SOPHOS
Cybersecurity made simple.
Sophos Cloud Optix help
## Contents

**About Sophos Cloud Optix**........................................................................................................... 1
**Getting started**............................................................................................................................... 2
**Add your AWS environment**........................................................................................................ 3
  - Add AWS environments using CLI scripts.................................................................................. 4
  - Add AWS environments using AWS CloudFormation................................................................. 5
  - Add your Amazon EKS clusters.................................................................................................. 10
  - Troubleshooting for AWS........................................................................................................... 11
  - Add remediation (Guardrails)..................................................................................................... 11
  - Permissions needed to run Sophos Cloud Optix scripts for AWS............................................. 12
  - What does the Sophos Cloud Optix script to add AWS environments do?............................. 15
  - AWS CLI script variables.......................................................................................................... 17
  - Set up AWS CLI to run scripts.................................................................................................. 18
  - Remove your AWS environment............................................................................................... 19
**Add your Microsoft Azure environment**.................................................................................... 21
  - Remove your Azure environment............................................................................................. 22
  - Troubleshooting for Azure....................................................................................................... 22
  - What does the Sophos Cloud Optix script to add Azure environments do?............................. 23
**Add your Google Cloud Platform environment**.......................................................................... 26
  - Add a GKE cluster to an existing GCP environment................................................................. 27
  - What does the Sophos Cloud Optix script for GCP do?............................................................ 27
**Add your Kubernetes environment**............................................................................................ 29
**Add your IaC environments**......................................................................................................... 30
  - Add code repositories using GitHub....................................................................................... 30
  - Add code repositories using Bitbucket..................................................................................... 31
  - Add code repositories via Jenkins pipeline............................................................................... 33
  - Monitor your IaC environment.................................................................................................. 33
**Remediation**............................................................................................................................... 38
  - Create the remediation role....................................................................................................... 38
  - Turn on automatic remediation............................................................................................... 39
  - Use manual remediation........................................................................................................... 39
  - Which issues can you remediate?............................................................................................. 39
**Anomaly detection**....................................................................................................................... 41
  - About anomaly alerts.............................................................................................................. 41
  - User login anomalies............................................................................................................... 42
  - Outbound network traffic anomalies....................................................................................... 42
  - Applications inferred from host behavior............................................................................... 43
  - High-risk activity...................................................................................................................... 43
**Topology: network visualization**................................................................................................ 44
  - View traffic flow....................................................................................................................... 45
  - View host details....................................................................................................................... 46
  - View inferred databases........................................................................................................... 46
  - IAM visualization..................................................................................................................... 46
**Spend Monitor**............................................................................................................................ 48
  - Setting up environments for **Spend Monitor**........................................................................ 48
  - Detailed set up instructions for AWS environments............................................................... 48
  - Turn on **Spend Monitor** in Sophos Cloud Optix................................................................... 49
  - Spend Monitor Thresholds....................................................................................................... 49
**Compliance policies**.................................................................................................................... 50
  - Use out-of-the-box policies...................................................................................................... 50
  - Customize policies.................................................................................................................. 50
  - View policy reports................................................................................................................ 51
  - Track policy compliance.......................................................................................................... 51

(2020/05/06)
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.

For more information, see the 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 reference
Sophos Cloud Optix product info
2 Getting started

You need a subscription to use Sophos Cloud Optix.

Get a subscription or sign up for a free trial. Then read this document to find out how to:

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

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

Related concepts

Add your AWS environment (page 3)
You can choose which method you use to add your AWS environment to Sophos Cloud Optix.

Sophos Cloud Optix Licensing (page 63)
Subscriptions are based on the number of cloud assets in the cloud environments that you add to Sophos Cloud Optix.

Related tasks

Add your Microsoft Azure environment (page 21)
You can add your Azure environment to Sophos Cloud Optix by running the PowerShell script Sophos provides.

Add your Google Cloud Platform environment (page 26)
You can add a Google Cloud Platform (GCP) project to Sophos Cloud Optix by running the script Sophos provides.

Add your IaC environments (page 30)
Sophos Cloud Optix can monitor code submitted to your Infrastructure as Code (IaC) repositories for potential security issues.
3 Add your AWS environment

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

Note
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.

Note
Sophos Cloud Optix does not support AWS's legacy EC2-Classic platform, which was deprecated in 2013. AWS environments on the EC2-VPC platform can be added.

