CYBERCLOAK CLOUD DEPLOYMENT GUIDE

AWS edition

Abstract

The scope of this document is to guide the intended audience to deploy and log into the CyberCloak Cloud application within an aws environment. Deploying the application incorrectly could lead to unintended outcomes and this guide ensures the deployment is successful.

Blue Ridge Networks

Table of Contents

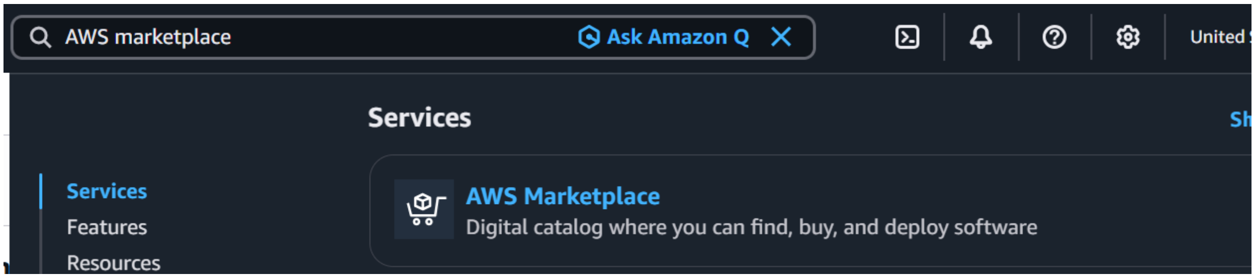
Subscribing to CyberCloak

Preface

The prerequisites that are needed for a successful deployment is having the correct permissions and access to the needed services within aws.

Initial setup

CyberCloak Cloud will be installed via the AWS service **AWS Marketplace.** From the main console page in the search bar type AWS Marketplace to find and open the service.

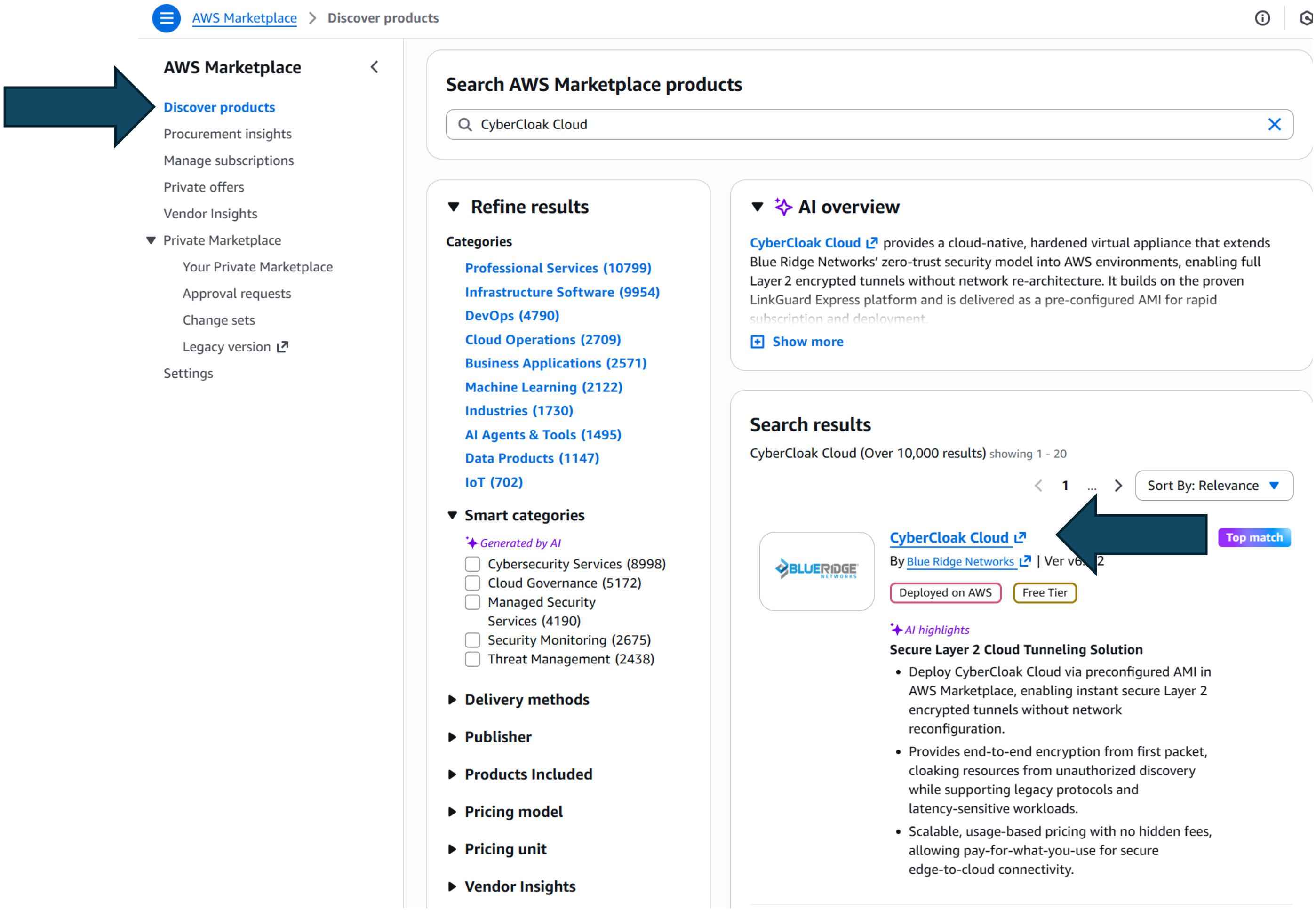


AWS marketplace

AWS Marketplace

Digital catalog where you can find, buy, and deploy software

Within the Marketplace on the left navigation pane select **Discover products** and search for **CyberCloak Cloud** and select the product.



