

# GCP Administration Guide

FortiAnalyzer 7.0



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO LIBRARY**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD LABS**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



April 5, 2024

FortiAnalyzer 7.0 GCP Administration Guide

05-700-704748-20240405

# TABLE OF CONTENTS

<b>About FortiAnalyzer for GCP</b>	<b>4</b>
Machine type support	4
Models	4
Licensing	5
Order types	5
Creating a support account	5
Registering and downloading licenses	5
<b>Deploying FortiAnalyzer on GCP</b>	<b>7</b>
Initial deployment	7
Registering and downloading your license	8
Connecting to the FortiAnalyzer-VM	9
Adding a disk to the FortiAnalyzer-VM for logging	10
<b>Deploying FortiAnalyzer-VM using Google Cloud SDK</b>	<b>14</b>
Obtaining the deployment image	14
Uploading the deployment image to Google Cloud	14
Creating a FortiAnalyzer custom image	15
Deploying a FortiAnalyzer-VM instance	16
<b>HA for FortiAnalyzer on GCP</b>	<b>18</b>
Deploying FortiAnalyzer HA instances on GCP	18
Transition of secondary IP address during failover topography	19
Configuring FortiAnalyzer HA	20
<b>Change log</b>	<b>22</b>

# About FortiAnalyzer for GCP

FortiAnalyzer-VM for GCP delivers centralized logging, analytics, and reporting features. As a GCP VM instance, FortiAnalyzer allows you to collect, correlate, and analyze geographically and chronologically diverse security data. Aggregate alerts and log information from Fortinet appliances and third-party devices in a single location to get a simplified, consolidated view of your security position. In addition, you will have detailed data capture for forensic purposes to comply with policies regarding privacy and security breach disclosures.

Highlights of FortiAnalyzer for GCP include the following:

- Graphical summary reports provide network-wide reporting of events, activities, and trends occurring on FortiAnalyzers and third-party devices.
- Network event correlation enables IT administrators to quickly identify and react to security threats across the network.
- Scalable performance and capacity supports thousands of FortiAnalyzers and can dynamically scale storage based on retention and compliance requirements.
- Choice of standalone, collector, or analyzer mode allows deployment of individual instances or optimization for specific operations, such as store and forward or analytics.
- Seamless integration with the Fortinet product portfolio enables tight integration to allow FortiAnalyzer resources to be managed from FortiGate or FortiManager user interfaces.

## Machine type support

You can deploy FortiAnalyzer for GCP as VM instances. Supported machine types may change without notice. Currently FortiAnalyzer supports standard machine types, high memory machine types, and high CPU machine types with minimum 2 vCPUs and 7.5 GB of RAM and maximum 96 vCPUs and 624 GB of RAM in the predefined machine type lineup. You can also customize the combination of vCPU and RAM sizes within this range. You can find more details on predefined machine types [here](#).

Latest supported machine types can be seen under machine type selection if you try to launch FortiAnalyzer from the marketplace listing or Compute Engine portal.

## Models

FortiAnalyzer-VM is licensed based on the amount of logging per day and storage capacity. Refer to price lists and order SKUs available through your resellers/distributors. These are also referred to as bring your own license (BYOL) models.

FortiAnalyzer-VM can be deployed using different CPU and RAM sizes and launched on various private and public cloud platforms.

## Licensing

You must have a license to deploy FortiAnalyzer for GCP. The following sections provide information on licensing FortiAnalyzer for GCP:

- [Order types on page 5](#)
- [Creating a support account on page 5](#)
- [Registering and downloading licenses on page 5](#)

### Order types

FortiAnalyzer for GCP supports only Bring Your Own License (BYOL). There is no Pay As You Go/On-Demand (PAYG) subscription available yet.

BYOL is annual perpetual licensing, as opposed to PAYG, which is an hourly subscription available with marketplace-listed products. BYOL licenses are available for purchase from resellers or your distributors, and prices are listed in the publicly available price list that is updated quarterly. BYOL licensing provides the same ordering practice across all private and public clouds, no matter what the platform is. You must activate a license for the first time you access the instance from the GUI or CLI before you can start using various features.

### Creating a support account

FortiAnalyzer-VM for GCP supports BYOL licensing models.

For BYOL, you typically order a combination of products and services, including support entitlement.

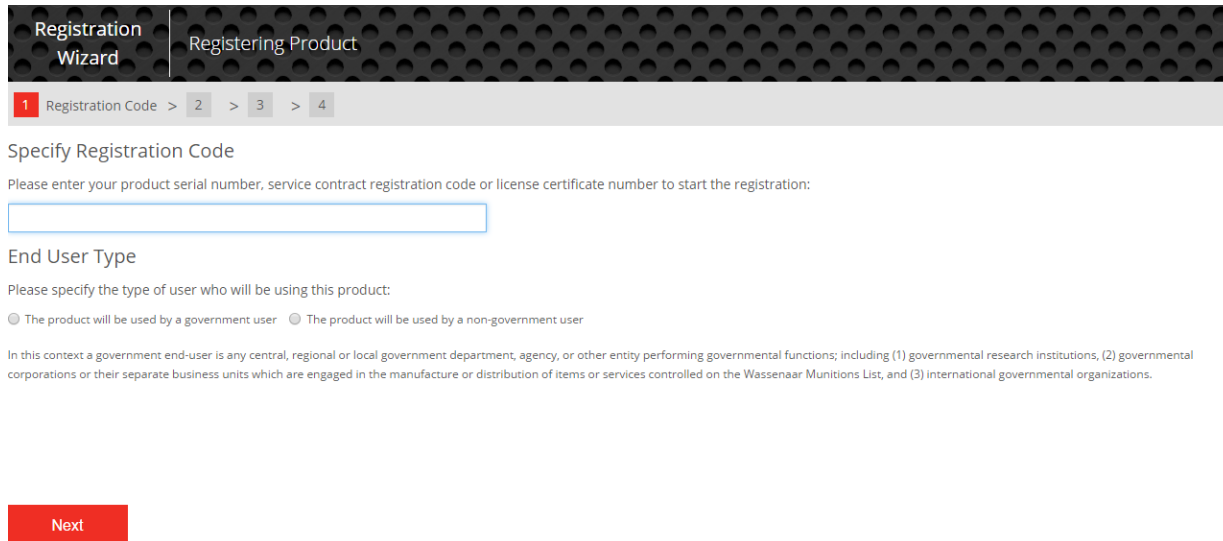
You must create a FortiCare support account and obtain a license to activate the product through the FortiCare support portal. If you have not activated the license, you will see the license upload screen when logging into the FortiAnalyzer and cannot proceed to configure the FortiAnalyzer. See [Registering and downloading licenses on page 5](#).

