



FortiAnalyzer - AWS Cookbook

Version 6.4

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<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>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



March 9, 2023

FortiAnalyzer 6.4 AWS Cookbook

05-640-620617-20230309

TABLE OF CONTENTS

About FortiAnalyzer for AWS	4
Instance type support	4
BYOL	5
PAYG	5
Region support	5
Licensing	6
Order types	6
Creating a support account	7
Registering and downloading licenses	7
Deploying FortiAnalyzer-VM	9
Deploying FortiAnalyzer-VM using 1-Click Launch	9
Deploying FortiAnalyzer-VM using manual launch	12
Adding additional storage (optional)	16
Installing a valid license	17
Uploading the license file via the GUI	20
Configuring your FortiAnalyzer-VM	21
HA for FortiAnalyzer on AWS	22
Deploying FortiAnalyzer HA instances on AWS	22
Configuring FortiAnalyzer HA	23
Change log	25

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 as opposed to on-demand, which is an hourly subscription. 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 FortiAnalyzer-VM using 1-Click Launch on page 9](#)
- [Deploying FortiAnalyzer-VM using manual launch on page 12](#) (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 16](#).

FortiAnalyzer-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 FortiAnalyzer-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. BYOL and PAYG have different kinds of limits.

Supported instances in the AWS marketplace listing may be changed without notice and may vary between BYOL and PAYG models. See [Order types on page 6](#).

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.

BYOL

- t3.large / t3.xlarge / t3.2xlarge
- m4.large / m4.xlarge / m4.2xlarge / m4.4xlarge / m4.10xlarge / m4.16xlarge
- m5.large / m5.xlarge / m5.2xlarge / m5.4xlarge / m5.8xlarge / m5.12xlarge / m5.16xlarge / m5.24xlarge
- c4.2xlarge / c4.4xlarge / c4.8xlarge
- c5.xlarge / c5.2xlarge / c5.4xlarge / c5.9xlarge / c5.12xlarge / c5.18xlarge / c5.24xlarge
- h1.2xlarge / h1.4xlarge / h1.8xlarge / h1.16xlarge
- d2.xlarge / d2.2xlarge / d2.4xlarge / d2.8xlarge

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

PAYG

The FortiAnalyzer PAYG license Type is determined by the number of managed devices it can support. Each PAYG License Type in FortiAnalyzer has a Pre-defined limit for storage capacity and maximum logging per day.

Each license type has its own set of supported AWS Instance Types as shown below:

License Type	Storage Capacity	Logging/Day (Gb/Day)	Supported Instance types
2 Managed Devices	500 GB	1 Gb/Day	m5.large / m5.xlarge
10 Managed Devices	1 TB	1 Gb/Day	t2.medium / t2.large / t2.xlarge m5.large / m5.xlarge / m5.2xlarge / m5.4xlarge / m5.12xlarge h1.2xlarge / h1.4xlarge / h1.8xlarge
30 Managed Devices	3 TB	5 Gb/Day	t2.medium / t2.large / t2.xlarge / t2.2xlarge
100 Managed Devices	10 TB	25 Gb/Day	m5.large / m5.xlarge / m5.2xlarge / m5.4xlarge / m5.12xlarge / m5.24xlarge
500 Managed Devices	24 TB	100 Gb/Day	h1.2xlarge / h1.4xlarge / h1.8xlarge / h1.16xlarge

Region support

The following regions are supported on both BYOL and PAYG deployments. See [Order types on page 6](#).



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
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 6](#)
- [Creating a support account on page 7](#)
- [Registering and downloading licenses on page 7](#)

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 7](#).

For the latest on-demand pricing and support details, see the following marketplace product pages:

- [FortiAnalyzer Centralized Security Management \(Max 2 managed devices\)](#)
- [FortiAnalyzer Centralized Security Management \(Max 10 managed devices\)](#)
- [FortiAnalyzer Centralized Security Management \(Max 30 managed devices\)](#)
- [FortiAnalyzer Centralized Security Management \(Max 100 managed devices\)](#)
- [FortiAnalyzer Centralized Security Management \(Max 500 managed devices\)](#)

Creating a support account

FortiAnalyzer for AWS supports both on-demand (PAYG) and bring-your-own-license (BYOL) licensing models. See [Order types on page 6](#).

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.

