SOPHOS

Cybersecurity made simple.

Sophos Cloud Optix

help

Contents

1 About Sophos Cloud Optix

Sophos Cloud Optix is an AI-powered security and compliance platform for public cloud environments.

Sophos Cloud Optix:

- Provides a real-time inventory of your servers, storage, and network elements in the cloud.
- Helps you manage resources, monitor security, and meet compliance standards in one simple-to-use interface.

You can get Sophos Cloud Optix in the following ways:

1. You can sign up for a free 30-day trial of Sophos Cloud Optix in Sophos Central.
2. You can buy Sophos Cloud Optix as a standalone license. This is the full version of Sophos Cloud Optix, managed in Sophos Central.
3. You can buy Sophos Cloud Optix on a pay-as-you-go (PAYG) basis through AWS Marketplace.
4. You can also get a subset of Sophos Cloud Optix. This is known as Sophos Cloud Optix for EDR and is only available if you have an Intercept X Advanced for Server with EDR term license.

Sophos Managed Service Provider (MSP) partners can also get Sophos Cloud Optix in Sophos Central and buy it on a monthly basis, based on aggregate usage across their customers.

For more information, see the Sophos Cloud Optix product info on the Sophos website.

Note
The Sophos Cloud Optix service is hosted in the US. Customers in other countries can purchase and use the US-hosted service. The service is not currently available from Cuba, Iran, North Korea, Russia, South Sudan, Sudan, Syria, Ukraine, and Venezuela.

Related concepts

Sophos Cloud Optix for EDR (page 106)
Find out which Sophos Cloud Optix features are included with Intercept X Advanced for Server with EDR.

Related reference

Sophos Cloud Optix product info
Sign up for a free trial

2 Getting started

You need a subscription or free trial account to use Sophos Cloud Optix.

Sophos Cloud Optix subscriptions are based on the number of cloud assets in the cloud environments that you add to the service.

If you have an AWS account, you can subscribe to Sophos Cloud Optix on a pay-as-you-go (PAYG) basis, with no contract term commitment. You pay monthly, in arrears, through your AWS account, based on your actual usage of Cloud Optix. See the AWS Marketplace listing for details.

You can sign up for a free 30-day trial of Sophos Cloud Optix Sophos Central. If you already have a Sophos Central account, click **Free Trials** in Sophos Central Admin to activate your free trial.

You can only link an email address to one Sophos Cloud Optix account. You can only add a cloud environment, for example an AWS account, to one Sophos Cloud Optix account.

Sophos Cloud Optix for EDR

If you have an Intercept X Advanced for Server with EDR term license, you can use Sophos Cloud Optix for EDR. This is a subset of the full product.

You can get Sophos Cloud Optix separately if you don't have an Intercept X Advanced for Server with EDR term license.

To see the features included in Sophos Cloud Optix for EDR compared to the full Sophos Cloud Optix product, see Sophos Cloud Optix for EDR.

Initial setup

When you have a license or free trial, read this help to find out how to do the following:

- Add your cloud environments, like AWS, Azure, GCP, and Kubernetes, to Sophos Cloud Optix.
- View your deployment, network traffic, and potential threats.

Sophos Cloud Optix needs no agents. The initial setup connects the service to your public cloud environments. We provide scripts to do this, which only take a few moments to run. These scripts setup read-only access by default.

Inventory and topology information should start showing in Sophos Cloud Optix within 15 minutes.

Related concepts

Add your AWS environment (page 4)
You can choose which method you use to add your AWS environment to Sophos Cloud Optix.

Sophos Cloud Optix licensing (page 103)
Subscriptions are based on the number of cloud assets in the cloud environments that you add to Sophos Cloud Optix.

Sophos Cloud Optix for EDR (page 106)
Find out which Sophos Cloud Optix features are included with Intercept X Advanced for Server with EDR.

Related tasks

Add your Microsoft Azure environment (page 25)

You can add your Azure environment to Sophos Cloud Optix by running the PowerShell script Sophos provides.

Add your Google Cloud Platform environment (page 32)
You can add a Google Cloud Platform (GCP) project to Sophos Cloud Optix by running the script Sophos provides.

Add your IaC environments (page 36)
Sophos Cloud Optix can monitor code submitted to your Infrastructure as Code (IaC) repositories for potential security issues.

Related reference

Sign up for a free trial

Sophos Cloud Optix (PAYG) on AWS Marketplace

3 Add your AWS environment

You can choose which method you use to add your AWS environment to Sophos Cloud Optix.

You can add your AWS environments to Sophos Cloud Optix in many ways.

You can add them easily using AWS **Quick-start** setup, to get up and running with core features. You don't have to run scripts or create additional resources in your AWS environment.

If you use **Quick-start** you get a limited set of features. If you want to use advanced features then you need to use one of the full setup options. You can do this at a later stage for the same account. For more details see AWS Quick-start.

You can do a full setup with the following methods, which create the resources required to collect VPC flow logs and Cloudtrail logs from your environment.

- Using the Sophos Cloud Optix AWS CLI script provided for Linux and macOS.
- Using AWS CloudFormation.
- Using the Terraform template provided.

If you're using AWS Organizations to centrally manage multiple AWS accounts, you must use the AWS CloudFormation setup method to add your accounts to Sophos Cloud Optix.

After adding your AWS account to Cloud Optix, you can add Amazon Elastic Kubernetes Service (EKS) clusters if you want to. You must add these clusters to Sophos Cloud Optix separately, using the Amazon CLI script provided by Sophos.

Conditions

Before you add AWS environments you must be aware of the following points:

1. By adding your AWS environment, you authorize Sophos to access information via APIs and to collect log data from your environment. Your cloud provider may charge you for this. See Cloud provider charges or contact your provider for details.
2. AWS regions that aren't connected to the global AWS infrastructure, including AWS GovCloud (US) and AWS China, are not supported.
3. Sophos Cloud Optix doesn't support AWS's legacy EC2-Classic platform, which was deprecated in 2013. You can add AWS environments that are on the EC2-VPC platform.

Related tasks

Add your Amazon EKS clusters (page 13)
You can add Amazon EKS clusters to AWS accounts you have added to Sophos Cloud Optix.

Add AWS environments using CLI scripts (page 6)
You can add your AWS environment using a script.

AWS Quick-start (page 5)
These instructions tell you how to use the AWS Quick-start option to connect your AWS accounts to Sophos Cloud Optix easily.

Related information

Add AWS environments using AWS CloudFormation (page 7)

You can add AWS environments to Sophos Cloud Optix using AWS CloudFormation.

3.1 AWS Quick-start

These instructions tell you how to use the AWS Quick-start option to connect your AWS accounts to Sophos Cloud Optix easily.

Using a simple CloudFormation template, **Quick-start** creates a read-only IAM role in your AWS account. Sophos Cloud Optix uses this role to access information via APIs to monitor security.

Quick-start gets you up and running with core features, including inventory and security configuration benchmark scanning. The following advanced features are not supported by the **Quick-start** setup option:

- Network traffic information flow displayed on Network Visualization.
- Searching for outbound network traffic information.
- Outbound network traffic anomaly detection and alerts.
- Activity Logs, including Activity Log visualizations and identification of high risk activities.
- User login anomaly detection and alerts.

To use these features, use one of the full setup options.

If you use **Quick-start** you can use a full setup option later without removing the environment you already created.

After adding your AWS account to Cloud Optix, you can optionally add Amazon Elastic Kubernetes Service (EKS) clusters. You must add these clusters to Sophos Cloud Optix separately, using the Amazon CLI script provided by Sophos

To use **Quick-start**, do as follows:

1. Sign in to your AWS console with the account you want to add to Sophos Cloud Optix
2. Sign in to Sophos Cloud Optix.
3. In Sophos Cloud Optix, under Settings click **Environments**.
4. Click **Add new environment** and select **AWS** from the list.
5. Click the **Add an AWS account using CloudFormation (Quick-start)** setup option.
6. Read the information and click **Launch Stack**.
   This opens **Quick create stack** in your AWS console and automatically populates it with the parameters required to connect your environment to Sophos Cloud Optix. Do not change any of these parameters.
7. In your AWS console, turn on **I acknowledge that AWS CloudFormation might create IAM resources with custom names**.
8. In your AWS console, Click **Create Stack**.
   This creates an IAM role (*`Avid-Role`*) in your AWS account and connects your AWS account to Sophos Cloud Optix.

Related tasks

Add your Amazon EKS clusters (page 13)

You can add Amazon EKS clusters to AWS accounts you have added to Sophos Cloud Optix.

3.2 Add AWS environments using CLI scripts

You can add your AWS environment using a script.

To run the script, you need to have AWS CLI version 1.11.188 or later installed on the computer where you plan to run the script. For more information see Set up AWS CLI to run scripts (page 22).

Note
The instructions for using the script are only valid for a Linux or macOS AWS CLI. The scripts do not work with Windows.

Tip
If you want to run the script with limited permissions, see Permissions needed to run Sophos Cloud Optix scripts. If not, you must use an IAM Administrator role to run the script.

1. Click **Settings** (in the left-hand menu) and select **Environments**.
2. Click **Add New Environment**.
3. On the **Add your cloud environment** page, select the **AWS** tab.
4. Download the Sophos Cloud Optix script provided on this tab.
5. Run the script with the variables provided. You can copy and paste the command you need to run from your Sophos Cloud Optix console.

   ```
   EXTERNAL_ID=<…> CUSTOMER_ID=<…> REQUEST_ID=<…> DNS_PREFIX_FLOW=<…>
   DNS_PREFIX_CLOUDTRAIL=<…> bash avidConfigScript.sh
   ```

   The variables let you customize your setup in various ways, including these:

   - Use a non-default AWS region.
   - Reuse an existing CloudTrail instead of creating a new one.
   - Disable AWS Virtual Private Cloud (VPC) Flow logs (but note that this prevents the **Topology** traffic visualization and anomaly detection from working).

   For more details of these variables, see AWS CLI script variables.

After the script has finished running, you will see an "All steps done!" message. If there are no errors, your environment shows in the Sophos Cloud Optix dashboard.

After adding your AWS account to Cloud Optix, you can add Amazon Elastic Kubernetes Service (EKS) clusters if you want to. You must add these clusters to Sophos Cloud Optix separately, using the Amazon CLI script provided by Sophos.

Related concepts

Permissions needed to run Sophos Cloud Optix scripts for AWS (page 17)
You can create custom roles with the appropriate permissions needed to run the Sophos Cloud Optix scripts that add AWS environments.

Troubleshooting for AWS (page 16)
If there are problems with adding an AWS environment, run the uninstall script and try again.

Resources created in your AWS environments (page 14)

A full deployment of Sophos Cloud Optix adds AWS environments to the service and sets up communication between AWS and Sophos.

Related reference

AWS CLI script variables (page 20)
AWS script variables

Related information

Set up AWS CLI to run scripts (page 22)
To add environments with scripts you must first set up the AWS CLI.

3.3 Add AWS environments using AWS CloudFormation

You can add AWS environments to Sophos Cloud Optix using AWS CloudFormation.

Introduction

To add a single AWS account using AWS CloudFormation, follow the instructions on the Add your AWS environment page to add the account in your Sophos Cloud Optix console.

You can also add multiple AWS accounts using AWS CloudFormation StackSets. To do this you must choose one AWS account as a master account, then assign target member accounts. You use details from your Sophos Cloud Optix console to configure your AWS CloudFormation StackSet.

This starts Stack Instance creation in the specified target member accounts and adds those accounts to Sophos Cloud Optix.

Note
After adding your AWS account to Cloud Optix, you can add Amazon Elastic Kubernetes Service (EKS) clusters if you want to. You must add these clusters to Sophos Cloud Optix separately, using the Amazon CLI script provided by Sophos.

You must do as follows:

- Collect information from your Sophos Cloud Optix console.
- If you're not using AWS Organizations, assign roles to your master AWS account and target member AWS accounts.
- Configure the CloudFormation StackSet in the master account.
- Create the CloudFormation StackSet.
- If you're using AWS Organizations, you'll also need to deploy an additional CloudFormation template to use an existing CloudTrail.

Note
If you're using AWS Organizations to centrally manage multiple AWS accounts, follow the additional instructions after you have created and configured the CloudFormation StackSet.

Related concepts

Add your AWS environment (page 4)

You can choose which method you use to add your AWS environment to Sophos Cloud Optix.

Related tasks

Add your Amazon EKS clusters (page 13)
You can add Amazon EKS clusters to AWS accounts you have added to Sophos Cloud Optix.

Collect information from your Sophos Cloud Optix console

The information is used to link the StackSet to your Sophos Cloud Optix accounts.

Before creating AWS CloudFormation StackSets you must collect information from your Sophos Cloud Optix account. This is used later in the AWS **Create StackSet** assistant.

1. Sign into your Sophos Cloud Optix account.
2. Under **Settings** click **Environments > Add New Environment**.
3. On the **Add your cloud environment** page, note the details under **Add multiple AWS accounts using CloudFormation StackSets**.

   You must take note of the following parameters:

   - DnsPrefixCloudTrail
   - ExternalId
   - ReqID
   - CustomerId
   - DnsPrefixFlow
4. Go to the AWS console to create your CloudFormation StackSets.

Assign a role to the AWS account chosen as your master account

You must first choose an AWS account as your master account.

Restriction
You must not do this if you're using AWS Organizations. Go straight to Create CloudFormation StackSet in the Master AWS account.

Choose an AWS account to be your master account. To assign the appropriate role to this account, do as follows:

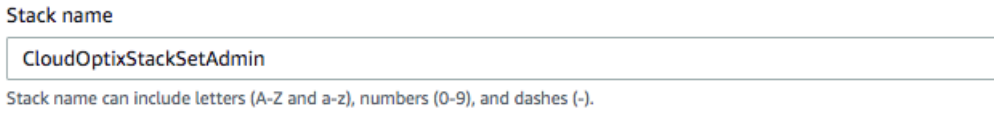
1. Sign into the AWS console using the account you have chosen.
2. Click the **Launch Stack** button here to go to the **Quick stack create** page with the correct parameters:

   Note
   You must click the **Launch Stack** button on this help page. It is configured with the correct parameters.

3. In **Quick create stack** check the **Template URL** is `https://avidcore.s3-us-west-2.amazonaws.com/aws/cloudformation/cloudformation/AWSCloudFormationStackSetAdministrationRole.yml`.

4. Check that the **Stack name** is `CloudOptixStackSetAdmin`.



5. Turn on **I acknowledge that AWS CloudFormation might create IAM resources with custom names**
6. Click **Create stack** to create the role in your master account.
7. Sign out of your AWS console.

Assign roles to each target member AWS account

You assign roles for the designated target member accounts.

Restriction
You must not do this if you're using AWS Organizations. Go straight to Create CloudFormation StackSet in the Master AWS account.

This process does not add the AWS master account to Sophos Cloud Optix. It only adds the target member accounts. If you want to add the master account, you must do it separately.

To create an AWS CloudFormation StackSet in every target member account, follow these instructions for each account:

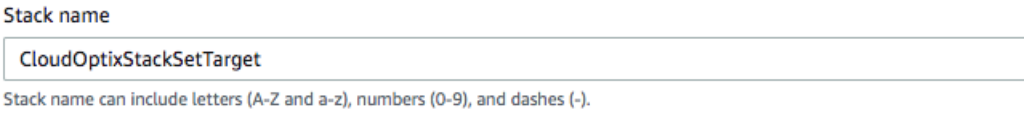
1. Sign into the AWS console using an account you have chosen as a target account.

   You must not be signed into your chosen master account.
2. Click the **Launch Stack** button here to go to the **Quick stack create** page with the correct parameters:

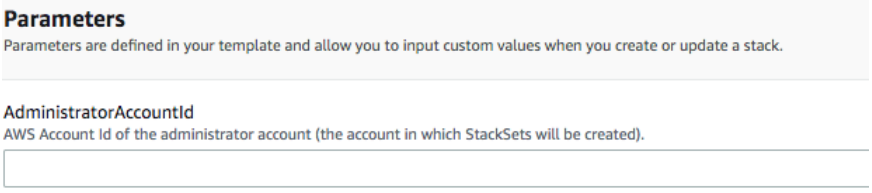
Note
You must click the **Launch Stack** button on this help page. It is configured with the correct parameters.

3. In **Quick create stack**, check that the **Template URL** is `https://avidcore.s3-us-west-2.amazonaws.com/aws/cloudformation/cloudformation/AWSCloudFormationStackSetExecutionRole.yml`.

4. Check that the **Stack name** is `CloudOptixStackSetTarget`



5. Under **Parameters**, enter the **AWS Account ID** of your admin account in **AdministratorAccountId**.



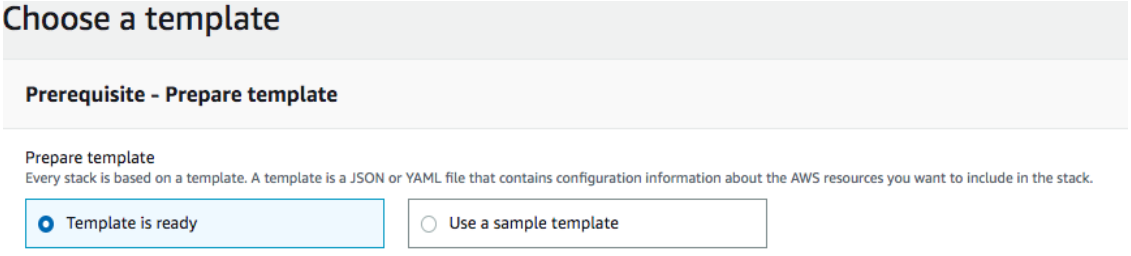
6. Turn on **I acknowledge that AWS CloudFormation might create IAM resources with custom names**.
7. Click **Create stack** to create the role in the target account.
8. Sign out of your target member account's AWS console.
9. Sign into the next target member account and repeat as required.

Configure CloudFormation StackSet in the master AWS account

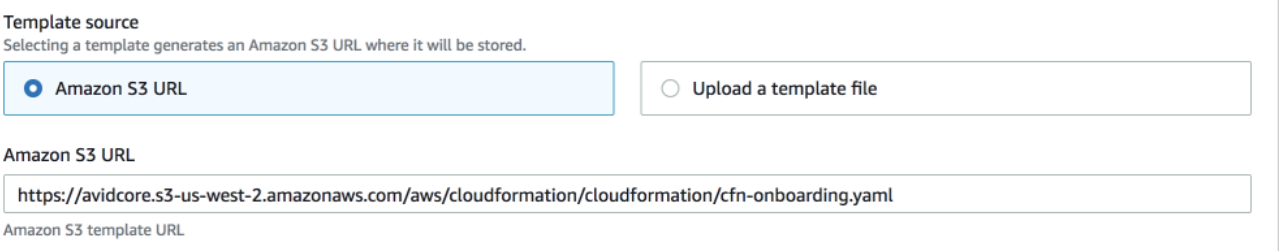
Using the Create StackSet assistant.

To create the AWS CloudFormation StackSet do as follows:

1. Sign into the AWS console with your AWS master account.
2. Select the **CloudFormation** service.
3. Select **StackSets**.
4. Select **Create StackSet**.
5. On the **Choose a template** page select **Template is ready**.