### Registering and downloading licenses

Licenses for the BYOL licensing model can be obtained through any Fortinet partner. If you don't have a partner, contact [gcp-sales@fortinet.com](mailto:gcp-sales@fortinet.com) for assistance in purchasing a license.

After you purchase a license or obtain an evaluation license, you will receive a PDF with an activation code.

1. Go to [Customer Service & Support](#) and create a new account or log in with an existing account.
2. Go to *Asset > Register/Renew* to start the registration process.



The screenshot shows the 'Registration Wizard' interface for 'Registering Product'. It features a progress bar with four steps: 1. Registration Code (active), 2, 3, and 4. Below the progress bar, the section is titled 'Specify Registration Code'. It instructs the user to 'Please enter your product serial number, service contract registration code or license certificate number to start the registration:' and provides a text input field. Below this is the 'End User Type' section, which asks the user to 'Please specify the type of user who will be using this product:'. It offers two radio button options: 'The product will be used by a government user' and 'The product will be used by a non-government user'. A detailed footnote explains the definition of a government end-user. At the bottom of the form is a red 'Next' button.

3. In the *Specify Registration Code* field, enter your license activation code, then select *Next* to continue registering the product.
4. Enter your details in the other fields as required.
5. At the end of the registration process, download the license (.lic) file to your computer. You will upload this license later to activate the FortiAnalyzer-VM.

After registering a license, Fortinet servers may take up to 30 minutes to fully recognize the new license. When you upload the license (.lic) file to activate the FortiAnalyzer-VM, if you get an error that the license is invalid, wait 30 minutes and try again.

# Deploying FortiAnalyzer on GCP

Deploying a FortiAnalyzer on GCP consists of the following steps:

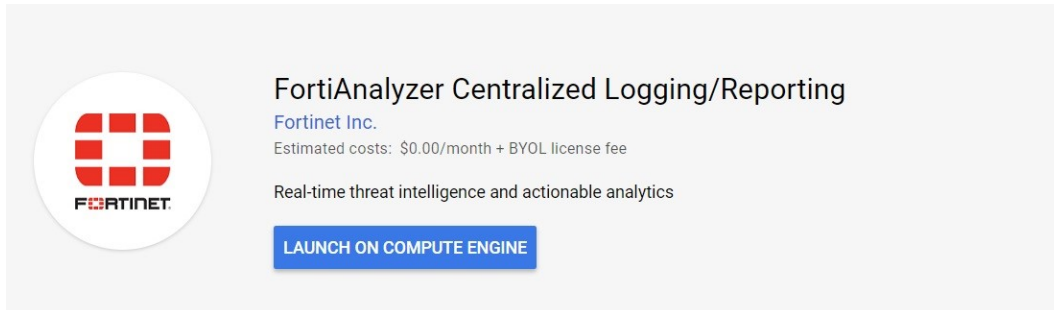
1. [Initial deployment on page 7](#)
2. [Registering and downloading your license on page 8](#)
3. [Connecting to the FortiAnalyzer-VM on page 9](#)
4. [Adding a disk to the FortiAnalyzer-VM for logging on page 10](#)

## Initial deployment



FortiAnalyzer-VM requires a minimum disk size of 500GB.

1. In the Google Cloud marketplace Cloud Launcher, find *FortiAnalyzer Centralized Logging/Reporting*.



**Runs on**  
Google Compute Engine

**Type**  
Single VM  
BYOL

### Overview

FortiAnalyzer delivers critical insight into threats across the entire attack surface and provides instant visibility, situation awareness, real-time threat intelligence and actionable analytics.

With action-oriented views and deep drill-down capabilities, FortiAnalyzer offers centralized logging and reporting for Fortinet's Security Fabric.

2. Click **LAUNCH ON COMPUTE ENGINE**.
3. Configure the variables as required:

<b>Deployment name</b>	Enter the name of the FortiAnalyzer-VM to appear in the Compute Engine portal.
<b>Zone</b>	Choose the zone to deploy the FortiAnalyzer to.
<b>Machine type</b>	Choose the instance type required.
<b>Boot disk type</b>	Choose the desired boot disk type.

<b>Boot disk size in GB</b>	Resize the disk to match the minimum disk size (500GB). Note you must add additional disks for logging in later steps.
<b>Network name</b>	Select the network located in the selected zone.
<b>Subnetwork name</b>	Select the subnet where the FortiAnalyzer resides. Currently the Cloud Launcher solution supports one network interface.
<b>Firewall</b>	Leave all selected, or allow at least HTTPS if the strictest security is allowed in your network as the first setup. Change firewall settings as needed later.
<b>External IP</b>	Select <i>Ephemeral</i> . You will need to access the FortiAnalyzer management GUI via this public IP address.

Leave the other options as shown.

4. Click *Deploy*. When deployment is complete, the screen appears as below.

FortiAnalyzer Centralized Logging/Reporting  
Solution provided by Fortinet Inc.

Site address	https://[redacted]:443/
Admin user	admin
Admin password (Temporary)	[redacted]
Instance	[redacted]-faz564-test002
Instance zone	us-central1-f
Instance machine type	n1-standard-2

[More about the software](#)

Get started with FortiAnalyzer Centralized Logging/Reporting

[Visit the site](#) SSH

## Registering and downloading your license

Licenses for the BYOL licensing model can be obtained through any Fortinet partner. If you don't have a partner, contact [gcpsales@fortinet.com](mailto:gcpsales@fortinet.com) for assistance in purchasing a license.

After you purchase a license or obtain an evaluation license (60-day term), you will receive a PDF with an activation code.

