FortiManager - AWS Cookbook

Version 6.4.0

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 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

September 7, 2022
FortiManager 6.4.0 AWS Cookbook
02-640-621426-20220907

TABLE OF CONTENTS

About FortiManager for AWS

FortiManager's security-operationalized visibility across your Fortinet Security Fabric enables true security effectiveness and foresight to identify and understand the scope of threats and facilitates actionable responses and risk remediation.

Quantifiable security solution information produces measurable accountability and uses those ratings to compare your security preparedness internally and to that of your industry peers.

Centralized change management helps you update policies and objects, maintain provisioning templates and easily configure changes to your APs, switches, SD-WAN and SDN connectors and more, to mitigate security events and apply configuration changes and policy updates.

Network administrators can better control their network by logically grouping devices into administrative domains (ADOMs), effectively applying policies and distributing content security/firmware updates. FortiManager is one of several versatile network security management products that provide diversity of deployment types, growth flexibility, advanced customization through APIs, and simple licensing, all through central management and configuration.

Instance type support

You can deploy FortiManager for AWS as a virtual machine.

The following lists supported instance types for each FortiManager listing on the AWS marketplace. Supported instances may change without notice.

Bring your own license (BYOL)

The BYOL listing supports the following instance types. The m4.large instance type is recommended.

- c4.2xlarge
- c4.4xlarge
- c4.8xlarge
- c5.2xlarge
- c5.4xlarge
- c5.9xlarge
- c5.18xlarge
- c5.xlarge
- d2.2xlarge
- d2.4xlarge
- d2.8xlarge
- d2.xlarge
- h1.2xlarge
- h1.4xlarge
- h1.8xlarge
- h1.16xlarge

- m4.2xlarge
- m4.4xlarge
- m4.10xlarge
- m4.16xlarge
- m4.large
- m4.xlarge
- m5.2xlarge
- m5.4xlarge
- m5.12xlarge
- m5.24xlarge
- m5.large
- m5.xlarge
- c5.12xlarge
- c5.24xlarge
- m5.16xlarge
- m5.8xlarge

On-demand

Listing name	Supported instance types	Recommended instance type
FortiManager Centralized Security Management (Max 2 managed devices)	• m5.large • m5.xlarge • t2.medium	m5.large
FortiManager Centralized Security Management (Max 10 managed devices)	• h1.2xlarge • h1.4xlarge • h1.8xlarge • m5.2xlarge • m5.4xlarge • m5.12xlarge • m5.large • m5.xlarge • t2.large • t2.xlarge • m5.8xlarge	
FortiManager Centralized Security Management (Max 30 managed devices)	• h1.2xlarge • h1.4xlarge • h1.8xlarge • h1.16xlarge • m5.2xlarge • m5.4xlarge • m5.12xlarge • m5.24xlarge • m5.large	

Listing name	Supported instance types	Recommended instance type
	• m5.xlarge • t2.2xlarge • t2.large • t2.xlarge • m5.16xlarge • m5.8xlarge	
FortiManager Centralized Security Management (Max 100 managed devices)	• h1.2xlarge • h1.4xlarge • h1.8xlarge • h1.16xlarge • m5.2xlarge • m5.4xlarge • m5.12xlarge • m5.24xlarge • m5.large • m5.xlarge • t2.2xlarge • t2.large • t2.xlarge • m5.16xlarge • m5.8xlarge	m5.xlarge
FortiManager Centralized Security Management (Max 500 managed devices)	• h1.2xlarge • h1.4xlarge • h1.8xlarge • h1.16xlarge • m5.2xlarge • m5.4xlarge • m5.12xlarge • m5.24xlarge • m5.large • m5.xlarge • t2.2xlarge • t2.xlarge • m5.16xlarge • m5.8xlarge	m5.2xlarge

Models

FortiManager-VM is licensed based on the number of managed devices, amount of logging per day, and storage capacity. Refer to price lists and order SKUs available through your resellers/distributors. These are also referred to as BYOL models.

You can deploy FortiManager-VM using different CPU and RAM sizes and launch them on various private and public cloud platforms.

Licensing

You must have a license to deploy FortiManager-VM for AWS.

Order types

On AWS, there are usually two order types: BYOL and on-demand.

BYOL offers perpetual (normal series and v-series) licensing as opposed to on-demand, 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.

With an on-demand subscription, the FortiManager-VM becomes available for use immediately after you create the instance. Different tiers on number of managed devices with term-based prices (hourly or annually) are mentioned in the marketplace product page.

For BYOL and on-demand deployments, 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 the FortiManager-VM).

For BYOL, you typically order a combination of products and services including support entitlement. On-demand includes support, for which you must contact Fortinet Support with your customer information. See *Support Information* on the marketplace product page.

To purchase on-demand, subscribe to the product on the marketplace. FortiManager will obtain the 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:

- FortiManager Centralized Security Management (Max 2 managed devices)
- FortiManager Centralized Security Management (Max 10 managed devices)
- FortiManager Centralized Security Management (Max 30 managed devices)
- FortiManager Centralized Security Management (Max 100 managed devices)
- FortiManager Centralized Security Management (Max 500 managed devices)

Creating a support account

FortiManager-VM for AWS supports on-demand and BYOL licensing models. See Order types on page 7.

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

First, if you do not have a Fortinet account, create one at Customer Service & Support.

BYOL

You must obtain a license to activate the FortiManager-VM. If you have not activated the license, you see the license upload screen when you log in to the FortiManager-VM and cannot proceed to configure the FortiManager-VM.

You can obtain licenses for the BYOL licensing model through any Fortinet partner. If you do not have a partner, contact awssales@fortinet.com for assistance in purchasing a license.

