FortiAnalyzer - About FortiAnalyzer for AWS

Version 6.0

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 COOKBOOK
https://cookbook.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

January 15, 2019
FortiAnalyzer 6.0 About FortiAnalyzer for AWS
05-600-480495-20190115

TABLE OF CONTENTS

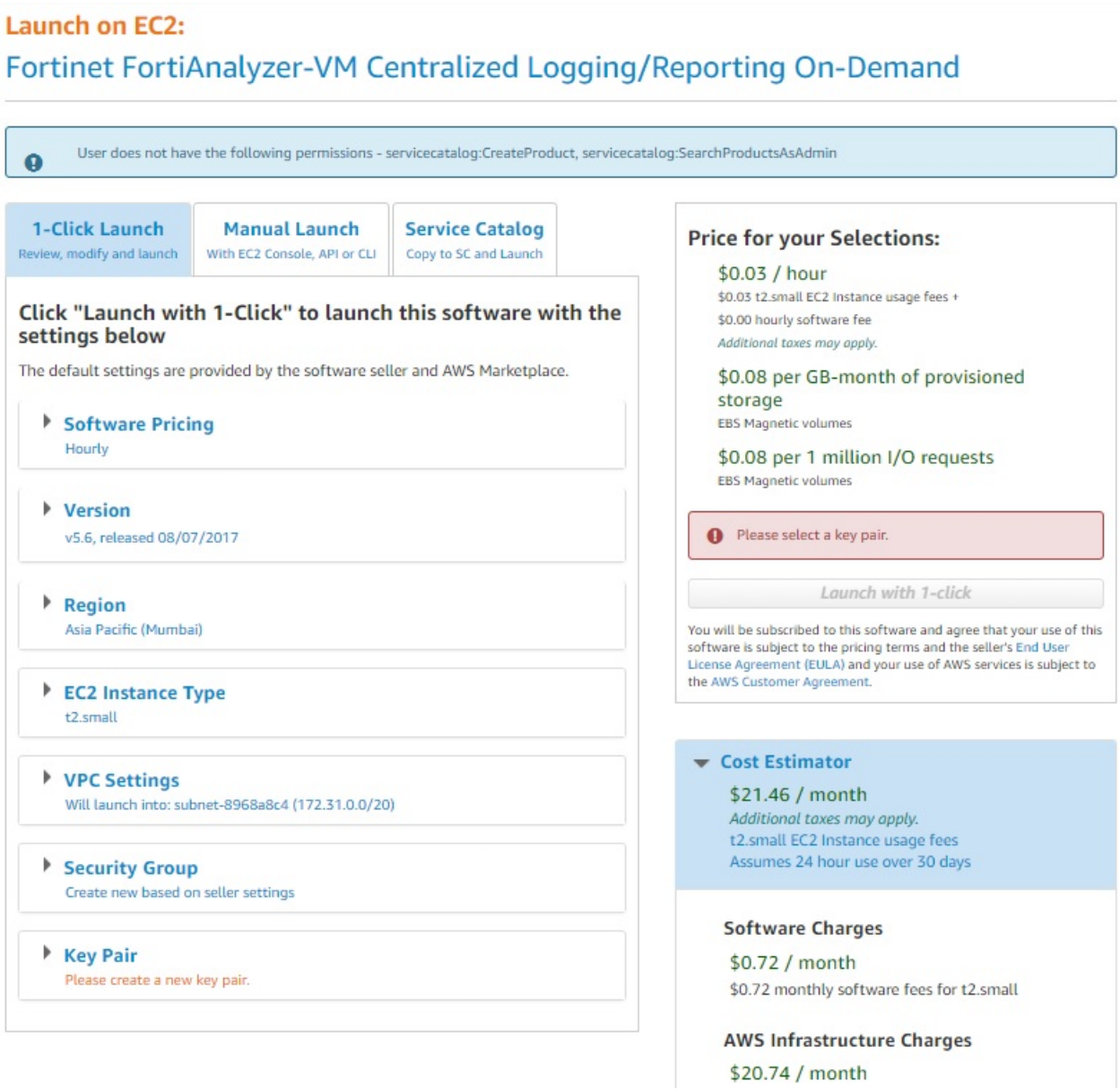
Deploying FortiAnalyzer VM **4**
Deploying FortiAnalyzer VM using 1-Click Launch 4
Deploying FortiAnalyzer VM using manual launch 10
Adding Additional Storage (Optional) **15**
Uploading the License File via the GUI **17**
Configuring Your FortiAnalyzer VM **18**
Change Log **19**

Deploying FortiAnalyzer VM

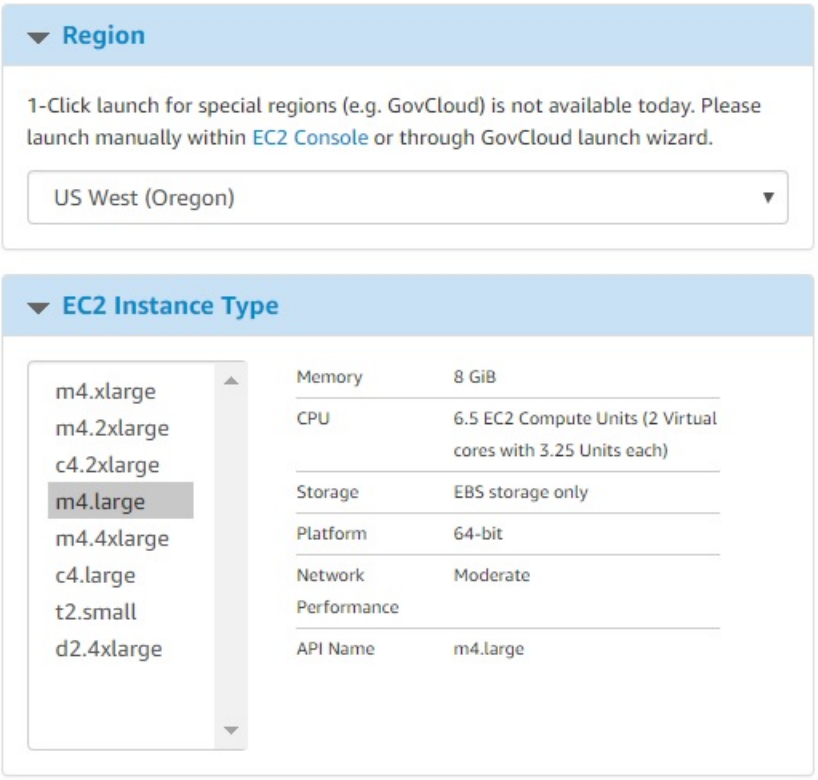
You can deploy FortiAnalyzer VM in one of two ways: through 1-click or manual launch.

