
CloudOptics Documentation

Release 1.0

Team CloudOptics

Jan 08, 2023

Contents

1	Introduction	3
1.1	Subscribing CloudOptics as SaaS	3
1.2	Install CloudOptics on a Server	3
1.3	Procuring CloudOptics from AWS Marketplace	5
2	Initial Configuration Of CloudOptics	7
3	Prepare & Onboard Cloud Accounts	11
3.1	Prepare AWS Account for Onboarding (Access Key)	11
3.2	Prepare AWS Account for Onboarding (Cross Account)	14
3.3	Prepare AWS Account Billing for Onboarding	17
3.4	Prepare Azure Account for Onboarding	21
3.5	Prepare Google Cloud Account for Onboarding	25
3.6	Prepare OpenStack Account for Onboarding	31
4	Add Cloud Accounts to CloudOptics	35
4.1	Adding an AWS Account	35
4.2	Adding an Azure Account	35
4.3	Adding Google Cloud Account	35
5	Advisory Assessment	39
5.1	Placing An Assessment Order	39
5.2	Adding Cloud Account To Order	40
5.3	Download Sample Report	40
5.4	Pay For Report	41
5.5	Download Report(s)	41
6	Threat Intel Contextualization (AWS Only)	43
6.1	Configure Systems Manager	43
7	Infra Vulnerability Assessment (AWS Only)	47

Please follow the instructions to install & configure the product.

CHAPTER 1

Introduction

CloudOptics has the ability to manage a single cloud account or multiple clouds. Product also has the capability to onboard multiple customers at the same time, having various cloud accounts of their own.

Following guide will help choose the right product edition to get started.

Trial version of the product comes with a no obligation 2-weeks entitlement. Trial version comes fully functional with all modules of CloudOptics to secure your critical infrastructure.

Please select the target environment where you want to install the product for detailed steps.

1.1 Subscribing CloudOptics as SaaS

CloudOptics is available as SaaS for organizations to subscribe online and consume. Please follow instructions below to use SaaS -

1. Please visit <https://app.cloudoptics.io/#/setup> & register
2. Please follow on screen instructions to complete the registration

1.2 Install CloudOptics on a Server

In order to install CloudOptics on any machine of your choice in any environment, please follow these instructions.

1.2.1 Eligibility

1. CloudOptics platform license can be procured by a Managed Service Provider (MSP) by writing to sales@cloudoptics.io Post email, download authorization will be provided along with a license key.

MSP version allows a company to host CloudOptics platform in a multi-tenant mode so all of their customer can be serviced directly by the MSP



1 License Information — 2 Administrator Account Setup — 3 Subscription Details

<input type="text" value="Administrator First Name"/>	<input type="text" value="Administrator Last Name"/>
<input type="text" value="Administrator Email Id"/>	<input type="text" value="Administrator Phone"/>
<input type="text" value="Company Name"/>	<input type="text" value="Company Address"/>
<input type="text" value="Company City"/>	<input type="text" value="Company State"/>
<input type="text" value="Company Zip Code"/>	

Next

2. CloudOptics platform license can also be procured by an end customer for its own use, by writing to sales@cloudoptics.io Post email, download authorization will be provided along with a license key.

End user version allows a company to host CloudOptics platform in a their account in a single tenant mode, so all of their cloud accounts can be onboarded and monitored.

1.2.2 Pre-Requisite

We recommend following machine configuration for installing CloudOptics

- Ubuntu 18.04 Operating System
- sudo access on the machine
- 16GB RAM, 4 vCPU, 100GB Hard Disk
- [Docker Community Edition](#)

1.2.3 Networking Requirement

- Inbound access on port 8080 to access Platform console
- Outbound access to connect with various target clouds & Licensing Server

1.2.4 Quick Installation

Please execute following command to get the required script.

```
curl -sO http://remote.cloudoptics.io/install.sh  
  
chmod +x install.sh
```


Execute following command to start the installation

```
./install.sh
```

Installation script will configure public IP of the machine for accessing product console.

1.3 Procuring CloudOptics from AWS Marketplace

You could also launch CloudOptics from AWS Marketplace.

CHAPTER 2

Initial Configuration Of CloudOptics

Before you begin, please collect SMTP server details from you administrator.

In your browser, please open url <http://<public ip>:8080/#/setup>

1. You should see following screen.

Please fill the information correctly as the license generated will be against the entity. This information may not be edited afterwards.

2. Successful license generation will present following screen.
3. Next you need to configure SMTP server details to receive emails

Thats it!!! You should be greeted with the login page.

Please Enter License Information


	Administrator First Name
	Administrator Last Name
	Administrator Email Id
	Administrator Phone#
	Company Name
	Company Address Line 1
	Company Address Line 2
	Company Address City
	Company Address State
	Company Address Zip Code

Generate License

Setup Administrator Account

 aseem@cloudoptics.io

 aseem@cloudoptics.io

 Password

 Confirm Password

Create Account

Please Enter SMTP Server Details

	mail.smtp.host
	mail.smtp.port
	mail.user
	mail.password
	mail.sender.mailid
	mail.sender.name


Update



Login To Continue

	<input type="text" value="Username"/>
	<input type="password" value="Password"/>

SIGN IN

 [Forgot your password?](#)

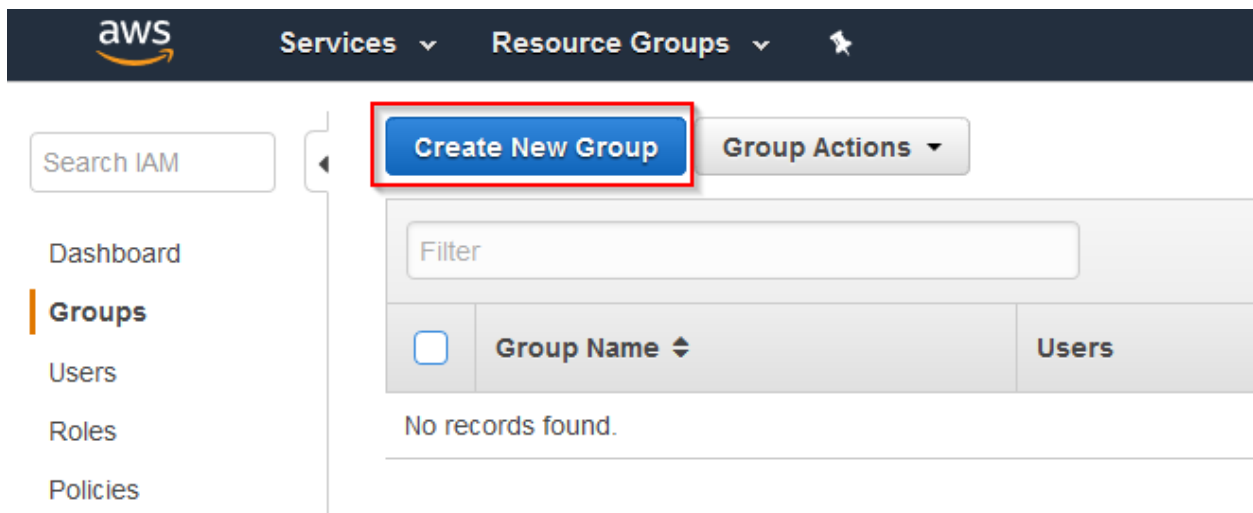
Prepare & Onboard Cloud Accounts

CloudOptics supports various types of cloud integrations. Before onboarding cloud accounts need to be prepared for CloudOptics. Please use specific guide for integrating your cloud.

3.1 Prepare AWS Account for Onboarding (Access Key)

Please follow the instruction to prepare your AWS account for onboarding into the product. This uses AccessKey method. Please note, CWPP features will not be accessible using this approach.

1. Sign-in to AWS Console & go to IAM Service to create a new group “CloudOpticsGroup”



2. Please use following IAM Permissions to add to group
 - ReadOnlyAccess

- AWSCloudTrailReadOnlyAccess
- CloudWatchReadOnlyAccess

Review

Review the following information, then click **Create Group** to proceed.