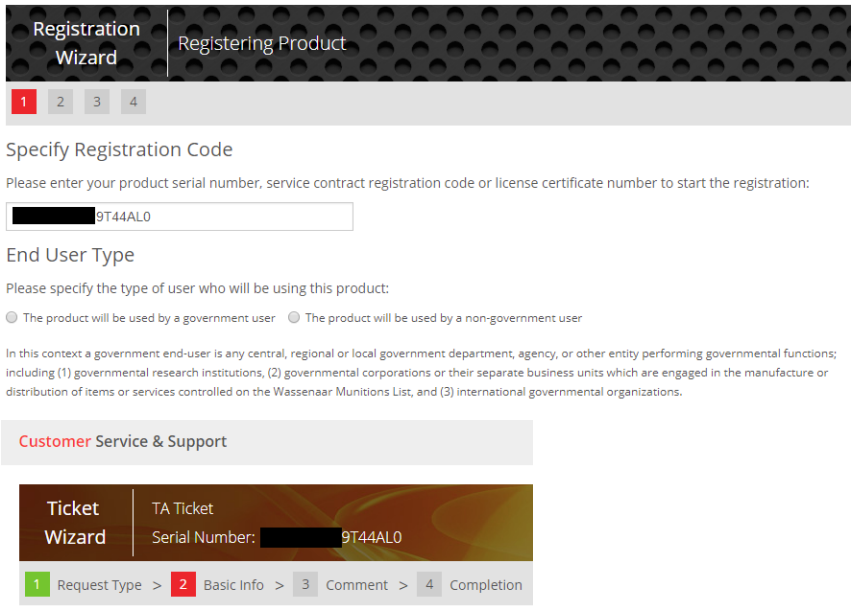
After you purchase a license or obtain an evaluation license (60-day term), you receive a PDF with an activation code.

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/Activate* to start the registration process. In the *Specify Registration Code* field, enter your license activation code and select *Next* to continue registering the product. Enter your details in the other fields.
3. At the end of the registration process, download the license (.lic) file to your computer. You will upload this license later to activate the FortiManager-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 FortiManager-VM, if you get an error that the license is invalid, wait 30 minutes and try again.

On-demand

1. Deploy and boot the FortiManager-VM on-demand Elastic Compute Cloud (EC2) instance and log in to the FortiManager-VM GUI management console.
2. From the Dashboard, copy the FortiManager-VM serial number.
3. Go to Customer Service & Support and create a new account or log in with an existing account.
4. Go to *Asset* > *Register/Activate* to start the registration process.
5. In the *Specify Registration Code* field, enter the serial number, and select *Next* to continue registering the product. Enter your details in the other fields.
6. After completing registration, contact Fortinet Customer Support and provide your FortiManager instance's serial number and the email address associated with your Fortinet account.



Deploying FortiManager on AWS

Bring your own license (BYOL) is perpetual licensing as opposed to on-demand, which is an hourly subscription. The BYOL license is available from resellers or your distributors.

You can deploy FortiManager-VMs on the AWS Elastic Compute Cloud (EC2). You must have an Amazon Elastic Compute Cloud (EC2) account prior to deploying the VM. You can deploy the FortiManager-VM using AWS marketplace launch or directly from the EC2 console.

With BYOL licensing, deploying FortiManager on AWS consists of the following steps:

1. Initial deployment on page 9
2. Registering and downloading your license on page 13
3. Connecting to FortiManager on page 14
4. Adding additional storage (optional) on page 14

With on-demand licensing, deploying FortiManager on AWS consists of the following steps:

1. Initial deployment on page 9
2. Adding additional storage (optional) on page 14

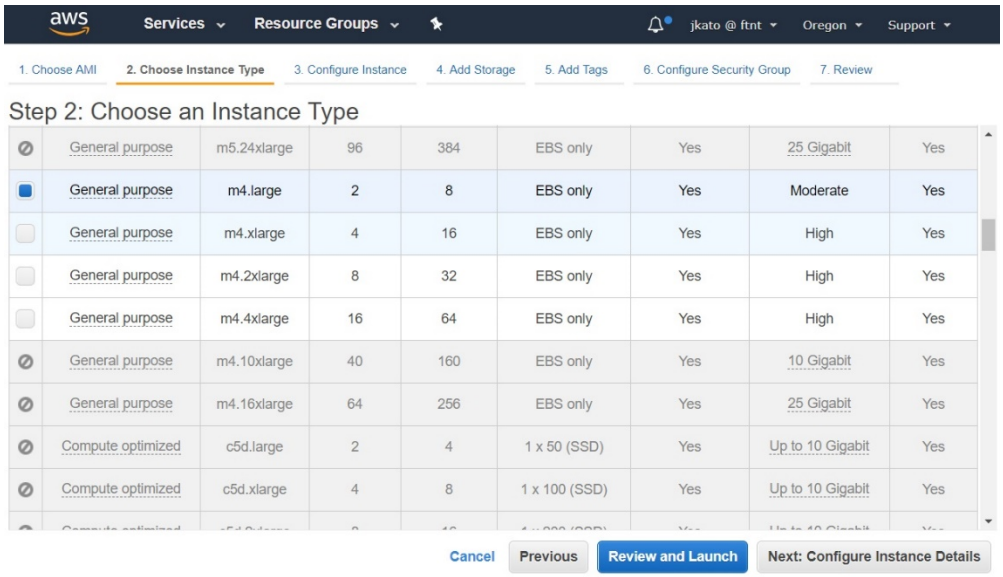
Initial deployment

This example deploys a FortiManager instance from the EC2 console.

