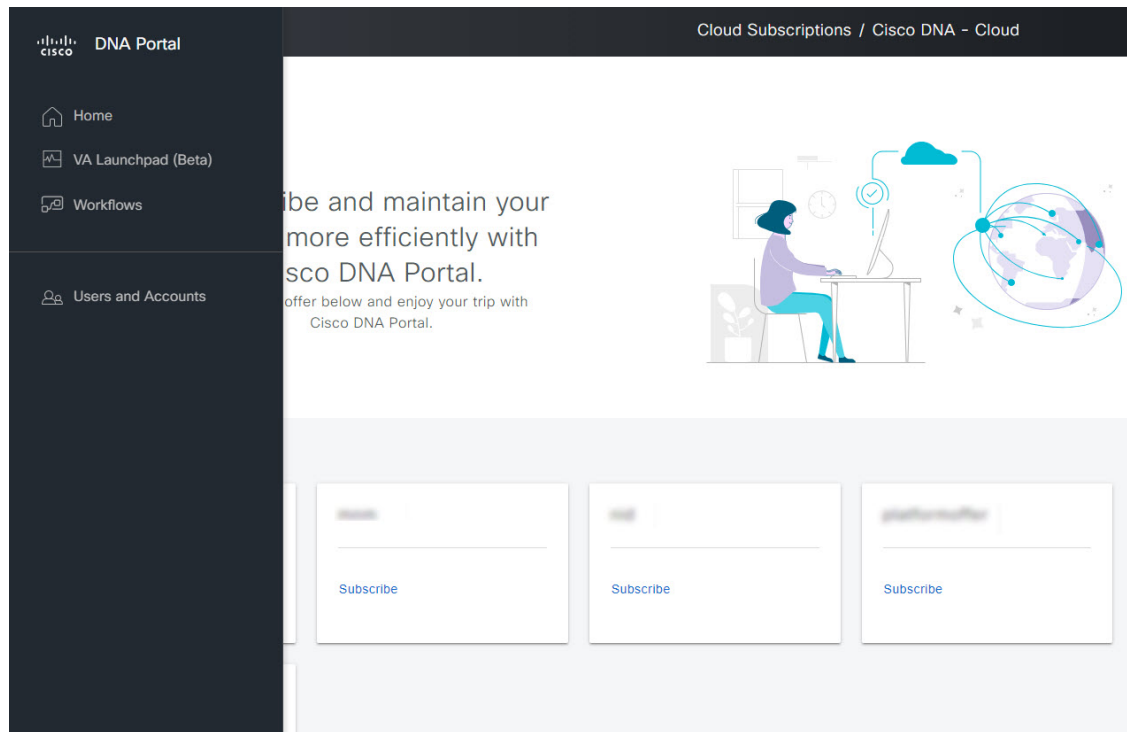
`http://<localhost>:<client-port-number>/valaunchpad`

For example:

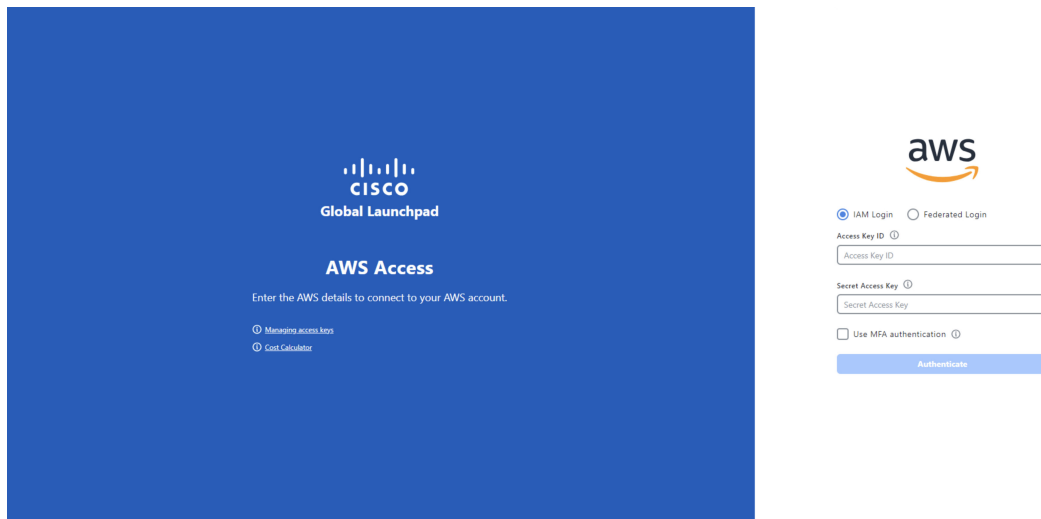
`http://192.0.2.1:90/valaunchpad`

- 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.



