



AWS Administration Guide

FortiAnalyzer 7.6



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



March 14, 2025

FortiAnalyzer 7.6 AWS Administration Guide

05-760-1055726-20250314

TABLE OF CONTENTS

About FortiAnalyzer for AWS	4
Instance type support	4
Bring your own license (BYOL)	4
Region support	7
Licensing	8
Order types	8
Creating a support account	9
Deploying FortiAnalyzer-VM	12
Deploying -VM using 1-Click Launch	12
Deploying FortiAnalyzer-VM using manual launch	14
Adding additional storage (optional)	18
Installing a valid license	19
Configuring your FortiAnalyzer-VM	20
PAYG instance scaling	21
Scaling up the FortiAnalyzer instance	21
Scaling down the FortiAnalyzer instance	26
HA for FortiAnalyzer on AWS	28
Deploying FortiAnalyzer HA instances on AWS	28
Configuring FortiAnalyzer HA	29
Change log	31

About FortiAnalyzer for AWS

Fortinet FortiAnalyzer securely aggregates log data from Fortinet devices (both physical and virtual) and other syslog-compatible devices. Using a comprehensive suite of easily-customized reports, users can filter and review records, including traffic, event, virus, attack, web content, and email data, mining the data to determine your security stance and assure regulatory compliance. FortiAnalyzer is one of several versatile Fortinet management products that provide a diverse deployment types, growth flexibility, advanced customization through APIs and simple licensing.

Highlights of FortiAnalyzer for AWS include the following:

- Predefined and customized charts help monitor, maintain, and identify attack patterns, acceptable use policies, and demonstrate policy compliance
- Scalable architecture allows the device to run in collector or analyzer modes for optimized log processing
- Advanced features such as event correlation, forensic analysis, and vulnerability assessment provide essential tools for in-depth protection of complex networks

Bring your own license (BYOL) is annual perpetual licensing. The BYOL license is available from resellers or your distributors.

This guide describes how to deploy FortiAnalyzer-VM for AWS in one of two ways:

- [Deploying -VM using 1-Click Launch on page 12](#)
- [Deploying FortiAnalyzer-VM using manual launch on page 14](#) (for those who require custom configuration)

1-Click Launch creates the minimum size of EBS storage for quick setup and viewing. For production purposes, you will need more storage later. To have more storage initially, use manual launch. You can also manually add storage after the launch as described in [Adding additional storage \(optional\) on page 18](#).

-VMs can be deployed on the AWS Elastic Compute Cloud (EC2). Prior to deploying the VM, an Amazon EC2 account is required. You can deploy the -VM using the AWS Marketplace launch or directly from the EC2 console.

Instance type support

FortiAnalyzer supports the following instance types on AWS. Depending on the instance type, certain maximum limits are applied.

Supported instances in the AWS marketplace listing may be changed without notice and may vary between BYOL models. See [Order types on page 8](#).

For more detail about AWS instance types, see [Amazon EC2 Instance Types](#).

The corresponding size of disks to the FortiAnalyzer instances have to be manually added, up to the allowed limits. The following lists instance types supported for the different licensing models.

Bring your own license (BYOL)

The BYOL listing supports the following instance types

Instance category	Instance family	Instance type	vCPU	Memory (GiB)
General purpose	T3	t3.xlarge	4	16
		t3.2xlarge	8	32
	M4	m4.xlarge	4	16
		m4.2xlarge	8	32
		m4.4xlarge	16	64
		m4.10xlarge	40	160
		m4.16xlarge	64	256
	M5	m5.xlarge	4	16
		m5.2xlarge	8	32
		m5.4xlarge	16	64
		m5.8xlarge	32	128
		m5.12xlarge	48	192
		m5.16xlarge	64	256
		m5.24xlarge	96	384

General purpose	M6a*	m6a.xlarge	4	16
		m6a.2xlarge	8	32
		m6a.4xlarge	16	64
		m6a.8xlarge	32	128
		m6a.16xlarge	64	256
		m6a.32xlarge	128	512
	M6i*	m6i.xlarge	4	16
		m6i.2xlarge	8	32
		m6i.4xlarge	16	64
		m6i.8xlarge	32	128
		m6i.16xlarge	64	256
		m6i.32xlarge	128	512
	M7a*	m7a.xlarge	4	16
		m7a.2xlarge	8	32
		m7a.4xlarge	16	64
		m7a.8xlarge	32	128
		m7a.16xlarge	64	256
		m7a.32xlarge	128	512

Compute Optimized	C4	c4.4xlarge	16	30
		c4.8xlarge	36	60
	C5	c5.2xlarge	8	16
		c5.4xlarge	16	32
		c5.9xlarge	36	72
		c5.12xlarge	48	96
		c5.18xlarge	72	144
		c5.24xlarge	96	192

Storage Optimized	D2	d2.xlarge	4	30.5
		d2.2xlarge	8	61
		d2.4xlarge	16	122
		d2.8xlarge	36	244
	H1	h1.2xlarge	8	32
		h1.4xlarge	16	64
		h1.8xlarge	32	128
		h1.16xlarge	64	256

The amount of logging per day and storage capacity vary depending on the license used. Refer to price lists available through your resellers/distributors.

Region support

The following regions are supported. See [Order types on page 8](#).



Instance support may vary depending on the regions.

For detail about regions, refer to [Regions and Availability Zones](#).

Region code	Description
Us-east-1	North Virginia
Us-east-2	Ohio
Us-west-1	North California
Eu-central-1	Frankfurt
Eu-west-1	Ireland
Eu-west-2	London
Eu-west-3	Paris
Ap-southwest-1	Singapore
Ap-southeast-2	Sydney
Ap-south-1	Mumbai
Ap-northeast-1	Tokyo
Ap-northeast-2	Seoul

Region code	Description
Sa-east-1	Sao Paulo
Ca-central-1	Quebec
Us-gov-1	GovCloud

AWS China is supported but does not appear with these regions when you log into the AWS portal. To use AWS resources on AWS China, you must have an AWS China account separate from your global AWS account.