Group Name CloudOpticsGroup [Edit Group Name](#)

Policies [Edit Policies](#)

- arn:aws:iam::aws:policy/ReadOnlyAccess
- arn:aws:iam::aws:policy/AWSCloudTrailReadOnlyAccess
- arn:aws:iam::aws:policy/CloudWatchReadOnlyAccess

3. Verify the name & permissions in next screen to create the group

Summary

Group ARN: arn:aws:iam::[redacted]:group/CloudOpticsGroup

Users (in this group): 0

Path: /

Creation Time: [redacted]

Permissions

Managed Policies

The following managed policies are attached to this group. You can attach up to 10 managed policies.

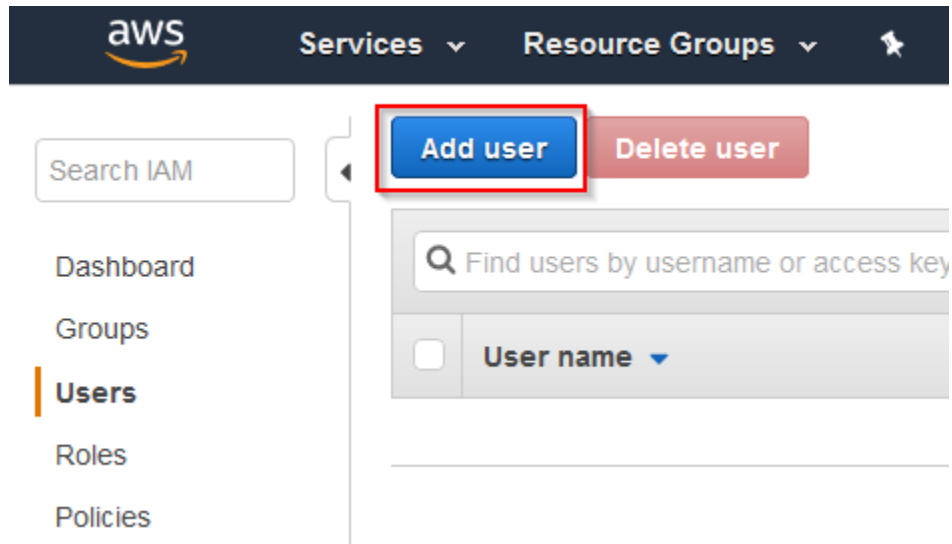
[Attach Policy](#)

Policy Name	Actions
ReadOnlyAccess	Show Policy Detach Policy Simulate Policy
AWSCloudTrailReadOnlyAccess	Show Policy Detach Policy Simulate Policy
CloudWatchReadOnlyAccess	Show Policy Detach Policy Simulate Policy

4. Go to AddUser in AWS IAM Console

5. Add user CloudOptics with ProgrammaticAccess

6. Next we will add this user to “CloudOpticsGroup”



Add user

1

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

[Add another user](#)

Select AWS access type


Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)


Access type* ☒ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.


☐ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Add user

Set permissions for CloudOptics

 Add user to group

 Copy permissions from existing user

 Attach existing policies directly

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions

Add user to group

Create group

Refresh


Group	Attached policies
<input checked="" type="checkbox"/> CloudOpticsGroup	ReadOnlyAccess and 2 more

- Copy Access Key ID & Secret Access Key in a notepad as shown in screen below. We will need it to onboard AWS account into CloudOptics

Warning: The Secret Key will not be shown again. So it is important to make a note of it.

Add user

1 2 3 4

 **Success**
 You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

 Users with AWS Management Console access can sign-in at: [https://\[redacted\].signin.aws.amazon.com/console](https://[redacted].signin.aws.amazon.com/console)

Download .csv

User	Access key ID	Secret access key
CloudOptics	[redacted]	[redacted] Show

3.2 Prepare AWS Account for Onboarding (Cross Account)

Please follow the instruction to prepare your AWS account for onboarding into the product.

- Sign-in to AWS Console & go to IAM Service to create a new role “CloudOpticsRole” Please follow the actions in the screenshot below.

Please note account number (673199402158) and external id (cloudoptics) needs to exactly match.

IAM > Roles > Create role 1

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity Info

Trusted entity type 2

☐ **AWS service**
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

☒ **AWS account**
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ **Web identity**
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

☐ **SAML 2.0 federation**
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

☐ **Custom trust policy**
Create a custom trust policy to enable others to perform actions in this account.

An AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

3 ☐ This account

3 ☒ **Another AWS account**

Account ID

4 Identifier of the account that can use this role

4

Account ID is a 12-digit number.

Options





5 ☒ **Require external ID (Best practice when a third party will assume this role)**
You can increase the security of your role by requiring an optional external identifier, which prevents "confused deputy" attacks. This is recommended if you do not own or have administrative access to the account that can assume this role. The external ID can include any characters that you choose. To assume this role, users must be in the trusted account and provide this exact external ID. [Learn more](#)

6 **External ID**

Important: The console does not support using an external ID with the Switch Role feature. If you select this option, entities in the trusted account must use the API, CLI, or a custom federation proxy to make cross-account iam:AssumeRole calls. [Learn more](#)

2. Please use following IAM Permissions to add to the role being created

- ReadOnlyAccess
- SecurityAudit
- AWSCloudTrailReadOnlyAccess
- CloudWatchReadOnlyAccess

<input type="checkbox"/>	Policy name <small>↗</small>	Type	Description
<input type="checkbox"/>	+  ReadOnlyAccess	AWS managed	Provides read-only access to AWS
<input type="checkbox"/>	+  SecurityAudit	AWS managed - job fun...	The security audit template grants
<input type="checkbox"/>	+  CloudWatchReadOnlyAccess	AWS managed	Provides read only access to Clou
<input type="checkbox"/>	+  AWSCloudTrail_ReadOnlyAccess	AWS managed	Provides read only access to AWS

3. Verify the name to create the role

IAM > Roles > Create role

Step 1
Select trusted entityStep 2
Add permissionsStep 3
Name, review, and create

Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

1 CloudOpticsRole

Maximum 64 characters. Use alphanumeric and '+', '=', '@', '-', '_' characters.

Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles **1**

Policies

Identity providers

Account settings

▼ Access reports

Access analyzer

Archive rules

Analyzers

Summary Edit

Creation date
November 17, 2021, 04:27 UTC-08:00

ARN
arn:aws:iam::123456789012:role/CloudOpticsRole **2**

Link to switch roles in console
<https://signin.aws.amazon.com/switchrole?roleName=CloudOpticsRole&account=123456789012>

Last activity
✔ 24 hours ago

Maximum session duration
4 hours

Permissions

Trust relationships

Tags

Access Advisor

Revoke sessions

Permissions policies (4) Info

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter. **3**

Policy name ↗

Type

Description

↻ Simulate Remove

Add permissions ▲

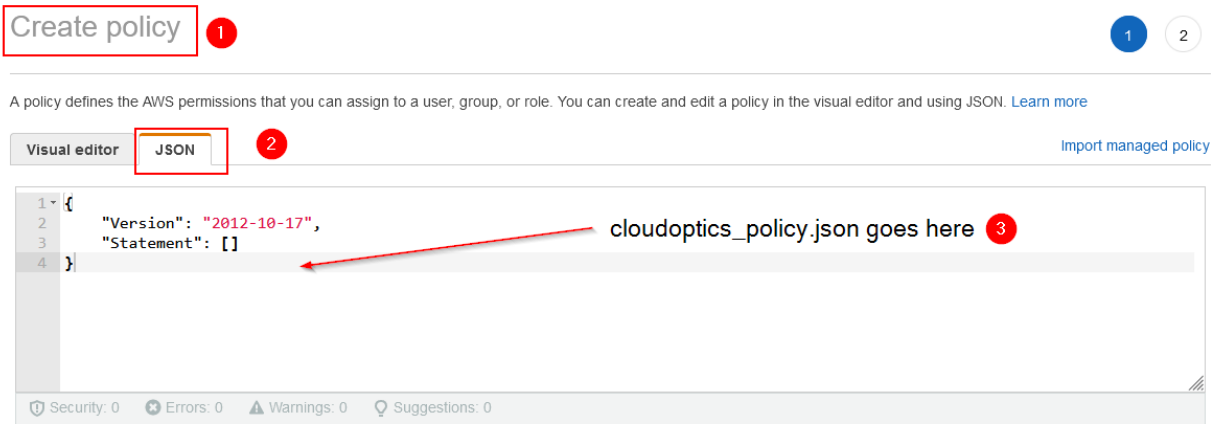
Attach policies

Create inline policy

4. After creating the role, go the role and create inline policy

5. Download cloudoptics_policy.json from [here](#).

6. Add cloudoptics_policy.json as per the image



7. Make a note of role ARN. It will be needed to onboard account into CloudOptics.

Please follow further instructions for CNAPP

8. Download co_kms_key_policy.json from [link](#).

9. Create a KMS key in the region of your workloads as per the image

- KMS Key Alias : CloudOptics-KMS-Key
- Key Administrator : CloudOpticsRole
- AWS Account to be added : 673199402158

10. Edit the KMS Key policy as per the image and insert co_kms_key_policy.json contents here

3.3 Prepare AWS Account Billing for Onboarding

Please follow the instruction to prepare your AWS account billing for onboarding into the product.