To deploy a FortiManager instance from the EC2 console:

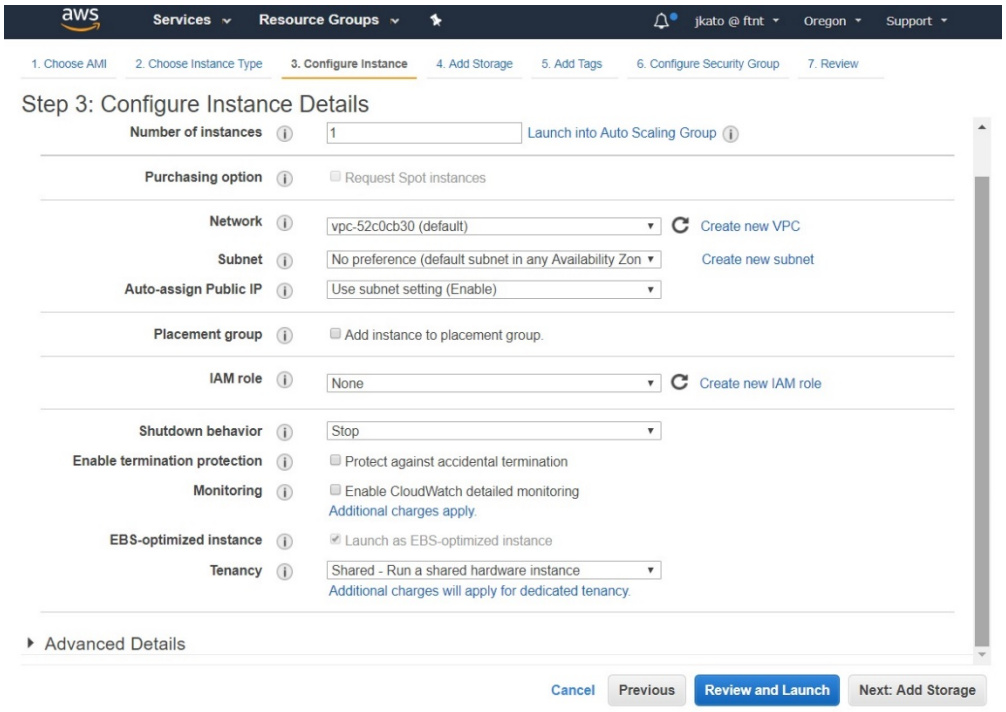
1. Launch the FortiManager-VM instance:
   a. Find the FortiManager listing on the AWS marketplace. Choose the FortiManager version based on the number of devices you want to manage.
   b. After configuring the software, click *Continue to Launch*. For a BYOL instance, select *Launch through EC2*, then click *Launch*.

2. Select one of the supported instance types. Click *Next: Configure Instance Details*.



3. 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. Other as needed depending on your IT infrastructure requirements

   Click *Next: Add Storage*.



4. You can configure disks by choosing one of the following options:
   a. Leave the disks at default values. You can add additional disks later.
   b. Increase the second volume's disk size. The second volume is used for logging.
   c. Add additional disks.

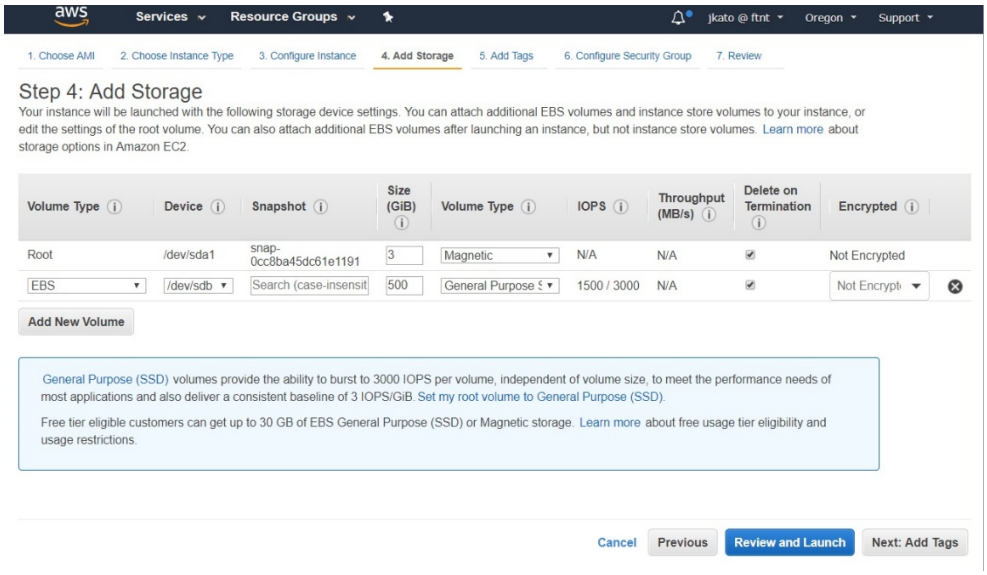
   You can configure the volume type as *EBS*, the device as */dev/sdb*, and the size based on your requirements. You are entitled to consume disks according to the licensed limit of the purchased BYOL license.

   For more detail about disk sizes and the maximum limit of licensed numbers of devices, see the product listing page.

