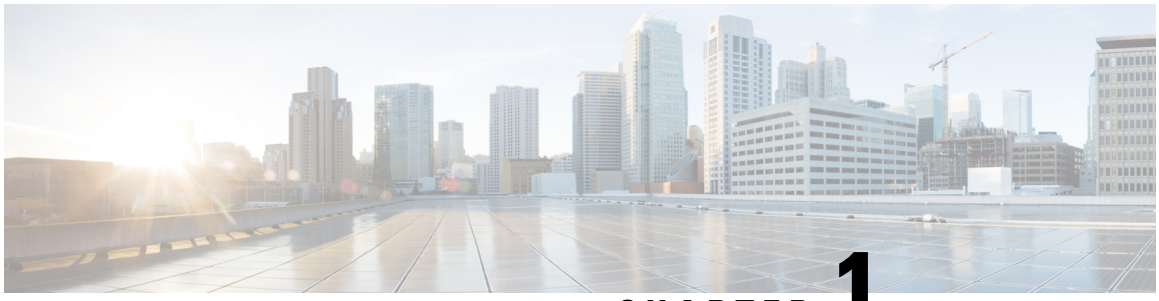
Cisco Global Launchpad 1.7 Administrator Guide

First Published: 2023-12-07

Last Modified: 2024-03-18

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Cisco Global Launchpad Overview

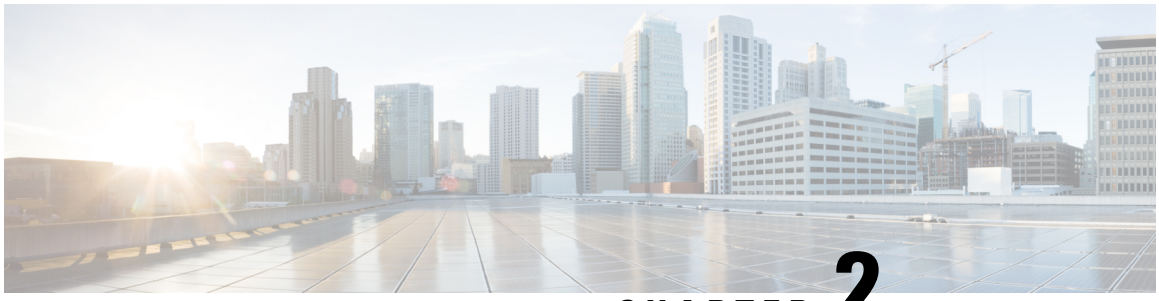
Cisco Global Launchpad Overview

Note Cisco DNA Center has been rebranded as Cisco Catalyst Center, and Cisco DNA Center VA Launchpad has been rebranded as Cisco Global Launchpad. During the rebranding process, you will see the former and rebranded names used in different collaterals. However, Cisco DNA Center and Catalyst Center refer to the same product, and Cisco DNA Center VA Launchpad and Cisco Global Launchpad refer to the same product.

Cisco Global Launchpad provides you with the tools you need to install and manage your Catalyst Center Virtual Appliance (VA). It helps you create and manage the services and components that are required for the AWS cloud infrastructure.

For specific information about deploying Catalyst Center using Cisco Global Launchpad, see the *Cisco DNA Center on AWS Deployment Guide*.

Cisco Global Launchpad Overview



CHAPTER 2

Access Cisco Global Launchpad

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.

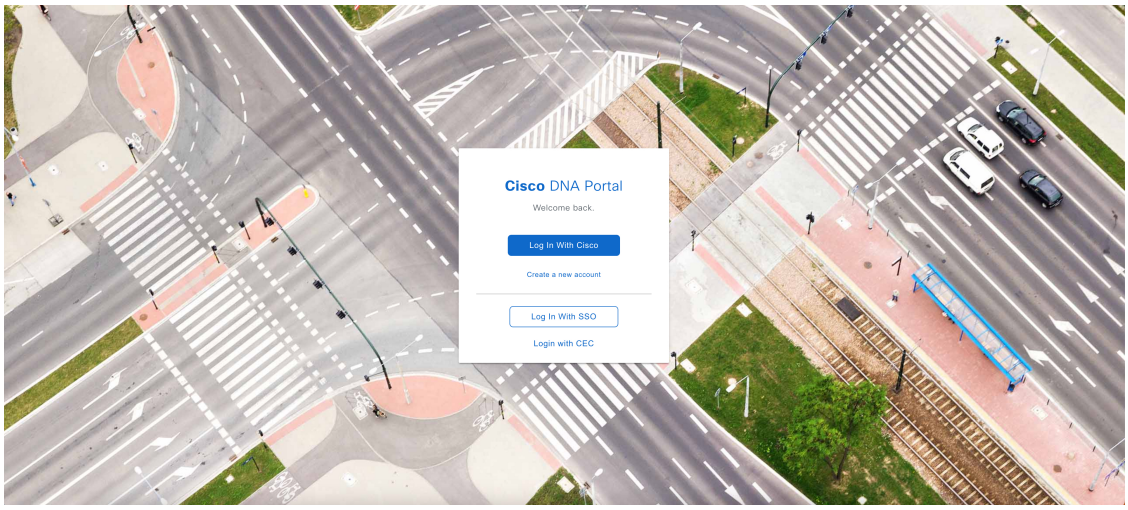
Create a Cisco Account

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

Step 1 In your browser, enter:

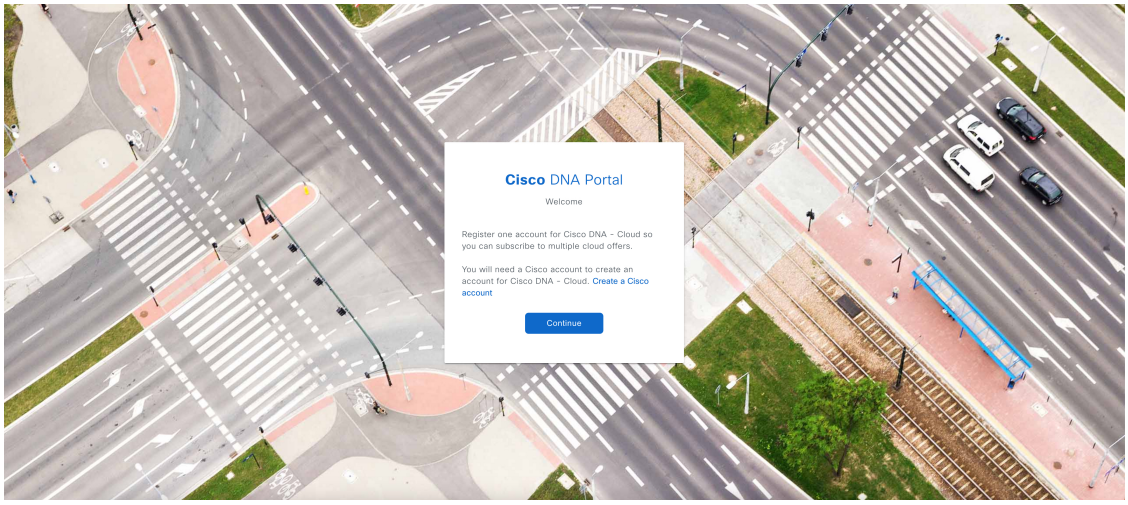
`dna.cisco.com`

The **Cisco DNA Portal** login window is displayed.

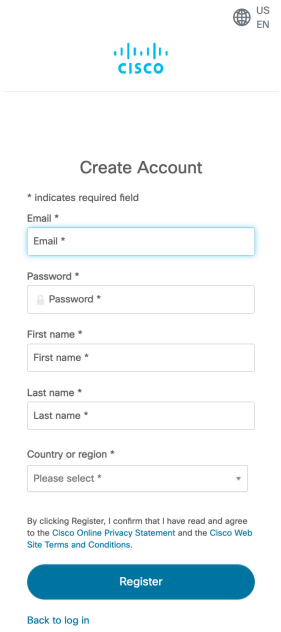


Step 2 Click **Create a new account**.

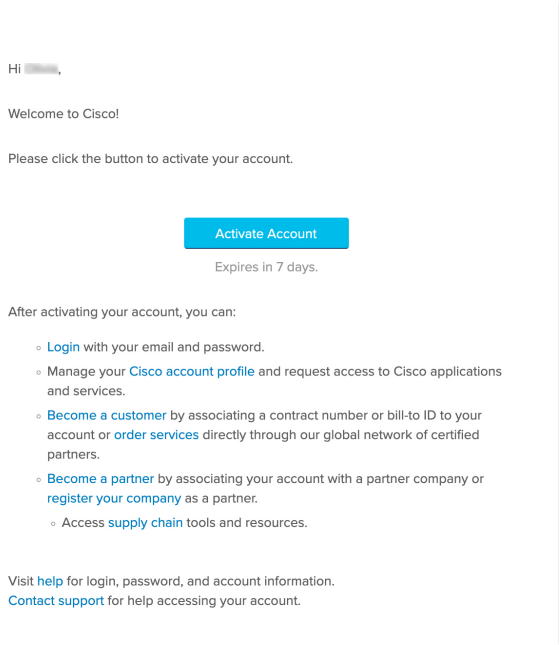
Step 3 On the **Cisco DNA Portal Welcome** window, click **Create a Cisco account**.



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**.



Create a Cisco DNA Portal Account

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

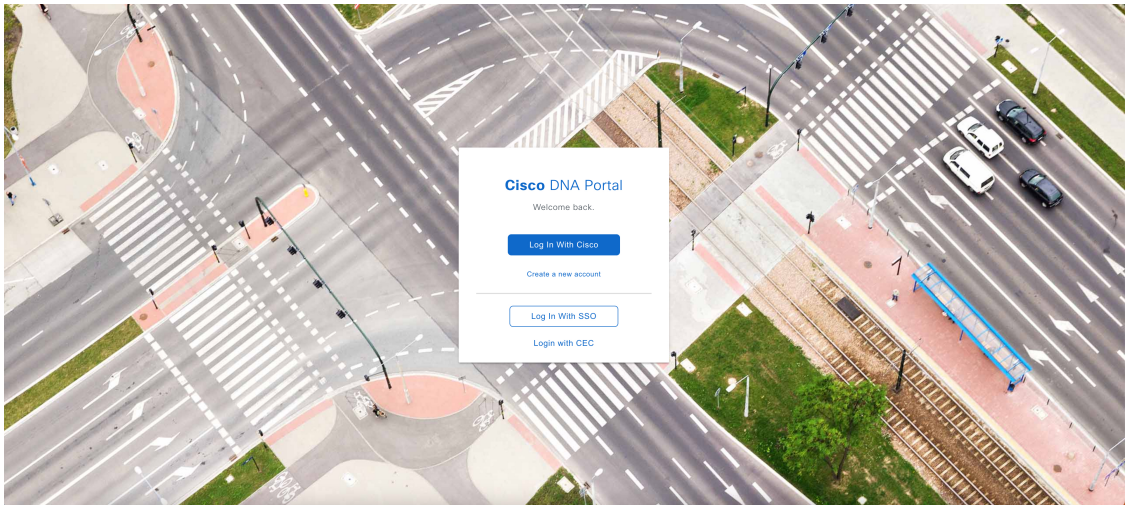
Before you begin

Make sure that you have a Cisco account. For more information, see Create a Cisco Account, on page 3.

Step 1 In your browser, enter:

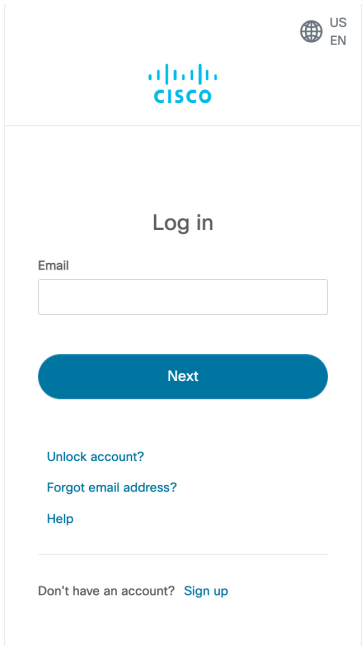
`dna.cisco.com`

The **Cisco DNA Portal** login window is displayed.

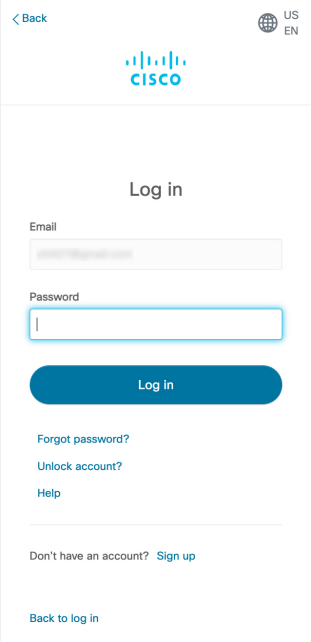


Step 2 Click **Log In With Cisco**.

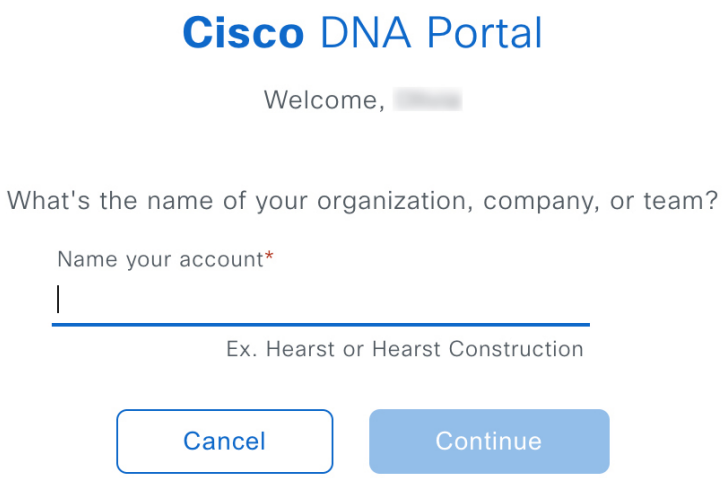
Step 3 Enter your Cisco account email in the **Email** field, and click **Next**.



Step 4 Enter your Cisco account password in the **Password** field, and click **Log in**.

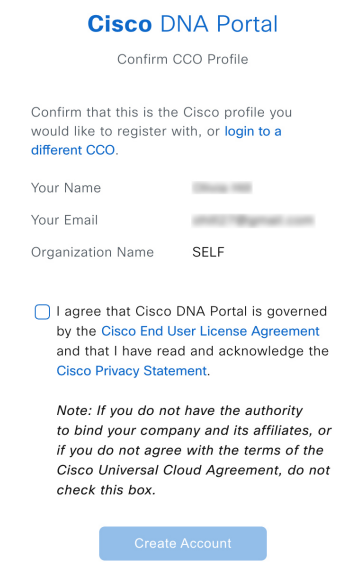


Step 5 On the **Cisco DNA Portal Welcome** window, enter the name of your organization or team in the **Name your account** field. Then click **Continue**.

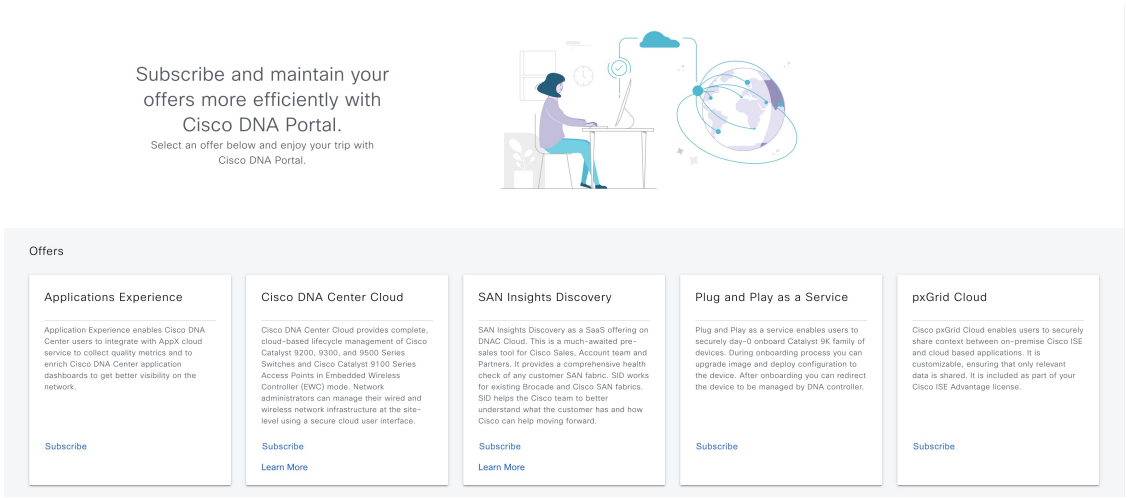


Step 6 On the **Cisco DNA Portal Confirm CCO Profile** window, do the following:

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.



