

## Table of Contents

Document Changelog	1
1. Introduction	2
2. Amazon Web Services	3
2.1. Obtain the Endpoint Protector AMI	3
2.2. Launch the EC2 image	4
2.2.1. Request an Elastic IP	9
2.2.2. Secure your Instance	11
3. Google Cloud Platform	12
3.1. Obtain the Endpoint Protector GCP image	12
3.2. Download the image	12
3.3. Create a bucket	12
3.4. Import the image to the custom image list	14
3.5. Create an Endpoint Protector VM Instance	15
3.6. Request a Static IP	16
3.7. Create Firewall rules	17
4. Azure	19
4.1. Obtain the Endpoint Protector Azure VM	19
4.2. Create the Storage Account and Container	19
4.3. Create the disk	22
4.4. Create the Virtual Machine	24
5. Endpoint Protector Licensing	27
6. Disclaimer	28

# 1. Introduction

This User Manual is intended to provide short guidance when using the Endpoint Protector Server in Amazon Web Services or Google Cloud Platform.

**Important:** This document is not intended as a step-by-step guide to creating an AWS or GCP account. The precondition to already having such accounts in place and understanding the bases of how these 3rd party services are the responsibility of each Administrator.

- **Amazon Web Services** - the Endpoint Protector AMI is provided as an Amazon EC2 instance
- **Google Cloud Platform** - the Endpoint Protector image is provided as a \*.tar.gz.
- **Azure** - the Endpoint Protector image will be uploaded into your account.

**Note:** For information related to the use of Endpoint Protector – main components, features, and functionality, please refer to the [Endpoint Protector User Manual](#).

## 2. Amazon Web Services

### 2.1. Obtain the Endpoint Protector AMI

Endpoint Protector is not generally available in the AWS Marketplace. To have access to the Amazon Machine Image (AMI), you need to contact your Endpoint Protector Representative directly or submit a request on our [website](#) by providing information such as the AWS Account no. and Region and Availability Zone.

You will receive a reply from an Endpoint Protector Representative, notifying you when the Endpoint Protector Amazon Machine Image has been shared with your account.

#### A. Cloud Service



Endpoint Protector can be deployed using various cloud service providers such as Amazon Web Services (AWS), Microsoft Azure or Google Cloud Platform (GCP).

**Note:** Having a cloud account (e.g.: AWS, GCP) and understanding how these third-party services work is the responsibility of each company's Administrator.

For more details, please read the [Cloud Service User Manual](#).

#### Request a server

Select your Cloud Service environment

- ☒ Amazon Web Services (AWS)  
☐ Google Cloud Platform (GCP)  
☐ Microsoft Azure

First Name\*

Last Name\*

Work Email\*

Work Phone Number\*

AWS Account Number

Region and availability zone

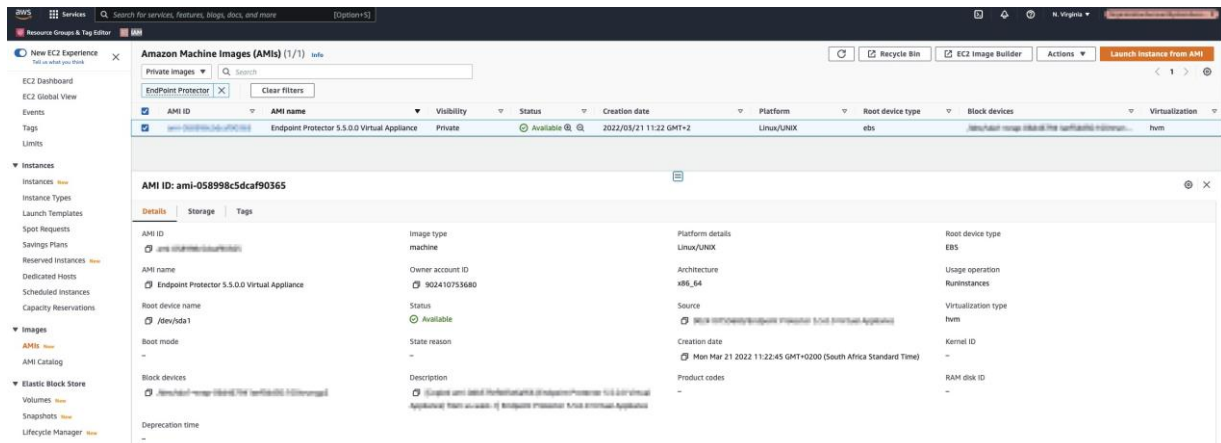
**Request Server**

## 2.2. Launch the EC2 image

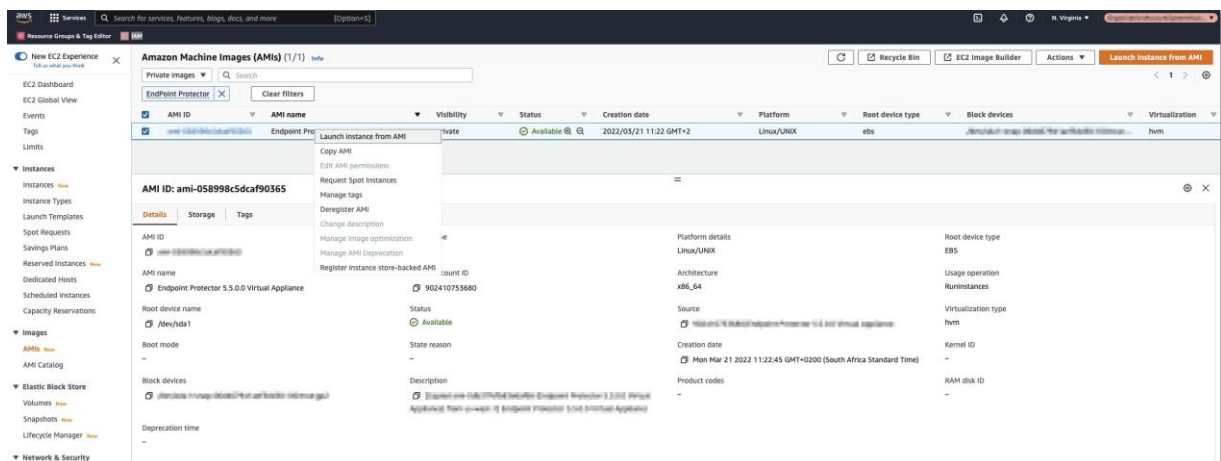
As the Endpoint Protector image has already been shared with you, this process is similar to any other EC2 launch.

To launch the EC2 image, follow these steps:

1. Go to **Services: EC2** and select your **region**
2. Go to **Images: AMIs** and select the type of the Private image and search for **Endpoint Protector**



3. Right-click and select **Launch Instance**



4. Enter the **Name** and **Create tags** as per your policies;
5. Select an **Instance Type**;

**Note:** For help in selecting the instance type that best fits your needs, contact [support@endpointprotector.com](mailto:support@endpointprotector.com).

6. Select an available **key pair** or create a **new key pair**;

If you select to use a key pair you might have to share it with our Support Team for support requests. In this case, ensure it is used only for this instance. We would recommend selecting the option **Proceed without a Key Pair** and then click **Launch Instances**.

aws

Services

Search for services, features, blogs, docs, and more

[Option+S]

Resource Groups & Tag Editor

IAM

You've been opted into the new launch experience. [Find out more](#) about this experience or [send us feedback](#). You can still return to the previous version by opting-out.

EC2 > Instances > Launch an instance

Launch an instance

Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Info

Name

My\_Epp\_Appliance

Add additional tags

Application and OS Images (Amazon Machine Image)

Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

AMI from catalog

Recents

My AMIs

Quick Start

Amazon Machine Image (AMI)

Endpoint Protector 5.5.0.0 Virtual Appliance

ami-058998c5dcaf90365

Published

Architecture

Virtualization

Root device type

ENA Enabled

2022-03-21T09:22:45.000Z

x86\_64

hvm

ebs

Yes

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Instance type

Info

Instance type

t2.medium

Family: t2 2 vCPU 4 GiB Memory

On-Demand Linux pricing: 0.0464 USD per Hour

On-Demand Windows pricing: 0.0644 USD per Hour

Compare instance types

Key pair (login)

Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

Proceed without a key pair (Not recommended)

Default value

Create new key pair

Summary

Number of Instances

1

Software Image (AMI)

[Copied ami-0db37fefb83e6af66 ...read more]

ami-058998c5dcaf90365

Virtual server type (instance type)

t2.medium

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 100 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet

Cancel

Launch Instance

5 | Endpoint Protector | Cloud Services User Manual

7. Configure the **Network** section:

▼ **Network settings**

Edit

Network

Subnet

Auto-assign public IP

Enable

Security groups (Firewall) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

We'll create a new security group called 'launch-wizard-7' with the following rules:

☒ Allow SSH traffic from

Helps you connect to your instance

Anywhere  
0.0.0.0/0

☐ Allow HTTPs traffic from the internet

To set up an endpoint, for example when creating a web server

☐ Allow HTTP traffic from the internet

To set up an endpoint, for example when creating a web server

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

8. Edit Network Section and provide the following information:

- Select a **VPC** and a **Subnet**
- Enable the **Auto-assign public IP**
- Select **Create security group** and then provide a **name** and **description**
- **Remove** the existing Inbound rules
- **Add two new Inbound security group rules:**
  - Type **HTTPS**, Protocol **TCP**, Port range **443**, Source type **Custom**, Source 0.0.0.0/0 (**mandatory**)
  - Type **HTTP**, Protocol **TCP**, Port range **80**, Source type **Custom**, Source 0.0.0.0/0 (**optional**)

## ▼ Network settings

### VPC - *required* [Info](#)

ap-south-1

(default) ▼



### Subnet [Info](#)

my-subnet

▼

[Create new subnet](#)

### Auto-assign public IP [Info](#)

Enable

▼

### Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group☐ Select existing security group

### Security group name - *required*

My EPP Appliance

▼

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and .\_-:/()#,@[]+=&:{}!\$\*

### Description - *required* [Info](#)

My EPP Security Group

▼

### Inbound security groups rules

#### ▼ Security group rule 1 (TCP, 443, 0.0.0.0/0, HTTPS)

[Remove](#)

##### Type [Info](#)

HTTPS

▼

##### Protocol [Info](#)

TCP

▼

##### Port range [Info](#)

443

▼

##### Source type [Info](#)

Custom

▼

##### Source [Info](#)

Q Add CIDR, prefix list or security group

0.0.0.0/0 X

##### Description - *optional* [Info](#)

HTTPS

▼

#### ▼ Security group rule 2 (TCP, 80, 0.0.0.0/0, HTTP)

[Remove](#)

##### Type [Info](#)

HTTP

▼

##### Protocol [Info](#)

TCP

▼

##### Port range [Info](#)

80

▼

##### Source type [Info](#)

Custom

▼

##### Source [Info](#)

Q Add CIDR, prefix list or security group

0.0.0.0/0 X

##### Description - *optional* [Info](#)

HTTP

▼

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

[Add security group rule](#)



9. The **Storage** section does not require any changes;

▼ **Configure storage** [Info](#) Advanced

1x 100 GiB gp2 ▼ Root volume

[i](#) Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage [×](#)

[Add new volume](#)

0 x File systems Edit

10. On the **Summary** section click **Launch Instance**;

▼ **Summary**

Number of instances [Info](#)

1

Software Image (AMI)

[Amazon Linux 2 AMI \(HVM\) ...read more](#)

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

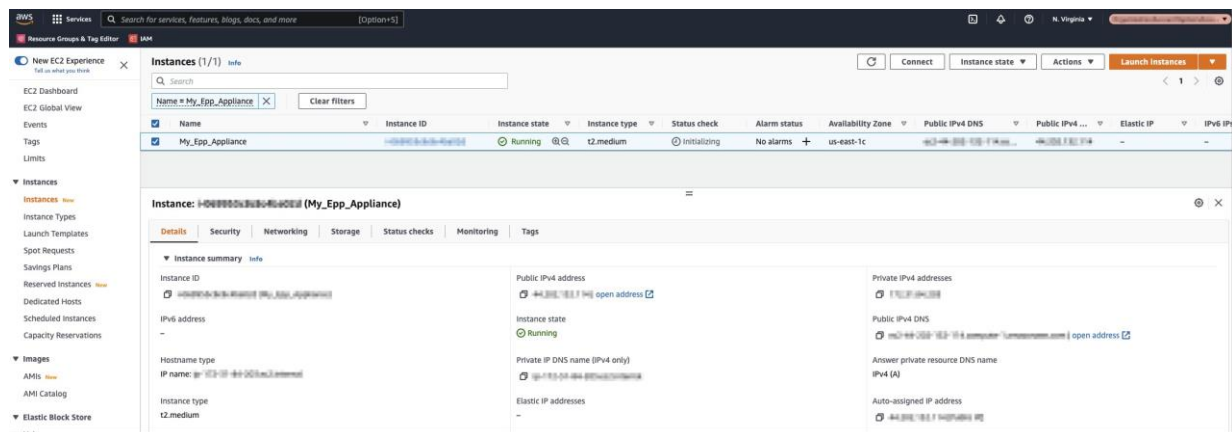
1 volume(s) - 100 GiB

[i](#) **Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet [×](#)

[Cancel](#) [Launch Instance](#)

11. Wait for the instance to start - this might take a few minutes while the **Status Checks** appear as **Initializing**.