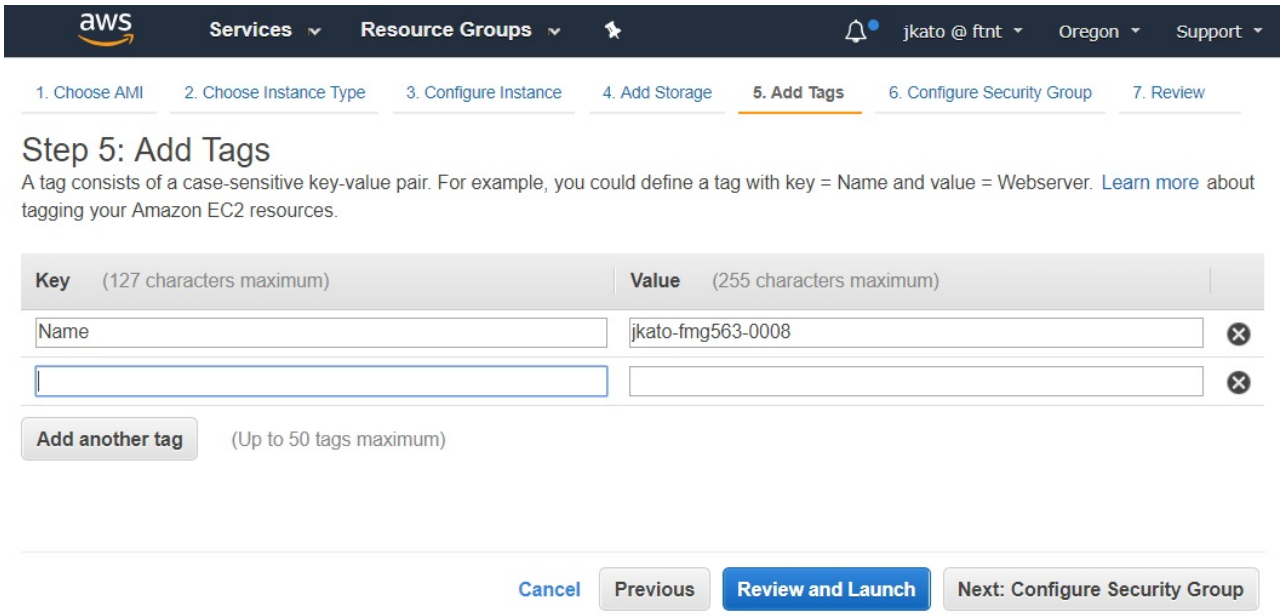
   The FortiManager system reserves a certain portion of disk space for system use and unexpected quota overflow. The remaining space is available for allocation to devices. Reports are stored in the reserved space. The following describes the reserved disk quota relative to the total available disk size (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.
   - **Large disk** (less than or equal to 5 TB): system reserves 10% or 200 GB of disk space, whichever is smaller.
   - **Very large disk** (greater 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 Adding additional storage (optional).

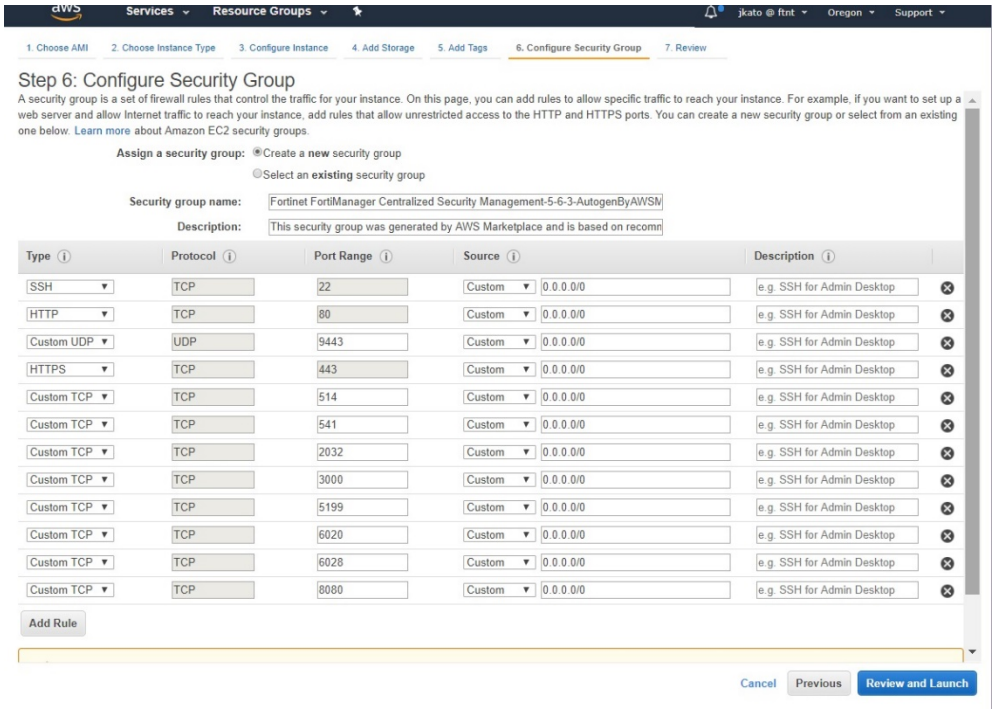
   Click *Next: Add Tags*.