Note
AWS regions that aren't connected to the global AWS infrastructure, including AWS GovCloud (US) and AWS China, are not supported.

You can add an AWS account to Sophos Cloud Optix in the following ways:

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

The user interface and instructions in this guide help you with the different methods.

Related concepts
Permissions needed to run Sophos Cloud Optix scripts for AWS (page 12)
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 11)
If there are problems with adding an AWS environment, run the uninstall script and try again.

What does the Sophos Cloud Optix script to add AWS environments do? (page 15)
The Sophos Cloud Optix script adds AWS environments and sets up communication between AWS and Cloud Optix.

Related tasks
Add your Amazon EKS clusters (page 10)
You can add Amazon EKS clusters to AWS accounts you have added to Sophos Cloud Optix.

Add AWS environments using CLI scripts (page 4)
You can add your AWS environment using a script.

Related information
Add AWS environments using AWS CloudFormation (page 5)
You can add AWS environments to Sophos Cloud Optix using AWS CloudFormation.

### 3.1 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 18).

**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](#) for AWS. 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.

```bash
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 will now show in the Sophos Cloud Optix dashboard.

For detailed information about the changes the script makes in your environment, see [What does the Sophos Cloud Optix script to add AWS environments do?](#)

**Related concepts**

- [Permissions needed to run Sophos Cloud Optix scripts for AWS](#) (page 12)
- [Troubleshooting for AWS](#) (page 11)

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

[What does the Sophos Cloud Optix script to add AWS environments do?](#) (page 15)
The Sophos Cloud Optix script adds AWS environments and sets up communication between AWS and Cloud Optix.

**Related reference**
- AWS CLI script variables (page 17)
- AWS script variables

**Related information**
- Set up AWS CLI to run scripts (page 18)

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

### 3.2 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.

To add multiple AWS accounts using AWS CloudFormation StackSets you must choose one AWS account as an admin account, then assign target accounts. These grant access to the admin account. You use details from your Sophos Cloud Optix console to configure your AWS CloudFormation StackSet.

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

You must do as follows:
- Collect information from your Sophos Cloud Optix console.
- Assign a role to the AWS account chosen as your admin account.
- Assign roles to each target AWS account.
- Create the CloudFormation StackSet in the Admin account.
- Configure and create CloudFormation StackSet.

**Related concepts**
- Add your AWS environment (page 3)

You can choose which method you use to add your AWS environment 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. Click **Settings > 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 admin account**

You must first choose an AWS account as an admin account.

Choose an AWS account to be an admin account. To assign the appropriate role to the admin account, do the following:

1. Sign into AWS 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:

![Launch Stack button](image)

**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/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 admin account.

7. Sign out of your admin account.

**Assign roles to each target AWS account**

You assign roles for the designated target accounts.

To create an AWS CloudFormation StackSet in every target account, follow these instructions.
Note
You must not be signed into your chosen admin account.

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

For each target AWS account, do the following:

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

   ![Launch Stack button](image)

   **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/AWSCloudFormationStackSetExecutionRole.yml`.

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

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

   **Parameters**
   Parameters are defined in your template and allow you to input custom values when you create or update a stack.

   **AdministratorAccountId**
   AWS Account Id of the administrator account (the account in which StackSets will be created).

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 the target account.
9. Sign into the next target account and repeat as required.
Create CloudFormation StackSet in the Admin account.

Using the Create StackSet assistant.

To create the AWS CloudFormation StackSet do the following:

1. Sign into AWS with your admin 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/cfn-onboarding.yaml
8. Click **Next**.

Configure and 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 populate the fields in the AWS CloudFormation StackSet assistant. This will link your StackSets to Sophos Cloud Optix.

**Warning**
Do not delete or amend any fields that are pre-populated by Sophos Cloud Optix. The onboarding will fail.

Ensure you are signed into your chosen AWS admin account and do the following:

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:
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 will fail.

6. Do not change any other fields.

7. Click **Next**.

8. You don't need to do anything on the **Configure StackSet options** page.

9. Click **Next**.

10. On the **Set deployment options** page, select **Deploy stacks in accounts**.

11. In the **Account numbers** field, enter the account numbers of the target accounts you want to add to Sophos Cloud Optix (the accounts in which you created the `AWSCloudFormationStackSetExecutionRole`).
12. In **Specify regions**, choose one region. The CloudFormation stack instance will be created in this region for the target account.

13. Click **Next**.

14. This takes you to a **Review** page which shows you all the options you have entered. Check this carefully.

15. Turn on **I acknowledge that AWS CloudFormation might create IAM resources with custom names**.

16. Close the assistant. This creates the stack instance and adds the target accounts to Sophos Cloud Optix.

### 3.3 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.

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.
3.4 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.

3.5 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 39)
How to turn on automatic remediation.

**Use manual remediation** (page 39)
How to use manual remediation.

3.6 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.