1. Sign-in to AWS Console & create a S3 bucket to export billing data

2. Please navigate to AWS Billing dashboard and click on create report

KMS > Customer managed keys > Create key

Step 1
Configure key

Step 2
Add labels

Step 3
Define key administrative permissions

Step 4
Define key usage permissions

Step 5
Review

Review

Key configuration

Key type Symmetric	Key spec SYMMETRIC_DEFAULT	Key usage Encrypt and decrypt
Origin AWS KMS	Regionality Multi-Region key	

ⓘ You cannot change the key configuration after the key is created.

Alias and description

Alias CloudOptics-KMS-Key	Description This key is for use by CloudOptics
------------------------------	---

Tags

Key	Value
name	cloudoptics

KMS > Customer managed keys > Key ID: mrk-f8c40fd47b59448759b5371178283a2e7a21

Key actions ▼ Edit

General configuration

Alias CloudOptics-KMS-Key	Status Enabled	Creation date Jan 08, 2023 11:19 GMT+5:30
ARN arn:aws:kms:ap-southeast-1:111111111111:key:mrk-f8c40fd47b59448759b5371178283a2e7a21	Description This key is for use by CloudOptics	Regionality Multi-Region primary

Key policy Cryptographic configuration Tags Key rotation Regionality Aliases

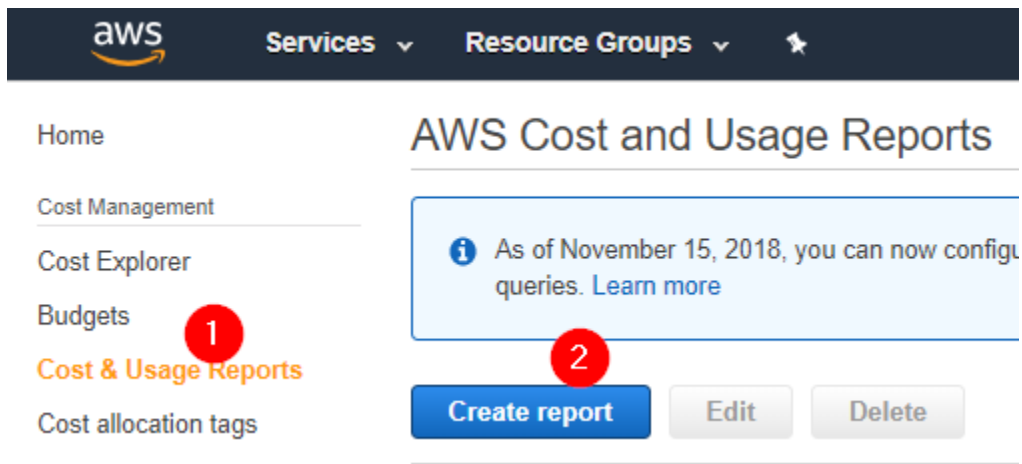
Key policy

Edit

```

1 {
2   "Version": "2012-10-17",
3   "Id": "key-consolepolicy-3",
4   "Statement": [

```



AWS Cost and Usage Reports > Create report

Step 1
Report content

Step 2
Delivery options

Step 3
Review

Report content

Report name - required

MyBills

Report includes

- Account identifiers
- Invoice and Bill Information
- Usage Amount and Unit
- Rates and Cost
- Product Attributes (e.g., instance type, operating system, and region)
- Pricing Attributes (e.g., offer types, and lease lengths)
- Reservation identifiers and related details (for reserved instances only)

Additional report details

☒ Include resource IDs ⓘ

Data refresh settings ⓘ

☒ Automatically refresh your Cost & Usage Report when charges are detected for previous months with closed bills.

Cancel

Next


Step 1
[Report content](#)

Step 2
Delivery options

Step 3
[Review](#)

Delivery options

S3 bucket - required

test-

[Configure](#)

[Verify](#)

✔ Valid Bucket

Report path prefix

report-prefix



Time granularity

☐ Hourly

☒ Daily

The time granularity on which report data are measured and displayed.

Report versioning

☐ Create new report version

☒ Overwrite existing report

Enable report data integration for

☐ Amazon Athena

☐ Amazon Redshift

☐ Amazon QuickSight

Compression type

GZIP

File format

text/csv

[Cancel](#)

[Previous](#)

[Next](#)

3. Provide the bill report name & select Resource Id

4. Configure S3 target bucket for report delivery and select rest of the options as shown below.

5. Go to IAM section and create a policy named “CostExplorerAPI”

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ce:*",
        "cur:DescribeReportDefinitions"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

6. Go to “CloudOptics” user and attach “CostExplorerAPI” policy to the user.

Users > **CloudOptics**

Summary

User ARN arn:aws:iam: [redacted] :user/CloudOptics

Path /

Creation time [redacted]

Permissions Groups (1) Tags Security credentials Access Advisor

▼ Permissions policies (11 policies applied)

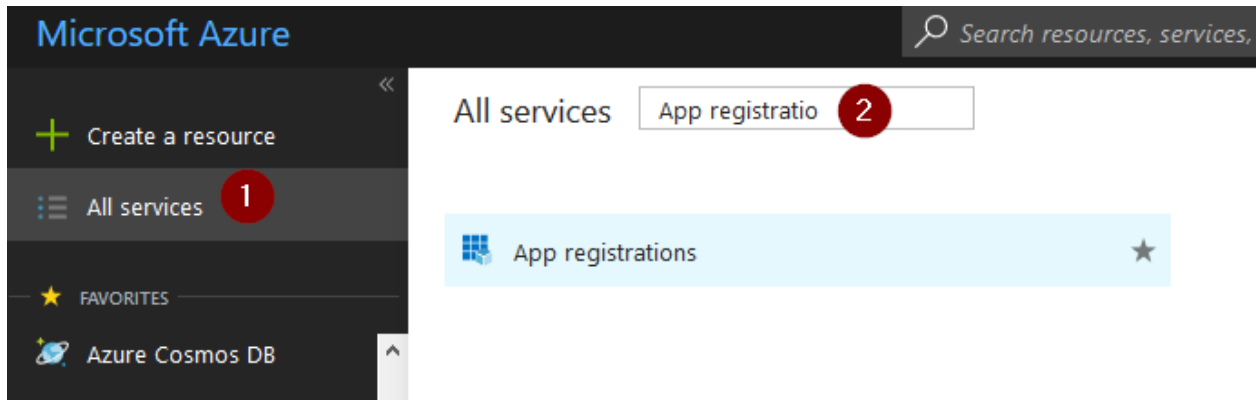
Add permissions

Policy name ▼	Policy type ▼
Attached directly	
▶ CostExplorerAPI	Managed policy

3.4 Prepare Azure Account for Onboarding

Please follow the instruction to prepare your Azure account for onboarding into the product.

