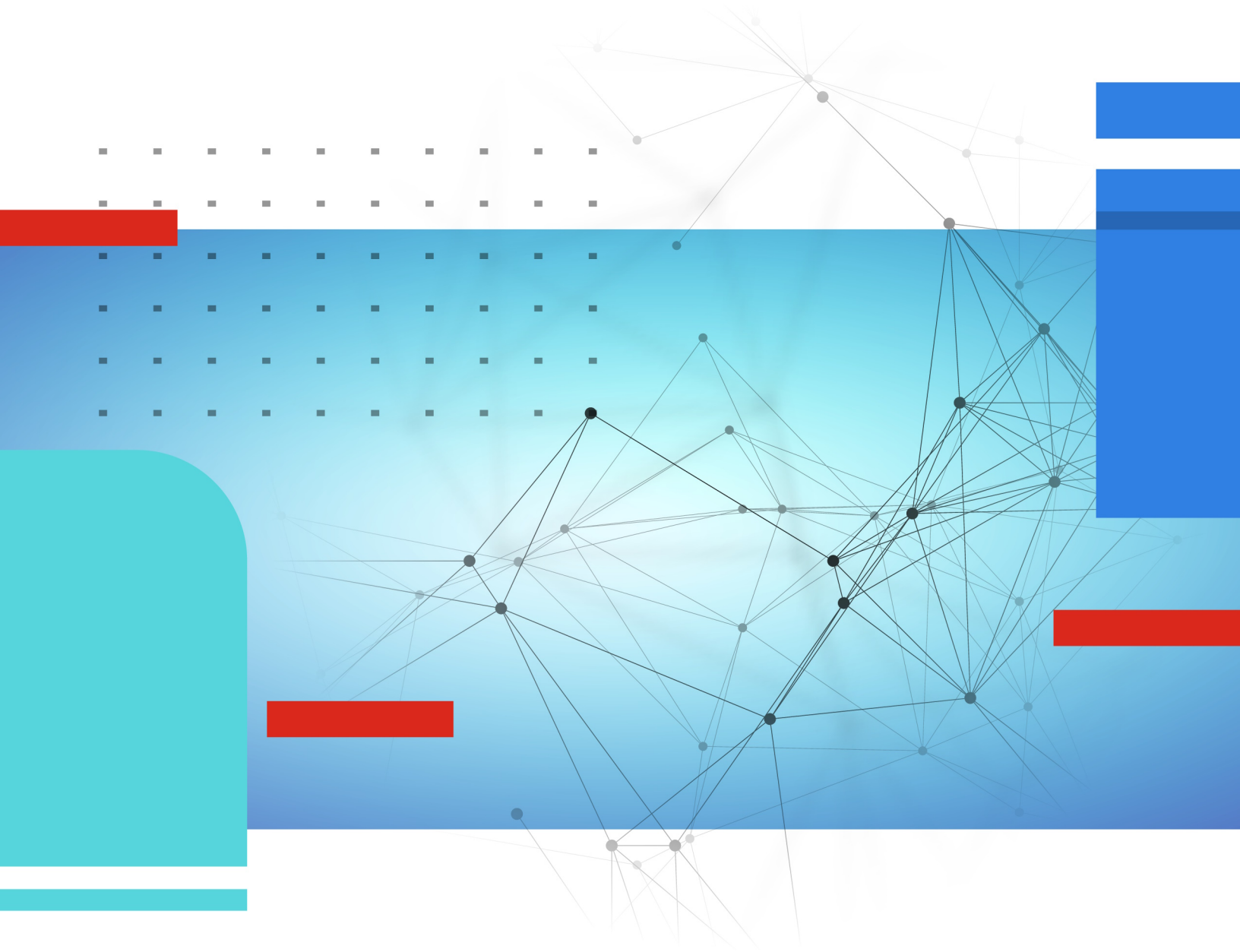
OCI Deployment Guide

FortiMail 7.2.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

October 22, 2024
FortiMail 7.2.0 OCI Deployment Guide
06-720-000000-20241022

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-10-22	Initial release of FortiMail 7.2.0 OCI Deployment Guide