```json
{
    "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.

```json
{
  "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": "*
    }
  ]
}
```

3.7 What does the Sophos Cloud Optix script to add AWS environments do?

The Sophos Cloud Optix script adds AWS environments and sets up communication between AWS and Cloud Optix.

The script sets up two communication channels with the environment:

- Pull channel to gather infrastructure information about instances, security groups, etc. The script periodically opens this channel via the provider APIs.
- Push channel for sending near-real-time information about your activity logs (for example, VPC Flow Logs and CloudTrail logs).

**Pull channel**

To enable the pull, the script creates a read-only role: Avid-Role.

If the role already exists in the environment, the script checks for appropriate policy permissions and continues running. Otherwise it creates a new role with the policy permission arn:aws:iam::aws:policy/SecurityAudit and the following permissions:

- `elasticfilesystem:DescribeMountTargetSecurityGroups`
- `elasticfilesystem:DescribeMountTargets`
Push channel

For push, the script then creates and configures:

- A trail (CloudTrail) **CT-AvidSecure** to deliver AWS CloudTrail log events from all regions to an S3 bucket **avid-cloudtrail-<ACCOUNT>**. If the bucket does not already exist in your account, it will create it. 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, which allows the CloudTrail to send events to CloudWatch and has the permissions for **s3:GetBucketAcl, s3:PutObject** and allowed to perform following actions **logs:CreateLogStream, logs:PutLogEvents** on resources associated with log group **CT-Avid-LogGroup**.

- A role **Avid-Lambda-to-CloudWatch** which allows an AWS Lambda function to read CloudWatch events using policy permissions **arn:aws:iam::aws:policy/CloudWatchEventsReadOnlyAccess** and is allowed to perform the following actions **logs:CreateLogGroup, logs:CreateLogStream, logs:DescribeLogGroups, logs:DescribeLogStreams, logs:PutLogEvents**.

- Creates a subscription filter and associates it with **CT-Avid-LogGroup** to subscribe to the real-time stream of log events ingested through the trail about and deliver them to AWS Lambda function **Avid-CloudTrail-function**. The Lambda function reads and parses the log, and sends the parsed events to Sophos Cloud Optix collectors running for your specific account.

The script also enables VPC Flow Logs in all regions and ships them to the Sophos Cloud Optix platform. In order to do this, the script does the following:

- Enables VPC Flow Logs to capture information about the IP traffic, and publishes to CloudWatch Logs under log group **Flowlogs-Avid-LogGroup**.

- Creates a role **Avid-VPCFlow-Role** which allows the AWS VPC-Flow-Logs to perform the following actions **logs:CreateLogGroup, logs:CreateLogStream, logs:DescribeLogGroups, logs:DescribeLogStreams, logs:PutLogEvents**.

- Creates a subscription filter and associates it with **Flowlogs-Avid-LogGroup** to subscribe to the real-time stream of log events ingested through the trail about and deliver them to AWS Lambda function **Avid-VPC-LOGS-function**. The Lambda function reads and parses the flow logs, and sends them to Sophos Cloud Optix collectors running for your specific account.

**Note**

If you prefer not to enable VPC Flow Logs, use the **FLOW_LOGS** variable in the script to specify that. The **Topology** feature will not show inbound/outbound traffic visualization, and the anomaly detection won’t find unusual traffic patterns, if you don’t enable VPC Flow Logs.
3.8 AWS CLI script variables

AWS script variables

Required variables

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXTERNAL_ID</td>
<td>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.</td>
</tr>
<tr>
<td>CUSTOMER_ID</td>
<td>The Customer UUID used for all uploads and connections.</td>
</tr>
<tr>
<td>REQUEST_ID</td>
<td>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.</td>
</tr>
<tr>
<td>DNS_PREFIX_FLOW</td>
<td>The customer specific prefix that allows connection back to the appropriate collector node in the Sophos Cloud Optix backend for flowlogs.</td>
</tr>
<tr>
<td>DNS_PREFIX_CLOUDTRAIL</td>
<td>The customer specific prefix that allows connection back to the appropriate collector node in the Sophos Cloud Optix backend for CloudTrail logs.</td>
</tr>
</tbody>
</table>