### To register and download your license:

1. Go to [Customer Service & Support](#) and create a new account or log in with an existing account.
2. In *Asset Management*, click *Register Product*, or click the *Register More* button.
3. Enter your registration code, and confirm the other details required for registration including your end user type.
4. At the end of the registration process, download the license (.lic) file to your computer. You will upload this license later to activate the FortiAnalyzer-VM.



After registering a license, Fortinet servers may take up to 30 minutes to fully recognize the new license. When you upload the license (.lic) file to activate the FortiAnalyzer-VM, if you get an error that the license is invalid, wait 30 minutes and try again.

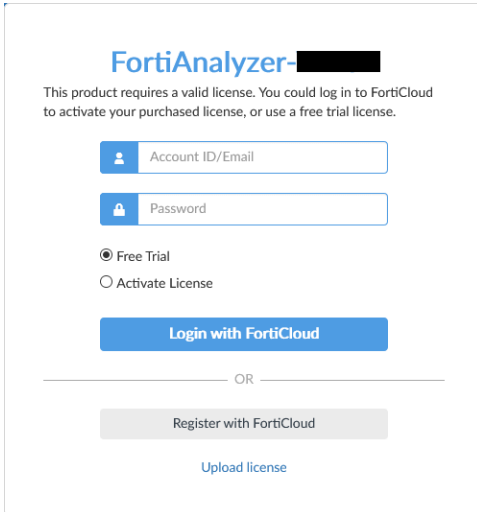
For more information, see the [FortiCloud Asset Management Administration Guide](#).

## Connecting to the FortiAnalyzer-VM

### To activate a license for FortiAnalyzer VM:

1. Connect to the FortiAnalyzer using your browser.


The login dialog box is displayed.



The image shows the FortiAnalyzer login interface. At the top, it says 'FortiAnalyzer-XXXXXX'. Below that, a message states: 'This product requires a valid license. You could log in to FortiCloud to activate your purchased license, or use a free trial license.' There are two input fields: 'Account ID/Email' and 'Password'. Below these fields are two radio buttons: 'Free Trial' (selected) and 'Activate License'. A blue button labeled 'Login with FortiCloud' is positioned below the radio buttons. Below this button is a horizontal line with 'OR' in the center. Underneath the line is a gray button labeled 'Register with FortiCloud'. At the bottom, there is a blue link labeled 'Upload license'.

2. Take one of the following actions:

Action	Description
<b>Free Trial</b>	<p>If a valid license is not associated with the account, you can start a free trial license.</p> <ol style="list-style-type: none"> <li>1. Select <i>Free Trial</i>, and click <i>Login with FortiCloud</i>.</li> <li>2. Use your FortiCloud account credentials to log in, or create a new account. FortiAnalyzer connects to FortiCloud to get the trial license. The system will restart to apply the trial license.</li> <li>3. Read and accept the license agreement.</li> </ol> <p>For more information, see the <a href="#">FortiAnalyzer 7.0.0 VM Trial License Guide</a>.</p>
<b>Activate License</b>	<p>If you have a license file, you can activate it .</p> <ol style="list-style-type: none"> <li>1. Select <i>Activate License</i>, and click <i>Login with FortiCloud</i>.</li> <li>2. Use your FortiCloud account credentials to log in. FortiAnalyzer connects to FortiCloud, and the license agreement is displayed.</li> <li>3. Read and accept the license agreement.</li> </ol>
<b>Upload License</b>	<ol style="list-style-type: none"> <li>1. Click <i>Browse</i> to upload the license file, or drag it onto the field.</li> </ol>

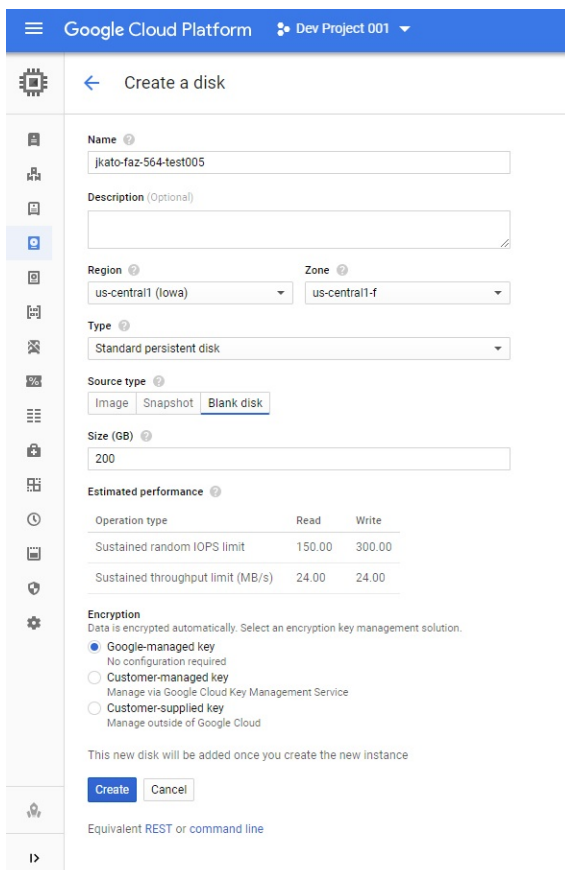
Action	Description
	<p>2. Click <i>Upload</i>. After the license file is uploaded, the system will restart to verify it. This may take a few moments.</p> <hr/> <div style="display: flex; align-items: center;">  <p>To download the license file, go to the Fortinet Technical Support site (<a href="https://support.fortinet.com/">https://support.fortinet.com/</a>), and use your FortiCloud credentials to log in. Go to <i>Asset Managmeent &gt; Products &gt; Product List</i>, then click the product serial number.</p> </div> <hr/>

- Once registration is complete, log into the FortiAnalyzer-VM with the username *admin* and the supplied temporary password. From the previous step, there is a temporary admin password automatically generated on the Google Cloud.

## Adding a disk to the FortiAnalyzer-VM for logging

You are required to add another disk to store logs.

- Log into the GCP Compute Engine.
- Go to the *Disks* page.
- Create a blank disk in the same zone where the FortiAnalyzer-VM resides. Disk size varies depending on the license.



Google Cloud Platform Dev Project 001

← Create a disk

Name

Description (Optional)

Region  Zone

Type

Source type

Size (GB)

Estimated performance

Operation type	Read	Write
Sustained random IOPS limit	150.00	300.00
Sustained throughput limit (MB/s)	24.00	24.00

Encryption

Data is encrypted automatically. Select an encryption key management solution.