Step 2 Under the AWS logo, click the **IAM Login** radio button.

Step 3 Enter your credentials in the fields.

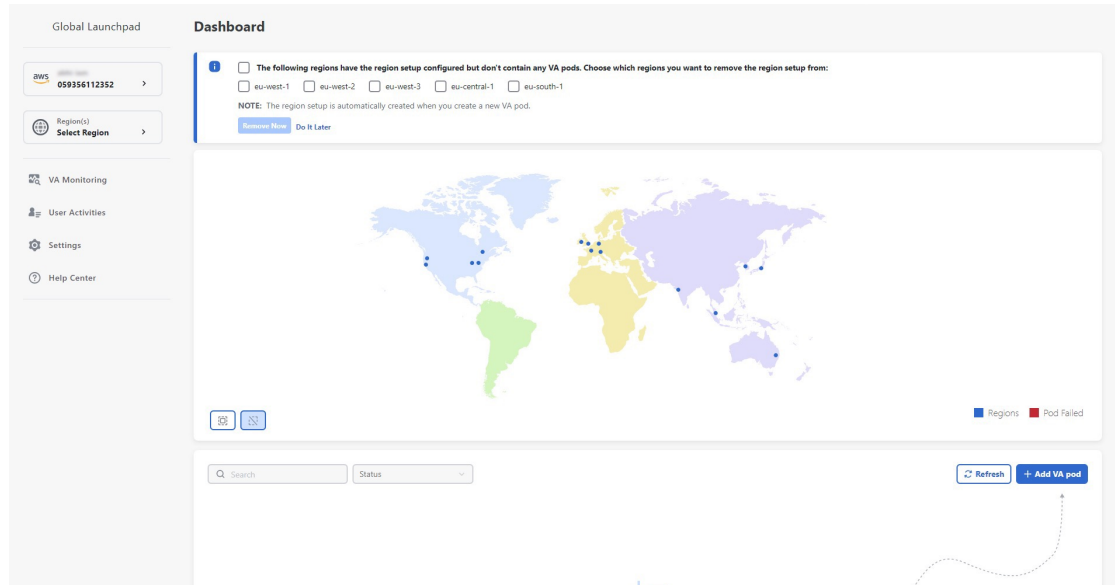
For information about how to get an Access Key ID and Secret Access Key, see the AWS [Managing access keys](#) topic in the *AWS Identity and Access Management User Guide* on the AWS website.

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](#).



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.



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:

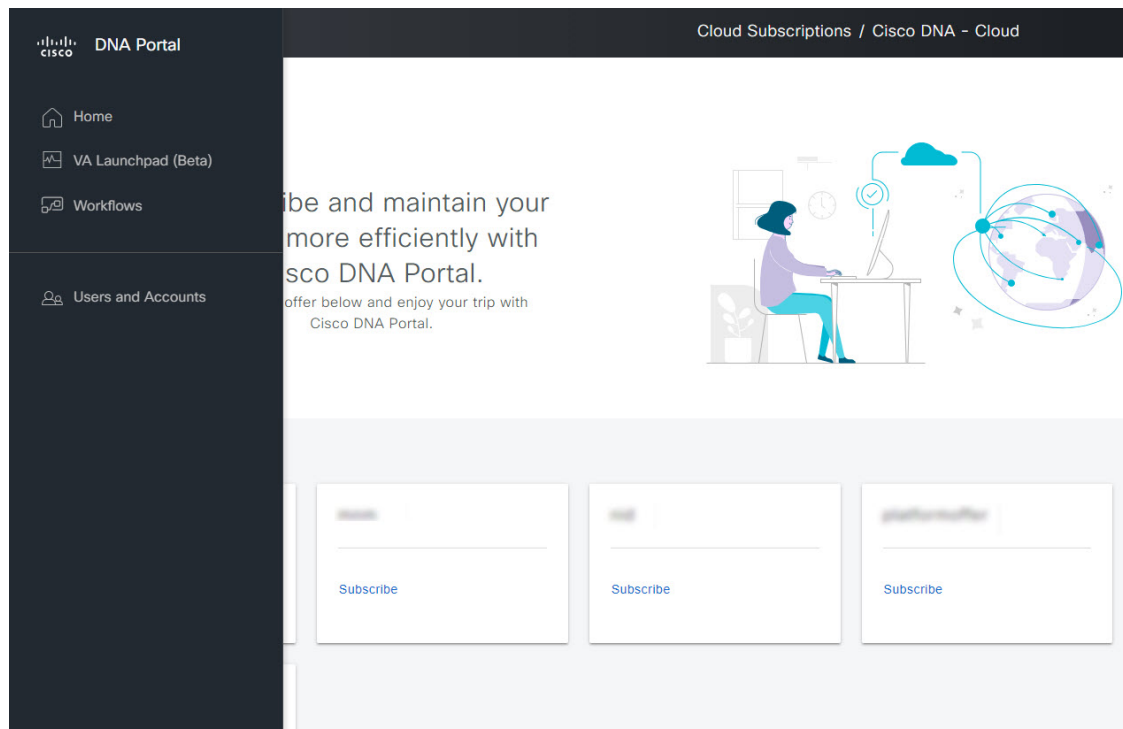
http://<localhost>:<client-port-number>/valaunchpad

For example:

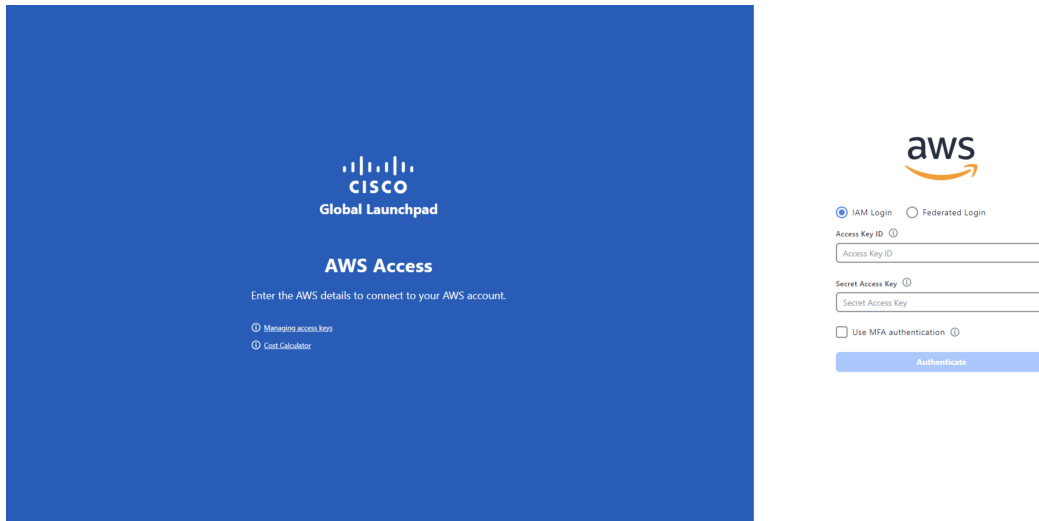
http://192.0.2.1:90/valaunchpad

- 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)**.



The AWS login window is displayed.



Step 2 Under the AWS logo, click the **Federated Login** radio button.