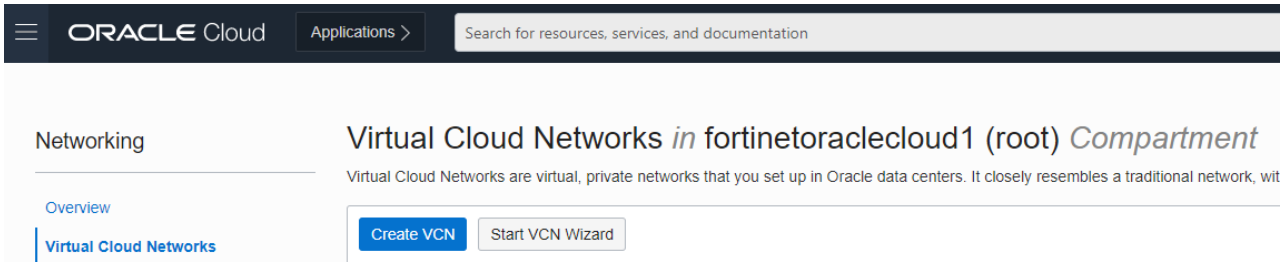
Introduction

This document describes how to deploy FortiMail VM on Oracle Cloud Infrastructure (OCI). Note that some company or product related information is hidden on purpose in the screen captures.

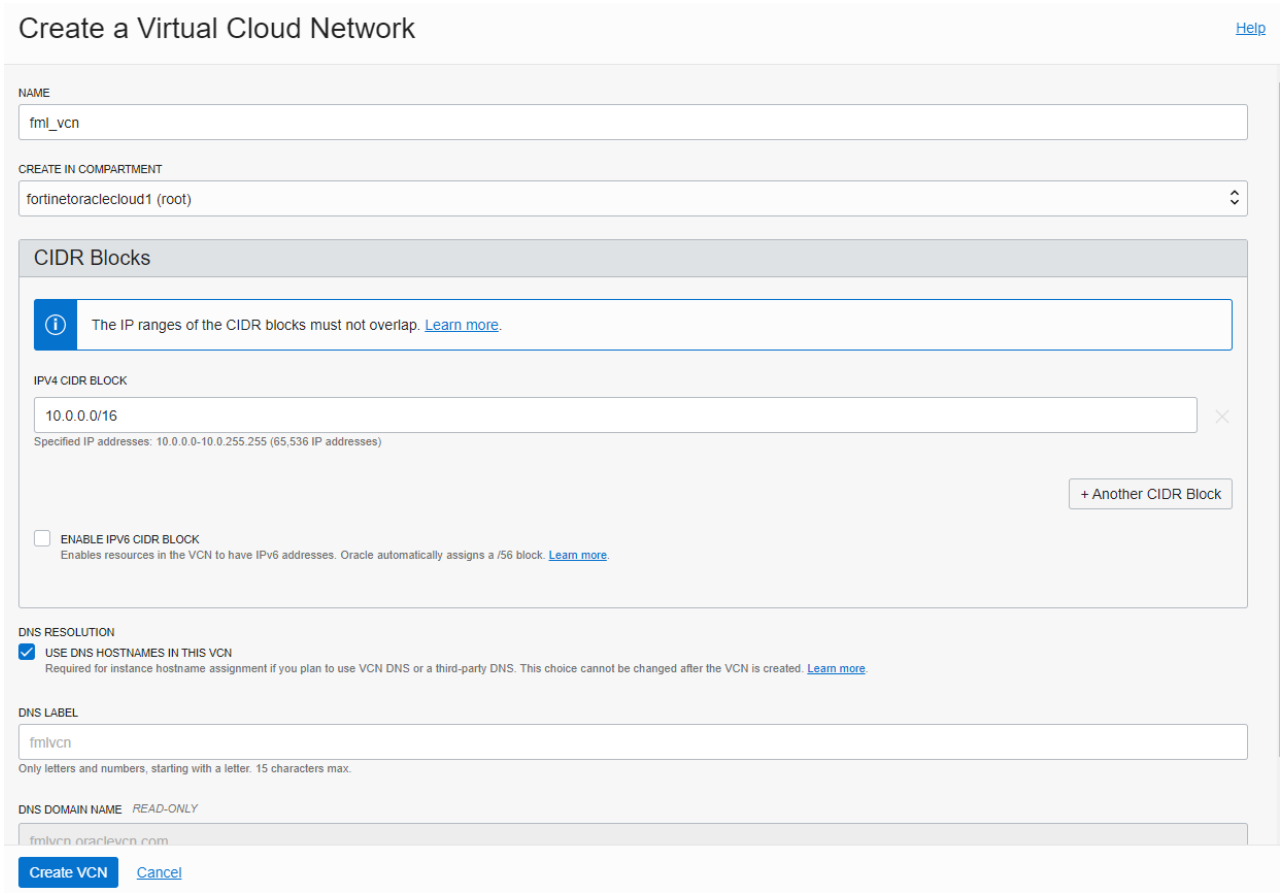
For details about how to use FortiMail, see the FortiMail Administration Guide on https://docs.fortinet.com.