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.

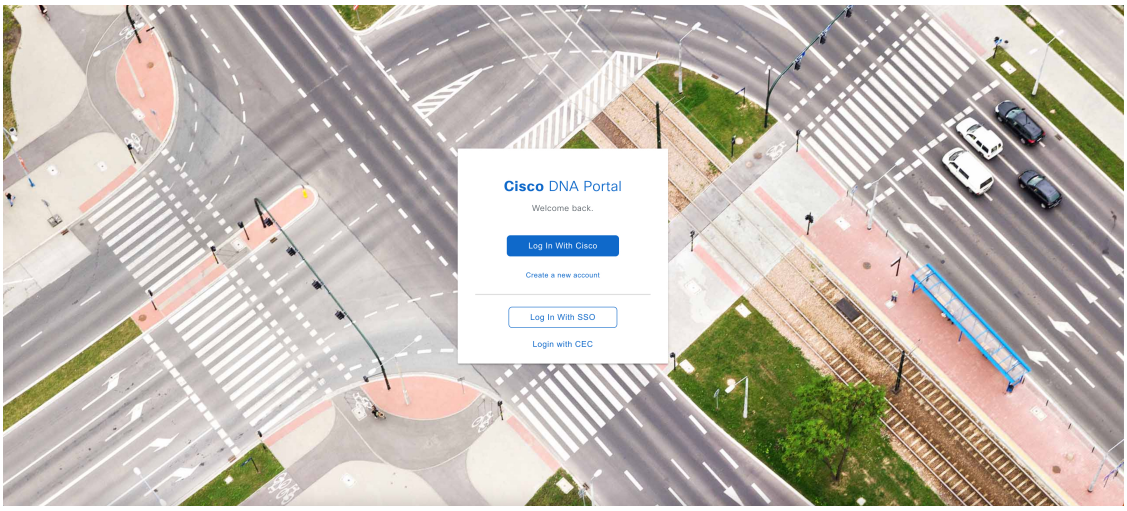
Before you begin

Make sure that you have a Cisco account and a Cisco DNA Portal account. For more information, see Create a Cisco Account, on page 3 and Create a Cisco DNA Portal Account, on page 5.

Step 1 In your browser, enter:

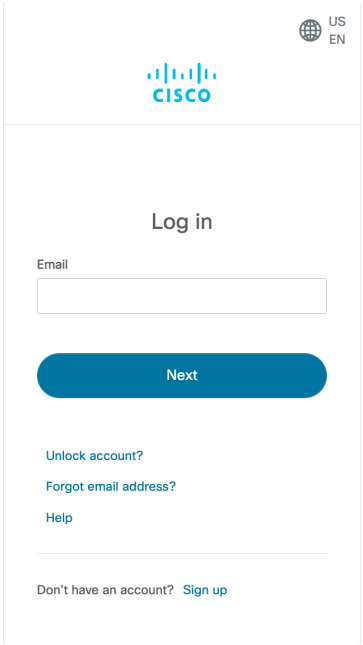
`dna.cisco.com`

The **Cisco DNA Portal** login window is displayed.

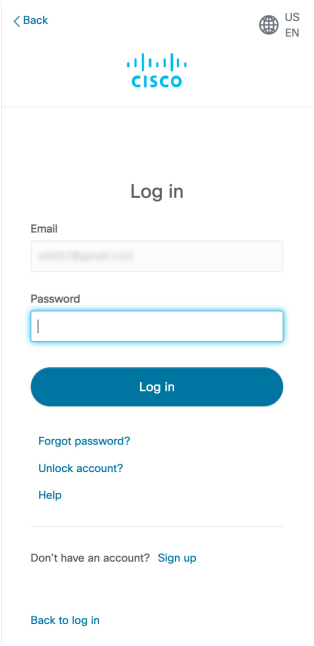


Step 2 Click **Log In With Cisco**.

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

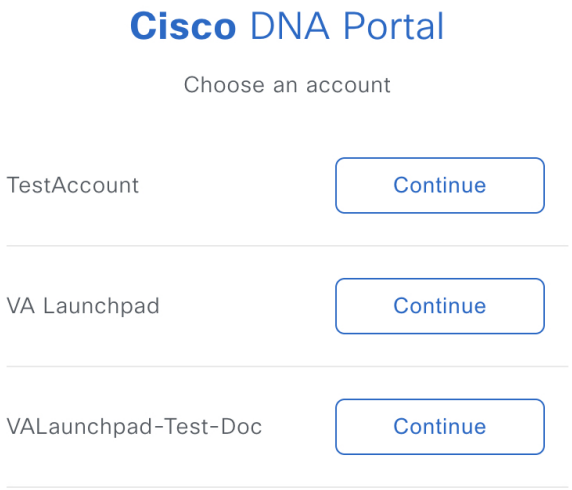


Step 4 Enter your Cisco account password in the **Password** field, and click **Log in**.

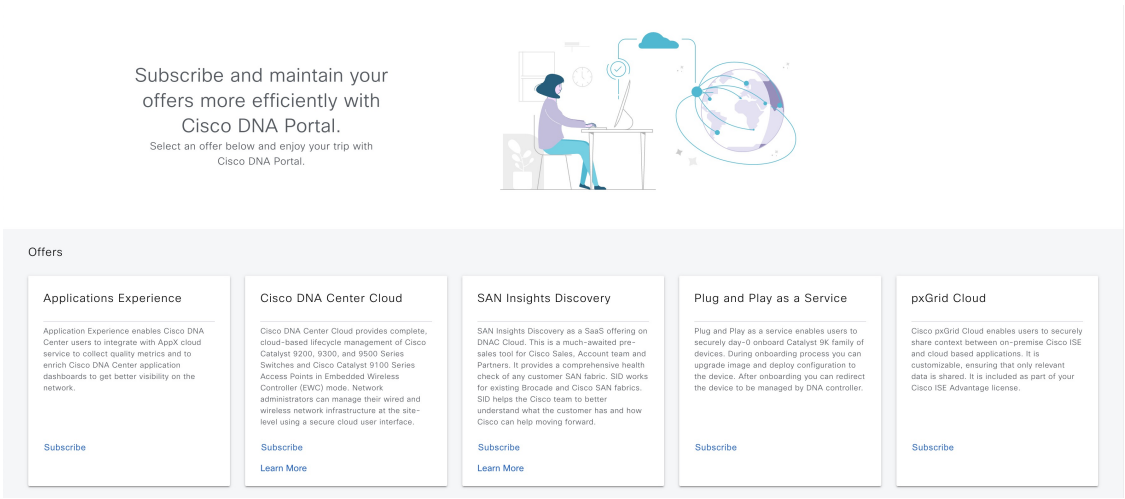


If you only have one Cisco DNA Portal account, the **Cisco DNA Portal** home page displays.

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 11: This method uses the credentials from your Cisco account.
- Log In Using Federated Identity, on page 15: 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 Catalyst 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 18
  - Generate Federated User Credential Using AWS CLI, on page 22

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:

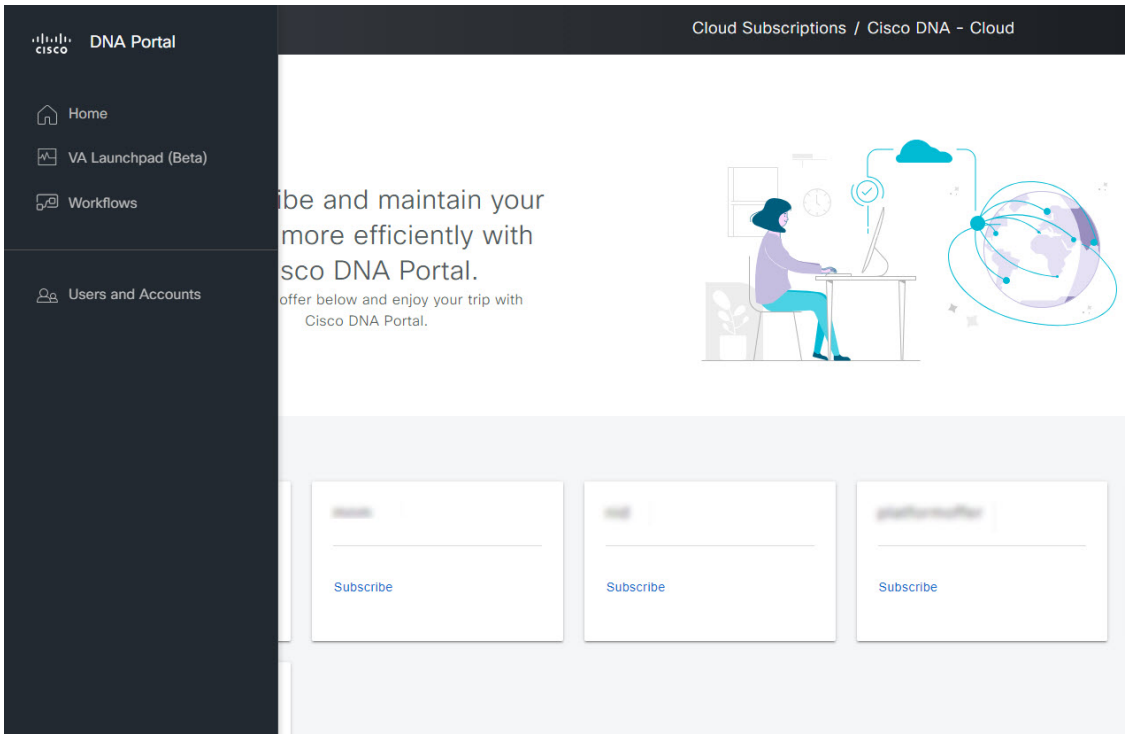
  http://<localhost>**:**<client-port-number>**/valaunchpad**

  For example:

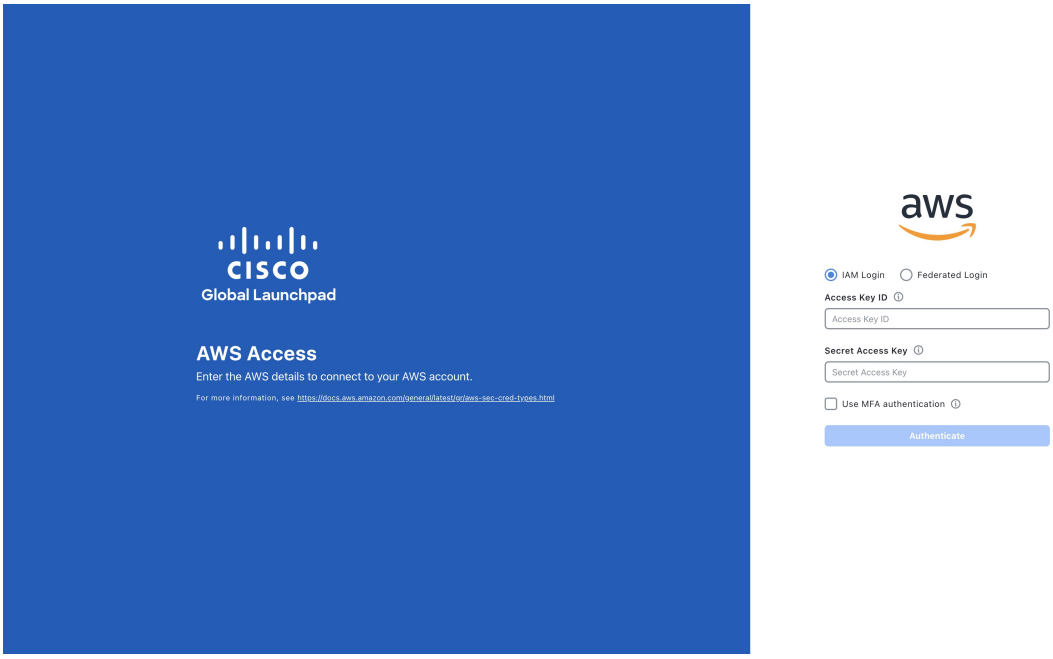
  http://192.0.2.1:90/valaunchpad

- 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 8.)

  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.

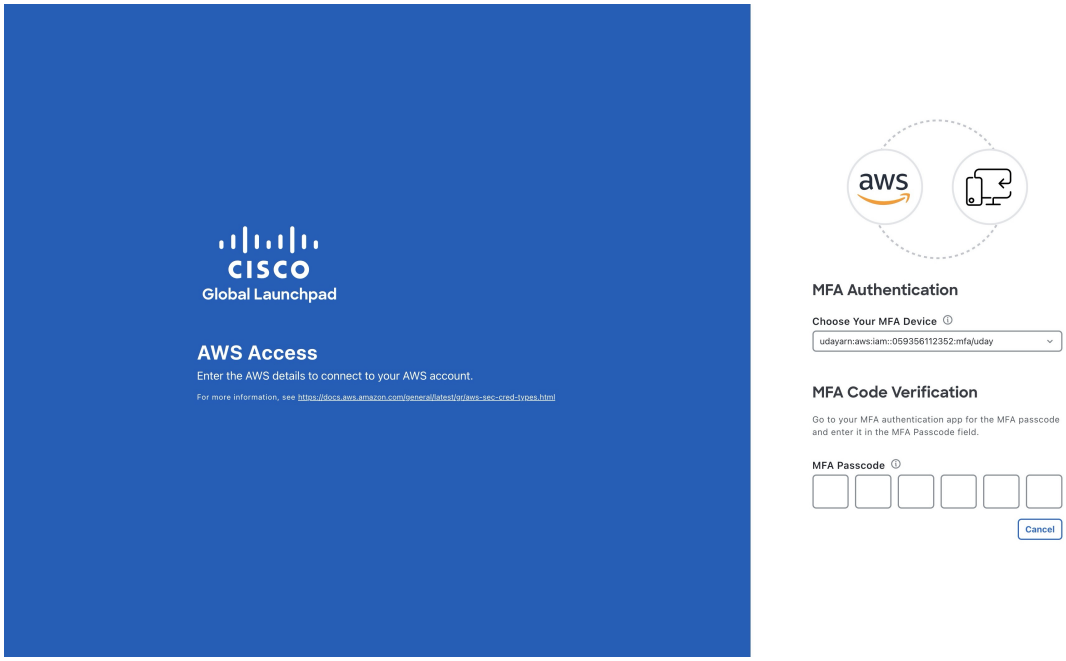
Step 3 Enter your credentials in the fields.

For information about how to get an Access Key ID and Secret Access Key, see the AWS Account and Access Keys topic in the *AWS Tools for PowerShell User Guide* on the AWS website.

Step 4 (Optional) If your company uses MFA, click the **Use MFA authentication** check box.