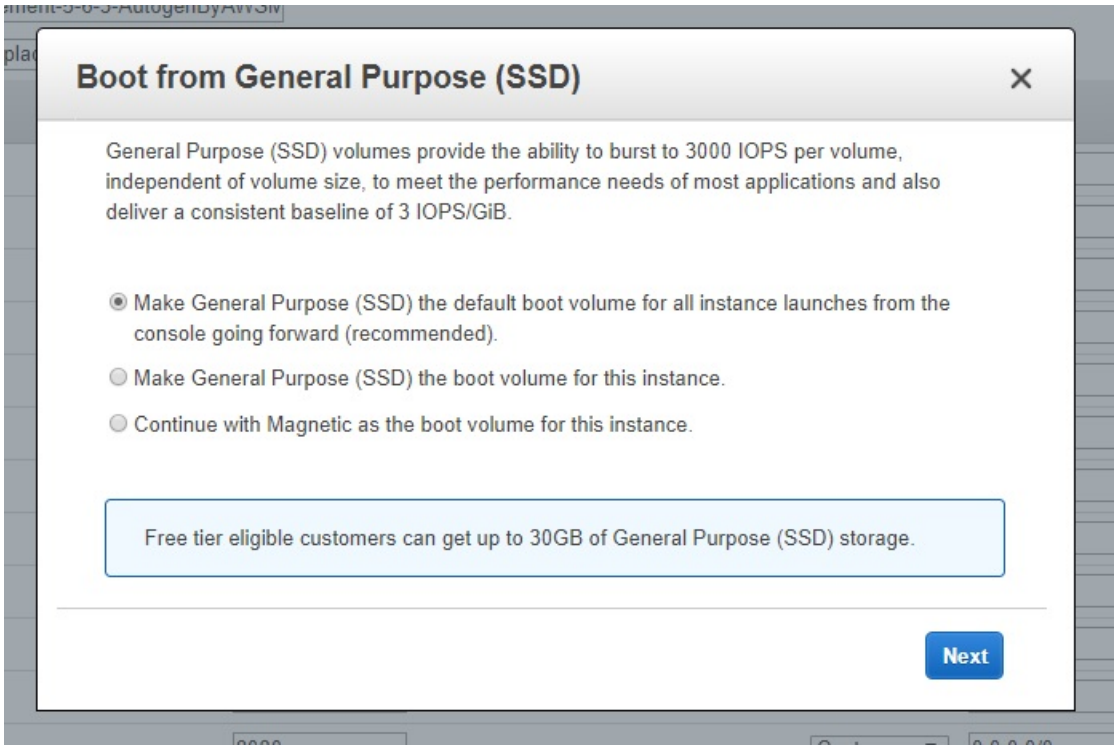
5. Create or add tags as required. Name tags are convenient to use to distinguish EC2 instance names. You can also leave this section blank and continue by clicking *Next: Configure Security Group*.



6. Review all open ports configured by default. Usually, these can stay as-is. Most strict configuration is to allow SSH or HTTPS to access the FortiManager management console. Accessing the GUI requires the HTTPS port to be open. Refer here to see each port's purpose.



7. Review the configuration and launch the instance:
   a. Click *Review and Launch*. A popup may ask if you want to make General Purpose (SSD) the default boot volume. Select the desired option, then click *Next*.



b. Review the configuration and click *Launch Instance*.

c. Select a key pair, check the acknowledgment checkbox, then click *Launch Instance*.

8. An on-demand FortiManager-VM instance requires connectivity to FortiCare to obtain a valid license. Otherwise, the FortiManager-VM shuts down for self-protection. Ensure the following:
   - Outgoing connectivity to https://directregistration.fortinet.com:443 is allowed in security groups and ACLs.
   - A public IP address (either default or EIP) is assigned.

Registering and downloading your license

You can obtain licenses for the BYOL licensing model through any Fortinet partner. If you do not have a partner, contact awssales@fortinet.com for assistance in purchasing a license.

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

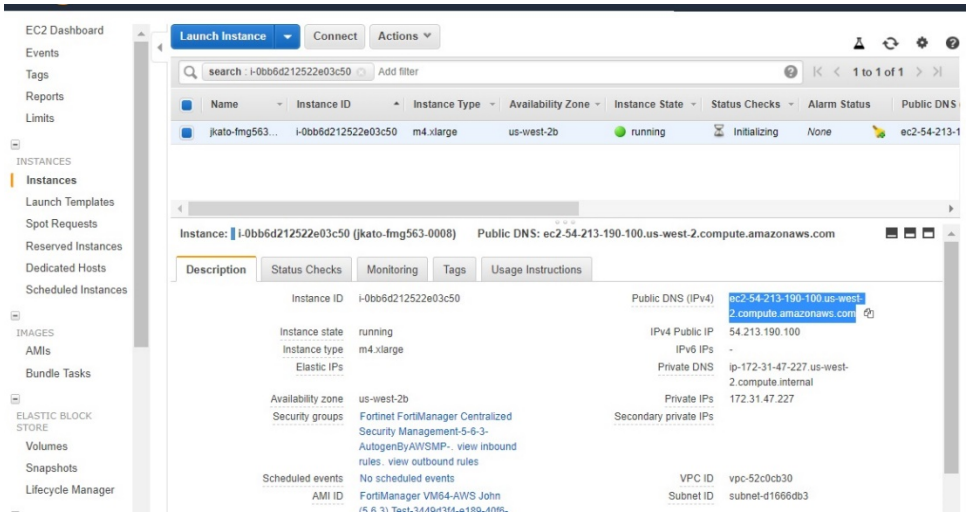
To register and download your license:

1. Go to Customer Service & Support and create a new account or log in with an existing account.
2. Go to *Asset* > *Register/Activate* to start the registration process. In the *Specify Registration Code* field, enter your license activation code and select *Next* to continue registering the product. Enter your details in the other fields.
3. At the end of the registration process, download the license (.lic) file to your computer. You will upload this license later to activate the FortiManager-VM.
4. 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 FortiManager-VM, if you get an error that the license is invalid, wait 30 minutes and try again.

Connecting to FortiManager

To connect to FortiManager:

1. Log in to the EC2 console and navigate to the FortiManager instance. Find the public DNS or elastic IP address that you can access over the Internet.



2. In a browser, go to https://<public DNS or elastic IP address>.
3. Once deployed, log in to FortiManager with the username "admin". The initial password is the instance ID. Changing the initial password at the first login is highly encouraged.
4. Go to *System Settings* to see the system status on the dashboard. Check if you have sufficient disk space. Otherwise, you must add a disk/volume.

