

Implementation Guide

Netskope AWS Control Tower Integration

Cloud Security Posture Management and Storage Scan services



Table of Contents

Foreword	3
Solution overview and features	4
Architecture diagram.....	4
Pre-requisites	6
Deployment and Configuration Steps	7
Netskope Configuration - Rest API Token and External ID	8
Configure Account Enrollment Template	10
Using the integration	15
Best Practices	18
Solution Estimated Pricing.....	18
Partner contact information.....	18

Foreword

The Netskope CSPM and Storage Scan services are multi-account security solutions that provides visibility into resources, configurations, data protection, and malware on the AWS cloud. Implementing this solution, you can identify and remediate risky misconfigurations, identify sensitive data (DLP), and detect malware and ransomware.

The purpose of this AWS Implementation Guide is to enable every AWS Marketplace customer to seamlessly activate, deploy and configure the Netskope CSPM and Storage Scan in AWS Control Tower environment while taking full advantage of the resources pre-configured by AWS Control Tower as part of the initialization.

Solution overview and features

[Netskope Cloud Security Posture Management \(CSPM\)](#) enables you to gain the visibility and control across the AWS accounts in multi-account environment to secure your data, applications, and services, maintain best practices and standards compliance, and to automate your incident response. Netskope Storage Scan services allows AWS customers to easily identify and protect sensitive data on the organization's S3 buckets and to detect malware.

With the integration between AWS Control Tower and Netskope CSPM and Storage Scan services you can automatically enroll your existing AWS Control Tower accounts into Netskope CSPM and Storage Scan services, as well as help assure that new accounts provisioned by the AWS Control Tower account factory will be also immediately protected by the Netskope Security Cloud services.

Architecture diagram

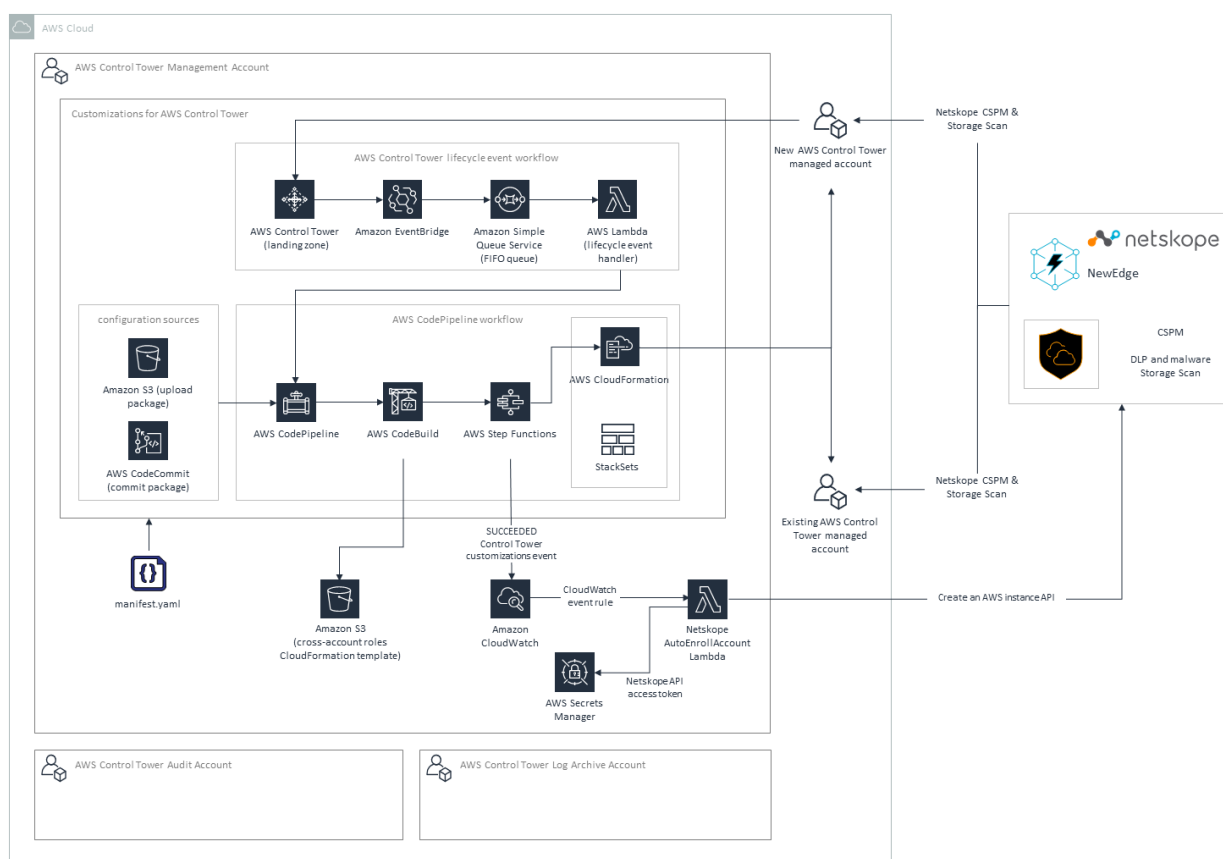


Figure 1. Netskope CSPM and Storage Scan service with AWS Control Tower Architecture Diagram

This solution uses the [Customization for AWS Control Tower](#) (CfCT) solution to deploy the integration, the solution source code can be found on GitHub repository. This repository contains two [AWS CloudFormation](#) templates and the manifest file. The first template, `Netskope-CSPM-StorageScan-Account-Enrolment-ControlTower.yaml` shall be deployed in the AWS Control Tower management account home region. The CloudFormation stack deployed using this template creates the following resources on the AWS Control Tower management account:

- [AWS Secrets Manager](#) secret encrypted by AWS Key Management Service (KMS) key to store your Netskope API access token.
- [Amazon CloudWatch event rule](#) triggered by the SUCCEEDED status event from the Customizations for AWS Control Tower [AWS Step Functions](#).
- [AWS Lambda](#) function `NetskopeAutoAddInstanceLambda` invoked by the CloudWatch event rule above. Upon receiving a SUCCEEDED event from the CfCT, this Lambda function calls the Netskope [Get Instance Info](#), [Create an AWS Instance](#) and [Update an AWS Instance](#) APIs to create or update the AWS account enrolment in your Netskope tenant.