Optional variables

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS_DEFAULT_REGION</td>
<td>Use this if you want to install in a region that is different than your configured default region for AWS CLI.</td>
</tr>
<tr>
<td>TRAIL_NAME</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Variable Description

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FLOW_LOGS</td>
<td>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.</td>
</tr>
<tr>
<td>FLOWLOG_REGIONS</td>
<td>Command separated list of AWS regions.</td>
</tr>
</tbody>
</table>

#### 3.9 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 12)
  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.

**3.10 Remove your AWS environment**

Find out how to 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 18)
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:**
   ```bash
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
   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` file is created, with details of the resources that were created. If the `.tfstate` file 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.

You must run the Cloud Optix script using Azure PowerShell.

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

**Note**
By adding your Microsoft Azure 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.

To add your Azure subscriptions, you should do as follows:

- Use an Azure AD Account with Global Administrator Permission at Tenant level and Owner permission at Subscription level.
- Run the Cloud Optix script using Azure PowerShell. See [Quickstart for PowerShell in Azure Cloud Shell](#).

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 Provider environment** page, select the **Azure Subscription** tab.
4. Follow the steps shown to go to Azure and open Azure PowerShell. You must not run the script using PowerShell on your computer.
5. Download the script and run it in Azure PowerShell.
   ```bash
   ./create-azure-app.ps1 -CustomerId <...> -RequestId <...> -avidFlowAddress <...
   >-avidActivityAddress <...
   ```
   The script lets you choose all subscriptions or only the subscriptions you want to add.
   The script creates an AD application, service principal, add response URL and grant permission at subscription. By default, this grants ‘Reader’ permission to the app if no role name is provided.
6. After the script has run, enable user and group data sync with Azure AD.
   To do this, you must authorize using an admin account for the subscriptions you have added.
7. At the end of the script, a URL is shown. Go to the URL to authenticate.
   You need to be an Application Administrator in the Active Directory containing the subscriptions you added (or ask an Application Administrator to authenticate for you).

**Related concepts**
- [What does the Sophos Cloud Optix script to add Azure environments do?](#)
  The script sets up Sophos Cloud Optix so that it can receive data from your Azure AD environment.

**Related tasks**
- [Troubleshooting for Azure](#)
If there are problems with adding an Azure environment, remove it and start again.

Related reference
Quickstart for PowerShell in Azure Cloud Shell

4.1 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 Settings (in the left-hand menu) and select Environments.
2. In the list, find the environment you want to remove and click the trashcan icon (on the right).
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.

4.2 Troubleshooting for Azure

If there are problems with adding an Azure environment, remove it and start again.

Do as follows:

1. Check avidsecure-script-output.log for errors.
2. Follow the instructions in Remove your Azure environment (page 22).
3. Add your environment again.

Related tasks
Add your Microsoft Azure environment (page 21)
You can add your Azure environment to Sophos Cloud Optix by running the PowerShell script Sophos provides.

4.3 What does the Sophos Cloud Optix script to add Azure environments 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:
   • 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:
   • 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. The attributes used to create the role are as follows:
      • Role name: `AvidNetWatcher + <First 8 characters of subscription id without '-'>`
      • Description: This role can configure flow logs, list storage and NSG resources, create/delete storage accounts, list keys, and create/delete Azure Functions.
b) Creates a resource group for the subscription with the following attributes:
   - **Name:** avidflowlogsgroup
   - **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:
   - **Name:** avidact + <first 8 characters of SubscriptionId without '-' > + <first 8 characters of CustomerId without '-' >
   - 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:
   - **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:

- **Name:** `AvidActivityLogs + <first 8 characters of SubscriptionId without '-'> + <first 8 characters of CustomerId without '-'>`

- 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 following application information to ClusterRole and ClusterRoleBinding to add the environment to the service:

- Subscription name
- Subscription id
- Tenant id
- Encrypted key for AD application

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.
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 27)
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:
— 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
  
  ```json
  ["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 26)*

You can add a Google Cloud Platform (GCP) project to Sophos Cloud Optix by running the script Sophos provides.
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. This 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 26)
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 30)
Sophos provides a GitHub app which you can install to give Sophos Cloud Optix access to your repositories.