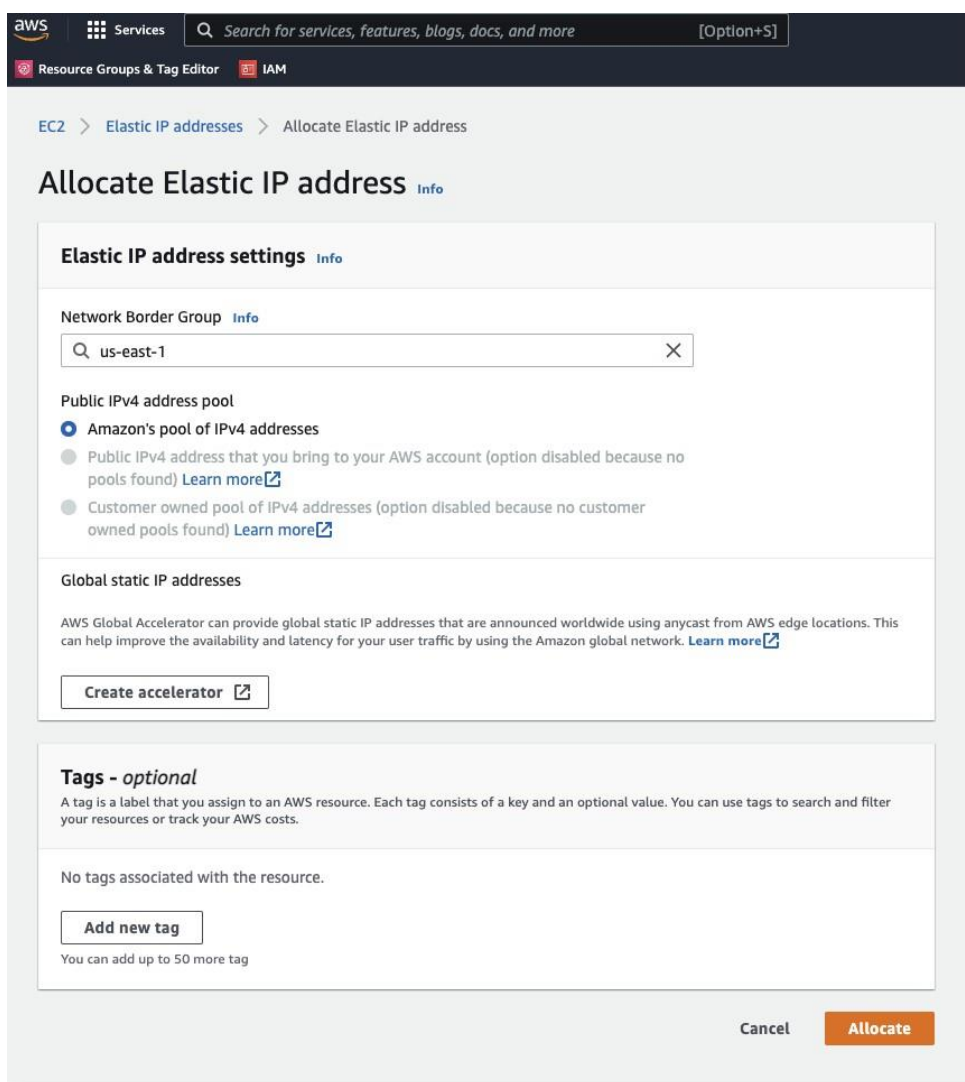




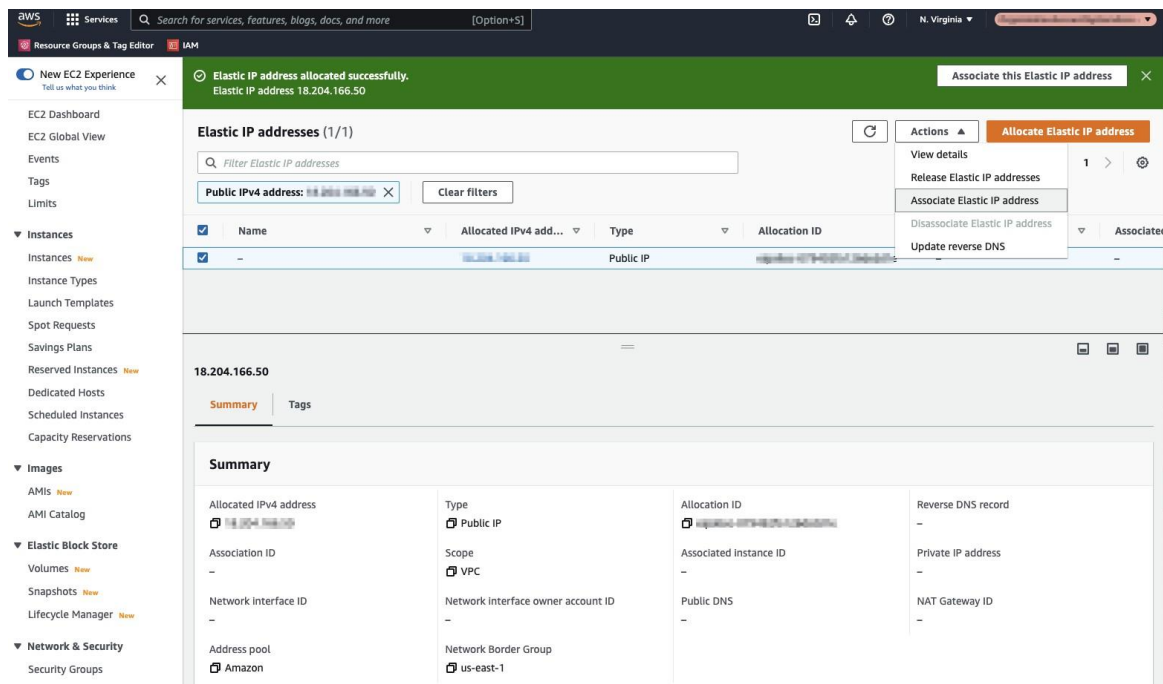
### 2.2.1. Request an Elastic IP

This step is required so the Endpoint Protector Clients can communicate with the same IP Address in case of an instance restart. Without an Elastic IP (Static IP) the instance will assign a new IP address every time it is restarted and the Endpoint Protector Clients have to be reinstalled.

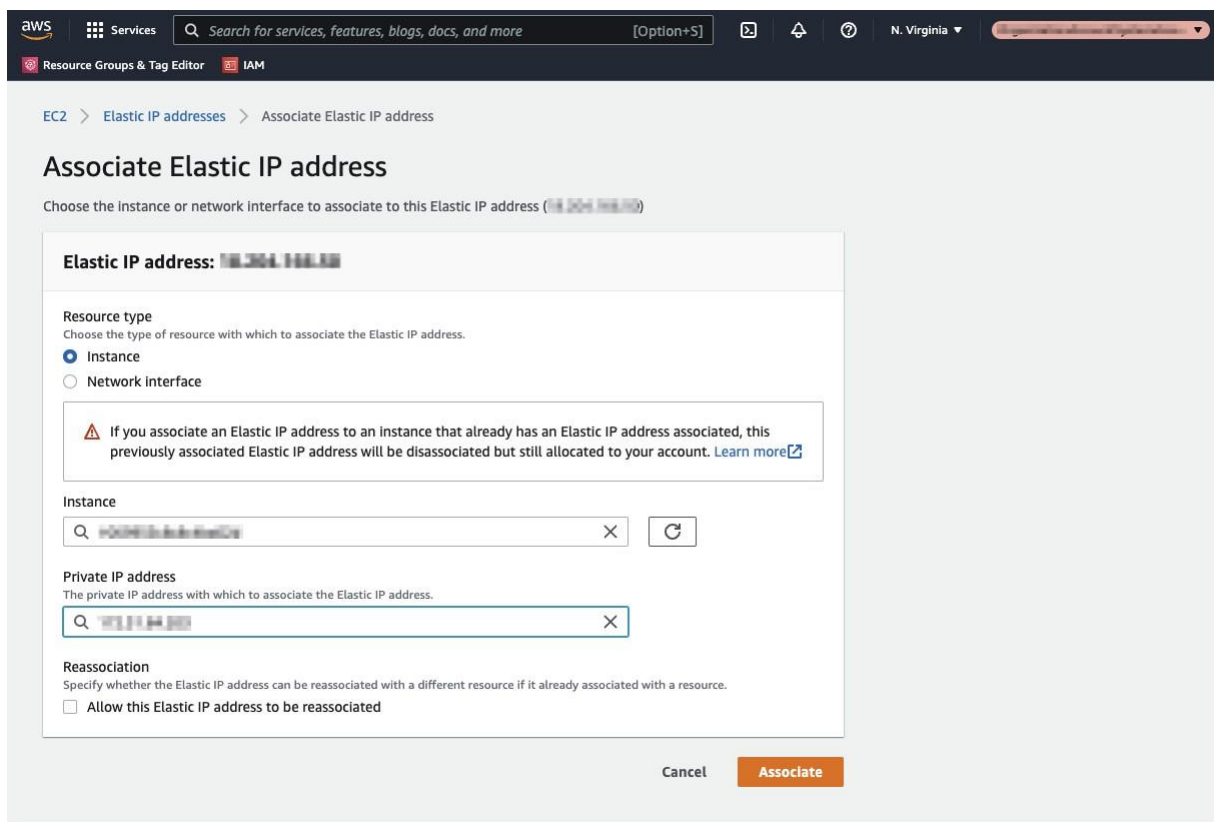
To request an Elastic IP, go in the AWS Management Console to the option **Network & Security, Elastic IPs**, and click **Allocate New Address**.



1. Associate the **Elastic IP** with your Endpoint Protector Instance.



2. Select the **Endpoint Protector Instance** from the dropdown list, the **Private IP address**, and then click **Associate**;



The Elastic IP is now associated with your Endpoint Protector Instance. After a few minutes, the Endpoint Protector Instance will be running associated with the Elastic IP.

---

### 2.2.2. Secure your Instance

We recommend further securing your Instance by making all possible settings in the AWSInterface under the option **Security Groups**.

# 3. Google Cloud Platform

## 3.1. Obtain the Endpoint Protector GCP image

Endpoint Protector is not available from the default images on the Google Cloud Platform. To obtain it, you will need to follow the process hereby described.

**Note:** This part of the process is similar to uploading any other custom image in the Console.

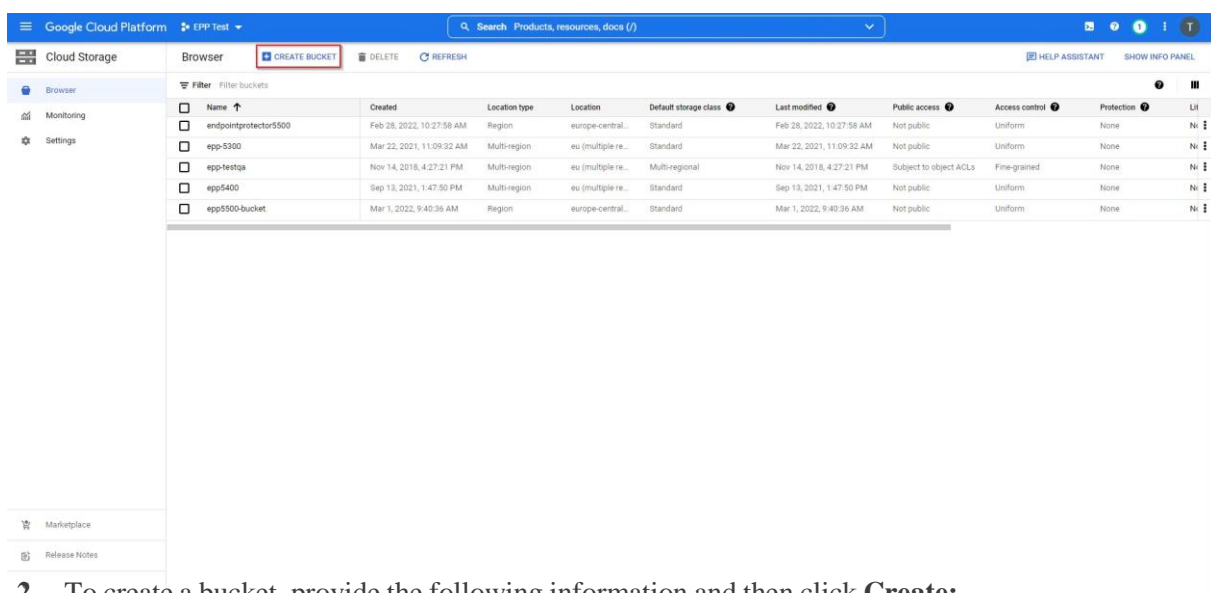
## 3.2. Download the image

The Endpoint Protector image can be downloaded from the link provided by your Endpoint Protector Representative. If this image has already been obtained, you can skip this step.