AWS Marketplace > Discover products

AWS Marketplace

- Discover products
- Procurement insights
- Manage subscriptions
- Private offers
- Vendor Insights
- ▼ Private Marketplace
  - Your Private Marketplace
  - Approval requests
  - Change sets
  - Legacy version
- Settings

Search AWS Marketplace products

CyberCloak Cloud

▼ Refine results

Categories

- Professional Services (10799)
- Infrastructure Software (9954)
- DevOps (4790)
- Cloud Operations (2709)
- Business Applications (2571)
- Machine Learning (2122)
- Industries (1730)
- AI Agents & Tools (1495)
- Data Products (1147)
- IoT (702)

▼ Smart categories

Generated by AI

- □ Cybersecurity Services (8998)
- □ Cloud Governance (5172)
- □ Managed Security Services (4190)
- □ Security Monitoring (2675)
- □ Threat Management (2438)

- ▶ Delivery methods
- ▶ Publisher
- ▶ Products Included
- ▶ Pricing model
- ▶ Pricing unit
- ▶ Vendor Insights

▼ AI overview

CyberCloak Cloud provides a cloud-native, hardened virtual appliance that extends Blue Ridge Networks' zero-trust security model into AWS environments, enabling full Layer 2 encrypted tunnels without network re-architecture. It builds on the proven LinkGuard Express platform and is delivered as a pre-configured AMI for rapid subscription and deployment.

Show more

Search results

CyberCloak Cloud (Over 10,000 results) showing 1 - 20

< 1 ... > Sort By: Relevance ▼

CyberCloak Cloud — Top match

By Blue Ridge Networks | Ver v6. 2

Deployed on AWS | Free Tier

AI highlights

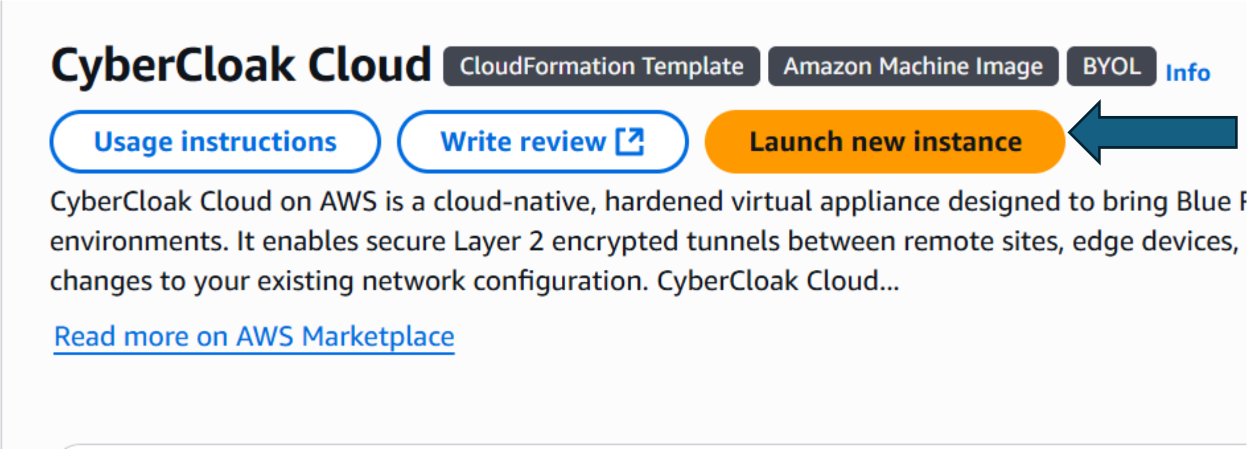
Secure Layer 2 Cloud Tunneling Solution

- Deploy CyberCloak Cloud via preconfigured AMI in AWS Marketplace, enabling instant secure Layer 2 encrypted tunnels without network reconfiguration.
- Provides end-to-end encryption from first packet, cloaking resources from unauthorized discovery while supporting legacy protocols and latency-sensitive workloads.
- Scalable, usage-based pricing with no hidden fees, allowing pay-for-what-you-use for secure edge-to-cloud connectivity.

On the Next screen select the View purchase options which will lead to the licensing page. Currently licensing is designed around a **Bring Your Own License (BYOL)** model. It will be free to accept on AWS Marketplace and will be purchased directly through Blueridge Networks. After accepting the offer the application can now be deployed.

Deploying CyberCloak

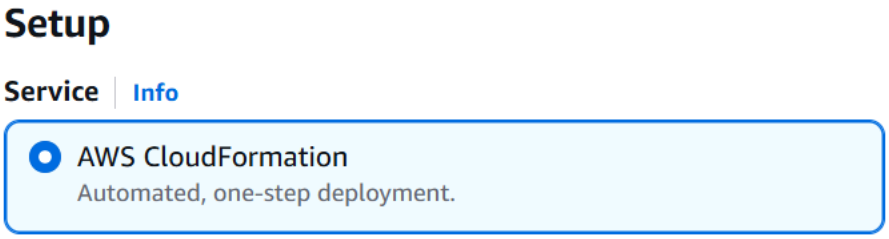
Under Manage subscriptions on the left navigation pane CyberCloak Cloud should appear and then on the top right select the Launch new instance on the right.