Creating a Virtual Cloud Network and Public-facing Subnet

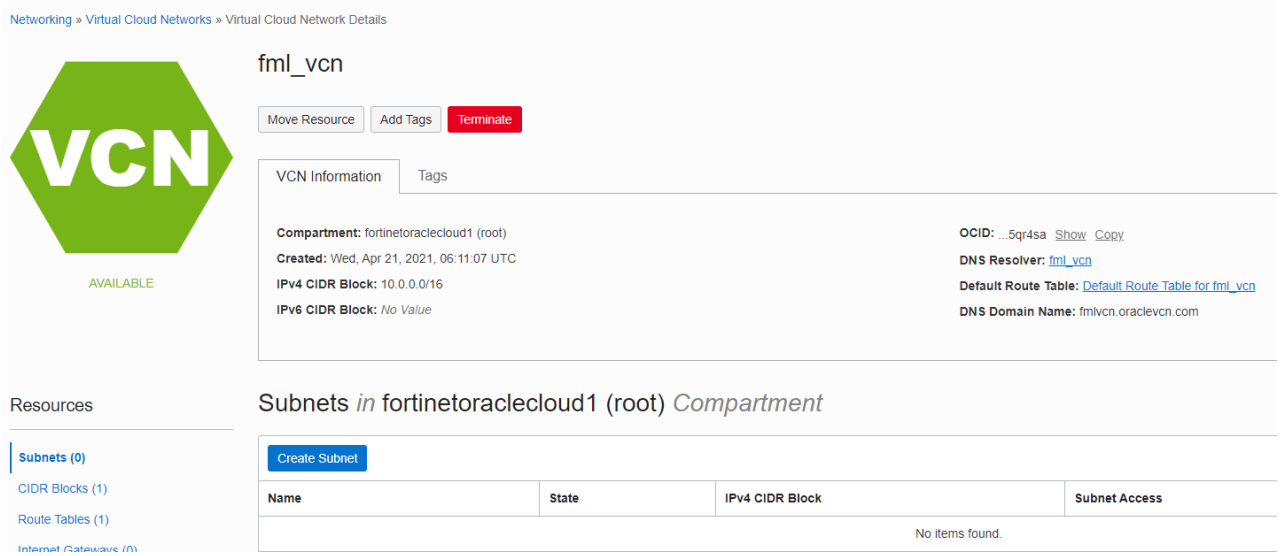
1. In OCI, go to **Networking > Virtual Cloud Networks**, and click **Create Virtual Cloud Network**.