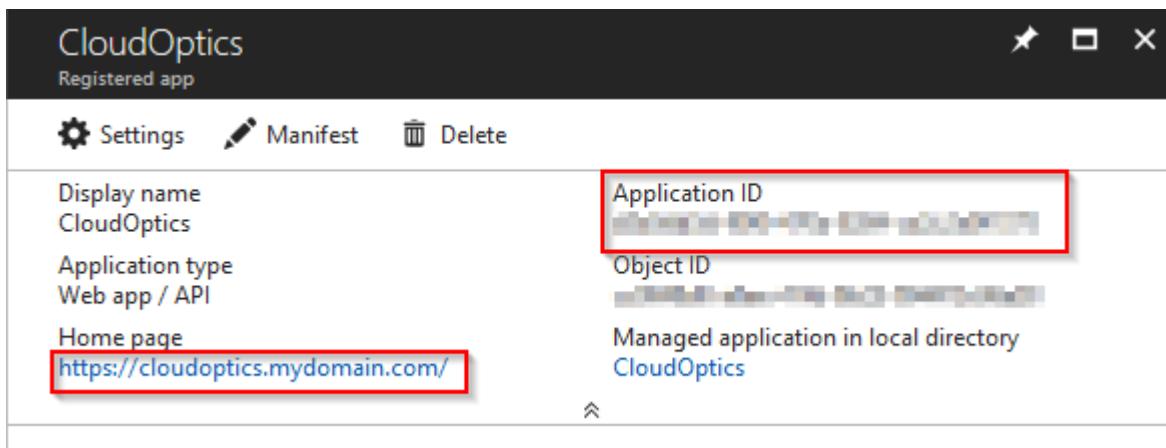
1. Sign-in to <https://portal.azure.com/> Console & click as directed in screen below



2. Register a new application, with following information

- Display Name - CloudOptics
- Home Page - Intended login URL for CloudOptics

Once created, copy Application Id value in a notepad as “Client Id”



3. Click on “Settings” then further on “Keys” as per screen below

4. Create a new key with name “CloudOptics Key”, expiry date as “Never Expires” and hit save. Once saved value filed will be shown. Please copy the value field in a notepad as “Azure Secret Key”

Warning: This value will not be shown again. So it is important to make a note of it.

5. Go back to portal home and follow the sequence as directed below and copy the Directory ID as “Tenant Id”

6. From the portal, find out “Subscription ID”

CloudOptics
Registered app

Settings 1 Manifest Delete

Display name	Application ID
CloudOptics	f074574a-68b3-4af4-a1db-552b6479b3ca
Application type	Object ID
Web app / API	a905bcd1-c48b-48bd-ac23-a059818157c8
Home page	Managed application in local directory
http://app.cloudoptics.in/co/	CloudOptics

Settings

Filter settings

GENERAL

Properties >

Reply URLs >

Owners >

API ACCESS

Required permissions >

Keys 2 >

TROUBLESHOOTING + SUPPORT

Troubleshoot >

New support request >

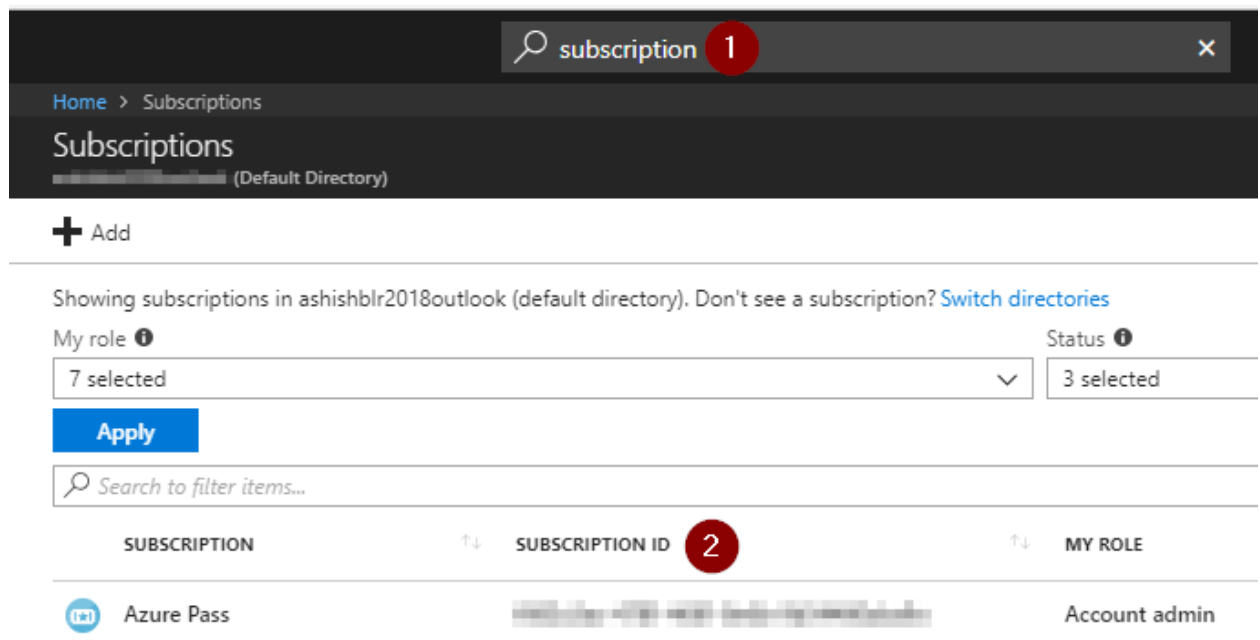
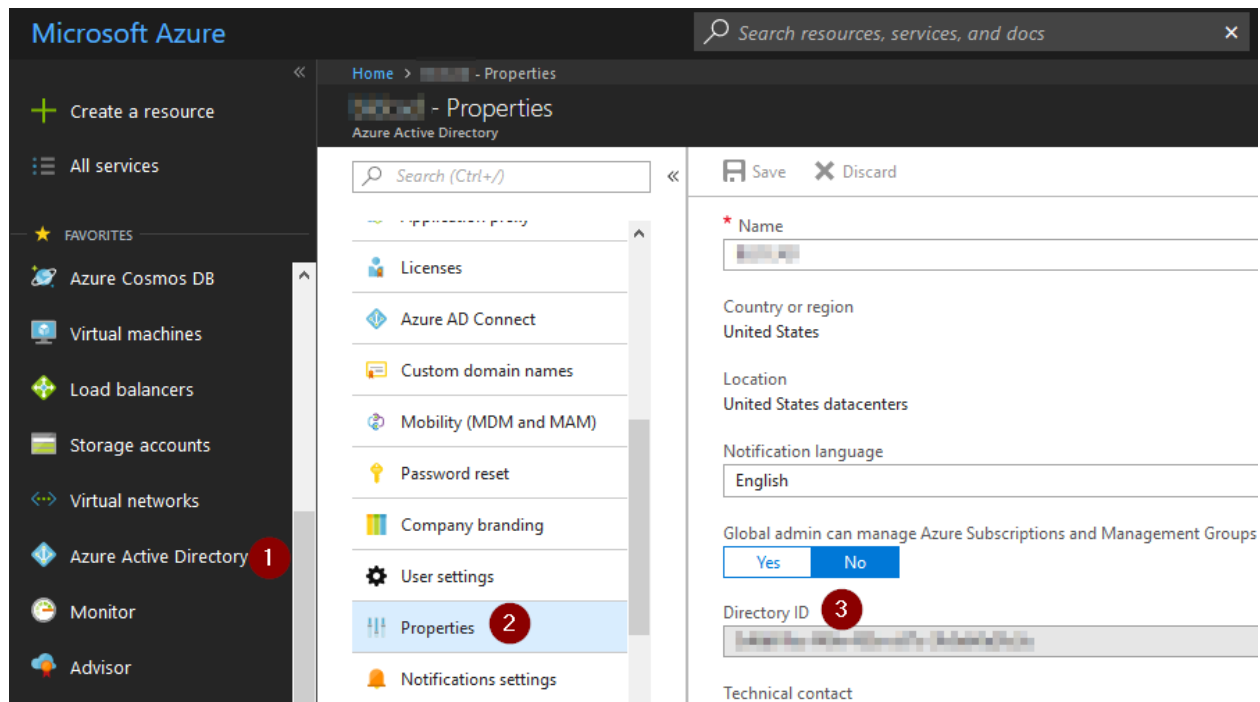
Keys

Save Discard Upload Public Key

! Copy the key value. You won't be able to retrieve after you leave this blade.