CyberCloak Cloud

CyberCloak Cloud on AWS is a cloud-native, hardened virtual appliance designed to bring Blue F
environments. It enables secure Layer 2 encrypted tunnels between remote sites, edge devices,
changes to your existing network configuration. CyberCloak Cloud...

Once selected AWS will prompt for the setup information needed to deploy the application. Currently CloudFormation is highly recommended, since it will run all the necessary steps needed for a successful installation. It is not recommended to run the setup through Amazon EC2.

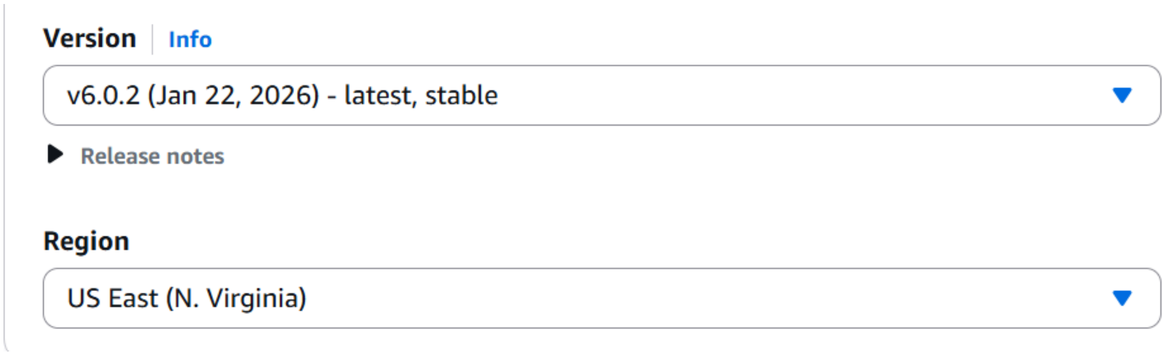


Setup

Service

● AWS CloudFormation
Automated, one-step deployment.

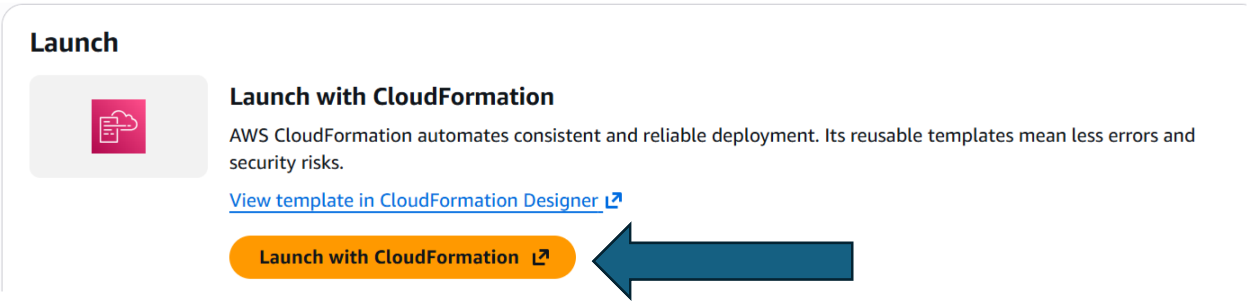
Select the Version, the default is the latest stable release.
Select the Region that the application would be deployed to.



Version: v6.0.2 (Jan 22, 2026) - latest, stable

Region: US East (N. Virginia)

Then select the Launch with Cloud formation button on the bottom



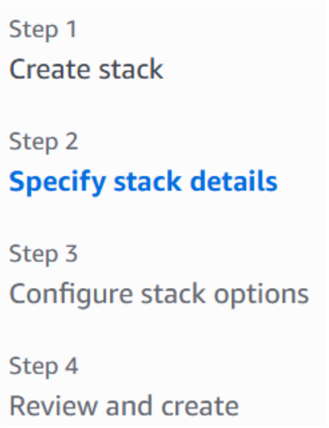
Launch

Launch with CloudFormation

AWS CloudFormation automates consistent and reliable deployment. Its reusable templates mean less errors and security risks.

View template in CloudFormation Designer
Launch with CloudFormation

Cloud formation will have 4 steps to set up before it can be run. They are shown in the image below.