Licensing

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

- [Order types on page 8](#)
- [Creating a support account on page 9](#)

Order types

On AWS, there are usually two order types: bring your own license (BYOL) and pay as you go/on-demand (PAYG).

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 which 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.

PAYG has no licenses. FortiAnalyzer becomes available for use immediately after the instance is created. Term-based prices (hourly or annually) are mentioned in the marketplace product page.

In both BYOL and PAYG, cloud vendors charge separately for resource consumption on computing instances, storage, and so on, without use of software running on top of it (in this case FortiAnalyzer).

For BYOL, you typically order a combination of products and services including support entitlement. PAYG includes support, for which you must contact Fortinet Support with your customer information. See *Support Information* on the [marketplace product page](#).

To purchase PAYG/on-demand, subscribe to the product on the marketplace. FortiAnalyzer will obtain the PAYG/on-demand license from FortiCare using the API. You must contact Fortinet Support with your customer information to obtain support entitlements. See [Creating a support account on page 9](#).

Starting in FortiAnalyzer 7.6.2, a more flexible AWS Marketplace product has been created. The product provides the same functionality and feature set as the previously listed products with added flexibility of scaling the underlying instance up or down to achieve the desired feature capacity to match your requirements without redeploying FortiAnalyzer.

As an example, to have FortiAnalyzer support 2GB/Day logging rate, select an instance size that has 8vCPU and the recommended 6 months of storage space for that log rate (360GB). As your environment grows beyond the 2GB/Day log rate, shutdown the FortiAnalyzer instance and select an instance size that has 16vCPU to support a logging rate up to

100GB/Day. Make sure to add and expand the available disk space as well; in this example, it would require 18TB of storage space.

For up to date on-demand pricing and support details for 7.6 version of FortiAnalyzer, see the following marketplace product pages:

- [Fortinet FortiAnalyzer \(PAYG\) Centralized Logging/Reporting](#)

Use the following chart as a guideline to size your cloud instance to fit your environment; it is recommended to have 180 days of storage:

vCPU Count	Logging Rate	Storage
8vCPU	2GB/Day	360GB
16vCPU	100GB/Day	18TB
32vCPU	500GB/Day	90TB
64vCPU	1500GB/Day	270TB

For up to date on-demand pricing and support details for 7.6, 7.4, 7.2, and 7.0 versions of FortiAnalyzer, see the following marketplace product pages:

- [FortiAnalyzer Centralized Logging/Reporting \(2 managed devices\)](#)
- [FortiAnalyzer Centralized Logging/Reporting \(10 managed devices\)](#)
- [FortiAnalyzer Centralized Logging/Reporting \(30 managed devices\)](#)
- [FortiAnalyzer Centralized Logging/Reporting \(100 managed devices\)](#)
- [FortiAnalyzer Centralized Logging/Reporting \(500 managed devices\)](#)

Creating a support account

FortiAnalyzer for AWS supports the bring-your-own-license (BYOL) and On-demand (PAYG) licensing models. See [Order types on page 8](#).

To make use of Fortinet technical support and ensure products function properly, you must complete certain steps to activate your entitlement. Our support team can identify your registration in the system thereafter.

First, if you do not have a Fortinet account, you can create one at [Fortinet Account Creation](#).

BYOL

Licenses for the BYOL licensing model can be obtained through any Fortinet partner. If you don't have a partner, contact awssales@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.

To register a BYOL license:

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.

Registration Wizard | Registering Product

1 Registration Code > 2 > 3 > 4

Specify Registration Code

Please enter your product serial number, service contract registration code or license certificate number to start the registration:

End User Type

Please specify the type of user who will be using this product:

The product will be used by a government user The product will be used by a non-government user

In this context a government end-user is any central, regional or local government department, agency, or other entity performing governmental functions; including (1) governmental research institutions, (2) governmental corporations or their separate business units which are engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List, and (3) international governmental organizations.

Next

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.

On-demand (PAYG)

To register an on-demand license:

1. Deploy and boot the FortiAnalyzer-VM on-demand Elastic Compute Cloud (EC2) instance.
2. In the AWS management console, view the newly booted instance's instance ID. You can see the account that this instance was launched in by clicking your credentials on the top navigation bar.
3. Obtain the FortiAnalyzer-VM serial number visible at the top of the *Register with FortiCare* section or by running "get system status" via the CLI of the new FAZ/FMG instance during an SSH session.
4. Go to [FortiCloud](#) and create a new account or log in with an existing account.
5. Go to *Asset Management > Register Now* to start the registration process.
6. In the *Registration Code* field, enter the serial number, and select *Next*.
7. In the *AWS account ID* field, enter the account ID that you gathered from AWS.
If you provide an AWS account ID that does not match the one that the FortiAnalyzer reported to FortiCare during its initial bootup, FortiCloud rejects it.
8. Complete the registration.
9. After completing the registration, contact [Fortinet Customer Support](#) to provide your FortiAnalyzer instance's serial number and the email address associated with your Fortinet account.



After registering a PAYG instance, Fortinet servers may take up to 30 minutes to fully recognize the new license.