6. Select **Amazon S3 URL** as the template source.
7. Enter the template URL: `https://avidcore.s3-us-west-2.amazonaws.com/aws/cloudformation/cloudformation/cfn-onboarding.yaml`



8. Click **Next**.

Create CloudFormation StackSet

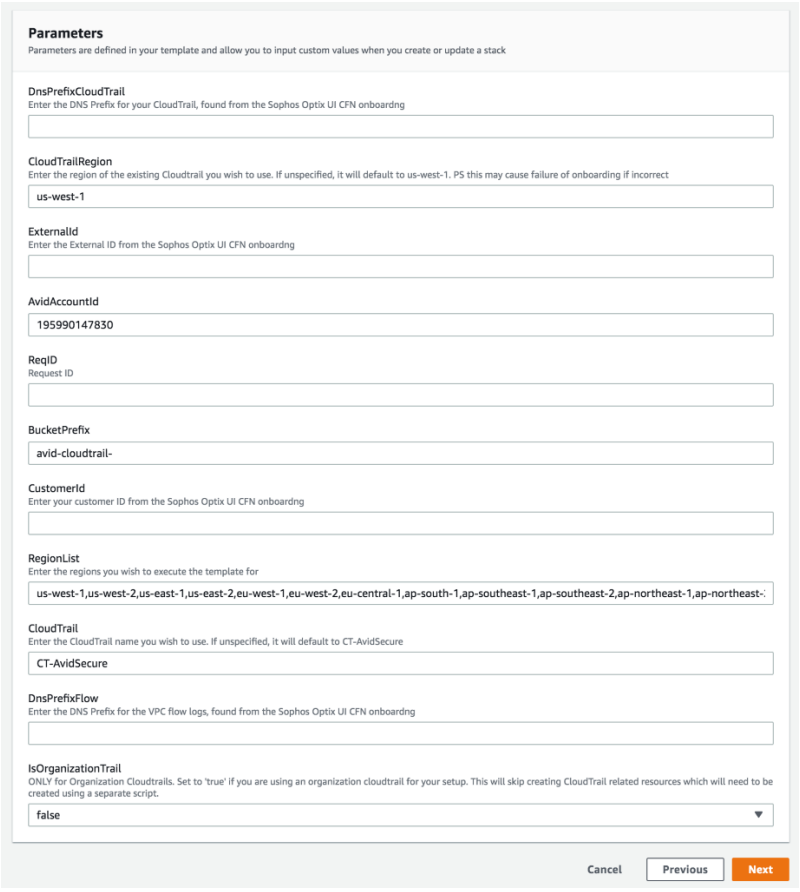
Use Sophos Cloud Optix information in the Create StackSet assistant.

Use the parameters you obtained earlier from your Sophos Cloud Optix account to fill in the fields in the AWS CloudFormation StackSet assistant. This links your StackSets to Sophos Cloud Optix.

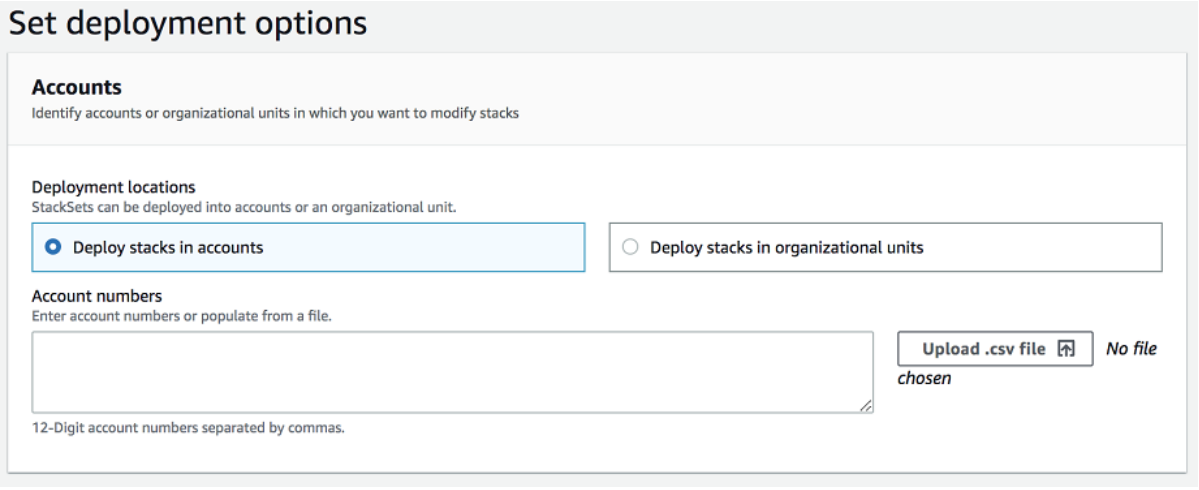
Warning
Do not delete or amend any fields that are pre-populated by Sophos Cloud Optix or on-boarding fails.

Ensure you are signed into your chosen AWS master account and do as follows:

1. Enter `OptixStackSet` into **StackSet name** on the **Specify StackSet details** page.
2. You may change the pre-populated description field if necessary.
3. Enter the following parameters from Sophos Cloud Optix:
   - DnsPrefixCloudTrail
   - ExternalId
   - ReqID
   - CustomerId
   - DnsPrefixFlow
4. Do not change the fields **AvidAccountId** and **BucketPrefix**.
5. The pre-populated list in the **RegionList** must only be changed if some of your regions do not have a default Amazon Virtual Private Cloud (VPC). You must remove those regions from the **RegionList** field or the on-boarding process fails.
6. 6. If you're using AWS Organizations, set the **isOrganizationTrail** parameter to true. Otherwise, set this parameter to false.
7. Do not change any other fields.



8. Click **Next**.
9. You don't need to do anything on the **Configure StackSet options** page.
10. Click **Next**.
11. On the **Set deployment options** page, select **Deploy stacks in accounts**.
12. In the **Account numbers** field, enter the account numbers of the target member accounts you want to add to Sophos Cloud Optix (the accounts in which you created the *`AWSCloudFormationStackSetExecutionRole`*).



13. In **Specify regions**, choose one region. The CloudFormation stack instance is created in this region for the target member account.
14. Click **Next**.

15. This takes you to a **Review** page which shows you all the options you have entered. Check this carefully.
16. Turn on **I acknowledge that AWS CloudFormation might create IAM resources with custom names**.
17. Close the assistant. This creates the stack instance and adds the target member accounts to Sophos Cloud Optix.

Additional instructions for AWS Organizations

AWS Organizations users must follow these additional steps.

If you are using AWS Organizations you must deploy an additional CloudFormation template to update your existing AWS Organization CloudTrail for Sophos Cloud Optix.

Note
You must sign in with the AWS Organization's master account that owns your CloudTrail.

1. Sign into the AWS console using your master account.
2. Click the **Launch Stack** button here to go to the **Quick stack create** page with the correct parameters:

   Note
   You must click the **Launch Stack** button on this help page. It is configured with the correct parameters.

3. In **Quick create stack** enter the name of the existing CloudTrail that you want to use in the CloudTrail field.
4. Enter the region of the existing CloudTrail in the CloudTrailRegion field. The field defaults to us-west-1.

   Check this carefully. Onboarding fails if this information is incorrect.
5. Use the parameters you obtained earlier from your Sophos Cloud Optix console to fill in the following fields:
   - CustomerId
   - DnsPrefixCloudTrail
6. Turn on **I acknowledge that AWS CloudFormation might create IAM resources with custom names**.
7. Click **Create Stack**.

3.4 Add your Amazon EKS clusters

You can add Amazon EKS clusters to AWS accounts you have added to Sophos Cloud Optix.

Sophos Cloud Optix will provide additional detailed inventory information for your Amazon Elastic Kubernetes Service (Amazon EKS) clusters, and additional security checks against your EKS configuration.

You can add other AWS environments to Sophos Cloud Optix in many ways. You must add EKS clusters with this method.

Before you can add EKS clusters to your environments, you need to:

- Install AWS CLI (version 1.16.96 or higher) on a Linux or Mac computer.
- Install AWS IAM Authenticator for Kubernetes for authentication to your EKS cluster.
- Install the kubectl utility to communicate with the cluster API server (select the version that corresponds to your EKS cluster).
- Ensure that the AWS account that you're using to add the cluster to Sophos Cloud Optix has permissions in the EKS cluster.
- Ensure that Endpoint Public Access is enabled.

Running the Sophos script creates a read-only service account in your EKS cluster, and adds the cluster to your Sophos Cloud Optix console.

1. Click **Settings > Environments > Add new Environment**
2. Under **Enable features for existing environments** select **Add Amazon EKS clusters**.
3. Download the Sophos Cloud Optix script.
4. Run the script.

Related tasks

AWS Quick-start (page 5)
These instructions tell you how to use the AWS Quick-start option to connect your AWS accounts to Sophos Cloud Optix easily.

Related reference

Installing the AWS CLI

Installing aws-iam-authenticator

Installing kubectl

Amazon EKS Cluster Endpoint Access Control

3.5 Resources created in your AWS environments

A full deployment of Sophos Cloud Optix adds AWS environments to the service and sets up communication between AWS and Sophos.

There are three full deployment methods:

- Using the Sophos Cloud Optix AWS CLI script provided for Linux and macOS.
- Using AWS CloudFormation.
- Using the Terraform template provided.

Full deployment sets up two communication channels with the environment:

- Pull channel to gather infrastructure information about instances, security groups, etc. This uses a read-only IAM Role in your AWS account.
- Push channel to export CloudTrail Logs and VPC Flow Logs to Sophos Cloud Optix for analysis. This requires resources to be created and configured in your AWS environment.

You can also set up Sophos Cloud Optix for AWS environments using **Quick-start**, which only sets up the pull channel. You can perform a full deployment to add the push channel later, if necessary.

Pull channel

To set up the pull channel Avid-Role, a read-only IAM role, is created.

If this role already exists in the environment, the deployment continues after checking for the appropriate policy permissions. If not, the new role is created, with the SecurityAudit AWS managed policy (*arn:aws:iam::aws:policy/SecurityAudit*) and the following additional permissions:

- *elasticfilesystem:DescribeMountTargetSecurityGroups*
- *elasticfilesystem:DescribeMountTargets*
- *sns:ListSubscriptions*
- *s3:GetAccountPublicAccessBlock*
- *ce:GetCostAndUsage*
- *ce:GetCostForecast*
- *ce:GetUsageForecast*
- *eks:List**

Push channel

Resources are required to export CloudTrail Logs and VPC Flow Logs to Sophos Cloud Optix.

To export CloudTrail Logs, the following resources are created and configured:

- A trail (CloudTrail) *CT-AvidSecure* to deliver AWS CloudTrail log events from all regions to an S3 bucket *avid-cloudtrail-<ACCOUNT>*. If the bucket doesn't already exist in your account, it's created. The trail is configured to log all management and data events, and deliver to the newly created log group *CT-Avid-LogGroup* for CloudWatch.
- A role *Avid-CT-to-CW* for CloudTrail. This allows the CloudTrail to send events to CloudWatch and has the permissions for *s3:GetBucketAcl*, *s3:PutObject*, and is allowed to perform the following actions: *logs:CreateLogStream*, *logs:PutLogEvents*, on resources associated with log group *CT-Avid-LogGroup*.
- A role *Avid-Lambda-to-CloudWatch*. This allows an AWS Lambda function to read CloudWatch events using the policy permission *arn:aws:iam::aws:policy/CloudWatchEventsReadOnlyAccess*. The role can do the following actions: *logs:CreateLogGroup*, *logs:CreateLogStream*, *logs:DescribeLogGroups*, *logs:DescribeLogStreams*, *logs:PutLogEvents*.
- A subscription filter is created and associated with *CT-Avid-LogGroup* to subscribe to the real-time stream of log events and deliver them to the AWS Lambda function *Avid-CloudTrail-function*. The Lambda function reads and parses the log, and sends the parsed events to Sophos Cloud Optix.

VPC Flow Logs are turned on and exported to the Sophos Cloud Optix service for analysis.

Note
You can choose not to export VPC Flow Logs to Sophos Cloud Optix, or only export VPC Flow Logs from specific AWS regions. If you do this, some advanced features such as AI-powered anomaly detection and traffic visibility in **Network Visualization**, will not work.

To export VPC Flow Logs the following steps are taken:

- VPC Flow Logs are turned on to capture IP traffic information and publish it to CloudWatch Logs under log group *Flowlogs-Avid-LogGroup*.
- An IAM role *Avid-VPCFlow-Role* is created, which allows the AWS VPC-Flow-Logs to perform the following actions: *logs:CreateLogGroup*, *logs:CreateLogStream*, *logs:DescribeLogGroups*, *logs:DescribeLogStreams*, *logs:PutLogEvents*.
- A subscription filter is created and associated with *Flowlogs-Avid-LogGroup* to subscribe to the real-time stream of log events and deliver them to the AWS Lambda function *Avid-VPC-LOGS-function*. The Lambda function reads and parses the flow logs and sends them to Sophos Cloud Optix.

3.6 Troubleshooting for AWS

If there are problems with adding an AWS environment, run the uninstall script and try again.

There is a link to the uninstall script in the product. Do as follows.

1. Click **Settings** (in the left-hand menu) and select **Environments**.
2. Make sure you're on the **Cloud Environments** tab.
3. Find the environment with problems and click the dustbin icon (on the right of the page).

   You'll see a dialog that includes the script you need.
4. Run the script provided. Then add your AWS environment again.

3.7 Add remediation (Guardrails)

You can enable remediation features for AWS environments.

By default, Sophos Cloud Optix needs only Read-only access to your AWS environment.

If you want to enable the optional remediation features (Guardrails), you need to set up additional roles:

1. Go to **Settings > Environments**.
2. Select an AWS environment and click **Edit** (the pen icon on the far right).
3. Follow the instructions provided and generate the **Remediate Role ARN** and **Remediate External Id**.

Now you can start using remediation.

See Turn on automatic remediation or Use manual remediation.

Related tasks

Turn on automatic remediation (page 45)
How to turn on automatic remediation.

Use manual remediation (page 45)

How to use manual remediation.

3.8 Permissions needed to run Sophos Cloud Optix scripts for AWS

You can create custom roles with the appropriate permissions needed to run the Sophos Cloud Optix scripts that add AWS environments.

Generally, we recommend that you run the Sophos Cloud Optix scripts using an IAM "Administrator" role. However, if you want to run the script with limited permissions, you can use the permissions provided here to create a custom role.

The permissions you need vary depending on whether you want to add or delete an environment, or add remediation.

Permissions needed to add an AWS environment

Set the permissions for adding an AWS environment as follows.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:AttachRolePolicy",
                "iam:PutRolePolicy",
                "iam:PassRole",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:GetPolicy",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:ListAttachedRolePolicies",

                "ec2:DescribeFlowLogs",
                "ec2:CreateFlowLogs",
                "ec2:DeleteFlowLogs",
                "ec2:DescribeVpcs",

                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:PutBucketPolicy",
                "s3:PutEncryptionConfiguration",
                "s3:Get*",

                "sts:GetCallerIdentity",

                "lambda:AddPermission",
                "lambda:CreateFunction",
                "lambda:GetFunction",
                "lambda:GetPolicy",
                "lambda:ListVersionsByFunction",

                "cloudtrail:CreateTrail",
                "cloudtrail:DescribeTrails",
                "cloudtrail:PutEventSelectors",
                "cloudtrail:StartLogging",
                "cloudtrail:UpdateTrail",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:ListTags",
                "cloudtrail:GetEventSelectors",

                "logs:CreateLogGroup",
                "logs:DeleteLogGroup",
                "logs:DescribeLogGroups",
                "logs:PutSubscriptionFilter",
                "logs:PutRetentionPolicy",
                "logs:ListTagsLogGroup"
            ],
            "Resource": "*"
        }
```

Permissions needed to delete an AWS environment

Set the permissions for deleting an AWS environment as follows.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",

                "ec2:DeleteFlowLogs",
                "ec2:DescribeFlowLogs",

                "sts:GetCallerIdentity",

                "lambda:DeleteFunction",
                "lambda:GetFunction",

                "cloudtrail:DeleteTrail",

                "logs:DeleteLogGroup",
                "logs:DescribeLogGroups"
            ],
            "Resource": "*"
        }
    ]
}
```

Permissions needed to enable remediation features

Set the permissions for enabling remediation features as follows.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreatePolicyVersion",
                "iam:CreateRole",
                "iam:DeletePolicyVersion",
                "iam:GetPolicy",
                "iam:GetRole",
                "iam:ListPolicyVersions",

