Amazon Web Services, Google Cloud Platform & Azure - User Manual
Table of Contents

1. Introduction ............................................... 1

2. Amazon Web Services ................................. 3
   2.1. Obtaining the Endpoint Protector AMI ..................... 3
   2.2. Launching the EC2 image ................................ 4
   2.3. Requesting an Elastic IP ................................ 7
   2.4. Securing your Instance ................................. 9

3. Google Cloud Platform ............................ 10
   3.1. Obtaining the Endpoint Protector GCP image ............ 10
       3.1.1. Downloading the image ............................ 10
   3.2. Creating a bucket .................................. 10
   3.3. Importing the image to the custom image list .......... 12
   3.4. Creating an Endpoint Protector VM Instance ............ 13
   3.5. Requesting a Static IP ............................... 14
   3.6. Creating Firewall rules ............................... 14

4. Azure ....................................................... 16
   4.1. Obtaining the Endpoint Protector Azure VM .......... 16
       4.1.1. Creating a Storage Account and Blob ............ 16
   4.2. Creating a disk ....................................... 18
   4.3. Creating a VM ......................................... 20

5. Endpoint Protector - Licensing .................. 23

6. Disclaimer ............................................... 24
1. Introduction

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

**Information**
For Amazon Web Services, the Endpoint Protector AMI is provided as an Amazon EC2 instance.

**Information**
For Google Clout Platform, the Endpoint Protector image is provided as a *.tar.gz.

**Information**
For Azure, the Endpoint Protector image will be uploaded into your account.

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

**Note**
This document is not intended as a step by step guide in creating an AWS nor a GCP account. The precondition to already have such accounts in place and understand the bases of how these 3rd party services is the responsibility of each Administrator.
2. Amazon Web Services

2.1. Obtaining the Endpoint Protector AMI

Endpoint Protector is not generally available in the AWS Marketplace. In order to have access to the AMI, either contact your Endpoint Protector Representative directly or make 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, advising when the Endpoint Protector AMI has been shared with your account.
2.2. Launching the EC2 image

As the Endpoint Protector image has already been shared with you, this process is similar to any other EC2 launch and is composed of the following simple steps:

2.2.1.1. Go to Services: EC2 > Select your region

2.2.1.2. Go to Images: AMIs > Choose the Private images type and search for Endpoint Protector

2.2.1.3. Right-click and choose Launch Instance

2.2.1.4. Choose an Instance Type
2.2.1.5. The Instance Configuration does not require changes

2.2.1.6. The Storage also does not require changes

2.2.1.7. The **Instance Tag** need to be added as you consider

2.2.1.8. To Configure the Firewall, we recommend the following:

- **Create a new Security Group**
• Provide a Group Name and a Description

• Under **Inbound Rules** chose from the dropdown menu to create a new **Custom TCP rule**. Add the port 443 (mandatory) and 80 (not mandatory). Each of them will have the source set for: Anywhere, 0.0.0.0. When you are done, click **Review and Launch**.

2.2.1.9. **Review** the settings of the instance and **Launch** it

2.2.1.10. **Select an existing key pair or create a new key pair**

If you choose 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 choosing the option **Proceed without a Key Pair** and then click **Launch Instances**.
2.2.1.11. Finish the process by pressing **View Instances**

2.2.1.12. Wait for the instance to start

This might take a few minutes while the **Status Checks** appears as **Initializing**.

2.3. Requesting an Elastic IP

This 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 on **Allocate New Address**.
2.3.1.1. Associate the Elastic IP with your Endpoint Protector Instance.

2.3.1.2. Select the Endpoint Protector Instance from the dropdown list and click Yes, 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.
2.4. Securing your Instance

We recommend further securing your Instance by making all possible settings in the AWS Interface under the option **Security Groups**.
3. Google Cloud Platform

3.1. Obtaining the Endpoint Protector GCP image

Endpoint Protector is not available among the default images in GCP. To have it available in the Console, 3 simple steps will have to be completed.

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

3.1.1. Downloading the image

The Endpoint Protector image can be downloaded from the link provided by your Endpoint Protector Representative. Alternatively, if this image has already been obtained, the step is no longer needed.