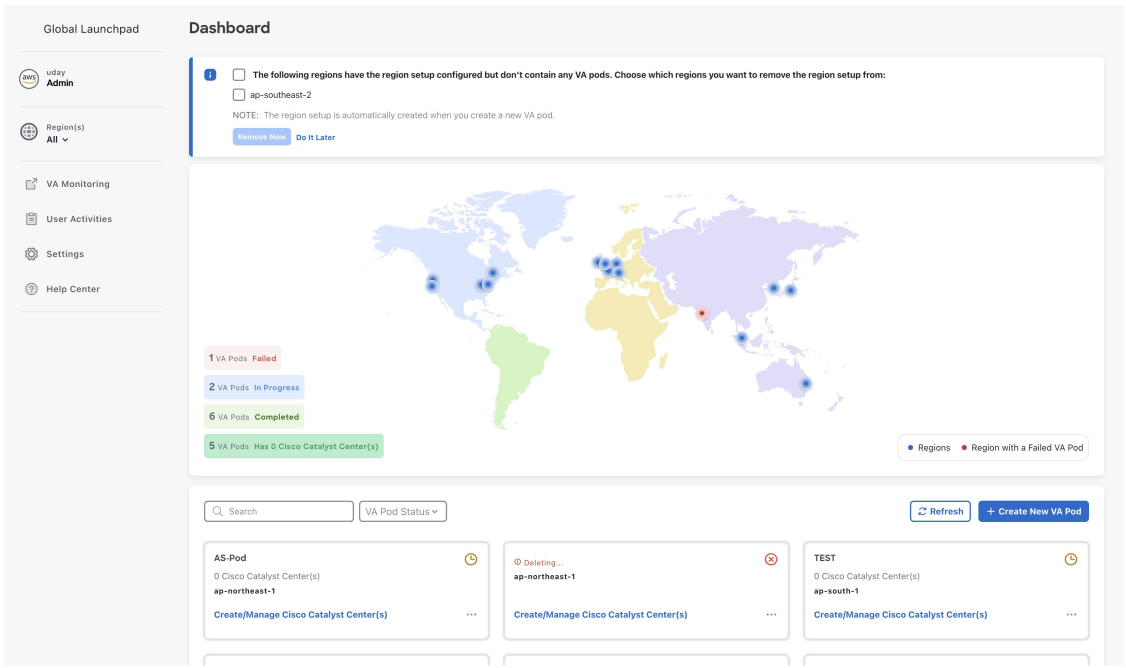
Step 5 Click **Authenticate**.

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, on page 29.



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 Catalyst 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 18 or Generate Federated User Credential Using AWS CLI, on page 22.

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:

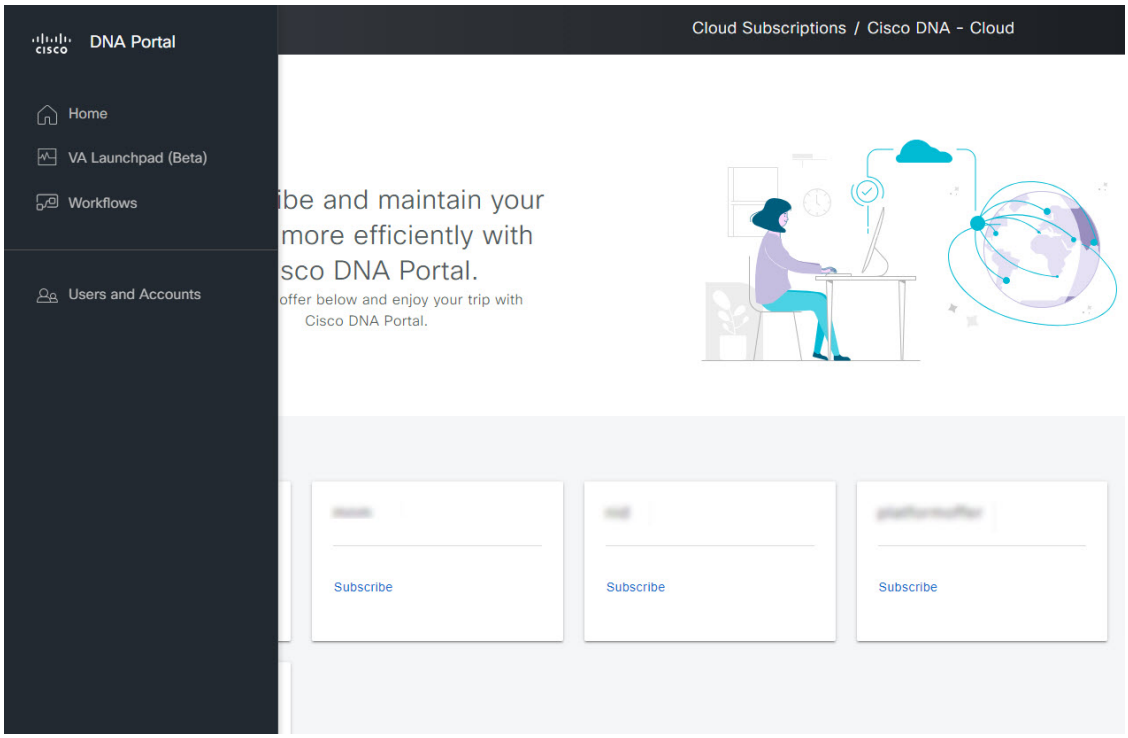
  `http://``<localhost>`**`:`**`<client-port-number>`**`/valaunchpad`**

  For example:

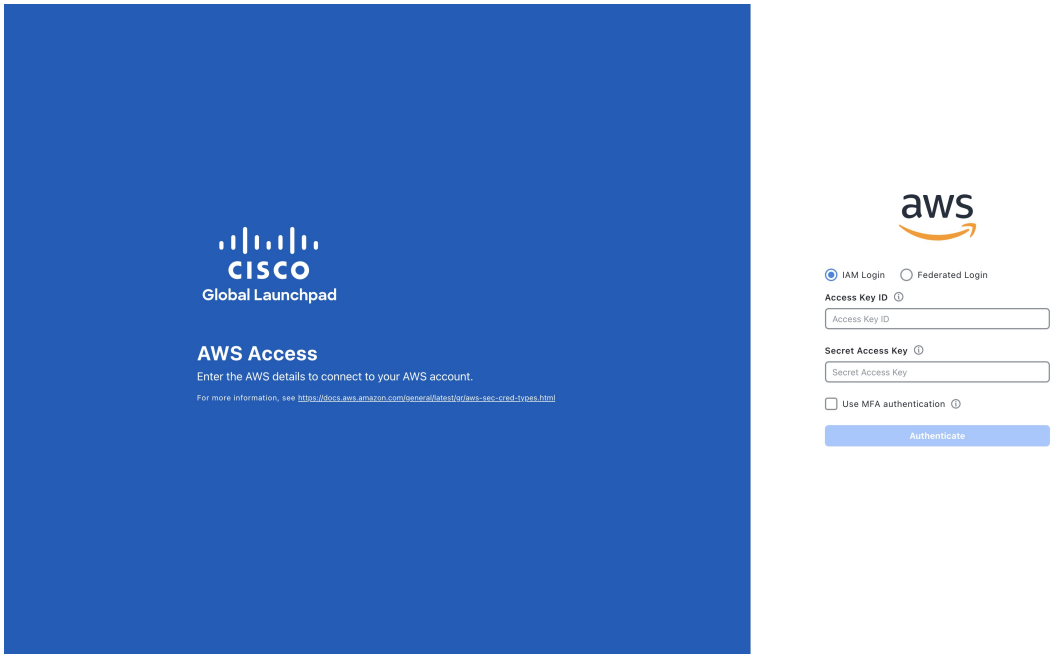
  `http://192.0.2.1:90/valaunchpad`

- 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 8.)

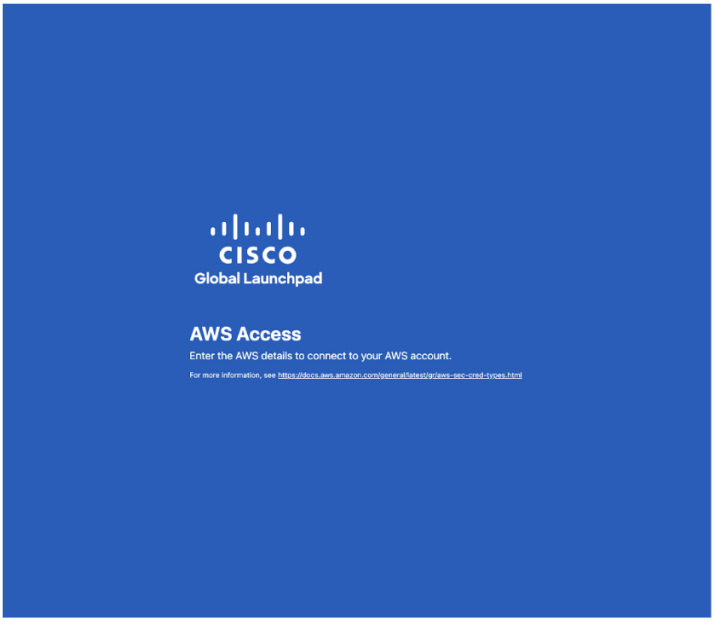
  From the **Cisco DNA Portal** home page, click the menu icon and choose **VA Launchpad (Beta)**.

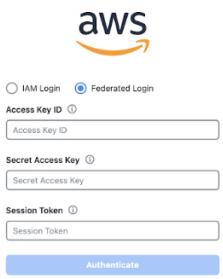


The AWS login window is displayed.



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





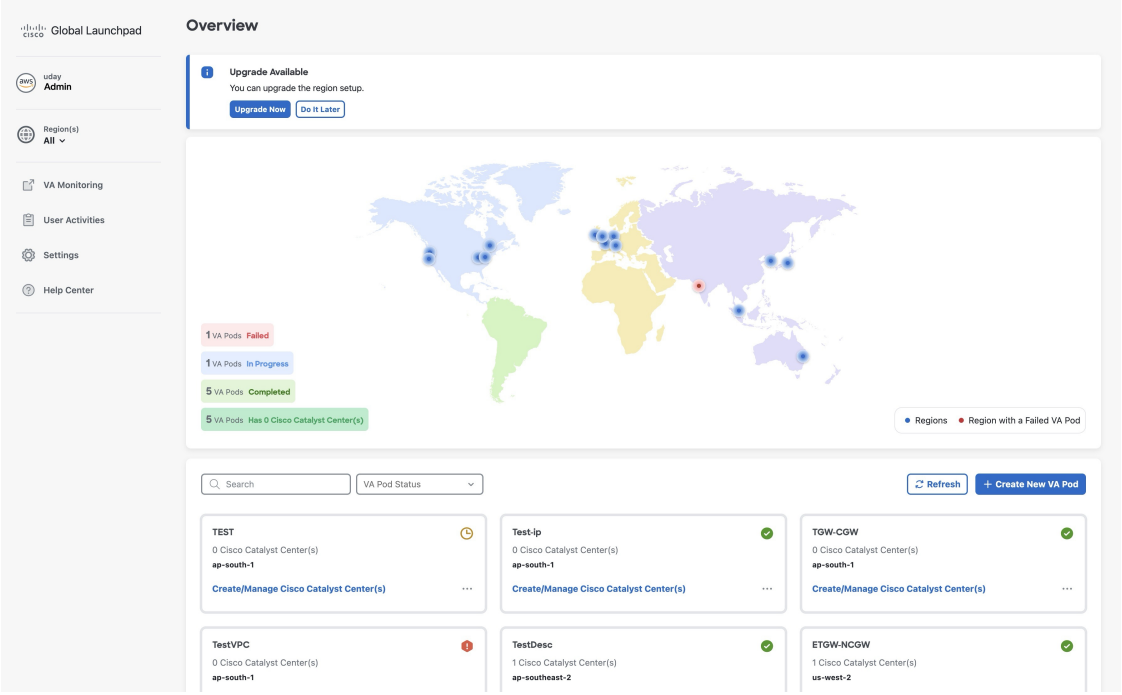
Step 3 Enter your credentials in the fields.

For more information, see Generate Federated User Credentials Using saml2aws, on page 18 or Generate Federated User Credential Using AWS CLI, on page 22.

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, on page 29.



Step 6 If you encounter any login errors, you need to resolve them and log in again. For more information, see the *Cisco Catalyst 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)
      --mfa=MFA                 The name of the mfa. (env: SAML2AWS_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, choose a provider and press **Enter**.

```
[                                    ~ % saml2aws configure                          ]
? Please choose a provider:  [Use arrows to move, type to filter]
  Akamai
  Auth0
  AzureAD
> Browser
  F5APM
  GoogleApps
  JumpCloud
```

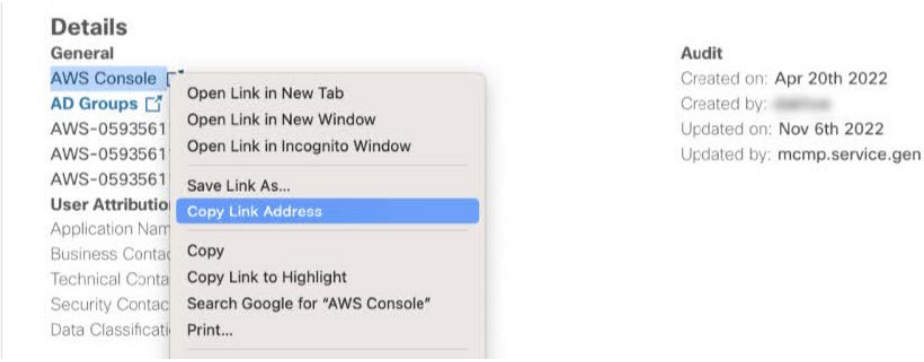
c) At the **AWS Profile** prompt, press **Enter** to use the default AWS profile.

```
[                                    ~ % saml2aws configure                          ]
? Please choose a provider: Browser
? AWS Profile (saml)
```

d) At the **URL** prompt, enter the URL of your identity provider (IdP) and press **Enter**.

```
[redacted] ~ % saml2aws configure
? Please choose a provider: Browser
[? AWS Profile saml
? URL (https://cloudsso.cisco.com/idp/startSSO.ping?PartnerSpId=https://signin.a
ws.amazon.com/saml)
```

Note You can get this information from your IdP.



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

```
[redacted] — saml2aws configure — 80×24

  exec [<flags>] [<command>...]
    Exec the supplied command with env vars from STS token.

  console [<flags>]
    Console will open the aws console after logging in.

  list-roles [<flags>]
    List available role ARNs.

  script [<flags>]
    Emit a script that will export environment variables.


[redacted] ~ % saml2aws configure
? Please choose a provider: Browser
[? AWS Profile saml
[? URL https://cloudsso.cisco.com/idp/startSSO.ping?PartnerSpId=https://signin.aw
s.amazon.com/saml
[? Username [redacted]
? Password
```

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`.

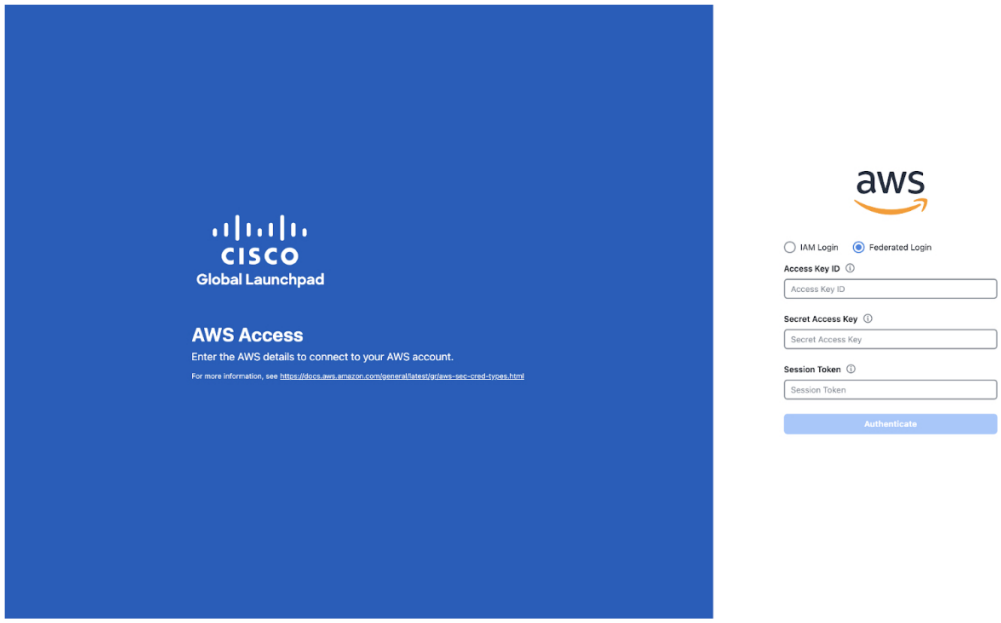
```
~ % saml2aws script
export AWS_ACCESS_KEY_ID=
export AWS_SECRET_ACCESS_KEY=
export AWS_SESSION_TOKEN=

export AWS_SECURITY_TOKEN=IQoJb3JpZ2luX2VjEAQaCXVzLWVhc3QtMSJIMEYCIQC57/JKBcFRmVhjeAC/48J6VXn3anqxs/LhFqy1ERf2twIhAJFt15wqZ83sHyBE
rPnbbu6xMZPjSj9+r5EwY73PRNEpKvoCCLz//////////wEQABoMMDU5MzU2MTEyMzUyIgx/PGnuyGmIFxpRKJcqzgJx+973k27K54YYewpvBmF0MbAmiZUCT3txuqkUb0
qjuOWrXPjRAil9bgBLC2jXel9q9VJIfEQYUGnQ+8WuuECXzy1tXF+/ZaDpjVnyry4Bw30ggZhPRJJiohT2T0+KxTZPLshMdhPGTqi2U/Jf1glIAipRDux/MydlLDKveSIP
ptVkPTnAMgLvAOtTYpzDmTGNwKc9Hs66S0qcreTWpGSuCNxjzvuENsky6uAZVOTivtgmEFzk6VjiXYOaoBLWLEk+LGziXeVucpyGSugCjzJVzNACZQFOfFEePb21KjJzra
EX7ioLcO7LbomZ0UP6ME2pza5uWZ0/AEicPUhpvRfkn5fS+fSu0syHdvprYIDWLX25zmNrqzhxT6vqR7EjJMmnL2OGfsYRheJQFDIBY0/5dyian4zPJGFhtaqGC5WHX74T
HfZyCfzu+yAr9b0zMMaGvKAGOpoBBkUU7OtSu4raGjuu8W8lDhXuqEhvkvt0qhPzmpcjgjV25MKyL4rM1aGCXXtIpoJ9/IVEfuRIwLl23qYDyLYptNn9x0qDDghh/YsOgd
+Nu+BPNYG4qjMCRGni1oypwN1Bj6TCLNmWQjYGQ5d17owrFCPquoRoas+BOmE86GHKYluOsiCeeA9SCMsf8+2zoJvyvAjME0tXPFgvVA==
export SAML2AWS_PROFILE=saml
export AWS_CREDENTIAL_EXPIRATION=2023-03-13T17:34:38+05:30
```

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.