The `manifest.yaml` file for CfCT describes the target AWS accounts and Organization Units (OUs) which you'd like to automatically enroll into Netskope Security Cloud. This `manifest.yaml` file is configured to launch [AWS CloudFormation StackSet](#) from the second template, `Netskope-CSPM-StorageScan-RoleTemplate-ControlTower.yaml`. This template file creates the cross-account IAM role that will be used by Netskope.

When you trigger the CfCT code pipeline, the CfCT solution deploys AWS CloudFormation StackSets with the resources defined in the `NetskopeCSPM-StorageScan-RoleTemplate-ControlTower.yaml` template across the AWS accounts and OUs defined in the `manifest.yaml` file.

Later, when you create a new managed account using [AWS Control Tower Account Factory](#), the CfCT solution uses the [AWS Control Tower Lifecycle Event](#) to invoke the same CodePipeline workflow and deploys the AWS IAM roles will be used by Netskope on the newly created account. When the CfCT solution completed the Netskope AWS IAM role deployment, the CfCT Step Functions send the SUCCEEDED event in the Amazon CloudWatch which triggers the `NetskopeAutoAddInstanceLambda` Lambda function to configure your AWS account in the Netskope tenant.

Pre-requisites

The following pre-requisites are required to implement the Netskope integration with AWS Control Tower:

- Fully deployed AWS Control Tower. For information about setting up an AWS Control Tower landing zone, see [Getting Started with AWS Control Tower](#). You also need administrator privileges in the AWS Control Tower management account.
- [Customizations for AWS Control Tower](#) (CfCT) solution deployed in your AWS Control Tower home account. Follow the [implementation guide](#) to deploy CfCT solution.
- An active Netskope Security Cloud tenant. You can subscribe from AWS Marketplace by following the instruction in the next section.

This solution guide assumes working knowledge with AWS management console. We also recommend that you become familiar with the following AWS services:

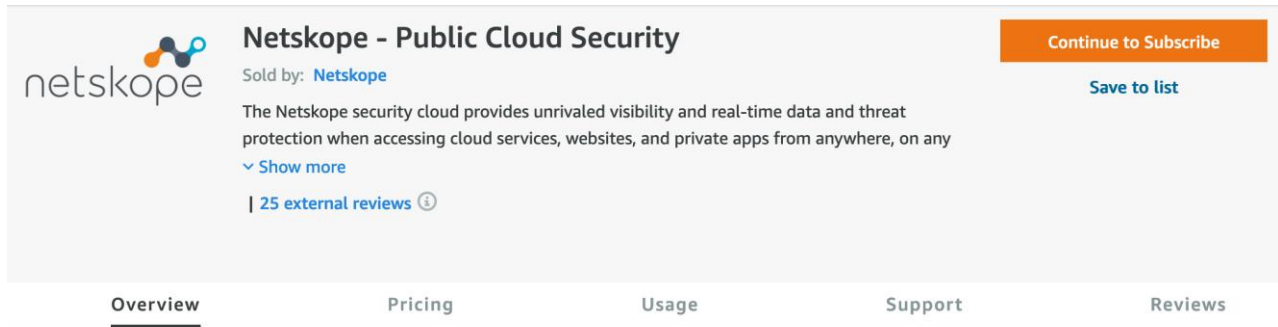
- [AWS Lambda](#)
- [Amazon CloudWatch](#)
- [AWS CloudFormation](#)
- [AWS Step Functions](#)

If you are new to AWS, see [Getting Started with AWS](#) . For additional information about AWS Marketplace, see [AWS Marketplace Overview](#).

Deployment and Configuration Steps

Step 1.1: Subscribe to Netskope Public Cloud Security on AWS Marketplace.

Locate the [Netskope Public Cloud Security in the AWS Marketplace](#).



Product Overview

Click on the **Continue to Subscribe** button.

Step 1.2: Guidance on Contract Duration and Renewal

In the new screen, you can configure your contract. You can select the **Contract Duration** and set the **Renewal Settings**.

Step 1.3: Select Contract Options

Select the Contract Options to be activated with your contract. Please note that this solution is applicable for **CASB_API** and **IAAS_STORAGE**

Step 1.4: Create the Contract and Pay

Once you have configured your contract, you can click on the Create contract button. You will be prompted to confirm the contract. If you agree to the pricing, select the **Pay Now** button.

Step 1.5: Set up Account

To complete registration, choose Setup your account and follow the remaining instructions.

Netskope Configuration - Rest API Token and External ID

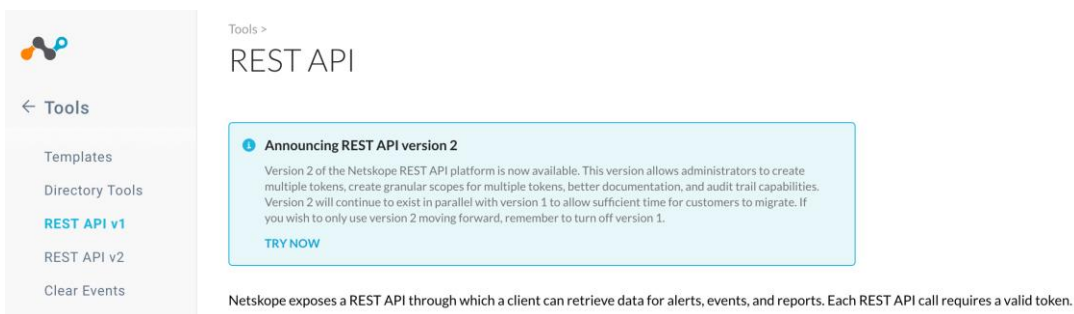
Step 2.1: Log into the Netskope

Using your Netskope tenant URL, login to your Netskope portal.