                "sts:GetCallerIdentity"
            ],
            "Resource": "*"
        }
    ]
}
```

3.9 AWS CLI script variables

AWS script variables

Required variables

The script for adding an AWS environment takes the following variables:

Variable	Description
EXTERNAL _ID	Specify this for the assumed role that Sophos Cloud Optix uses when acting on your behalf. It is added in the trust policy of the read-only role that Sophos Cloud Optix creates in your environment.
CUSTOMER_ID	The Customer UUID used for all uploads and connections.

Variable	Description
REQUEST_ID	The self-generated ID used to validate the account addition request and associate the callback from the environment for linking the account added. The *REQUEST_ID* keeps refreshing and is valid for 7 days to allow multiple environments to be added from within a customer account via scripting.
DNS_PREFIX_FLOW	The customer specific prefix that allows connection back to the appropriate collector node in the Sophos Cloud Optix backend for flowlogs.
DNS_PREFIX_CLOUDTRAIL	The customer specific prefix that allows connection back to the appropriate collector node in the Sophos Cloud Optix backend for CloudTrial logs.

Optional variables

Optionally, the script can also use the following variables if they are specified:

Variable	Description
AWS_DEFAULT_REGION	Use this if you want to install in a region that is different than your configured default region for AWS CLI.
TRAIL_NAME	Use this if you want to reuse an existing CloudTrail instead of creating a new one (The default installation creates a new CloudTrail). Enter the existing trailname. Please note that a Lambda function should be attachable to the corresponding CloudWatch log group.
FLOW_LOGS	The default install enables VPC Flow Logs for every Amazon VPC across all regions. Specify 0 to skip VPC flow log enablement. If you want to control specific regions for flow logs, you should specify 1 and provide the list of regions in the variable *FLOWLOG_REGIONS*.
FLOWLOG_REGIONS	Command separated list of AWS regions.

3.10 Set up AWS CLI to run scripts

To add environments with scripts you must first set up the AWS CLI.

Introduction

Sophos provides scripts you can use with the AWS Command Line Interface (CLI) as a convenient way to add AWS accounts to Sophos Cloud Optix, add EKS clusters, delete environments, turn on remediation features, and more.

To use these scripts you must install and configure AWS CLI version 1.11.188 (or higher) on a Linux or macOS computer.

You must do as follows:

- Set up your AWS account to run scripts.
- Set up the AWS CLI and run the Sophos script You can do this on your local computer or on an EC2 instance.

Full instructions are in the sections below.

For more information, see Universal Command Line Interface for Amazon Web Services

Related concepts

Permissions needed to run Sophos Cloud Optix scripts for AWS (page 17)
You can create custom roles with the appropriate permissions needed to run the Sophos Cloud Optix scripts that add AWS environments.

Related reference

Installing the AWS CLI
Configuring the AWS CLI
Universal Command Line Interface for Amazon Web Services
Attaching an IAM Role to an Instance

Setting up your AWS account to run scripts

You must create a new user or Identity and Access Management (IAM) role in your AWS account, with the permissions needed to run the Sophos Cloud Optix script that you want to use. For convenience, you can run Sophos Cloud Optix scripts using an IAM administrator role.

If you want to run the scripts with limited permissions, you can create a custom IAM role with the specific permissions provided. See Permissions needed to run Sophos Cloud Optix scripts.

Setting up the AWS CLI on your local computer

Do as follows:

1. Install the AWS CLI on your Linux or macOS computer. See Installing the AWS CLI.
2. Configure the AWS CLI with the IAM Role or User that you created in step 1, using Access Keys. See Configuring the AWS CLI

3. Use the AWS CLI to download the script from Sophos and run it using the command provided in the Cloud Optix console. The script URL and command will depend on the script that you want to run.

Setting up the AWS CLI on an EC2 instance

Do as follows:

1. Create a Linux EC2 instance in your AWS account, or use an existing one.
2. Attach the IAM Role that you created in step 1 to this instance. See Attaching an IAM Role to an instance
3. Install the AWS CLI on your Linux EC2 instance. See Installing the AWS CLI
4. Use the AWS CLI to download the script from Sophos and run it using the command provided in the Cloud Optix console. The script URL and command will depend on the script that you want to run.

3.11 Remove your AWS environment

You can remove your AWS environment from Sophos Cloud Optix.

Introduction

There are three methods of removing an AWS environment:

- Use Sophos Cloud Optix.
- Use an AWS CLI script, if you don't have access to Sophos Cloud Optix.
- Use Terraform, if the environment was added with Terraform.

Related information

Set up AWS CLI to run scripts (page 22)
To add environments with scripts you must first set up the AWS CLI.

Using the Sophos Cloud Optix console

Removing an AWS environment with the console.

Do as follows:

1. Go to **Settings > Environments**.
2. Follow the instructions.

Using an AWS CLI script

You can remove an AWS environment with a script provided by Sophos.

This method is useful if you can't access the Sophos Cloud Optix console. Do as follows:

1. From the AWS CLI download the script to your system.

Enter the following command: `curl -s "http://avidcore.s3-us-west-2.amazonaws.com/undo-add-account.sh" -o undo-add-account.sh`

2. Run the script using the command: `bash undo-add-account.sh`

The script removes the environment from Sophos Cloud Optix and removes the Sophos Cloud Optix resources from your AWS environment.

Using Terraform

You can remove environments you created with Terraform.

When you add an AWS environment to Sophos Cloud Optix using Terraform, a `.tfstate` is created, with details of the resources that were created. If the `.tfstate` still exists you can remove the environment. To do this use the `terraform destroy` command.

When prompted to enter a region, you must enter the same value used when you added the environment to Sophos Cloud Optix.

If you no longer have the `.tfstate` file you can use the AWS CLI script to remove your environment.

4 Add your Microsoft Azure environment

You can add your Azure environment to Sophos Cloud Optix by running the PowerShell script Sophos provides.

Note
By adding your Microsoft Azure environment, you authorize Sophos to access information via APIs and collect log data from your environment. For some data, such as network flow logs, your cloud provider may charge you. See Cloud provider charges or contact your provider for details. You can choose not to enable export of network flow logs if you don't need the advanced features that require this data.

You must run the PowerShell script in Cloud Shell. Access this from your Azure portal.

Warning
You must not run the script using Windows PowerShell on your computer.

Sophos Cloud Optix can't connect to free trial Azure accounts. This is because of a restriction in the subscription permissions with free trials of Azure.

To add your Azure subscriptions, you must run the script provided by Sophos. This registers an application in your Azure AD tenant. You can run the script as many times as you need to.

The user who first runs the script must have the Application Administrator role. One or more users can then add subscriptions by rerunning the script if needed. They must have the Owner role for each subscription they add to Sophos Cloud Optix.

For example, for multiple subscriptions, a user logged into Azure with the Application administrator role for your Azure tenant permissions runs it first. Users with the subscription Owner role for each subscription then rerun it to add the Azure subscriptions.

You can change the settings for your deployment using **Custom settings**. For example, you may not want to turn on network flow logs.

If you want to include AKS clusters, you must sign in to Azure with a profile that has the Cluster Admin role for each AKS cluster that you add. You can exclude AKS clusters in **Custom settings**.

To run the script, do as follows:

1. Click **Settings** and select **Environments**.
2. Click **Add New Environment**.
3. On **Add your Cloud Provider environment**, select **Azure**.
4. Click **Add an Azure subscription using a script in Azure PowerShell (includes AKS Clusters)**
5. Follow the steps shown to go to Azure and open Azure PowerShell.

   You must not run the script using Windows PowerShell on your computer.
6. Download the script using the command provided in Sophos Cloud Optix.
7. Click **Custom settings** to review the settings and change them if you need to.

   If you change the settings, you must copy the command in **Custom settings**. You use this when you run the script, not the command on the main screen.
8. Close **Custom settings**.
9. Run the script in Azure PowerShell, using either the command provided in Sophos Cloud Optix, or the one you copied from **Custom settings**.

The script lets you choose all subscriptions or only the subscriptions you want to add.

The script creates an AD application, a service principal, adds a response URL, and grants permissions at subscription level.

If you have all the required Azure roles to create the Enterprise App for your tenant (the Application Administrator role) and add your subscriptions (the Owner role for each subscription), you don't need to rerun the script. Other users can re-run the script to add subscriptions, if required.

After the script has run, you must turn on user and group data sync with Azure AD, using an admin account for the subscriptions you've added. To do this, go to the URL shown at the end of the script. You must be an Application Administrator in the Active Directory containing the subscriptions you added. If you aren't, ask an Application Administrator to authenticate for you.

Related concepts

What does the Sophos Cloud Optix script for Azure do? (page 26)
The script sets up Sophos Cloud Optix so that it can receive data from your Azure AD environment.

Related tasks

Troubleshooting for Azure (page 30)
How to resolve problems with adding Azure environments.

Related reference

Quickstart for PowerShell in Azure Cloud Shell

4.1 What does the Sophos Cloud Optix script for Azure do?

The script sets up Sophos Cloud Optix so that it can receive data from your Azure AD environment.

It enables Sophos Cloud Optix to receive data for your Azure subscriptions, users and groups in Azure AD, as well as flow log data. The script does as follows:

1. Creates an Azure Active Directory application, then creates an Azure service principal with it. It then assigns a Reader role to the service principal for all subscriptions (or individual subscriptions if you specify them when running the script). The service principal is a built-in role provided by Azure and takes the following attributes:

Attribute	Description
Active Directory application name:	*`AvidSecure Monitor App 999x9`*
Service principal:	A security identity used by applications or services to access specific Azure resources. This acts as a user identity (username and password or certificate) for an application.
Role details:	Role name: *`Reader`* Description: The Reader role allows the Active Directory application to read data in your company or school directory, such as users, groups, and apps. This role does not have permissions to make any changes. Permission: *`Directory.Read.All`* (admin consent for this is requested when the script completes).

2. Assigns permissions to the Active Directory application (*AvidSecure Monitor App 999x9*) for each Azure subscription. This enables Sophos Cloud Optix to read the *FlowLogs Enabled* status for all Network Security Groups (NSGs). The following attributes are used:

Attribute	Description
Role name:	*AvidFlowLogsReader + <first 8 characters of subscription id without '-'>*
Permission:	*Microsoft.Network/networkWatchers/queryFlowLogStatus/action*

3. Enables Microsoft.Insights to enable flow logs.
4. For each Azure subscription, the script then does as follows:

   a) Creates a Network Watcher custom role, which is assigned to an Azure Function that Sophos Cloud Optix creates. This enables the export of flow logs for current NSGs and new NSGs that are created. The setup includes enabling flow logs in Network Watcher, and creating Storage Accounts and an Azure Function App, to export flow logs to Sophos Cloud Optix.

   Note
   The Azure Function that uses the AvidNetWatcher role with these permissions is within your Azure environment. Once created, Sophos does not own or control it.

   The attributes used to create the role are as follows:

Attribute	Description
Role name:	This role can configure flow logs, list storage and NSG resources, create/delete storage accounts, list keys, and create/delete Azure Functions. These permissions are required to automatically create and remove the resources needed to export flow logs to Sophos Cloud Optix, when new NSGs are created and removed in your environment.

Attribute	Description
Description:	*AvidNetWatcher + <First 8 characters of subscription id without '-'>*
Permissions:	`Microsoft.Authorization/*/Read; Microsoft.Storage/storageAccounts/listServiceSas/Action; Microsoft.Storage/storageAccounts/*/Write; Microsoft.Compute/virtualMachines/Read; Microsoft.Compute/virtualMachines/Write; Microsoft.Compute/virtualMachines/Delete; Microsoft.Compute/virtualMachines/extensions/Read; Microsoft.Compute/virtualMachines/extensions/Write; Microsoft.Compute/virtualMachines/extensions/Delete; Microsoft.Compute/virtualMachineScaleSets/Read; Microsoft.Compute/virtualMachineScaleSets/Write; Microsoft.Compute/virtualMachineScaleSets/Delete; Microsoft.Compute/virtualMachineScaleSets/extensions/Read; Microsoft.Compute/virtualMachineScaleSets/extensions/Write; Microsoft.Compute/virtualMachineScaleSets/extensions/Delete; Microsoft.Insights/alertRules/*; Microsoft.Support/*; Microsoft.Network/*/read; Microsoft.Storage/*/read; Microsoft.Storage/storageAccounts/write; Microsoft.Storage/storageAccounts/Delete; Microsoft.Resources/deployments/*; Microsoft.Web/sites/functions/*; Microsoft.Storage/storageAccounts/listkeys/action; Microsoft.Resources/subscriptions/resourceGroups/*; Microsoft.Resources/deployments/operations/*; Microsoft.Web/serverfarms/write; Microsoft.Web/serverfarms/delete; Microsoft.Web/sites/write; Microsoft.Web/sites/delete; Microsoft.Web/*/read; Microsoft.Web/sites/sourcecontrols/write; Microsoft.Web/sites/sourcecontrols/delete; Microsoft.Network/*/action; Microsoft.Network/*/write; Microsoft.Compute/*/action; Microsoft.Compute/*/delete; Microsoft.Compute/*/write`

b) Creates a resource group for the subscription with the following attributes:

Attribute	Description
Name:	*avidflowlogsgroup*

Attribute	Description
Description:	The Sophos Cloud Optix script creates all the necessary resources, for example storage accounts or function apps, under this resource group, for ease of management and removal, if required.

c) Creates a storage account to export activity logs for the subscription as follows:

Attribute	Description
Name:	*avidact + <first 8 characters of SubscriptionId without '-'> + <first 8 characters of CustomerId without '-'>*
Attributes:	A one-day retention policy is assigned to the storage account.

d) Enables Azure Network Watcher for each region to enable flow logs for all network security groups in that region. The region list is obtained from Azure APIs.

e) Creates an Activity Log monitor with the following attributes:

Attribute	Description
Name:	*AvidActivityLogCollector*
Description:	Azure Log Monitor archives Activity Logs to an Azure storage account.

f) Creates a function app to send Activity Logs from the Azure storage account mentioned above to Sophos Cloud Optix. A function app is created in each region with the following attributes:

Attribute	Description
Name:	*AvidActivityLogs + <first 8 characters of SubscriptionId without '-'> + <first 8 characters of CustomerId without '-'>*
Description:	This function also runs every 5 minutes to check for the resources required to export flow logs and enables them if necessary. It checks whether NSGs have flow logs enabled and checks for the presence of the required storage account. If required, the following attributes are used to create these resources: Function names use the format: *AvidFlowLogs + <first 8 characters of SubscriptionId without '-'> + <first 8 characters of CustomerId without '-'> + 4 character region code* Storage Account names use the format: *avi + <first 8 characters of SubscriptionId without '-'> + <first 8 characters of CustomerId without '-'> + 4 character region code*

g) Creates a managed identity for the Activity Log function app. A managed identity enables Azure resources to authenticate to cloud services without storing credentials in code.

h) Assigns the Network Watcher role described earlier in this document to the Activity Log function app.

5. Adds all Azure AKS clusters to Sophos Cloud Optix, if this option is selected in Sophos Cloud Optix. For each AKS cluster, the script creates a service account called `avid-service-account` in the default namespace. The script creates a custom ClusterRole and ClusterRoleBinding, assigns the role to the service account, and sends the service account credentials to Sophos Cloud Optix.
6. Sends the subscription name, the subscription ID, the tenant ID, and the encrypted key for the AD application, to ClusterRole and ClusterRoleBinding. This adds the environment to the service.

When the script has finished, a URL is provided in the format: `"https://login.microsoftonline.com/(tenantId)/adminConsent?client_id=(appId)"`.

Visit this URL to authorize read-only access for Sophos Cloud Optix so that AD user and group information can be included in your inventory.

The script then sends an installation log file to Sophos Cloud Optix.

4.2 Troubleshooting for Azure

How to resolve problems with adding Azure environments.

Check the following:

1. You must run the on-boarding script provided by Sophos using Azure PowerShell on the Azure console. You must not use Windows PowerShell on a local computer.
2. Make sure the Azure environment has not already been added to a different Sophos Cloud Optix account. Environments can only be added to one account.
3. Make sure you have the required permissions in the Azure environment you want to add.
4. If you want to include AKS clusters when adding an Azure environment, check that the Azure account running the script has the additional permissions required.

If you still have problems, you can remove the environment and start again. To remove the environment, do as follows:

1. Check `avidsecure-script-output.log` for errors.
2. Follow the instructions in Remove your Azure environment (page 30).
3. Add your environment again.

Related tasks

Add your Microsoft Azure environment (page 25)