Deploying FortiAnalyzer VM using 1-Click Launch

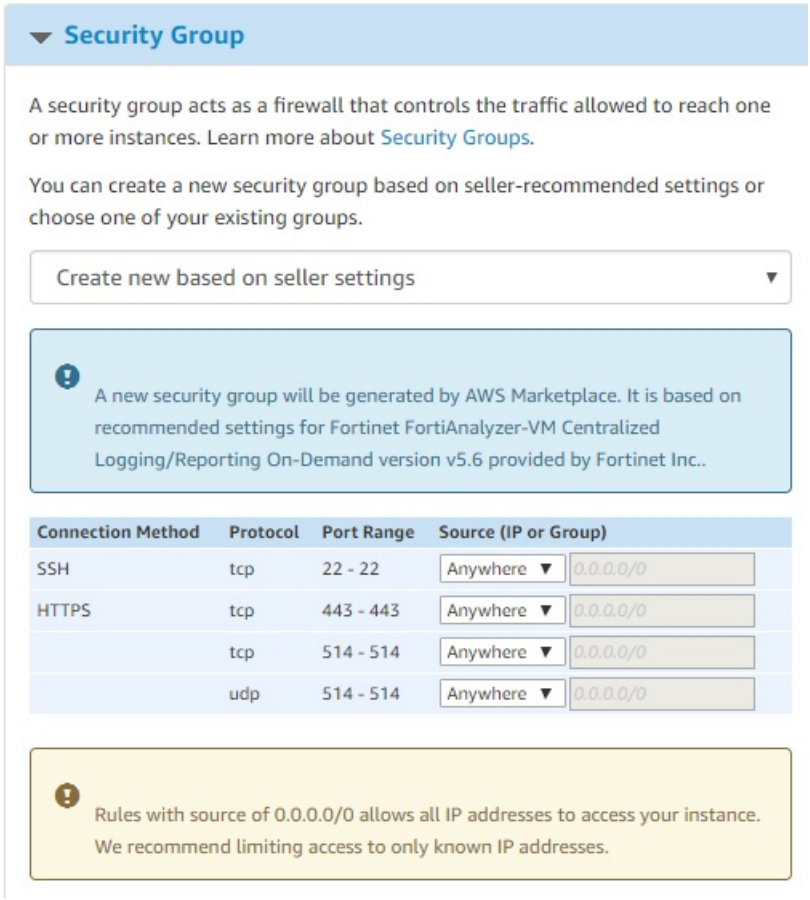
1. Go to the AWS Marketplace's page for FortiAnalyzer VM. Select *Continue*.



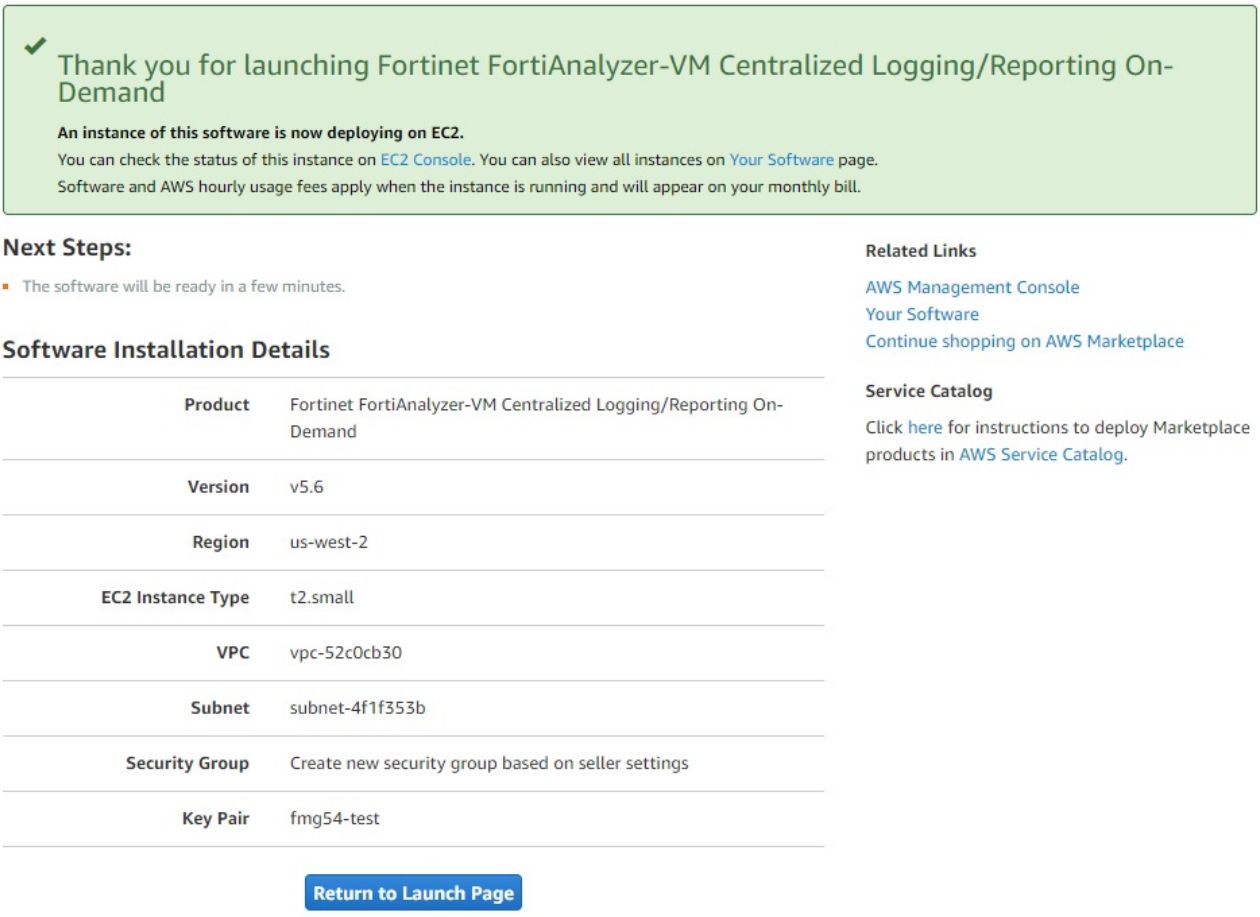
2. Select the desired region and instance type. Ensure the instance type fits the size of your deployment and potential future growth. Note *t2.small* is intended for free preview and its device support is limited to FortiGate-90 or smaller and FortiGate-VM 1vCPU models (VM00 and VM01).



3. 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. The remaining ports can also be opened to allow for all potential FortiAnalyzer communication.