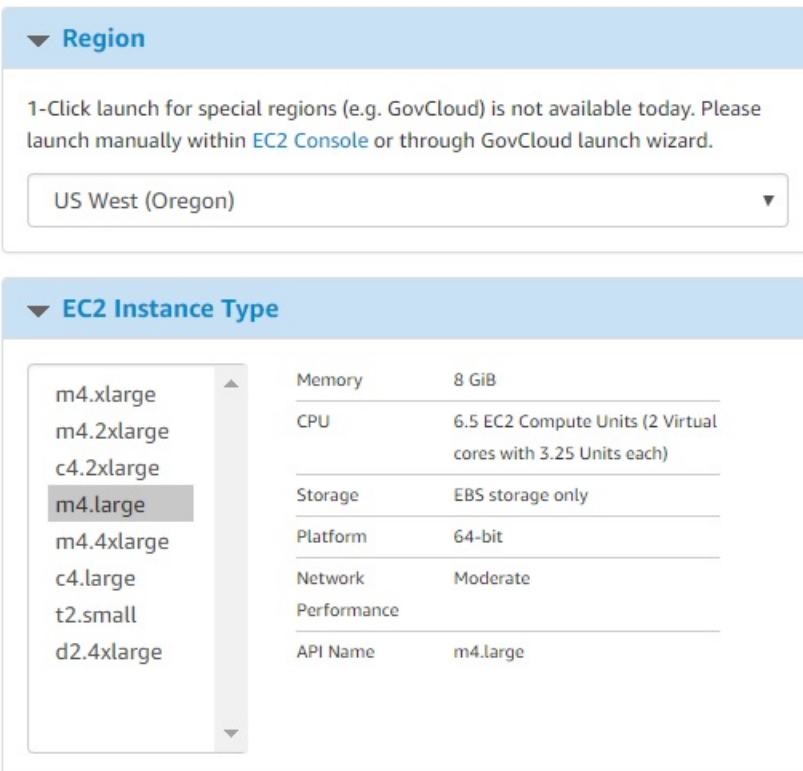
Deploying FortiAnalyzer-VM

You can deploy FortiAnalyzer-VM in one of two ways: through 1-click or manual launch.

Deploying -VM using 1-Click Launch

To deploy -VM using 1-Click Launch:

1. Go to the AWS Marketplace page for FortiAnalyzer-VM [BYOL](#). Select *Continue*.
2. Select the desired region and instance type. Ensure the instance type fits the size of your deployment and potential future growth.



▼ **Region**

1-Click launch for special regions (e.g. GovCloud) is not available today. Please launch manually within [EC2 Console](#) or through GovCloud launch wizard.

US West (Oregon) ▼

▼ **EC2 Instance Type**

m4.xlarge	Memory	8 GiB
m4.2xlarge	CPU	6.5 EC2 Compute Units (2 Virtual cores with 3.25 Units each)
c4.2xlarge	Storage	EBS storage only
m4.large	Platform	64-bit
m4.4xlarge	Network	Moderate
c4.large	Performance	
t2.small	API Name	m4.large
d2.4xlarge		

3. Select a VPC and subnet as required. Under *Security Group*, ensure *Create new based on seller settings* is selected from the dropdown list. The only open port required for the VM's initial configuration is port 443, which allows for an HTTPS connection to the GUI. You can also open the remaining ports to allow for all potential FortiAnalyzer communication.

▼ Security Group

A security group acts as a firewall that controls the traffic allowed to reach one or more instances. Learn more about [Security Groups](#).

You can create a new security group based on seller-recommended settings or choose one of your existing groups.

Create new based on seller settings ▼

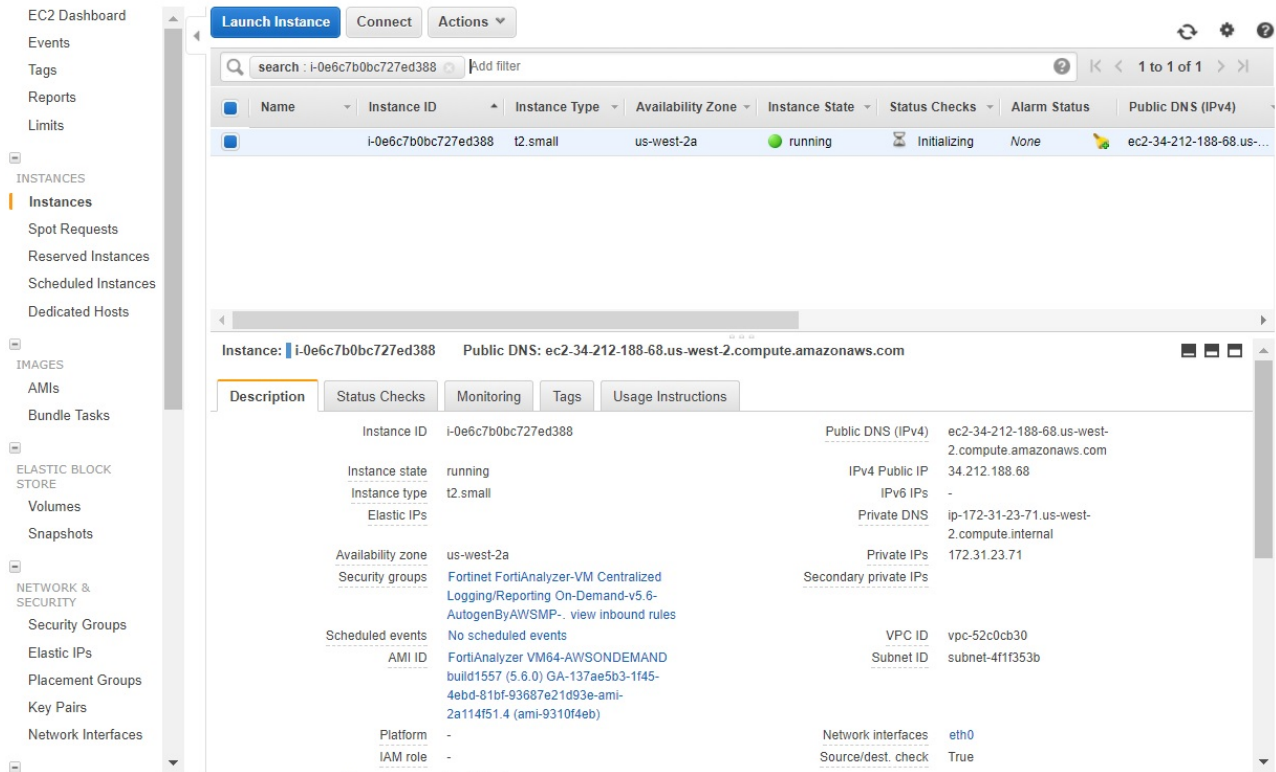
! A new security group will be generated by AWS Marketplace. It is based on recommended settings for Fortinet FortiAnalyzer-VM Centralized Logging/Reporting On-Demand version v5.6 provided by Fortinet Inc..