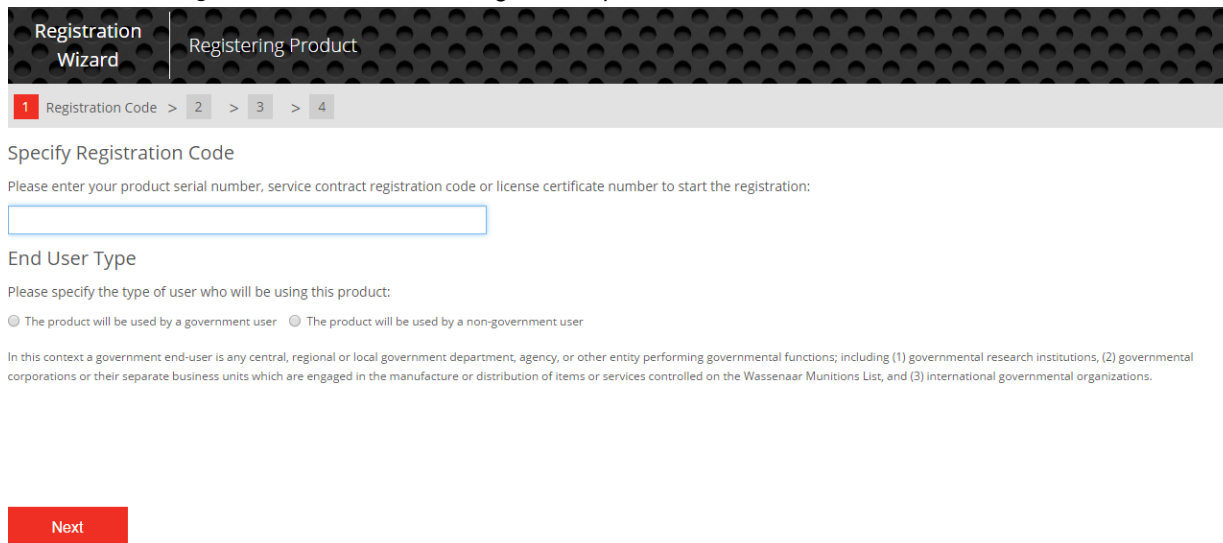
First, if you do not have a Fortinet account, you can create one at [Fortinet Account Creation](#).

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 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.

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 includes a text prompt: 'Please enter your product serial number, service contract registration code or license certificate number to start the registration:'. There is a text input field below this prompt. The next section is 'End User Type', with a prompt: 'Please specify the type of user who will be using this product:'. It contains 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, there 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-VM

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

Deploying FortiAnalyzer-VM using 1-Click Launch

To deploy FortiAnalyzer-VM using 1-Click Launch:

1. Go to the AWS Marketplace page for FortiAnalyzer-VM [on-demand](#) or [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. For an on-demand instance, t2.small is intended for free preview and its device support is limited.

▼ **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. For a BYOL instance, 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.



Thank you for launching Fortinet FortiAnalyzer-VM Centralized Logging/Reporting On-Demand

An instance of this software is now deploying on EC2.

You can check the status of this instance on [EC2 Console](#). You can also view all instances on [Your Software](#) page.

Software and AWS hourly usage fees apply when the instance is running and will appear on your monthly bill.

Next Steps:

- The software will be ready in a few minutes.

Software Installation Details

Product	Fortinet FortiAnalyzer-VM Centralized Logging/Reporting On-Demand
Version	v5.6
Region	us-west-2
EC2 Instance Type	t2.small
VPC	vpc-52c0cb30
Subnet	subnet-4f1f353b
Security Group	Create new security group based on seller settings
Key Pair	fmg54-test

[Return to Launch Page](#)

Related Links

[AWS Management Console](#)

[Your Software](#)

[Continue shopping on AWS Marketplace](#)

Service Catalog

Click [here](#) for instructions to deploy Marketplace products in [AWS Service Catalog](#).

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

The screenshot displays the AWS Management Console interface for an EC2 instance. The left sidebar shows the navigation menu with categories like INSTANCES, IMAGES, ELASTIC BLOCK STORE, and NETWORK & SECURITY. The main content area shows the instance details for **i-0e6c7b0bc727ed388**. The instance is a **t2.small** type in the **us-west-2a** availability zone, with a state of **running**. The public DNS (IPv4) address is **ec2-34-212-188-68.us-west-2.compute.amazonaws.com**. The instance is associated with the **Fortinet FortiAnalyzer-VM Centralized Logging/Reporting On-Demand-v5.6-AMI**.