☒ Google-managed key  
No configuration required

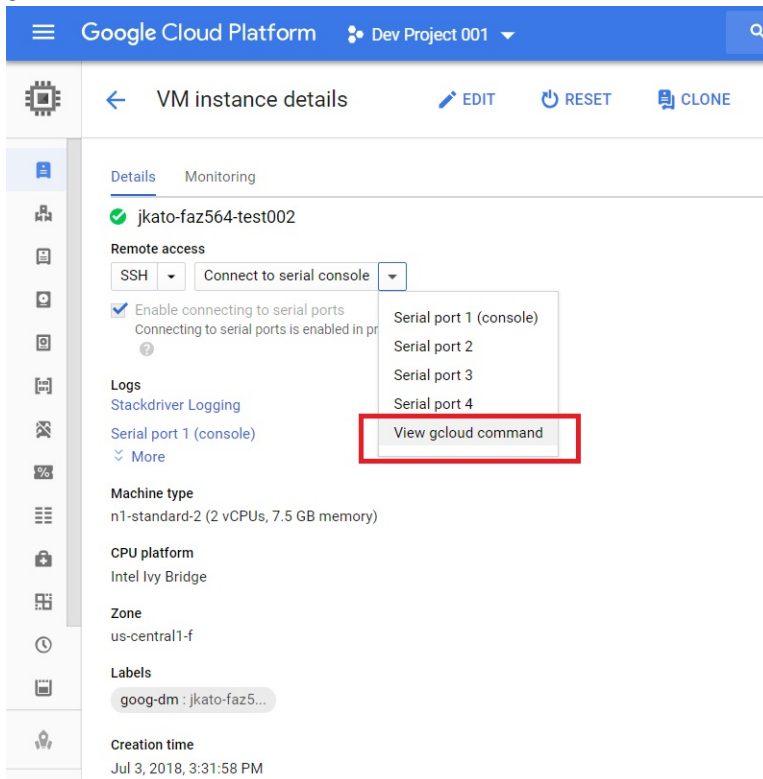
☐ Customer-managed key  
Manage via Google Cloud Key Management Service

☐ Customer-supplied key  
Manage outside of Google Cloud

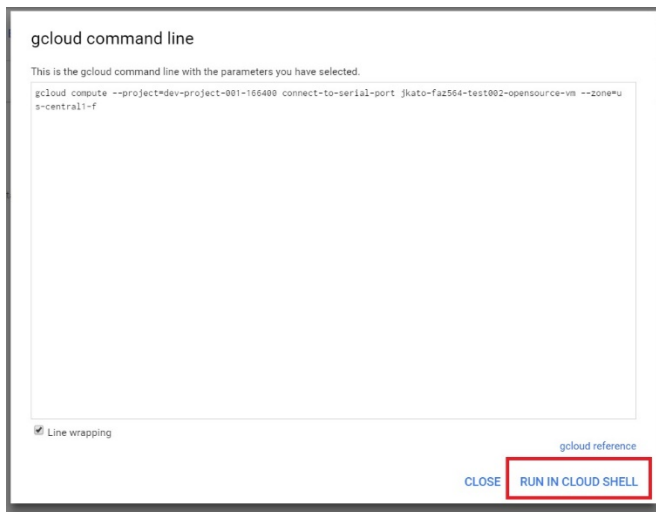
This new disk will be added once you create the new instance

Equivalent REST or command line

- Click **Create**. Ensure the disk appears in the *Disks* list.
- You must attach the disk to the FortiAnalyzer-VM instance. Navigate to the FortiAnalyzer-VM instance and start the `gcloud` command.



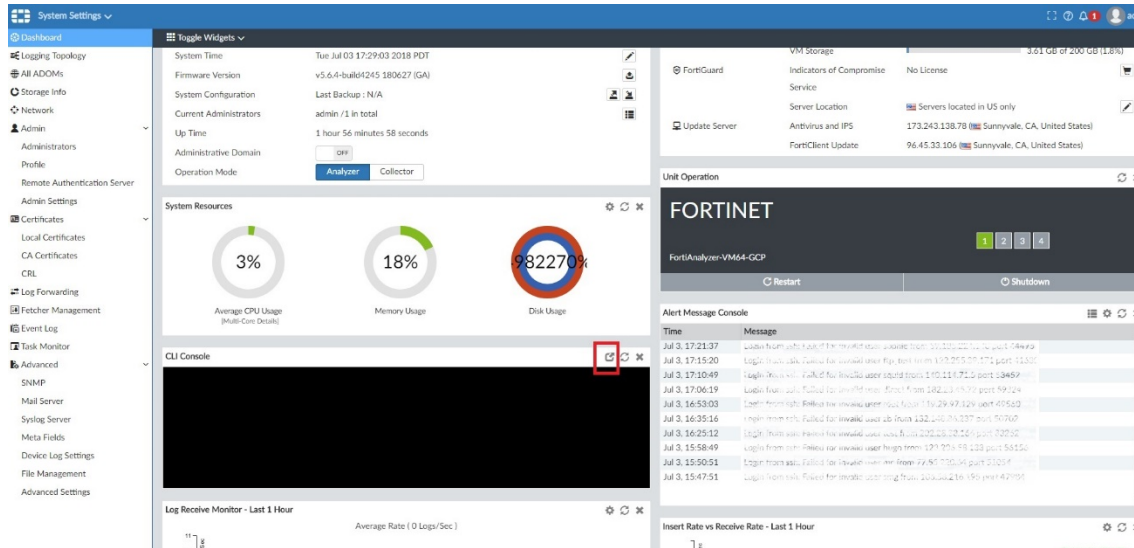
- Click **RUN IN CLOUD SHELL**.



- Delete the lines that appear in the command line.



8. Enter the following command:  
`gcloud compute instances attach-disk [INSTANCE_NAME] --disk [DISK_NAME]`  
 For example, the above instance has the instance name "jkato-faz564-test002" and disk name "jkato-faz-564-test005". In this case, the command is as follows:  
`gcloud compute instances attach-disk jkato-faz564-test002 --disk jkato-faz-564-test005`
9. After attaching the disk, log into the FortiAnalyzer-VM management GUI.
10. Click **System Settings**. Invoke the command line by clicking the icon in the CLI Console widget.