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

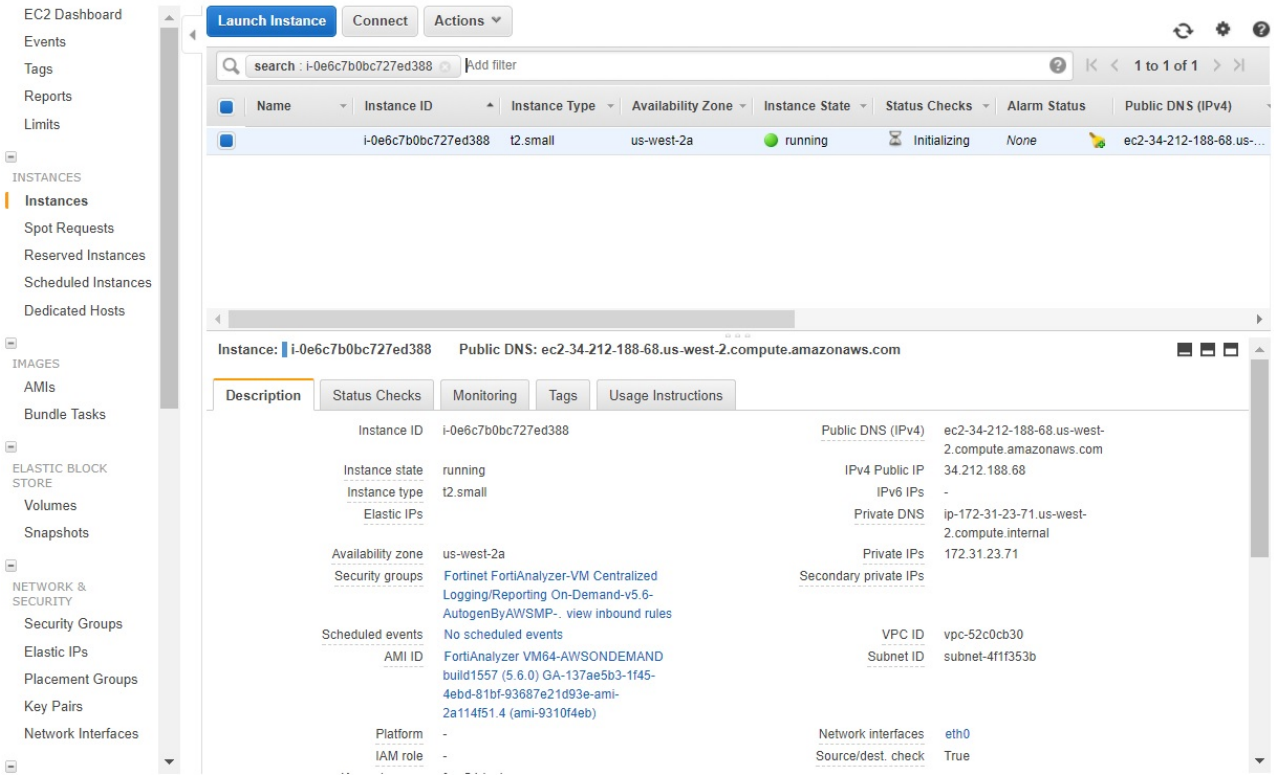
Related Links

AWS Management Console
Your Software
Continue shopping on AWS Marketplace

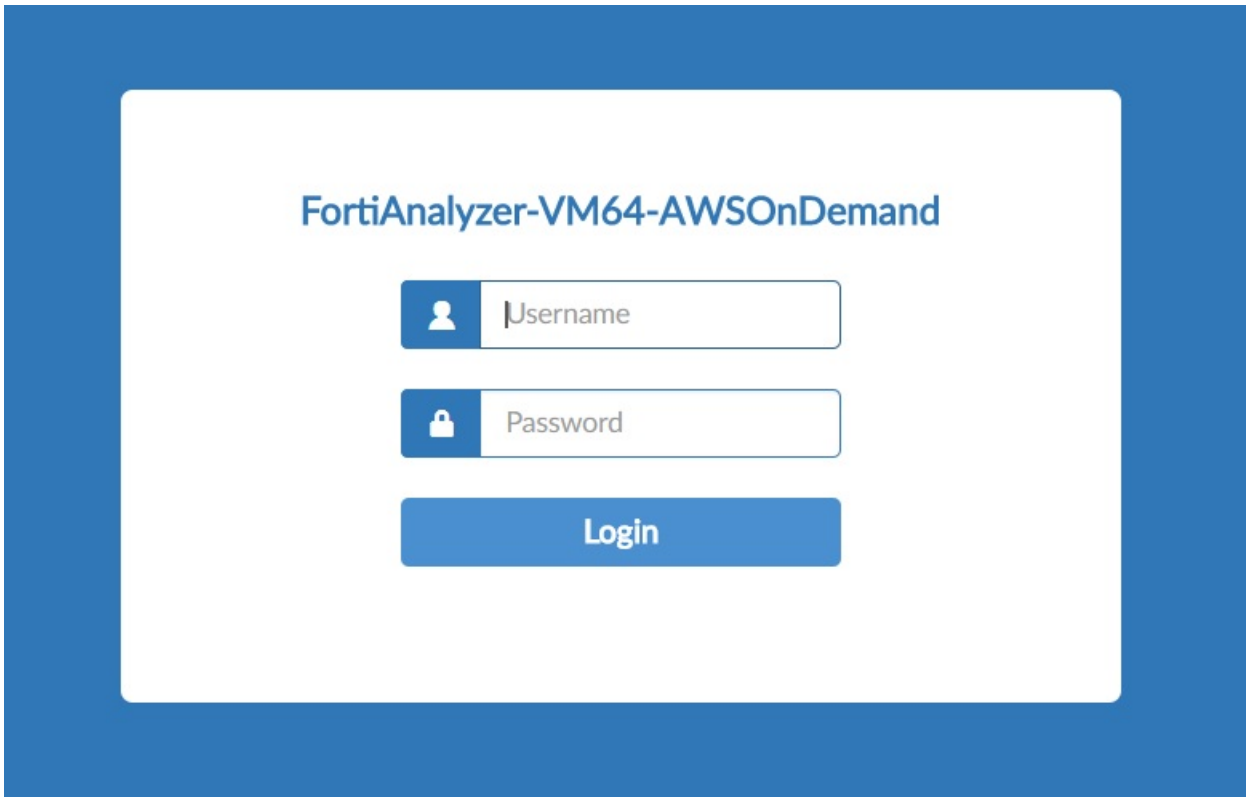
Service Catalog

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.

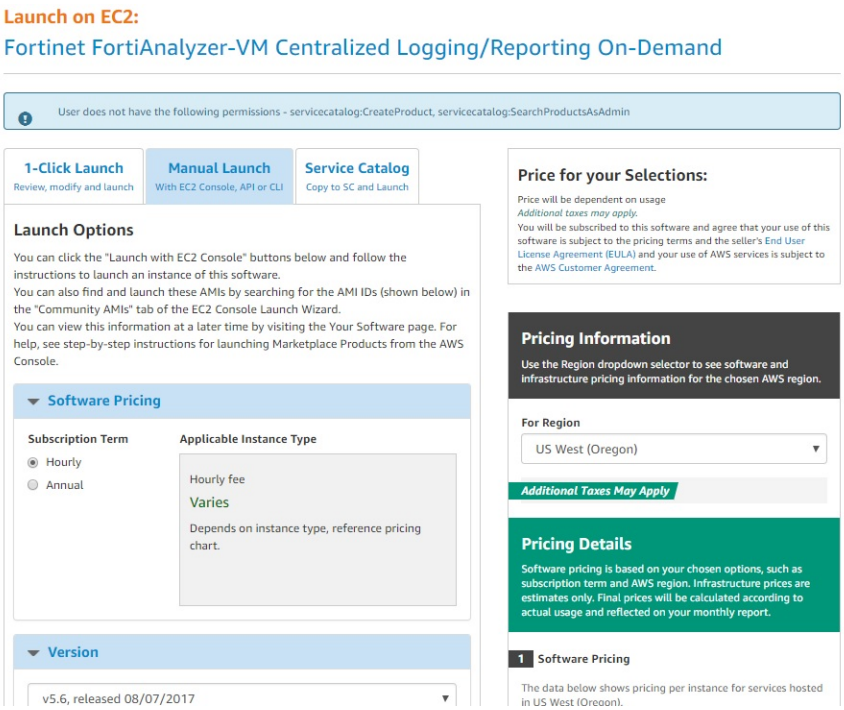


To connect to the FortiAnalyzer VM management GUI, open a web browser and use the public DNS IPv4 address as the URL: *https://<public DNS IPv4 address>*. Log in with the default username admin and the instance ID as the password to configure your FortiAnalyzer VM.