Category	Property	Value
Instance Details	Instance ID	i-0e6c7b0bc727ed388
	Instance state	running
	Instance type	t2.small
	Elastic IPs	-
Availability	Availability zone	us-west-2a
	Security groups	Fortinet FortiAnalyzer-VM Centralized Logging/Reporting On-Demand-v5.6-AutogenByAWSMP- view inbound rules
Events	Scheduled events	No scheduled events
	AMI ID	FortiAnalyzer VM64-AWSONDEMAND build1557 (5.6.0) GA-137ae5b3-1f45-4ebd-81bf-93687e21d93e-ami-2a114f51.4 (ami-9310f4eb)
Platform	Platform	-
	IAM role	-
Public DNS (IPv4)	Public DNS (IPv4)	ec2-34-212-188-68.us-west-2.compute.amazonaws.com
	IPv4 Public IP	34.212.188.68
Private DNS	Private DNS	ip-172-31-23-71.us-west-2.compute.internal
	Private IPs	172.31.23.71
VPC	VPC ID	vpc-52c0cb30
	Subnet ID	subnet-4f1f353b
Network	Network interfaces	eth0
	Source/dest. check	True

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

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 an instance type. Ensure the instance type fits the size of your deployment and potential future growth. Note `t2.small` is intended for free preview and its device support is limited to FortiGate-90 or smaller and FortiGate-VM 1vCPU models (VM00 and VM01). 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 adv

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](#)

4. 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

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 (less than or 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-Auto

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

7. Click **Review and Launch**. If there is no change needed, click **Launch**.

8. 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](#)

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

9. 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.

System Settings admin

Edit Log Storage Policy - ADOM : root

Data Policy

Keep Logs for Analytics	60	Days
Keep Logs for Archive	365	Days

Disk Utilization

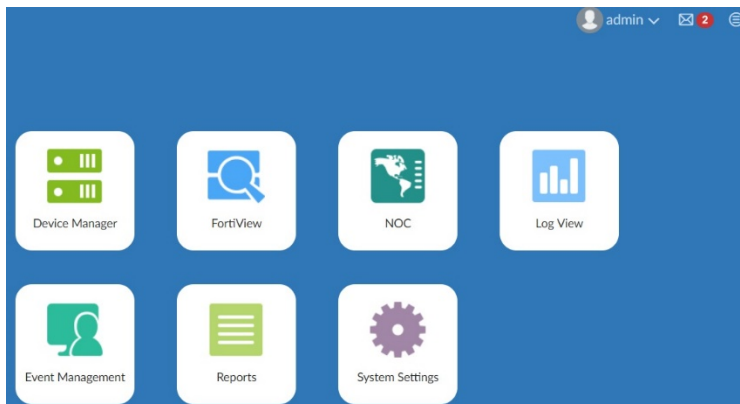
Maximum Allowed	65126	MB	Out of Available: 537.8 GB <input type="checkbox"/> Modify
Analytics : Archive	70%	30%	
Alert and Delete When Usage Reaches	90%		

*If analytic or archive log usages exceed the configured disk quota before the retention period expires, the oldest logs will be deleted.