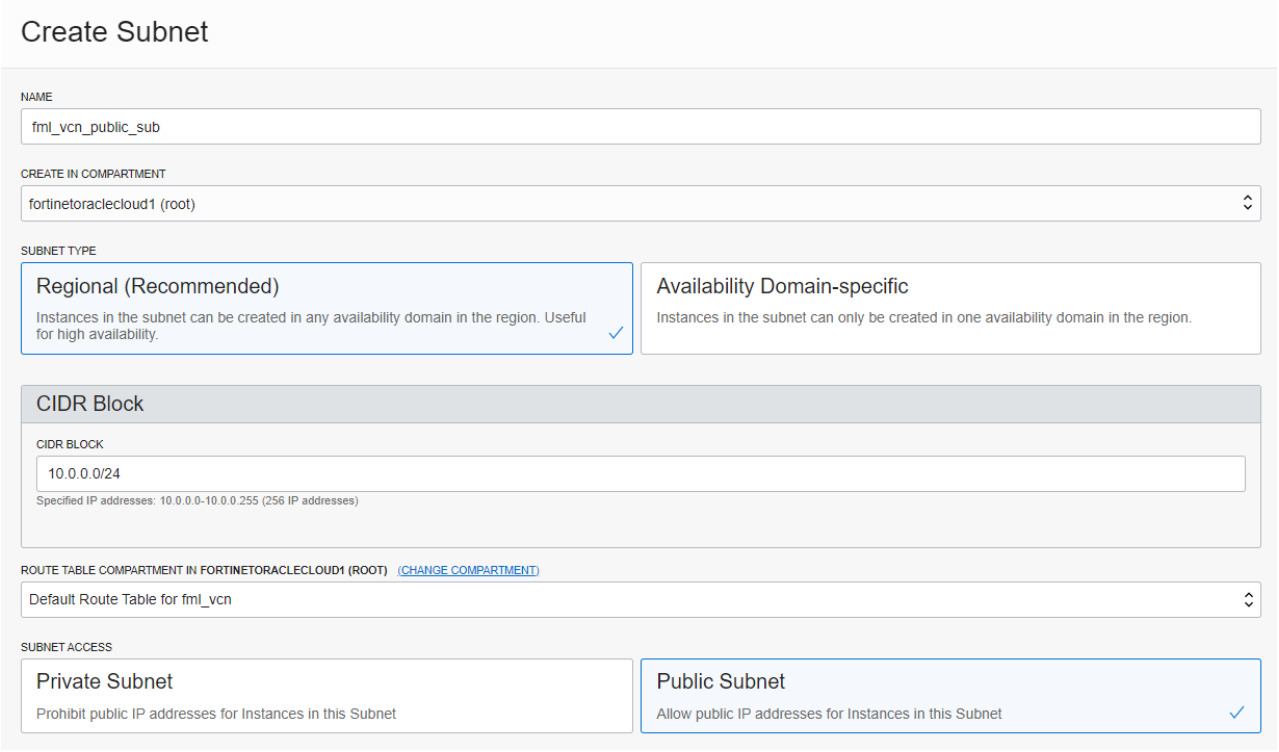
2. Enter the **NAME** and **IPV4 CIDR BLOCK**, then **Create VCN**.



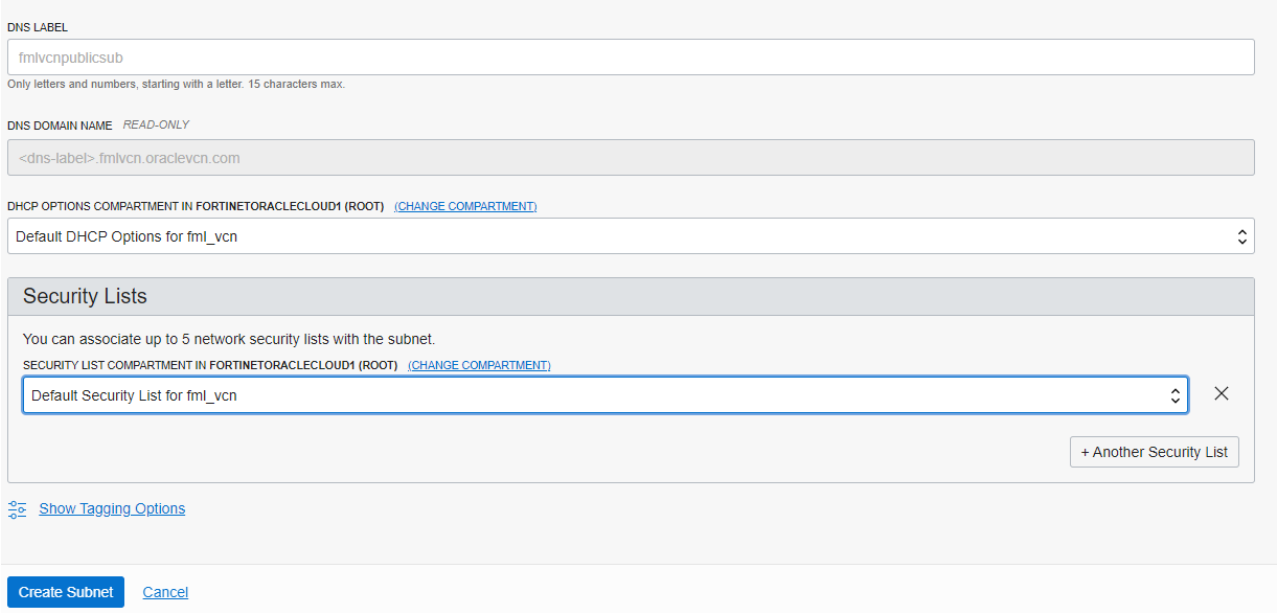
3. In the **VCN details** page, create a public-facing subnet.