Step 2.2: Create Rest API Token

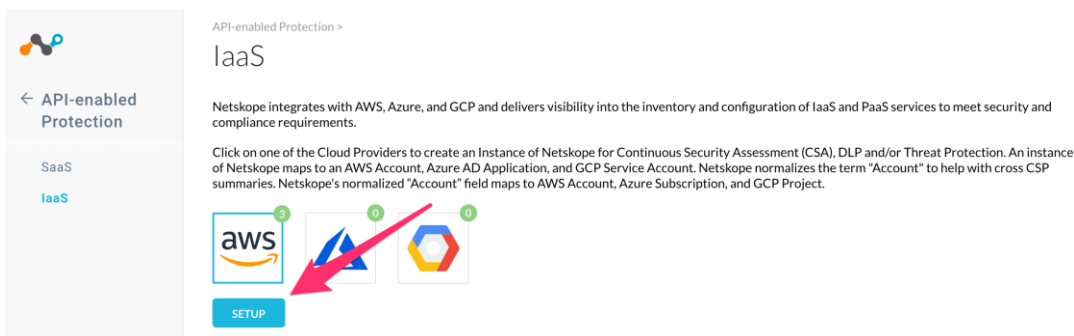
From Netskope console, select **Settings > Tools > REST API v1** from the side-bar navigation.



Choose **Generate New Token** and take a note of the token id and keep it secure.

Step 2.3: Retrieve External ID

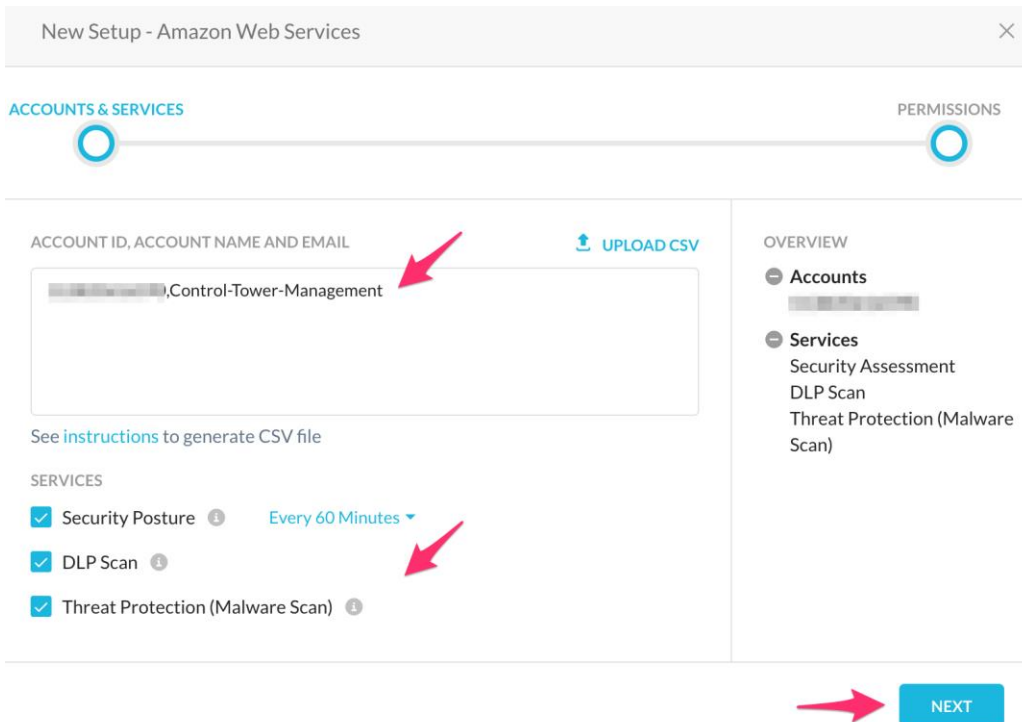
From Netskope console, navigate to **Settings > API-enabled Protection > IaaS**, then select **AWS** and click **Setup**.



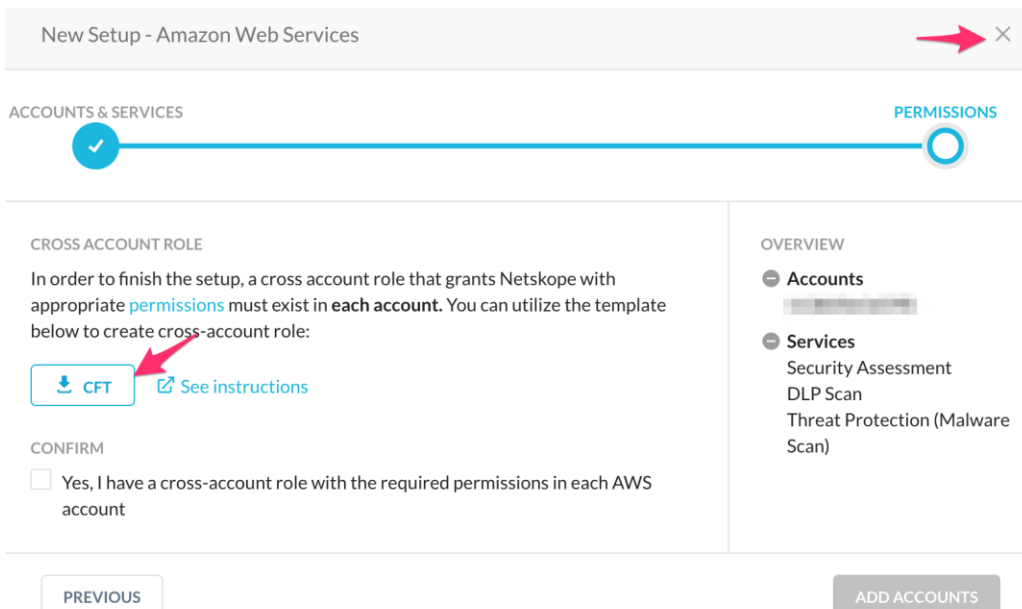
In the **New Setup** window, enter the following details:



- 12-digit AWS account ID of your AWS Control Tower management, followed by the account name. Follow the format as described in the text box.
- Keep the default service checked and click **Next**.



On the next dialog window, download the CFT file and exit the **New Setup** window.