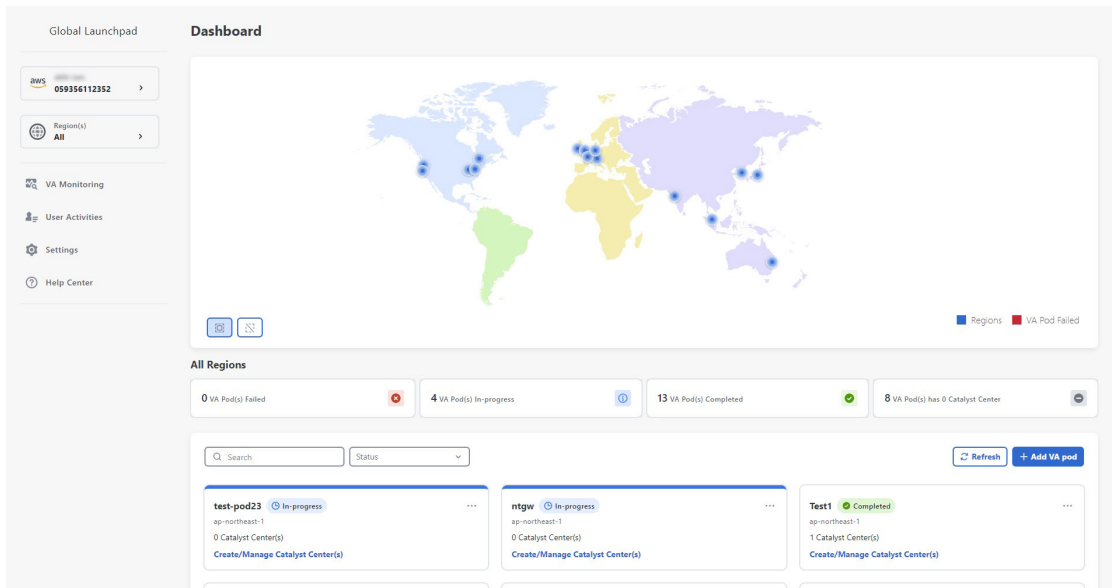
Step 3 Enter your credentials in the fields.

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:

```
[redacted] ~ % 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)
  --mfa=MFA           The name of the mfa. (env: SAML2AWS_MFA)
  -s, --skip-verify    Skip verification of server certificate. (env:
```

Step 3 Configure your account.

- Enter **saml2aws configure**.
- 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**.
- At the **AWS Profile** prompt, press **Enter** to use the default AWS profile.
- At the **URL** prompt, enter the URL of your identity provider (IdP) and press **Enter**.

Note You can get this information from your IdP.

- At the prompts, enter your username and password and press **Enter**.

Step 4 Generate your federated credentials.

- Enter **saml2aws login**.
- At the prompts, enter your username and password.
- 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.

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: [redacted]

devops

▼ Account: [redacted]

dflyreadonly

▼ Account: [redacted]

dflyreadonly

val

▼ Account: [redacted]

admin

[Sign in](#)

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.

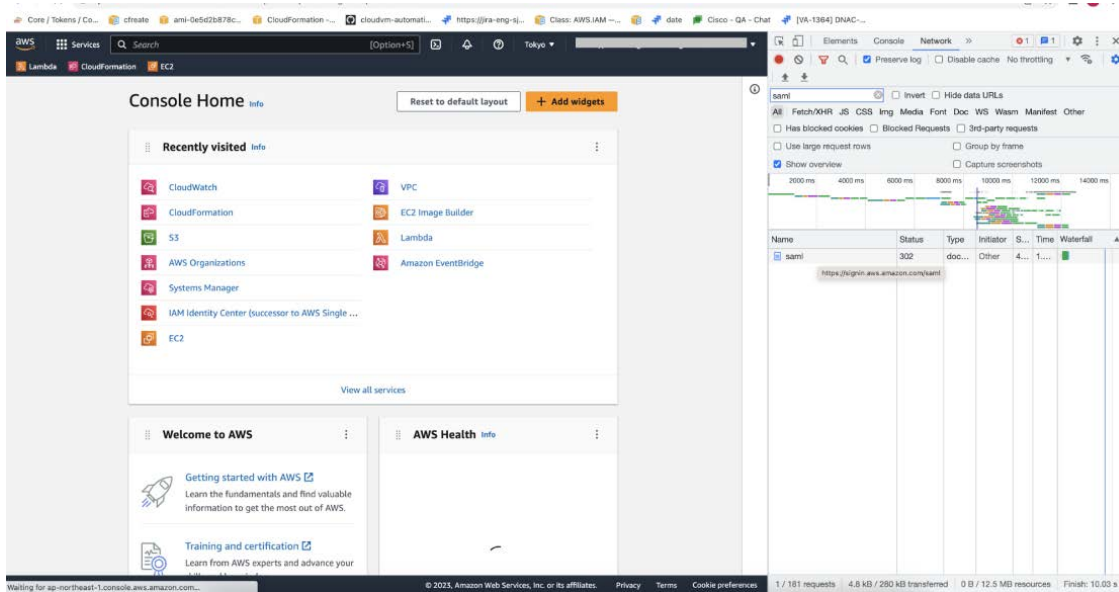
The screenshot shows the AWS IAM console interface with the Chrome Developer Tools panel open. The Network tab is active, and the 'Preserve log' checkbox is checked. The console displays a table of network requests with columns for Name, Sta., Type, Initiator, Size, Tr..., and Waterfall. Below the table, there are statistics for requests, data transferred, and resources. A 'Recorder panel updates' notification is visible at the bottom right of the Developer Tools panel.