Connection Method	Protocol	Port Range	Source (IP or Group)
SSH	tcp	22 - 22	Anywhere ▼ 0.0.0.0/0
HTTPS	tcp	443 - 443	Anywhere ▼ 0.0.0.0/0
	tcp	514 - 514	Anywhere ▼ 0.0.0.0/0
	udp	514 - 514	Anywhere ▼ 0.0.0.0/0

! Rules with source of 0.0.0.0/0 allows all IP addresses to access your instance. We recommend limiting access to only known IP addresses.

4. Provide the *Key Pair*, then click *Accept Terms & Launch with 1-Click* to deploy the instance. The next page displays a thank you message, and you also receive an email from AWS Marketplace about the subscription. Close the page and go to the EC2 console.

5. The public DNS address is used to connect to and configure the FortiAnalyzer-VM via the GUI.



To connect to the FortiAnalyzer-VM management GUI, open a web browser and use the public DNS IPv4 address as the URL: `https://<public DNS IPv4 address>`. Log in with the default username admin and the instance ID as the password to configure your FortiAnalyzer-VM.

Deploying FortiAnalyzer-VM using manual launch



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

To deploy FortiAnalyzer-VM using manual launch:

1. Go to the [AWS Marketplace's page for FortiAnalyzer-VM](#). Select *Continue*, then *Manual Launch*. Click the *Launch with EC2 Console* button beside your desired region.
2. Select a supported instance type. Ensure the instance type fits the size of your deployment and potential future growth. Click *Next: Configure Instance Details*.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance types Current generation Show/Hide Columns

Currently selected: m4.large (6.5 ECUs, 2 vCPUs, 2.4 GHz, Intel Xeon E5-2676v3, 8 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input checked="" type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	m4.large	2	8	EBS only	Yes	Moderate	Yes
<input type="checkbox"/>	General purpose	m4.xlarge	4	16	EBS only	Yes	High	Yes
<input type="checkbox"/>	General purpose	m4.2xlarge	8	32	EBS only	Yes	High	Yes

Cancel Previous **Review and Launch** Next: Configure Instance Details

3. Configure the various attributes:

- Network (ensure to select a VPC connected to the Internet gateway; by default, VPCs are connected to the Internet gateway)
- Subnet
- Enable *Auto-assign Public IP*
- Others as needed depending on your IT infrastructure requirements

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of lower prices.

Number of instances [Launch into Auto Scaling Group](#)

Purchasing option Request Spot instances

Network [Create new VPC](#)

Subnet [Create new subnet](#)

Auto-assign Public IP

Placement group

IAM role [Create new IAM role](#)

Shutdown behavior

Enable termination protection Protect against accidental termination

Monitoring Enable CloudWatch detailed monitoring
Additional charges apply.

EBS-optimized instance Launch as EBS-optimized instance

Tenancy
Additional charges will apply for dedicated tenancy.

[Advanced Details](#)

- Continue to adding storage. You can configure the volume type as EBS and the device as /dev/sdb and the size based on your requirements.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/sda1	snap-0424a254dfa93463a	3	General Purpose SSD (GP2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted
EBS	/dev/sdb	Search (case-insensit	550	Magnetic	N/A	N/A	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Cancel Previous **Review and Launch** Next: Add Tags

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

The FortiAnalyzer system reserves a certain portion of disk space for system use and unexpected quota overflow. The remaining space is available for allocation to devices. Reports are stored in the reserved space. The following describes the reserved disk quota relative to the total available disk size (other than the root device):

- Small disk (equal to 500 GB): system reserves 20% or 50 GB of disk space, whichever is smaller.
- Medium disk (less than or equal to 1 TB): system reserves 15% or 100 GB of disk space, whichever is smaller.
- Medium to large disk (less than or equal to 5 TB): system reserves 10% or 200 GB of disk space, whichever is smaller.
- Large disk (less than 5 TB): system reserves 5% or 300 GB of disk space, whichever is smaller.

To add additional storage at this point, follow the instructions in step 3.

5. Click *Next: Tag Instance*. A tag consists of a key-value pair. It is useful to create tags to quickly identify instances in the EC2 console.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maximum)
Name	FortiAnalyzer On-Demand Machine 1
Name	

Add another tag (Up to 50 tags maximum)

Cancel Previous **Review and Launch** Next: Configure Security Group

6. Click *Next: Configure Security Group*. The default provided security group is based on recommended settings for the FortiAnalyzer-VM.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags **6. Configure Security Group** 7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: Create a new security group
 Select an existing security group

Security group name: Fortinet FortiAnalyzer-VM Centralized Logging-Reporting On-Demand-v5-6-Aut

Description: This security group was generated by AWS Marketplace and is based on recom

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
HTTPS	TCP	443	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
Custom TCF	TCP	514	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
Custom UDF	UDP	514	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

Add Rule



Warning 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

Cancel Previous **Review and Launch**

- Click **Review and Launch**. If there is no change needed, click **Launch**.
- You are prompted to choose a key pair. Click the checkbox, then click **Launch Instances**.

Launch Status

✔ **Your instances are now launching**
 The following instance launches have been initiated: i-00592be16f152854f [View launch log](#)

i **Get notified of estimated charges**
 Create [billing alerts](#) to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. [Find out how to connect to your instances.](#)

▼ Getting started with your software

To get started with Fortinet FortiAnalyzer-VM Centralized Logging/Reporting On-Demand

[View Usage Instructions](#)

To manage your software subscription

[Open Your Software on AWS Marketplace](#)

▼ Here are some helpful resources to get you started

- [How to connect to your Linux instance](#)
- [Amazon EC2: User Guide](#)
- [Learn about AWS Free Usage Tier](#)
- [Amazon EC2: Discussion Forum](#)

- The public DNS IPv4 address is used to connect to and configure the FortiAnalyzer-VM via the GUI. You can find the public DNS IPv4 address by locating the FortiAnalyzer-VM instance in the EC2 console. To connect to the FortiAnalyzer-VM management GUI, open a web browser and use the public DNS IPv4 address as the URL: `https://<public DNS IPv4 address>`. Log in with the default username `admin` and the instance ID as the password to configure your FortiAnalyzer-VM.

Adding additional storage (optional)

It is possible to add additional storage to FortiAnalyzer after launch. Create an EBS storage and attach it to the FortiAnalyzer instance on EC2 console, then access FortiAnalyzer via SSH to run the command `exec lvm extend` to add the storage.