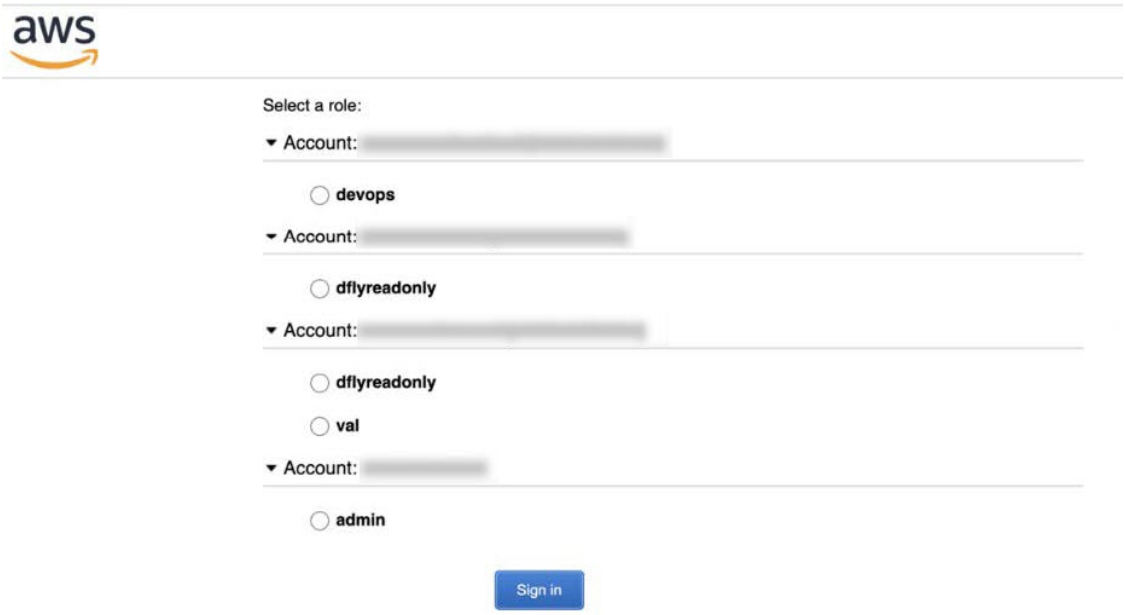
Generate Federated User Credential Using AWS CLI

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.

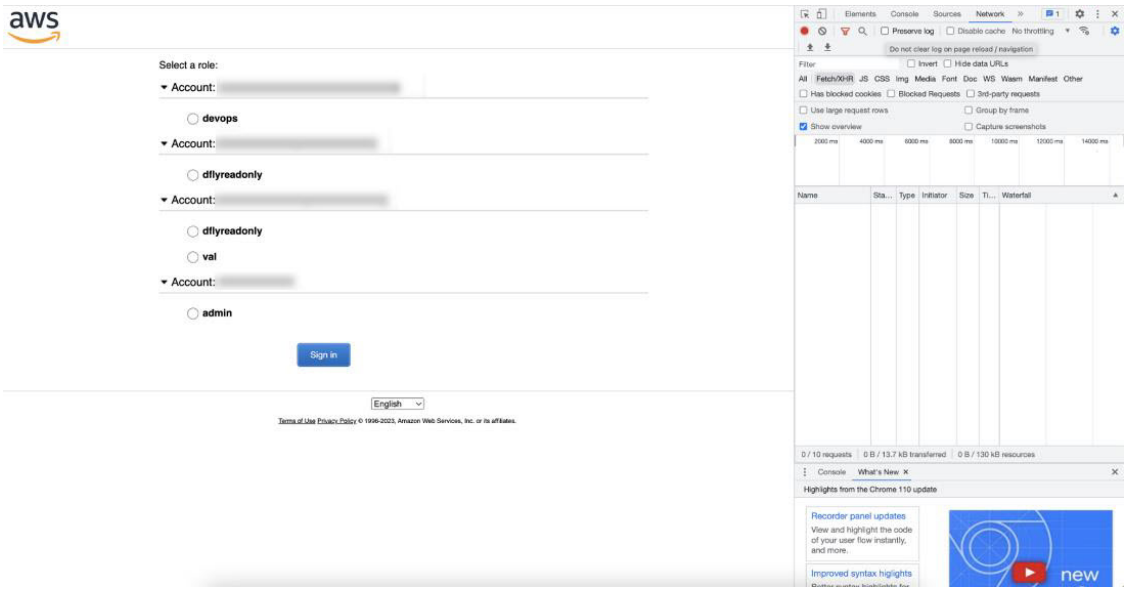
The following window is displayed.



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.

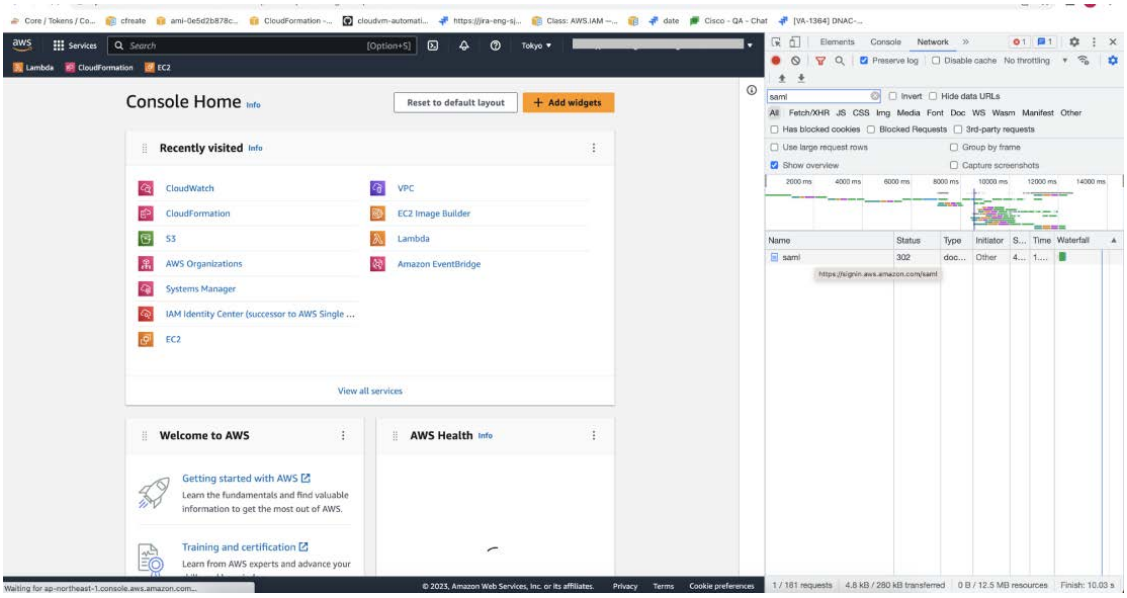
The **Developer Tools** panel is displayed, similar to the following window.



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**.

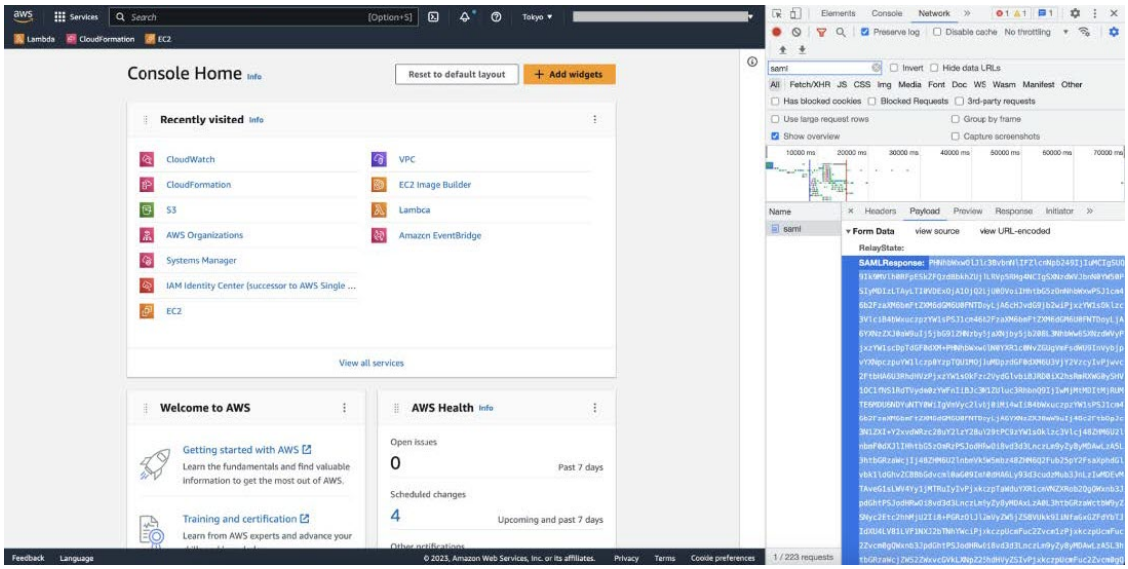
Step 6 In the **Developer Tools** panel, filter the required API calls by entering **`saml`** in the **Filter** field.



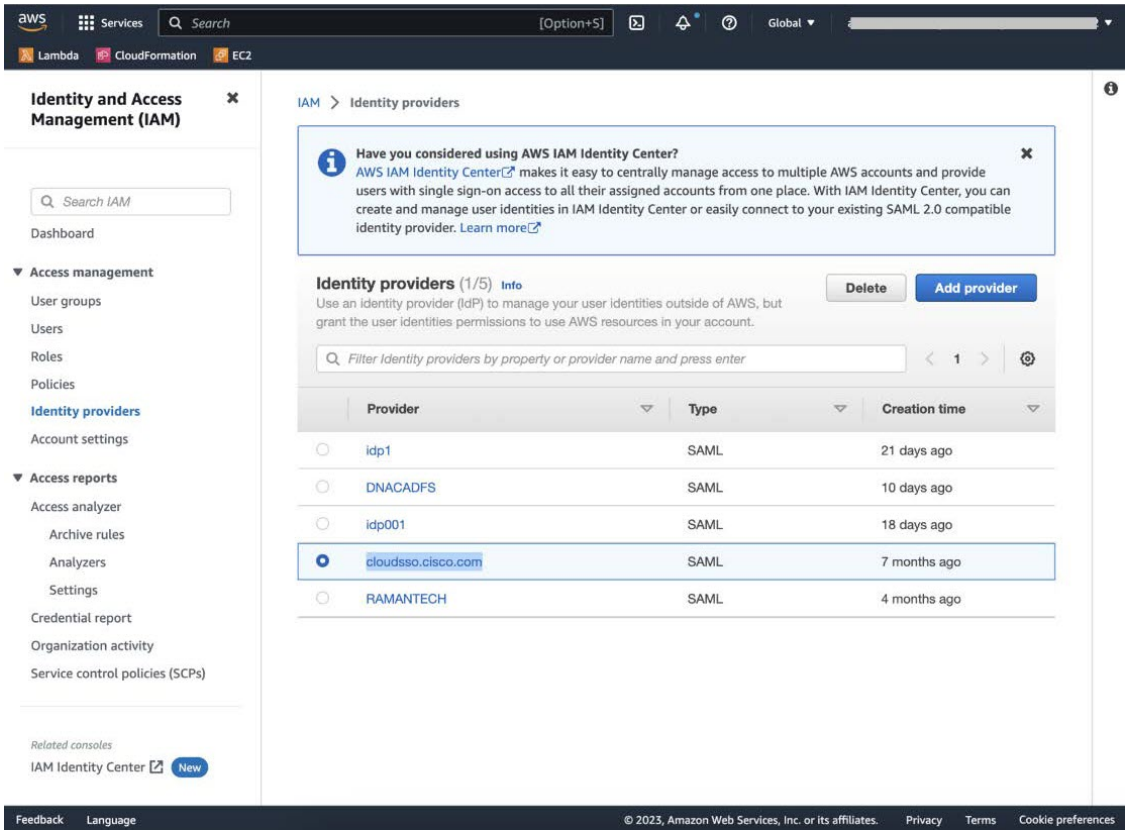
Step 7 Click the API request named **saml**.

Step 8 Click the **Payload** tab.

Step 9 Copy the value of the SAML response.