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.

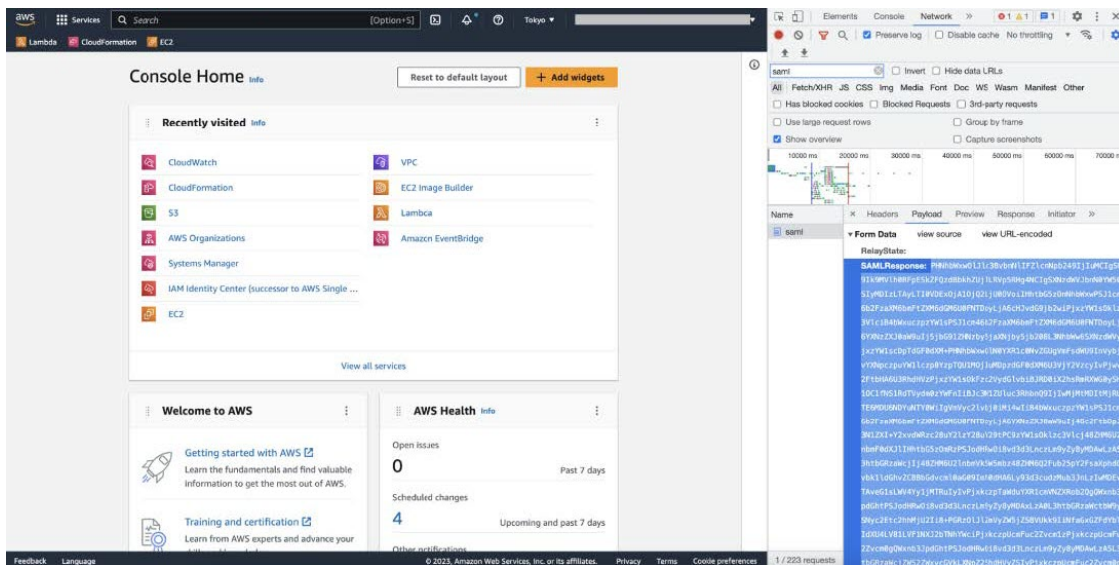
Generate Federated User Credential Using AWS CLI



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.



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.

The screenshot shows the AWS IAM console interface. On the left is the 'Identity and Access Management (IAM)' navigation pane with options like Dashboard, Access management, Access reports, and Related consoles. The main content area is titled 'IAM > Identity providers'. It features a notification banner about AWS IAM Identity Center, a 'Delete' button, and an 'Add provider' button. Below this is a search bar and a table of identity providers. The table has columns for 'Provider', 'Type', and 'Creation time'. The 'cloudsso.cisco.com' provider is selected with a radio button.

Provider	Type	Creation time
<input type="radio"/> idp1	SAML	21 days ago
<input type="radio"/> DNACADFS	SAML	10 days ago
<input type="radio"/> idp001	SAML	18 days ago
<input checked="" type="radio"/> cloudsso.cisco.com	SAML	7 months ago
<input type="radio"/> RAMANTECH	SAML	4 months ago