Open the CFT file using any text editor and search for the *ExternalId*. Copy the value for both the ExternalId and the AWS account ID (see reference below).

```
50 CrossAccountRole:
51   Properties:
52     AssumeRolePolicyDocument:
53       Statement:
54         - Action:
55           - sts:AssumeRole
56           Condition:
57             StringEquals:
58               sts:ExternalId: [REDACTED]
59           Effect: Allow
60           Principal:
61             AWS:
62               - arn:aws:iam::727061500630:root
63             Sid: ''
64           Version: '2012-10-17'
65     ManagedPolicyArns:
66       - arn:aws:iam::aws:policy/SecurityAudit
67     Path: /
68     RoleName: Netskope_Role
69     Type: AWS::IAM::Role
```

Configure Account Enrollment Template

Step 3.1: Clone [Netskope CSPM & Storage Scan services](#) GitHub repository.

From your local terminal, run:

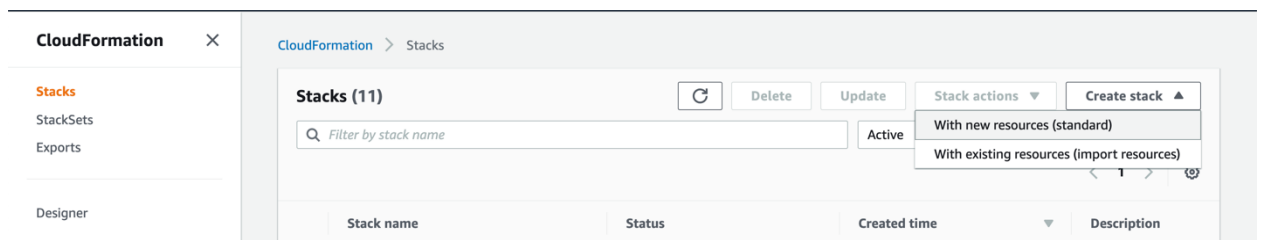
```
git clone https://github.com/netskopeoss/Netskope-CSPM-StorageScan-AWSControlTower
```

Step 3.2: Deploy CloudFormation Stack

Sign into the AWS Control Tower Management account as administrator and deploy the Netskope automation solution for enrolling AWS accounts managed by the AWS Control Tower in the Netskope CSPM and Storage Scan services.

3.2.1 Navigate to the AWS CloudFormation management console and change the region to the AWS Control Tower home region.

3.2.2 Click **Create Stack** and choose **with new resources (standard)**.



3.2.3 Choose **Upload a template file** then click on Choose file. Choose the Netskope-CSPM-StorageScan-Account-Enrolment-ControlTower.yaml from the directory on your disk where you cloned the GitHub repository to, click **Open** and then click **Next**.

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Create stack

Prerequisite - Prepare template

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.

Template is ready Use a sample template Create template in Designer

Specify template
A template is a JSON or YAML file that describes your stack's resources and properties.

Template source
Selecting a template generates an Amazon S3 URL where it will be stored.

Amazon S3 URL Upload a template file

Upload a template file

No file chosen

JSON or YAML formatted file

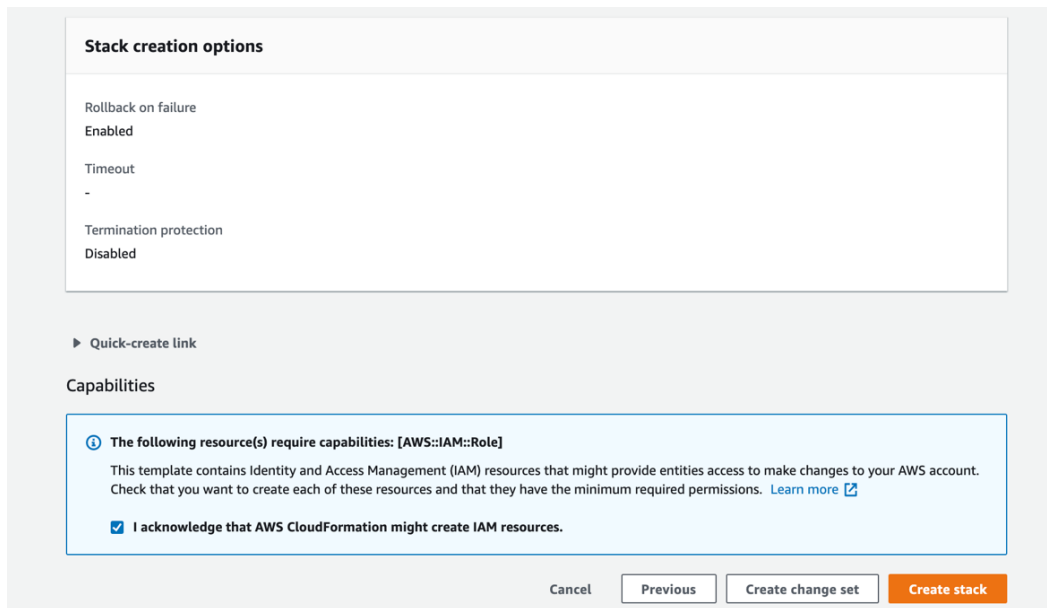
3.2.4 Enter the stack name and the parameters for your deployment:

Netskope tenant FQDN	Enter Netskope tenant FQDN (i.e., example.goskope.com), this is the FQDN URL that you use to login to Netskope console.
Netskope tenant REST API token	Enter Netskope tenant REST API token provided from Step 2
Netskope AWS Account ID	Enter Netskope trusted AWS Account ID provided from Step 2
STS external ID	Enter STS external ID provided by from Step 2
AWS PrincipalOrgID	Enter your AWS Organizations ID (i.e., o-12345678)
Security Administrator email address	Enter your Security Administrator email address
AWS KMS Key ID	Optional KMS Key ID to encrypt Netskope API token in Secrets Manager. If not specified AWS/secretsmanager will be used
Security Scan enabled	Enter ("true", "false"), whether Netskope CSPM Security violations Scan is enabled
CSPM security scan interval	Choose the CSPM security and compliance violations scan interval in minutes
DLP Scan enabled	Enter ("true", "false"), whether Netskope storage DLP Scan is enabled
MalwareScan Scan enabled	Enter ("true", "false"), whether Netskope storage Malware Scan is enabled