4. When creating the subnet, choose **SUBNET TYPE** as **Regional** and **SUBNET ACCESS** as **Public Subnet**.

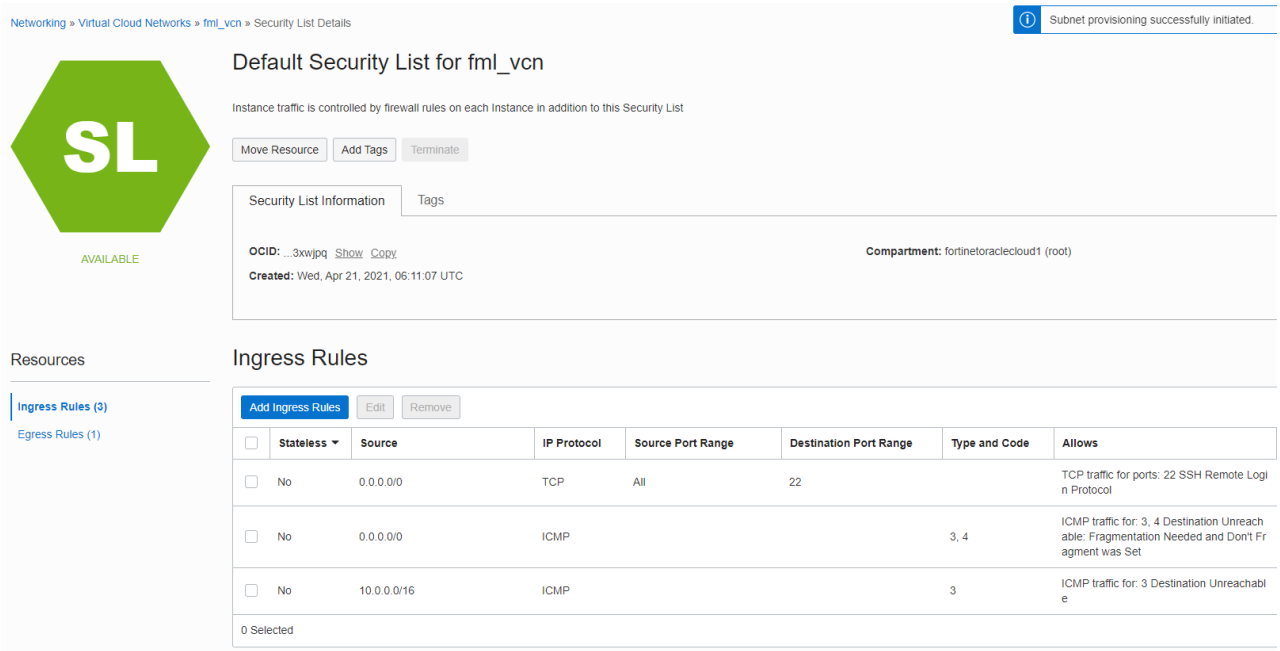


Leave **ROUTE TABLE**, **DHCP OPTIONS**, and **SECURITY LIST** as default, and you will need to modify them later.