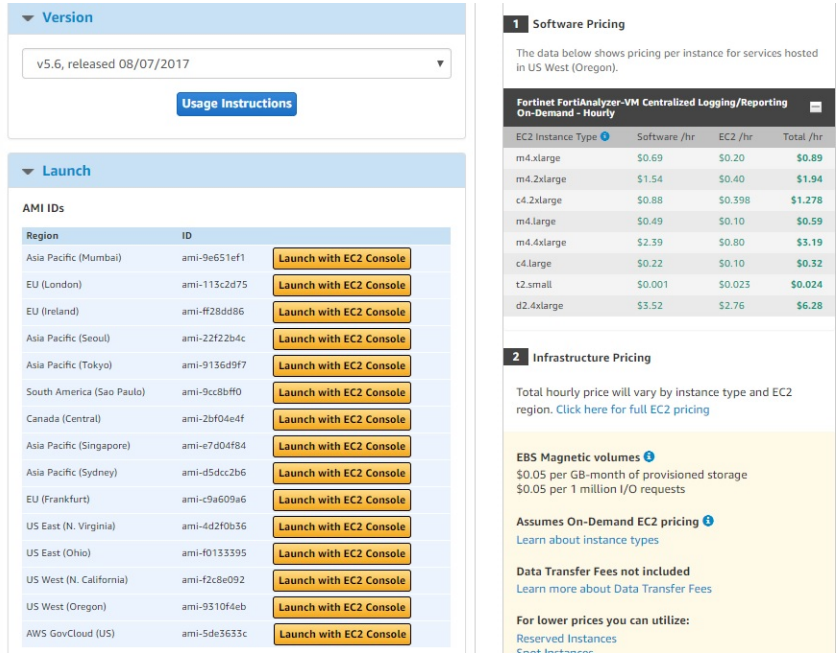

FortiAnalyzer-VM64-AWSOnDemand
Username
Password
Login

Deploying FortiAnalyzer VM using manual launch

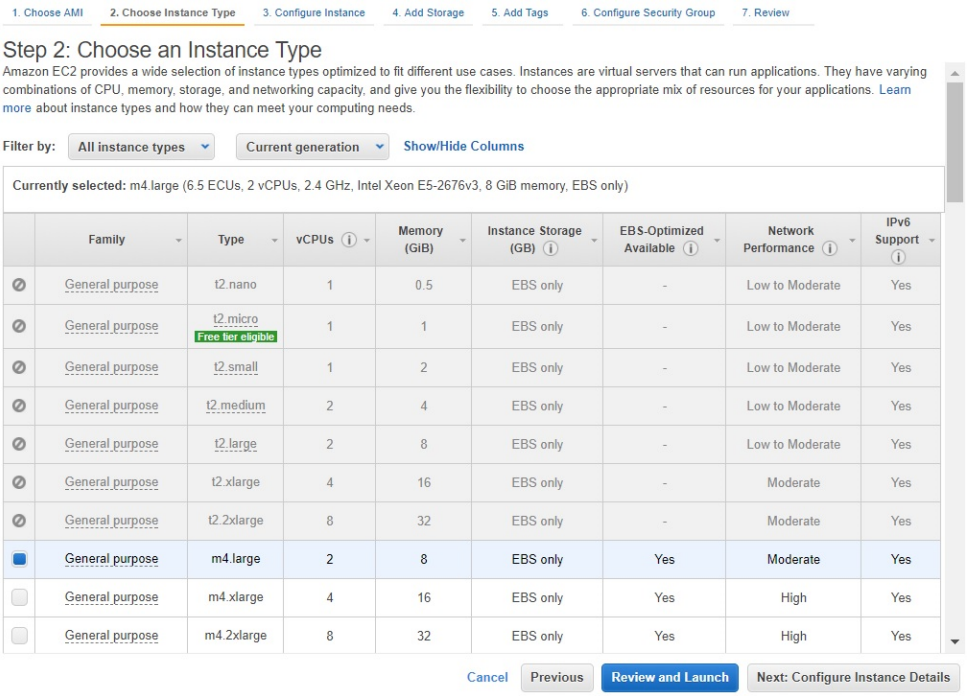
1. Go to the AWS Marketplace's page for FortiAnalyzer VM. Select *Continue*, then *Manual Launch*.



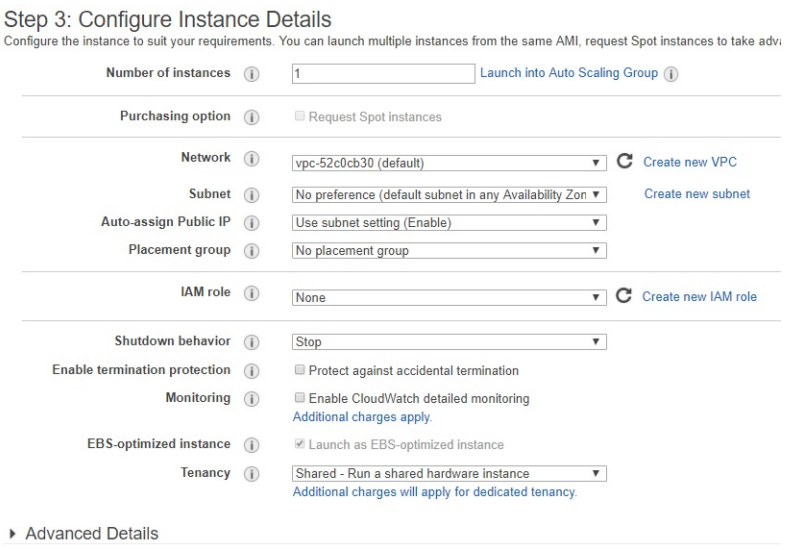
2. Click the *Launch with EC2 Console* button beside your desired region.