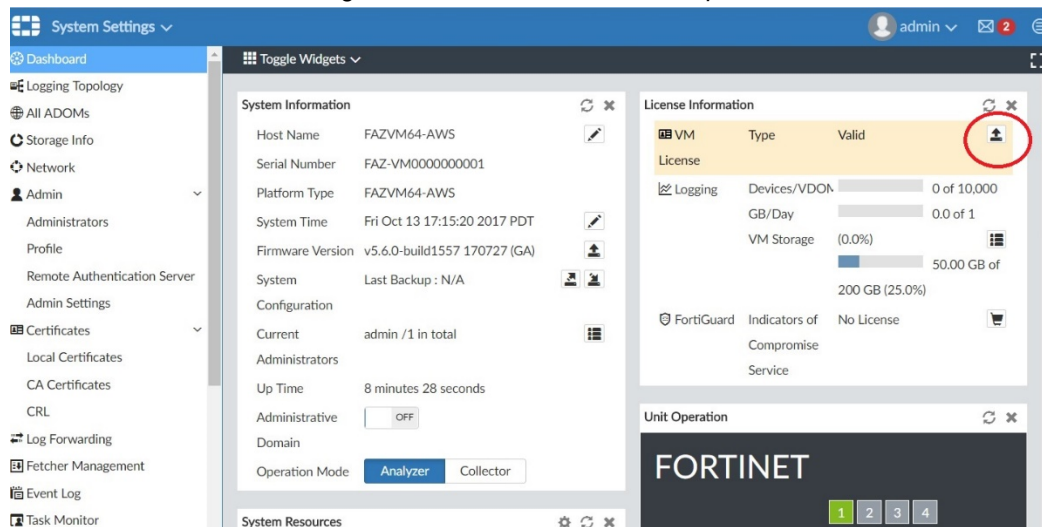
OK Cancel

Installing a valid license

1. By default, the license expires 14 days after deployment. Go to *System Settings*.



2. In the *License Information* widget on the *Dashboard*, click the *Upload License* button.

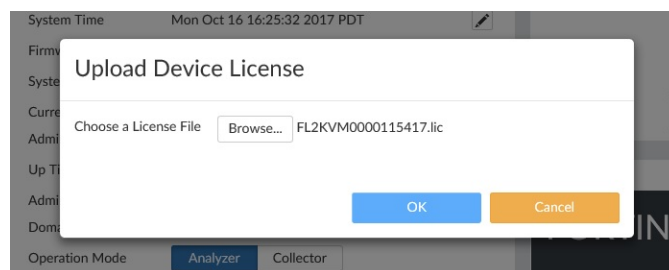
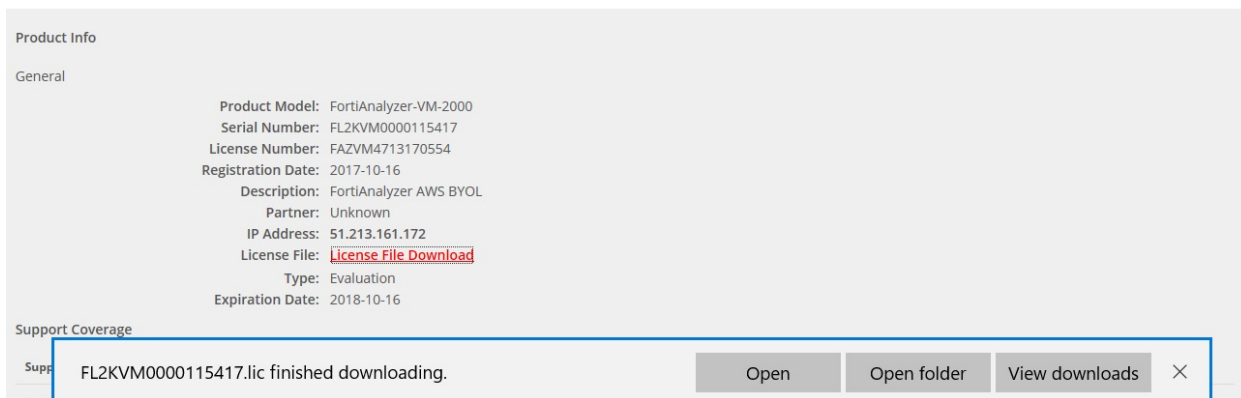


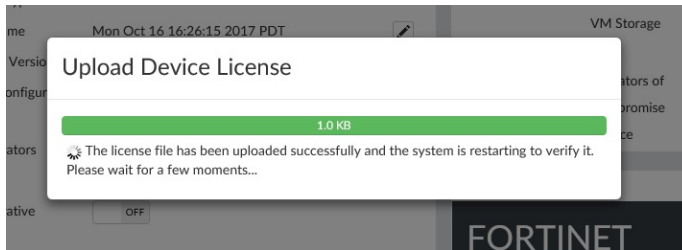
3. In the *Upload Device License* window, click *Browse*, locate the license file (.lic) on your computer, then click *OK* to upload the license file. A reboot message is shown, then the FortiAnalyzer VM system reboots and loads the license file. The license file is available once you register on the Fortinet Support Portal.