Add code repositories using Bitbucket (page 31)
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 33)
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:

![Sophos Cloud Optix App](image)

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**.
Select a Bitbucket account for the Sophos Cloud Optix App app to access

You are logged in as avidsid

Siddharth (avidsid)

Can't see the account you want? Change user

Sophos Cloud Optix App (https://optix.sophos.com) is requesting access to:

- Read your account information
- Read your repositories

This 3rd party vendor has not provided a privacy policy or terms of use. Atlassian's Privacy Policy is not applicable to the use of this App.

Grant access  Cancel
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.
### Click on an alert to open a detailed overview.

<table>
<thead>
<tr>
<th>Alert ID</th>
<th>Severity</th>
<th>Description</th>
<th>Type</th>
<th>Affected Resource</th>
<th>Last Seen</th>
<th>Provider</th>
<th>Environment</th>
<th>Compliance Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>A-30317</td>
<td>B</td>
<td>Ensure that the -u option is not set to true.</td>
<td></td>
<td></td>
<td>6 days ago</td>
<td>kC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A-30318</td>
<td>C</td>
<td>Ensure that the --name option is not set to true.</td>
<td></td>
<td></td>
<td>30 days ago</td>
<td>kC</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.
<table>
<thead>
<tr>
<th>Resource</th>
<th>FirstSeen</th>
</tr>
</thead>
<tbody>
<tr>
<td>redshift (Ref: new_cluster, File: ansible_test.yaml)</td>
<td>2 days ago</td>
</tr>
</tbody>
</table>

```
{
  "root": {
    "resourceType": "redshift",
    "reference": "new_cluster",
    "file": "ansible_test.yaml",
    "branch": "master",
    "repoURL": "https://github.com/AvidSid/DevSecOpsDemo",
    "committerName": "Siddharth Kundal",
    "committerEmail": "siddharth.kundal@sophos.com"
  }
}
```
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 38)
This section tells you how to create the role needed before you can use remediation.

Turn on automatic remediation (page 39)
How to turn on automatic remediation.

Use manual remediation (page 39)
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
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**
Sophos Cloud Optix

- 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 41)
Sophos Cloud Optix displays alerts when it detects anomalies in your environment.

*User login anomalies* (page 42)
Sophos Cloud Optix detects suspicious login events.

*Outbound network traffic anomalies* (page 42)
Sophos Cloud Optix detects anomalous outbound network traffic.

*Applications inferred from host behavior* (page 43)
Sophos Cloud Optix can infer the applications running from the behavior of the host computer instance.

*High-risk activity* (page 43)
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:

![Alert Icon]

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

An anomaly alert looks like this:

![Anomaly Alert Example]

Multiple logins from two different regions in short time
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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account ID</td>
<td>Account ID</td>
</tr>
<tr>
<td>Timeframe</td>
<td>The time period of the deviation (30-minute slots)</td>
</tr>
</tbody>
</table>
### 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.

---

**Table:**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Traffic</td>
<td>Total traffic observed in the timeframe</td>
</tr>
<tr>
<td>Expected Traffic</td>
<td>Traffic expected by machine learning models</td>
</tr>
<tr>
<td>Variation</td>
<td>Variation between actual and expected traffic</td>
</tr>
<tr>
<td>Destination port</td>
<td>Destination port</td>
</tr>
<tr>
<td>Destination protocol</td>
<td>Destination protocol</td>
</tr>
<tr>
<td>Top Originating IPs</td>
<td>Top IPs from which traffic flows</td>
</tr>
<tr>
<td>Top Destination IPs</td>
<td>Top IPs to which traffic flows</td>
</tr>
</tbody>
</table>

---
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.

![Sophos UTM Icon](image)

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.

Related concepts
Spend Monitor Thresholds (page 49)
You can configure rules to alert you if your cloud spend increases unexpectedly.

Compliance policies (page 50)
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 BigQuery 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-Roles.
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 50)
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 50)
You can customize Sophos Cloud Optix policies for your needs.

View policy reports (page 51)
Sophos Cloud Optix automatically generates reports for all out-of-the-box and custom policies.

Track policy compliance (page 51)
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 50).

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.

1. Go to **Settings > Integration**.
2. Click **Jira**.
3. Enter your Jira URL and the user name 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 will include an option to create a Jira ticket manually.
   - **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 enable the integration, select **Enable config** and click **Save**.