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
MIIC6jCCAdKgAwIBAgIQPP5He1K6QoZPQRiUjPzCUTANBgkqhkiG9w0BAQsFADAxMS8wLQY
DVQDEyZBREZTIFNpZ25pbmcgLSEFQzJBTUFaLU1IMUYzQ0Quc3NvLmNvbTAeFw0yMzAyMDY
wNTUyNDJaFw0yNDYyMDYwNTUNDJAMDExLzAtBgNVBAMTJkFERlMgU2lnbmluZyAtIEVDMkF
NQVotTUgXRjNDRC5zc28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsl
Sx/rQJ/wAOJ6ZRBbgYkfe7TMPsnOTqX0C+dh+yQ3O+X9xqRDPVKuSDHrv72bsGwk/
2VRdb38xdVueuFYRavyVPzjsSF95fkjC3qFDN+R5Dk1Cnba7GT6i+HGfacEpL8Vqd3jzNgh
guskM1OrHDHKDv5ksNMxppHIDPlVhyRCdKtPlPG5gBftoKvBZX+RxYcTaVUK/
NrMfkWmklyQTNRmpUDj+NawGGjr4byjH8hUu59cFJetaatzJo8qXuWWtPBtd+ESS/
DVR5dpilfyEBi4Dc22X91kOShJpeDu08EGfR605/nmRErlyy/p5f2sPKM0/
ix+XlQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA7kt4HeU/
zohOSDnnfmXypYi8WrJFxmVTS6Cjwe8eYZ6BwByEI4PjxcjPOu+sVNxrtBzJUwyPM+LKKMs
zYn5VQ/skrwcljW5P4msUMj4/J5K4vuYcKbJS4VyASKVZmWUWC23Whpc3U8ft6F7Jynp/
omrEh6Xrc4f4SqFdvIz35h2Sd/
HbcDp+sHZm4TgnA2XuSuvv0NJPF2VsRHMCMsn3eBTQfbbD5naLEpitjU8Zy5qW+Ic8Up5l
ATNzPP+kmaQY6SxPLeuAarrnp4vDrD7hpszneRfWX8h9v/Fg+wlnOsEeD1FYyLRoc
```

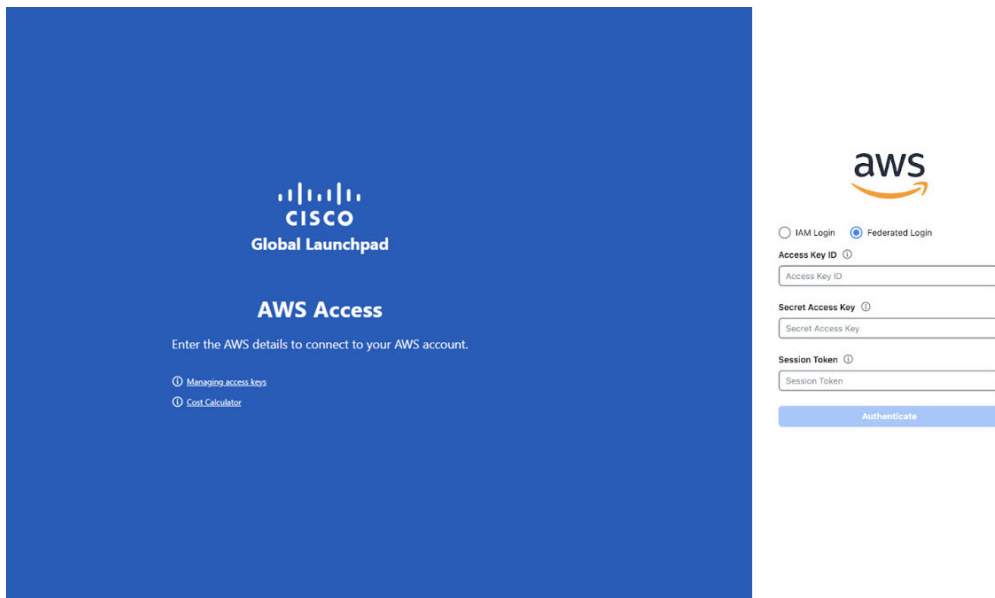
Output similar to the following output is displayed:

```
{
  "Credentials": {
    "AccessKeyId": "xxxx",
    "SecretAccessKey": "xxxxx",
    "SessionToken": "xxxxxxxxxx",
    "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": "POIUyTRFVNMKJGFKJHJHJcYLQCePSAZg="
}
```

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 (.
- 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**.