11. In the command line window, enter `exec lvm info`. The recently added disk is shown as *Unused*.

```
FAZVM64-GCP #
FAZVM64-GCP # exec lvm info
LVM Status: Not-Started
LVM size: 0GB

Disk1 :      Unused      209GB
Disk2 :      Unavailable  0GB
Disk3 :      Unavailable  0GB
Disk4 :      Unavailable  0GB
Disk5 :      Unavailable  0GB
Disk6 :      Unavailable  0GB
Disk7 :      Unavailable  0GB
Disk8 :      Unavailable  0GB
Disk9 :      Unavailable  0GB
Disk10:      Unavailable  0GB
Disk11:      Unavailable  0GB
Disk12:      Unavailable  0GB
Disk13:      Unavailable  0GB
Disk14:      Unavailable  0GB
Disk15:      Unavailable  0GB

FAZVM64-GCP #
```

12. Enter `exec lvm start` to start LVM disk management. Enter `y` to continue. The system reboots.

```
FAZVM64-GCP # exec lvm start
This operation will start managing disks using LVM.
All the data on the log disk will be ERASED!
Please backup your data before starting LVM.
The unit will REBOOT.
Do you want to continue? (y/n)y
```

13. Rebooting causes the connection to the CLI console and the management GUI to be lost. Repeat steps 9 to 11. The disk now appears as *Used*.

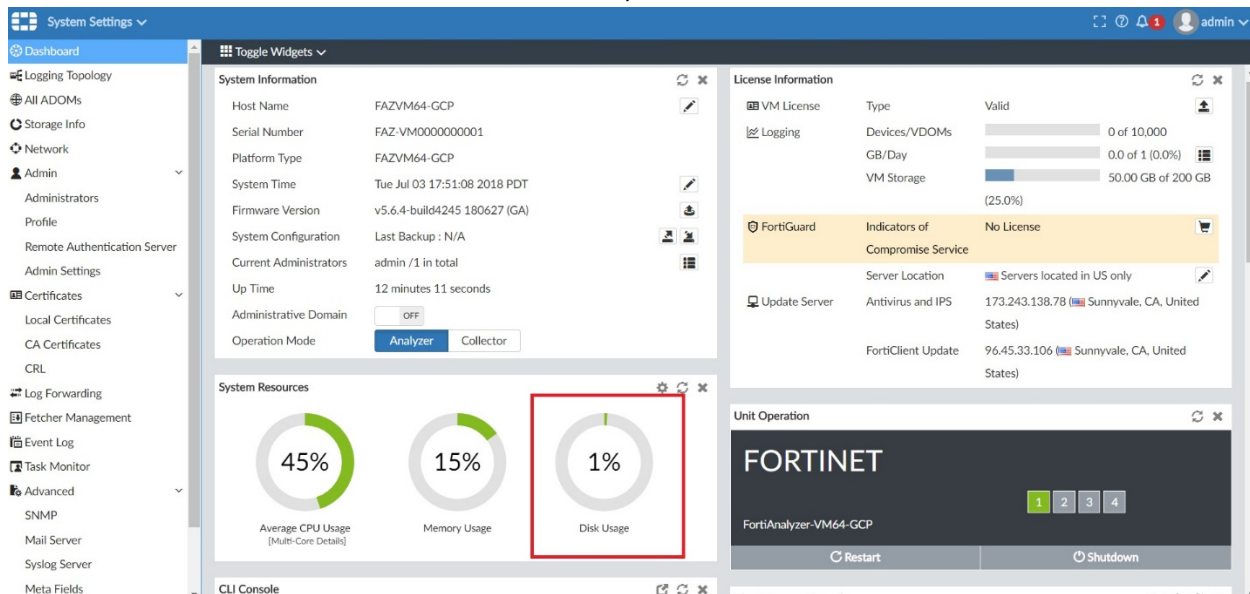
```
FAZVM64-GCP # exec lvm info
LVM Status: OK
LVM size: 209GB

Disk1 :      Used      209GB
Disk2 : Unavailable    0GB
Disk3 : Unavailable    0GB
Disk4 : Unavailable    0GB
Disk5 : Unavailable    0GB
Disk6 : Unavailable    0GB
Disk7 : Unavailable    0GB
Disk8 : Unavailable    0GB
Disk9 : Unavailable    0GB
Disk10: Unavailable    0GB
Disk11: Unavailable    0GB
Disk12: Unavailable    0GB
Disk13: Unavailable    0GB
Disk14: Unavailable    0GB
Disk15: Unavailable    0GB
```

14. Run `exec lvm extend`. This incorporates the disk into the FortiAnalyzer system.

```
FAZVM64-GCP # exec lvm extend
This operation will need to reboot the system.
Do you want to continue? (y/n)
```

15. To add more disks later, follow steps 4 to 6 in [Technical Note: Extending disk space in FortiAnalyzer VM / FortiManager VM](#).
16. Go to the Dashboard. You will now have sufficient disk space.



# Deploying FortiAnalyzer-VM using Google Cloud SDK

You can deploy FortiAnalyzer-VM (bring your own license (BYOL)) by using the Google Cloud SDK on your local PC. This is a method of deploying FortiAnalyzer-VM on GCP outside of the marketplace product listing and without creating an instance on the Google Cloud Compute Portal.

For details, see [Cloud SDK](#).



This deployment method only applies for BYOL.

---

This deployment consists of the following steps:

1. [Obtaining the deployment image on page 14](#)
2. [Uploading the deployment image to Google Cloud on page 14](#)
3. [Creating a FortiAnalyzer custom image on page 15](#)
4. [Deploying a FortiAnalyzer-VM instance on page 16](#)

## Obtaining the deployment image

**To obtain the deployment image:**

1. Sign in to [FortiCloud](#).
2. Go to *Support > VM Images*.
3. From the *Select Product* dropdown list, select *FortiAnalyzer*.
4. From the *Select Platform* dropdown list, select *Google*.
5. Download the deployment package file. The deployment package file is named "FAZ\_VM64\_GCP-vX-buildXXXX-FORTINET.out.gcp.tar.gz", where vX is the major version number and XXXX is the build number.