Step 1
Create stack

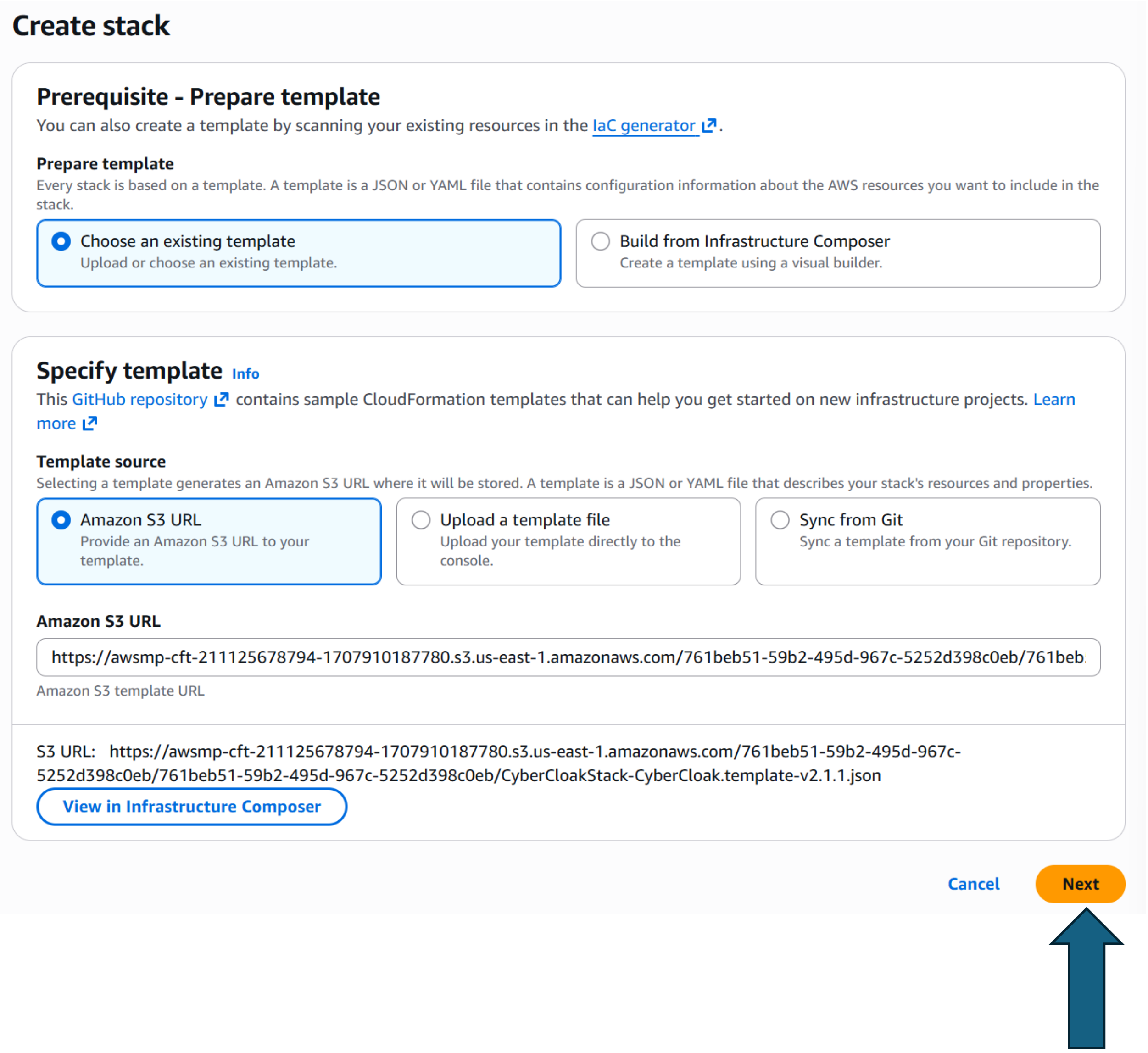
Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review and create

Step 1 Create Stack

Within the CloudFormation configuration all the defaults should be left alone and just continue by pressing the next button.



Create stack

Prerequisite - Prepare template

You can also create a template by scanning your existing resources in the IaC generator.

Prepare template

Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

● Choose an existing template
Upload or choose an existing template.

○ Build from Infrastructure Composer
Create a template using a visual builder.

Specify template Info

This GitHub repository contains sample CloudFormation templates that can help you get started on new infrastructure projects. Learn more

Template source

Selecting a template generates an Amazon S3 URL where it will be stored. A template is a JSON or YAML file that describes your stack's resources and properties.

● Amazon S3 URL
Provide an Amazon S3 URL to your template.

○ Upload a template file
Upload your template directly to the console.

○ Sync from Git
Sync a template from your Git repository.

Amazon S3 URL

https://awsmp-cft-211125678794-1707910187780.s3.us-east-1.amazonaws.com/761beb51-59b2-495d-967c-5252d398c0eb/761beb

Amazon S3 template URL

S3 URL: https://awsmp-cft-211125678794-1707910187780.s3.us-east-1.amazonaws.com/761beb51-59b2-495d-967c-5252d398c0eb/761beb51-59b2-495d-967c-5252d398c0eb/CyberCloakStack-CyberCloak.template-v2.1.1.json