You can add your Azure environment to Sophos Cloud Optix by running the PowerShell script Sophos provides.

4.3 Remove your Azure environment

You can remove a **Microsoft Azure** environment from **Sophos Cloud Optix**.

You need to remove components from both **Sophos Cloud Optix** and **Microsoft Azure**.

In **Sophos Cloud Optix**, do as follows:

1. Click **Environments**.
2. In the list, find the environment you want to remove and click the trashcan icon.
3. Copy the commands shown. You'll need them later.
4. Confirm that you want to continue. Click **OK**.

In **Microsoft Azure**, do as follows:

5. Sign in to the Azure Portal.

> **Note**
> You need to be a user with at least the Owner role in the subscription and Application Administrator rights in Active Directory.

6. Go to the **Cloud Shell**.
7. Start a Powershell-based shell.
8. Paste in and run the first command from the instructions you copied earlier.
9. Paste in and run the second command.

   Wait for the script to finish running.

To check that the script has successfully removed Cloud Optix components from your Azure environments:

10. Go to **Azure Active Directory** and open **App Registrations**.
11. Select All apps from the drop-down menu and search for “Avid”.
12. If there are any apps called “AvidSecure Monitor App”, manually delete them.

5 Add your Google Cloud Platform environment

You can add a Google Cloud Platform (GCP) project to Sophos Cloud Optix by running the script Sophos provides.

Note
By adding your GCP environment, you authorize Sophos to access information via APIs and to collect log data from your environment. Your cloud provider may charge you for this. See Cloud provider charges or contact your provider for details.

Before you start:

- You must have billing enabled for your GCP project in your Google account. If it isn't, for example a free trial, Google restricts access to APIs that Cloud Optix needs and the script will fail.
- You need to create a read-only service account in a GCP project or projects.
- You need to run the Sophos Cloud Optix shell script in the cloud shell from a project that has admin access to the GCP projects that you intend to add to Sophos Cloud Optix.

You create the service account by running the shell script provided in Sophos Cloud Optix.

1. Click **Settings** (in the left-hand menu) and select **Environments**.
2. Click **Add New Environment**.
3. On the **Add your Cloud Provider environment** page, select the **GCP** tab.

   This gives you help with creating the service account needed.
4. Go to Google Cloud Platform and select the project where you want to create the service account.
5. Open Google Cloud Shell.
6. Download the script using the command provided on the **GCP** tab in Sophos Cloud Optix.
7. Run the script as shown there. The script lets you choose all projects or only the project(s) you want to add.

   ```
   CUSTOMER_ID=<…> REQUEST_ID=<…> GCPFlowUrl=<…> GCPActivityUrl=<…> bash onboard-gcp.sh
   ```

   Note
   Select **Include GKE** to include GKE clusters. This provides inventory details, topology visualization, and security best practice checks.

8. Allow Cloud Optix to access your IAM data (optional).

   Follow the remaining steps shown on the **GCP** tab. This enables G Suite Domain-wide Delegation to the Sophos Cloud Optix service account that has just been created.

   You need to be an admin of the domain associated with the organization in GCP.

Related concepts

What does the Sophos Cloud Optix script for GCP do? (page 33)

The script creates a read-only service account in a GCP project.

5.1 Add a GKE cluster to an existing GCP environment

You can add a GKE (Google Kubernetes Engine) cluster to a GCP project that's already been added to Sophos Cloud Optix.

Add a cluster as follows:

1. Click **Settings** (in the left-hand menu) and select **Environments**.
2. Click **Add New Environment**.
3. On the **Add your Cloud Provider environment** page, select the **GCP** tab.
4. Go to Google Cloud Platform and select your project.
5. Open Google Cloud Shell.
6. Download the script using the command provided on the **GCP** tab in Sophos Cloud Optix. Then run it in the form shown there:

   ```
   CUSTOMER_ID=<…> REQUEST_ID=<…> bash onboard-gke.sh
   ```

   This creates a read-only service account in each GKE cluster.
7. If you have restricted access to the cluster, whitelist the Sophos IP addresses (shown in Cloud Optix) in the firewall rules of your master node.

Sophos Cloud Optix now provides:

- Inventory details: GKE clusters, nodepools, nodes, pods, services, and more.
- Topology visualization: Instances are shown as GKE nodes.
- Security best practice checks for GKE clusters. These are added to the GCP CIS benchmark policy.

5.2 What does the Sophos Cloud Optix script for GCP do?

The script creates a read-only service account in a GCP project.

The script does the following to add the GCP projects:

- Creates service account `avid-read-account` in the chosen base project (it prompts you to specify the project where you need to create the service account).
- For each project in the account (or the specific list as input by you), the script does as follows:
  - Grants service account roles/viewer (for reading all inventory) and roles/iam.securityReviewer (for reading all IAM related data for CIS benchmarks).
  - Enables APIs required to fetch inventory data. APIs enabled are `cloudapis.googleapis.com`, `admin.googleapis.com`, `stackdriver.googleapis.com`,`sqladmin.googleapis.com`, `storage-api.googleapis.com`, `cloudbilling.googleapis.com`, `cloudresourcemanager.googleapis.com`, `compute.googleapis.com`, `cloudkms.googleapis.com`, `dns.googleapis.com`, `logging.googleapis.com`, `cloudfunctions.googleapis.com`, `cloudmonitoring.googleapis.com`, `monitoring.googleapis.com` and `storage-component.googleapis.com`.

- Enables flow logs for all subnets.
- Creates Storage Buckets to store flow logs and activity logs with a retention policy for buckets to be 1 day.
- Enables activity logs by modifying IAM policy (`Enable various log types [{"logType": "ADMIN_READ"},{"logType": "DATA_READ"},{"logType": "DATA_WRITE"}]`).
- Creates sink for flow logs and activity logs (writes log data from stackdriver to storage account). Filters are applied to get only flow logs data and only admin and write activity logs.
- Grants sinks permissions to write in the respective buckets. (A service account is created and attached to each sink, which is given permission to only write data in the respective storage account).
- Deploys functions to read logs from storage and send to avi-collector. The code of functions is picked from a zip file stored in Sophos Cloud Optix Google Cloud storage account. Functions read data from storage accounts whenever a new file is written and send it to the Sophos Cloud Optix platform.

- Generates key for Sophos Cloud Optix account.
- Sends service account information to the Sophos Cloud Optix platform.

Related tasks

Add your Google Cloud Platform environment (page 32)
You can add a Google Cloud Platform (GCP) project to Sophos Cloud Optix by running the script Sophos provides.

5.3 Remove your GCP environment

You can remove a Google Cloud Platform environment from **Sophos Cloud Optix**.

You need to remove components from **Sophos Cloud Optix** first, then from Google Cloud Platform (GCP).

In Sophos Cloud Optix, do as follows:

1. Click Environments.
2. In the list, find the environment you want to remove and click the trashcan icon.
3. Copy the commands shown. You'll need them later in GCP.
4. Confirm that you want to continue. Click OK.

In **GCP**, do as follows:

5. Sign in to the GCP console.
6. Open Google Cloud Shell.
7. Paste and run the first command that you copied earlier.
8. Paste and run the second command.

   Wait for the script to finish.

Check that the script has successfully removed Sophos Cloud Optix components from your GCP environment. To do this, look for resources with "Avid" in their name and manually delete them.

6 Add your Kubernetes environment

You can add a native Kubernetes cluster to Sophos Cloud Optix by running the script Sophos provides.

Note
A "native" cluster is one that you have installed on servers that you own and manage. It may be hosted in the cloud, or on-premises in your own environment, and differs from Kubernetes services managed by cloud providers (AWS, Azure, GCP).

Note
Sophos Cloud Optix also supports Google Kubernetes Engine (GKE). You can add GKE clusters to Sophos Cloud Optix when you add GCP environments.

To add a Kubernetes cluster, do as follows.

1. Click **Settings** (in the left-hand menu) and select **Environments**.
2. Click **Add New Environment**.
3. On the **Add your Cloud Provider environment** page, select the **K8s** tab.
   This shows you the script and other information you need.
4. Use SSH to access your cluster's master node.
   You need to be an admin for the cluster you want to add.
5. Download the script shown on the **K8s** tab in Sophos Cloud Optix.
6. Run the script using the command shown.
7. Whitelist the IP addresses shown. You do this in the security group of your master node.
   Ths enables Sophos Cloud Optix to access the Kubernetes API server.

Sophos Cloud Optix will pull the inventory data, perform CIS Benchmark security best practice checks on the environment, and report any potential weaknesses.

Related tasks

Add your Google Cloud Platform environment (page 32)
You can add a Google Cloud Platform (GCP) project to Sophos Cloud Optix by running the script Sophos provides.

7 Add your IaC environments

Sophos Cloud Optix can monitor code submitted to your Infrastructure as Code (IaC) repositories for potential security issues.

Sophos Cloud Optix can also monitor code submitted to your Continuous Integration and Continuous Delivery (CI/CD) pipeline.

This can identify potential security issues before they reach production. Sophos Cloud Optix can currently check Terraform, AWS CloudFormation, Ansible, Kubernetes, and Azure Resource Manager (ARM) IaC template files.

Sophos Cloud Optix provides integrations for GitHub, Bitbucket and Jenkins. You can also use the Sophos Cloud Optix REST API as part of your development processes and (CI/CD) pipelines. See Getting Started With Cloud Optix REST API.

If you use the GitHub and Bitbucket integrations, you must grant Cloud Optix access to your code repositories.

1. Click **Settings**.
2. Select **Environments**.
3. Click **Add New Environment**.
4. On the **Add your Cloud Provider environment** page, select the **IaC Environment** tab. This tab provides everything you need to get set up.

Related tasks

Add code repositories using GitHub (page 36)
Sophos provides a GitHub app which you can install to give Sophos Cloud Optix access to your repositories.

Add code repositories using Bitbucket (page 37)
Sophos provides a Bitbucket app that you can install to give Sophos Cloud Optix access to your repositories.

Add code repositories via Jenkins pipeline (page 39)
Sophos provides a script which you can add to Jenkins to give Sophos Cloud Optix access to your repositories.

Related reference

Getting Started With Cloud Optix REST API

7.1 Add code repositories using GitHub

Sophos provides a GitHub app which you can install to give Sophos Cloud Optix access to your repositories.

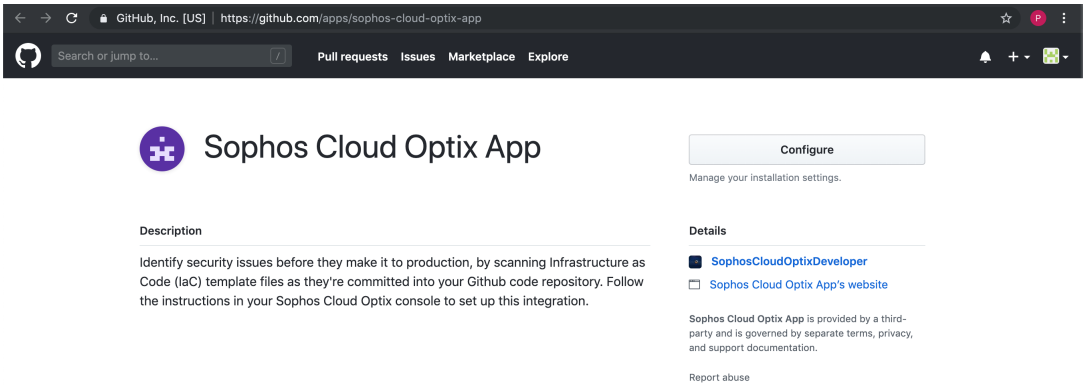
You can install the app in your GitHub account or your organization's account.

Once you have installed the app, it allows Sophos to scan the repository for configurations related to Terraform, AWS CloudFormation and so on, and identify potential vulnerabilities each time a push is made to the repository.

To install the app, do as follows.

Note
Before you start, ensure you've signed in to GitHub.

1. Click **Settings** (in the left-hand menu) and select **Environments**.
2. Click **Add New Environment**.
3. On the **Add your Cloud Provider environment** page, select the **IaC Environment** tab.
4. Click the link under **Integrate using GitHub App**.
   You see this screen:



5. Click **Configure**.
   This prompts you to install the app on your repositories (it may also show the option to install on your organization).
6. You now see a Sophos Cloud Optix welcome screen. If you are not redirected automatically enter your **Customer ID** and click **Configure**.

   The **Customer ID** is provided on the **IaC Environments** tab in Sophos Cloud Optix.

You are redirected to the **Environments** page in Sophos Cloud Optix.

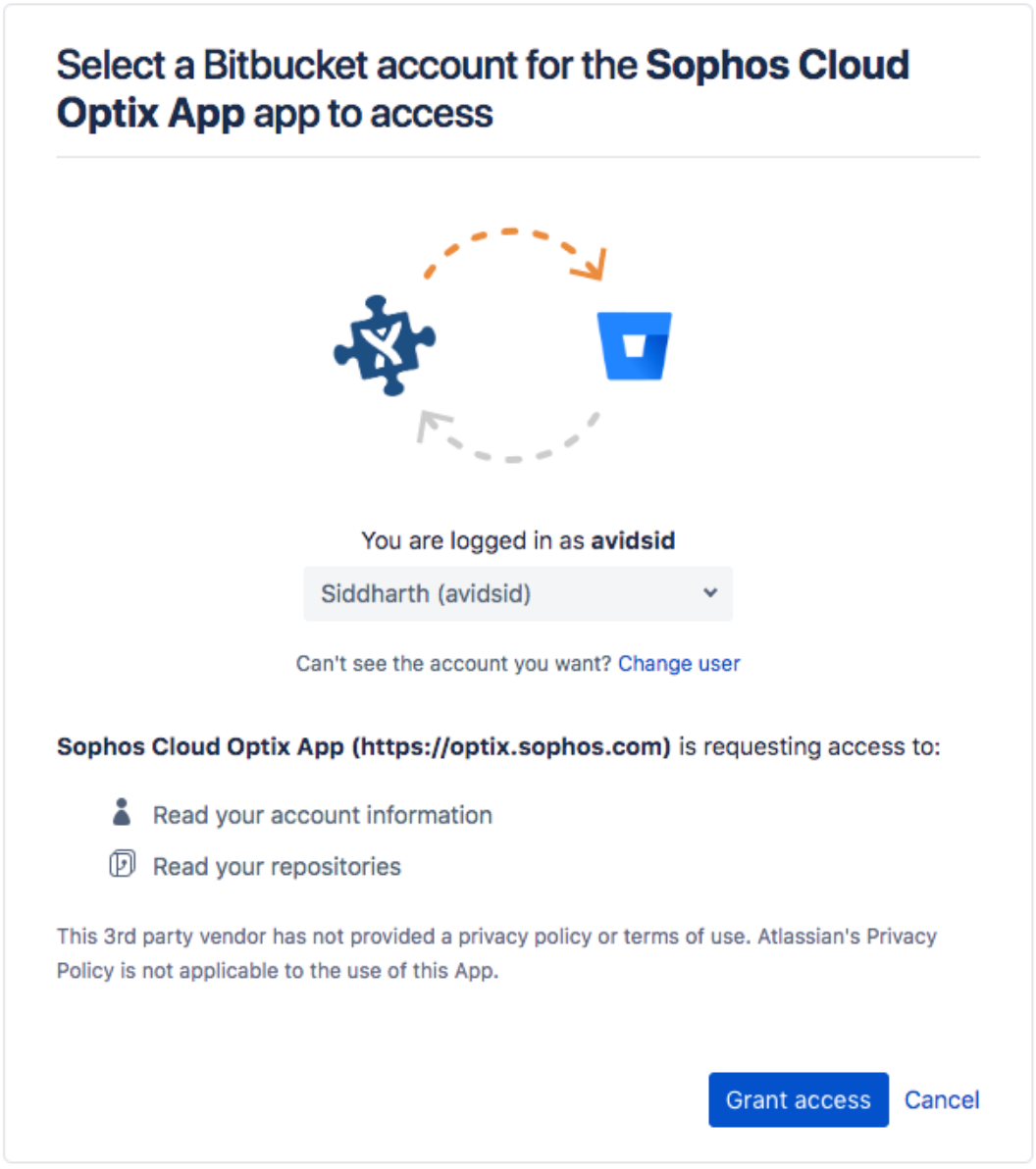
Note
The repositories you have given Sophos Cloud Optix access to are shown on the **IaC Environments** tab. Repositories are shown as **Pending** until a new change occurs in the repository. Sophos Cloud Optix will scan IaC templates in a repository when a change is first seen. The repository is then shown as **Active**.

7.2 Add code repositories using Bitbucket

Sophos provides a Bitbucket app that you can install to give Sophos Cloud Optix access to your repositories.

To install the Bitbucket app:

1. Click **Settings** (in the left-hand menu) and select **Environments**.
2. Click **Add New Environment**.
3. On the **Add your Cloud Provider environment** page, select the **IaC Environment** tab.
4. Click **Connect to Bitbucket**.
5. Select an account or a Team that you own. Click **Grant access**.



You are redirected to the **Environments** page in Sophos Cloud Optix.

Note
The repositories you have given Sophos Cloud Optix access to are shown on the **IaC Environments** tab. Repositories are shown as **Pending** until a new change occurs in the repository. Sophos Cloud Optix scans IaC templates in a repository when a change is first seen. The repository is then shown as **Active**.

7.3 Add code repositories via Jenkins pipeline

Sophos provides a script which you can add to Jenkins to give Sophos Cloud Optix access to your repositories.

Note
You can also use the Cloud Optix REST API as part of your development processes and Continuous Integration and Continuous Delivery (CI/CD) pipelines. See Getting Started With Cloud Optix REST API.

1. Click **Settings** (in the left-hand menu) and select **Environments**.
2. Click **Add New Environment**.
3. On the **Add your Cloud Provider environment** page, select the **IaC Environment** tab.
4. Copy the script shown under **Script for Jenkins Integrations** and add it to your build pipeline at the stage that best suits you.

When your pipeline next runs, you will see the repositories on the **IaC Environments** tab in the **Environments** page in Sophos Cloud Optix.

Related reference
Getting Started With Cloud Optix REST API

7.4 Monitor your IaC environment

You can monitor code repositories that you have added to Sophos Cloud Optix.

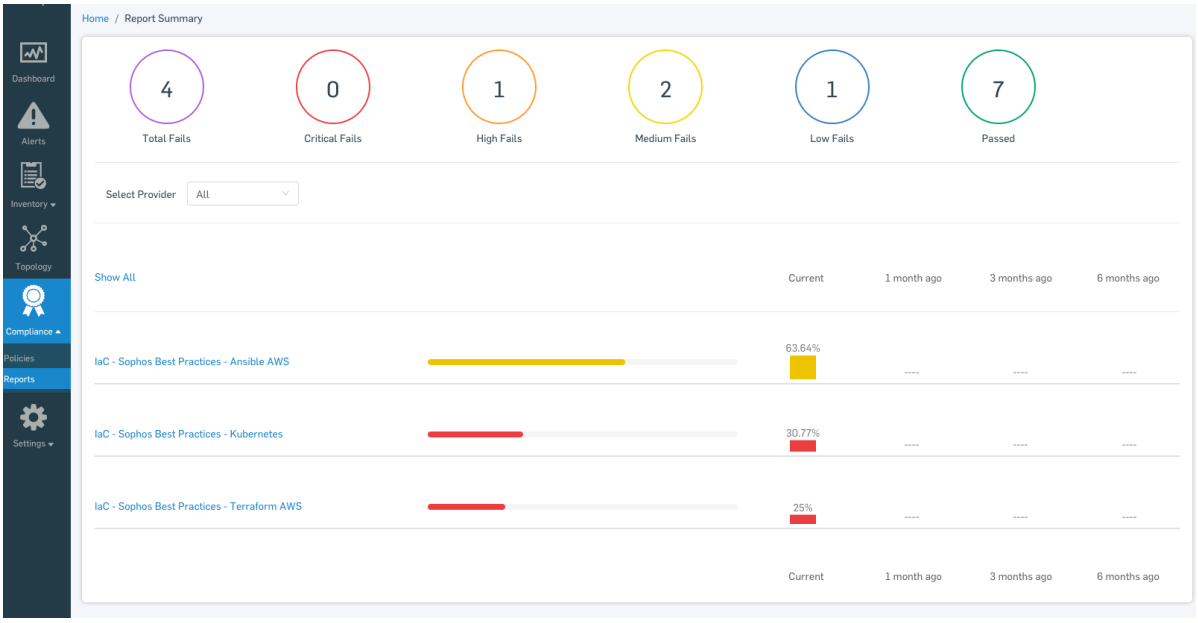
To see the repositories to which you have granted access, or from which events are received, go to **Settings > Environments** and look in the **IaC Environments** tab.

You can also see reports and alerts for your repositories.

Get IaC reports

You'll be able to see reports that have been generated based on the analysis of the files in your repositories. Go to **Compliance > Reports**.

Note
You will only see reports corresponding to configurations we can classify as related to Terraform, AWS CloudFormation, Kubernetes or Ansible. Hence you might not see reports on all repository push events.

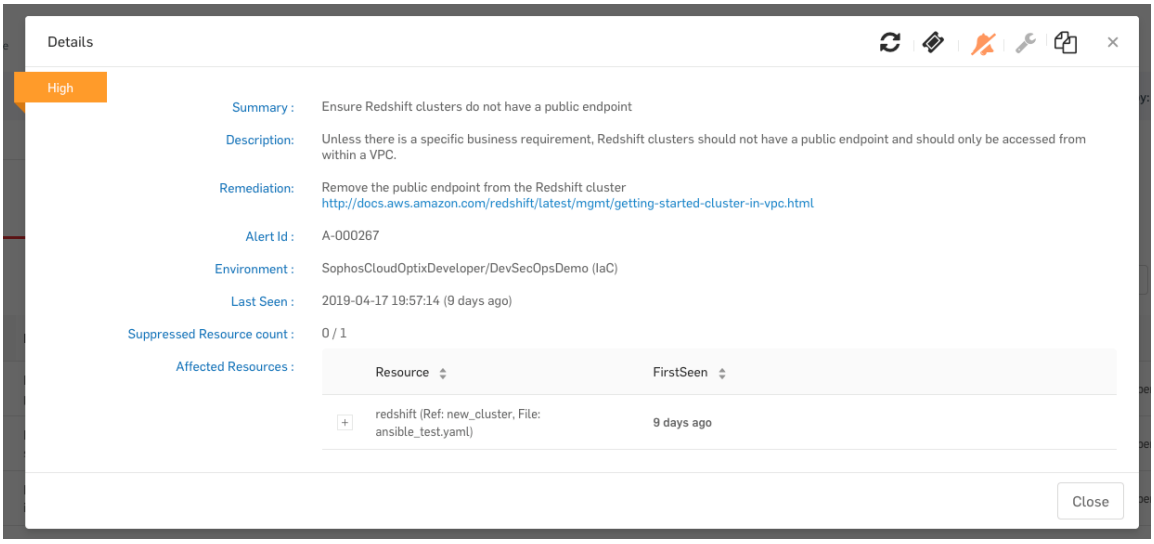


See IaC alerts

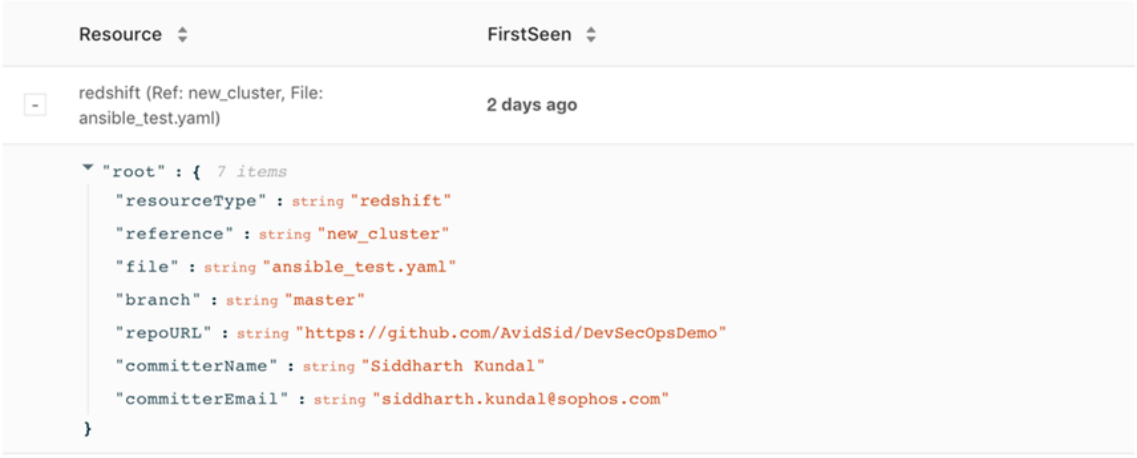
To see IaC alerts:

1. Go to **Alerts** and look for alerts with “IaC” in the **Type** column. You can filter the list to show only these alerts.
2. Look for alerts with “IaC” in the **Type** column. You can filter the list to show only these alerts.

3. Click on an alert to open a detailed overview.



4. Click the plus sign next to a resource for more details. This shows the branch, repository, file name and the variable which contains reference of the resource. You can use this information to identify the resource and fix the issue.



8 Remediation

You can use Sophos Cloud Optix for remediation of certain issues in AWS environments.

To use remediation, you must:

- Create the additional remediation role.
- Turn on automatic remediation (if you want it) or do remediation manually.

Related tasks

Create the remediation role (page 44)
This section tells you how to create the role needed before you can use remediation.

Turn on automatic remediation (page 45)
How to turn on automatic remediation.

Use manual remediation (page 45)
How to use manual remediation.

8.1 Create the remediation role

This section tells you how to create the role needed before you can use remediation.

By default, Sophos Cloud Optix uses read only permissions that are setup when you add AWS environments.

If you want to use remediation, you must run an additional script first, to provide specific write access permissions to your environment.

After you've added an AWS environment, do as follows:

1. Go to **Settings > Environments**.
2. Click **Edit environment** (the pen icon) beside the environment where you want to add remediation.
   The environment details are displayed.
3. At the bottom of the page, follow the link to instructions for creating the Remediate Role ARN and Remediate External Id.
4. You run the script shown via the AWS command-line interface.

The script creates a remediation role with the following permissions:

- s3:GetBucketAcl
- s3:PutBucketAcl
- s3:GetBucketPolicy
- s3:PutBucketPolicy
- s3:PutEncryptionConfiguration
- iam:GetAccountPasswordPolicy
- iam:UpdateAccountPasswordPolicy
- cloudtrail:UpdateTrail
- ec2:DeleteSecurityGroup
- ec2:DescribeSecurityGroups

- ec2:RevokeSecurityGroupIngress

8.2 Turn on automatic remediation

How to turn on automatic remediation.

1. Go to **Compliance > Policies**.
2. Find the policy where you want to turn on remediation. Click **Customize**.
3. In the list of rules, there's a **Guardrail** column. If the Guardrail option is shown next to a rule, click it to turn on automatic remediation for that rule.

The changes will take effect the next time Sophos Cloud Optix performs a scan.

8.3 Use manual remediation

How to use manual remediation.

1. Go to **Alerts**.
2. Click the **Alert ID** of an alert you want to remediate. This opens the alert details.
3. If the alert can be remediated, a wrench icon is shown in the top right. Click that and select the resources you want to remediate for this alert.

4. Click **Remediate**.

You'll get a pop-up message about the success or failure of remediation.

8.4 Which issues can you remediate?

Sophos Cloud Optix can remediate issues related to S3 buckets, security groups and IAM password policies, in AWS environments

This feature helps with administration and management. For example, it allows you to delete unused Security Groups, or to ensure that S3 buckets are properly protected according to your policy.

Sophos Cloud Optix currently supports remediation for the following rules:

IAM Password Policy

- Ensure IAM password policy requires at least one uppercase letter.
- Ensure IAM password policy requires at least one lowercase letter.
- Ensure IAM password policy requires at least one symbol.
- Ensure IAM password policy requires at least one number.