Passwords

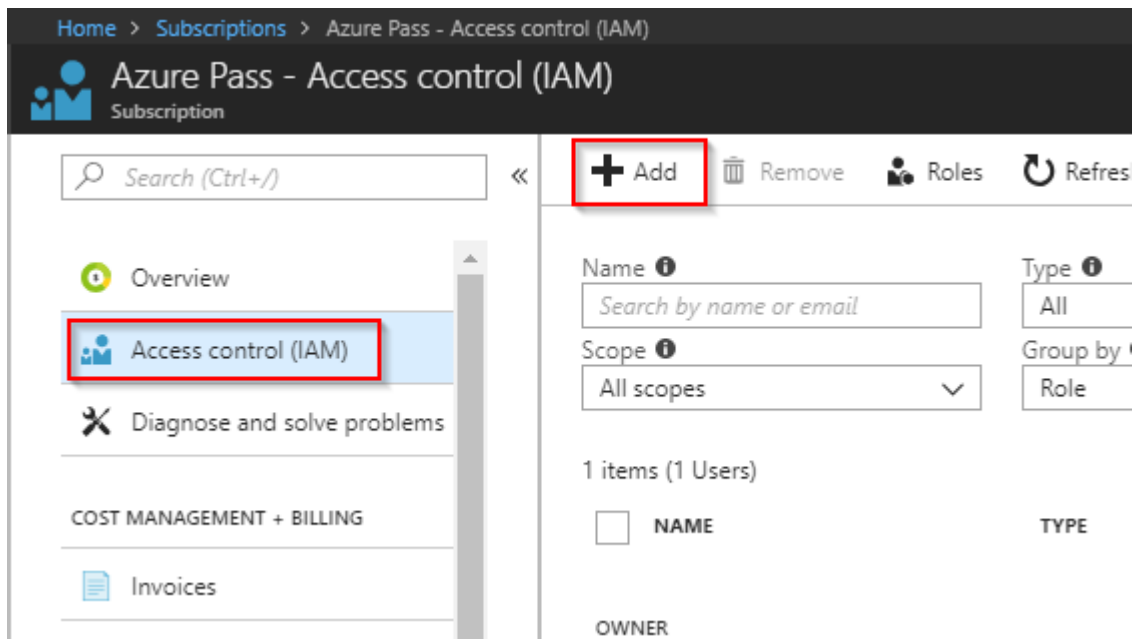
DESCRIPTION	EXPIRES	VALUE
	12/31/2299	Hidden
CloudOptics Key	12/31/2299	



7. You should now have 4 values in the notes. These values will be used in CloudOptics to onboard this Azure account

- Client ID
- Secret Key
- Tenant Id
- Subscription Id

8. Go to relevant Azure subscription and open Access Control (IAM) and click “Add”



9. Add the permissions of a “Reader” role to “CloudOptics” Application

Your Azure Account is now ready to be added in CloudOptics

3.5 Prepare Google Cloud Account for Onboarding

Please follow the instruction to prepare your Google Cloud Account for onboarding into the product.


1. Sign-in to <https://console.cloud.google.com> Console & select the project, you want to onboard
2. Start with creating a custom ‘Viewer’ role for CloudOptics. This role will be created from Google default role ‘Viewer’
3. Search and add following permissions for the role
 - storage.buckets.get
 - storage.buckets.getIamPolicy

Add permissions

Role ⓘ
Reader

Assign access to ⓘ
Azure AD user, group, or application

Select ⓘ
cloud

 CloudOptics

Google Cloud Platform
ISO27001-Application

IAM & admin 1

Roles
+ CREATE ROLE
CREATE ROLE FROM SELECTION

Roles for ISO27001-Application project

A role is a group of permissions that you can assign to members. You can create a role and add permissions to it, or copy an existing role and adjust its permissions. [Learn more](#)

Filter table

Type	Title ↓ 3	Used in	Status	
<input type="checkbox"/>	Viewer of Tenancy Units	Service Consumer Management	Enabled	⋮
<input checked="" type="checkbox"/>	Viewer 4	Project	Enabled	⋮
<input type="checkbox"/>	TPU Viewer	Cloud TPU	Enabled	⋮
<input type="checkbox"/>	TPU Admin	Cloud TPU	Enabled	⋮
<input type="checkbox"/>	Support Account Viewer	Support	Enabled	⋮
<input type="checkbox"/>	Support Account Administrator	Support	Enabled	⋮
<input type="checkbox"/>	Subscribe with Google Developer	Other	Enabled	⋮
<input type="checkbox"/>	Storage Object Viewer	Storage	Enabled	⋮

Create role from this role 5

Disable
Delete
Edit

Viewer
ID
Role launch stage
Description
Read access to all
716 assigned

- storage.buckets.list
- storage.objects.getIamPolicy
- storage.objects.list

Verify the permission as per screen below.

The screenshot shows the Google Cloud Platform IAM & admin console. The left sidebar lists various IAM-related sections, with 'Roles' selected. The main panel displays the 'CloudOpticsViewer' role, which is highlighted with a red box. To the right of the role name are links for '+ EDIT ROLE' and 'CREATE FROM ROLE'. Below the role name, a list of permissions is shown. A red box highlights the following permissions: storage.buckets.get, storage.buckets.getIamPolicy, storage.buckets.list, storage.objects.getIamPolicy, and storage.objects.list.

Role	Permissions
CloudOpticsViewer	source.repos.get source.repos.getIamPolicy source.repos.list spanner.databaseOperations.get spanner.databaseOperations.list spanner.databases.beginReadOnlyTransaction spanner.databases.get spanner.databases.getDDL spanner.databases.getIamPolicy spanner.databases.list spanner.databases.read spanner.databases.select spanner.instanceConfigs.get spanner.instanceConfigs.list spanner.instanceOperations.get spanner.instanceOperations.list spanner.instances.get spanner.instances.getIamPolicy spanner.instances.list spanner.sessions.create spanner.sessions.delete spanner.sessions.get spanner.sessions.list stackdriver.projects.get storage.buckets.get storage.buckets.getIamPolicy storage.buckets.list storage.objects.getIamPolicy storage.objects.list subscribewithgoogledeveloper.tools.get tpu.acceleratorTypes.get

4. Create a Service Account for the project

5. Add custom role created in step #2 above to the service account

6. Create a JSON key for the service account and save it on your local computer.

Warning: This JSON will not be shown again. So it is important to save it.

7. Navigate to API & Access area of the dashboard for the project

The screenshot shows the Google Cloud Platform interface for creating a service account. The left sidebar lists navigation options: IAM & admin (1), IAM, Identity & Organisation, Organisation policies, Quotas, Service accounts (2), Labels, Privacy & Security, Settings, Cryptographic keys, Identity-Aware Proxy, Roles, and Audit Logs. The main content area is titled 'Create service account' (3) and shows progress indicators for 'Service account details' (1) and 'Grant this service account access to the project (optional)' (2). The 'Service account details' section includes a text input for 'Service account name' with the value 'CloudOptics' (4), a label 'Display name for this service account', a text input for 'Service account ID' with the value 'cloudoptics' and a domain '@iso27001-application.iam.gserviceaccount.com', a text input for 'Service account description' with the value 'This account gives read-only access to CloudOptics' (5), and a label 'Describe what this service account will do'. At the bottom are 'CREATE' and 'CANCEL' buttons.

The screenshot shows the second step of the 'Create service account' process. The left sidebar is the same as the previous screenshot. The main content area shows progress indicators for 'Service account details' (1) and 'Grant this service account access to the project (optional)' (2). The 'Service account permissions (optional)' section includes a text input for 'Role' with the value 'CloudOpticsViewer' (highlighted by a red box), a label 'Created on: 2019-01-10 Based on: Viewer', and a '+ ADD ANOTHER ROLE' link. At the bottom are 'CONTINUE' and 'CANCEL' buttons.

orm ISO27001-Application

Create service account

✓ Service account details ✓ Grant this service account access to the project (optional)

Grant users access to this service account (optional)

Grant access to users or groups that need to perform actions as this service account. [Learn more](#)

Service account users role ?
Grant users the permissions to deploy jobs and VMs with this service account

Service account admins role ?
Grant users the permission to administer this service account

Create key (optional)

Download a file that contains the private key. Store the file securely because this key can't be recovered if lost. However, if you are unsure why you need a key, skip this step for now.

+ CREATE KEY 1

DONE CANCEL

Create key (optional)

Download a file that contains the private key. Store the file securely because this key can't be recovered if lost. However, if you are unsure why you need a key, skip this step for now.