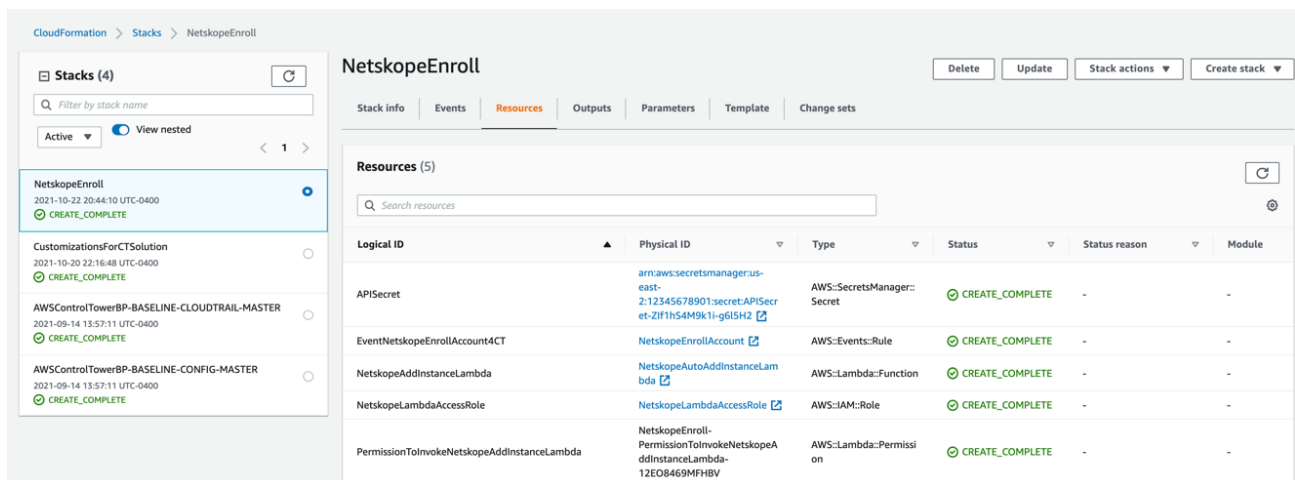
3.2.5 Click **Next**.

3.2.6 Optionally, enter the Tags for your CloudFormation stack and / or click Next.

3.2.7 Acknowledge creating IAM resources and click **Create stack**.



3.2.8 When CloudFormation stack is in the CREATE_COMPLETE state, you can navigate to the Resources tab and see the resources created by the stack.



You deployed the Netskope enrollment automation solution for AWS accounts managed by AWS Control Tower. This template deploys the AWS Lambda function that will perform account registration in Netskope.

Step 3.3: CfCT Manifest Modification

Next, you need to deploy AWS IAM cross-account role that will be used by the Netskope CSPM and Storage Scan services across your AWS Organizations accounts. You will use the Customizations for AWS Control Tower (CfCT) solution for this deployment. The CfCT Customizations Pipeline workflow will deploy the required AWS IAM role on the AWS accounts specified in the manifest.yaml file. The AWS Step Functions

SUCCEEDED event upon customizations workflow completion will trigger the enrollment automation you deployed on step 3.2 and will provision your AWS Accounts in you Netskope tenant.

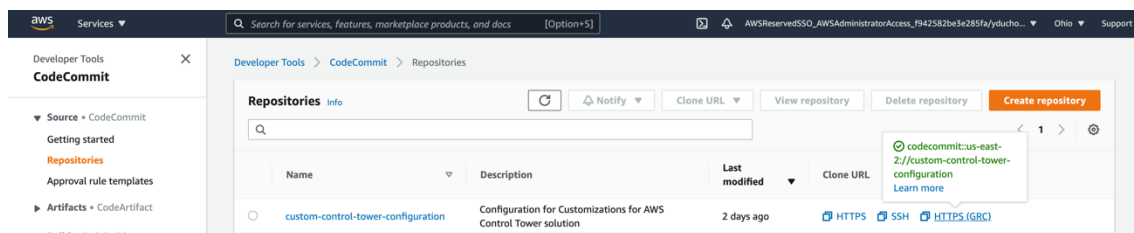
From the AWS Control Tower Management account, perform the following:

- 3.3.1 Open the manifest.yaml file you cloned from the Netskope GitHub repository.
- 3.3.2 Replace the AWS Region reference in the manifest with the AWS Region where your Control Tower landing zone is deployed.
- 3.3.3 Replace the **TrustedAccountID** and the **ExternalID** with the corresponding values for you Netskope tenant.
- 3.3.4 Set the values for the **SecurityScan**, **DLPScan** and **TrustedAccountID** to true or false to configure the Netskope Security Cloud functionality you'd like to use to protect your AWS accounts.
- 3.3.5 Configure the AWS Organizations Units and accounts you'd like to enroll in Netskope CSPM and Storage Scan services in the deployment_targets section of the manifest file. Please refer to the [Customizations for AWS Control Tower Develop Guide](#) for more details about working with the manifest file.
- 3.3.6 Save the manifest file.

Step 3.4: Merging CfCT Manifest File

This instruction assume that you are using AWS [CodeCommit](#) as the Customizations for AWS Control Tower CodePipeline source repository. You can also use Amazon S3 as your configuration source as described in [this Documentation](#). Steps for deploying the Control Tower customizations for Netskope account enrollment using Amazon S3 as a configurations source are similar to the steps using AWS CodeCommit below.

- 3.3.7 Sign into the AWS CodeCommit management console, choose the **custom-control-tower-configuration** repository and copy its **HTTPS (GRC) URL**:



- 3.3.8 If not yet installed, install the git-remote-codecommit package in your local machine:

```
pip install git-remote-codecommit
```

- 3.3.9 Assuming you already have proper AWS CLI credentials for accessing the control-tower-configuration repository in your Control Tower landing zone management account, clone this repository to your local machine:

```
git clone (HTTPS (GRC) URL copied above
```

3.3.10 Using text editor, merge the manifest.yaml file in the cloned repository by the one you edited on step 3.3. If your manifest file is empty, you can simply replace it with the one you edited on step 3.3.