Adding additional storage (optional)

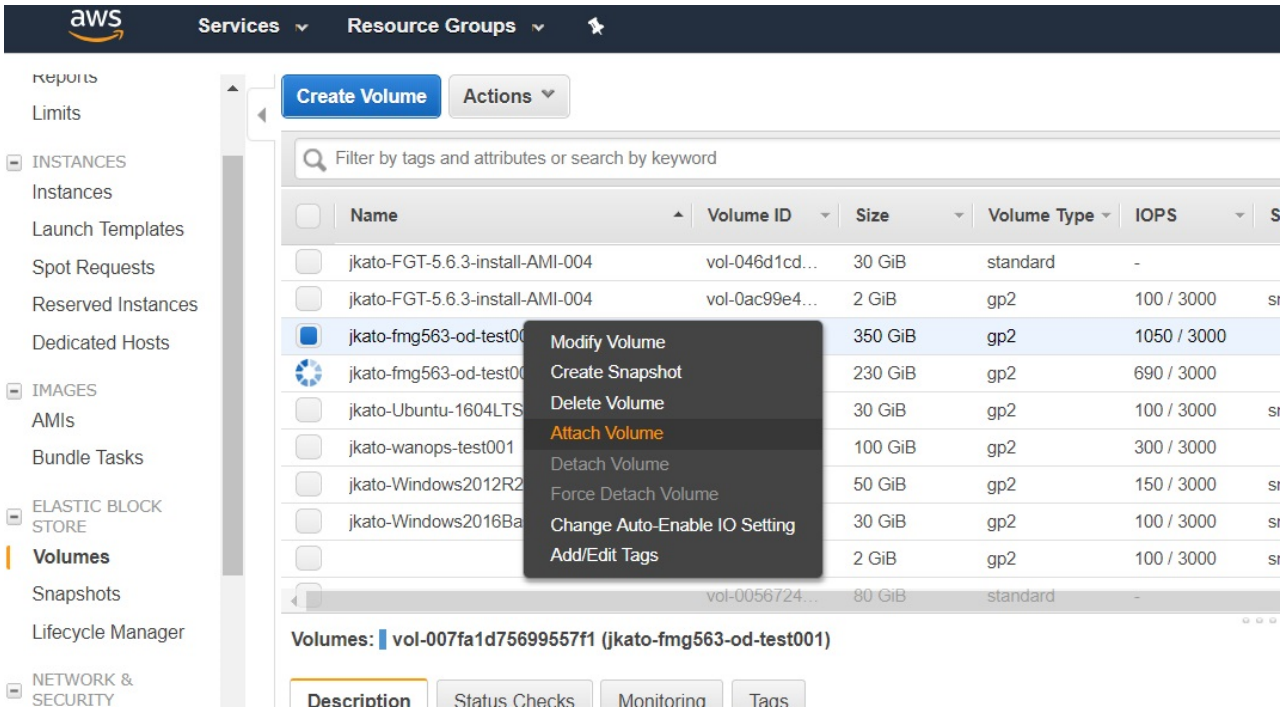
You can add additional storage to FortiManager after launch. Create an EBS storage and attach it to the FortiManager instance on EC2 console, then access FortiManager via the CLI window on the GUI or SSH to run the `exec lvm extend` command to add storage.

For details, refer to Technical Note: Extending disk space in FortiAnalyzer VM / FortiManager VM.

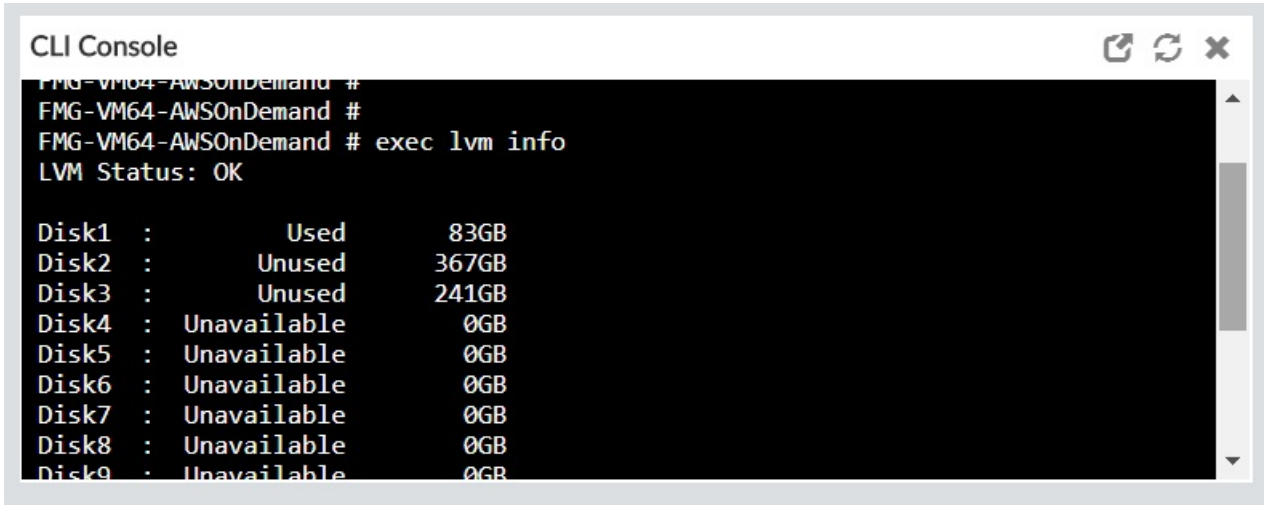
This example creates and attaches two volumes.