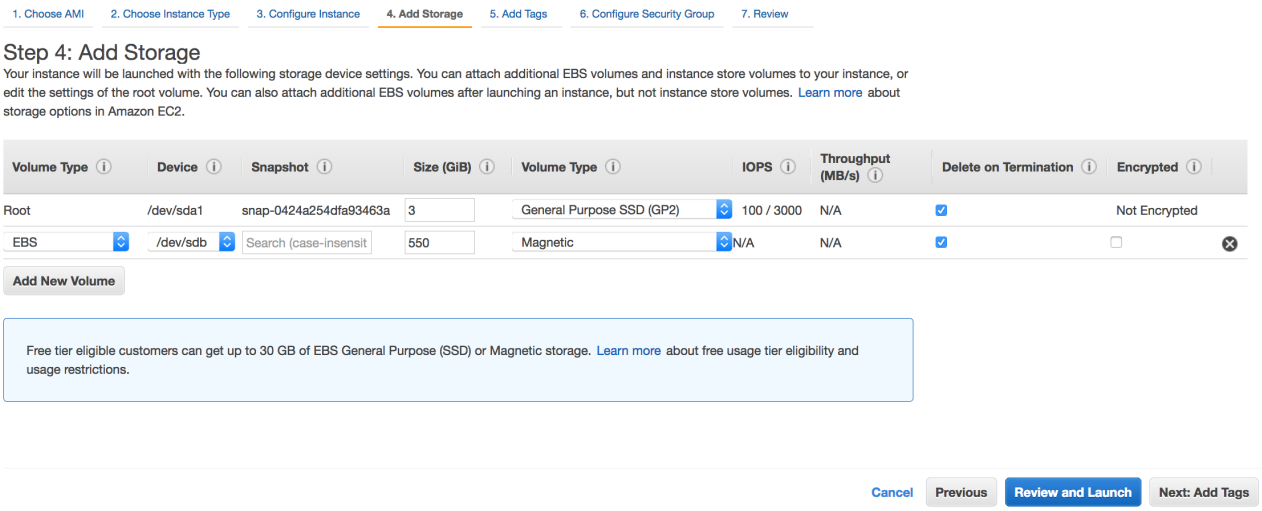
3. Select an instance type. Ensure the instance type fits the size of your deployment and potential future growth. Note t2.small is intended for free preview and its device support is limited to FortiGate-90 or smaller and FortiGate-VM 1vCPU models (VM00 and VM01). Click *Next: Configure Instance Details*.



4. Configure the various attributes:
   a. Network (ensure to select a VPC connected to the Internet gateway; by default, VPCs are connected to the Internet gateway)
   b. Subnet
   c. Enable *Auto-assign Public IP*
   d. Others as needed depending on your IT infrastructure requirements



5. 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.

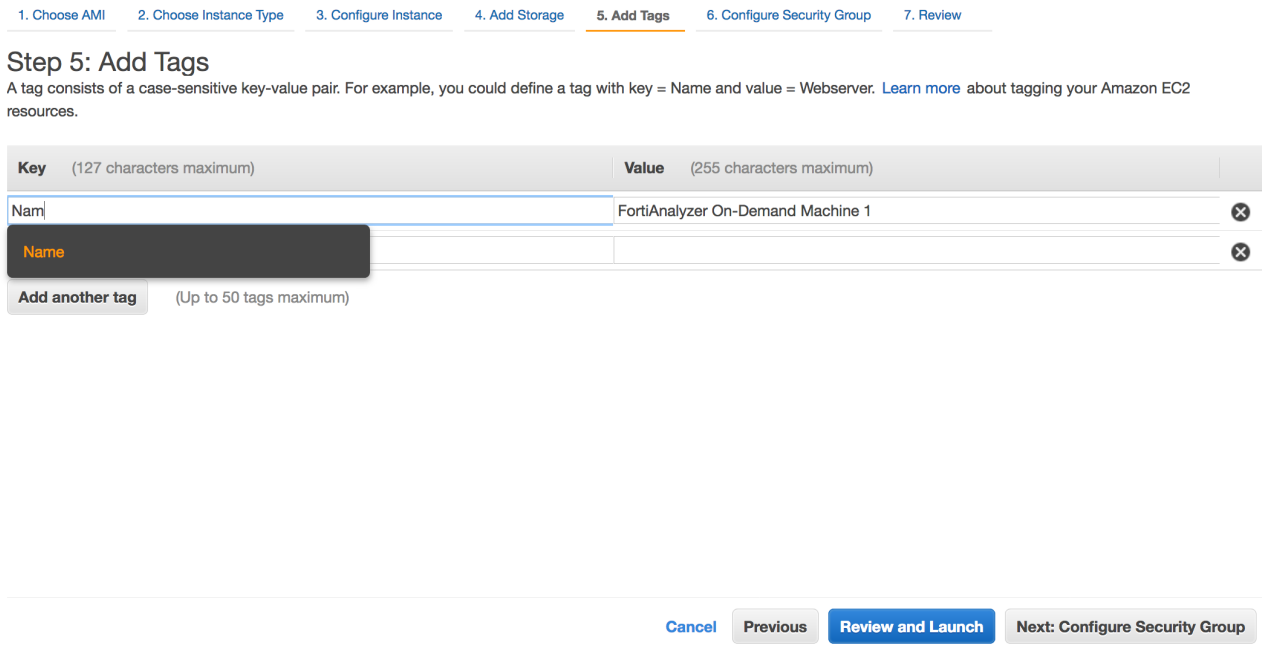


The FortiAnalyzer system reserves a certain portion of disk space for system use and unexpected quota overflow. The remaining space is available for allocation to devices. Reports are stored in the reserved space. The following describes the reserved disk quota relative to the total available disk size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

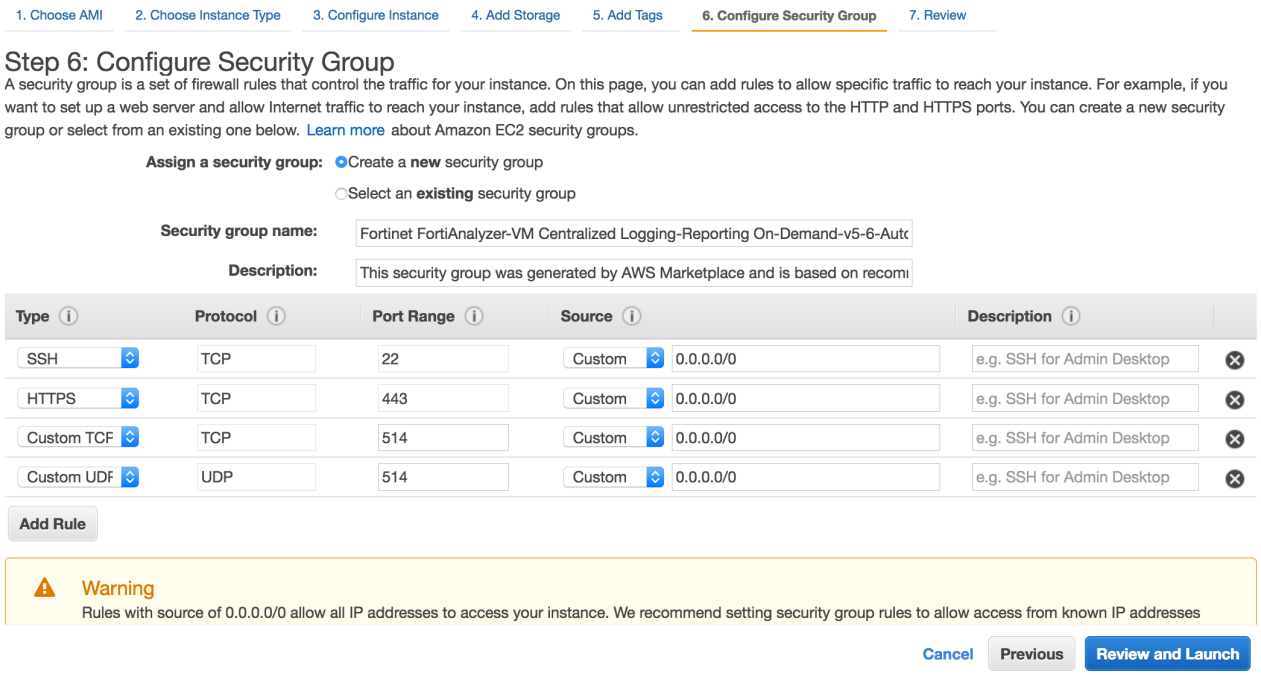
- Small disk (less than or equal to 500 GB): system reserves 20% or 50 GB of disk space, whichever is smaller.
- Medium disk (less than or equal to 1 TB): system reserves 15% or 100 GB of disk space, whichever is smaller.
- Medium to large disk (less than or equal to 5 TB): system reserves 10% or 200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