## 3.3. Create a bucket

To upload the Endpoint Protector image to the Google Cloud Platform, create a bucket:

1. On the Google Cloud Platform Console, go to the [Cloud Storage Browser page](#) and click **Create bucket**;



2. To create a bucket, provide the following information and then click **Create**:

- **Name** – add a name for the bucket

- **Storage** – select the **standard** storage class
- **Location** – select a location to store the image

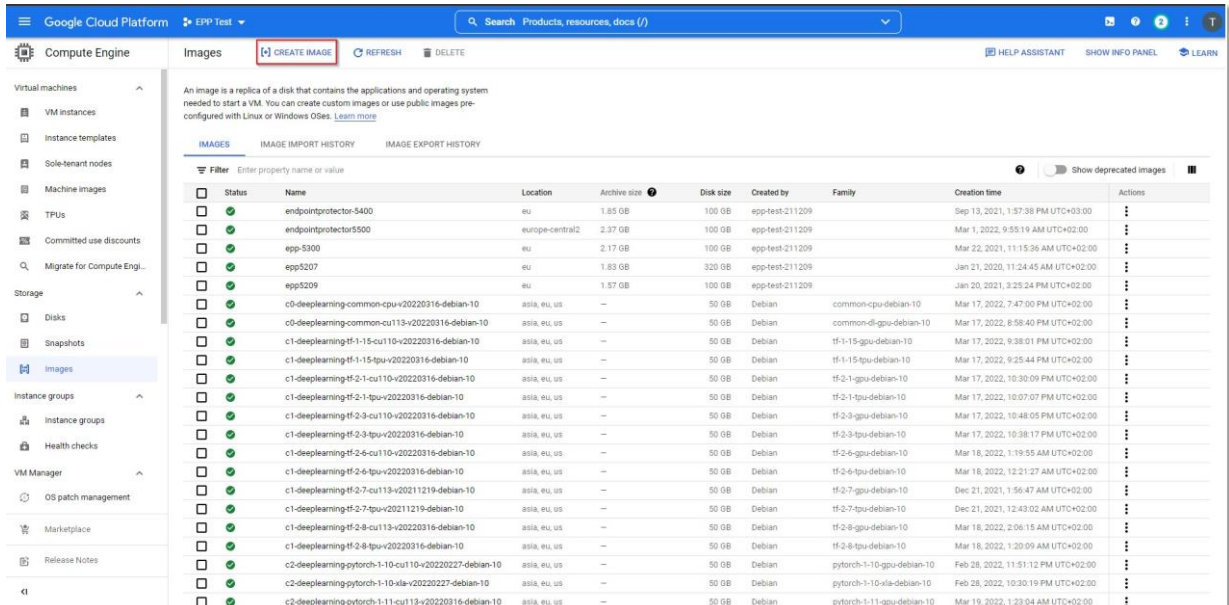
3. On the newly created **Bucket details** page, click **Upload files** and select the Endpoint Protector image file [received from Endpoint Protector](#).

**Note:** Depending on the size of the compressed image and the speed of the network connection, the upload can take several hours.

### 3.4. Import the image to the custom image list

After the Endpoint Protector image has been uploaded to Google Cloud Storage, import the custom image list.

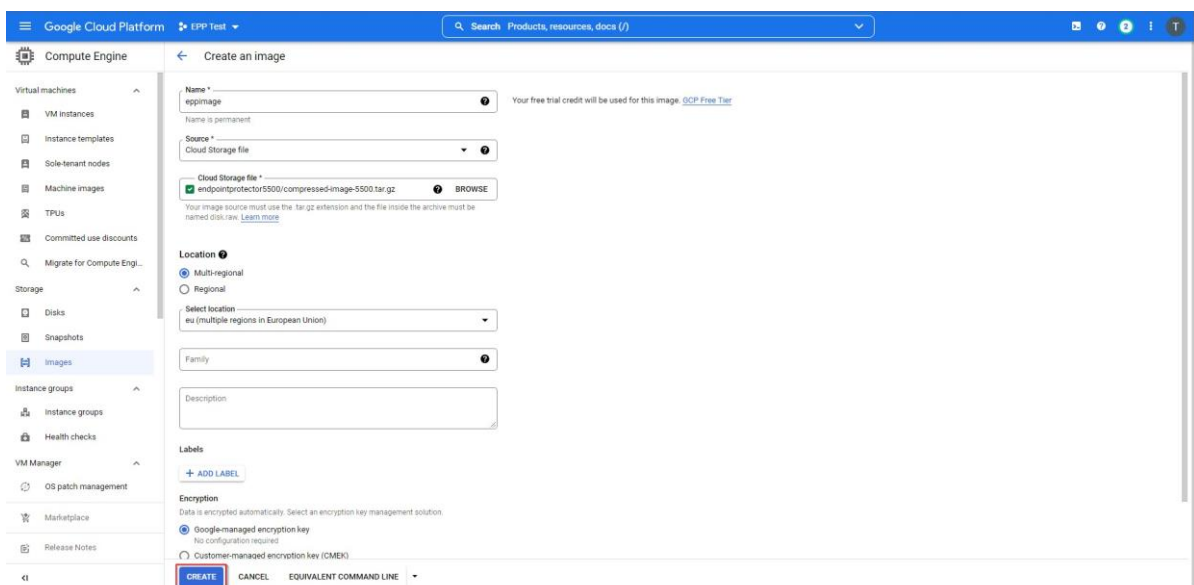
1. On the Google Cloud Platform Console, go to the **Image** page and click **Create image**;



2. To create the image, provide the following information and then click **Create**:

- **Name** – add a name for the image
- **Source** – select **Cloud Storage file**
- **Cloud Storage file** – upload the Endpoint Protector image file
- **Location** – select **Multi-regional**
- **Encryption** – select **Google-managed encryption key**

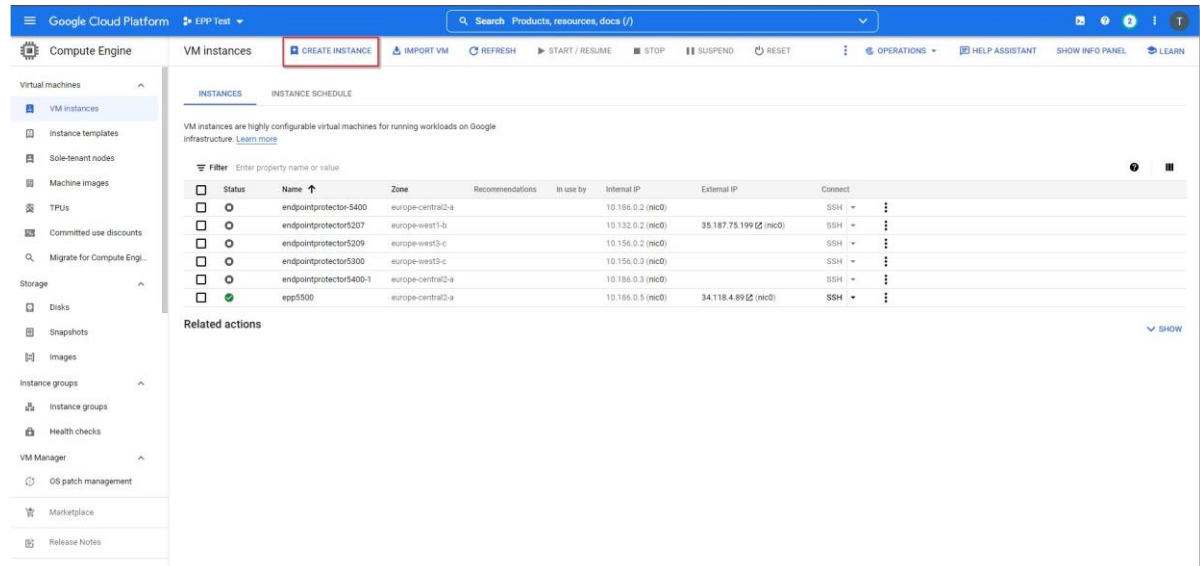
**Note:** The process can take several minutes depending on the size of the boot disk image.