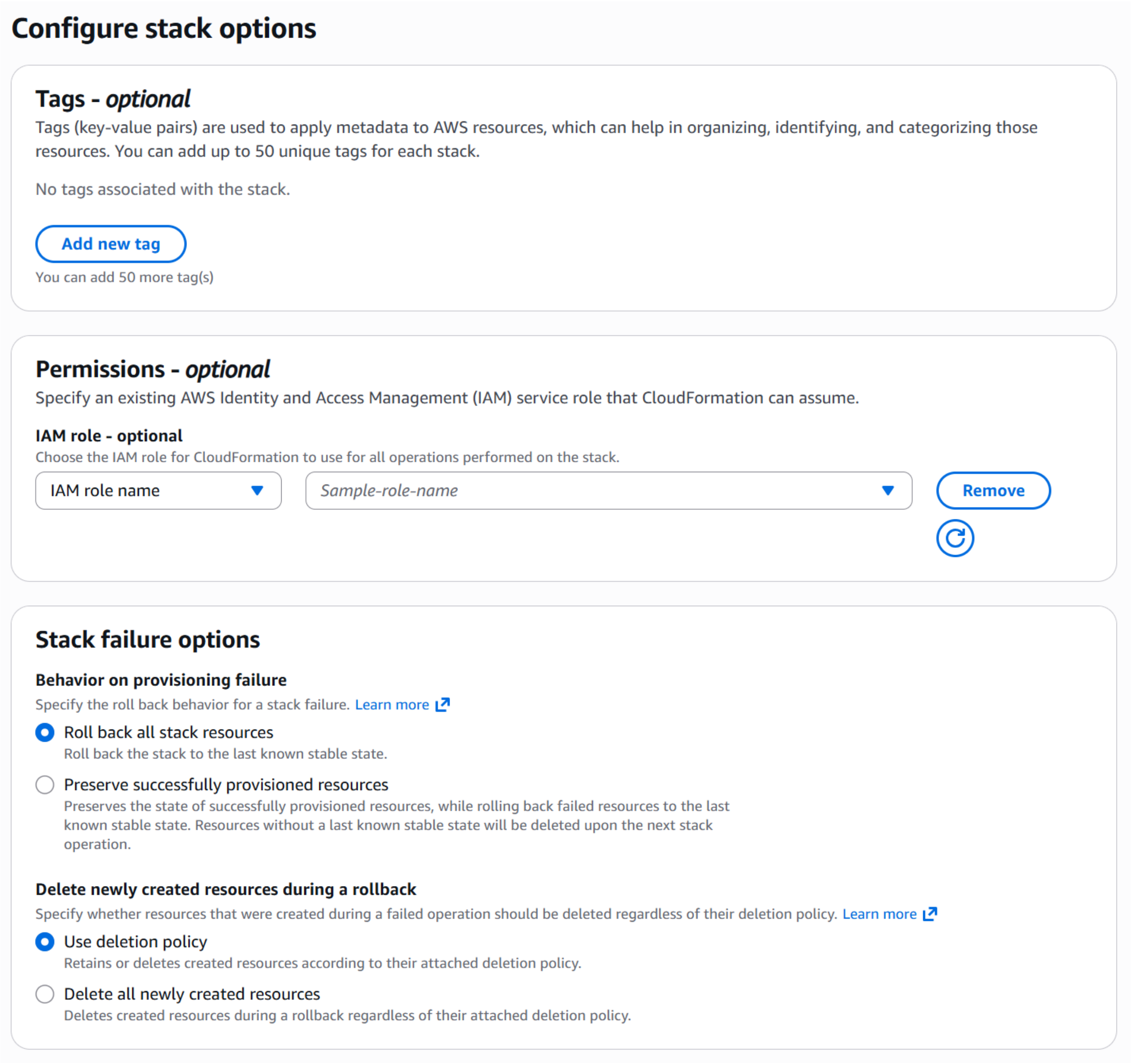
Step 2 Specify Stack Details

Continue filling out the information needed for the script here including

Parameter	*Expected value*	*Description*
Stack Name	String	Name of the stack
Allowed CyberCloak CIDR	IP range in String Format	CIDR for all allowed CyberCloak clients. This is likely 0.0.0.0/0 to allow access from everywhere and CyberCloak will authenticate all access.
Allowed Management CIDR	IP range in String Format	Initial CIDR allowed to access the CyberCloak management UI.
Deployment Tag	String	Default value used for the deployment
Enclave Address	IP range in String Format	Initial CIDR for the Enclave Bridge within the CyberCloak server.
Image ID	Marketplace AMI	This is the alias of the Marketplace AMI that will be deployed as part of this stack
Instance Type	EC2 Instance Type	EC2 instance type to use for CyberCloak instances - default is t3.small.

Step 3 Configure stack options

Options on this page should be left to their default options unless there are changes the administrator deploying the application deems necessary with permission or roll back/ deletion policies. Standard deployment is to leave the default settings, Check the box at the bottom acknowledging IAM resource creation and select Next.



Configure stack options

Tags - *optional*

Tags (key-value pairs) are used to apply metadata to AWS resources, which can help in organizing, identifying, and categorizing those resources. You can add up to 50 unique tags for each stack.

No tags associated with the stack.

You can add 50 more tag(s)

Permissions - *optional*

Specify an existing AWS Identity and Access Management (IAM) service role that CloudFormation can assume.

IAM role - optional

Choose the IAM role for CloudFormation to use for all operations performed on the stack.

IAM role name ▼ | *Sample-role-name* ▼

Stack failure options

Behavior on provisioning failure

Specify the roll back behavior for a stack failure. Learn more

● Roll back all stack resources
Roll back the stack to the last known stable state.

○ Preserve successfully provisioned resources
Preserves the state of successfully provisioned resources, while rolling back failed resources to the last known stable state. Resources without a last known stable state will be deleted upon the next stack operation.

Delete newly created resources during a rollback

Specify whether resources that were created during a failed operation should be deleted regardless of their deletion policy. Learn more

● Use deletion policy
Retains or deletes created resources according to their attached deletion policy.