- Ensure IAM password policy requires minimum length of 14 or greater.
- Ensure IAM password policy prevents password reuse.
- Ensure IAM password policy expires passwords within 90 days or less.

S3 Bucket Encryption and Public Read/Write Permission

- Ensure encryption is turned on for S3 buckets.
- Ensure S3 buckets do not allow public read/list permission.
- Ensure S3 buckets do not allow public read/list bucket ACL permissions.
- Ensure S3 buckets do not allow public write permission.
- Ensure S3 buckets do not allow public write bucket ACL permissions.

Incident Management

- Ensure a support role has been created to manage incidents with AWS Support.

Sophos Cloud Optix Best Practices

- Flag resource(s) with public IP and Security Group with ingress from any source on any port.

9 Anomaly detection

Sophos Cloud Optix has several types of anomaly detection. They're turned on automatically.

The detection types are:

- User login anomalies.
- Outbound network traffic anomalies.
- Applications inferred from host behavior.
- High-risk activity.

Each of these detects security-related anomalous events based on account or user activities, API calls, flow log data, and network traffic patterns.

These detection types require different resources or learning periods to determine normal behavior. They can then identify unusual behavior.

Related concepts

About anomaly alerts (page 47)
Sophos Cloud Optix displays alerts when it detects anomalies in your environment.

User login anomalies (page 48)
Sophos Cloud Optix detects suspicious login events.

Outbound network traffic anomalies (page 48)
Sophos Cloud Optix detects anomalous outbound network traffic.

Applications inferred from host behavior (page 49)
Sophos Cloud Optix can infer the applications running from the behavior of the host computer instance.

High-risk activity (page 49)
Sophos Cloud Optix uses artificial intelligence (AI) to detect high-risk activity.

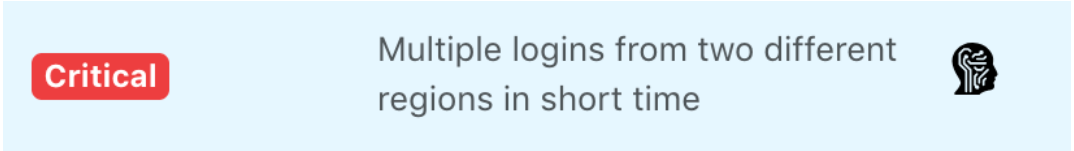
9.1 About anomaly alerts

Sophos Cloud Optix displays alerts when it detects anomalies in your environment.

On the **Alerts** page, look for alerts with this icon in the **Type** column:

Alternatively, click the **Type** filter and select **Anomaly (AI)**.

An anomaly alert looks like this:



9.2 User login anomalies

Sophos Cloud Optix detects suspicious login events.

This type of detection combines analysis of access time and location and user profiles. It learns what normal user activities in your cloud environment look like and then starts flagging suspicious events.

Use cases

This model detects suspicious console login events, API calls and assumed-role API calls to detect potential attacks based on compromised user credentials.

Learning period and customizations

This form of detection has a learning period of 7 days, after which it starts showing alerts.

It has a low rate of false positives and can be customized for a specific cloud environment via custom IP, role whitelists and alert suppression.

9.3 Outbound network traffic anomalies

Sophos Cloud Optix detects anomalous outbound network traffic.

This form of detection is a time series-based model. It learns the normal traffic flow in your environment, based on time and location patterns, and then detects unusual outbound traffic.

Use cases

This model helps in detecting suspicious spikes in traffic to find possible attacks that steal data.

Learning period and customizations

This form of detection has a self-training period of 21 days. Thereafter it starts showing alerts.

The current models are trained for each account ID and destination port. They are frequently retrained to capture the latest traffic behavior.

Alerts

Alerts for anomalous traffic include these details:

Field	Description
Account ID	Account ID
Timeframe	The time period of the deviation (30-minute slots)

Field	Description
Total Traffic	Total traffic observed in the timeframe
Expected Traffic	Traffic expected by machine learning models
Variation	Variation between actual and expected traffic
Destination port	Destination port
Destination protocol	Destination protocol
Top Originating IPs	Top IPs from which traffic flows
Top Destination IPs	Top IPs to which traffic flows

9.4 Applications inferred from host behavior

Sophos Cloud Optix can infer the applications running from the behavior of the host computer instance.

This form of detection uses a combination of instance metadata, traffic flow logs and security group information to accurately identify application workloads.

It uses set of rules that are continuously evolving and being refined by Sophos to improve detection in the customer environment.

Use cases

Provides better visibility into the cloud environment by inferring the running applications on different computer instances like Amazon EC2.

Learning period

Needs 1-day traffic flow logs before it can infer applications.

9.5 High-risk activity

Sophos Cloud Optix uses artificial intelligence (AI) to detect high-risk activity.

AI identifies high-risk events in cloud platform activity logs. It looks for activities that are unusual for particular identity access management (IAM) entities to perform.

Detected events are labeled as **High-risk** on the **Activity Logs** page and the dashboard.

Examples of events that could be labeled as high-risk are:

- Security Group changes
- NACL (Network Access Control List) changes

This helps you to focus on the most important issues.

10 Topology: network visualization

Sophos Cloud Optix provides network visualization for your cloud environment.

The **Topology** section shows both high-level and detailed information on your AWS, Azure and GCP networks, virtual machines, and any interconnections.

For example, the high-level view for AWS will show all VPCs in your AWS environment, along with any peer connections. This helps you understand entry and exit points which may need more security.

Note
If you've deployed Sophos UTM firewalls in your AWS environment, you'll see these in the network visualization.

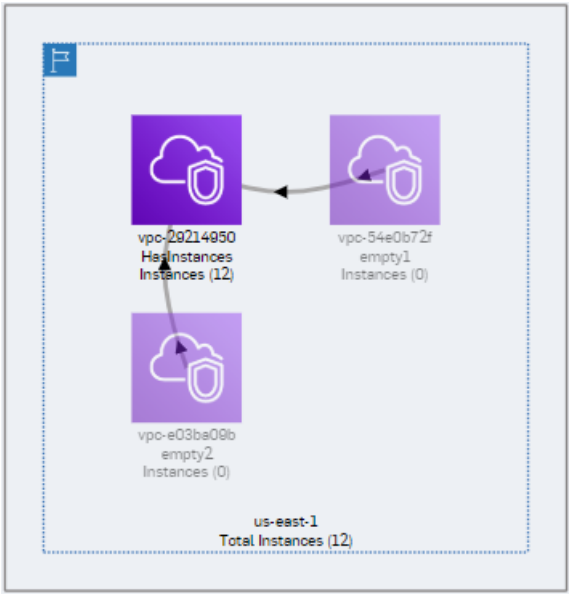
To use network visualization:

1. Go to **Topology**.
2. Select the environment type (for example, **AWS**) in the upper right of the page.
3. Click on any **VPC** to see detailed traffic flow and security information.

This shows the major resources of the VPC, including computer instances (EC2) and storage databases.

Note
If you have a large network layout, you can filter the visualization by tags, security groups, id or name.

Note
You can also export a visualization. Click the export icon in the upper right of the page. This generates an svg file of the current view.



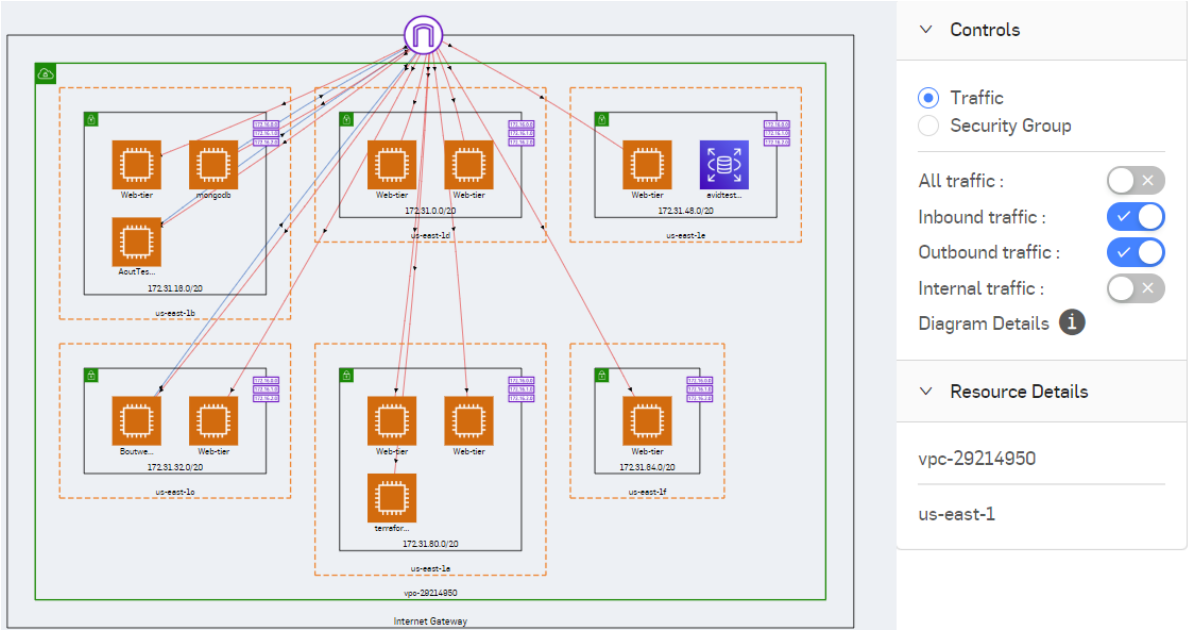
10.1 View traffic flow

Sophos Cloud Optix lets you view and analyze traffic flow in your cloud environment.

To view traffic flow:

1. Go to **Topology**.
2. Select the environment type (for example, **AWS**) in the upper right of the page.
3. Click on a **VPC**.
4. You can see a **Controls** panel on the right of the page.
   a) Select **Traffic** to view the actual traffic flow. This information is provided by VPC Flow Logs. You can view all traffic, or just the inbound, outbound, or internal traffic. The traffic lines are color coded to help you see which type of traffic is flowing. Click the icon next to **Traffic Details** to see a key to the colors.
   b) Select **Security Group** if you want to view the projected traffic pattern as allowed by the security groups configured in your environment.

The information displayed shows which of your resources have access to or from the public internet. This can help you identify areas where additional security may be useful or necessary.

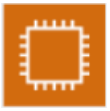


10.2 View host details

Sophos Cloud Optix shows details of hosts in your environment.

To view details:

1. Go to **Topology**.
2. Select the environment type (for example, **AWS**) in the upper right of the page.
3. Click on a **VPC**.
4. Click on a host.



Details are displayed in the **Resource Details** pane (on the right of the page). These include: inbound and outbound traffic ports, outbound traffic IPs, security groups, and tags applied to the host.

If we detect a Sophos UTM, we show the Sophos UTM icon instead.

Click the icon to see UTM version number, deployment type (standalone, HA or autoscaling) and a link to the UTM webadmin UI.

10.3 View inferred databases

Sophos Cloud Optix lets you view inferred database applications running on hosts.

This option uses instance metadata, traffic flow logs and security group information to accurately identify applications. The rules it uses are continuously being evaluated and added.

To view inferred databases:

1. Go to **Topology**.
2. Select the environment type (for example, **AWS**) in the upper right of the page.
3. Click on a **VPC**.
4. Turn on **Show inferred DBs**(at the top of the page).

10.4 IAM visualization

You can view AWS identity and access management (IAM) relationships.

Sophos Cloud Optix provides an easy-to-use visualization of your AWS identity and access management (IAM) principals, services and resources.

You can see relationships between services and resources such as IAM users, IAM groups, IAM roles, EC2 instances, and Lambda functions. This helps you assess the risks associated with granting access to services.

Use IAM visualization to answer important questions, such as:

- Which EC2 instances and Lambda functions have access to the S3 storage service?
- Which IAM users have access to the EC2 service?
- How do IAM users access a specific service, for example via group membership, IAM roles, or directly via in-line policies?
- Are any IAM users overprivileged? Do they have access to AWS services that they do not use?

To use IAM visualization, do as follows:

1. Go to **Inventory > IAM**.
2. Click the topology icon.
3. Select the AWS environment you want to investigate from the drop-down menu.
4. Use the **Resources** and **Services** filters, or the search box, to customize your visualization.
5. Click the icons to see additional information.

   For example, click the IAM group icon to see the IAM users in that group and the AWS services the group can access.

11 Spend Monitor

Monitor spending on cloud environments to quickly identify unauthorized usage.

Introduction

Unusual increases in spending on your environments can indicate security incidents, for example denial of wallet attacks. You can monitor spending regularly and set thresholds to receive alerts when unusual spending occurs.

Note
Spend monitoring data is not available in Sophos Cloud Optix for Azure subscriptions billed through Microsoft Cloud Solution Provider (CSP) plans.

Related concepts

Spend Monitor Thresholds (page 55)
You can configure rules to alert you if your cloud spend increases unexpectedly.

Compliance policies (page 57)
Sophos Cloud Optix provides security and compliance policies which give deeper insight into your current security posture.

Related reference

Export Cloud Billing data to BigQuery

Setting up environments for **Spend Monitor**

Spend Monitor must be turned on for each environment. It may already be turned on, depending on the environment type and when you added the environment to Sophos Cloud Optix. Once **Spend Monitor** is turned on you can set alert thresholds for each environment in **Compliance**.

Check what you need to do as follows:

- AWS environments: depending on when you added the account to Sophos Cloud Optix, you may need to add permissions in AWS so that Sophos Cloud Optix can access spend information. See Detailed set up instructions for AWS Environments.
- Azure environments: no additional permissions are required to allow Sophos Cloud Optix to access spend information. You may still need to turn on **Spend Monitor** in Sophos Cloud Optix.
- GCP environments: you must turn on Cloud Billing exports to BiqQuery in your Google account before you turn on **Spend Monitor** in Sophos Cloud Optix. See Export Cloud Billing data to BigQuery for more details. When Google has created a table containing billing information, go to **Settings > Environments** in Sophos Cloud Optix, enter the dataset and table name provided by BigQuery, then turn on **Spend Monitor**.

Detailed set up instructions for AWS environments

You must add the required permission to your AWS account before turning on **Spend Monitor**. Do as follows:

1. In your AWS console, go to your AWS account.
2. In **Roles**, select **Avid-Role**.
3. Click **Add Inline Policy**.
4. In **Service**, select **Cost Explorer Service**.
5. In **Action**, under **Read**, select **GetCostAndUsage**.
6. Name the policy and click **Create**.

Go to your Sophos Cloud Optix console to turn on **Spend Monitor**.

Turn on **Spend Monitor** in Sophos Cloud Optix

Once a cloud environment has been set up to link with **Spend Monitor** you must turn it on in Sophos Cloud Optix. For each environment do as follows:

1. Click **Settings**.
2. Click **Environments**.
3. Click the edit icon
   
   for the environment where you want to turn on spend monitoring.
4. Switch spend monitoring on.
5. Click **Save**.
6. Click **Spend Monitor** to see daily and monthly graphs and lists of spending on services.

Once **Spend Monitor** is turned on, the page provides the following:

- A graph of daily spend across AWS, Azure and GCP environments. Choose to see daily spend for all environments, or select a specific environment. Click the graph to see the top environments by spend on any day, and the top services that contributed to the spend on that day. Zoom out to see the daily spend for each day over the last 60 days.
- A graph of monthly spend over the last 6 months. Click the graph to see the top environments by spend in any month, and the top services that contributed to the spend in that month.
- A table showing the environments contributing most to your cloud spend, and the top services in terms of spend for those environments, for the current calendar month.

You can also set spending thresholds for individual environments in **Compliance**.

11.1 Spend Monitor Thresholds

You can configure rules to alert you if your cloud spend increases unexpectedly.

In the **Compliance** section, you'll find spend monitoring policies for AWS, Azure, and GCP, that include the following rules:

- Ensure that yesterday's total spend is not more than a set percentage higher than the previous day.

- Ensure that yesterday's total spend is not more than a set percentage higher than the same day last week.
- Ensure that the total spend in the last 30 days is not more than a set percentage higher than the previous 30 days.

By default, the rules are set to detect increases of 10%. You can configure this value for each rule.

If any threshold is exceeded, an entry in the **Result** column will show you how many rules failed.

You can click the entry in the **Result** column for more details.

12 Compliance policies

Sophos Cloud Optix provides security and compliance policies which give deeper insight into your current security posture.

It also provides ways for you to control and customize policies to meet the needs of your cloud environments.

Related concepts

Use out-of-the-box policies (page 57)
Sophos Cloud Optix provides out-of-the-box policies. These are based on popular standards, including cloud provider best practices (for example, AWS and Azure CIS Benchmarks).

Related tasks

Customize policies (page 57)
You can customize Sophos Cloud Optix policies for your needs.

View policy reports (page 58)
Sophos Cloud Optix automatically generates reports for all out-of-the-box and custom policies.

Track policy compliance (page 58)
Sophos Cloud Optix lets you track the compliance results over time.

12.1 Use out-of-the-box policies

Sophos Cloud Optix provides out-of-the-box policies. These are based on popular standards, including cloud provider best practices (for example, AWS and Azure CIS Benchmarks).

To see these policies, go to **Compliance > Out of Box Policies**.

You can do as follows:

- Click a policy name to see details of the rules it includes.
- Click **Enable** to apply the policy to your environments.
- Click **Customize** to create a custom policy. See Customize policies (page 57).

These policies assess security and compliance based on the information obtained via the API connections set up when you added your environment.

All the policies enabled in the environment run an assessment periodically and highlight any deviation via alerts and policy reports. You can see policy reports at **Compliance > Reports**.

12.2 Customize policies

You can customize Sophos Cloud Optix policies for your needs.

For example, you may want to do some of the following:

- Specify which environments the policy applies to (if you have different environments with different compliance needs.)
- Apply the policy only to certain resources or user groups.
- Remediate certain issues automatically.

To customize a policy:

1. Go to **Compliance > Policies**.
2. Do one of the following:
   - Click **Create Custom Policy** at the top of the page to create a completely new policy.
   - Select an existing policy in **Out of the Box Policies** and click **Customize**.
3. You can provide a **Policy Name** as well as **Compliance Tag** to differentiate the alerts that will be raised for this policy check.
4. Use the **Select Environments** filter if you want to specify the environments to check.
5. Use **Resource Tags** if you want to limit the policy's scope to certain resources (and so limit alerts).

   Tags are widely used in public cloud environments to logically group resources together: use the same tags here that you use in your environment.

   Note
   You can configure the tags as a key value pair, as you may have configured them in your environment.

6. In the list of rules, you can do as follows:
   - Choose whether rules are enabled.
   - Set the severity level of each rule.
   - Turn Guardrail (for auto-remediation) on or off, where this is available.
7. Click **Save**.

12.3 View policy reports

Sophos Cloud Optix automatically generates reports for all out-of-the-box and custom policies.

You can use these reports to assess the compliance status and get detailed information on the checks carried out and the number of checks passed or failed.

1. To see the reports, go to **Compliance > Reports**.

   All the reports are listed, together with historical data for their pass rate.
2. Click a report name to view the details, including when the report was last run and how many checks failed.

   You can export the report in PDF or CSV format.
3. Click the **Policy Name** link if you want to open more detailed results, which show:
   - Individual items in the compliance requirement that passed or failed.
   - An automatically concatenated list of affected resources.

   The detailed results page also lets you create a Jira or ServiceNow ticket, suppress the item, and remediate (if applicable).

12.4 Track policy compliance

Sophos Cloud Optix lets you track the compliance results over time.

You can look at the report history to track the progress of compliance and to find out when a particular compliance exception event first happened.