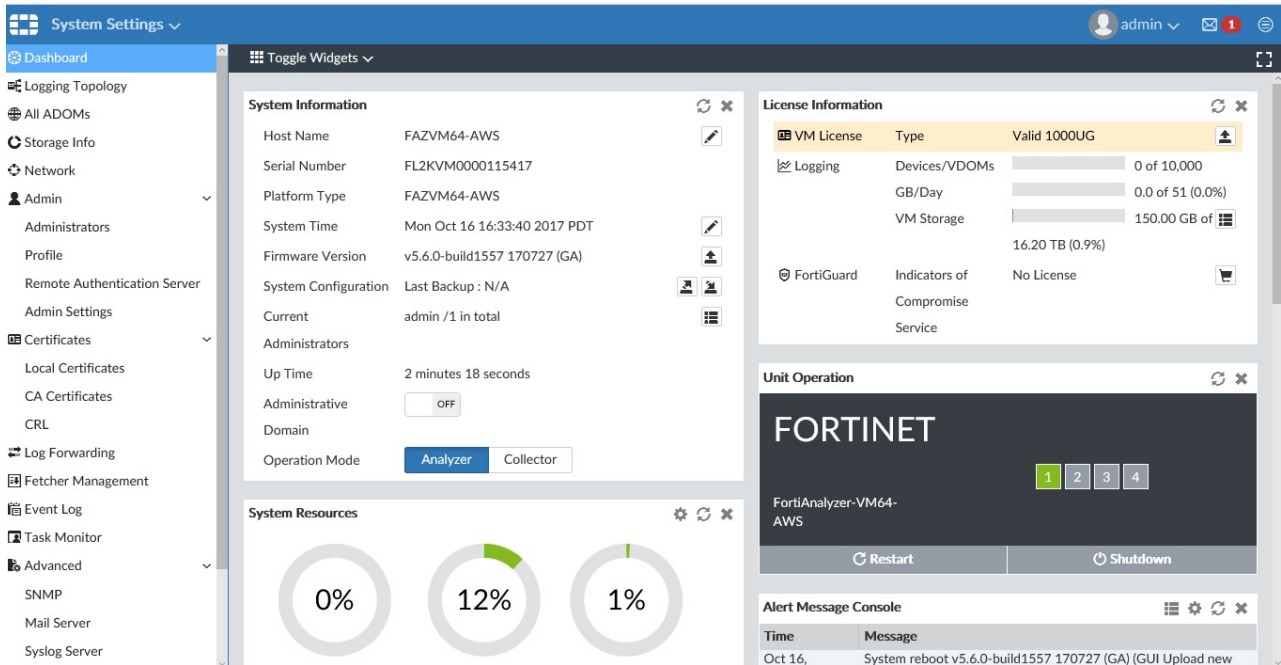
Registration Completed

Thank you for choosing this Fortinet product. Your registration process has completed successfully. Please be aware that the registration information may not reflect on your product immediately, a delay (up to 4 hours) can occur.





- Refresh the browser and log back into the FortiAnalyzer VM with the username *admin*. The registration status appears differently than before, reflecting the license in the *License Information* widget once the license has been validated.



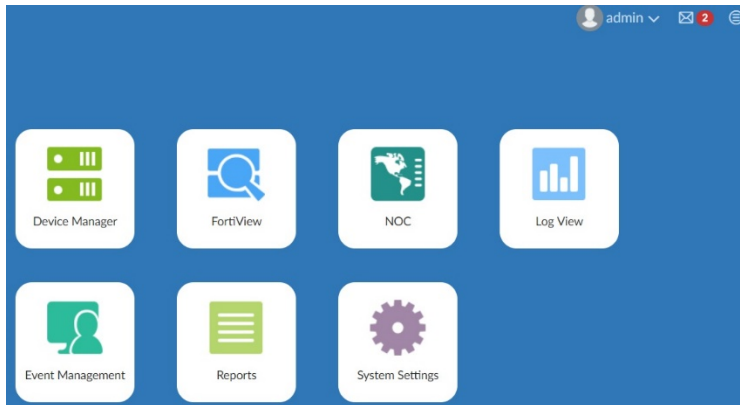
As part of the license validation process, the FortiAnalyzer VM compares its IP address with the IP information in the license file. If a new license file has been imported or the FortiAnalyzer's IP address has been changed, the FortiAnalyzer VM must be rebooted for the system to validate the change and operate with a valid license.