### 3.5. Create an Endpoint Protector VM Instance

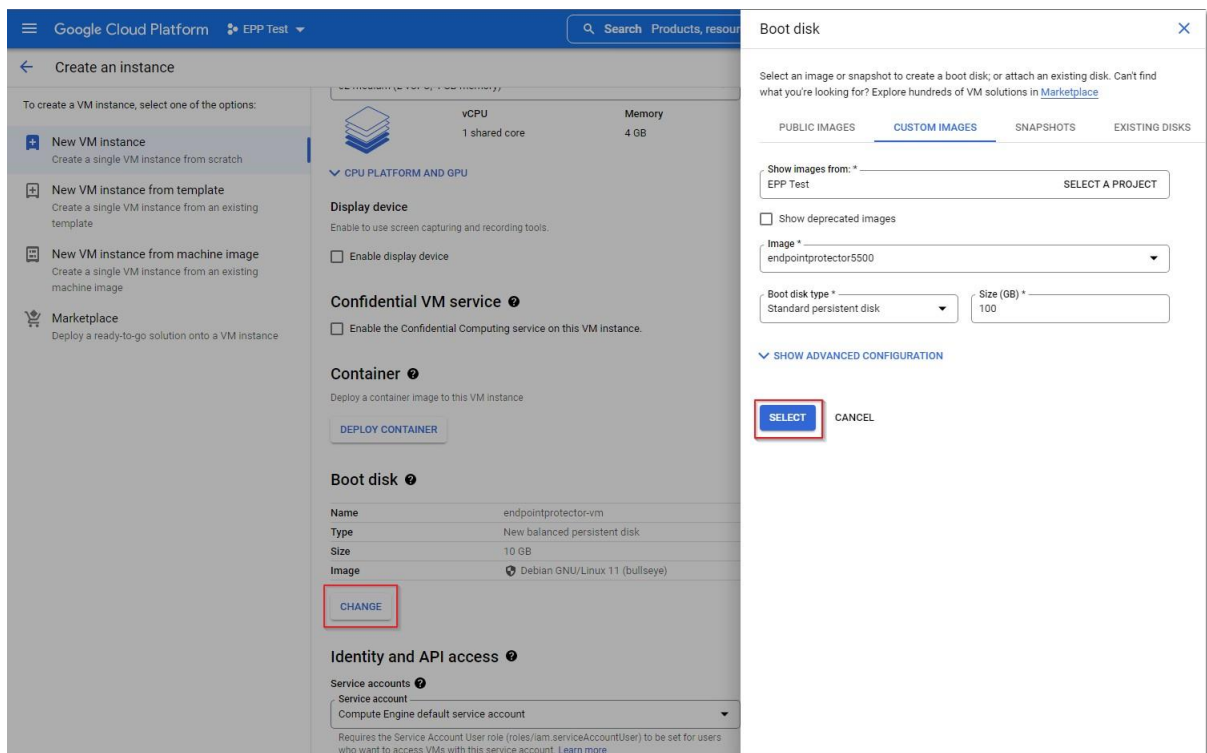
After the Endpoint Protector Image is available in the Google Cloud Platform images list, create a Virtual Machine Instance:

1. In the **Google Cloud Platform Console**, go to the **VM Instances** page and click **Create instance**;

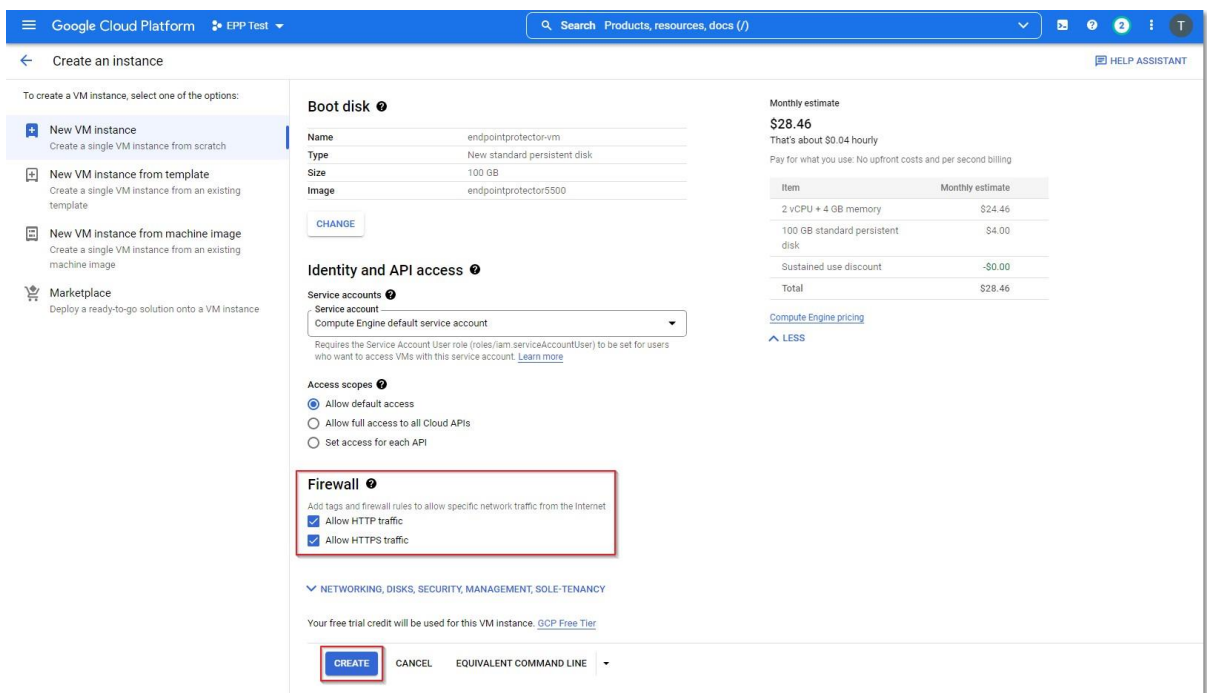


2. In the **Boot disk** section, click **Change** to begin configuring your boot disk and on the **Custom Images** tab, fill in the following:
  - **Image** - select the image you imported
  - **Boot disk type** - select **Standard persistent disk**
  - **Size** – add a size larger than the Endpoint Protector image size receivedClick **Select** to confirm the boot disk configuration.





- On the **Firewall** section, select **Allow HTTP traffic** and **Allow HTTPS traffic**, and then click **Create**.

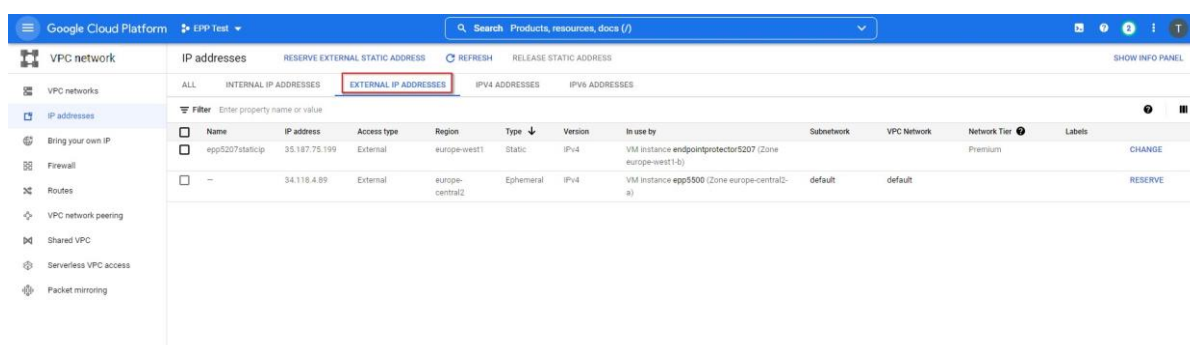


### 3.6. Request a Static IP

You will need to request a static IP so the Endpoint Protector Clients can communicate with the same IP Address in case of an instance restart.

Without a Static IP (Elastic IP) the instance will assign a new IP address every time it is restarted and the Endpoint Protector Clients have to be reinstalled.

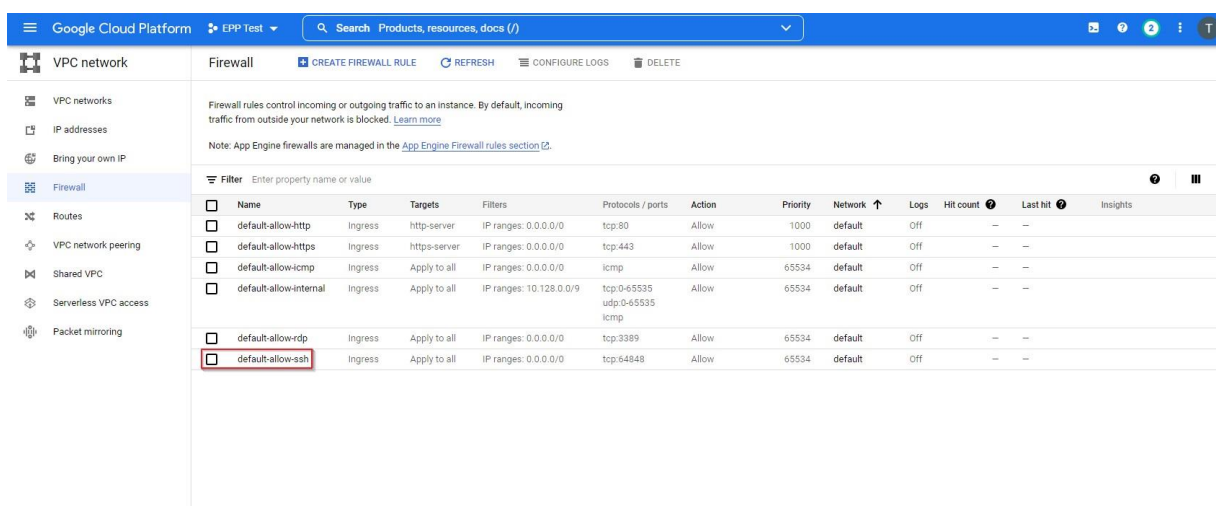
To request a Static IP, go to **IP addresses** and select the **External IP addresses** tab.