## Uploading the deployment image to Google Cloud

**To upload the FortiAnalyzer deployment image to Google Cloud:**

1. Log into Google Cloud.
2. Go to *Storage > Browser*.
3. Create a new bucket or go to an existing bucket.
4. Upload the newly downloaded deployment file.

## Creating a FortiAnalyzer custom image



This process uses environment variables with the GCloud SDK CLI commands.

### To create a FortiAnalyzer custom image:

1. Obtain and place the latest FortiAnalyzer-VM 7.0 image in your desired bucket:
  - a. Download the FortiAnalyzer-VM image from the Fortinet Support site. For more information, see [Obtaining the deployment image on page 14](#).
  - b. Place the obtained image in your desired bucket. For more information, see [Uploading the deployment image to Google Cloud on page 14](#).
2. Create a custom image via the Google Cloud CLI SDK. Assign environment variables with your project ID, the bucket where you placed the FortiAnalyzer-VM image, and the image name. This example uses the full name of the file downloaded from the Fortinet Support site in the image variable:

```
project=<your project id>

bucket=<name of your bucket>

source_image=<source image, e.g. FAZ_VM64_GCP-v7.4.2-build2397-FORTINET.out.gcp.tar.gz>

image_name=doc-FortiAnalyzer-vm-image

gcloud compute images create $image_name \
--project=$project \
--source-uri=https://storage.googleapis.com/$bucket/$source_image \
--storage-location=us
```

```
@cloudshell:~ (dev-project- )$ project=dev-project-
bucket=gcp-doc-bucket
source_image=FAZ_VM64_GCP-v7.4.2-build2397-FORTINET.out.gcp.tar.gz
image_name=doc-fortianalyzer-vm-image
@cloudshell:~ (dev-project- )$
@cloudshell:~ (dev-project- )$ gcloud compute images create $image_name \
--project=$project \
--source-uri=https://storage.googleapis.com/$bucket/$source_image \
--storage-location=us
Created [https://www.googleapis.com/compute/v1/projects/dev-project- /global/images/doc-fortianalyzer-vm-image].
NAME: doc-fortianalyzer-vm-image
PROJECT: dev-project-
FAMILY:
DEPRECATED:
STATUS: READY
@cloudshell:~ (dev-project- )$
```

## Deploying a FortiAnalyzer-VM instance



The networks in this example are already setup. Use existing networks and subnets or create them prior to running the commands in this document. Edit all GCP environment-specific variables to fit your GCP environment. This guide assumes familiarity with Linux distributions and Google Cloud CLI already installed and configured for your project and GCP environment. For information about installing the Google Cloud CLI SDK, see [Install the gcloud CLI](#).



This process uses environment variables with the GCloud SDK CLI commands. The custom image creation process is referenced to create the FortiAnalyzer-VM Instance.

### To deploy a FortiAnalyzer-VM instance:

#### 1. Define environment variables:

```
project=<your project id>
zone=us-central1-a
serviceaccount=<your service account>
image_name=doc-FortiAnalyzer-vm-image
image=projects/$project/global/images/$image_name
```

#### 2. Edit and run the following commands in GCP:

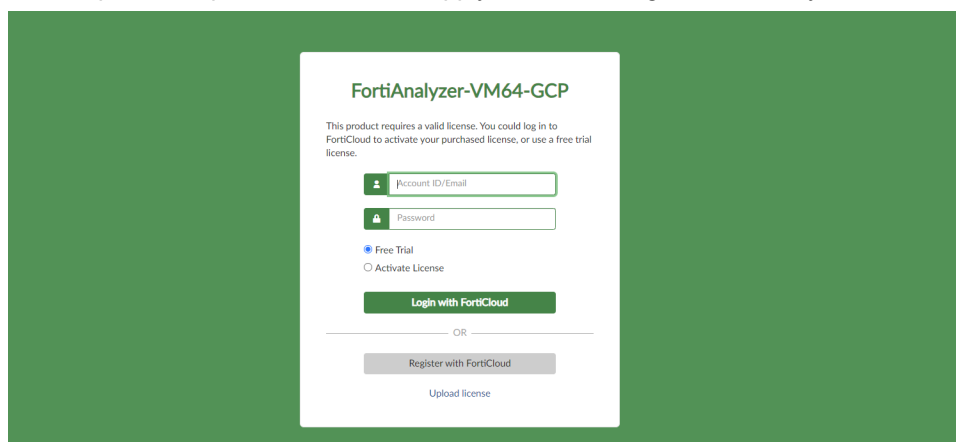
```
gcloud compute instances create doc-fortianalyzer-vm \
--project=$project \
--zone=$zone \
--machine-type=n2d-standard-2 \
--network-interface=network-tier=PREMIUM,private-network-
ip=10.0.1.10,subnet=unprotected-public-subnet \
--service-account=$serviceaccount \
--scopes=https://www.googleapis.com/auth/cloud-platform \
--create-disk=auto-delete=yes,boot=yes,device-name=doc-fortianalyzer-
vmboot,image=$image,mode=rw,size=10,type=projects/$project/zones/$zone/diskTypes/pd-
balanced \
--create-disk=auto-delete=yes,device-name=doc-fortianalyzer-
vmlog,mode=rw,size=10,type=projects/$project/zones/$zone/diskTypes/pd-balanced
```



```
@cloudshell:~ (dev-project) $ zone=us-central1-a
serviceaccount=aj-201@
.iam.gserviceaccount.com
image=projects/$project/global/images/$image_name
@cloudshell:~ (dev-project) $ gcloud compute instances create doc-fortianalyzer-vm \
--project=$project \
--zone=$zone \
--machine-type=n2d-standard-2 \
--network-interface=network-tier=PREMIUM,private-network-ip=10.0.1.10,subnet=unprotected-public-subnet \
--service-account=$serviceaccount \
--scopes=https://www.googleapis.com/auth/cloud-platform \
--create-disk=auto-delete=yes,boot=yes,device-name=doc-fortianalyzer-vmboot,image=$image,mode=rw,size=10,type=projects/$project/zones/$zone/diskTypes/pd-balanced \
--create-disk=auto-delete=yes,device-name=doc-fortianalyzer-vmlog,mode=rw,size=10,type=projects/$project/zones/$zone/diskTypes/pd-balanced
Created [https://www.googleapis.com/compute/v1/projects/dev-project-
/zones/us-central1-a/instances/doc-fortianalyzer-vm].

NAME: doc-fortianalyzer-vm
ZONE: us-central1-a
MACHINE TYPE: n2d-standard-2
PREEMPTIBLE:
INTERNAL_IP: 10.0.1.10
EXTERNAL_IP:
STATUS: RUNNING
@cloudshell:~ (dev-project) $
```