For details, refer to [Technical Note : How to extend disk space in FortiAnalyzer-VM](#).

```
FAZVM64-AWSOnDemand # exec lvm info
LVM Status: OK

Disk1 :      Used      83GB
Disk2 : Unavailable  0GB
Disk3 : Unavailable  0GB
Disk4 : Unavailable  0GB
Disk5 :      Unused   356GB
Disk6 :      Unused   232GB
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

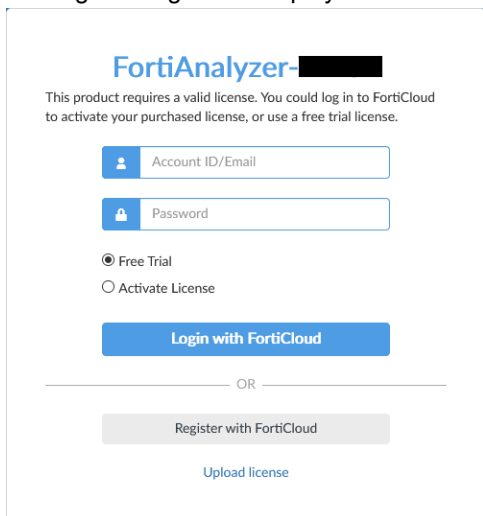
FAZVM64-AWSOnDemand # exec lvm extend
Disk5 will be added to LVM.
Disk6 will be added to LVM.
This operation will need to reboot the system.
Do you want to continue? (y/n)y
```

Log into the FortiAnalyzer GUI and add the volume in *System Settings > ADOMs*. For more information, see the FortiAnalyzer Administration Guide in the [Fortinet Documents Library](#).

Installing a valid license

To activate a license for FortiAnalyzer VM:

1. Connect to the FortiAnalyzer using your browser. The login dialog box is displayed.



2. Take one of the following actions:

Action	Description
Free Trial	<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"> 1. Select <i>Free Trial</i>, and click <i>Login with FortiCloud</i>. 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. 3. Read and accept the license agreement. <p>For more information, see the 7.6 VM Trial License Guide.</p>
Activate License	<p>If you have a license file, you can activate it .</p> <ol style="list-style-type: none"> 1. Select <i>Activate License</i>, and click <i>Login with FortiCloud</i>. 2. Use your FortiCloud account credentials to log in. FortiAnalyzer connects to FortiCloud, and the license agreement is displayed. 3. Read and accept the license agreement.
Upload License	<ol style="list-style-type: none"> 1. Click <i>Browse</i> to upload the license file, or drag it onto the field. 2. Click <i>Upload</i>. After the license file is uploaded, the system will restart to verify it. This may take a few moments. <hr/> <div style="display: flex; align-items: center;"> <p>To download the license file, go to the Fortinet Technical Support site (https://support.fortinet.com/), and use your FortiCloud credentials to log in. Go to <i>Asset Managmeent > Products > Product List</i>, then click the product serial number.</p> </div> <hr/>

3. Once registration is complete, log into the FortiAnalyzer-VM with the username *admin* and the supplied temporary password.

Configuring your FortiAnalyzer-VM

Click the help icon in the GUI banner to access the FortiAnalyzer online help and basic setup video. Refer to these and the [FortiAnalyzer Administration Guide](#) for more detailed configuration.

PAYG instance scaling

Starting in 7.6.2, FortiAnalyzer-VM now supports increasing or decreasing feature capacity when scaling the underlying instance size up or down.

The examples in this section assume that default settings have been used when deploying the FortiAnalyzer-VM.

See the following examples for:

- [Scaling up the FortiAnalyzer instance on page 21](#)
- [Scaling down the FortiAnalyzer instance on page 26](#)

Scaling up the FortiAnalyzer instance

This section assumes you have deployed a single VM of the Fortinet FortiAnalyzer (PAYG) Centralized Logging/Reporting and are ready to scale up the instance to increase the feature capacity to meet the needs of your environment.

For more information about selecting the size of the instance type and achieving your desired feature capacity see [Order types on page 8](#).



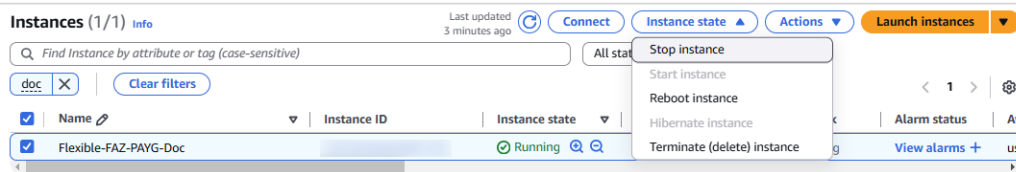
This process requires shutting down the VM to change the instance. Perform all necessary steps to ensure your FortiAnalyzer-VM is backed up and any downtime is scheduled.

In this example the following the FortiAnalyzer-VM instance is currently deployed with a m6i.2xlarge or 8vCPU instance type; based on this instance's vCPU count, it can support 2 GB/Day logging rate.

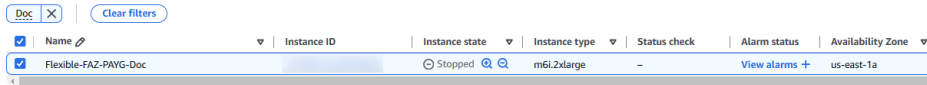
System Information		License Information	
Host Name	Flexible-FAZ-PAYG-Doc	Outbreak...	Not Licensed
Serial Num...	FAZAWSTA25	Security ...	Not Licensed
Platform Ty...	FAZVM64-AWSONdemand	Industrial...	Not Licensed
HA Status	Standalone	Security ...	Not Licensed
System Time	Mon Jan 27 12:11:05 2025 PST	Storage C...	Not Licensed
Firmware V...	v7.6.2 build3415 (Feature)	Logging	
System Con...	Last Backup: N/A	Devices/...	0 / 100 (0.0%)
Current Ad...	admin / 1 in total	GB/Day	0.0 / 2 (0.0%)
Up Time	7 minutes 32 seconds	Update Servers	