Key type

☒ JSON 2
Recommended

☐ P12
For backward compatibility with code using the P12 format

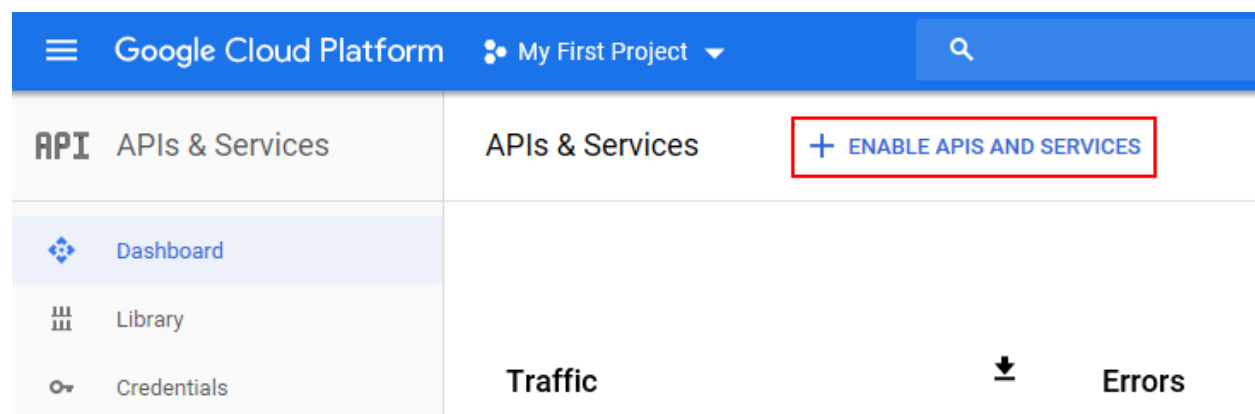
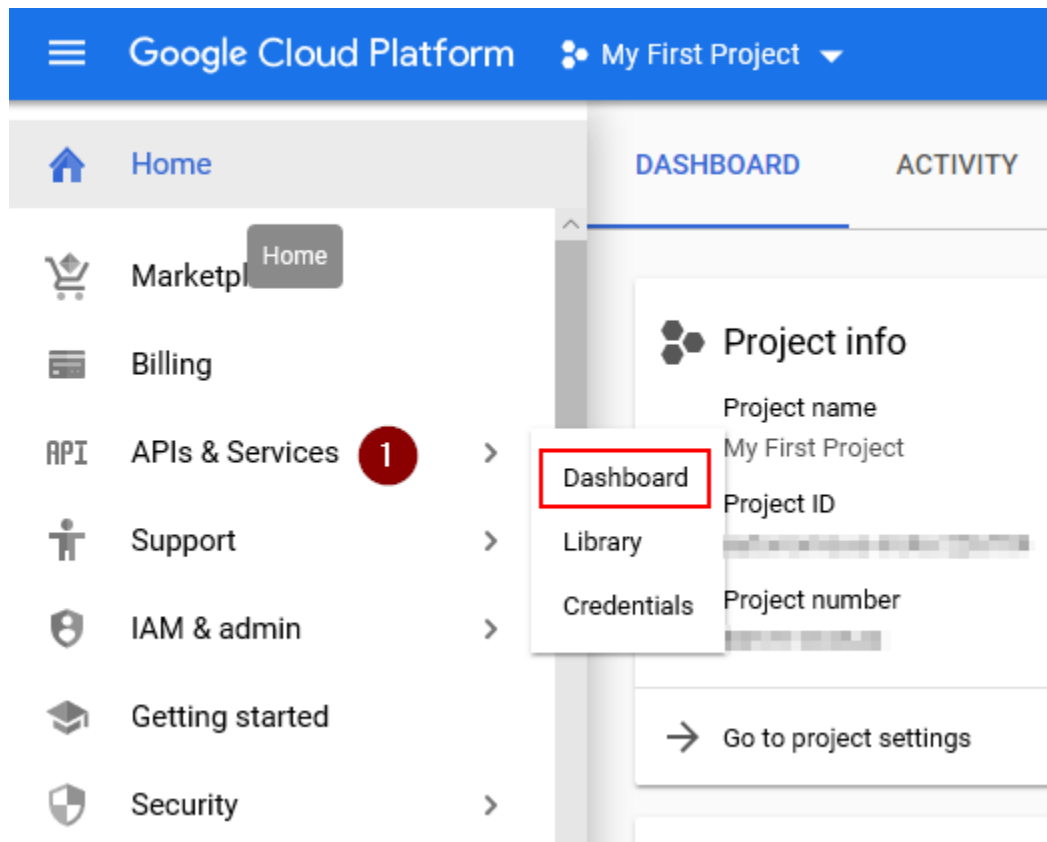
CREATE 3 CANCEL

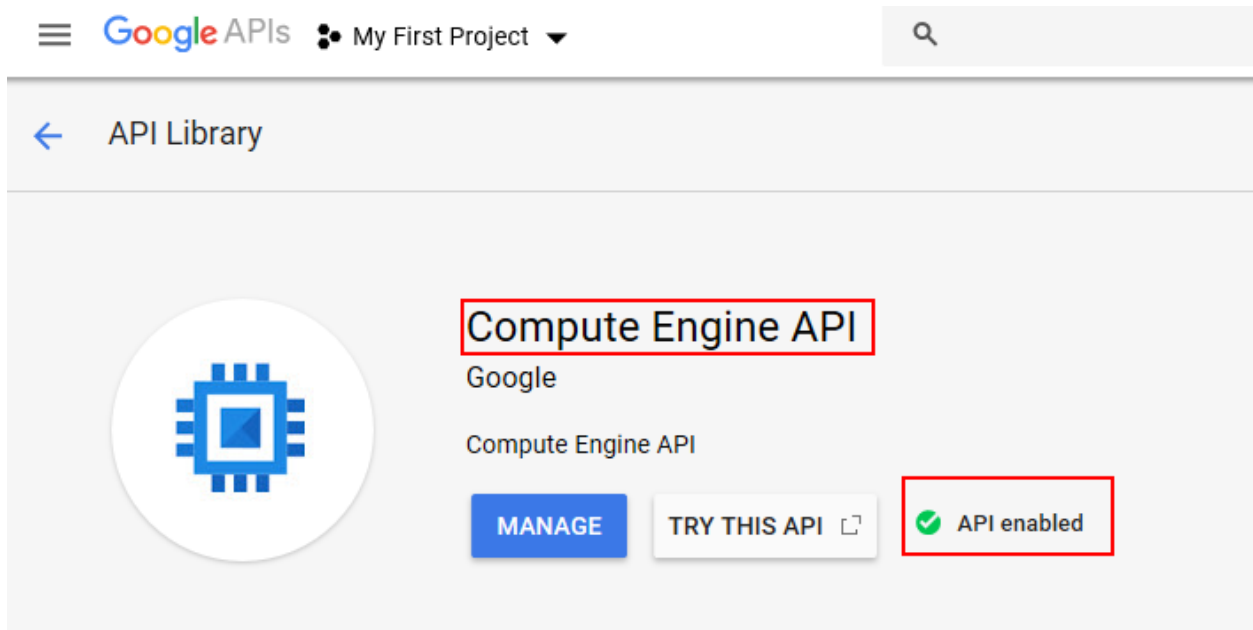
Private key saved to your computer



iso27001-application-dbc50a57cb40.json allows access to your cloud resources, so store it securely. [Learn more](#)

CLOSE





8. Enable Compute API & verify access as per screenshot below

9. Enable IAM API & verify access as per screenshot below

10. Enable KMS API & verify access as per screenshot below

11. Enable Resource Manager API & verify access as per screenshot below

12. Enable Storage API & verify access as per screenshot below

Your Google Cloud Account is now ready to be added in CloudOptics




3.6 Prepare OpenStack Account for Onboarding


Please follow the instruction to prepare your OpenStack account for onboarding into the product.


The screenshot shows the Google APIs console interface. At the top, there is a navigation bar with the Google APIs logo, a project selector set to "My First Project", and a notification badge with the number "1". Below the navigation bar, the left sidebar contains a menu with "APIs & Services" and "Identity and Access..." highlighted. The main content area is titled "Overview" and includes links for "DISABLE API" and "PROVIDE FEEDBACK". The "Details" section on the right lists the following information:


- Name:** Identity and Access Management (IAM) API
- By:** Google
- Service name:** iam.googleapis.com
- Overview:** Manages identity and access control for Google Cloud Platform resources, including the creation of service accounts, which you can use to authenticate to Google and make API calls.
- Activation status:** Enabled

The screenshot shows the Google Cloud Platform API Library interface. At the top, there is a navigation bar with the Google Cloud Platform logo, a project selector set to "My First Project", and a search icon. Below the navigation bar, the left sidebar contains a "API Library" link. The main content area displays the "Cloud Key Management Service (KMS) API" by Google. The description states: "Google Cloud KMS allows customers to manage encryption keys and perform cryptographic operations...". Below the description, there are three buttons: "MANAGE", "TRY THIS API", and a status indicator showing a green checkmark and the text "API enabled".