3. Obtain the newly deployed FortiAnalyzer-VM instance ID by running the following command: `gcloud compute instances describe doc-FortiAnalyzer-vm -zone=$zone | grep id`. For more information, see [Get the ID of a VM instance](#).
4. Access the newly deployed FortiAnalyzer-VM using the public IP address from step 2's output and the instance ID from step 4 as the password. You can apply a license using the FortiAnalyzer GUI.



# HA for FortiAnalyzer on GCP

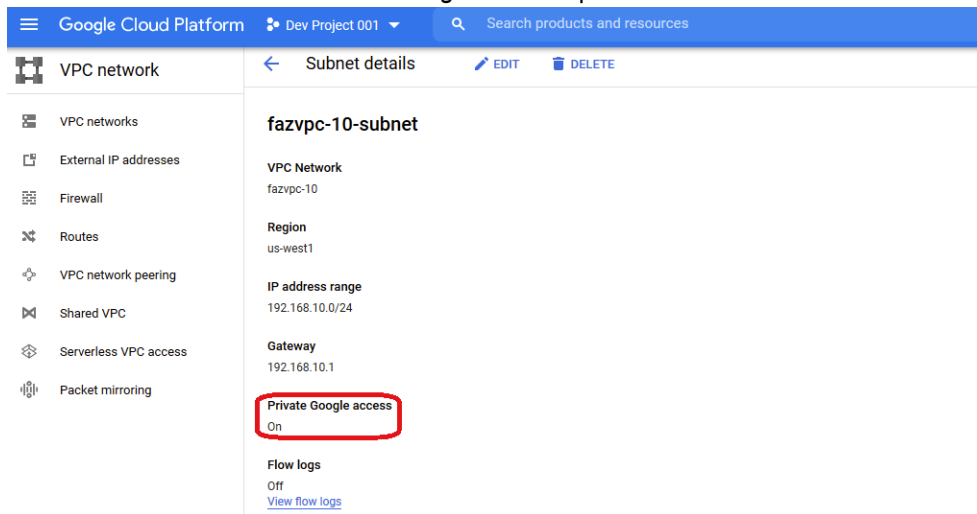
The following topics provide an overview of how to deploy FortiAnalyzer in high availability (HA) mode on GCP:

1. [Deploying FortiAnalyzer HA instances on GCP on page 18](#)
2. [Configuring FortiAnalyzer HA on page 20](#)

## Deploying FortiAnalyzer HA instances on GCP

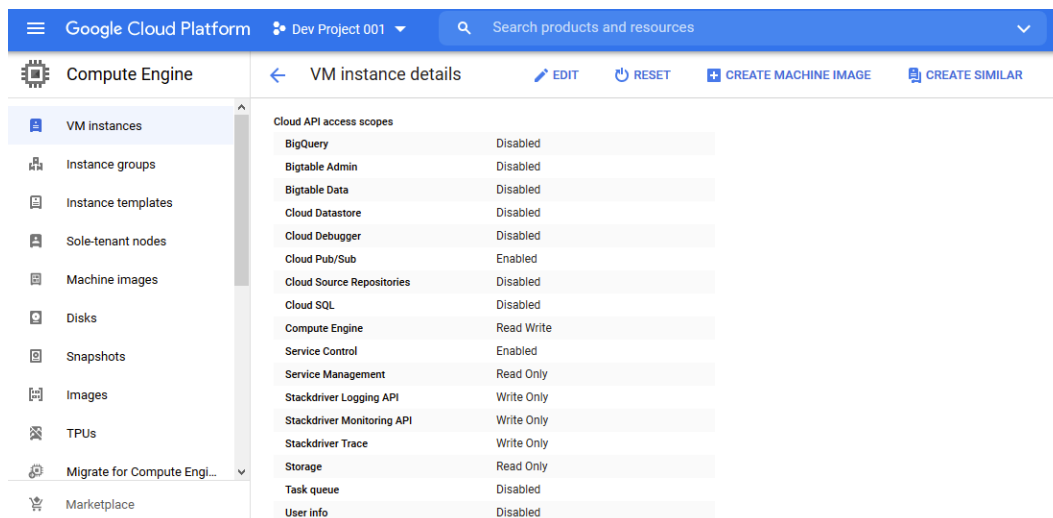
To deploy FortiAnalyzer instances on GCP:

1. In GCP, create the FortiAnalyzer instances in one Region in the same or different subnets. The subnets must have the *Private Google access* option enabled in the *Subnet details* menu.



2. Allocate a Static IP address to be used as the virtual IP (VIP) of the FortiAnalyzer HA. Alternatively, a Secondary Internal IP can also be used as the VIP if necessary.
  - While creating the External IP, ensure that the *Static IP Network Service Tier* is *Premium* and the region is the same as that of the FortiAnalyzer instances.

The External VIP is assigned to an instance when its mode is transitioned to Primary by the fazutil to call Google APIs from within the instance.
3. Assign the required permissions in IAM for the service account associated with each of the FortiAnalyzer instances.
4. Also ensure that the *Cloud API access scopes* for *Compute Engine* in each instance is set to *Read Write*.



Ensure that all the *Google Cloud Platform Quotas* under *ListGroup* have the necessary allocation as this may cause HA to fail otherwise.

- On a *GCP Firewall Policy*, create an inbound rule that allows traffic for the following ports between the primary and secondary units:

Protocol	Port	Purpose
Other*	112	To allow the keepalived adverts from the primary.
TCP	514	To allow initial log sync.
TCP	5199	To allow for configuration sync.