1. Go to **Compliance > Reports**.
2. Click a report name to open details.
3. In the **Reports** column, on the far right, click the **View history** icon (a rewind icon).

You now see the compliance status of the environment at any point in the past.

13 Integrations

You can integrate Sophos Cloud Optix with your existing business tools to automate cloud security monitoring, GRC (governance, risk and compliance) and DevSecOps processes.

These integrations can be enabled and customized at the **Settings > Integration** page.

13.1 Integrate with Jira

You can integrate Sophos Cloud Optix with Jira so that it can create or update Jira tickets for alerts.

In **Jira Integration** you configure the link between your Sophos Cloud Optix account and your Jira account, so that the two services can interact. In Jira integration permissions you'll find more detail on the Sophos Cloud Optix fields and permissions and how they are used in Jira.

In Sophos Cloud Optix, do as follows:

1. Go to **Settings > Integration**.
2. Click **Jira.**
3. Enter your Jira URL and the username and password needed to connect to it. Also enter the project key for the project where you want the tickets to be created.
4. In **Alert Levels**:
   a) Select which Sophos Cloud Optix alerts (for example, **Critical**) you want to create Jira tickets for.
   b) Optionally, change the Jira priority set for each alert level in Sophos Cloud Optix.
5. Select **Automatic** if you want to have Jira tickets created automatically when there is an alert.
   If you don't select this, the alert in Sophos Cloud Optix includes an option to create a Jira ticket manually.
6. In **Alert Post By**, choose how Jira updates tickets.
   - **Consolidated**: Updates the existing Jira ticket if another resource is affected by the same alert, or if the status changes (as in the Sophos Cloud Optix alerts page). This is the default.
   - **Affected Resources**: Creates a parent Jira ticket containing only the title of the alert. Then creates a separate Jira sub-task for each resource affected by the alert, puts the alert details in it, and links it to the parent.
7. To turn on the integration, click **Enable** and then **Save**.

In your alerts, you'll now see an option to create a ticket (if you accepted manual ticketing) and an icon linking to the Jira ticket when it's created.

Related concepts

Jira integration permissions (page 61)

Information on the Sophos Cloud Optix parameters in **Jira integration**.

13.1.1 Jira integration permissions

Information on the Sophos Cloud Optix parameters in **Jira integration**.

This section describes all the requirements, permissions used and fields accessed when creating, updating or deleting Jira tickets from Sophos Cloud Optix.

Create ticket

You need the following to create tickets in Jira:

- The Jira username must have permission to create tasks and sub-tasks in Jira.
- Your Jira configuration must allow all the fields referenced in the table to be set when creating a ticket.
- The priority configured in **Jira Integration** must match that in Jira exactly (it is case-sensitive).

Sophos Cloud Optix fields are used to populate fields in Jira in the following ways:

Jira field name	Description
Title	Sophos Cloud Optix: `Cloud-Provider` : `Account Name` - `Alert Summary`.
Description	`Alert ID`, `Alert Summary`, `Policy Name`, `Alert Description`, `Alert Remediation`.
Type	Set to `Task` or `Sub-Task`, depending whether **Alert Post By:** is set to **Consolidated** or **AffectedResources**.
Reporter	**UserName** as specified in **Jira integration**.
Labels	Sophos Cloud Optix Alert: `Account-Id`, `Alert-Id`, `Alert Summary`, `Account name`.
Priority	Controlled by the **Alert Levels > Jira priority** settings in **Jira integration**.
Comment	Populated after the Jira ticket is created, using **AffectedResources**.

Update ticket

The username must have permission to comment in Jira.

Jira field name	Description
Comment	Populated using **AffectedResources**.

Delete ticket

To delete tickets in Jira:

- The username must have permission to resolve tickets in Jira.
- The **Close Transition** name must match the one in Jira exactly.

Jira field name	Description
Status	**Done**.
Comment	Alert `Alert ID` has been closed by Sophos Cloud Optix.

Related tasks

Integrate with Jira (page 60)
You can integrate Sophos Cloud Optix with Jira so that it can create or update Jira tickets for alerts.

13.2 Integrate with Slack

Sophos Cloud Optix can push new alerts to your specified Slack channel for instant notification.

In Sophos Cloud Optix, do as follows:

1. Go to **Settings > Integrations**.
2. Click **Slack**.
3. Click **Authorize Slack**.
4. You are redirected to `slack.com`. Sign into your Slack account and authorize Sophos Cloud Optix to connect to it.
5. You are redirected to Sophos Cloud Optix **Slack Integration**.
6. Choose the Slack channel for Sophos Cloud Optix alerts.
7. Select which alerts you want to send to Slack.
8. To turn on the integration, click **Enable Config** and then **Save**.

13.3 Integrate with Teams

You can integrate Sophos Cloud Optix with Microsoft Teams to push new alerts to your specified channel.

Note
This feature is not yet available for all customers. To use this feature, contact your Sophos account manager.

You must first create an incoming webhook in Microsoft Teams for your channel. Then sign into Sophos Cloud Optix and use the webhook URL to connect to that channel.

To integrate with Microsoft Teams, do as follows:

1. In Microsoft Teams, add an incoming webhook to your channel.
2. Copy and save the unique URL for your webhook.
3. In Sophos Cloud Optix, click **Settings > Integrations**.
4. Click **Microsoft Teams**.
5. Paste the URL for your Microsoft Teams webhook in the **Webhook URL** field.

6. Click **Send OTP**.

   Sophos Cloud Optix sends a one-time passcode (OTP) to your Teams channel.
7. Go to Microsoft Teams and copy the OTP.
8. Go to your Sophos Cloud Optix account and paste the OTP into **Enter your OTP**.
9. Click **Verify**.
10. Select which alerts you want to send to Microsoft Teams.
11. Select **Enable** and click **Save**.

Related reference

Add an incoming webhook to a Teams channel

13.4 Integrate with ServiceNow

Sophos Cloud Optix can create and update ServiceNow tickets for alerts.

You must use a ServiceNow account that has the ITIL role. You also need the group name for the ServiceNow account.

In Sophos Cloud Optix, do as follows:

1. Go to **Settings > Integrations**.
2. Click **ServiceNow**.
3. Enter the ServiceNow URL, username and password, along with the assignment group for your tickets.

   The group name for the ServiceNow account goes in the **Assignment Group** field.
4. In **Alert Levels**:

   a) Select which Sophos Cloud Optix alerts (for example, **Critical**) you want to create ServiceNow tickets for.

   b) Optionally, change the ServiceNow priority set for each alert level in Sophos Cloud Optix.
5. Select **Automatic** if you want to have ServiceNow tickets created automatically when there is an alert.

   If you don't select this, the alert in Sophos Cloud Optix includes an option to create a ServiceNow ticket manually.
6. To turn on the integration, click **Enable** and then **Save**.

If there is a change in the status of an issue, or additional resources are affected, ServiceNow updates the existing ticket for the issue (if it is still open).

For example, if a policy violation alert is cleared the ServiceNow ticket is closed.

Related reference

ServiceNow Base system roles

13.5 Integrate with Splunk

Sophos Cloud Optix can send data to your Splunk Enterprise or Cloud instance using Splunk's HTTP event collector (HEC) interface.

Sophos Cloud Optix can send the following data:

- Security monitoring and compliance alerts.
- Anomaly alerts.
- GuardDuty alerts from AWS.
- Audit events generated in Sophos Cloud Optix (like user login, policy changes, configuration changes).
- DevSecOps alerts as a result of scanning IaC (infrastructure as code) templates.

To integrate with Splunk, do as follows:

1. In your **Splunk** instance, generate an HEC token.
2. In Sophos Cloud Optix, go to **Settings > Integration**.
3. Click **Splunk**.
4. Enter your Splunk **URL** and **HEC Token**.
5. In **Alert Levels**, select which Sophos Cloud Optix alerts (for example, **Critical**) you want to send to Splunk.
6. In **Alert Post By**, choose how alerts are updated:
   - **Consolidated**: A single alert is updated each time another resource is affected by the same alert type (as in the Sophos Cloud Optix alerts page).
   - **Affected Resources**: A separate alert is pushed for each affected resource.
7. Select **Enable Sophos Cloud Optix Logs** if you want to send audit events for Sophos Cloud Optix (including user login events, policy related events, and configuration changes) to Splunk for consolidation of all events.
8. To turn on the integration, click **Enable** and then **Save**.

13.6 Integrate with PagerDuty

You can push Sophos Cloud Optix alerts to PagerDuty.

In Sophos Cloud Optix, do as follows:

1. Go to **Settings > Integration**.
2. Click **PagerDuty**.
3. Enter the PagerDuty **URL**, your **User name**, **API key**, and **Service name**.
4. In **Alert Levels**:
   a) Select which Sophos Cloud Optix alerts (for example, **Critical**) you want to send to PagerDuty.
   b) Optionally, change the PagerDuty priority set for each alert level in Sophos Cloud Optix.
5. To turn on the integration, click **Enable** and then **Save**.

13.7 Integrate with Sophos Cloud Optix API

Some Sophos Cloud Optix functions can be programmatically accessed via API.

For the detailed API documentation, go to **Settings > Integrations > Sophos Cloud Optix API** or browse to https://optix.sophos.com/apiDocumentation.

13.8 Integrate with Amazon GuardDuty

Sophos Cloud Optix lets you aggregate Amazon GuardDuty alerts into the Sophos Cloud Optix dashboard, regardless of region.

This integration provides a consolidated view of all the AWS related security events.

When integration is turned on, other tools integrated with Sophos Cloud Optix (for example, Jira, Slack, ServiceNow, Splunk) automatically work for Amazon GuardDuty as well. GuardDuty alerts are sent as tickets or messages to those tools.

In Sophos Cloud Optix, do as follows:

1. Enable the Amazon GuardDuty service in your desired regions in your AWS Console.
2. In Sophos Cloud Optix, go to **Settings > Integration**.
3. Click **AWS GuardDuty**.
4. Find the configuration script provided there and run it via AWS CLI.

Once the script has run, any GuardDuty alerts automatically appear on the Sophos Cloud Optix dashboard.

13.9 Integrate with Amazon SNS

You can send Sophos Cloud Optix alerts to an Amazon SNS (Simple Notification Service) topic you've created in your AWS account.

As part of integration, you need to add the SNS:Publish permission to the Avid-Role role in the AWS account.

The instructions here tell you how to add that permission by using an AWS managed policy. For other ways to do it, see Set the AmazonSNS permission in AWS.

In your **AWS console**, do as follows:

1. Go to your AWS account.
2. Go to **Roles** and select **Avid-Role**.
3. Select **Attach Policy**, search for "AmazonSNSFullAccess" and attach it.

In **Sophos Cloud Optix**, do as follows:

4. Go to **Settings > Integration**.
5. Click **Amazon SNS**.
6. Turn on **Enable**.
7. In **AWS account**, select an account that you've added to Sophos Cloud Optix.
8. Enter the **SNS topic ARN** (Amazon Resource Name).
9. In **Alert Levels**, select the type(s) of alert that you want to send.
10. Click **Save**.

Sophos Cloud Optix sends a test message to your SNS topic.

Related concepts

Set the AmazonSNS permission in AWS (page 66)

You need to edit permissions in your AWS account before you integrate Sophos Cloud Optix with Amazon SNS.

13.9.1 Set the AmazonSNS permission in AWS

You need to edit permissions in your AWS account before you integrate Sophos Cloud Optix with Amazon SNS.

You can edit the permissions in one of the following ways.

Attach an AWS managed policy to the role

1. In your AWS console, go to your AWS account.
2. Go to **Roles** and select **Avid-Role**.
3. Select **Attach Policy**, search for "AmazonSNSFullAccess" and attach it.

Create a new policy and attach it to the role

1. In your AWS console, go to your AWS account.
2. Go to **Roles** and select **Avid-Role**.
3. Select **Attach Policy** and click **Create Policy**.
4. In the policy:
   - In **Service**, select **SNS**.
   - In **Action**, under **Write** select **Publish**.
   - In **Resource**, click **Specific** and click **Add ARN**. Add **Account-Id**, **Region** and **Topic Name**.
5. Name the policy and click **Create**.
6. In the **Attach** screen, search for the policy you've just created, and attach it to the role.

Create an inline policy

1. In your AWS console, go to your AWS account.
2. Go to **Roles** and select **Avid-Role**.
3. Click **Add Inline Policy**.
4. In the policy:
   - In **Service**, select **SNS**.
   - In **Action**, under **Write** select **Publish**.
   - In **Resource**, click **Specific** and click **Add Arn**. Add **Account-Id**, **Region** and **Topic Name**.
5. Name the policy and click **Create**.

13.10 Integrate with Azure Sentinel

Sophos Cloud Optix can send alert data to your Microsoft Azure Sentinel workspace.

Note
This feature is not yet available for all customers. To use this feature, contact your Sophos account manager.

To integrate with Azure Sentinel, do as follows:

1. In Azure Sentinel, create a new workspace to receive Sophos Cloud Optix alerts.
2. Copy and save the **Workspace ID** and the **Primary key** for your workspace.
3. In Sophos Cloud Optix, go to **Settings > Integrations**.
4. Click **Azure Sentinel**.
5. Enter the **Workspace ID** and **Primary Key** for the workspace you created in Azure Sentinel.

   The **Log Type** field controls the record type for the data sent to Azure Sentinel. Sophos sets this to `SophosCloudOptix`, or you can enter your own alternative.
6. In **Alert Levels**, select which Sophos Cloud Optix alerts you want to send to Azure Sentinel.
7. To turn on the integration, select **Enable**, and then click **Save**.

14 Search capabilities

Learn how to use search terms on your inventory data.

In Sophos Cloud Optix there are many search options. You can do as follows:

- Perform simple searches, for example you can enter an AWS EC2 name to find alerts related to that instance.
- Combine different search terms for advanced queries.
- Save searches so that you or other members of your team can run them.
- Search all of your inventory data or restrict your search to specific areas, for example Alerts or Containers. To do this use the drop-down list. If you are within a specific section of Sophos Cloud Optix, for example **Storage - AWS**, search defaults to that area. You can over-ride this using the drop-down list.
- Use the logical operators NOT, AND, and OR. They are not case sensitive.
- Specify date ranges.
- Combine different query terms in queries using logical operator precedence. You can modify the order expressions are used in with ellipses.

Example:	`s3 AND (tags.name:test* OR isPublic:true)`

For examples of complex searches, see Search examples.

Saved searches can be viewed, run, edited, and deleted from the **Search** page. Administrators using the same Sophos Cloud Optix account can see and update each others' searches. This allows administrators to create searches for other administrators to use. The names of the creator of a search and the person who last edited it are shown in the saved searches list.

Terms

You can search for terms used by the various cloud services supported by Sophos Cloud Optix.

The format is `<fieldName>:<fieldValue>`. If you don't specify a `fieldName`, all valid fields are searched for the `fieldValue`. Where you have nested fields you can match that by nesting `fieldName` terms in your search string.

Valid expressions for `fieldName` and `fieldValue` are single word tokens, phrases, boolean and numeric values. Regular expressions and wildcards are also supported in `fieldValue`.

Example:	`EC2 or instanceId:i-123456 OR isPublic:true or nodeCount:5 OR tags.Name:test OR tags.\*:security`

Use of wildcards

In `fieldValue` you can use a question mark to match a single character, or an asterisk to match several characters. The only supported wildcard for `fieldName` is the asterisk. You must precede it with a backslash as an escape character.

Example:	`test* OR tags.Name:Cluster?-nodepool* OR tags.\*_cluster_\*:test*`

For a full list of field names and values you can use, see Supported search field names.

Phrases

You can use phrases contained within double quotes in `fieldValue`. This is useful when searching for a continuous string of characters separated by white space.

Example:	`"testing purposes" OR description:"security group" OR kubeNode \*:"test container"`

Regular expressions

You can use regular expressions in `fieldValue`.

Example:	`/.*test*./ or name:/Cluster.*DoNotRemove/ or \*container\*:test`

Date ranges

You can use dates in range queries in the format yyyy-MM-dd. You can also use now to represent the current time.

You can also perform date math operations in date queries.

Note
Upper case M refers to months, lower case m refers to minutes.

Table 1: Date range examples

Required date range	Search string
A specific date, for example 2020-06-05	<fieldName>:[2020-06-05 TO 2020-06-05]
The last month	<fieldName>:[now-1M TO *]
This calendar year	<fieldName>:[now/y TO *]
A time between two specific dates	<fieldName>:[2020-01-01 TO 2020-06-05]
The last 15 days	<fieldName>:[now-15d TO *]
The last week	<fieldName>:[now-1w TO *]

Special characters

You can't use the period character in `fieldName` and you must use a backslash as an escape character before special characters like colons.

In `fieldValue` special characters like the colon or backslash can either be contained within double quotes or preceded by a backslash as an escape character.

Related reference

Supported search field names (page 70)
Tables of valid search field names and types.

Search examples (page 99)
See how to combine different terms to create complex searches.

14.1 Supported search field names

Tables of valid search field names and types.

To find specific information you can use these field names and field values in the search box, in the format:

<fieldName>:<fieldValue>

For example: `s3 AND isPublic:true`

Table 2: Alerts

Field name	Field type
alertType	String
alertSummary	String
alertId	String
lastSeen	Date
score	Numeric
provider	String
policies.policyTagName	String
level	String
state	String

AWS field names

Table 3: AWS - Hosts

Field name	Field type
instanceId	String
imageId	String
runningState	String
instanceType	String
region	String
availabilityZone	String
startTime	Date
launchedBy	String
subnetId	String
vpcId	String
isPublic	Boolean
isVulnerable	Boolean
hasContainerNodes	Boolean
tags.<tag-name>	String
patchStatus	String
outGoingIp	String
outGoingPort	String

Table 4: AWS - Clusters

Field name	Field type
instanceId	String