To scale up the instance:

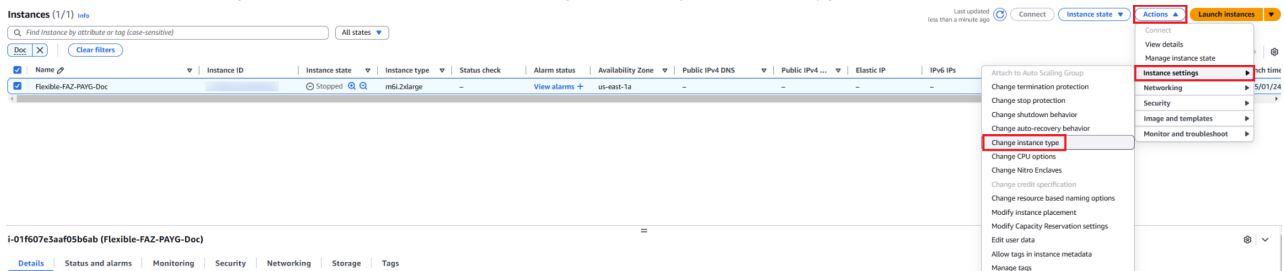
1. Log in to the AWS console to access the FortiAnalyzer-VM PAYG instance.
2. To shutdown the instance, select the instance and then, from the *Instance state* dropdown, select *Stop instance*.



3. Wait for the instance to stop. The *Instance state* will change to *Stopped*.



4. From the *Actions* dropdown, select *Instance Settings > Change instance type*.



5. In the *Change instance type* dialog, change to the new instance type. In this example, change to an instance type of 4xlarge.
 - a. In the *New instance type* field, select *m6i.4xlarge*.
 - b. Click *Change*.

Change instance type [Info](#) | [Get advice](#)

You can change the instance type only if the current instance type and the instance type that you want are compatible.

Instance ID (Flexible-FAZ-PAYG-Doc)

Current instance type
m6i.2xlarge

New instance type

EBS-optimized
EBS-optimized is enabled by default for this instance type

▼ Instance type comparison

Attribute	m6i.2xlarge	m6i.4xlarge
On-Demand Linux pricing	0.3840 USD per Hour	0.7680 USD per Hour
On-Demand Windows pricing	0.7520 USD per Hour	1.5040 USD per Hour
vCPUs	8 (4 core)	16 (8 core)
Memory (MiB)	32768	65536
Storage (GB)	-	-
Supported root device types	ebs	ebs
Network performance	Up to 12.5 Gigabit	Up to 12.5 Gigabit
Architecture	x86_64	x86_64
Burstable	false	false
Free-tier eligible	false	false
Current generation	true	true

[Compare more instance type attributes](#)

Advanced details

CPU options | [Info](#)

None

Specify CPU options
Configure CPUs for your instance to optimize performance and save on licensing costs.

[Cancel](#) Change

6. After the instance type change has been completed, from the *Instance state* dropdown, select *Start instance*.

The screenshot shows the AWS Management Console 'Instances' page. At the top right, the 'Instance state' dropdown menu is open, and the 'Start instance' option is highlighted with a red rectangular box. Below the dropdown, a table lists instance details for 'Flexible-FAZ-P...'. The instance is currently in a 'Stopped' state and has been changed to 'm6i.4xlarge'.

7. Add more disk space as needed.

In this example, add the recommended six months of log storage for the new logging rate of 100GB/Day or 18TB. Two 9TB disks must be created for this example.

- a. Create the disk in *EC2 > EBS > Volumes > Create Volume*.
The *Create volume* dialog opens.
- b. Configure the volume settings such as *Availability Zone* to match the availability zone or location where your instance is running for best performance. Other settings can be adjusted for cost and/or speed as needed.

- c. To save the configuration, click *Create volume*.

Create volume [info](#)
 Create an Amazon EBS volume to attach to any EC2 instance in the same Availability Zone.

Volume settings

Volume type [info](#)
 General Purpose SSD (gp2)

Size (GiB) [info](#)
9000
Min: 1 GiB, Max: 16384 GiB.

IOPS [info](#)
 16000
16000 IOPS for volume sizes greater than 5333 GiB.

Throughput (MiB/s) [info](#)
 Not applicable

Availability Zone [info](#)
 us-east-1a

Snapshot ID - optional [info](#)
 Don't create volume from a snapshot

Encryption [info](#)
Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instances.
 Encrypt this volume

Tags - optional [info](#)
 A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
 No tags associated with the resource.
[Add tag](#)
You can add 50 more tags.

Snapshot summary [info](#) [refresh](#)
Click refresh to view backup information
 The volume type that you select and the tags that you assign determine whether the volume will be backed up by any Data Lifecycle Manager policies.

[Cancel](#) Create volume

- d. Repeat the above steps to create the second disk.
- e. To add each disk to the FortiAnalyzer-VM instance, from the *Actions* menu, select *Attach Volume*.
 The *Attach volume* dialog opens.
- f. In the *Instance* field, select the FortiAnalyzer-VM Instance
- g. From the *Device name* dropdown, select the device name.
- h. Click *Attach Volume*.

Attach volume [info](#)
 Attach a volume to an instance to use it as you would a regular physical hard disk drive.

Basic details

Volume ID
[vol-020be02e75e53987e](#)

Availability Zone
 us-east-1a

Instance [info](#)
(Flexible-FAZ-PAYG-Doc) (stopped)
Only instances in the same Availability Zone as the selected volume are displayed.

Device name [info](#)
 /dev/sdc
Recommended device names for Linux: /dev/sda1 for root volume, /dev/sd[f-g] for data volumes.

ⓘ Newer Linux kernels may rename your devices to /dev/xvdf through /dev/xvdp internally, even when the device name entered here (and shown in the details) is /dev/sdf through /dev/sdp.

[Cancel](#) Attach volume

- 8. Once the instance has started and you have logged in, expand the disk to use the added storage space.



To use the added storage in the FortiAnalyzer-VM, follow the steps in [Adding additional storage \(optional\)](#) on page 18.