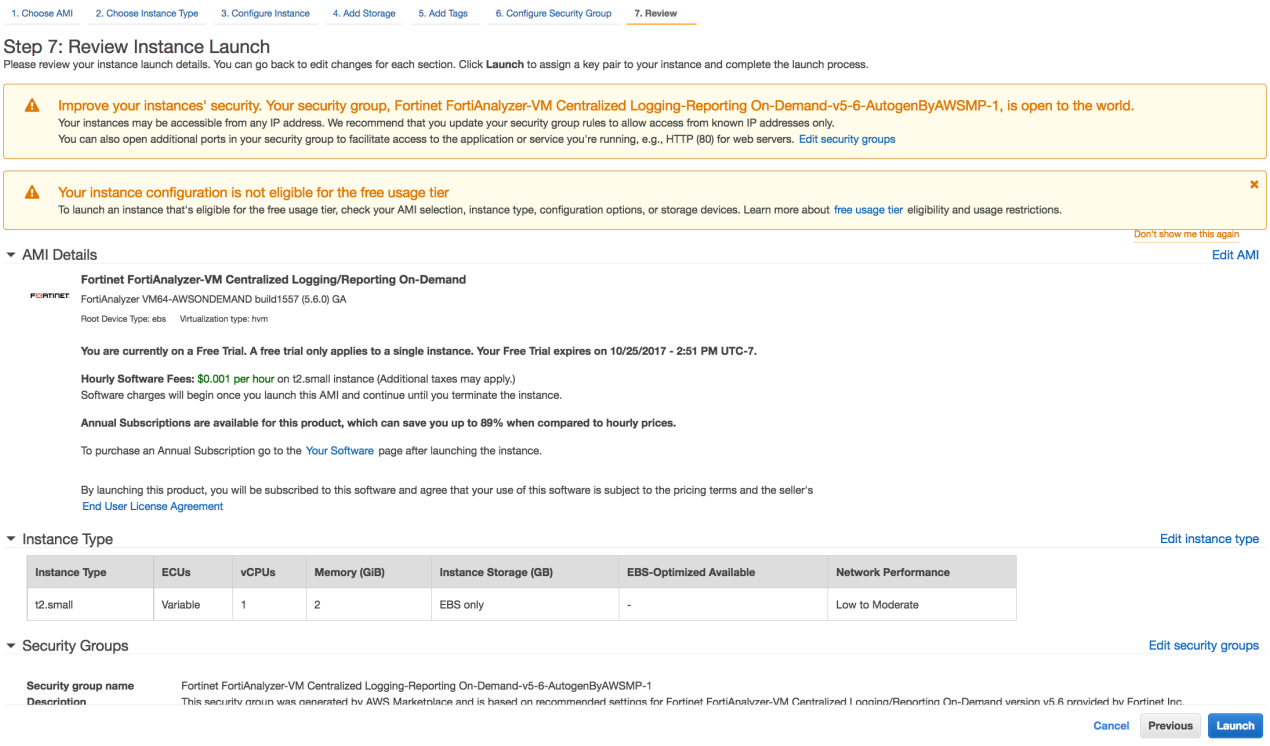
6. Click *Next: Tag Instance*. A tag consists of a key-value pair. It is useful to create tags to quickly identify instances in the EC2 console.



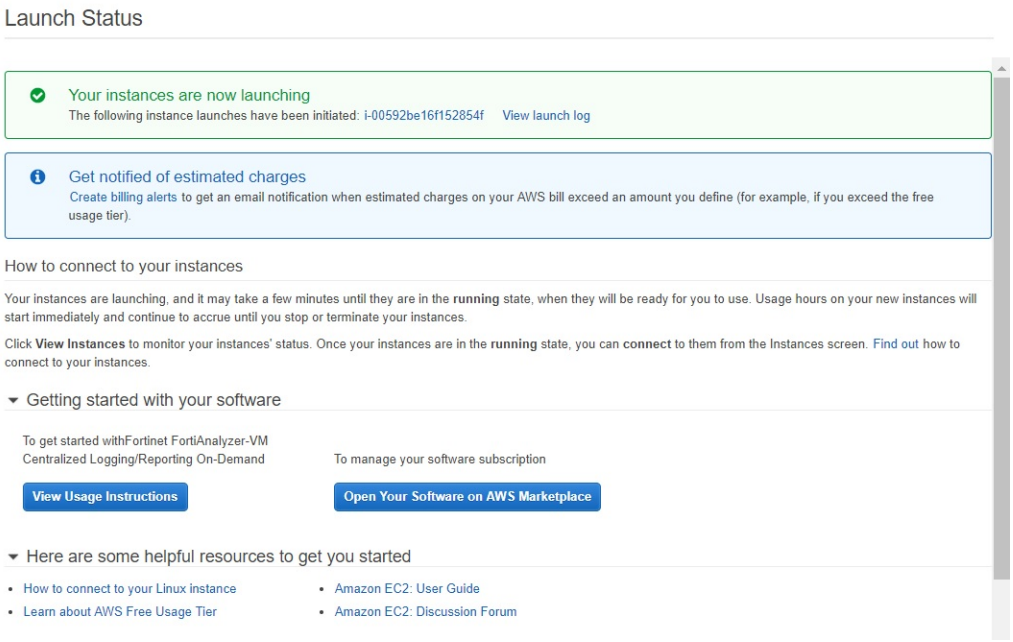
7. Click *Next: Configure Security Group*. The default provided security group is based on recommended settings for the FortiAnalyzer VM.