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



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
MIIC6jCCAdKgAwIBAgIQPP5He1K6QoZPQrIuPjzCUTANBgkqhkiG9w0BAQsFADAxMS8wLQY
DVQDEyZBREZTIFNpZ25pbmcgLSBFQzJBTUFaLU1IMUYzQ0Quc3NvLmNvbTAeFw0yMzAyMDY
wNTUyNDJaFw0yNDAyMDYwNTUNDJaMDExLzAtBgNVBAMTJkFERlMgU2lnbmluZyAtIEVDMkF
NQVotTUgxRjNDRC5zc28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsl
Sx/rQJ/wAOJ6ZRBbgYkfE7TMPsnOTqX0C+dh+yQ3O+X9xqRDPVKuSDHrv72bsGwk/
2VRdb38xdVueuFYRavyVPzjsSF95fkjC3qFDN+R5Dk1Cnba7GT6i+HGfacEpL8Vqd3jzNgh
guskMlOrHDHKDv5ksNMxppHIDPlVhyRCdKEtP1PG5gBftoKvBZX+RxYcTaVUK/
NrMfkWmklyQTNRmpUDj+NAwGGjr4byjH8hUu59cFJetatzJo8qxuWWtPBtd+ESs/
DVR5dpilfyEBi4Dc22X91kOShJpeDuO8EGfR6O5/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:

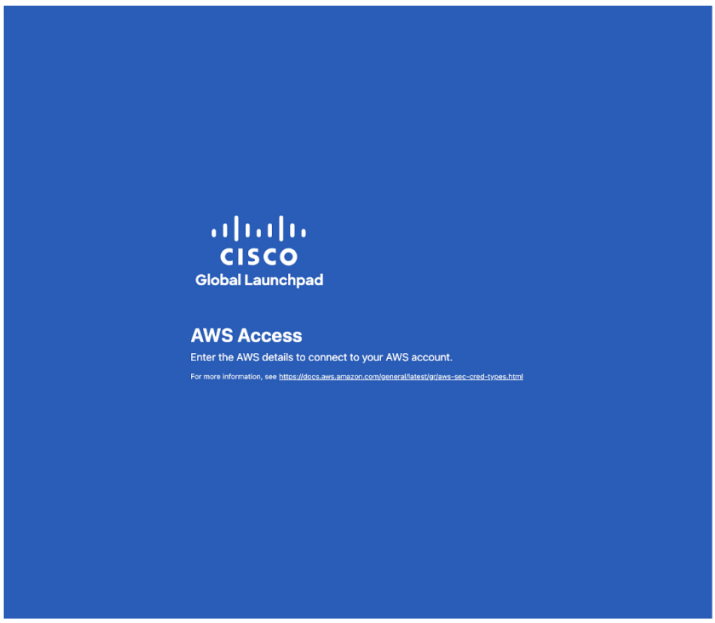
```
{
"Credentials": {
"AccessKeyId": "xxxx",
"SecretAccessKey": "xxxxx",
"SessionToken": "xxxxxxxxx,
"Expiration": "2023-03-10T18:07:15+00:00"
},
"AssumedRoleUser": {
"AssumedRoleId": "xxx:user@sso.com",
"Arn":"arn:aws:sts::059356109852:assumed-role/ADFS-AWS-ADMIN/user@sso.com"
},
"Subject": "SSO\\USER",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

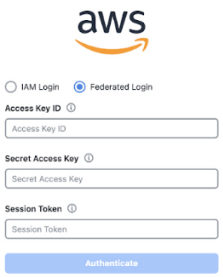
Step 13 Note the values of the following generated credentials:

- 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 ( ).

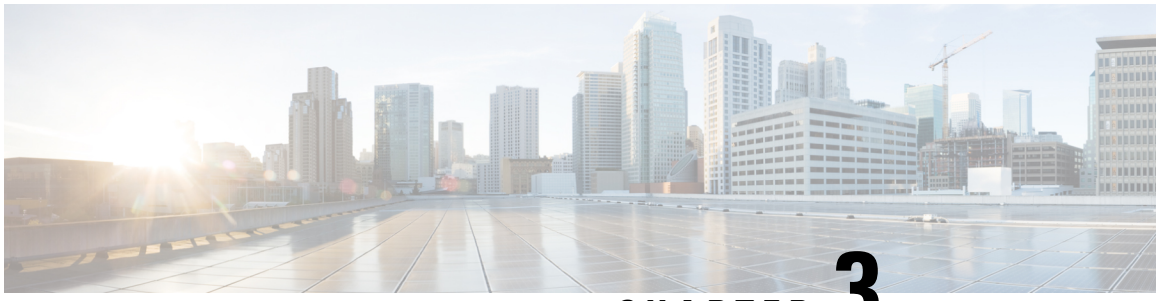
b. In the **Confirmation** dialog box, click **Log Out**.

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**.



CHAPTER 3

Manage Regions

Regions Overview

A region is an isolated area containing dedicated resources. To achieve the greatest possible fault tolerance and stability, resources are not shared or replicated in other regions.

A region is created when you create the first VA pod in that region. After a region has been created, you can add more VA pods to it. A region is created based on its AWS configuration template. Whenever AWS updates a region template version, Cisco Global Launchpad notifies you that you need to update the corresponding region in Cisco Global Launchpad. You are notified of the region version update when you first log in to Cisco Global Launchpad or when you change the region view.

When you delete all the VA pods from a region, the region is not automatically deleted. Cisco Global Launchpad permits empty regions. You can always create other VA pods in it later. However, if you no longer want to use an empty region and you want to delete it, you must do so manually using Cisco Global Launchpad.

Configure a Region

You can choose a region from the list of supported regions in Cisco Global Launchpad.

Before you begin

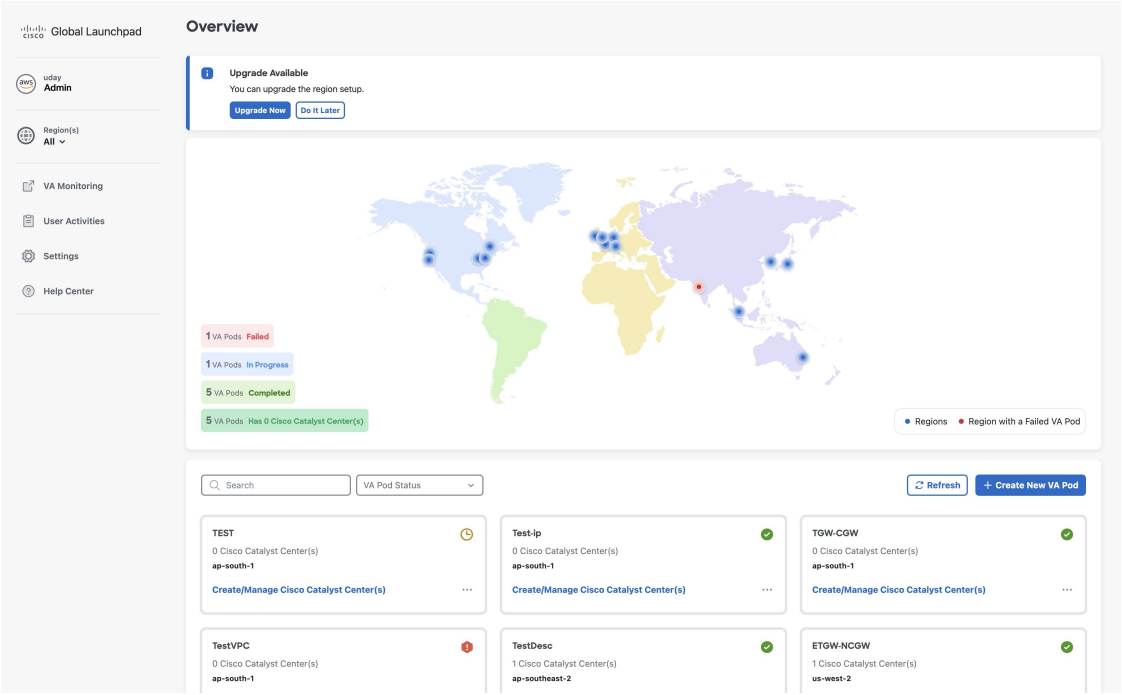
Confirm with your AWS administrator that the relevant regions are enabled in AWS. On Cisco Global Launchpad, the **Region** drop-down list only displays enabled regions.

Step 1 On the **Dashboard** pane, if you're prompted to update the region version, follow the prompts to complete the update.

Note You must update a region when an updated version is available. Cisco Global Launchpad automatically checks if an updated region version is available whenever you log in or change the selected region. If an updated region version is detected, Cisco Global Launchpad prompts you to update it. Follow the on-screen prompts.

The update may take a few minutes. Do not close the tab or window until the process has completed.

If the update fails, Cisco Global Launchpad restores the region to the last working version and displays an error. In this case, contact Cisco TAC for assistance.



Step 2 In the left navigation pane, from the **Region** drop-down list, choose one of the following regions:

- ap-northeast-1 (Tokyo)
- ap-northeast-2 (Seoul)
- ap-south-1 (Mumbai)
- ap-southeast-1 (Singapore)
- ap-southeast-2 (Sydney)
- ca-central-1 (Canada)
- eu-central-1 (Frankfurt)
- eu-south-1 (Milan)
- eu-west-1 (Ireland)
- eu-west-2 (London)
- eu-west-3 (Paris)

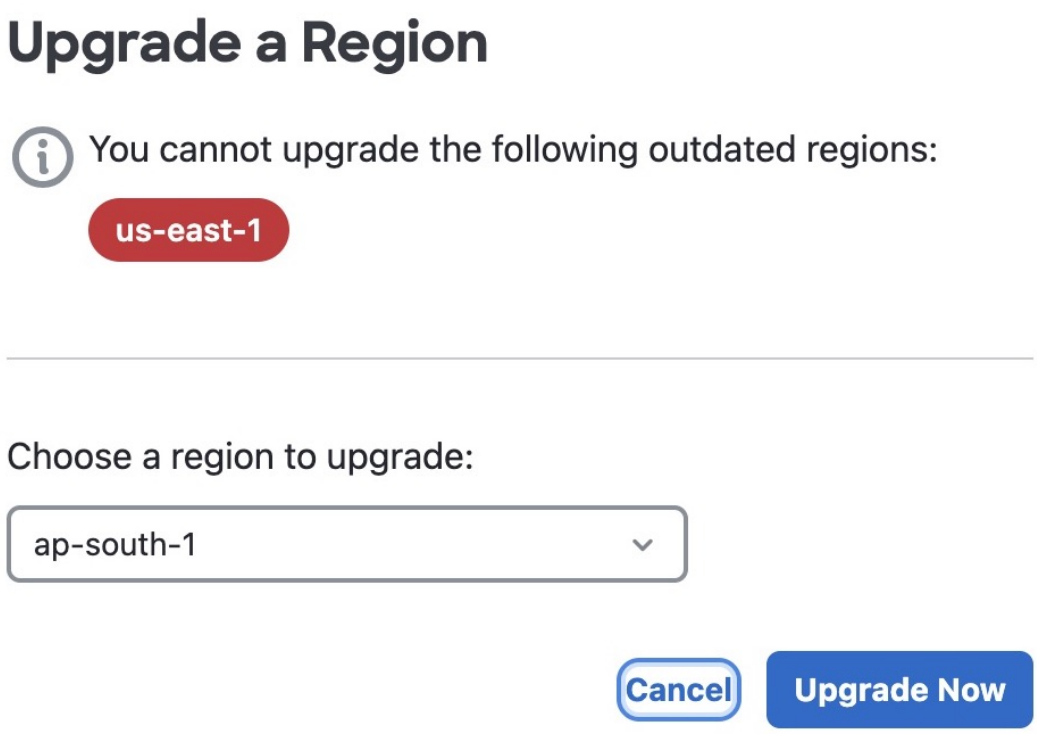
- us-east-1 (Virginia)
- us-east-2 (Ohio)
- us-west-1 (N. California)
- us-west-2 (Oregon)

If you're prompted to update the region version, follow the prompts to complete the update. For information, see Update a Region, on page 29.

Note Only enabled regions are displayed in the **Region** drop-down list.

Update a Region

Whenever you log in or change the selected region, Cisco Global Launchpad automatically checks if an updated region is available. If an updated region is detected, Cisco Global Launchpad prompts you to update it.



If you choose to update the region, click **Upgrade Now** and follow the prompts. The update may take a few minutes. Do not close the tab or window until the process has completed. If the update succeeds, click **Ok** to continue. If the update fails, Cisco Global Launchpad restores the region to the last working version and displays an error. In this case, contact Cisco TAC for assistance.

If you choose not to update the region, click **Do It Later**. Note that if you choose not to update the region, you may experience issues with the VA pod operation.

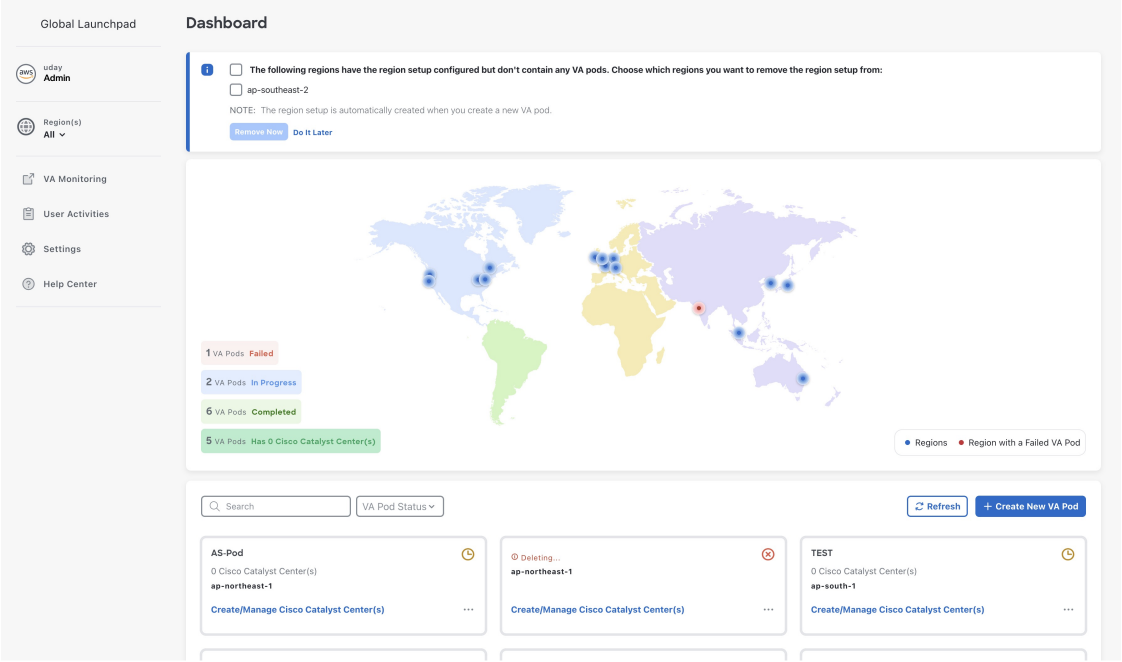
Remove a Region

When there are no VA pods in a region and you want to delete the region, complete the following procedure.

Note When the last VA pod is deleted in a region, the region itself isn't deleted. This means that **+ Create New VA Pod** will remain enabled, allowing you to create new VA pods in the region.

Step 1 Make sure that all VA pods in the selected region are deleted. For information, see Delete a VA Pod, on page 33.

When no VA pods exist in the selected region, a banner is displayed at the top of the **Dashboard** pane.

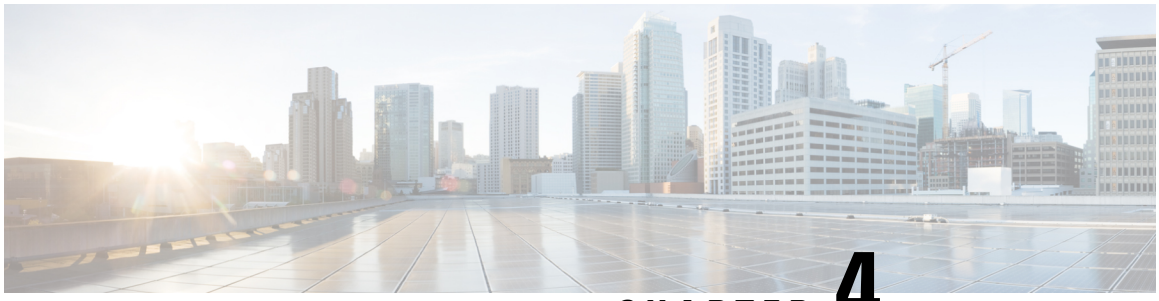


Step 2 In the banner, click **Remove**.

The removal process can take up to a minute. You can't create any new VA pods during this process.

When the region is deleted, a successful notification message is displayed in the top-right corner of the **Dashboard** pane.

Note When you create a new VA pod in the selected region for the first time, a new region is created automatically.



CHAPTER 4

Manage VA Pods

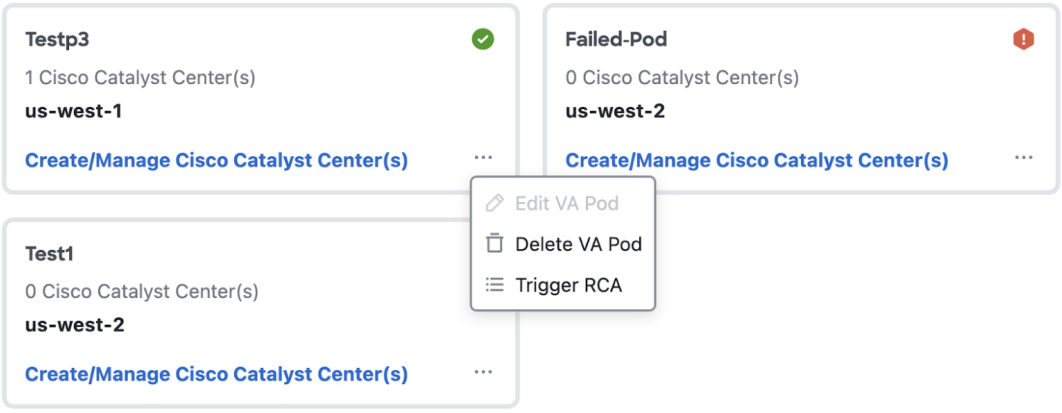
Edit a VA Pod

You can edit your VA pod only if you chose **VPN GW** as your preference while creating the VA pod.

Note While editing a VA pod, you will not receive email notifications about the VA pod because Amazon EventBridge (an AWS service that's used to trigger email notifications) is disabled. When the VA pod edits are configured successfully, you'll receive email notifications about this VA pod again because Amazon EventBridge is re-enabled.

Step 1 On the **Dashboard** pane, locate the VA pod.

Step 2 In the bottom-right corner of the VA pod card, click the ellipsis icon (**...**) and choose **Edit VA Pod**.



Step 3 In the **Modify VPN Details** page, make the desired edits to the following VPN details and then click **Next**:

- Customer Gateway IP

Make sure that the Customer Gateway IP is a valid public address.

- VPN Vendor
- Platform
- Software

Step 4 Review the edited details, and when you're ready, click **Proceed to On-Prem Configuration**.

Step 5 Configure the on-premises connectivity.

a) From the **Configure On-premise** screen, click **Download Configuration File**.

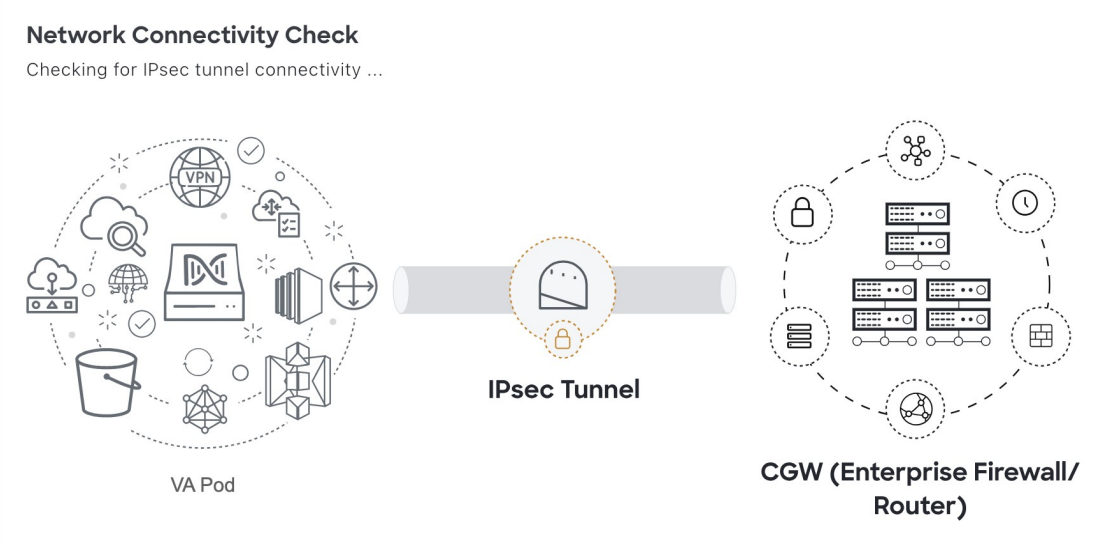
b) Forward this file to your network administrator to configure the on-premises-side IPsec tunnel.

The network administrator can make the necessary changes to this file and apply this configuration to your Enterprise firewall or router to bring up IPsec tunnels.

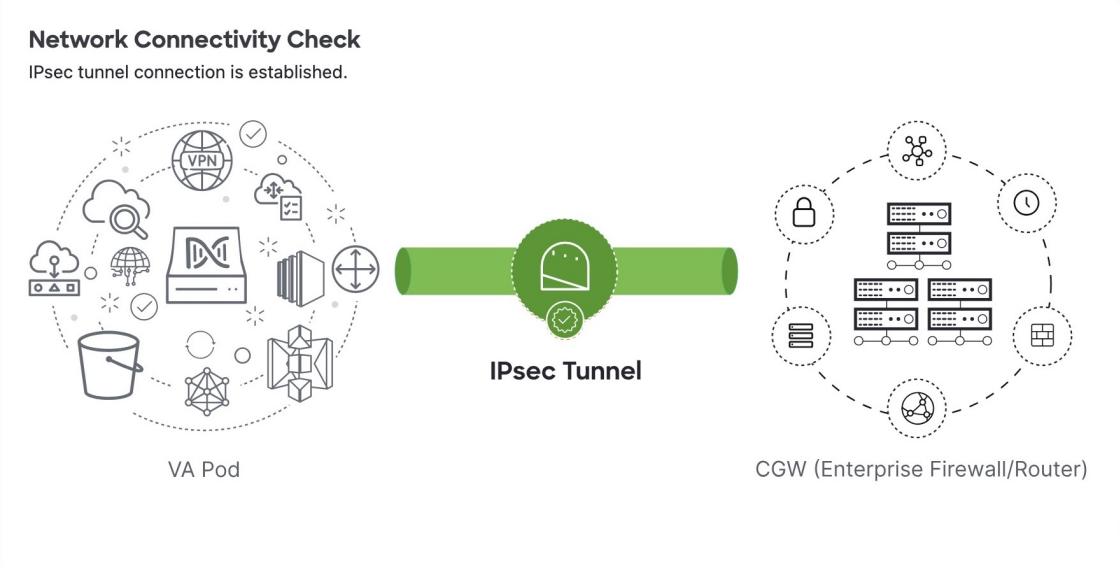
c) Click **Proceed to Network Connectivity Check**.

Step 6 Check the status of your network configuration.

When your network administrator is configuring the IPsec tunnel, the IPsec tunnel configuration status displays as not configured with a padlock icon.



When your network administrator completes the configuration and the IPsec tunnel configures successfully, the IPsec tunnel configuration status displays green with a success icon.



Step 7 (Optional) To return to the **Dashboard** pane, click **Go to Dashboard**.