name	String
region	String
roleArn	String

Field name	Field type
version	String
createdAt	Date
status	String
vpcId	String
endpointPublicAccess	Boolean
endpointPrivateAccess	Boolean
isPublic	Boolean
isVulnerable	Boolean
tags.<tag-name>	String

Table 5: AWS - Node Groups

Field name	Field type
instanceId	String
name	String
region	String
createdTime	Date
desiredCapacity	Numeric
createdAt	Date
placementGroup	String
serviceLinkedRoleARN	String
status	String
subnets	String
launchConfiguration	String
tags.<tag-name>	String

Table 6: AWS - Nodes

Field name	Field type
instanceId	String

Field name	Field type
name	String
namespace	String
publicIp	String
vmId	String
podCIDR	String
startTime	Date
tags.<tag-name>	String

Table 7: AWS - Pods

Field name	Field type
instanceId	String
name	String
namespace	String
nodeName	String
status	String
startTime	Date
hostIP	String
isPublic	Boolean
isPrivileged	Boolean
tags.<tag-name>	String

Table 8: AWS - Containers

Field name	Field type
instanceId	String
name	String
image	String
imagePullPolicy	String
status	String

Field name	Field type
startedTime	Date
privileged	Boolean
kubeHost.nodeName	String
kubeHost.namespace	String
tags.<tag-name>	String

Table 9: AWS - Services

Field name	Field type
instanceId	String
name	String
image	String
imagePullPolicy	String
status	String
startTime	Date
privileged	Boolean
kubeHost.nodeName	String
kubeHost.namespace	String
tags.<tag-name>	String

Table 10: AWS - Ingress

Field name	Field type
instanceId	String
name	String
namespace	String
startTime	Date
tags.<tag-name>	String

Table 11: AWS - Network Policy

Field name	Field type
instanceId	String
name	String
namespace	String
startTime	Date
tags.<tag-name>	String

Table 12: AWS - RBAC Roles

Field name	Field type
instanceId	String
roleType	String
name	String
namespace	String
creationTime	Date
tags.<tag-name>	String

Table 13: AWS - VPCs

Field name	Field type
vpcId	String
region	String
cidrBlock	String
lastModifiedBy	String
evoNetworkACLS.aclId	String
tags.<tag-name>	String

Table 14: AWS - Security Groups

Field name	Field type
secgrpId	String
name	String

Field name	Field type
vpcId	String
region	String
isOpenGroup	Boolean
lastModifiedBy	String
isUnusedGroup	Boolean
isNestedGroup	Boolean
isOverlappedGroup	Boolean
_ingressRules.protocol	String
_ingressRules.toPort	Numeric
_ingressRules.fromPort	Numeric
_ingressRules.ipRange	String
_ingressRules.groupIdName	String
_egressRules.protocol	String
_egressRules.toPort	Numeric
_egressRules.fromPort	Numeric
_egressRules.ipRange	String
_egressRules.groupIdName	String
tags.<tag-name>	String

Table 15: AWS - S3 buckets

Field name	Field type
name	String
owner	String
region	String
creationDate	Date
isRestricted	Boolean
lastModifiedBy	String

Field name	Field type
policy	String
defaultEncryption	String
isPublic	Boolean
tags.<tag-name>	String

Table 16: AWS - RDS

Field name	Field type
name	String
region	String
identifierId	String
arn	String
availabilityZone	String
secondaryAvailabilityZone	String
instanceClass	String
status	String
engine	String
engineVersion	String
multiAZ	Boolean
storageType	String
vpcId	String
networkInterface	String
creationDate	Date
isPubliclyAccessible	Boolean
isStorageEncrypted	Boolean
tags.<tag-name>	String

Table 17: AWS - IAM Users

Field name	Field type
name	String
userId	String
createDate	Date
isMfaActive	Boolean
isOverPrivileged	Boolean
accessKeyAge	Date
groupList	String
isActive	Boolean
passwordLastChanged	Date
passwordLastUsed	Date
lastActivity	Date

Table 18: AWS - IAM Groups

Field name	Field type
roleName	String
createDate	Boolean
isOverPrivileged	Boolean

Table 19: AWS - IAM Roles

Field name	Field type
name	String
isOverPrivileged	Boolean

Table 20: AWS - IAM External Access

Field name	Field type
region	String
accessLevels	String
findingId	String

Table 21: AWS - AWS Lambda

Field name	Field type
region	String
accessLevels	String
findingId	String
resource	String
resourceType	String
status	String
updatedAt	Date

Azure field names

Table 22: Azure - Hosts

Field name	Field type
name	String
resourceGroup	String
vmId	String
image	String
runningState	String
instanceType	String
region	String
startTime	Date
subnetId	String
vnetId	String
osType	String
isPublic	Boolean
classicPublicIpAddress	String
hasContainerNodes	Boolean

Field name	Field type
provisioningState	String
privateIP	String
primarySecurityGroup	String
vmScaleSetId	String
vmScaleSet	String
tags.<tag-name>	String
outGoingIp	String
outGoingPort	String

Table 23: Azure - Clusters

Field name	Field type
name	String
resourceGroup	String
instanceId	String
region	String
nodeResourceGroup	String
rbacEnabled	Boolean
httpEnabled	Boolean
version	String
tags.<tag-name>	String

Table 24: Azure - Node Groups

Field name	Field type
instanceId	String
name	String
region	String
createdTime	Date
desiredCapacity	Numeric

Field name	Field type
createdAt	Date
placementGroup	String
serviceLinkedRoleARN	String
status	String
subnets	String
launchConfiguration	String
tags.<tag-name>	String

Table 25: Azure - Nodes

Field name	Field type
instanceId	String
name	String
namespace	String
publicIp	String
vmId	String
podCIDR	String
startTime	Date
tags.<tag-name>	String

Table 26: Azure - Pods

Field name	Field type
instanceId	String
name	String
namespace	String
nodeName	String
status	String
startTime	Date
hostIP	String

Field name	Field type
isPublic	Boolean
isPrivileged	Boolean
tags.<tag-name>	String

Table 27: Azure - Containers

Field name	Field type
instanceId	String
name	String
image	String
imagePullPolicy	String
status	String
startedTime	Date
privileged	Boolean
kubeHost.nodeName	String
kubeHost.namespace	String
tags.<tag-name>	String

Table 28: Azure - Services

Field name	Field type
instanceId	String
name	String
image	String
imagePullPolicy	String
status	String
startTime	Date
privileged	Boolean
kubeHost.nodeName	String
kubeHost.namespace	String

Field name	Field type
tags.<tag-name>	String

Table 29: Azure - Ingress

Field name	Field type
instanceId	String
name	String
namespace	String
startTime	Date
tags.<tag-name>	String

Table 30: Azure - Network Policy

Field name	Field type
instanceId	String
name	String
namespace	String
startTime	Date
tags.<tag-name>	String

Table 31: Azure - RBAC Roles

Field name	Field type
instanceId	String
roleType	String
name	String
namespace	String
creationTime	Date
tags.<tag-name>	String

Table 32: Azure - Network Security Groups

Field name	Field type
name	String
instanceId	String
region	String
resourceGroup	String
isOpenGroup	Boolean
isUnusedGroup	Boolean
isOverlappedGroup	Boolean
tags.<tag-name>	String

Table 33: Azure - Virtual Networks

Field name	Field type
name	String
instanceId	String
region	String
resourceGroup	String
addressSpaces	String
dnsServerIPs	String
isDdosProtectionEnabled	Boolean
isVmProtectionEnabled	Boolean
tags.<tag-name>	String

Table 34: Azure - Resource Group

Field name	Field type
name	String
instanceId	String
region	String
tags.<tag-name>	String

Table 35: Azure - IoT Hub

Field name	Field type
iotHubName	String
instanceId	String
region	String
minTlsVersion	String
enableFileUploadNotifications	Boolean
tags.<tag-name>	String

Table 36: Azure - Storage Account

Field name	Field type
name	String
instanceId	String
region	String
resourceGroup	String
creationTime	Date
skuType	String
isPublic	Boolean
kind	String
tags.<tag-name>	String

Table 37: Azure - SQL Servers

Field name	Field type
name	String
instanceId	String
region	String
resourceGroup	String
administratorLogin	String
isAdLoginEnabled	Boolean

Field name	Field type
isPublic	Boolean
kind	String
isManagedServiceIdentityEnabled	Boolean
tags.<tag-name>	String

Table 38: Azure - DBs

Field name	Field type
name	String
instanceId	String
region	String
resourceGroup	String
type	String
administratorLogin	String
storageMB	Numeric
geoRedundantBackup	String
sslEnforcement	String
isPublic	Boolean
tags.<tag-name>	String

Table 39: Azure - Cosmos DBs

Field name	Field type
name	String
instanceId	String
region	String
resourceGroup	String
accountOfferType	String
documentEndpoint	String
kind	String

Field name	Field type
isMultipleWriteLocationsEnabled	Boolean
isVnetEnabled	Boolean
isPublic	Boolean
isAutomaticFailoverEnabled	Boolean
tags.<tag-name>	String

Table 40: Azure - Users

Field name	Field type
name	String
instanceId	String
mail	String
mainNickname	String
signInName	String
isActive	Boolean
userType	String
source	String

Table 41: Azure - Groups

Field name	Field type
name	String
instanceId	String
mail	String

Table 42: Azure - Function Apps

Field name	Field type
name	String
instanceId	String
region	String

Field name	Field type
resourceGroup	String
alwaysOn	Boolean
appServicePlanId	String
clientCertEnabled	String
containerSize	Numeric
defaultHostName	String
enabled	Boolean
state	String
repositorySiteName	String
httpsOnly	Boolean
lastModifiedTime	Date
os	String
tags.<tag-name>	String

Table 43: Azure - Logic Apps

Field name	Field type
name	String
instanceId	String
region	String
resourceGroup	String
alwaysOn	Boolean
appServicePlanId	String
clientCertEnabled	String
containerSize	Numeric
defaultHostName	String
enabled	Boolean
state	String

Field name	Field type
repositorySiteName	String
httpsOnly	Boolean
lastModifiedTime	Date
os	String
tags.<tag-name>	String

GCP field names

Table 44: GCP - Host

Field name	Field type
name	String
vmId	String
startTime	Date
description	String
type	String
status	String
zone	String
privateIP	String
publicIP	String
canIpForward	Boolean
cpuPlatform	String
kind	String
isPublic	String
hasContainerNodes	Date
tags.<tag-name>	String
outGoingIp	String
outGoingPort	String

Table 45: GCP - Clusters

Field name	Field type
name	String
description	String
loggingService	String
monitoringService	String
network	String
clusterIpv4Cidr	String
subnetwork	String
location	String
zone	String
endpoint	String
currentMasterVersion	String
createTime	Date
status	String
statusMessage	String
servicesIpv4Cidr	String
isMasterAuthorizedNetworksEnabled	Boolean
isLegacyABACEnabled	Boolean
isbasicAuthEnabled	Boolean

Table 46: GCP - Node Groups

Field name	Field type
name	String
cluster	String
status	String
isAutoRepairEnabled	Boolean
isAutoUpgradeEnabled	Boolean

Field name	Field type
machineType	String
imageType	String
serviceAccount	String

Table 47: GCP - Nodes

Field name	Field type
instanceId	String
name	String
namespace	String
publicIp	String
vmId	String
podCIDR	String
startTime	Date
tags.<tag-name>	String

Table 48: GCP - Pods

Field name	Field type
instanceId	String
name	String
namespace	String
nodeName	String
status	String
startTime	Date
hostIP	String
isPublic	Boolean
isPrivileged	Boolean
tags.<tag-name>	String

Table 49: GCP - Containers

Field name	Field type
instanceId	String
name	String
image	String
imagePullPolicy	String
status	String
startedTime	Date
privileged	Boolean
kubeHost.nodeName	String
kubeHost.namespace	String
tags.<tag-name>	String

Table 50: GCP - Services

Field name	Field type
instanceId	String
name	String
image	String
imagePullPolicy	String
status	String
startTime	Date
privileged	Boolean
kubeHost.nodeName	String
kubeHost.namespace	String
tags.<tag-name>	String

Table 51: GCP - Ingress

Field name	Field type
instanceId	String

Field name	Field type
name	String
namespace	String
startTime	Date
tags.<tag-name>	String

Table 52: GCP - Network Policy

Field name	Field type
instanceId	String
name	String
namespace	String
startTime	Date
tags.<tag-name>	String

Table 53: GCP - RBAC Roles

Field name	Field type
instanceId	String
roleType	String
name	String
namespace	String
creationTime	Date
tags.<tag-name>	String

Table 54: GCP - Firewall

Field name	Field type
instanceId	String
network	String
name	String
priority	Numeric

Field name	Field type
isDisabled	Boolean
isOpen	Boolean
isUnused	Boolean
direction	String

Table 55: GCP - VPCs

Field name	Field type
instanceId	String
startTime	Date
name	String
IPv4Range	String
routingMode	String
autoCreateSubnetworks	Boolean

Table 56: GCP - Buckets

Field name	Field type
instanceId	String
startTime	Date
name	String
encryption	String
owner	String
location	String
versioning	String
isPublic	Boolean
storageClass	String
tags.<tag-name>	String

Table 57: GCP - SQLs

Field name	Field type
instanceId	String
startTime	Date
name	String
state	String
backendType	String
databaseVersion	String
region	String
primaryIP	String
masterInstanceName	String
serviceAccount	String
diskType	String
SSLEnabled	Boolean
isPublic	Boolean
privateNetwork	String
tags.<tag-name>	String

Table 58: GCP - Users

Field name	Field type
instanceId	String
name	String
primaryEmail	String
isAdmin	Boolean
isDelegatedAdmin	Boolean
lastLoginTime	Date
creationTime	Date
isEnrolledIn2Sv	Boolean

Table 59: GCP - Groups

Field name	Field type
instanceId	String
name	String
email	String

Table 60: GCP - Role Bindings

Field name	Field type
role	String

Native K8s field names

Table 61: Native K8s - Nodes

Field name	Field type
instanceId	String
name	String
namespace	String
publicIp	String
vmId	String
podCIDR	String
startTime	Date
tags.<tag-name>	String

Table 62: Native K8s - Pods

Field name	Field type
instanceId	String
name	String
namespace	String
nodeName	String
status	String

Field name	Field type
startTime	Date
hostIP	String
isPublic	Boolean
isPrivileged	Boolean
tags.<tag-name>	String

Table 63: Native K8s - Containers

Field name	Field type
instanceId	String
name	String
image	String
imagePullPolicy	String
status	String
startedTime	Date
privileged	Boolean
kubeHost.nodeName	String
kubeHost.namespace	String
tags.<tag-name>	String

Table 64: Native K8s - Services

Field name	Field type
instanceId	String
name	String
image	String
imagePullPolicy	String
status	String
startTime	Date
privileged	Boolean

Field name	Field type
kubeHost.nodeName	String
kubeHost.namespace	String
tags.<tag-name>	String

Table 65: Native K8s - Ingress

Field name	Field type
instanceId	String
name	String
namespace	String
startTime	Date
tags.<tag-name>	String

Table 66: Native K8s - Network Policy

Field name	Field type
instanceId	String
name	String
namespace	String
startTime	Date
tags.<tag-name>	String

Table 67: Native K8s - RBAC Roles

Field name	Field type
instanceId	String
roleType	String
name	String
namespace	String
creationTime	Date
tags.<tag-name>	String

Related concepts

Search capabilities (page 68)
Learn how to use search terms on your inventory data.

Related reference

Search examples (page 99)
See how to combine different terms to create complex searches.

14.2 Search examples

See how to combine different terms to create complex searches.

The table lists examples of searches combining different terms and techniques.

For more details on how to use the various search elements, see Search capabilities.

Table 68: Examples

Search objective	Query
Find alerts seen in the last 2 days that are related to GDPR policy checks.	Alert AND lastSeen:[now-2d TO *] AND policies.policyTagName:GDPR
Find hosts that were started in the last 3 days, are not part of an auto scaling group, and have a public interface.	Host AND startTime:[now-3d TO *] AND isPublic:true AND NOT "Auto Scaling"
Find public, unencrypted S3 buckets created in the last year.	creationDate:[now/y TO *] AND isPublic:true AND not _exists_:defaultEncryption
Find S3 buckets created in the last 6 months, by aws-pcg in the us-west-2 region.	creationDate:[now-6M TO *] AND isPublic:true AND owner:aws-pcg* AND region:us-west-2
Find over-privileged IAM users created over a month ago that have been inactive.	User AND isOverPrivileged:true AND createDate:[* TO now-1M] AND not _exists_:lastActivity
Find security groups that allow inbound traffic from any port and from any IP address.	_ingressRules.toPort:"-1" and _ingressRules.fromPort:"-1" and _ingressRules.ipRange:"0.0.0.0/0"
Find hosts with outbound traffic from specific IP addresses and ports.	outGoingIp:("IP1" "IP2" "IP3") and outGoingPort:("PORT1" "PORT2" "PORT3")

Related concepts

Search capabilities (page 68)
Learn how to use search terms on your inventory data.

Related reference

Supported search field names (page 70)
Tables of valid search field names and types.

15 Administration roles

You can use pre-defined administration roles to divide up security tasks according to each administrator's responsibility level.

You can't edit or delete these roles.

Super Admin

Super Admin administrators have access to everything in Sophos Cloud Optix.

They can manage administrators, roles, and role assignments in Sophos Central, and can control other administrators' access to information in Sophos Cloud Optix using environment tags.

They can also configure third-party integrations, for example Jira, Slack, and ServiceNow, and the Sophos Cloud Optix API.

There must be at least one administrator with the Super Admin role.

Admin

Admin administrators have access to all environments in Sophos Cloud Optix. A Super Admin administrator can restrict access to specific environments.

Admin administrators can't manage administrators and role assignments or configure third-party integrations or the Sophos Cloud Optix API.

Read-only

Read-only administrators have read-only access to all environments in Sophos Cloud Optix. Super Admin administrators can restrict access to specific environments.

They can't do the following:

- Manage administrators and role assignments.
- Add, edit or delete cloud environments.
- Configure third-party integrations.
- Configure the Sophos Cloud Optix API.

They also can't see some options, for example **Edit** buttons.

Custom

Sophos Central Super Admin administrators can add Custom roles. Custom roles are not available for the standalone Sophos Cloud Optix console.

Custom roles are based on the pre-defined Admin and Read-only administrator roles but also enable you to restrict access to specific products in Sophos Central, including Sophos Cloud Optix.

Custom administrators do not have access to any environments in Sophos Cloud Optix until a Super Admin provides them with access. They can't do the following:

- Manage administrators and role assignments.
- Configure third-party integrations.
- Configure the Sophos Cloud Optix API.

Related information

Environment access control (page 101)
You can control which cloud environments each administrator can see in their Sophos Cloud Optix console.

15.1 Environment access control

You can control which cloud environments each administrator can see in their Sophos Cloud Optix console.

Introduction

You can group cloud environments together and control who can access them. To do this you create an environment tag for each group and assign the tag to administrators. For example you can create separate tags for AWS accounts, Azure subscriptions or GCP projects.

Only administrators with the Super Admin role can create and edit environment tags and assign them to other administrators.

Administrators with tags assigned to them can only see information about those environments in their Sophos Cloud Optix console. The same level of access, full or read-only, applies to all environments to which the administrator is granted access. The level of access is defined by the administrator's role.

Related concepts

Administration roles (page 100)
You can use pre-defined administration roles to divide up security tasks according to each administrator's responsibility level.