 Google APIs  My First Project 




 API Library







Cloud Resource Manager API


Google


Creates, reads, and updates metadata for Google Cloud Platform resource containers.

[MANAGE](#) [TRY THIS API](#)  API enabled

 Google APIs  My First Project 




 API Library



Google Cloud Storage

Google

Google Cloud Storage is a RESTful service for storing and accessing your data on Google's ...

[MANAGE](#)  API enabled

Add Cloud Accounts to CloudOptics

Before onboarding, cloud accounts need to be prepared for CloudOptics. If you have not prepared your AWS/Azure accounts yet, please come back after making those changes.

After preparing the target cloud accounts, login to <https://app.cloudoptics.io/#/login> as Administrator

4.1 Adding an AWS Account

1. Click on + “Create Account” under “Security Monitoring”, select “AWS” from account type and provide requested information


4.2 Adding an Azure Account

1. Click on + “Create Account” under “Security Monitoring”, select “Azure” from account type and provide requested information

4.3 Adding Google Cloud Account

1. Click on + “Create Account” under “Security Monitoring”, select “Azure” from account type and provide requested information

Add New Cloud Account



[Click to prepare account](#)

Account Type
AWS

Account Alias *

Access Type
Read


Account Number *

Access Key *

Secret Key *

Add Service

Add New Cloud Account



[Click to prepare account](#)

Account Type
AZURE

Account Alias *

Access Type

Azure Subscription Id *


Azure Client Id *

Secret Key *

Azure TenantId

Add Service

Add New Cloud Account



Click to prepare account

Account Type

GoogleCloud

Account Alias *

Access Type

GCP JSON *

Add Service

4.3. Adding Google Cloud Account

37

Advisory Assessment

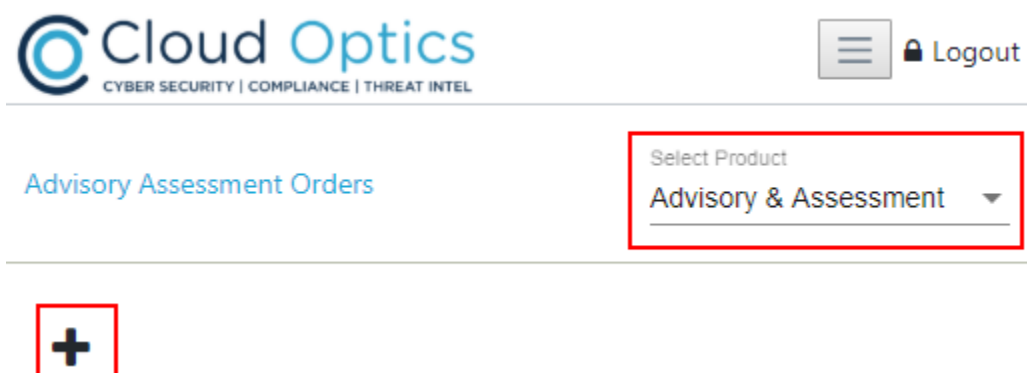
Using CloudOptics, you could do one time assessments for your cloud account. Various assessment options such as Security, Cost, Compliance assessments are available.

At high level following steps need to be followed -

1. Place an order
2. Add a cloud account to order
3. Download Sample Report (Optional)
4. Pay for the assessment
5. Download Report(s)

5.1 Placing An Assessment Order

1. Open the order dialog box by clicking on + icon in “Advisory Assessment” product selection



2. Complete the order wizard by entering estimated VMs and selecting assessment options

Place An Order

×

1 Select Category and Services

2 Summary

3 Done

Enter estimated Virtual Machine per account *

40

This product category provides advisory/assessment services for desired accounts.

☐ Cloud Config Assessment

☐ Security Controls Assessment ISO 27001 2013 - (Optional)

☐ Security Controls Assessment HIPAA 45.CFR.164 - (Optional)

☐ Security Controls Assessment PCI 3.2 - (Optional)

☐ Security Controls Assessment NIST-CSF 1.0 - (Optional)

Cancel

Next

3. You should receive an email indicating successful order placement within 10 minutes.

5.2 Adding Cloud Account To Order

1. On the newly placed order, click on + icon to add cloud account. Account preparation instructions link is there in the popup.

+

Referral Code: FL

Cloud Config Assessment


Cloud Config Assessment

AWS

673199402155

Add New Cloud Account

close



Instructions to fill below form

Account Type

AWS

Account Alias *

Access Type

Account Number *

Access Key *

Secret Key *

Add Account

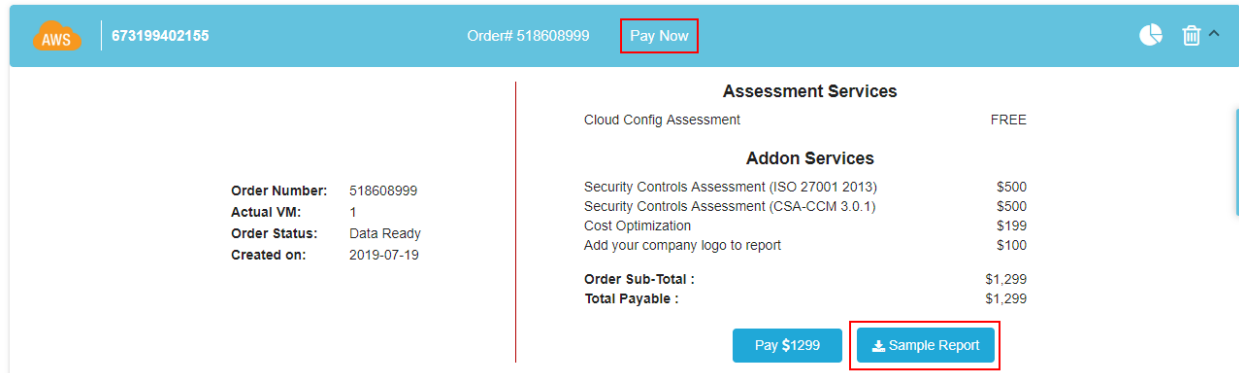
Cancel

2. As soon as account is added, assessment begins and an email notification is issued indicating successful addition to assessment order.

5.3 Download Sample Report

On completion of assessment, an email notification is sent. Most accounts finish assessments within 30 minutes. It may take longer depending on number of resources discovered in your account.

Using following button, all sample reports may be downloaded. Sample reports contain only a subset of assessment results and PSD exports are watermarked with text “Sample”.



Order Details:

- Order Number: 518608999
- Actual VM: 1
- Order Status: Data Ready
- Created on: 2019-07-19

Assessment Services

- Cloud Config Assessment: FREE

Addon Services

- Security Controls Assessment (ISO 27001 2013): \$500
- Security Controls Assessment (CSA-CCM 3.0.1): \$500
- Cost Optimization: \$199
- Add your company logo to report: \$100

Order Sub-Total: \$1,299
Total Payable: \$1,299

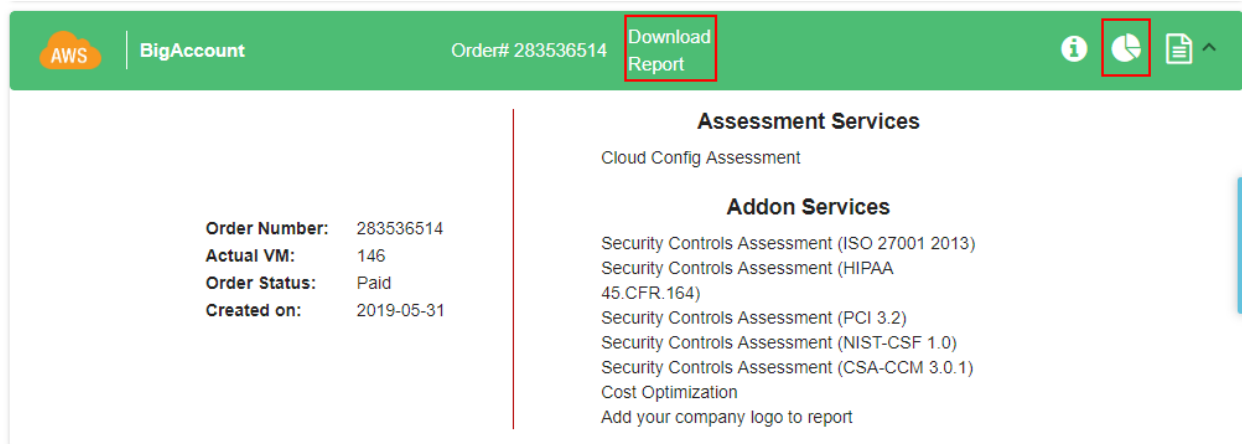
[Pay \\$1299](#) [Sample Report](#)

5.4 Pay For Report

Completed order display line items and prices based on resources detected in the account. All major credit cards are accepted for payment. We use Stripe payment system.