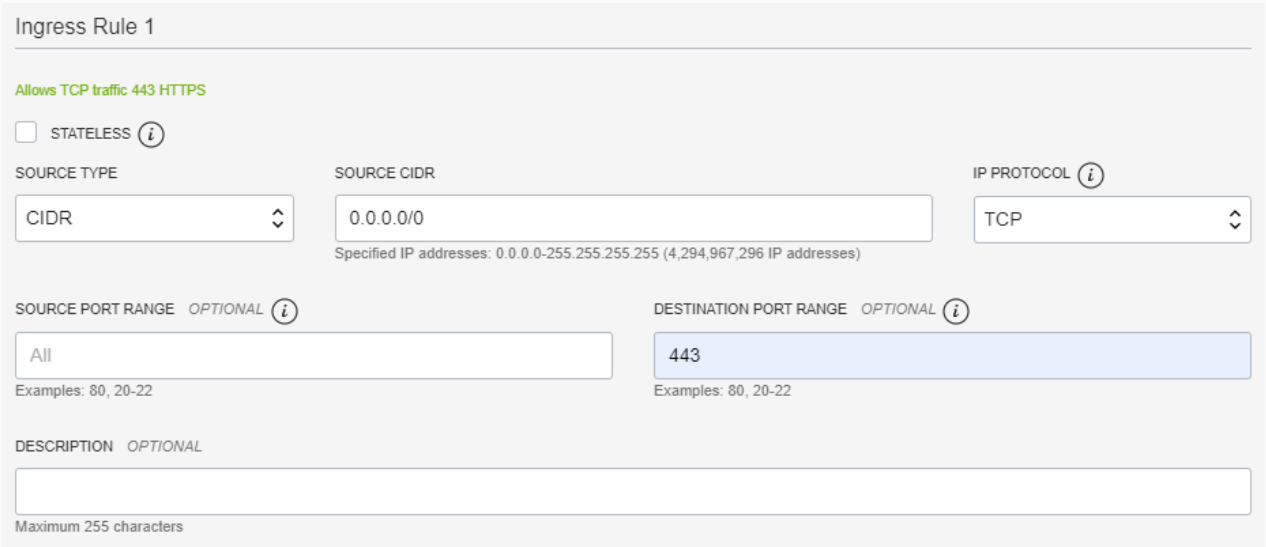


5. To access FortiMail with HTTPS, add an **Ingress Rule** in **Default Security List**.

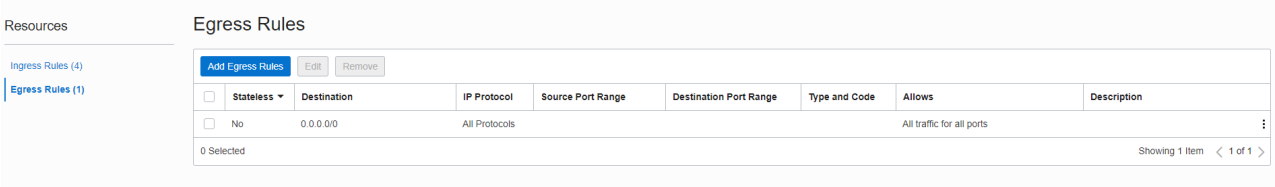
   You will see that three rules are set up by default, including port 22 for SSH access. There would be more ports needed for later testing, such as port 25 for SMTP, and you can always add or modify these rules later.