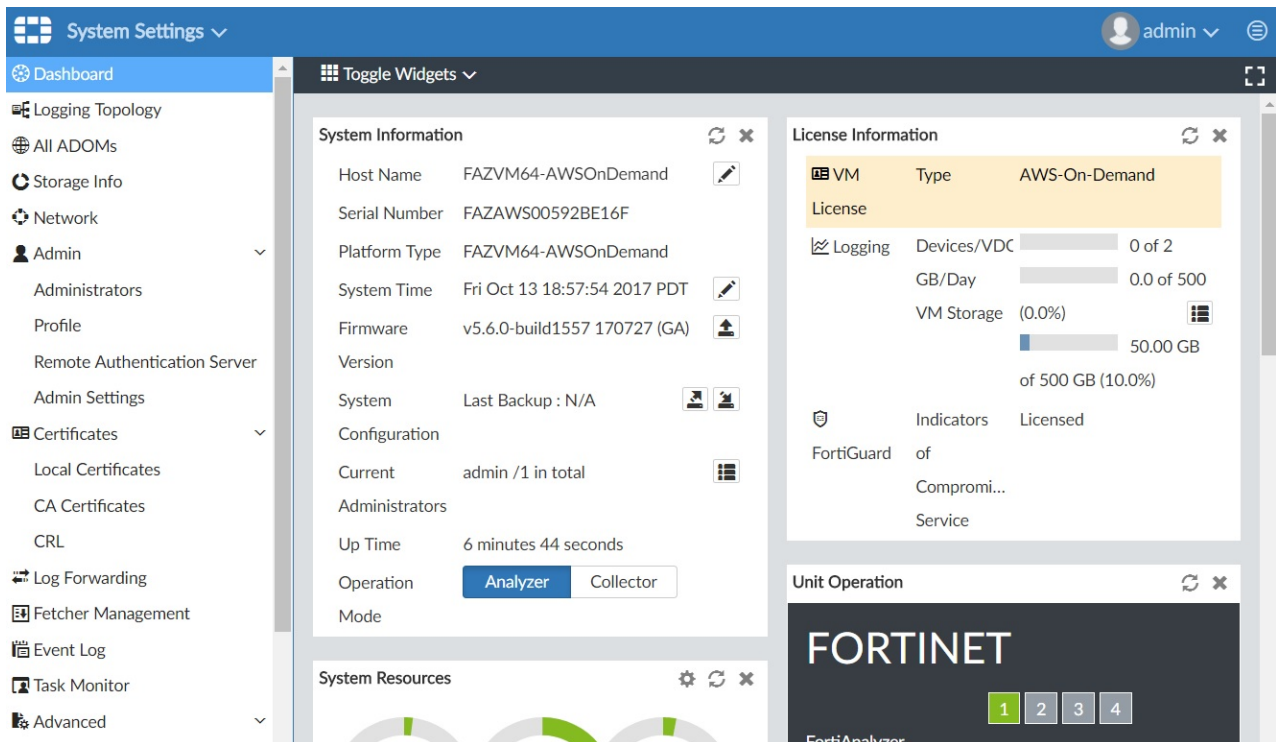
If the IP address in the license file and the IP configured in the FortiAnalyzer-VM do not match, you receive an error message when you log back into the VM. If this occurs, you must change the IP address in the Fortinet Customer Service & Support portal to match the management IP and re-download the license file. After an invalid license file has been loaded onto the FortiAnalyzer-VM, the GUI is locked until a valid license file is uploaded. You can upload a new license file via the CLI.