3.3.11 Check in the manifest file into the CodeCommit repository:

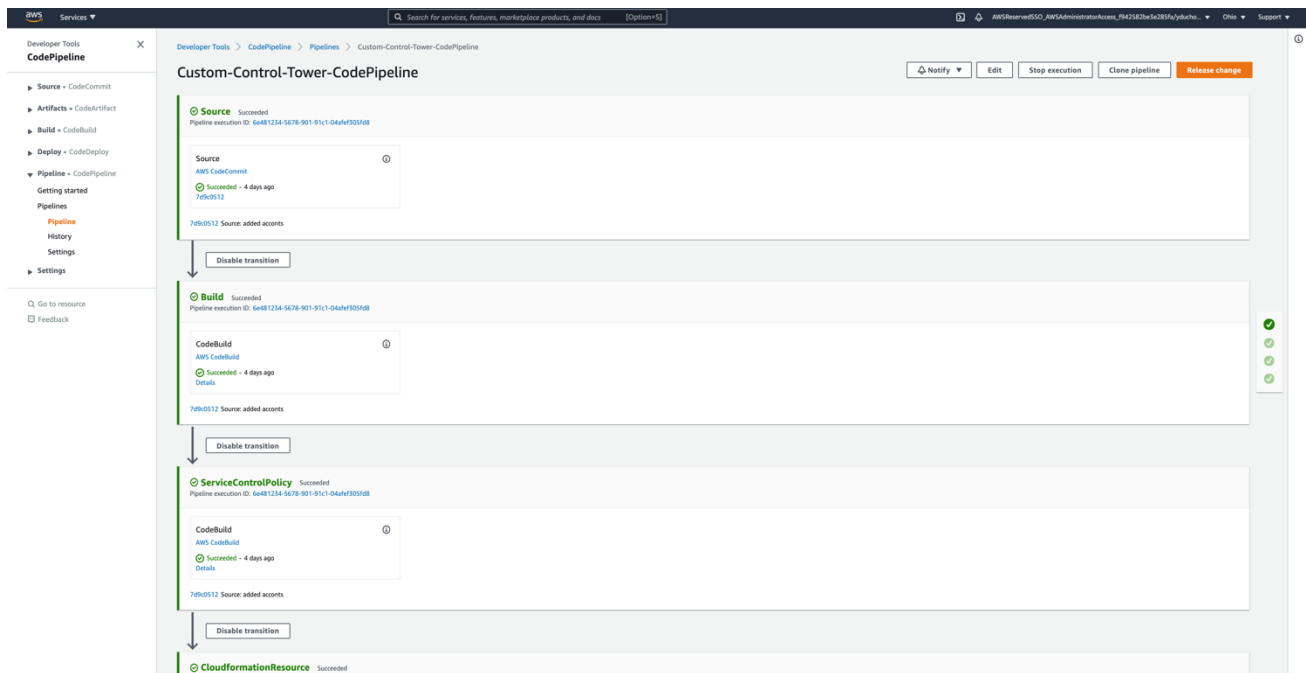
```
git status git add -A  
  
git commit -m 'Netskope Automatic Accounts enrollment'  
  
git push
```

Step 3.4: Verification steps:

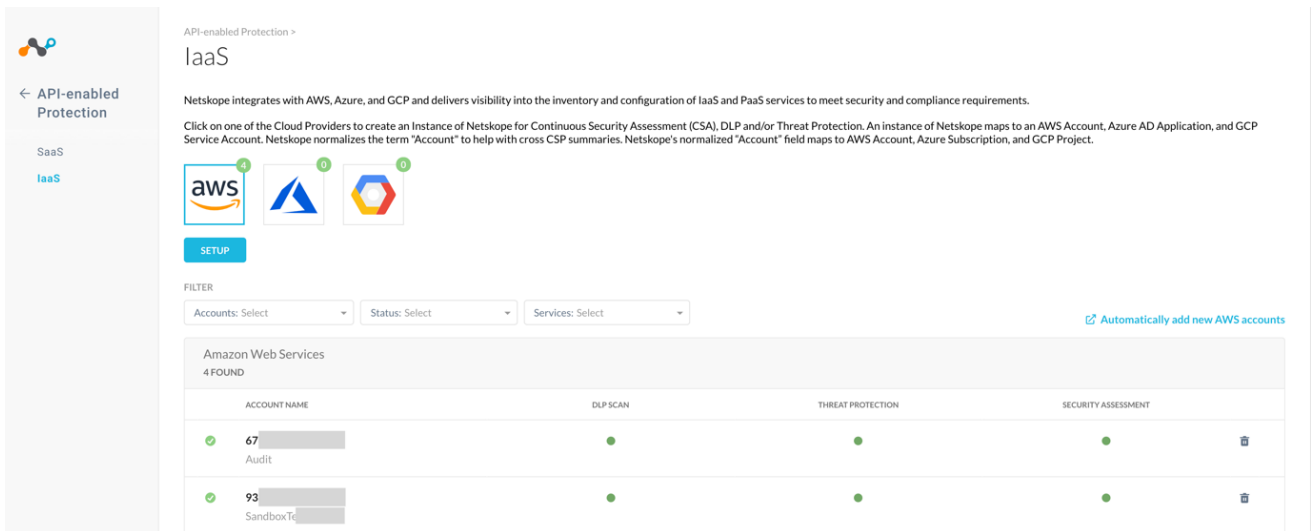
Git commit to the CfCT repo will trigger the Customizations for AWS Control Tower workflow for deploying Netskope cross-account AWS IAM roles on your AWS accounts, you can check its progress on the CodePipeline.