Delete a VA Pod

You can delete a VA pod on Cisco Global Launchpad.

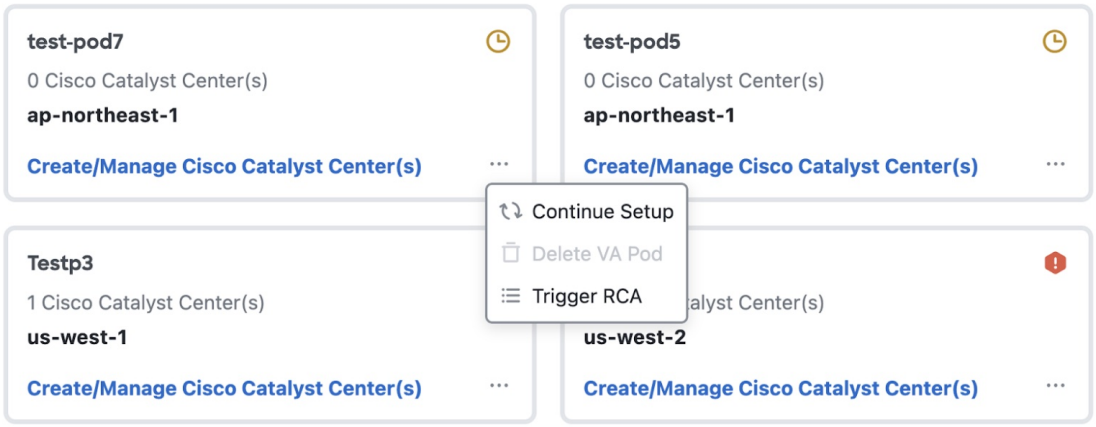
Note

- You can't delete a VA pod while you are deleting a Catalyst Center VA that is in the pod. You must wait for the Catalyst Center VA to be deleted first.
- Deleting a VA pod doesn’t delete the TGW because the TGW can be in use by a preexisting VPN or VPC.

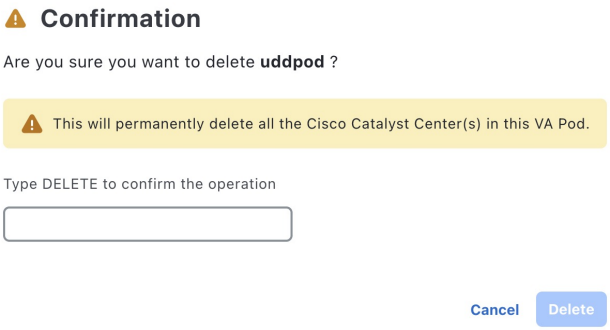
Step 1 On the **Dashboard** pane, locate the VA pod.

Step 2 In the bottom-right corner of the VA pod card, click the ellipsis icon (**...**) and choose **Delete VA Pod**.

Note If a Catalyst Center VA in a VA pod is in the process of being deleted, the **Delete VA Pod** option is not available.

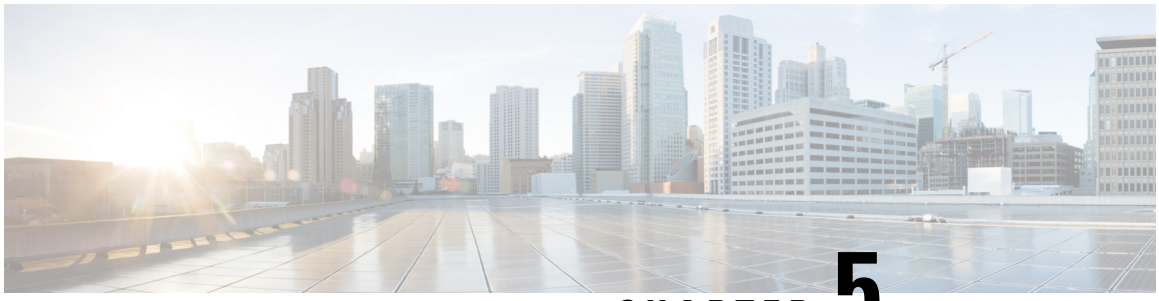


Step 3 In the **Confirmation** dialog box, in the text field, type **`DELETE`**.



Step 4 Click **Delete** to confirm that the deletion of the VA pod.

Deleting a VA pod takes approximately 20 to 40 minutes.



CHAPTER 5

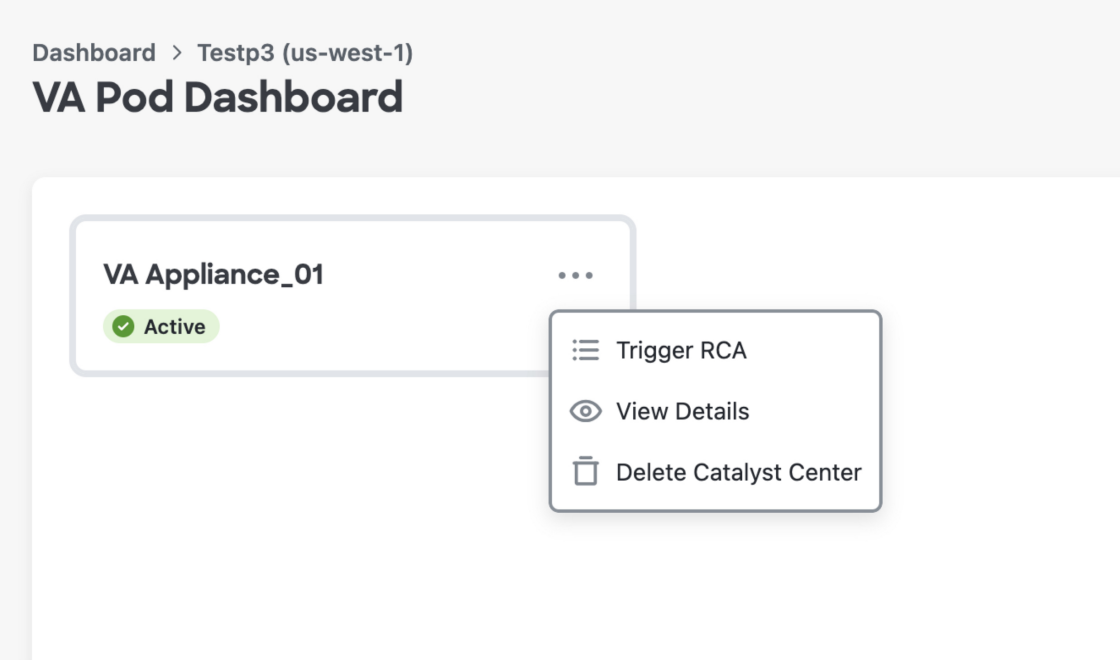
Manage Cisco Catalyst Center VAs

View Catalyst Center VA Details

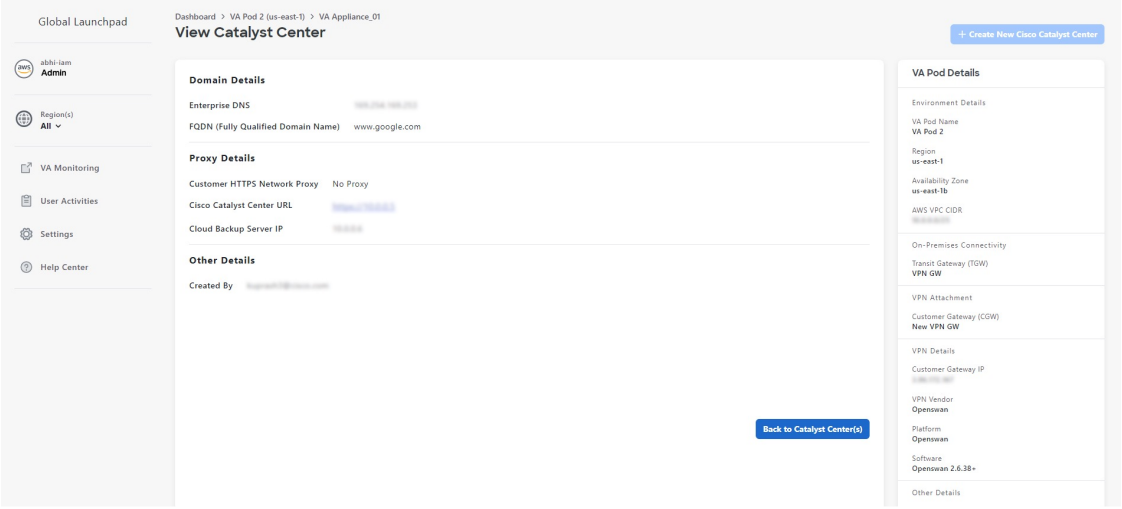
You can view Catalyst Center VA details in Cisco Global Launchpad.

Step 1 On the **Dashboard** pane, locate the VA pod containing the Catalyst Center VA you want to view, and in the VA pod card, click **Create/Manage Cisco Catalyst Center(s)**.

Step 2 In the bottom-right corner of the Catalyst Center VA card, click the ellipsis icon (**...**) and choose **View Details**.



Step 3 In the **Catalyst Center Virtual Appliance Details** window, view the following Catalyst Center VA details.



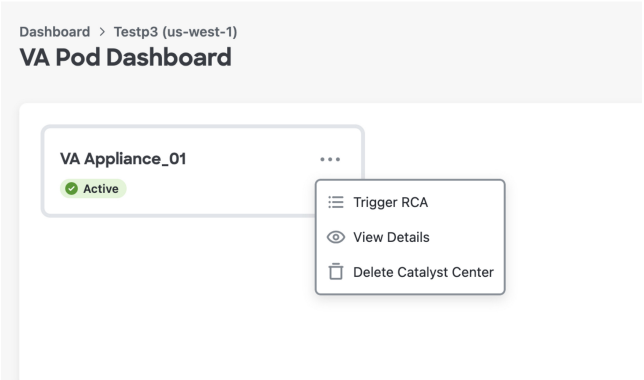
Step 4 (Optional) To exit this window, click **Back to Catalyst Center(s)**.

Delete an Existing Catalyst Center VA

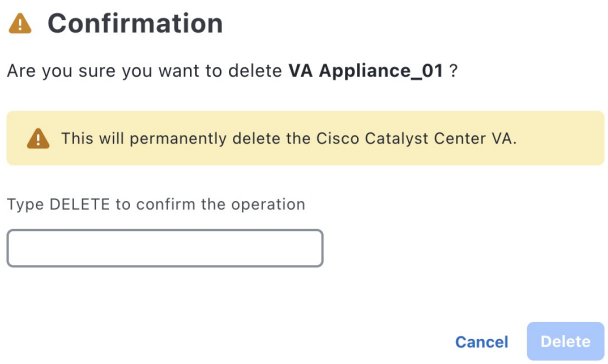
You can delete an existing Catalyst Center VA from Cisco Global Launchpad.

Step 1 On the **Dashboard** pane, locate the VA pod containing the Catalyst Center VA you want to delete, and in the VA pod card, click **Create/Manage Cisco Catalyst Center(s)**.

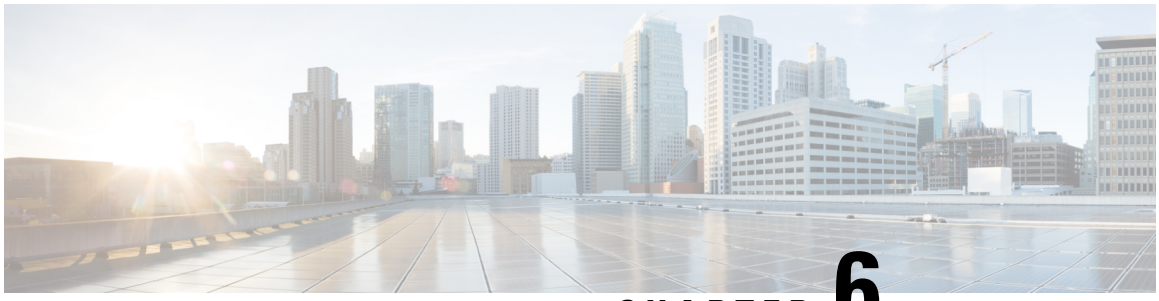
Step 2 In the bottom-right corner of the Catalyst Center VA card, click the ellipsis icon (**...**) and choose **Delete Cisco Catalyst Center**.



Step 3 In the **Confirmation** dialog box, in the text field, type **DELETE**.



Step 4 Click **Delete** to confirm that the deletion of the Catalyst Center VA.



CHAPTER 6

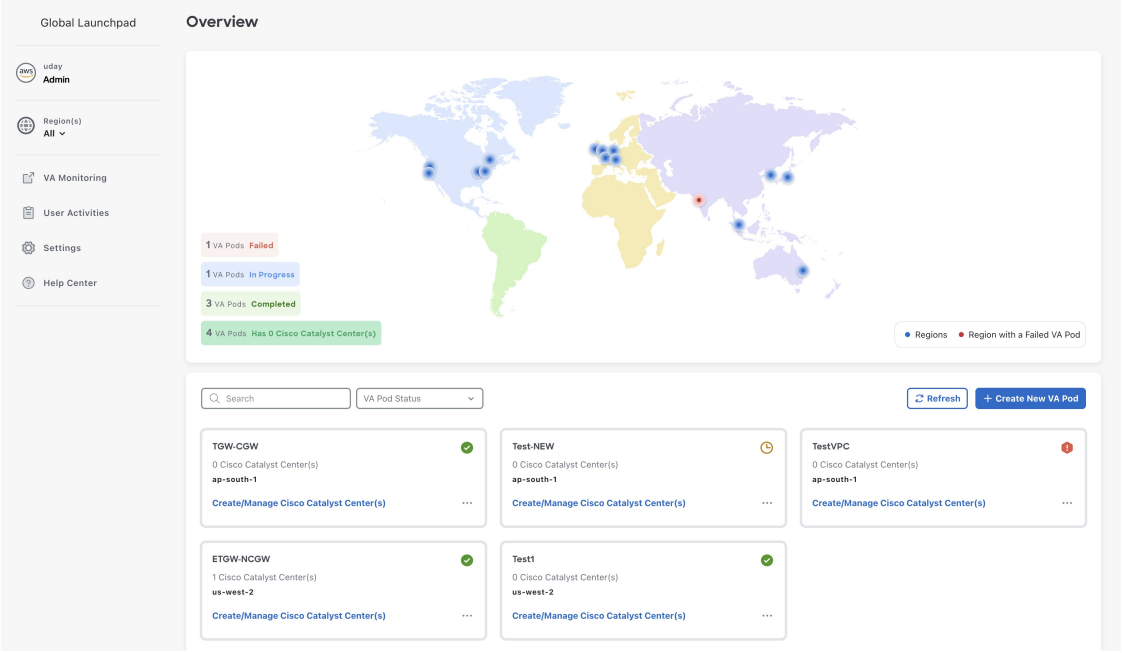
Understand the Dashboard and User Activity Details

View, Search, and Filter Dashboard Details

The **Global Dashboard** pane provides insights into all deployed VA pods and Catalyst Center VAs across all available regions.

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

At the top of the **Dashboard** is a global map that displays the available regions. On the map, a blue region icon indicates an available region. A red blinking region icon indicates a region with a failed VA pod creation. Below the map, a card is displayed for each VA pod in the selected region.



Step 2 From the left navigation pane, click the **Region** drop down list and check the check box next to the region or regions you want to view. Check the **Select All** check box to display information about all the regions.

Step 3 From the **Dashboard** pane, you can perform the actions described in the following table:

Action	Steps
Display region details.	**a.** On the map, hover your cursor over a region icon ( ). The region's name is displayed. **b.** On the map, click a region icon to select it. The region icon is displayed as selected ( ). Click additional region icons to include them in the following status highlights: • **VA Pods Failed**: Number of failed VA pods • **VA Pods In Progress**: Number of VA pods in the process of being created. • **VA Pods Completed**: Number of VA pods that have completed the creation process. • **VA Pods that have Catalyst Centers**: Number of VA pods that have Catalyst Center VAs and the total number of Catalyst Center VAs among them. VA pod information is displayed in the card view below the map.

Action	Steps
Search for a VA pod.	**a.** In the **Search by VA Pod Name** field, enter either the partial or full name of the VA pod. **b.** Press the **Enter** key. The **Dashboard** pane displays the VA pods in the card view below the map, and the status highlights are updated.
Filter by region and VA pod status.	From the **VA Pod Status** drop-down list, choose a VA pod status. The **Dashboard** pane displays the filter results based on the chosen status.
Update VA pod status.	To fetch the latest status of the VA pods, click **Refresh**. The **Dashboard** pane updates the status highlights and the information displayed in the VA pod card view.

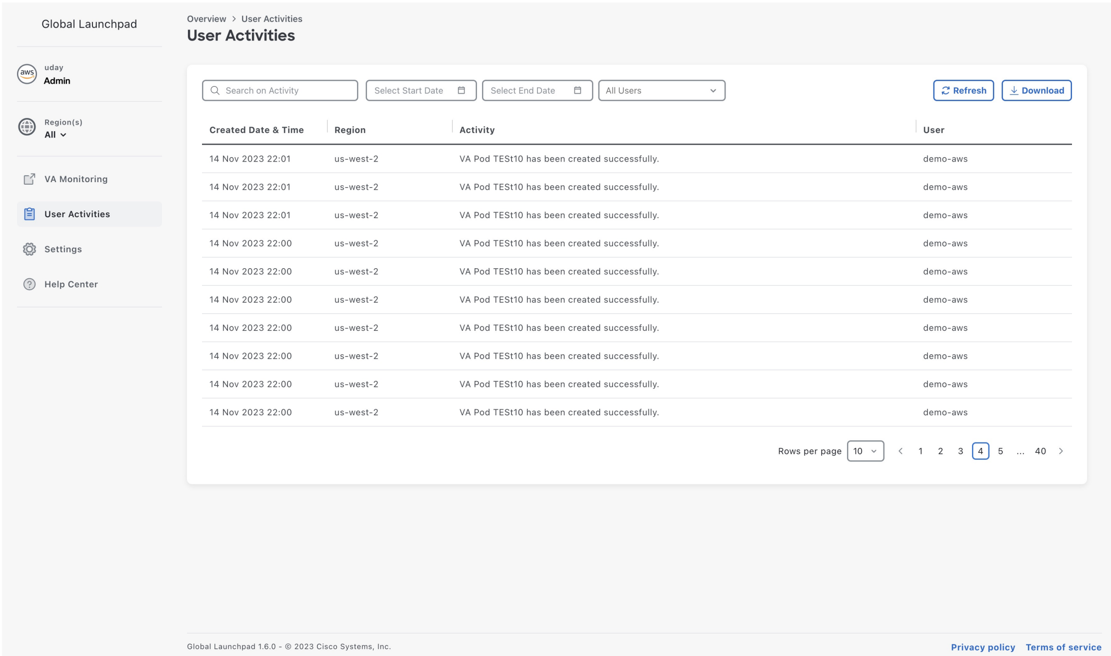
View, Search, and Filter User Activity Details

On the **User Activities** pane, you can view, search for, and filter all the user activity details for one or more chosen regions.

Step 1 From the left navigation pane, click the **Region** drop-down list and check the check box next to the region or regions that you want to view user activity details for. Check the **Select All** check box to display user activity information about all the regions.

Step 2 In the left navigation pane, click **User Activities**.

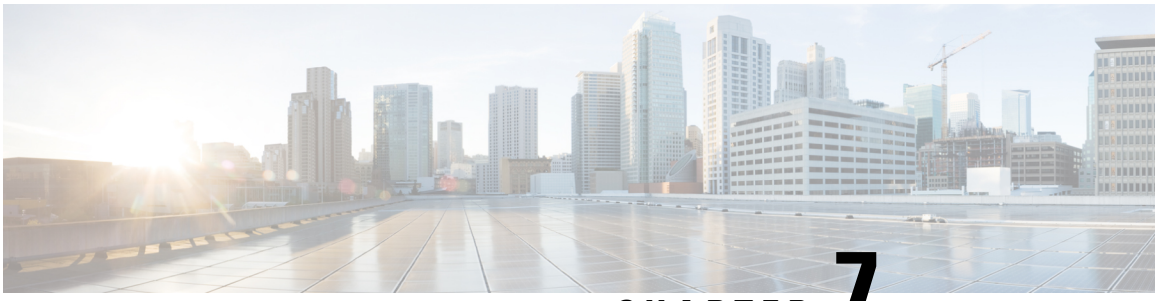
The **User Activities** pane displays in a table format.



Step 3 On the **User Activities** pane, you can view, search, and filter the data in the **User Activities** table by doing the following:

- To search for an activity, use the **Search on Activity** bar.
- To filter for an activity by date, click **Select Start Date** to choose a start date and click **Select End Date** to choose an end date.
- To filter for an activity by user, from the **All User** drop-down list, choose a user account.
- To update the data displayed, click **Refresh**.
- To download all the user activity data as a CSV file, click **Download**.

Step 4 To return to the **Dashboard** pane, click **Dashboard** in the breadcrumbs at the top of the **User Activities** pane.



CHAPTER 7

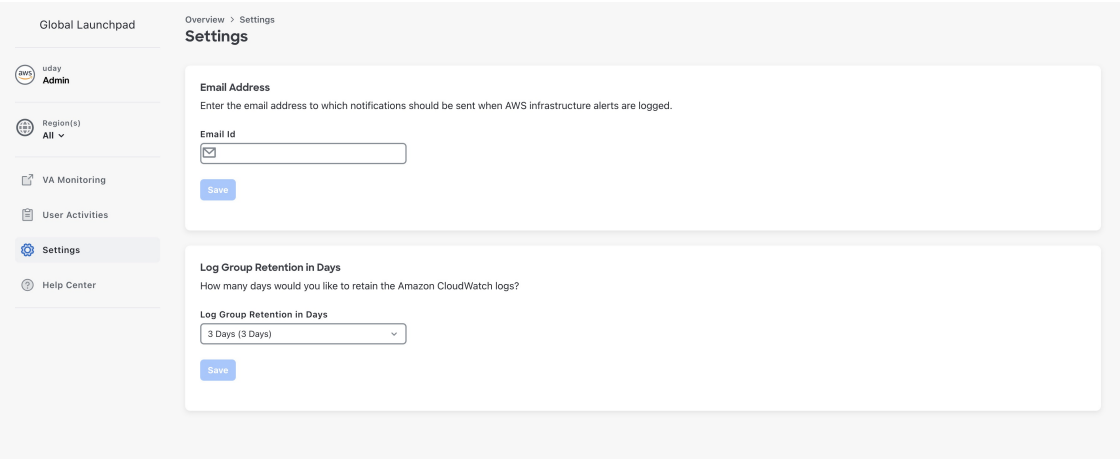
Manage Amazon Email Subscriptions, Logs, and Alarms

Subscribe to the Amazon SNS Email Subscription

To receive email notifications from Amazon Simple Notification System (SNS), you can subscribe to the Amazon SNS email subscription in Cisco Global Launchpad settings. Amazon SNS sends AWS alerts about deployed resources, changes, or resource over-utilization to the provided email.

Step 1 In the left navigation pane, click the settings icon ( ).

Step 2 In the **Settings** pane, in the **Email to notify** area, enter the preferred email address in the **Email ID** field.



When you update an email ID, the old email address is unsubscribed and the new email address is subscribed. Alerts about VA pods that are created after the email change are sent to the new email address. Alerts about existing VA Pods are not sent to the new email address.

If an existing user account has not confirmed their email subscription and updates their subscription with a new email address, both the old and new email addresses are subscribed and remain configured in Amazon SNS.