\* 112 VRRP (Virtual Router Redundancy Protocol), Common Address Redundancy Protocol (not IANA assigned)

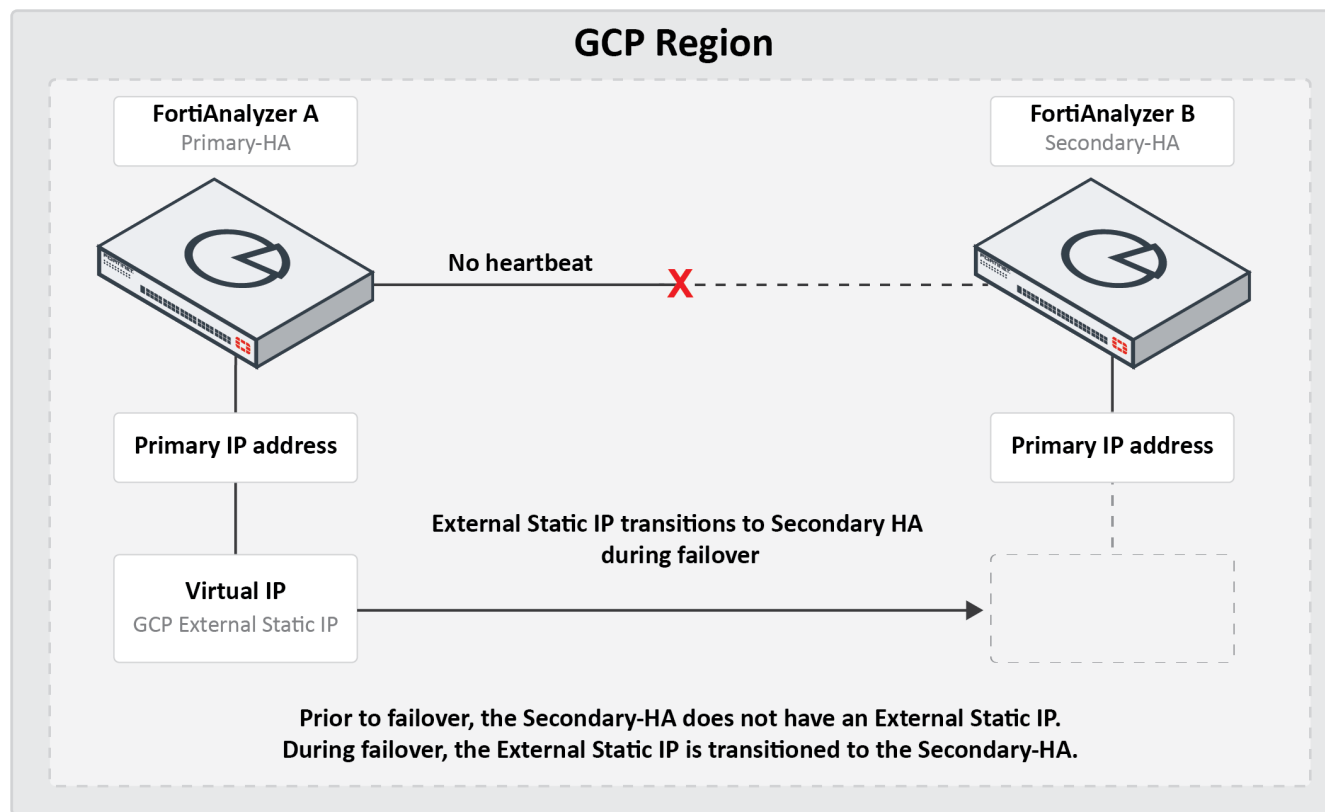
You can now configure the HA settings in FortiAnalyzer. See [Configuring FortiAnalyzer HA on page 20](#).

## Transition of secondary IP address during failover topography

In the example below, FortiAnalyzer-A is the Primary-HA and FortiAnalyzer-B is the Secondary-HA.

During failover, FortiAnalyzer-B becomes the new Primary unit. The External Static IP is transitioned from FortiAnalyzer-A to FortiAnalyzer-B, and can be accessed from the internet using the same IP. The addresses does not change during transition.

Prior to failover, the Secondary-HA (FortiAnalyzer-B) is not configured with a External Static IP address.



## Configuring FortiAnalyzer HA

### To configure FortiAnalyzer HA:

1. On FortiAnalyzer, configure high availability at *System Settings > HA*.  
See the [FortiAnalyzer Administration Guide](#) for more information on configuring HA.  
When configuring HA, use the primary private IP as the *Peer IP* and the External Static IP as the *VIP*.

**Cluster Status**

Refresh

<input type="checkbox"/> Role	Serial Number	IP	Host Name	Uptime/Downtime	Initial Logs Sync	Configuration Sync	Message
No record found.							

**Cluster Settings**

Operation Mode: Standalone High Availability

Preferred Role: ☐ Primary ☒ Secondary

**Cluster Virtual IP**

Interface:

IP Address:

**Cluster Settings**

Peer IP and Peer SN

Peer IP	Peer SN
<input type="text"/>	<input type="text"/> +

Group Name:

Group ID:  (1-255)

Password:

Heart Beat Interval:  Seconds

Failover Threshold:

Priority:  (80-120)

Log Data Sync: ☒ ON

Apply

2. Import the Google Root CA to FortiAnalyzer. In order for the fazutil to call the Google API successfully, you must import the Google Cloud CA certificates to each FortiAnalyzer instance. For more information on Google Trust Services, see <https://pki.goog/repository/>.
  - a. Go to *System Settings > Certificates > CA Certificates*.
  - b. Click *Import*.
  - c. Browse to the file location and select it, or drag-and-drop it into the pop-up window.
  - d. Click *OK*.

## Change log

Date	Change description
2021-04-22	Initial release.
2021-08-11	Updated <a href="#">Connecting to the FortiAnalyzer-VM on page 9</a> .
2021-09-17	Added <a href="#">HA for FortiAnalyzer on GCP on page 18</a>
2023-05-18	Updated <a href="#">Initial deployment on page 7</a>
2024-03-08	Updated <a href="#">Deploying FortiAnalyzer HA instances on GCP on page 18</a> .
2024-04-05	Added <a href="#">Deploying FortiAnalyzer-VM using Google Cloud SDK on page 14</a> .



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.