Uploading the license file via the GUI

1. Navigate to *System Settings*.



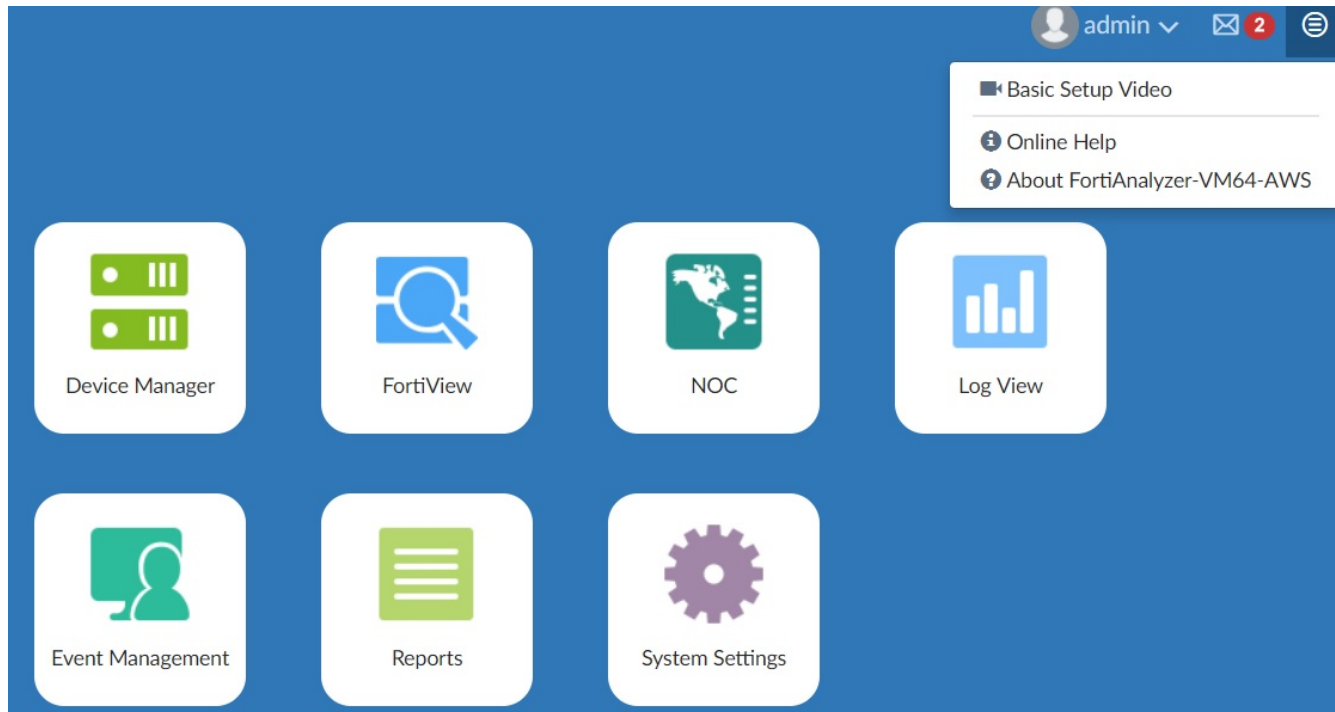
2. The *License Information* widget on the *Dashboard* displays as *AWS-On-Demand*.



Unlike perpetual BYOL licensing, there is no interface to upload a license file for on-demand use. For on-demand deployments, contact Fortinet Customer Support as indicated on the AWS Marketplace product listing page and notify your deployment. When contacting Fortinet Support, be ready to provide your FortiAnalyzer VM instance's serial number and your Fortinet account's email ID.

Configuring your FortiAnalyzer-VM

Click the top-right menu icon to access the FortiAnalyzer online help and basic setup video. Refer to these and the [FortiAnalyzer Administration Guide](#) for more detailed configuration.



HA for FortiAnalyzer on AWS

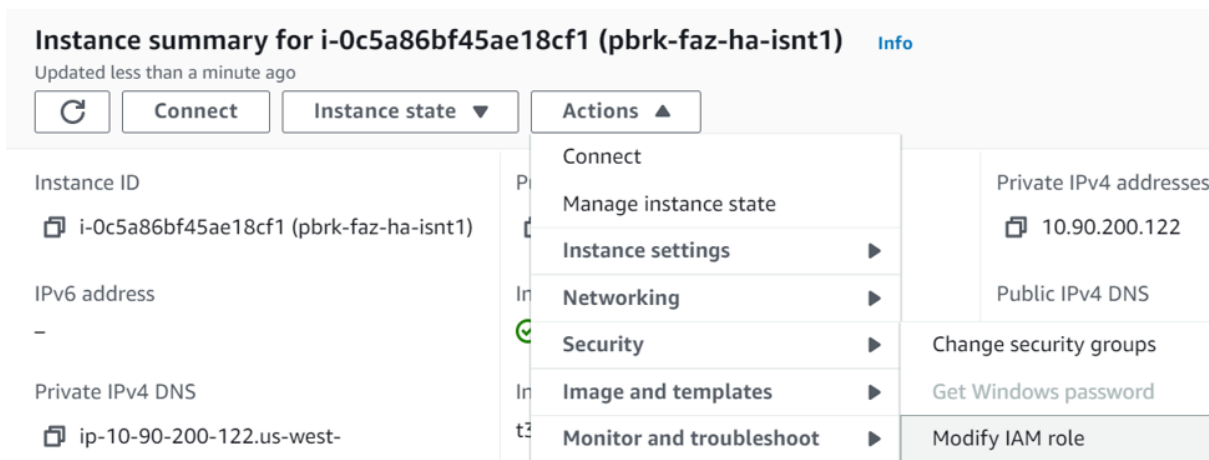
The following topics provide an overview of how to deploy FortiAnalyzer in high availability (HA) mode on AWS:

1. [Deploying FortiAnalyzer HA instances on AWS on page 22](#)
2. [Configuring FortiAnalyzer HA on page 23](#)

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*.



- 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
```

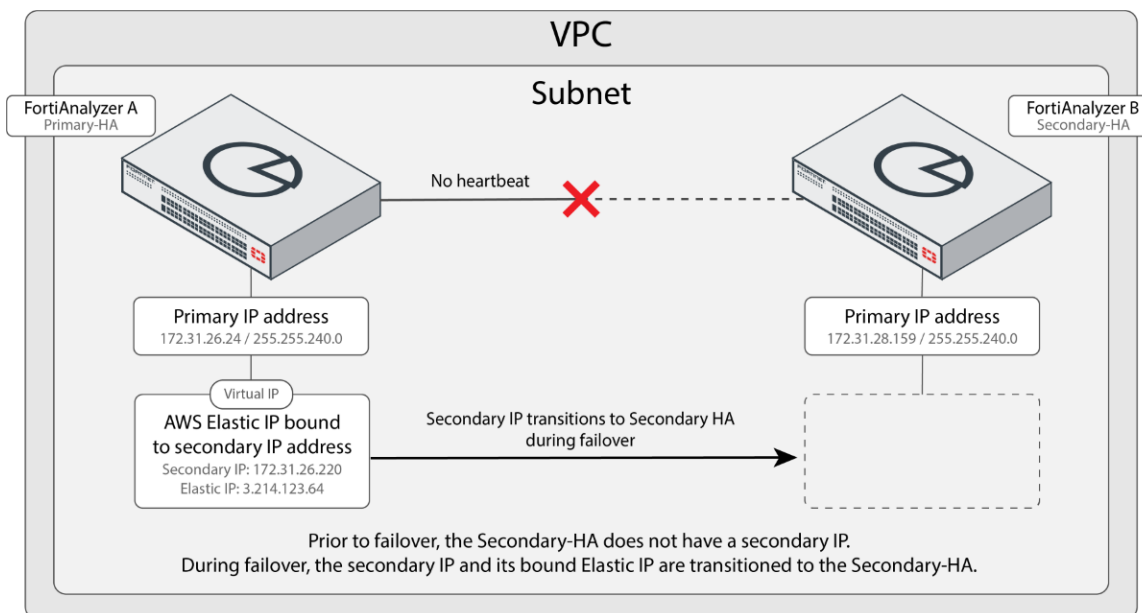
4. Create an *Inbound Rule* on the AWS *Network Security Group* assigned to the FortiAnalyzer HA interface.
 - a. To allow the keepalived adverts from the Primary:
 - On the Primary instance, allow TCP traffic destined for Port 112 from the local subnet of the Secondary instance and vice versa.
 - If both instances are in the same subnet, allow Port 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*.

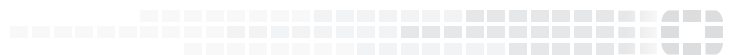
2. Import the Amazon Root CA to FortiAnalyzer. In order for the fazutil to be able to call EC2 API successfully, you must manually import the Amazon Cloud CA Certificates to each FortiAnalyzer instance. For more information on Amazon Trust Services, see <https://www.amazontrust.com/repository/>.
 - a. Go to *System Settings > Certificates > 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
2020-04-09	Initial release.
2021-07-13	Updated Instance type support on page 4 .
2021-07-22	Updated supported instance types for BYOL in Instance type support on page 4 .
2021-10-14	Updated Deploying FortiAnalyzer HA instances on AWS on page 22 and Configuring FortiAnalyzer HA on page 23 .
2021-11-30	Updated Configuring FortiAnalyzer HA on page 23 .
2022-09-07	Updated Order types on page 6 .
2023-03-09	Updated Order types on page 6 .



FORTINET®



Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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 General Counsel, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.