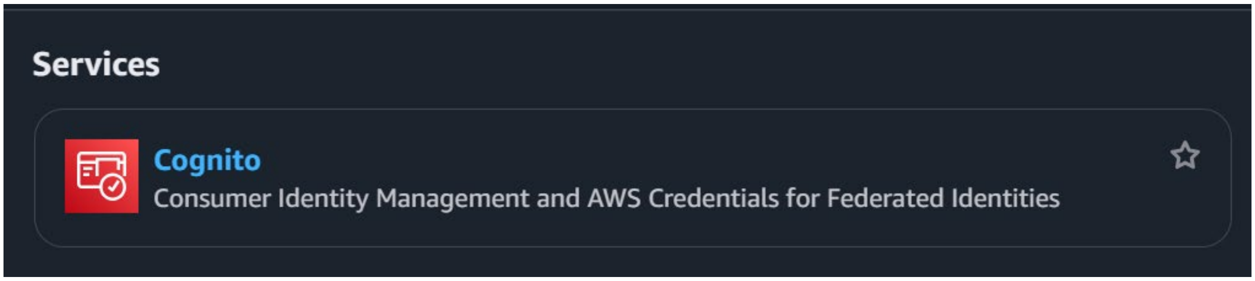
○ Delete all newly created resources
Deletes created resources during a rollback regardless of their attached deletion policy.

Step 4 Review and Create

As the step states Review all the settings confirm everything is correct and click submit. CloudFormation will then go through and deploy the application, and it should be available in EC2 momentarily.

Credential Creation

Before we can connect to CyberCloak an account will need to be created within Cognito. Search for Cognito in the AWS search bar and select Cognito.