3.4.1 Navigate to AWS CodePipeline Console on your AWS Control Tower Management account.

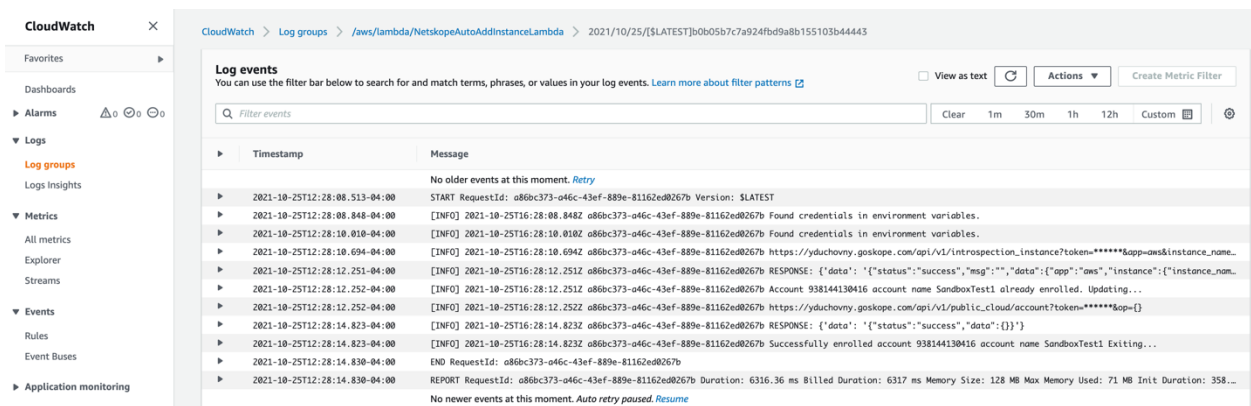
3.4.2 Choose **Custom-Control-Tower-CodePipeline** to track the status of the pipeline at various stages.



3.4.3 When the last stage of the pipeline completed, open the Netskope management console, navigate to **Settings > API-enabled Protection > IaaS** and check that your existing AWS accounts configured in the manifest file successfully enrolled in the Netskope CSPM and Storage Scan services.



3.4.4 You also can monitor the NetskopeAutoAddInstanceLambda automation Lambda function execution logs by opening AWS CloudWatch management console, navigating to **Logs -> Log groups** menu and choosing the NetskopeAutoAddInstanceLambda log group for your Lambda function.

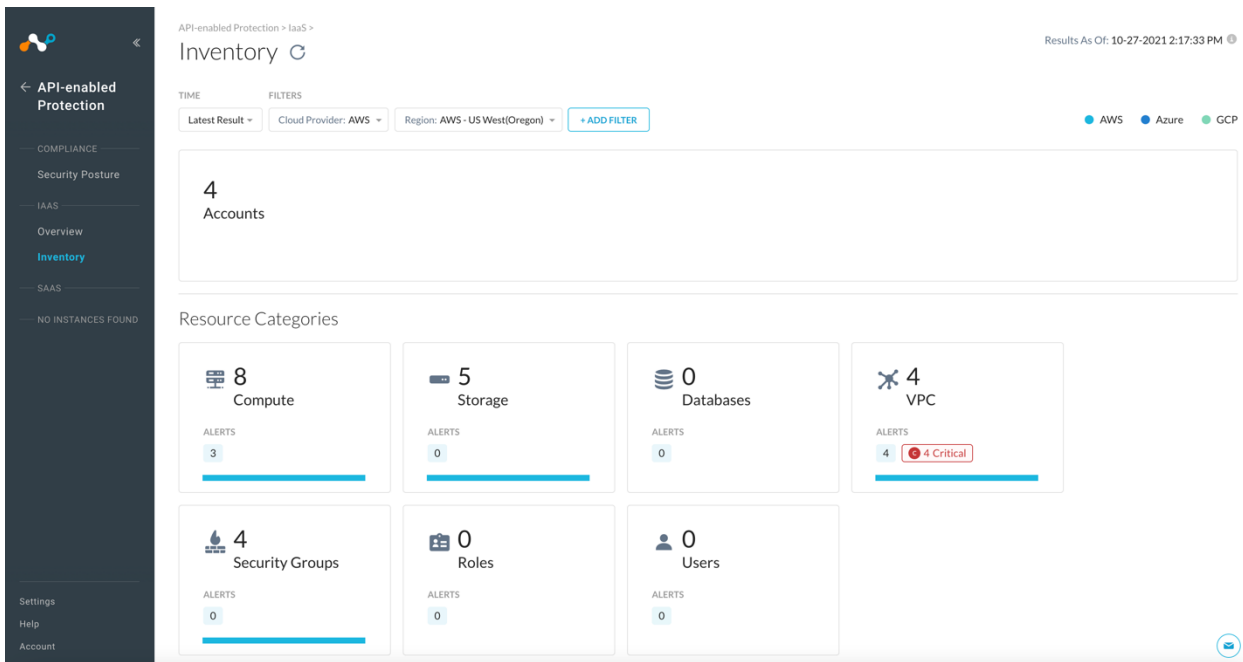


Using the integration

Step 4.1: How to use Netskope CSPM

When your existing or new AWS accounts enrolled into Netskope CSPM, Netskope performs the complete scan of AWS instances and services running on these account and makes the list of your AWS inventory available for you in one single place on the Netskope Management console and via the [View Cloud Provider Inventory API](#).

To view your AWS instances and services, sign into the Netskope Management console, navigate to **API-enabled Protection->Inventory** and use the filters on top of the page to find the accounts, instances and more.



Next, you can configure Netskope Security Posture policies that will provide you a clear picture of your cloud security posture and enable you to see how the environment is performing against standards and best practices like CIS (Center for Internet Security) benchmarks.

To configure Netskope Security Posture policies, on the Netskope Management console navigate to **Policies->Security Posture** and click **New Policy**.