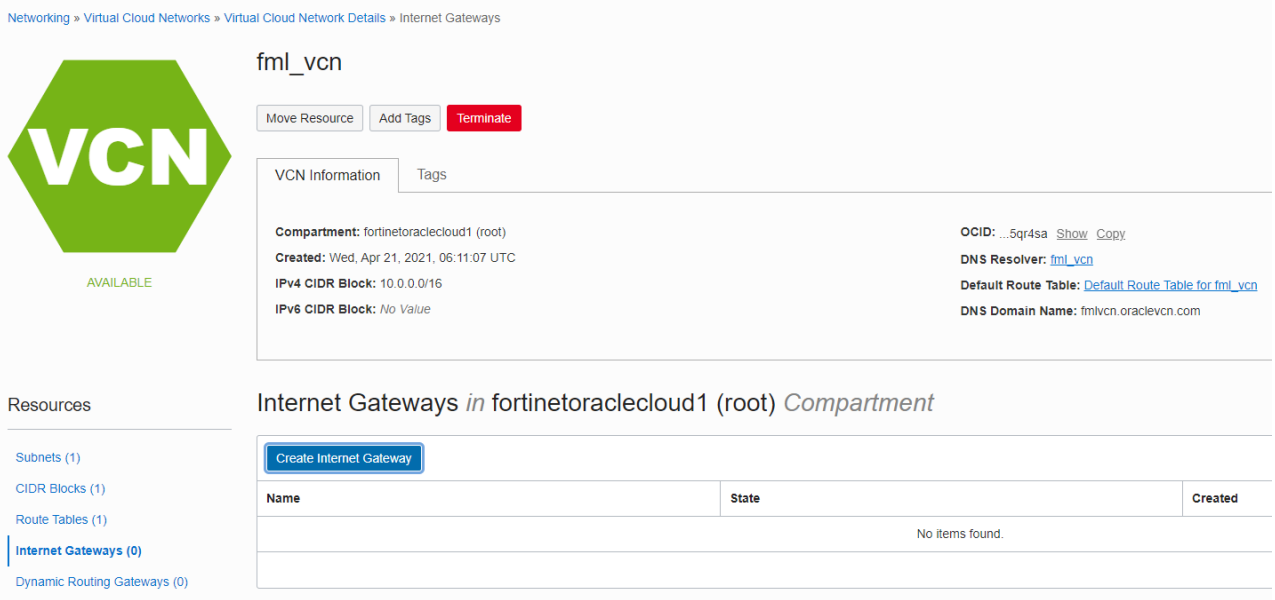
Add an **Ingress Rule** as below, and set **IP PROTOCOL** as **TCP** and **DESTINATION PORT** as **443**.

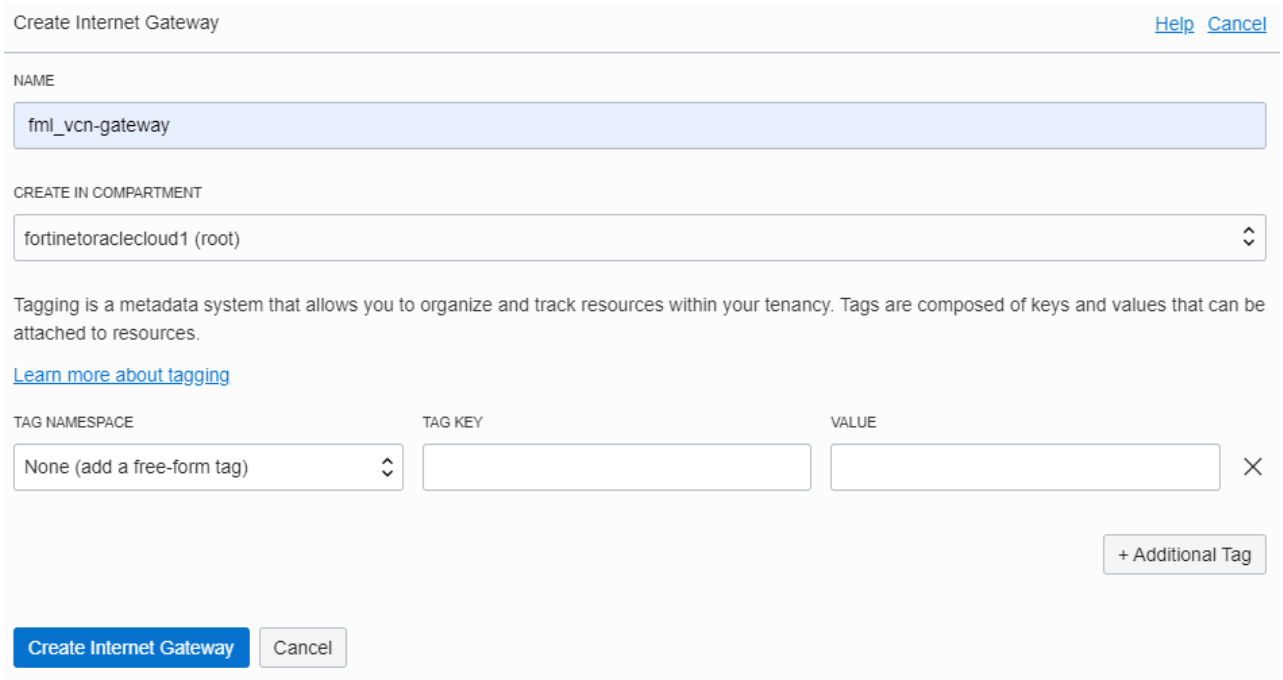


The Egress Rules are set for ALL TRAFFIC FOR ALL PORTS, and there is no need to modify it.