- a. In the FortiAnalyzer-VM CLI, enter the following command to verify the new disks have registered correctly:

```
execute lvm info
```

- b. In the FortiAnalyzer-VM CLI, enter the following command to prepare the new storage for use:

```
execute lvm extend
```

```

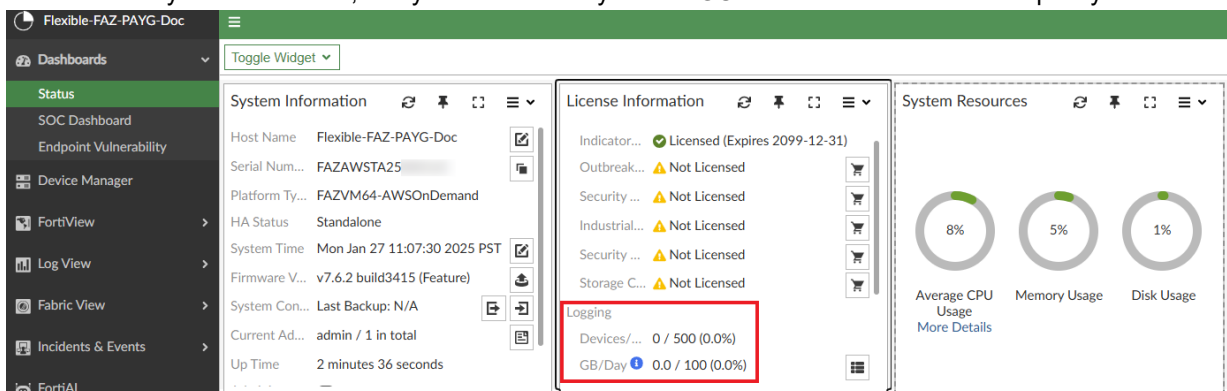
exe lvm extend

Connected
Flexible-FAZ-PAYG-Doc # execute lvm info
LVM Status: OK
LVM Size: 360GB
File System: ext4 353GB

Disk1 :      Unused      9000GB
Disk2 :      Unused      9000GB
Disk3 :      Used        360GB
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

Flexible-FAZ-PAYG-Doc # exe lvm extend
This operation will need to reboot the system.
And all data in unused disks will be lost.
Do you want to continue? (y/n)y
    
```

- c. After FortiAnalyzer-VM restarts, verify in the FortiAnalyzer-VM GUI that the desired feature capacity is shown.



- d. In the FortiAnalyzer-VM CLI, enter the following command again to verify the disks are now in a "Used" state:

```
execute lvm info
```

```
Connected
Flexible-FAZ-PAYG-Doc # exe lvm info
LVM Status: OK
LVM Size: 18360GB
File System: ext4 18071GB

Disk1 :      Used      9000GB
Disk2 :      Used      9000GB
Disk3 :      Used      360GB
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

Flexible-FAZ-PAYG-Doc # █
```

Scaling down the FortiAnalyzer instance

In this example we will be reducing the instance size or scaling down a FortiAnalyzer-VM to better fit a smaller environment.

This example assumes that the FortiAnalyzer-VM has been deployed from the new Fortinet FortiAnalyzer (PAYG) Logging/Reporting and is running on an instance with 16vCPU.



This process requires shutting down the VM to change the instance. Perform all necessary steps to ensure your FortiAnalyzer-VM is backed up and any downtime is scheduled.

To scale down the instance:

1. Log in to the AWS EC2 console to access the FortiAnalyzer-VM PAYG instance.
2. To shutdown the instance, select the instance and then, from the *Instance state* dropdown, select *Stop instance*.
3. Wait for the instance to stop. The *Instance state* will change to *Stopped*.
4. From the *Actions* dropdown, select *Instance Settings > Change instance type*.
 - a. In the *Change instance type* dialog, change to the new instance type.
In this example, change to an instance type of 2xlarge.
 - b. In the *New instance type* field, select *m6i.2xlarge*.
 - c. Click *Change*.

Change instance type [Info](#) | [Get advice](#)

You can change the instance type only if the current instance type and the instance type that you want are compatible.

Instance ID (Flexible-FAZ-PAYG-Doc)

Current instance type
m6i.4xlarge

New instance type

EBS-optimized
EBS-optimized is enabled by default for this instance type

▼ Instance type comparison

Attribute	m6i.4xlarge	m6i.2xlarge
On-Demand Linux pricing	0.7680 USD per Hour	0.3840 USD per Hour
On-Demand Windows pricing	1.5040 USD per Hour	0.7520 USD per Hour
vCPUs	16 (8 core)	8 (4 core)
Memory (MiB)	65536	32768
Storage (GB)	-	-
Supported root device types	ebs	ebs
Network performance	Up to 12.5 Gigabit	Up to 12.5 Gigabit
Architecture	x86_64	x86_64
Burstable	false	false
Free-tier eligible	false	false
Current generation	true	true

[Compare more instance type attributes](#)

Advanced details

CPU options | [Info](#)

None

Specify CPU options
Configure CPUs for your instance to optimize performance and save on licensing costs.

[Cancel](#) Change

5. After the instance type change has been completed, from the *Instance state* dropdown, select *Start instance*.
6. After the instance is started, log in to verify the desired capacity is shown in the GUI.

The screenshot shows the FortiAnalyzer GUI for instance Flexible-FAZ-PAYG-Doc. The left sidebar contains navigation options like Dashboards, Status, SOC Dashboard, Endpoint Vulnerability, Device Manager, FortiView, Log View, Fabric View, Incidents & Events, and FortiAI. The main content area is split into two panels: System Information and License Information. The System Information panel shows details like Host Name, Serial Number, Platform Type, HA Status, System Time, Firmware Version, System Connection, Current Admins, and Up Time. The License Information panel shows various license statuses (Not Licensed) and a 'Logging' section which is highlighted with a red box. The Logging section displays 'Devices/... 0 / 100 (0.0%)' and 'GB/Day 0.0 / 2 (0.0%)'.