Understanding environment access control

You need to know what environment tags allow administrators with different roles to do..

Administrator capabilities

Super Admin administrators always see all environments in Sophos Cloud Optix and cannot have environment tags assigned to them.

Administrators with environment tags assigned to them do not automatically see new environments that are added to Sophos Cloud Optix, including environments they add themselves. A Super Admin needs to add new environments to tags and assign the tags to the appropriate administrators to provide access.

Administrators with environment tags assigned to them do not see Audit Logs in Sophos Cloud Optix. Audit Logs provide information about activity relating to all environments in Sophos Cloud Optix and are not available to administrators with restricted access.

Only Super Admin administrators can configure third-party integrations (for example Jira, Slack, ServiceNow) and the Sophos Cloud Optix API. Information available through the integrations and the Sophos Cloud Optix API is not limited to specific environments for specific administrators.

New administrators

When you add Admin or Read-only administrators they can see all environments in Sophos Cloud Optix. A Super Admin can then restrict the new administrator's access to specific environments by assigning environment tags to them.

When you add a new administrator with a Custom role in Sophos Central they can't see any environments in Sophos Cloud Optix. A Super Admin must then allow access to specific environments by assigning environment tags to them.

Tip
Use a Custom role in Sophos Central to prevent new administrators from being able to see information about all Sophos Cloud Optix environments.

Create environment tags

Super Admin administrators can create environment tags as follows:

1. Under **Settings** click **Users**.
2. On the **Environment Tags** tab click **Add Environment Tag**.
3. Enter a **Tag Name**.
4. Select cloud environments for the tag.
5. Select the administrators you want to assign the tag to and click **OK**.
   The new tag is now listed on the environment tags tab.

You can also add tags to environments. To do this, click **Settings > Environments**. You can also assign tags to administrators later.

Assign environment tags to administrators

Super Admin administrators can assign existing environment tags to other Sophos Cloud Optix administrators as follows:

1. Under **Settings** click **Users**.
   A list of current Sophos Cloud Optix administrators is displayed.
2. Click the tag icon
   
   under **Actions** for an administrator.
3. Choose the environment tags to assign to them and click **Apply**.

   Administrators can now only see information in Sophos Cloud Optix for the environments associated with the tags assigned to them.

16 Sophos Cloud Optix licensing

Subscriptions are based on the number of cloud assets in the cloud environments that you add to Sophos Cloud Optix.

Sophos Cloud Optix is a subscription-based SaaS service, and is available as follows:

- Term license: purchased up front for a 12, 24 or 36 month term.
- MSP Flex: for Managed Service Providers, billed monthly in-arrears based on usage.
- Pay-as-you-go (PAYG) via AWS Marketplace: billed monthly in arrears based on usage, via your AWS bill.
- If you have an Intercept X Advanced for Server with EDR term license, you can use Sophos Cloud Optix for EDR. To find out the differences between this and Sophos Cloud Optix see Sophos Cloud Optix for EDR.

You can add as many cloud environments (for example AWS Accounts, Azure Subscriptions, GCP Projects) as you need to a single Sophos Cloud Optix account.

Subscriptions may also include a maximum daily log data volume, where log data includes ingestion of network flow logs and activity logs. Add-on subscriptions are available for additional log data volumes.

Cloud asset means a single virtual machine instance, including any server instance or database instance, that runs in a cloud environment that benefits from, or whose configuration is accessed by Sophos Cloud Optix.

The following are currently considered as cloud assets:

- AWS EC2
- AWS RDS
- Azure VM
- Azure SQL Server
- Azure DB Server
- Azure Cosmos DB
- Google VM
- Google SQL
- Kubernetes Nodes (to avoid duplication, these are not counted if they are already counted under AWS EC2 VM, Azure VM or GCP VM)

Usage reporting in Sophos Cloud Optix

A cloud asset is counted and reported in your console if it has been seen during the last 30 days.

When Sophos Cloud Optix connects to your cloud environment (for example an AWS account) the service records the number of cloud assets for that specific environment at that point in time. Sophos Cloud Optix records the highest number of cloud assets seen on any given day in the last 30 days, for each cloud environment. If there are multiple cloud environments on your account, these are added together and reported in your console as the usage.

Usage calculation for MSP Flex billing

MSP Flex billing is based on aggregate usage of Sophos Cloud Optix across multiple customers, billed monthly in arrears.

A cloud asset is counted and reported for billing if it's seen during 30 days prior to billing.

When Sophos Cloud Optix connects to a customer's cloud environment (for example an AWS account) the service records the number of cloud assets for that specific environment at that point in time. Sophos Cloud Optix records the highest number of cloud assets seen on any given day in the last 30 days, for each cloud environment. If there are multiple cloud environments on the customer's account, these are added together and reported as the usage for that customer. If the MSP has multiple Sophos Cloud Optix customers, the usage for each customer is aggregated for monthly billing.

The following table shows how usage recording works over a 30 day period. In this example the customer has three cloud environments (for example AWS accounts) in Sophos Cloud Optix.

Table 69: MSP Flex billing example

Instance	Cloud assets used during 30 day period	Number of cloud assets recorded
Environment #1	25 on one day	50
	50 on another day	
Environment #2	10 on one day	20
	20 on another day	
Environment #3	25 on one day	25
	Zero usage on another day	

In this example the total monthly usage for this customer is 95 cloud assets.

Usage calculation for PAYG via AWS Marketplace

Sophos Cloud Optix is available via AWS SaaS subscription on a pay-as-you-go (PAYG) basis. Billing is based on actual usage, calculated on an hourly basis, billed monthly in arrears. See the Sophos Cloud Optix (PAYG) page on AWS Marketplace.

Once you've signed up for Sophos Cloud Optix via AWS Marketplace and added your cloud environments to the service, Sophos Cloud Optix continuously monitors the number of cloud assets on your account and sends this information to AWS on an hourly basis. AWS calculates the total usage over the month and includes this in your monthly AWS bill.

You can cancel Sophos Cloud Optix PAYG SaaS subscriptions on AWS Marketplace at any time.

Sophos Cloud Optix for EDR

Sophos Cloud Optix for EDR is only available with term licenses for Intercept X Advanced for Server with EDR. It's not included with MSP Flex licenses for Intercept X Advanced for Server with EDR.

If you have a term license for Intercept X Advanced for Server with EDR, the number of cloud assets you can have in Sophos Cloud Optix for EDR depends on the number of servers you have in your Intercept X Advanced for Server with EDR license. You can have up to 120% of the number of servers.

For example, if you have 150 servers, you can have 180 cloud assets. This covers cloud assets that are counted for licensing by Sophos Cloud Optix that are not counted as servers, such as database instances. Your Sophos Cloud Optix for EDR entitlement and usage is displayed on the Sophos Cloud Optix dashboard.

Related concepts

Sophos Cloud Optix for EDR (page 106)
Find out which Sophos Cloud Optix features are included with Intercept X Advanced for Server with EDR.

Related reference

Sophos Cloud Optix (PAYG) on AWS Marketplace

17 Sophos Cloud Optix for EDR

Find out which Sophos Cloud Optix features are included with Intercept X Advanced for Server with EDR.

An Intercept X Advanced for Server with EDR term license includes Sophos Cloud Optix for EDR. For more information about licensing, see Sophos Cloud Optix licensing.

This includes a set of powerful cloud security features, powered by Sophos Cloud Optix. It's a subset of Sophos Cloud Optix and you can't buy it separately.

You can upgrade to the full Sophos Cloud Optix service for additional cloud security features. It's available on subscription or on a free trial.

The table compares the features in the two versions of the product.

Table 70: Sophos Cloud Optix for EDR compared to full Cloud Optix product

Feature	Cloud Optix for EDR	Cloud Optix
Support for AWS, Azure, GCP and Kubernetes environments	Y	Y
Security Monitoring (CSPM best practice rules. Automated and on-demand scans.)	Daily and on-demand scans	Configurable scan frequency
Asset Inventory	Y	Y
Advanced search capabilities	Y	Y
AI-powered Anomaly Detection	Y	Y
Guardrails	Y	Y
Email Alerts	Y	Y
AWS Service Integrations (SSM, GuardDuty, Inspector, IAM Access Analyzer)	Y	Y
Compliance Policies and Reports	CIS	Y
Custom Policies	-	Y
Network Visualization	-	Y
IAM Visualization	-	Y
Spend Monitor	-	Y

Feature	Cloud Optix for EDR	Cloud Optix
Alert Management Integrations	-	Y
Rest API	-	Y
IaC Template Scanning (DevSecOps)	-	Y
Environment Access Control	-	Y

Accessing Sophos Cloud Optix for EDR.

If you have an Intercept X Advanced for Server with EDR term license, **Cloud Optix** appears in Sophos Central Admin, under **My Products**.

To use Sophos Cloud Optix for EDR click **Cloud Optix**.

Use of Sophos Cloud Optix for EDR is governed by the Sophos Services Agreement. You must accept this agreement in Sophos Central to use it.

Related concepts

Sophos Cloud Optix licensing (page 103)
Subscriptions are based on the number of cloud assets in the cloud environments that you add to Sophos Cloud Optix.

18 Cloud provider charges

Your cloud provider will charge you for Cloud Optix activity that collects or sends log data. The charge depends on usage and amount of data.

We recommend that you do as follows:

- Monitor the charges in your cloud provider dashboard.
- If you have a Cloud Optix trial, consider using a cloud environment that generates less log data.

This is how Cloud Optix uses data and why you might incur charges:

1. Cloud Optix creates an access IAM role (AWS), access key (Azure), or service account (GCP).

   This enables Cloud Optix to use the cloud provider's APIs to perform continuous assessment and to provide an inventory of resources.

   Cloud providers don't usually charge for this.

2. Cloud Optix enables logs (if not enabled already) and sets up continuous streaming of log data to Cloud Optix.

   This collects admin activity logs (for example AWS CloudTrail) and Network Flow Logs, to provide the network traffic view, anomaly detection alerts, and more.

   Cloud providers do charge for this.

Note
If you're concerned about provider charges, you can choose not to enable logs, but you'll lose some Cloud Optix functionality. Use the **Custom settings** on the **Add an environment** page.

Tip
In AWS, the first CloudTrail is free, but subsequent CloudTrails incur additional cost. You can customize the Cloud Optix setup to reuse an existing CloudTrail.

Here are more details of charges for each stage in log streaming.

Network Flow Logs

All Cloud providers charge for Network Flow Logs. Please see the following references for guidance on flow log pricing from each cloud provider.

AWS: https://aws.amazon.com/cloudtrail/pricing/

https://aws.amazon.com/about-aws/whats-new/2018/01/cloudwatch-introduces-tiered-pricing-with-up-to-90-percent-discount-for-vpc-flow-logs-and-other-vended-logs/

Azure: https://azure.microsoft.com/en-us/pricing/details/network-watcher/

GCP: https://cloud.google.com/stackdriver/

Log routing

AWS: https://aws.amazon.com/cloudwatch/pricing/

Azure: https://azure.microsoft.com/en-us/pricing/details/storage/

GCP: https://cloud.google.com/storage/pricing

Serverless functions

A serverless function (created in your environment by Cloud Optix) is triggered when new logs reach CloudWatch, Azure storage or GCP sink. This takes the logs and sends them via https to the Cloud Optix service.

Cloud providers charge for serverless functions on the basis of usage.

AWS: https://aws.amazon.com/lambda/pricing/

Azure: https://azure.microsoft.com/en-us/pricing/details/functions/

GCP: https://cloud.google.com/functions/pricing

Data transfer to Cloud Optix

The Cloud Optix service is hosted in the AWS US-West region. Cloud providers may charge for data transfer to the service in this region.

AWS: https://aws.amazon.com/lambda/pricing/

Azure: https://azure.microsoft.com/en-us/pricing/details/bandwidth/

GCP: https://cloud.google.com/pricing/list

19 Multi-factor authentication

You can turn on multi-factor authentication to improve the security of your Sophos Cloud Optix account.

This means you must use another form of authentication, as well as username and password, when you sign in to Sophos Cloud Optix.

Note
If you are accessing Sophos Cloud Optix from Sophos Central, you should configure MFA from the Sophos Central Admin console, not through Sophos Cloud Optix.

Note
If you've signed in with Google authentication, you can't turn on multi-factor authentication in Sophos Cloud Optix. Turn it on in your Google account instead. Google authentication is not available if you are accessing Cloud Optix from Sophos Central.

Turn on multi-factor authentication

1. Click your customer name (in the upper right of the page).
2. Select **Profile**.
3. Click the **Multi-factor Authentication** tab. You'll see a QR code.
4. On your mobile phone, open an authenticator (we recommend Google Authenticator).
5. Scan the QR code.

   A code is shown on your mobile phone.
6. Enter the code in **Authentication Code** and click **Submit**.

The next time you sign in, you'll be prompted for a one-time passcode. You can find it in Google Authenticator.

Sign in with multi-factor authentication

Enter your email address and password.

1. Enter your email address and password.
2. Click **Sign in**.

   You're prompted to enter "MFA OTP" (Multi-factor authentication one-time passcode).
3. On your mobile phone, go to Google Authenticator and look for the Sophos Cloud Optix passcode.
4. Enter the code in the sign-in screen and click **Sign in** again.

Turn off multi-factor authentication

If you are an Admin user, you can turn off multi-factor authentication for your own sign-in or for other users on your account (for example if a user loses their mobile phone).

Read-only users can't turn off multi-factor authentication in the Sophos Cloud Optix user interface.

1. Go to **Settings > Users**.
2. Find the user.
3. In the **Action** column, click the padlock icon to turn off multi-factor authentication.

20 How Sophos stores and manages your data

Find out how Sophos looks after your data, and about our GDPR compliance

To use Sophos Cloud Optix, you need to connect to one or more cloud environments, for example an Amazon Web Services (AWS) account, a Microsoft Azure subscription, or a Google Cloud Platform project. When you connect a cloud environment, you explicitly authorize Sophos to access information via APIs and collect log data.

Data movement between Sophos Cloud Optix and cloud environments

Data is transferred from the customer's cloud environment to Sophos Cloud Optix in the following ways:

1. Infrastructure metadata is pulled from the environment using the cloud platform's APIs, for example AWS SDK.
2. Network flow logs and usage logs are pushed to Sophos Cloud Optix log collectors by a serverless function in the customer's cloud environment, for example AWS Lambda.

In both cases, the data transfer uses TLS encryption.

How data is stored, protected, and managed

Infrastructure metadata includes inventory information about your cloud resources, such as instances/VMs, storage buckets and security groups, and their associated security states.

Activity logs, such as AWS CloudTrail logs, may include information about an IAM entity that accessed or made changes to the infrastructure. VPC/Network flow logs include information about which IP address is communicating with another IP address, and the port and protocol used, for example 1.1.1.1 to 2.2.2.2 on port 80 via TPC.

All infrastructure metadata and log information collected by the service is stored using industry-standard AES 256 encryption.

You can remove a cloud environment from your Sophos Cloud Optix account at any time. All associated infrastructure metadata and log information is deleted automatically.

Sophos Cloud Optix also offers optional third-party integrations, for example Slack, Jira, ServiceNow, PagerDuty, and Splunk. Credentials you provide to use these integrations are stored using AES 256 encryption.

Sophos Cloud Optix and GDPR

To the extent that the General Data Protection Regulation (GDPR) or, portion of it, applies to a customer's use of the Sophos Cloud Optix service, Sophos represents that it complies with GDPR in the Sophos Services Agreement, which governs the use of Sophos Cloud Optix.

Section 10.2 of the Sophos Services Agreement states: "Each party agrees to comply with all laws applicable to the actions and obligations contemplated by this Agreement", which includes GDPR.

Related reference

Sophos Services Agreement

Sophos commitment to GDPR and data protection

21 Supported web browsers

Check that Sophos Cloud Optix can run on your web browser.

We currently support the following browsers:

- Google Chrome
- Mozilla Firefox
- Microsoft Internet Explorer 11
- Microsoft Edge
- Apple Safari (Mac only)

We recommend that you always run an up-to-date version.

22 Get additional help

To get help from Sophos Support:

1. Click **Help** in the top right of the user interface and select **Create Support Ticket**.
2. Fill in the form. Be as precise as possible so that Support can help you effectively.
3. Optionally, select **Enable Remote Assistance**. This enables Support to directly access your Sophos Central session to be better able to help you.
4. Click **Send**.

Sophos will contact you within 24 hours.

Note
If you selected Remote Assistance, this function is enabled when you click **Send**. Remote Assistance will automatically be disabled after 72 hours. To disable it sooner, click on your account name (upper right of the user interface), select **Licensing & Administration**, and click the **Sophos Support** tab.

Submit feedback

To submit feedback or a suggestion to Sophos Support:

1. Click **Help** in the top right of the user interface and select **Give Feedback**.
2. Fill in the form.
3. Click **Send**.

Additional help

You can also find technical support as follows:

- Visit the Sophos Community at community.sophos.com/ and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at www.sophos.com/en-us/support.aspx.

23 Legal notices