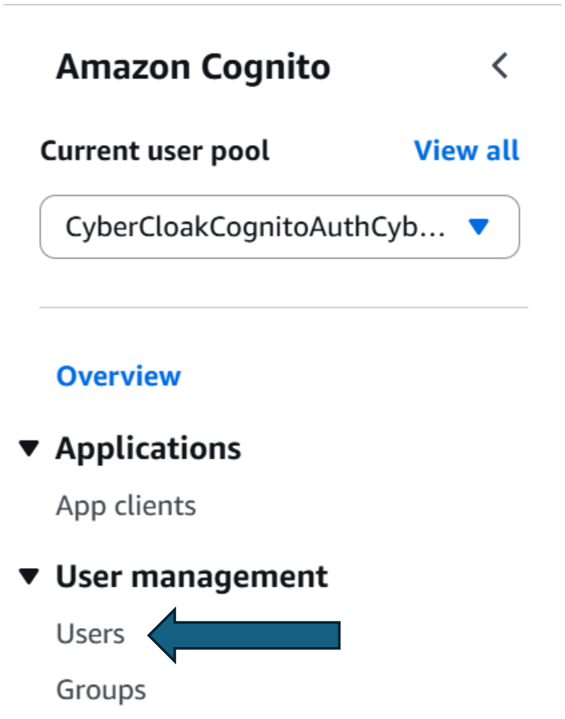


Services

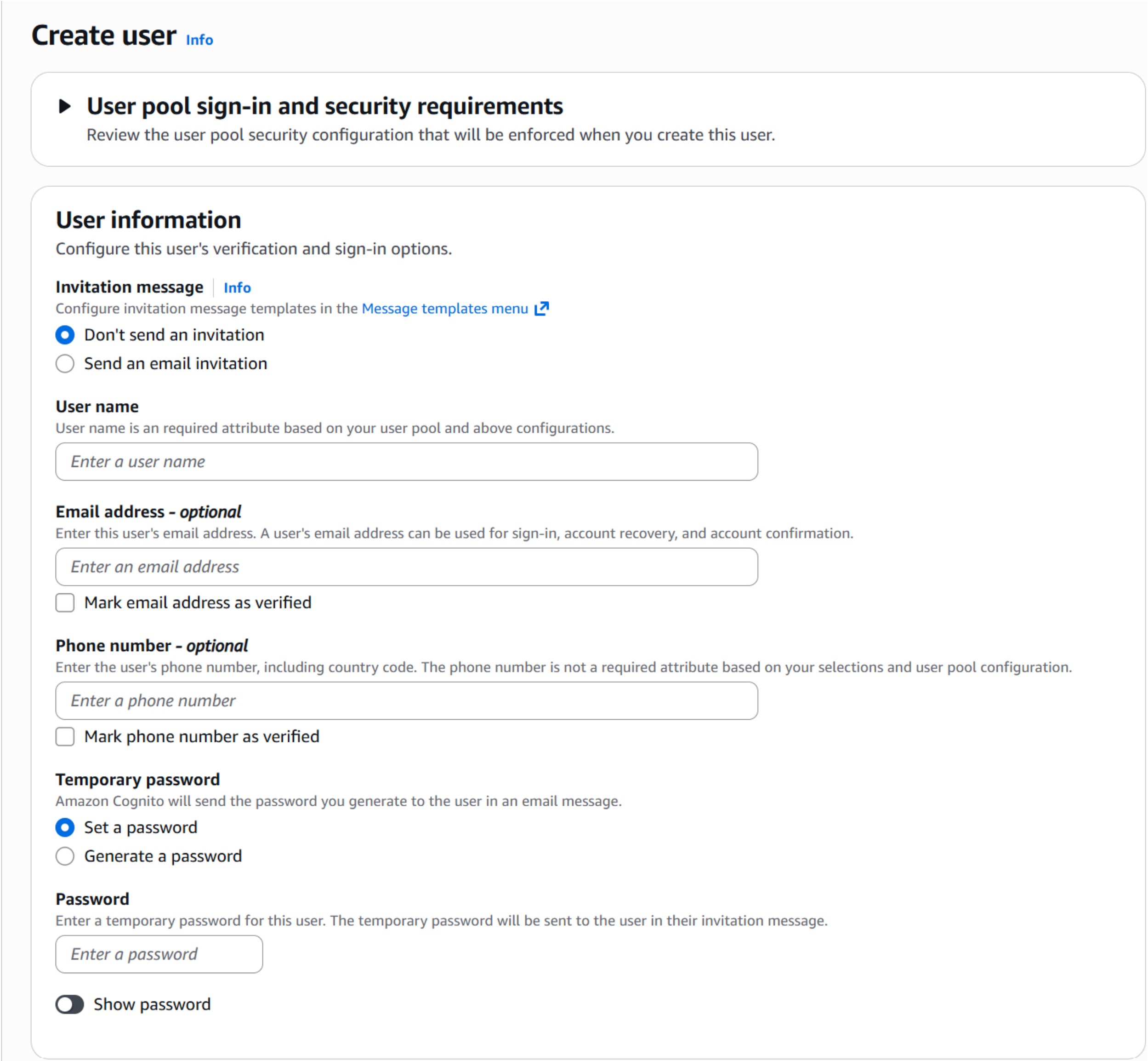
Cognito

Consumer Identity Management and AWS Credentials for Federated Identities

Once in Cognito a user pool should have been created by CloudFormation. Select the pool and then on the left navigation pane under User management select Users. Then click the create user button.



Create the username and a temporary password. All the other fields can be left to their defaults.



Create user Info

▶ **User pool sign-in and security requirements**

Review the user pool security configuration that will be enforced when you create this user.

User information

Configure this user's verification and sign-in options.

Invitation message | Info

Configure invitation message templates in the Message templates menu

● Don't send an invitation

○ Send an email invitation

User name

User name is an required attribute based on your user pool and above configurations.

Enter a user name

Email address - *optional*

Enter this user's email address. A user's email address can be used for sign-in, account recovery, and account confirmation.

Enter an email address

□ Mark email address as verified

Phone number - *optional*

Enter the user's phone number, including country code. The phone number is not a required attribute based on your selections and user pool configuration.

Enter a phone number

□ Mark phone number as verified

Temporary password

Amazon Cognito will send the password you generate to the user in an email message.

● Set a password

○ Generate a password

Password

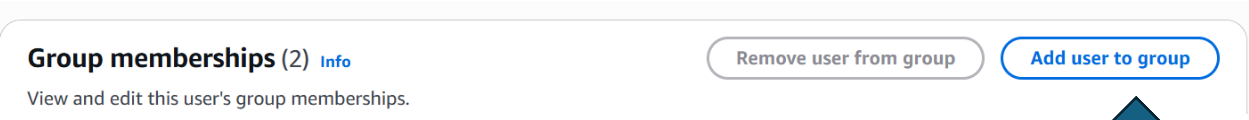
Enter a temporary password for this user. The temporary password will be sent to the user in their invitation message.

Enter a password

○ Show password

Once the User is created, add the necessary groups for access.

Select the Add user to a group button. Select the groups the user should be apart of and then click Add.



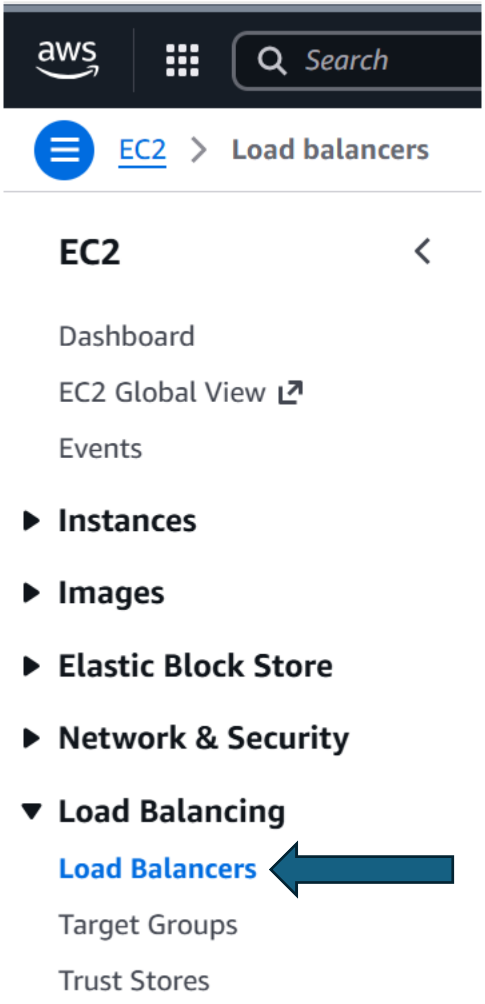
Group memberships (2) Info

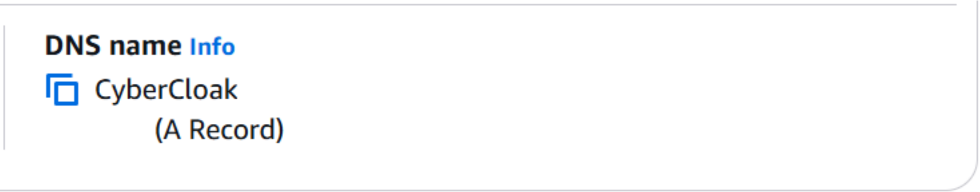
View and edit this user's group memberships.