3.2. Creating a bucket

In order to upload the Endpoint Protector image in the Google Cloud Platform, a bucket will have to be created. This can be done by following some simple steps:

3.2.1.1. In the GCP Console, go to the Cloud Storage Browser page: (https://console.cloud.google.com/storage/browser)
3.2.1.2. At the top of the page, click on Create bucket

3.2.1.3. Provide a unique bucket name, the standard storage class and a location where to store the image

3.2.1.4. After creating the new bucket, the browser navigates to it

3.2.1.5. At the top of the page, click Upload files

3.2.1.6. Select the Endpoint Protector image file from paragraph 3.1.1 Downloading the image
3.3. Importing the image to the custom image list

After the Endpoint Protector image has been uploaded to the Google Cloud Storage, it needs to be imported in the custom image list.

3.3.1.1. In the GCP Console, go to the Image page: (https://console.cloud.google.com/compute/images)

3.3.1.2. At the top of the page, click Create image

3.3.1.3. Provide a unique name for the image

3.3.1.4. Optimally, provide an image family for the new image or configure specific encryption settings for the image

3.3.1.5. Click the Source menu and select the Cloud Storage file

Information

Depending on the size of the compressed image and the speed of the network connection, the upload can take several hours.
3.3.1.6. Browse for the Endpoint Protector image file that you uploaded to Cloud Storage

3.3.1.7. Click the Create button to import the image

Information
The process can take several minutes depending on the size of the boot disk image.

3.4. Creating an Endpoint Protector VM Instance

With the Endpoint Protector Image now available in the GCP images list, the standard steps to create a VM Instance remain:

3.4.1.1. In the GCP Console, go to the VM Instances page: (https://console.cloud.google.com/compute/instances)

3.4.1.2. Click the Create instance button

3.4.1.3. In the Boot disk section, click Change to begin configuring your boot disk.

3.4.1.4. In the Custom images tab, click the image that you imported
3.4.1.5. At **Boot disk type**, choose Standard persistent disk. Its size should be bigger than the received Endpoint Protector image size.

3.4.1.6. Click **Select** to confirm the boot disk configuration.

3.4.1.7. In the Firewall section, tick **Allow HTTP traffic** and **Allow HTTPS traffic**.

3.4.1.8. Click the **Create** button to create the instance.

### 3.5. Requesting a Static IP

This is required 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 the [External IP addresses page](https://console.cloud.google.com/networking/addresses).

### 3.6. Creating Firewall rules

3.6.1.1. In the GCP Console, go to the Firewall rules page: [https://console.cloud.google.com/networking/firewalls/list](https://console.cloud.google.com/networking/firewalls/list).
3.6.1.2. Click on **default-allow-ssh**

3.6.1.3. Click **Edit** to change the SSH rule, then change the specified protocols and ports from: **tcp:22** to **tcp:64848**

3.6.1.4. Click **Save**
4. Azure

4.1. Obtaining the Endpoint Protector Azure VM

Endpoint Protector is not generally available in the Azure Marketplace. In order to have access to the VM, contact your Endpoint Protector Representative and provide information such as the access keys to a Blob specifically created for the Endpoint Protector VM.

⚠️ Note
We will upload the Endpoint Protector VM to your Blob as soon as possible. Once this step is done, we advise on regenerating the access key.

4.1.1. Creating a Storage Account and Blob

💡 Information
This part of the process is similar to creating any other Storage Account and Blob on Azure. If you are already familiar with it or have created a dedicated Blob already, proceed to step 4.2 Creating a disk.

The prerequisite in obtaining the Azure Endpoint Protector VM is creating a dedicated Storage account / Blob for it. To do so, please follow some simple steps:

1. 4.1.1.1. Open the Azure portal (https://portal.azure.com)
2. 4.1.1.2. Go to Storage accounts and click on +Add
3. 4.1.1.3. Provide a Name to the Storage Account. For the Account kind, choose Storage (general purpose v1). For the Location, preferably choose the nearest to the location of the computers that will be protected by Endpoint Protector. For Replication, choose Locally-redundant storage (LRS). For Re
source group, either choose from an existing one or create a new one.