5.5 Download Report(s)

After payment order status changes to “Download Report” and all ordered assessment reports can be reviewed/download by clicking report icon.



Order Details:

- Order Number: 283536514
- Actual VM: 146
- Order Status: Paid
- Created on: 2019-05-31

Assessment Services

- Cloud Config Assessment

Addon Services

- Security Controls Assessment (ISO 27001 2013)
- Security Controls Assessment (HIPAA 45.CFR.164)
- Security Controls Assessment (PCI 3.2)
- Security Controls Assessment (NIST-CSF 1.0)
- Security Controls Assessment (CSA-CCM 3.0.1)
- Cost Optimization
- Add your company logo to report

[Download Report](#)

Threat Intel Contextualization (AWS Only)

Using CloudOptics, you could be aware of virtual machines affected by latest vulnerabilities as they become known. Users of cloudOptics need to subscribe to threat intel feed and hunt for machines where they might be present. CloudOptics does it for you, automatically.

This service is available only for AWS account right now.

Follow these steps to enable your AWS account for onboarding into this service.

6.1 Configure Systems Manager

Please follow these steps for each of the regions in use.

1. Open the “Systems Manager” service and go to quick setup.

The screenshot shows the AWS Systems Manager console. On the left, the navigation pane has 'Quick Setup' highlighted with a red circle containing the number '1'. The main area is titled 'Systems Manager Quick Setup' and contains a section for 'Permissions (Required)'. Under the 'Instance profile role' heading, the 'Use the default role' option is selected with a blue radio button and a red circle containing the number '2'. The 'Choose an existing role' option is unselected with a radio button.

2. Choose the options as suggested in the guide below.

Warning: We recommend using tags to select assets, however if VMs are not tagged correctly then manual addition may be required.

After enabling AWS account add this service to your account from subscription panel in CloudOptics.

Assume role for Systems Manager

Use the default role ☒

Quick Setup creates a new assume role that enables Systems Manager to securely run commands on your instances.

3

Choose an existing role ☐

Uses an existing service role. The role must contain the required permissions policy. Choose the role from the following list

Quick Setup options

Quick Setup configures the following Systems Manager components based on best practices. Select the check boxes for actions you want to schedule. [Learn more](#)

- ☒ Update Systems Manager (SSM) Agent every two weeks
- ☒ Collect inventory from your instances every 30 minutes
- ☐ Scan instances for missing patches daily
- ☐ Install and configure the CloudWatch agent
- ☐ Update the CloudWatch agent once every 30 days

4

Learn more about the metrics included in [the CloudWatch agent's basic configuration](#) and [Amazon CloudWatch pricing](#).

Targets

Targets are the Amazon EC2 instances to manage with Systems Manager.

Target selection method

- ☒ Specify instance tags
- ☐ Choose instances manually

5

Tags

Enter a tag key

Enter a tag key

6

Enter a tag value

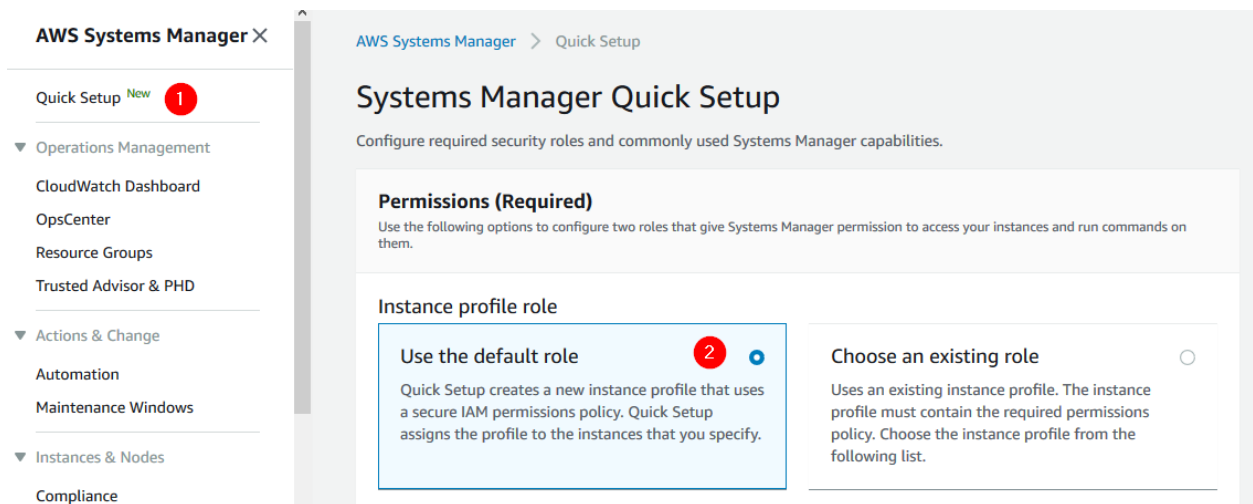
Infra Vulnerability Assessment (AWS Only)

Using CloudOptics, you could scan each of your AWS virtual machines and create an actionable report. Users of cloudOptics need to order suitable assessment to use this service.

This service is available only for AWS account right now.

This is one time activity. Follow these steps to enable your AWS account for onboarding into this service. These steps need to be repeated for each of the regions in use.

1. Open the “Systems Manager” service and go to quick setup.



2. Choose the options as suggested in the guide below.

Warning: We recommend using tags to select assets, however if VMs are not tagged correctly then manual addition may be required.

3. Go to CloudOpticsGroup and add following permission to the group

Assume role for Systems Manager

Use the default role ☒

Quick Setup creates a new assume role that enables Systems Manager to securely run commands on your instances.

3

Choose an existing role ☐

Uses an existing service role. The role must contain the required permissions policy. Choose the role from the following list

Quick Setup options

Quick Setup configures the following Systems Manager components based on best practices. Select the check boxes for actions you want to schedule. [Learn more](#)

- ☒ Update Systems Manager (SSM) Agent every two weeks
- ☒ Collect inventory from your instances every 30 minutes
- ☐ Scan instances for missing patches daily
- ☐ Install and configure the CloudWatch agent
- ☐ Update the CloudWatch agent once every 30 days

4

Learn more about the metrics included in [the CloudWatch agent's basic configuration](#) and [Amazon CloudWatch pricing](#).

Targets

Targets are the Amazon EC2 instances to manage with Systems Manager.

Target selection method

- ☒ Specify instance tags
- ☐ Choose instances manually

5

Tags

Enter a tag key


6

- AmazonInspectorFullAccess

Post addition group should like below.

[IAM](#) > [Groups](#) > **CloudOpticsGroup**

▼ Summary

Group ARN: arn:aws:iam::[redacted]:group/CloudOpticsGroup 

Users (in this group): 1

Path: /

Creation Time: 2018-05-13 11:27 UTC+0530

Users




Permissions

Access Advisor

Managed Policies

The following managed policies are attached to this group. You can attach up to 10 managed policies.

[Attach Policy](#)

Policy Name	Actions
 AmazonInspectorFullAccess	Show Policy Detach Policy Simulate Policy
 ReadOnlyAccess	Show Policy Detach Policy Simulate Policy
 AWSCloudTrailReadOnlyAccess	Show Policy Detach Policy Simulate Policy

After enabling AWS account go to Advisory Assessment panel in CloudOptics and order the scan.