To add additional storage:

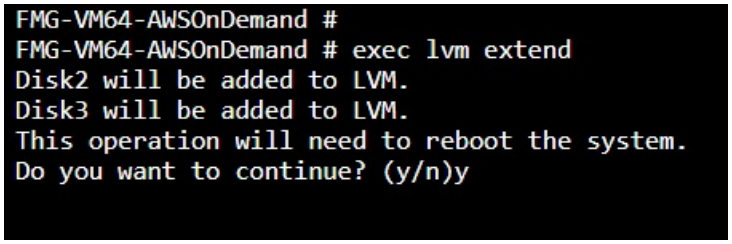
1. In the EC2 console, create a disk volume and attach it to the FortiManager EC2 instance.



2. Log in to FortiManager using the GUI or SSH. If using the GUI, open the CLI.
3. Run `exec lvm info` to check the disk status. Two volumes have been added and are *Unused*.



4. Run `exec lvm extend`. Reboot the system as instructed.



5. Log in to the FortiManager GUI. Go to the Dashboard and verify you now have enlarged disk space under *System Resources* > *Disk Usage*.

SDN connector integration with AWS

You can use FortiManager to create SDN connectors for AWS and install the SDN connectors to FortiOS.

The SDN connectors in FortiManager define the connector type and include information for FortiOS to communicate with and authenticate with the products. In some cases the FortiGate must communicate with products through the SDN connector, and in other cases the FortiGate communicates directly with the products.

FortiOS works without the SDN connector to communicate directly with AWS.

Following is an overview of creating SDN connectors for AWS using FortiManager:

1. Create an SDN connector object for AWS. See Creating Fabric connector objects for AWS on page 17.
2. Import address names from AWS to the SDN connector object. See Importing address names to fabric connectors on page 19.
   The address names are imported and converted to firewall address objects. The objects do not yet include IP addresses. The objects display on the *Firewall Objects* > *Addresses* pane.
3. In the policy package in which you will be creating the new policy, create an IPv4 policy and include the firewall address objects for AWS. See Creating an IP address policy on page 20.
4. Install the policy package to FortiGate. See Installing a policy package on page 21.
   FortiGate communicates with AWS to dynamically populate the firewall address objects with IP addresses.

If the filter names change in AWS after you import them to FortiManager, you must modify the filter again.

Certificate-based SDN connector integration

Configuring certificate-based AWS SDN connector integration consists of the following:

1. Creating Fabric connector objects for AWS on page 17
2. Configuring dynamic firewall addresses for Fabric connectors on page 18
3. Importing address names to fabric connectors on page 19
4. Creating an IP address policy on page 20
5. Installing a policy package on page 21

Creating Fabric connector objects for AWS

With FortiManager, you can create a fabric connector for Amazon Web Services (AWS), and then import address names from AWS to automatically create dynamic objects that you can use in policies. When you install the policies to one or more FortiGate units, FortiGate uses the information to communicate with AWS and dynamically populate the objects with IP addresses. Fortinet SDN Connector is not required for this configuration.

When you create a fabric connector for AWS, you are specifying how FortiGate can communicate directly with AWS.

If ADOMs are enabled, you can create one fabric connector per ADOM.

Requirements:

- FortiManager version 6.0 ADOM or later
- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with AWS.

Following is a high-level overview of the configuration procedure:

To create a fabric connector object for AWS:

1. Go to *Fabric View* > *Fabric Connectors*.
2. Click *Create New*. The *Create New Fabric Connector* wizard is displayed.
3. Under *SDN*, select *AWS*, and click *Next*.
4. Configure the following options, and then click *OK*:

Name	Type a name for the fabric connector object.
Type	Displays *Amazon Web Services (AWS)*.
AWS access key ID	Type the access key ID from AWS.
AWS secret access key	Type the secret access key from AWS.
AWS region name	Type the region name from AWS.
AWS VPC ID	Type the AWS VPC ID.
Update Interval (s)	Specify how often in seconds that the dynamic firewall objects should be updated.
Status	Toggle *On* to enable the fabric connector object. Toggle *OFF* to disable the fabric connector object.

Configuring dynamic firewall addresses for Fabric connectors

You cannot import address names to fabric connectors created for Microsoft Azure and Nuage Virtualized Services Platform. Instead you must create dynamic firewall objects that can be dynamically populated when FortiGate communicates with Microsoft Azure and Nuage Virtualized Services Platform.

To configure dynamic firewall addresses for Microsoft Azure fabric connectors:

1. Go to *Policy & Objects* > *Object Configurations*.
2. In the tree menu, go to *Firewall Objects* > *Addresses*.
3. In the content pane, click *Create New* and select *Address*.
4. Complete the following options for Microsoft Azure fabric connectors:

Address Name	Type a name for the firewall address object.
Type	Select *Fabric Connector Address*.
SDN	Select the Microsoft Azure fabric connector.
Filter	Type the name of the filter for the AWS instance.

5. Set the remaining options as required, and click *OK*

To configure dynamic firewall addresses for Nuage fabric connectors:

1. Go to *Policy & Objects* > *Object Configurations*.
2. In the tree menu, go to *Firewall Objects* > *Addresses*.
3. In the content pane, click *Create New* and select *Address*.
4. Complete the following options for Nuage fabric connectors:

Address Name	Type a name for the firewall address object.
Type	Select *Fabric Connector Address*.
SDN	Select the Nuage Virtualized Services Platform fabric connector.
Organization	Type the name of the organization for the Nuage Virtualized Services Platform.
Subnet Name	Type the name of the subnet for the Nuage Virtualized Services Platform.
Policy Group	Type the name of the policy group for the Nuage Virtualized Services Platform.