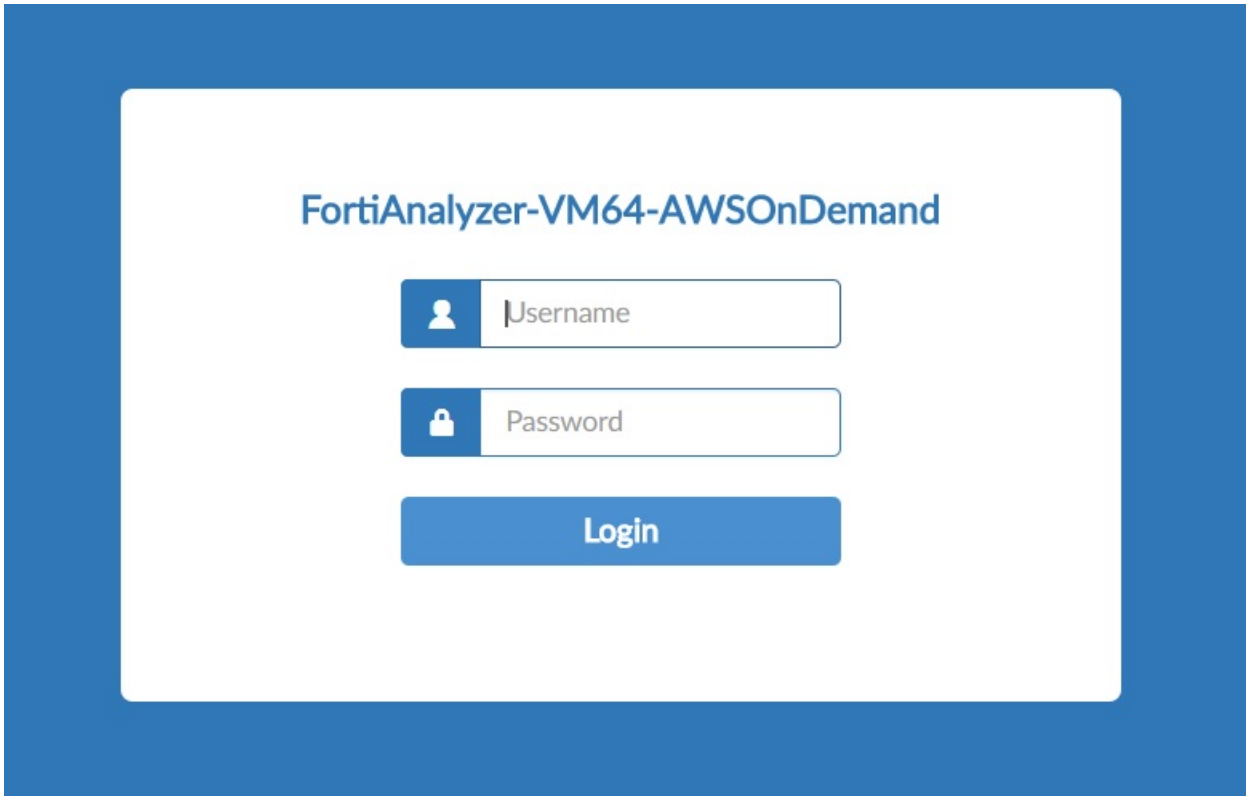
8. Click *Review and Launch*. If there is no change needed, click *Launch*.



9. You are prompted to choose a key pair. Click the checkbox, then click *Launch Instances*.



10. 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.



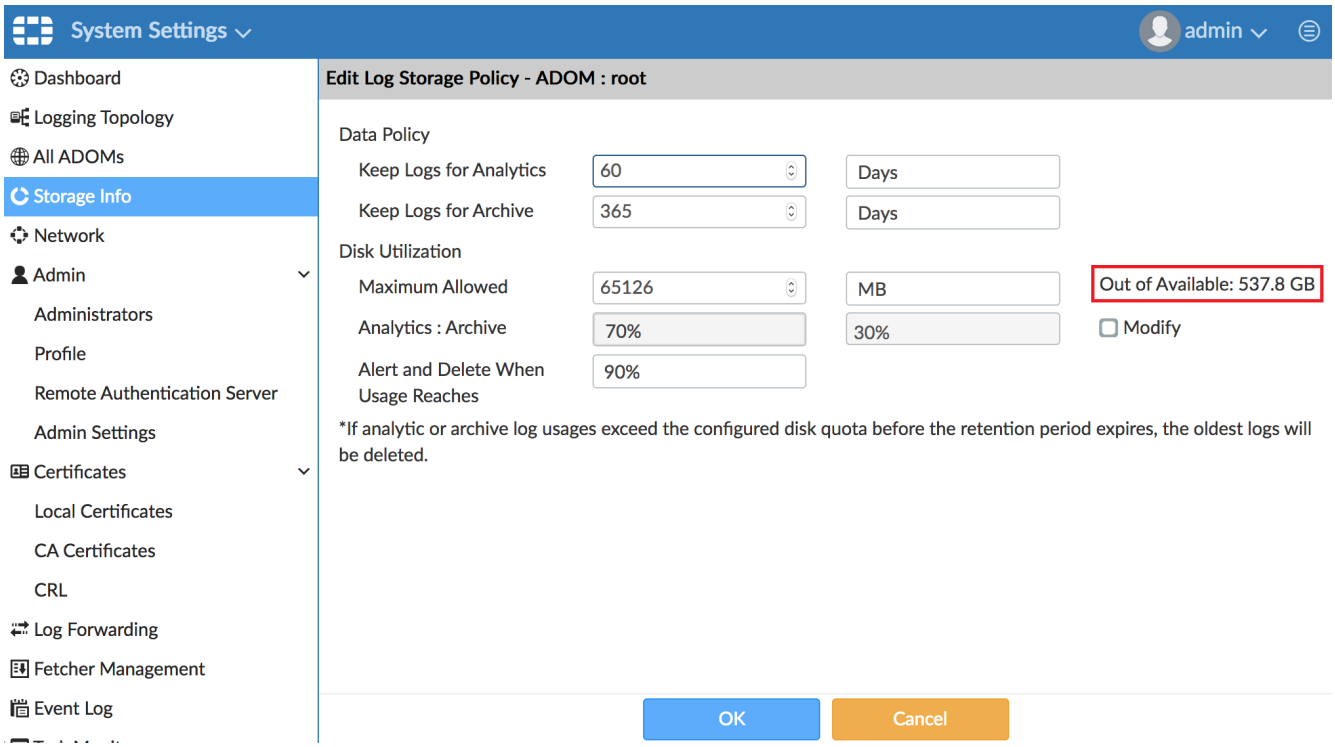
Adding Additional Storage (Optional)

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.