The user should now be able to log into the CyberCloak application.

Connecting to CyberCloak

Once CloudFormation successfully deploys the application, and the EC2 instance is created. On the left navigation pane select Load Balancer. Select the newly created instance and in the menu below copy the **DNS name** value and paste it into a new web URL tab. This is how the application will be accessed. In the image below the DNS name A record would be the name created in step 2 of cloud formation. The Name *CyberCloak* is being used as a placeholder.



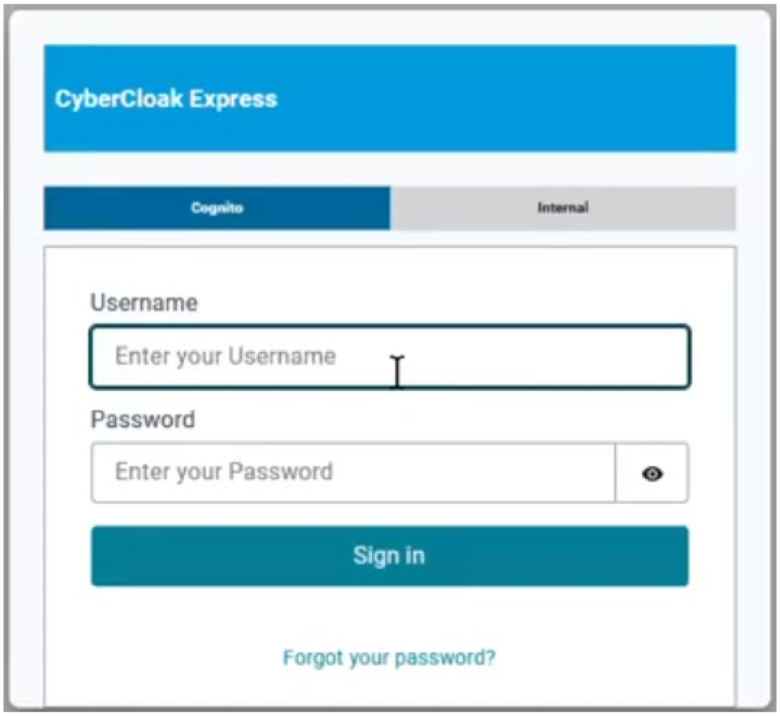


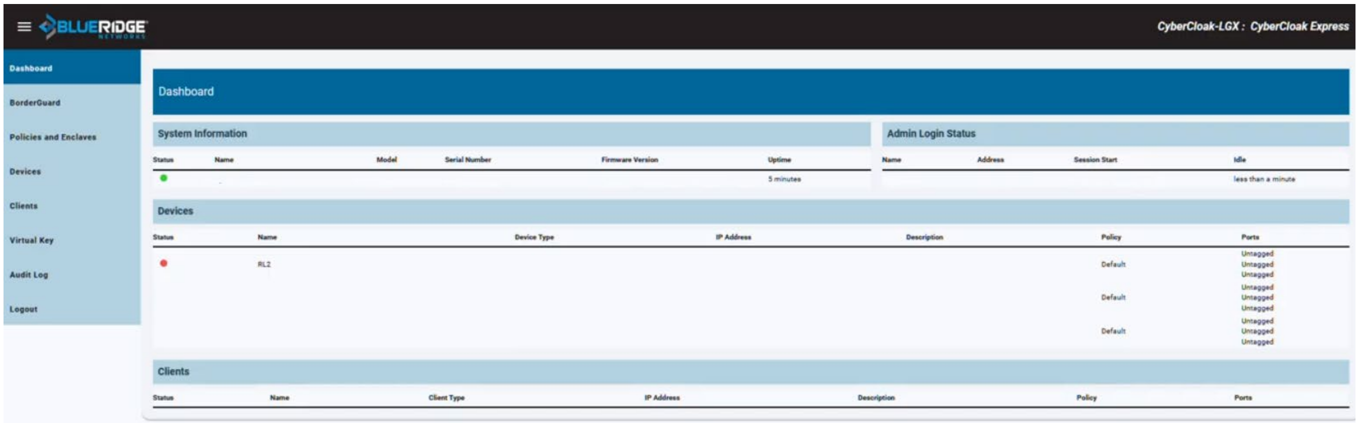
DNS name Info

CyberCloak
(A Record)

Note: Always include "https://" at the beginning of the address. "http://" is not allowed.

The user account created in cognito should be able to log in now and once logged in will be prompted to change their password and set up their preferred 2fa application by scanning the QR code with their Phone and typing in the code provided by their 2fa provider. Once logged in the user will be presented with the application dashboard.





Dashboard

System Information

Status	Name	Model	Serial Number	Firmware Version	Uptime
●					5 minutes

Admin Login Status

Name	Address	Session Start	Idle
			less than a minute

Devices

Status	Name	Device Type	IP Address	Description	Policy	Ports
●	RL2				Default	Untagged Untagged Untagged
					Default	Untagged Untagged Untagged
					Default	Untagged Untagged Untagged

Clients

Status	Name	Client Type	IP Address	Description	Policy	Ports