### 3.7. Create Firewall rules

To create a Firewall rule, on the Google Cloud Platform Console, follow these steps:

1. Go to the **Firewall** page and select **default-allow-ssh**;



2. Click **Edit** and on the **Protocols and ports** section provide the following information:

- select **Specified protocols and ports**
- check the **tcp** box and enter **64848**

Google Cloud Platform

EPP Test

Search Products, resources, docs (/)

2

T

VPC network

Firewall rule details

EDIT

DELETE

VPC networks

IP addresses

Bring your own IP

Firewall

Routes

VPC network peering

Shared VPC

Serverless VPC access

Packet mirroring

default-allow-ssh

Description

Allow SSH from anywhere

Logs

Turning on firewall logs can generate a large number of logs which can increase costs in Cloud Logging. [Learn more](#)

On

Off

Network

default

Priority \*

65534

CHECK PRIORITY OF OTHER FIREWALL RULES ?

Priority can be 0 - 65535

Direction

Ingress

Action on match

Allow

Targets

All instances in the network

Source filter

IPv4 ranges

Source IPv4 ranges \*

0.0.0.0/0 for example: 0.0.0.0/0, 192.168.2.0/24

Second source filter

None

Protocols and ports ?

Allow all

Specified protocols and ports

tcp

64848

udp

all

Other protocols

protocols, comma separated, e.g. ah, sctp

# 4. Azure

## 4.1. Obtain the Endpoint Protector Azure VM

Endpoint Protector is not generally available in the Azure Marketplace. To have access to the Virtual Machine, contact your Endpoint Protector Representative and provide information such as the access keys to a Container specifically created for the Endpoint Protector Virtual Machine.

**Note:** We will upload the Endpoint Protector Virtual Machine to your Container as soon as possible. Once this step is done, we advise regenerating the access key.

## 4.2. Create the Storage Account and Container

This part of the process is similar to creating any other Storage Account and Container on Azure. If you are already familiar with it or have created a dedicated Container already, proceed to the next step.

To obtain the Azure Endpoint Protector Virtual Machine, you need to create a dedicated Storage account / Container, following these steps:

1. Open the [Azure portal](#);
2. Go to **Storage accounts** and click **+Create**;
3. To **create a storage account**, provide the following information:
  - **Subscription** – select **Pay-As-You-Go**
  - **Resource group** – select a group from the available list or create a new one
  - **Storage account name** – add a name for the storage account
  - **Region** – select the nearest the location of the computers that will be protected by Endpoint Protector
  - **Performance** – select **Standard** performance
  - **Redundancy** – select **Locally-redundant storage (LRS)**
4. Click **Review + create**;

Microsoft Azure

Search resources, services, and docs (G+)

Home > Storage accounts >

## Create a storage account

Basics | Advanced | Networking | Data protection | Encryption | Tags | Review + create

**Project details**

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription \*

Resource group \*  [Create new](#)

**Instance details**

If you need to create a legacy storage account type, please click [here](#).

Storage account name \*

Region \*

Performance \* ☒ Standard: Recommended for most scenarios (general-purpose v2 account)  
☐ Premium: Recommended for scenarios that require low latency.

Redundancy \*

[Review + create](#) [< Previous](#) [Next : Advanced >](#)

- Go to **Storage accounts** and click the newly created account;
- Go to **Containers** and click **+Container**;
- Give the container the same name as you did to the storage account and for the **Publicaccess level** select **Container (anonymous read access for containers and blobs)**;

Microsoft Azure

Search resources, services, and docs (G+)

Home > eppcososys\_165253824932 >

**eppcososys**  
Storage account

Upload | Open in Explorer | Delete | Move | Refresh | Mobile | Feedback

Overview

Activity log

Tags

Diagnose and solve problems

Access Control (IAM)

Data migration

Events

Storage browser (preview)

**Data storage**

Containers

File shares

Queues

Tables

**Security + networking**

Networking

Azure CDN

Access keys

Shared access signature

Encryption

Security

**Data management**

Geo-replication

Data protection

**Essentials**

Resource group (movie) : EndpointProtectorRG

Location : West Europe

Subscription (movie) : Pay-As-You-Go

Subscription ID : 300ced05-744f-4c0e-8d2a-da3fb6ac34f3

Disk state : Available

Tags (add) : Click here to add tags

Performance : Standard

Replication : Locally-redundant storage (LRS)

Account kind : StorageV2 (general purpose v2)

Provisioning state : Succeeded

Created : 5/11/2022, 10:23:51 AM

**Properties** | Monitoring | Capabilities (7) | Recommendations | Tutorials | Developer Tools

**Blob service**

Hierarchical namespace	Disabled
Default access tier	Hot
Blob public access	Enabled
Blob soft delete	Enabled (7 days)
Container soft delete	Enabled (7 days)
Versioning	Disabled
Change feed	Disabled
NFS v3	Disabled
Allow cross-tenant replication	Enabled

**File service**

Large file share	Disabled
Active Directory	Not configured
Soft delete	Enabled (7 days)
Share capacity	5 TiB

**Queue service**

**Security**

Require secure transfer for REST API operations	Enabled
Storage account key access	Enabled
Minimum TLS version	Version 1.2
Infrastructure encryption	Disabled

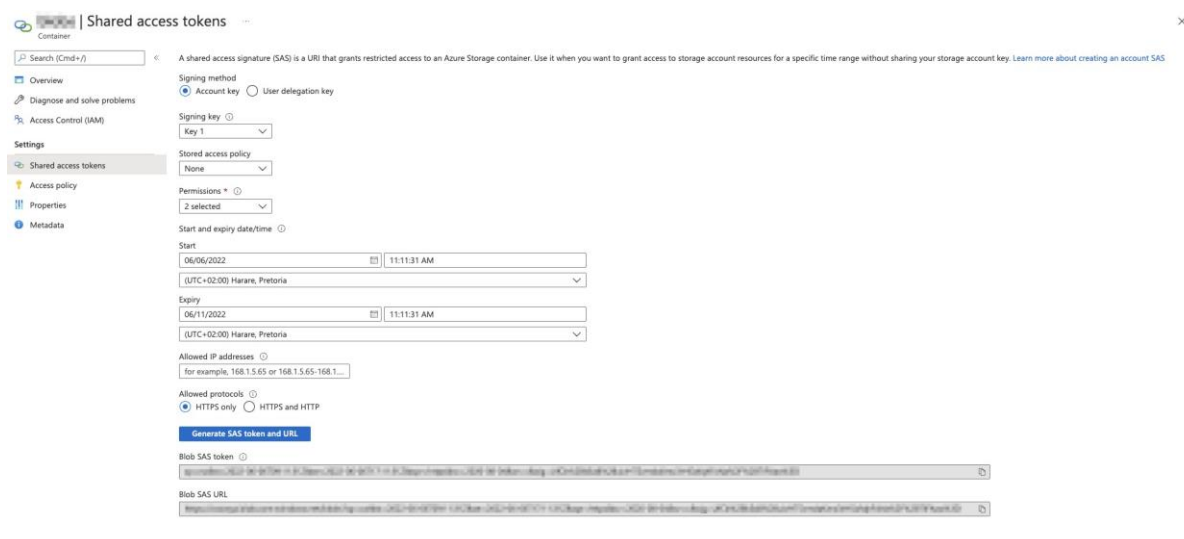
**Networking**

Allow access from	All networks
Number of private endpoint connections	0
Network routing	Microsoft network routing
Access for trusted Microsoft services	Yes
Endpoint type	Standard

7. Select the container you created, and then click **Shared access tokens**.

**Important: Make sure you are creating a token on the container level, not the storageaccount!**

8. Configure the **SAS token** with **Create, Write and Add Permissions** with a **5-day** window to allow the CoSoSys team to copy the image;



The screenshot shows the 'Shared access tokens' configuration page in the Azure Portal. The left sidebar includes a search bar and navigation links for Overview, Diagnose and solve problems, Access Control (IAM), Settings, Shared access tokens (selected), Access policy, Properties, and Metadata. The main content area contains the following fields:

- Signing method:** ☒ Account key, ☐ User delegation key
- Signing key:** Key 1 (dropdown)
- Stored access policy:** None (dropdown)
- Permissions:** 2 selected (dropdown)
- Start and expiry date/time:** Start: 06/06/2022 11:11:31 AM (UTC+02:00) Harare, Pretoria; Expiry: 06/11/2022 11:11:31 AM (UTC+02:00) Harare, Pretoria
- Allowed IP addresses:** for example, 168.1.5.65 or 168.1.5.65-168.1...
- Allowed protocols:** ☒ HTTPS only, ☐ HTTPS and HTTP
- Generate SAS token and URL:** (button)
- Blob SAS token:** (text field with a copy icon)
- Blob SAS URL:** (text field with a copy icon)

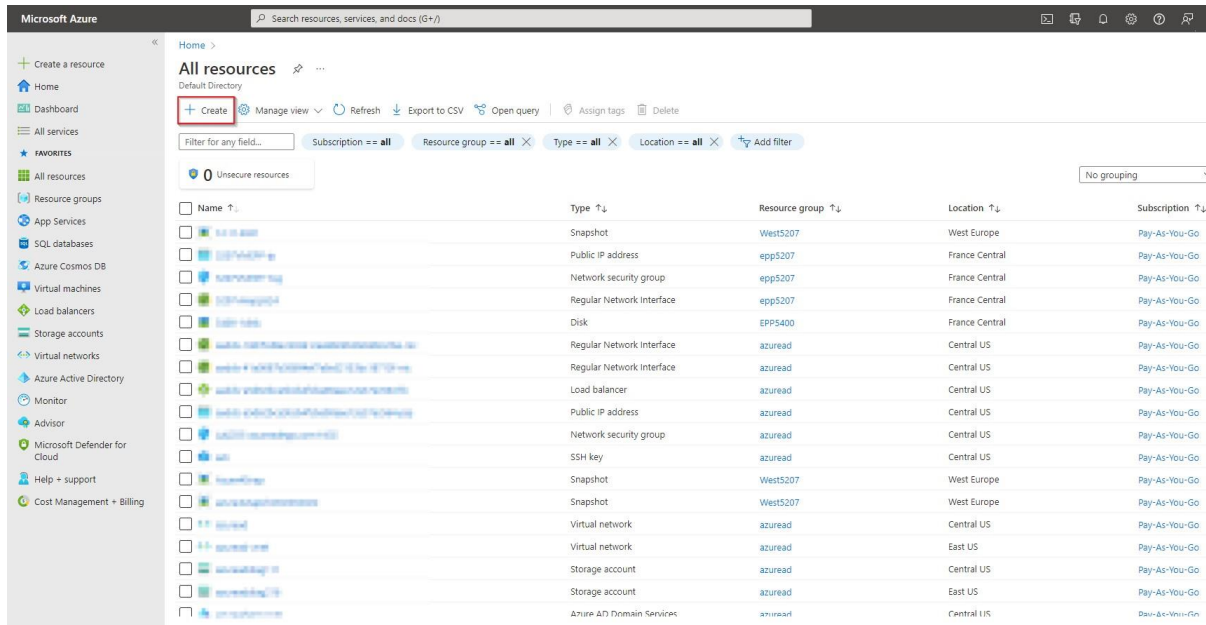
9. Copy the **Blob SAS URL** and send it to CoSoSys.

**Note:** CoSoSys will copy the Endpoint Protector Virtual Machine to your storage account and notify you when the process is over.

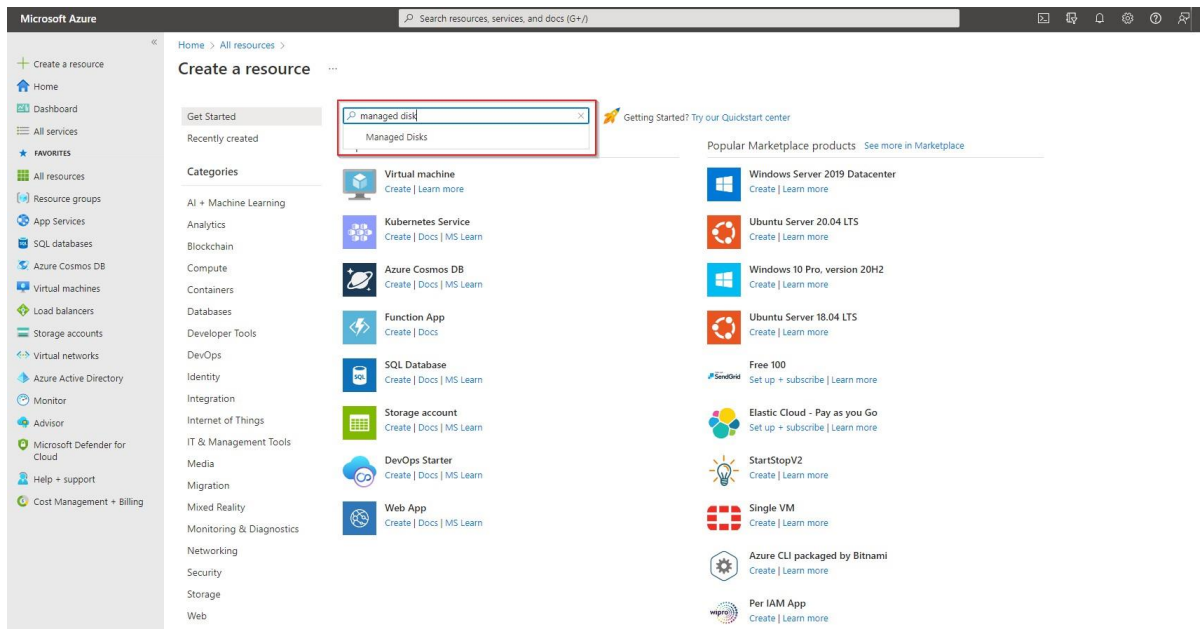
## 4.3. Create the disk

Before starting the Endpoint Protector Virtual Machine, you have to prepare a disk and a Virtual Machine. To create a disk, follow these steps.

1. From the top right side of the page, go to **All resources** and click **+Create**;

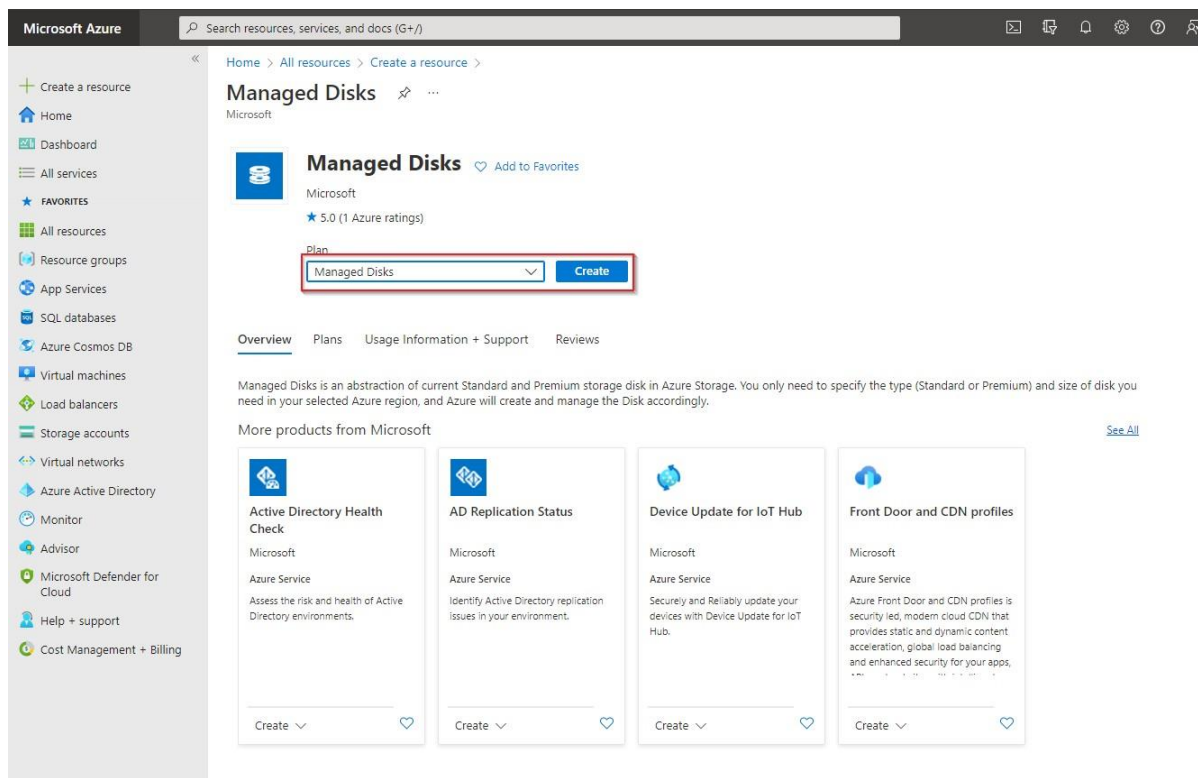


2. Search the marketplace for **Managed Disks**;



3. Go to **Managed Disks** and select **Create**;





4. To create a managed disk, provide the following information

- **Subscription** - select **Pay-As-You-Go**
- **Resource group** – select the previously created one
- **Disk name** – add a name for the storage account
- **Region** – select the nearest the location of the computers that will be protected by Endpoint Protector
- **Availability Zone**
- **Source type** - select **Storage Blob**
- **Source subscription** - select **Pay-As-You-Go**
- **Source blob** – enter the URL received from CoSoSys after providing the key and URL mentioned above.
- **OS type** - select **Linux**
- **Security type** – select **Standard**
- **VM generation** – select **Generation 1**
- **Size** - select **128 GB**