HA for FortiAnalyzer on AWS

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

1. [Deploying FortiAnalyzer HA instances on AWS on page 28](#)
2. [Configuring FortiAnalyzer HA on page 29](#)

Deploying FortiAnalyzer HA instances on AWS

To deploy FortiAnalyzer instances on AWS:

1. In AWS, create the FortiAnalyzer instances in one VPC in the same or different subnet.
2. Allocate an Elastic 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.
 - The External VIP is assigned to an instance when its mode is transitioned to Primary by the fazutil to call AWS EC2 APIs within the instance.
3. Assign an existing IAM role or create one with the permissions required to assign/re-assign IP addresses for the FortiAnalyzer instance.
 - a. Assign said IAM role to both FortiAnalyzer instances by going to the FortiAnalyzer *Instance Summary* > *Actions* > *Security* > *Modify IAM Role*.
 - b. Select the previously mentioned IAM role, and click Save.

The screenshot shows the AWS Management Console interface for an EC2 instance. The title is "Instance summary for i-0c5a86bf45ae18cf1 (pbrk-faz-ha-isnt1)". Below the title are buttons for "Connect", "Instance state", and "Actions". The "Actions" menu is expanded, showing options like "Connect", "Manage instance state", "Instance settings", "Networking", "Security", "Image and templates", and "Monitor and troubleshoot". The "Security" option is selected, and a sub-menu is visible with "Change security groups", "Get Windows password", and "Modify IAM role". The "Modify IAM role" option is highlighted. On the left, the instance details are partially visible: Instance ID is i-0c5a86bf45ae18cf1 (pbrk-faz-ha-isnt1), IPv6 address is -, and Private IPv4 DNS is ip-10-90-200-122.us-west-2.

- c. In cases where an IAM role assignment cannot be completed, you can add the AWS Access ID and Shared Access Key for an IAM user with the appropriate access using the FortiAnalyzer CLI. In the FortiAnalyzer CLI, enter the following:

```
config system ha
  set aws-access-key-id <access_key_id>
  set aws-secret-access-key <secret_key>
end
```

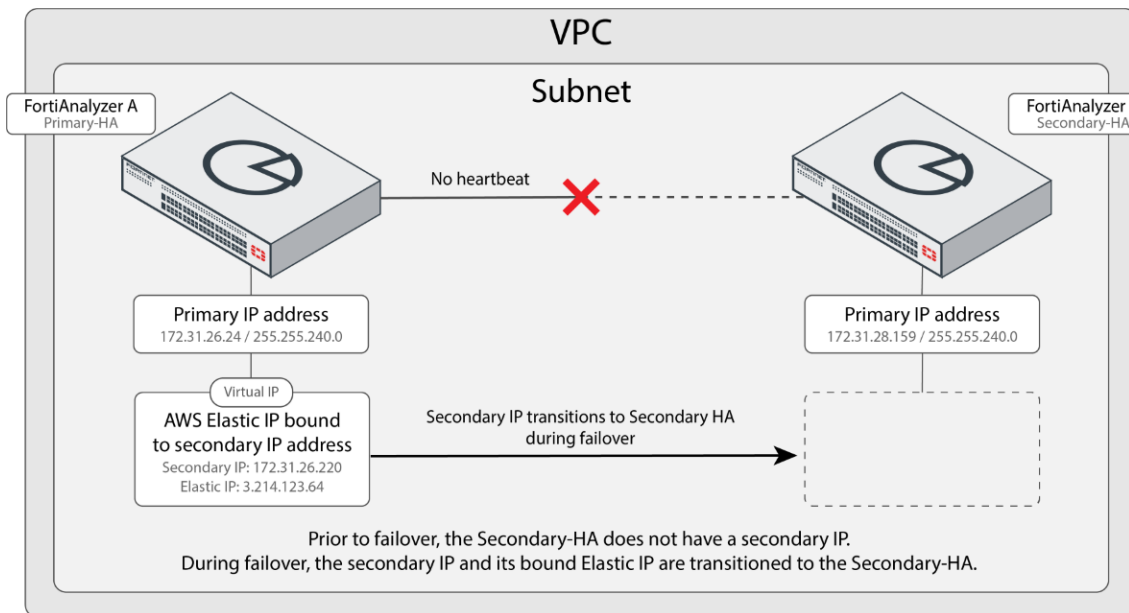
4. Create an *Inbound Rule* on the *AWS Network Security Group* assigned to the FortiAnalyzer HA interface.
 - a. To allow the keepalived adverts from the Primary:
 - On the Primary instance, allow IP access to protocol 112 (VRRP protocol) from the local subnet of the Secondary instance and vice versa.
 - If both instances are in the same subnet, allow IP Protocol 112 from the same local subnet.
 - b. To allow initial logs sync:
 - On the Primary instance, allow inbound TCP traffic destined for port 514, originating from the local subnet of the Secondary instance and vice versa.
 - c. To allow for configuration sync:
 - On the Primary instance, allow inbound TCP traffic destined for port 5199, originating from the local subnet of the Secondary instance and vice versa.

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 secondary IP is transitioned from FortiAnalyzer-A to FortiAnalyzer-B, and can be accessed from the internet using the same Elastic IP. Neither the secondary IP or Elastic IP addresses change during transition.

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



Configuring FortiAnalyzer HA

To configure FortiAnalyzer HA:

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

2. Import the Amazon Root CA to FortiAnalyzer. In order for the fazutil to be able to call EC2 API successfully, you must manually import the Amazon Cloud CA Certificates to each FortiAnalyzer instance. For more information on Amazon Trust Services, see <https://www.amazontrust.com/repository/>.
 - a. Go to *System Settings > Certificates*.
 - b. From the *Create New/Import* dropdown, select *CA Certificate*
 - c. Browse to the file location and select it, or drag-and-drop it into the *Certificate File* field.
 - d. Click *OK*.

Change log

Date	Change Description
2024-07-29	Initial release.
2025-02-18	Updated Order types on page 8. Added PAYG instance scaling on page 21.
2025-03-14	Updated Deploying FortiAnalyzer HA instances on AWS on page 28. Updated Instance type support on page 4.



www.fortinet.com

Copyright© 2025 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.