5. Set the remaining options as required, and click *OK*

Importing address names to fabric connectors

After you configure a Fabric connector, you can import dynamic objects from cloud platforms, such as AWS, to the Fabric connector, and dynamic firewall address objects are automatically created.

When you import address names from AWS, you must add filters to display the correct instances before importing address names.

To import address names for AWS:

1. Go to *Policy & Objects* > *Object Configurations*.
2. In the tree menu, go to *Security Fabric* > *Fabric Connectors*.
3. In the content pane, right-click the fabric connector, and select *Import*.
   The *Import SDN Connector* dialog box is displayed.

4. Create a filter to select the correct AWS instances:
   a. Click *Add Filter*.
      The *Filter Generator* dialog box is displayed.

b. Click *Add Filter*, and select a filter.
A filtered list of instances is displayed.

c. Click *OK*.
The *Import SDN Connector* dialog box is displayed, and it contains the filter.
You can add additional filters, or edit and delete filters.

d. (Optional) Repeat this procedure to add additional filters.

5. Select the filters, and click *Import*.
The address names are imported and converted to dynamic firewall address objects that are displayed on the *Firewall Objects* > *Addresses* pane. The name of the dynamic firewall address uses the following naming convention: `AWS-<random identifier>`. Use the *Details* column and the instance ID to identify the object.

Creating an IP address policy

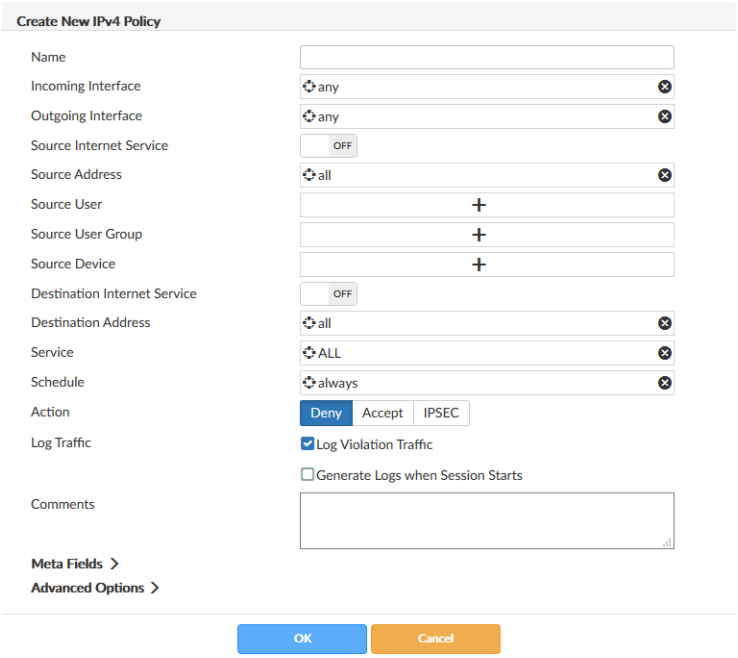
The section describes how to create new IPv4 and IPv6 policies.

IPv6 security policies are created both for an IPv6 network and a transitional network. A transitional network is a network that is transitioning over to IPv6, but must still have access to the Internet or must connect over an IPv4 network. IPv6 policies allow for this specific type of traffic to travel between the IPv6 and IPv4 networks.

On the *Policy & Objects* tab, from the *Tools* menu, select *Display Options*. In the *Policy* section, select the *IPv6 Policy* checkbox to display this option.

To create a new IPv4 or IPv6 policy:

1. Ensure that you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu for the policy package in which you will be creating the new policy, select *IPv4 Policy* or *IPv6 Policy*. If you are in the Global Database ADOM, select *IPv4 Header Policy*, *IPv4 Footer Policy*, *IPv6 Header Policy*, or *IPv6 Footer Policy*.
4. Click *Create New*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list, but above the implicit policy. The *Create New Policy* pane opens.



5. Complete the options.
6. Click *OK* to create the policy.
   You can select to enable or disable the policy in the right-click menu. When disabled, a disabled icon will be displayed in the *Seq.#* column to the left of the number.

Installing a policy package

When installing a policy package, objects that the policy references are installed to the target device. Default or per-device mapping must exist or the installation will fail.

Some objects that are not directly referenced in the policy will also be installed to the target device, such as FSSO polling objects, address and profile groups, and CA certificates.

To install a policy package to a target device:

1. Ensure you are in the ADOM that contains the policy package.
2. Go to *Policy & Objects* > *Policy Packages*.
3. Select a policy package and from the *Install* menu or right-click menu select *Install Wizard*. The *Install Wizard* opens.
4. Follow the steps in the install wizard to install the policy package. You can select to install policy package and device settings or install the interface policy only.

Configuring an AWS SDN connector using IAM roles

To configure an AWS SDN connector using IAM roles:

1. In *Policy & Objects*, go to *Fabric Connectors* > *SDN*.
2. Edit the existing AWS connector or create a new one.
3. Under *AWS Connector*, enable *Use Metadata IAM*. Ensure that the IAM role attached to the instance has sufficient permissions.

The following summarizes minimum sufficient IAM roles for this deployment:

```
{
   "Version": "2012-10-17",
   "Statement": [
   {
   "Action": [
   "ec2:Describe*"
   ],
   "Resource": "*",
   "Effect": "Allow"
   }
   ]
}
```

Change log

Date	Change Description
2020-04-09	Initial release.
2021-02-08	Added Configuring an AWS SDN connector using IAM roles on page 22.
2021-07-22	Updated supported instance types in Instance type support on page 4.
2022-09-07	Updated Order types on page 7.