Here you can choose the instances and Security Posture standards and frameworks you'd like Netskope to monitor your environment for:

The screenshot shows the 'Edit Security Posture Policy' configuration page. The page includes a sidebar with navigation options like 'Policies', 'SSL Decryption', and 'Security Posture'. The main content area is titled 'Edit Security Posture Policy' and contains the following configuration options:

- Instances:** Amazon Web Services (dropdown), Instance = All (text input)
- Profile & Action:**
 - Profile: PCI-DSS v3.2.1 (AWS), CIS AWS Foundations Benchmark v1.4.0, NIST CSF v1.1 (AWS), CIS AWS Foundations Benchmark v1.2.0, GDPR 1996/679 (AWS), + 7 more
 - Action: Alert (dropdown), Show Rules (166) (checkbox)
- Policy Name:** AWS_ALL (text input)
- Status:** Enabled (checkbox)

Buttons for 'CANCEL' and 'SAVE' are located at the top right of the configuration area.

To help assure your AWS cloud security posture aligned with your organization’s specific security standards you also can write [custom security assessment rules](#) using Domain Specific Language (DSL).

The Netskope Security Posture Assessment results are available for you on the Netskope Management console and via the [View Security Assessment Violations](#) API. To view Security Posture Assessment results on the Netskope Management console, navigate to **API-enabled Protection->Security Posture** and use the filters on top of the page to find the accounts, instances and more.

API-enabled Protection > Compliance > Security Posture

Results As Of: 10-27-2021 2:17:33 PM

TIME: Latest Result | Resource Category: Select | Tags: Select Tags | Cloud Provider: AWS | +ADD FILTER

Raw Findings | Rules | Resources

FAILED FINDINGS: 131 (0 muted, 131 unmuted)
PASSED FINDINGS: 425 (0 muted, 425 unmuted)
TOTAL FINDINGS: 556

Unknown findings: 0
No errors encountered.

FINDINGS HISTORY (Last 7 Days): Passed, Muted, Failed

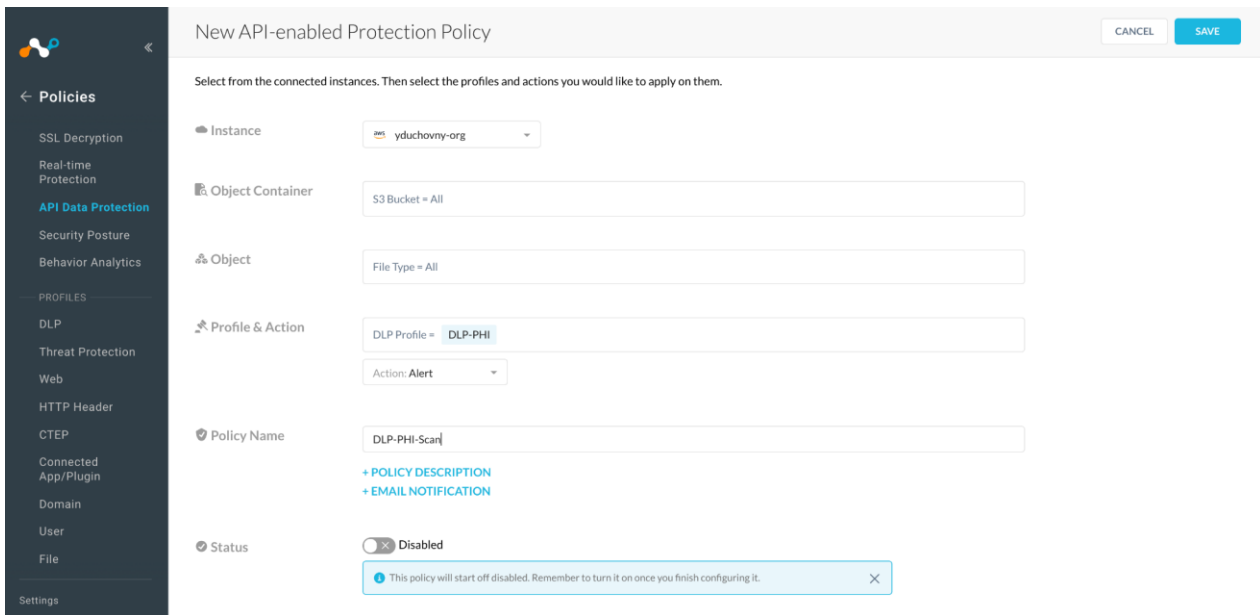
Findings: 556 FOUND, 6 ACCOUNTS | Sort by: Status | MUTE | EXPORT

STATUS	RULE NAME	SEVERITY	CLOUD PR...	INSTANCE NAME & ID	RESOURCE CATEGORY	RESOURCE TYPE	RESOURCE NAME & ID
Failed	Establish an access control syste...	Critical	AWS	Log Archive	Identity	Role	AWSControlTowerEx... AROAXKGQANC3V6...
Failed	Establish an access control syste...	Critical	AWS	Test_SB	Identity	Role	SO0111-RevokeUnus... AROAWBKLWQEW...
Failed	Ensure Lambda functions have an ...	High	AWS	Test_SB	Compute	Function	CIS-1_4_0-3-9-remidi... CIS-1_4_0-3-9-remidi...

You can also take a look at the [CSPM security violation findings Auto-Remediation framework](#) if you’d like to remediate some of the security violations findings automatically.

Step 4.2: How to use Netskope Storage Scan services

Netskope Storage Scan services enable you to identify sensitive data and detect malware on your S3 buckets. When your AWS account is enrolled into Netskope Storage Scan, you can configure retroactive and ongoing scans for your S3 buckets. To configure the Netskope Storage Scan policies from the Netskope Management console, navigate to **Policies->API Data Protection** and click on **NEW POLICY**. You can define the AWS account, AWS S3 buckets and DLP profiles when you’re defining the Storage Scan policy from the Netskope Management Console.



You can also use [Netskope Storage Scan Policies](#) API to define granular policies for scanning your organizations' S3 buckets.

For more information about Netskope CSPM and Storage Scan services, please refer to the [Netskope Knowledge Portal](#) and the [Netskope Community](#).

Best Practices

- Visit [Netskope Knowledge portal](#) to learn more about Netskope product setup, administration, and features.
- Find the latest resource such as blogs, case studies and references in [Netskope resource center](#).

Solution Estimated Pricing

Please visit [Netskope AWS Marketplace page](#) for an updated price list.

Partner contact information

<https://www.netskope.com/contact-us>