5. Click **Review + Create** and wait for the **Successfully created disk** message to be displayed.

Microsoft Azure

Search resources, services, and docs (G+)

Home > All resources > Create a resource > Managed Disks >

## Create a managed disk

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* ⓘ Pay-As-You-Go

Resource group \* ⓘ EndpointProtectorRG  
[Create new](#)

**Disk details**

Disk name \* ⓘ eppdisk

Region \* ⓘ (Europe) West Europe

Availability zone None

Source type ⓘ Storage blob

Source subscription ⓘ Pay-As-You-Go

Source blob \* ⓘ https://west5207storage.blob.core.windows.net/west5207storage/epp5207-25...  
[Browse](#)

OS type ⓘ  
☐ None (data disk)  
☒ Linux  
☐ Windows

Security type ⓘ Standard

VM generation ⓘ  
☒ Generation 1  
☐ Generation 2

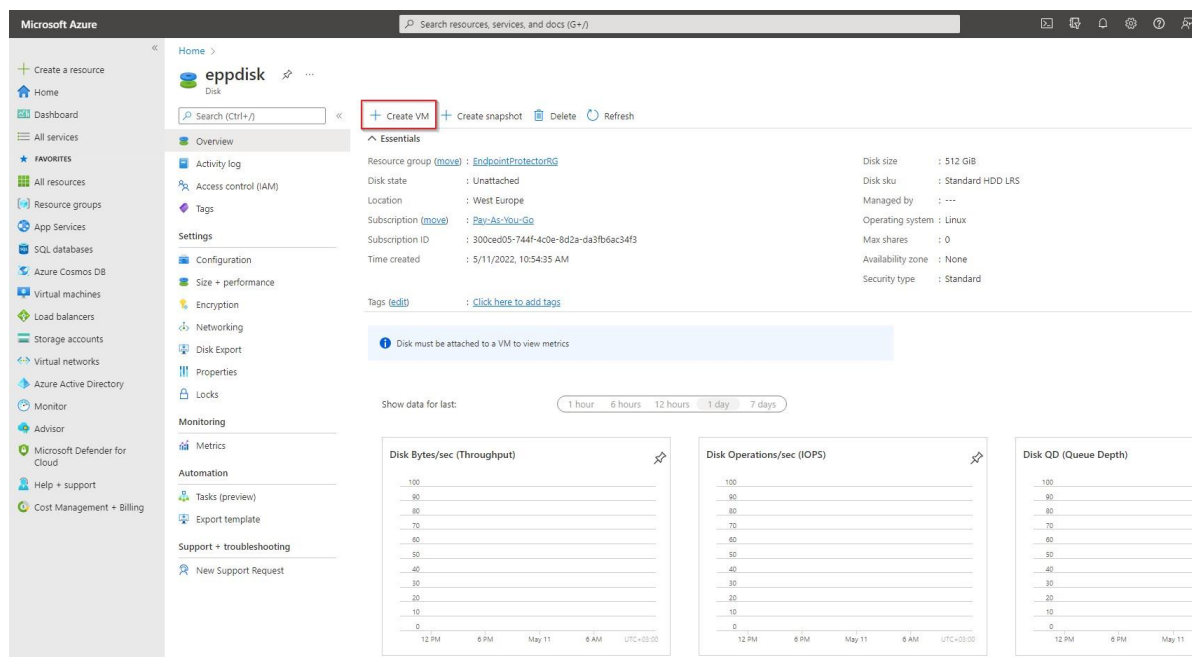
Size \* ⓘ 512 GiB  
Standard HDD LRS  
[Change size](#)

[Review + create](#) [< Previous](#) [Next : Encryption >](#)

## 4.4. Create the Virtual Machine

To start the Endpoint Protector Virtual Machine in Azure, follow these steps:

1. Go to the **All resources** page, select the newly created disks and then click **Create VM**



2. To create the Virtual Machine, provide the following information: On

the **Basics** tab, fill in the following:

- **Subscription** – select **Pay-As-You-Go**
- **Resource group** – select the group used when creating the disk
- **Virtual Machine Name** – enter a name for the Virtual Machine
- **Size** - select a virtual machine profile based closest to the recommended requirements for the disk file used

The screenshot shows the 'Create a virtual machine' page in the Microsoft Azure portal, specifically the 'Basics' tab. The left sidebar contains navigation links for various Azure services. The main content area has a breadcrumb 'Home > eppdisk >' and a title 'Create a virtual machine'. A warning message states: 'Changing Basic options may reset selections you have made. Review all options prior to creating the virtual machine.' Below this, there are tabs for 'Basics', 'Disks', 'Networking', 'Management', 'Advanced', 'Tags', and 'Review + create'. The 'Basics' tab is active, showing 'Project details' and 'Instance details' sections. In the 'Project details' section, 'Subscription' is set to 'Pay-As-You-Go' and 'Resource group' is set to 'EndpointProtectorRG'. In the 'Instance details' section, 'Virtual machine name' is 'EndpointProtector', 'Region' is '(Europe) West Europe', 'Availability options' is 'No infrastructure redundancy required', 'Security type' is 'Standard', 'Image' is 'eppdisk - Gen1', 'Azure Spot instance' is unchecked, and 'Size' is 'Standard\_B2s - 2 vcpus, 4 GiB memory (\$35.04/month)'. There are links for 'See all images' and 'Configure VM generation' near the image selection, and 'See all sizes' near the size selection.

On the **Networking** tab, fill in the following:

- **Public IP** - click **Create new** and select **Basic SKU** and **Static Assignment**.
- **Select inbound ports** – add **HTTP (80)** and **HTTPS (443)**

Click **Review + create** and then **Create**.

**Note:** For Additional Features, we recommend selecting **HDD** instead of **SSD** to avoid unnecessary payments for an unused **SSD** attached to the Virtual Machine.

**Create a virtual machine**

Basics Disks **Networking** Management Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

**Network interface**

When creating a virtual machine, a network interface will be created for you.

Virtual network \* (new) EndpointProtectorRG-vnet [Create new](#)

Subnet \* (new) default (10.6.0.0/24)

Public IP (new) EndpointProtector-ip [Create new](#)

NIC network security group ☐ None ☒ Basic ☐ Advanced

Public inbound ports \* ☐ None ☒ Allow selected ports

Select inbound ports \* HTTP (80), HTTPS (443)

Delete public IP and NIC when VM is deleted ☐

Accelerated networking ☐ The selected image does not support accelerated networking.

**Load balancing**

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

[Review + create](#) < Previous Next: Management > [OK](#)

- Once the deployment has finished, go to **Virtual Machines** on the right side and select the Endpoint Protector image.

**EndpointProtector**

Virtual machine

Connect Start Restart Stop Capture Delete Refresh Open in mobile CU / PS Feedback

⚠ EndpointProtector virtual machine agent status is not ready. Troubleshoot the issue →

**Essentials**

Resource group (new): EndpointProtectorRG

Status: Running

Location: West Europe

Subscription (new): EPC-AS-300-00

Subscription ID: 300ced05-744f-4c0e-b62a-da3fbaac34f3

Tags (new): [Click here to add tags](#)

Operating system: Linux

Size: Standard B2s (2 vcpus, 4 GiB memory)

Public IP address: 52.157.151.105

Virtual network/subnet: EndpointProtectorRG-vnet/default

DNS name: Not configured

**Properties** Monitoring Capabilities (7) Recommendations Tutorials

**Virtual machine**

Computer name: -

Health state: -

Operating system: Linux

Publisher: -

Offer: -

Plan: -

VM generation: V1

Agent status: Not Ready

Agent version: Unknown

Host group: None

Host: -

Proximity placement group: -

Colocation status: N/A

Capacity reservation group: -

**Network**

Public IP address: 52.157.151.105

Public IP address (IPv6): -

Private IP address: 10.6.0.4

Private IP address (IPv6): -

Virtual network/subnet: EndpointProtectorRG-vnet/default

DNS name: Configure

**Size**

Size: Standard B2s

vCPUs: 2

RAM: 4 GiB

**Disk**

OS disk: eppdisk

Encryption at host: Disabled

Azure disk encryption: Not enabled

- Open a web browser and connect to the Public IP address assigned to the Endpoint Protector image.