Note Multiple user accounts should not concurrently update their email ID. If this occurs, the latest updated email ID is used for email notification.

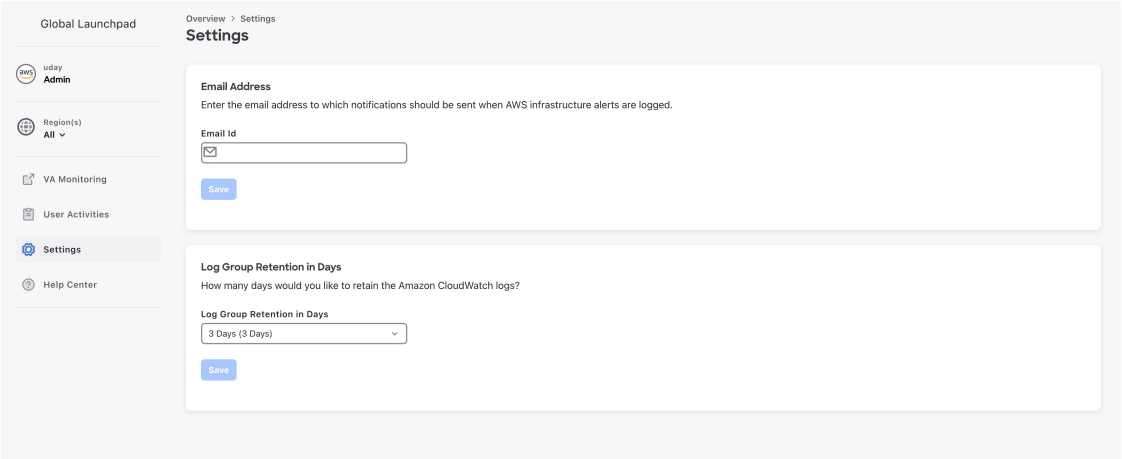
Step 3 Click **Save**.

Configure Log Retention

You can set the number of days to keep Amazon CloudWatch logs. By default, the logs are kept indefinitely.

Step 1 In the left navigation pane, click the settings icon ( ).

The **Settings** pane is displayed.



Step 2 Under **Log Group Retention In Days**, click the **Select Log Group Retention In Days** drop-down list and choose a retention period for the Amazon CloudWatch logs.

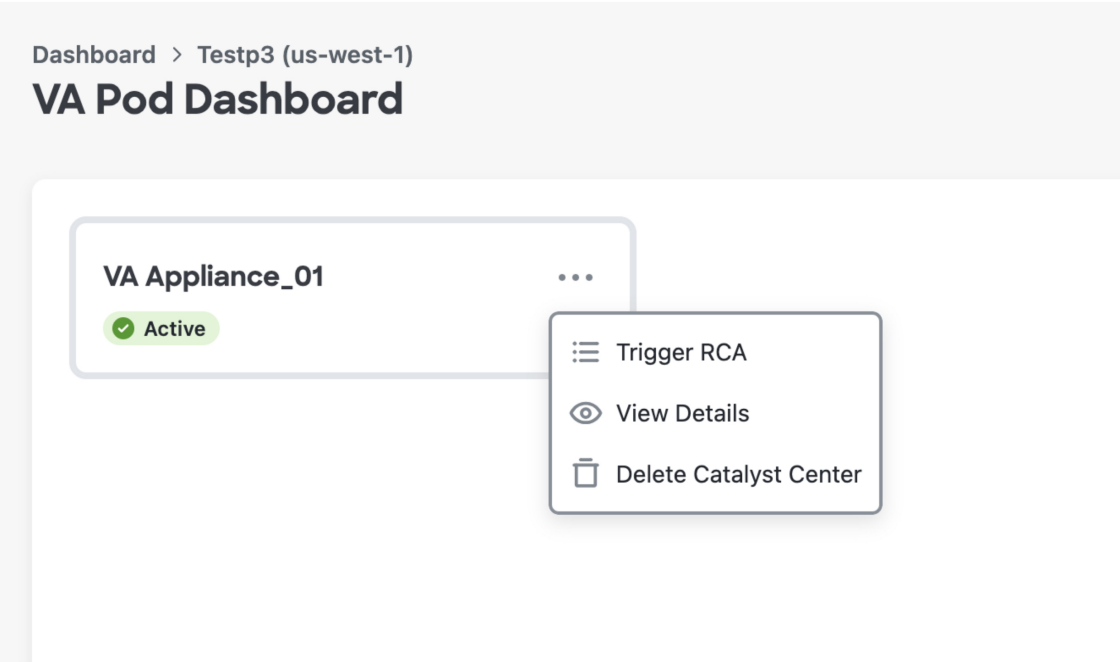
Step 3 Click **Save**.

Trigger a Root Cause Analysis (RCA)

On Cisco Global Launchpad, you can trigger a root cause analysis (RCA) to help you identify the root cause ofAWS infrastructure or Catalyst Center VA deployment issues. The RCA operation collects logs from AWS and stores them in the AWS S3 bucket. The RCA bundle includes backup logs, backend logs, Amazon CloudWatch alarm logs, and AWS resources and event logs.

Step 1 On the **Dashboard** pane, locate the VA pod containing the Catalyst Center VA that you want to trigger an RCA on, and in the VA pod card, click **Create/Manage Cisco Catalyst Center(s)**.

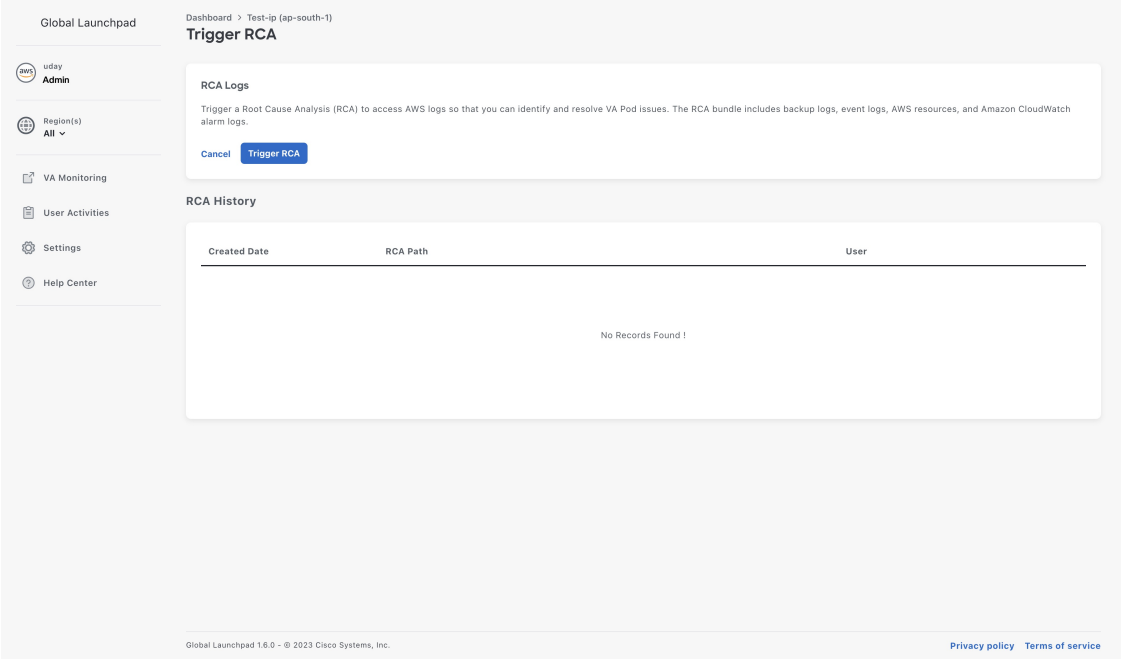
Step 2 In the bottom-right corner of the Catalyst Center VA card, click the ellipsis icon (**...**) and choose **Trigger RCA**.



Step 3 In the **Trigger RCA** window, in the **RCA Logs** area, click **Trigger RCA** to gather and bundle the AWS logs.

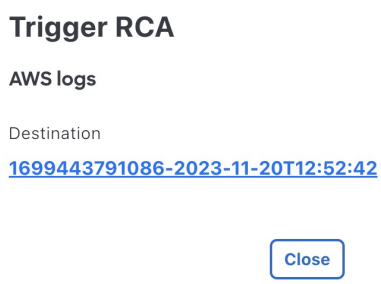
Cisco Global Launchpad uses AWS Config and Amazon CloudWatch to record, assess, and audit the used resources.

Note In the **Trigger RCA** window, if previous RCAs have been performed, you can view the last five successfully triggered RCAs in the **RCA Logs** table.



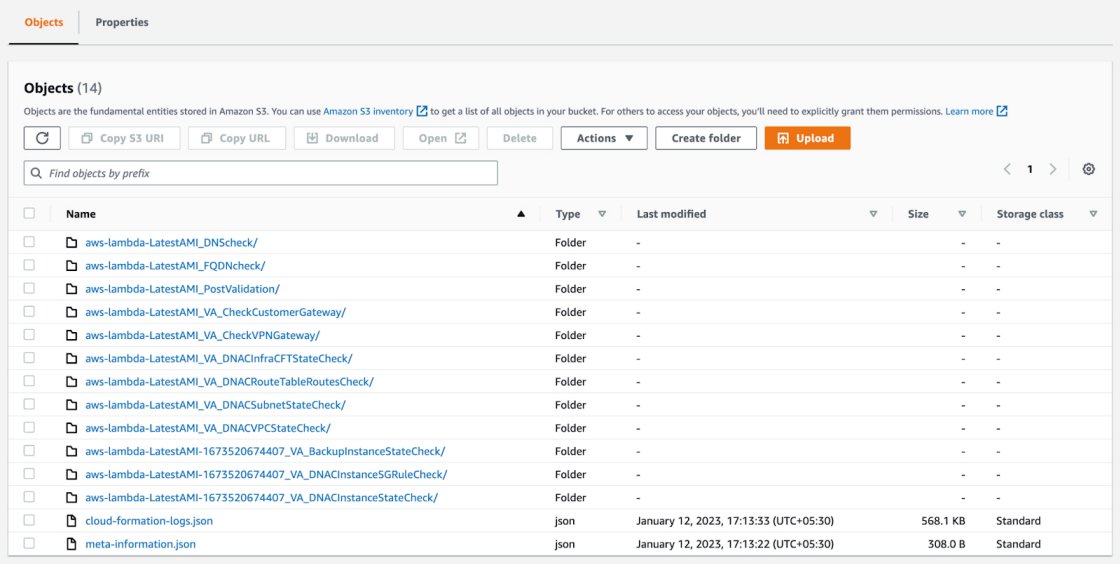
This process takes a few minutes.

After the process completes, the URL to the S3 bucket, where the AWS logs are located, is displayed.



Step 4 Under **Destination**, click the URL displayed to go to the AWS S3 bucket.

The AWS console opens in a new browser window. After you log in to AWS, the contents of the S3 bucket are displayed.



Depending on the resources created, the number of log groups vary.

AWS Config and Audit Log Details

AWS Config is an AWS tool that continually assesses, monitors, and evaluates resource configurations to aid in operational troubleshooting by correlating configuration changes to specified events and states. Cisco Global Launchpad uses AWS Config to audit the configuration. When AWS Config detects a change in the configuration, Cisco Global Launchpad generates an email notifying you that configuration changes have taken place.

View Amazon CloudWatch Alarms

Cisco Global Launchpad uses Amazon CloudWatch alarms to monitor resource usage and check for unusual behavior. The AWS RCA feature also uses Amazon CloudWatch alarms.

If a threshold is met, alerts are sent to the email ID that you configured during your first log in to Cisco Global Launchpad or to the email ID in the user settings, if it was updated. For more information, see Subscribe to the Amazon SNS Email Subscription, on page 43.

Note

- The Amazon CloudWatch alarms for lambda functions remain in the insufficient data state unless a failure occurs in the corresponding lambda function execution. When a lambda function fails, Amazon CloudWatch gathers the metrics and triggers the alarm. The threshold for all lambda alarms is one, so Amazon CloudWatch can capture alerts if there are any failure.
- For some alarms, like S3, the metrics are only reported once per day at midnight in Greenwich Mean Time (GMT). So it may take 24 to 48 hours for the dashboard metrics to update, which is an expected behavior.

Before you begin

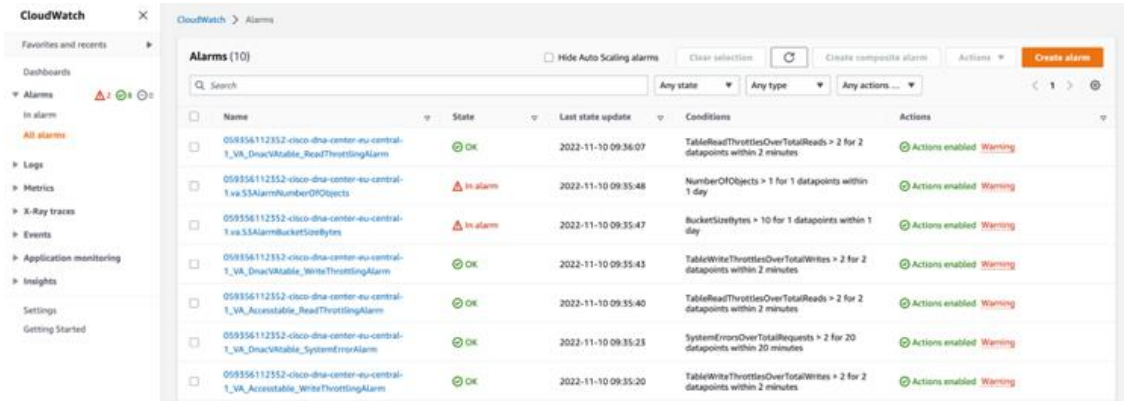
Make sure you successfully configured your AWS account. For more information, see the *Cisco Catalyst Center on AWS Deployment Guide*.

Step 1 Log in to the AWS console.

The AWS console is displayed.

Step 2 From the AWS dashboard, click **CloudWatch** > **Alarms** > **All Alarms**.

The **Alarms** page displays the status of all the alarms.

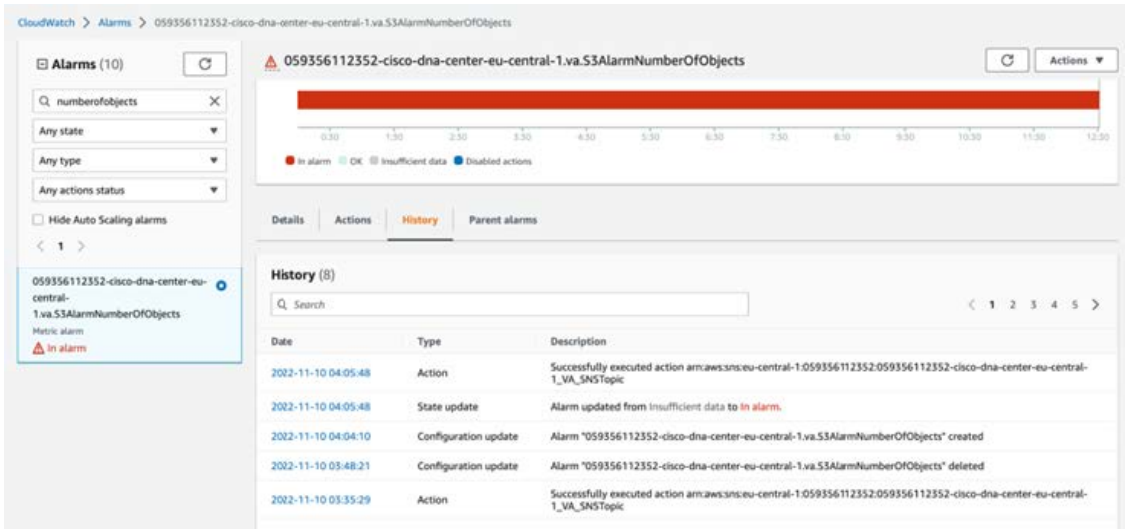


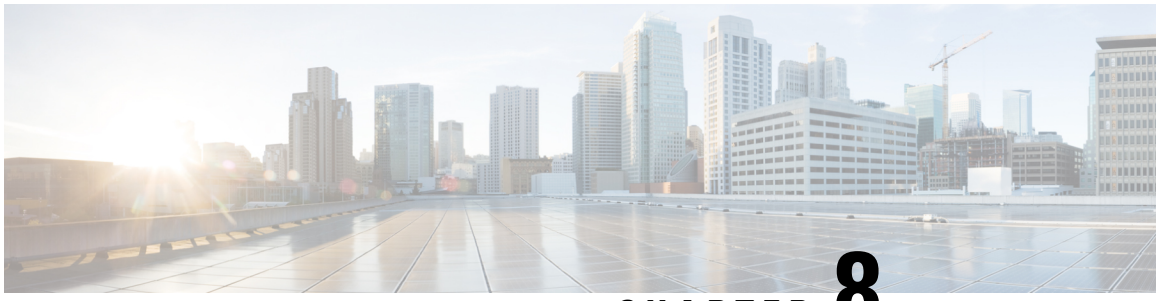
Step 3 On the **Alarms** page, enter the environment name used to deploy Catalyst Center in the **Search** field.

Alarms pertaining to the Catalyst Center instance with the specified environment name are displayed.

Step 4 Click the name of an alarm.

Details about the alarm are displayed in the **Details** tab. To view other information, click the **Actions**, **History**, or **Parent alarms** tabs.





CHAPTER 8

Backup and Restore

About Backup and Restore

Use the backup and restore functions to create backup files and restore them to a different appliance. With Catalyst Center VAs, there are two methods to back up and restore data:

- Back up data from a Catalyst Center hardware appliance and restore the data to a Catalyst Center VA.
- Back up data from one Catalyst Center VA and restore the data to another Catalyst Center VA.

Backup and Restore—Hardware Appliance to VA

This procedure provides a high-level overview of how you can back up the data from a Catalyst Center hardware appliance and restore it to a Catalyst Center VA. For detailed instructions, see the "Backup and Restore" chapter in the *Cisco DNA Center Administrator Guide, Release 2.3.5*.

Before you begin

Make sure that the hardware appliance used for the backup is a 44-core Catalyst Center appliance.

Step 1 Back up the data from the Catalyst Center hardware appliance.

Make sure that the backup server is connected to Catalyst Center through a VPN.

Step 2 Create a Catalyst Center VA. For more information, see "Create a New Catalyst Center VA" in the *Cisco Catalyst Center on AWS Deployment Guide*.

Make sure the Catalyst Center VA is up and running.

Step 3 Connect the Catalyst Center VA to the backup server from Step 1.

Make sure that the backup server is reachable from the Catalyst Center VA.

Step 4 Configure the backup server on the Catalyst Center VA.

Step 5 Restore the data on to the Catalyst Center VA.

Backup and Restore—VA to VA

This procedure provides a high-level overview of how you can back up the data from one (source) Catalyst Center VA and restore it to another (target) Catalyst Center VA. For detailed instructions, see the "Backup and Restore" chapter in the *Cisco DNA Center Administrator Guide, Release 2.3.5*.

Before you begin

- Make sure that you successfully deployed two Catalyst Center VAs with Cisco Global Launchpad, AWS CloudFormation, or AWS Marketplace. For more information, see *Cisco Catalyst Center on AWS Deployment Guide*.
- Make sure that both Catalyst Center VAs are up and running.
- Make sure that the backup server is connected to the source Catalyst Center VA through a VPN.
- Make sure that the backup server is reachable from the target Catalyst Center VA.

Step 1 Back up the data from the source Catalyst Center VA to a backup server.

Step 2 Bring up the target Catalyst Center VA that you want to restore the data to.

Step 3 Connect the target Catalyst Center VA to the backup server. (See Step 1.)

Step 4 Configure the backup server on the target Catalyst Center VA.

Step 5 Restore the data to the target Catalyst Center VA.