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

---

**Related concepts**

- **Jira integration permissions** (page 54)
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:

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

Update ticket

The username must have permission to comment in Jira.

<table>
<thead>
<tr>
<th>Jira field name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</td>
<td>Populated using AffectedResources.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Jira field name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Done.</td>
</tr>
<tr>
<td>Comment</td>
<td>Alert ID has been closed by Sophos Cloud Optix.</td>
</tr>
</tbody>
</table>

**Related tasks**

*Integrate with Jira* (page 53)

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 into your specified Slack channel for instant notification.

1. Go to Settings > Integration.
2. Click Slack.
3. You are redirected to slack.com. Enter your workspace and authorize the Sophos Cloud Optix Slack bot to get the alerts and push them on a channel that you specify.
4. In Sophos Cloud Optix, in Alert Levels, select which alerts you want to send to Slack.
5. To enable the integration, select Enable config and click Save.

### 13.3 Integrate with ServiceNow

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

1. Go to Settings > Integration.
2. Click ServiceNow.
3. Enter the ServiceNow URL, username and password, along with the assignment group for your tickets.
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 will include an option to create a ServiceNow ticket manually.
6. To enable the integration, select Enable config and click 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 the policy violation alert is cleared on the next run of policy check, the ticket created in ServiceNow will be marked as closed.
13.4 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:

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 enable the integration, select Enable config and click Save.

13.5 Integrate with PagerDuty

You can push Sophos Cloud Optix alerts to PagerDuty.

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 enable the integration, select Enable config and click Save.
13.6 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.

13.7 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.

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 will automatically start appearing on the Sophos Cloud Optix dashboard.

13.8 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 will send a test message to your SNS topic.

Related concepts
Set the AmazonSNS permission in AWS (page 58)
You need to edit permissions in your AWS account before you integrate Sophos Cloud Optix with Amazon SNS.

13.8.1 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.
14 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

Super Admin administrators that are also Super Admin administrators in Sophos Central can add Custom roles in Sophos Central.

Custom roles are based on the pre-defined Sophos Central Admin and Read-only administrator roles but also enable you to restrict access to a specific product in Sophos Central, such as 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.
• Add, edit or delete cloud environments.
• Configure third-party integrations.
• Configure the Sophos Cloud Optix API.

Custom roles are only available for Sophos Cloud Optix in Sophos Central, and are not available for the standalone Sophos Cloud Optix console.

**Related information**

*Environment access control (page 60)*

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

### 14.1 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 in the Sophos Cloud Optix console.

**Note**

This capability is not currently available to all customers.

**Related concepts**

*Administration roles (page 59)*

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

**Understanding environment access control**

You can limit access to information to specific cloud environments by creating environment tags and assigning them to administrators. An environment tag defines a group of cloud environments, for example AWS accounts, Azure subscriptions, and 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.
Administrator capabilities

It's important to understand the relationships between the different administrator roles and what environment tags allow them to do.

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.
15 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.

You can add as many cloud environments (e.g. 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 (e.g. 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 has been seen during 30 days prior to billing.

When Sophos Cloud Optix connects to a customer’s cloud environment (e.g. 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 (e.g. AWS accounts) in Sophos Cloud Optix.

**Table 1: MSP Flex billing example**

<table>
<thead>
<tr>
<th>Instance</th>
<th>Cloud assets used during 30 day period</th>
<th>Number of cloud assets recorded</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environment #1</td>
<td>25 on one day</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>50 on another day</td>
<td></td>
</tr>
<tr>
<td>Environment #2</td>
<td>10 on one day</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>20 on another day</td>
<td></td>
</tr>
<tr>
<td>Environment #3</td>
<td>25 on one day</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>Zero usage on another day</td>
<td></td>
</tr>
</tbody>
</table>

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.

**Related reference**

Sophos Cloud Optix (PAYG) on AWS Marketplace
16 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/
GCP: https://cloud.google.com/stackdriver/

Log routing

AWS: https://aws.amazon.com/cloudwatch/pricing/
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/
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/
GCP: https://cloud.google.com/pricing/list
17 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.
18 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.
19 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.
20 Legal notices

Copyright © 2020 Sophos Limited. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos, Sophos Anti-Virus and SafeGuard are registered trademarks of Sophos Limited, Sophos Group and Utimaco Safeware AG, as applicable. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.