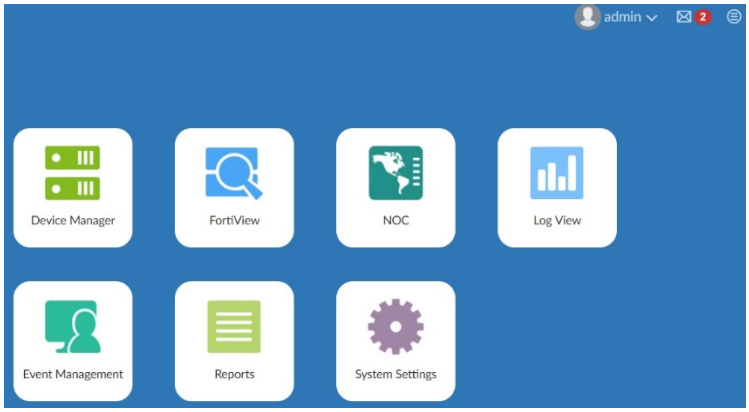
```
FAZVM64-AWSOnDemand # exec lvm info
LVM Status: OK

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.

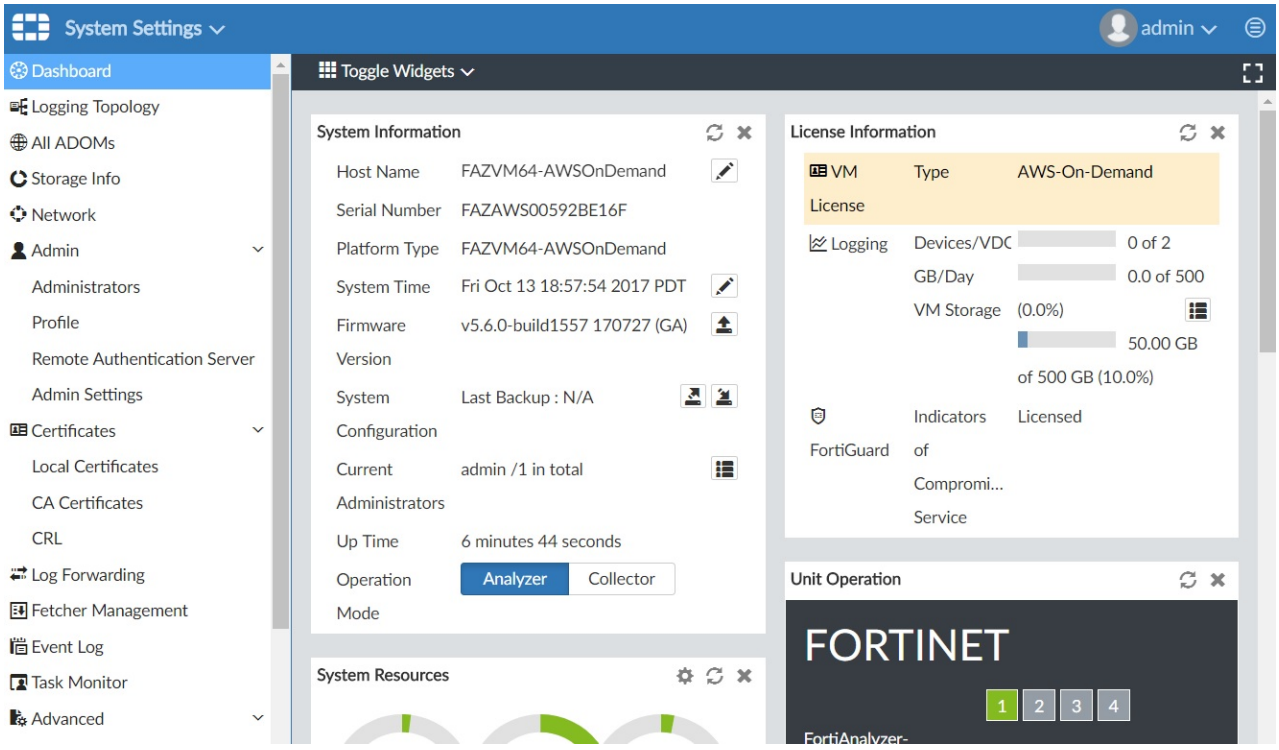

System Settings
admin
Dashboard
Logging Topology
All ADOMs
Storage Info
Network
Admin
Administrators
Profile
Remote Authentication Server
Admin Settings
Certificates
Local Certificates
CA Certificates
CRL
Log Forwarding
Fetcher Management
Event Log
Edit Log Storage Policy - ADOM : root
Data Policy
Keep Logs for Analytics
60
Days
Keep Logs for Archive
365
Days
Disk Utilization
Maximum Allowed
65126
MB
Out of Available: 537.8 GB
Analytics : Archive
70%
30%
Modify
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

Uploading the License File via the GUI

1. Navigate to *System Settings*.



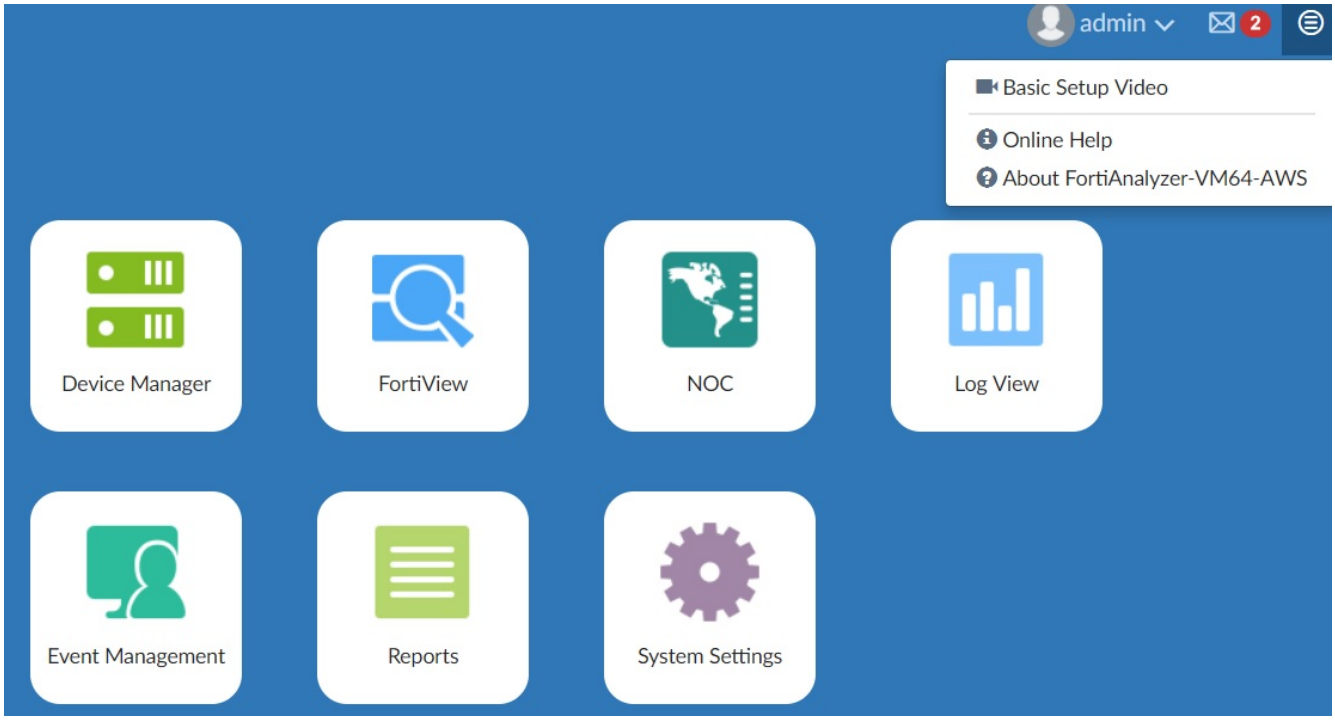
2. The *License Information* widget on the *Dashboard* displays as *AWS-On-Demand*.



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.



Change Log

Date	Change Description
2019-01-15	Initial release.

Copyright© 2019 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.