4.1.1.4. Go to Storage accounts and click on the newly created account.

4.1.1.5. Go to Blobs and click +Container. Give the same name to the container as you did the storage account. For the Public access level choose Container (anonymous read access for containers and blobs).

4.1.1.6. Go to Storage accounts and click on the newly created storage account and choose Access keys. Copy key1 and send it to CoSoSys.
4.1.1.7. Go to Storage accounts, select the newly created storage account. Go to Blobs, right click on the blob container and click Container properties. Copy the URL and sent it to CoSoSys along with key1 from the above step.

**Note**
This is required in order for us to copy the Endpoint Protector VHD to your account.

**Information**
CoSoSys will copy the Endpoint Protector VM to your storage account and notify you when the process is over. Afterwards, we strongly advise for you to regenerate the access keys.

4.2. Creating a disk

Before starting the Endpoint Protector VM, a disk and a VM will have to be prepared. In order to create a disk, some simple steps will have to be followed.

4.2.1.1. Go to All resources on the top right side of the page.

4.2.1.2. Click +Add and search the marketplace for Managed Disks.
4.2.1.3. Go to Managed Disks and choose Create.

4.2.1.4. Provide a Name, a Resource group (preferable the newly created one at step 4.1.1.3), a Location and Availability zone. For the Account type choose Standard (HDD), for Storage type choose Storage Blob.

**Information**
In the Source blob enter the URL entered the URL received from CoSoSys after providing the key and URL mentioned in steps 4.1.1.6 and 4.1.1.7.

For the OS type choose Linux and for the Size (GiB) choose 900 GB.
4.2.1.5. Click **Create** and wait until the message **Successfully created disk** appears.

### 4.3. Creating a VM

In order to complete the process of starting the Endpoint Protector VM in Azure, some final steps will have to be taken.

4.3.1.1. Go to **All resources** page and click on the newly created disks. Click on **Create VM**.

![Create VM](image)

4.3.1.2. Provide a **Name** and a **Resource group** (preferably the group used when creating the disk).

![Resource group](image)

4.3.1.3. Choose a virtual machine profile based closest to the recommended requirements for the disk file used and click **Select**.

**Tips**

*For **Additional Features**, choosing HDD instead of SSD would be recommended to avoid unnecessary payments for an unused SSD attached to the VM.*
4.3.1.4. For the **Public IP address Assignment** choose **Static**.

4.3.1.5. Go to **Network Security Group** and choose **Advanced**. Add two inbound rules by clicking on **Add an inbound rule**: one for TCP port **80** and another for port **443**. Make sure they have different **Priority** numbers.

4.3.1.6. Click **OK** in the **Create network security group** page, in the **Settings** page and in the **Summary** page.
4.3.1.7. Once the deployment has finished, go to **Virtual Machines** on the right side and choose the Endpoint Protector image.

4.3.1.8. Using your preferred web browser, connect to the Public IP address assigned to the Endpoint Protector image in one of the steps above.
5. Endpoint Protector - Licensing

Endpoint Protector is a Bring your Own License (BYOL) Instance. This means that you are paying Amazon (AWS) / Google (GCP) / Microsoft (Azure) for running the instance and then import the license previously purchased from CoSoSys or from any Endpoint Protector Partner.

The price of the Endpoint Protector Licenses with AWS, GCP or Azure is the same as licensing the Endpoint Protector Virtual Appliance. To purchase a license please contact your Endpoint Protector Representative or sales@cososys.com.
6. Disclaimer

Endpoint Protector Appliance does not communicate outside of your network except with liveupdate.endpointprotector.com and cloud.endpointprotector.com.

Endpoint Protector does not contain malware software and does not send at any time any of your private information (if Automatic Live Update Reporting is DISABLED).

Each Endpoint Protector Server has the default SSH Protocol (22) open for Support Interventions and there is one (1) System Account enabled (epproot) protected with a password. The SSH Service can be disabled at customers’ request.

Security safeguards, by their nature, are capable of circumvention. CoSoSys cannot, and does not, guarantee that data or devices will not be accessed by unauthorized persons, and CoSoSys disclaims any warranties to that effect to the fullest extent permitted by law.