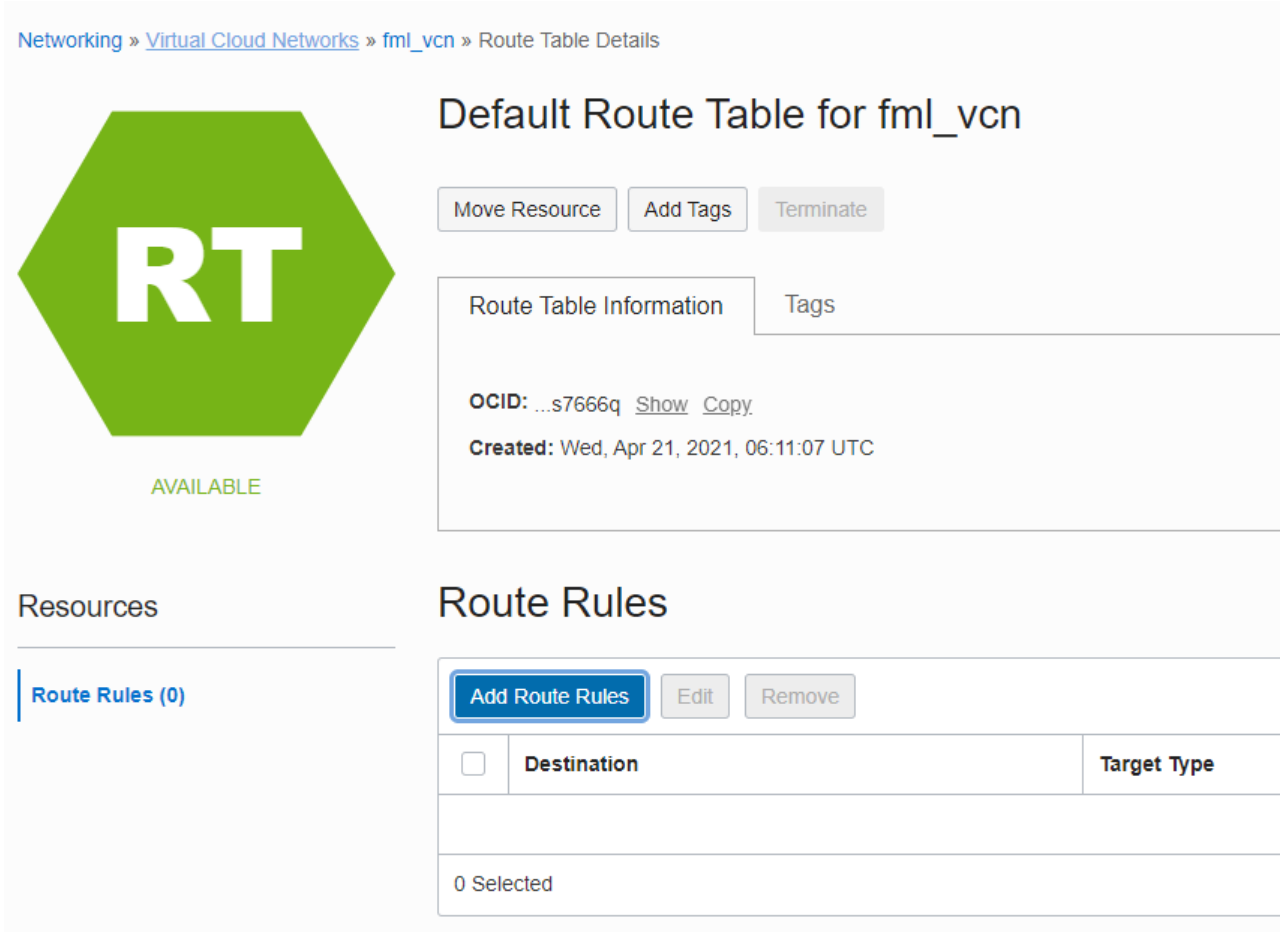


6. Create an **Internet Gateway** for your VCN.

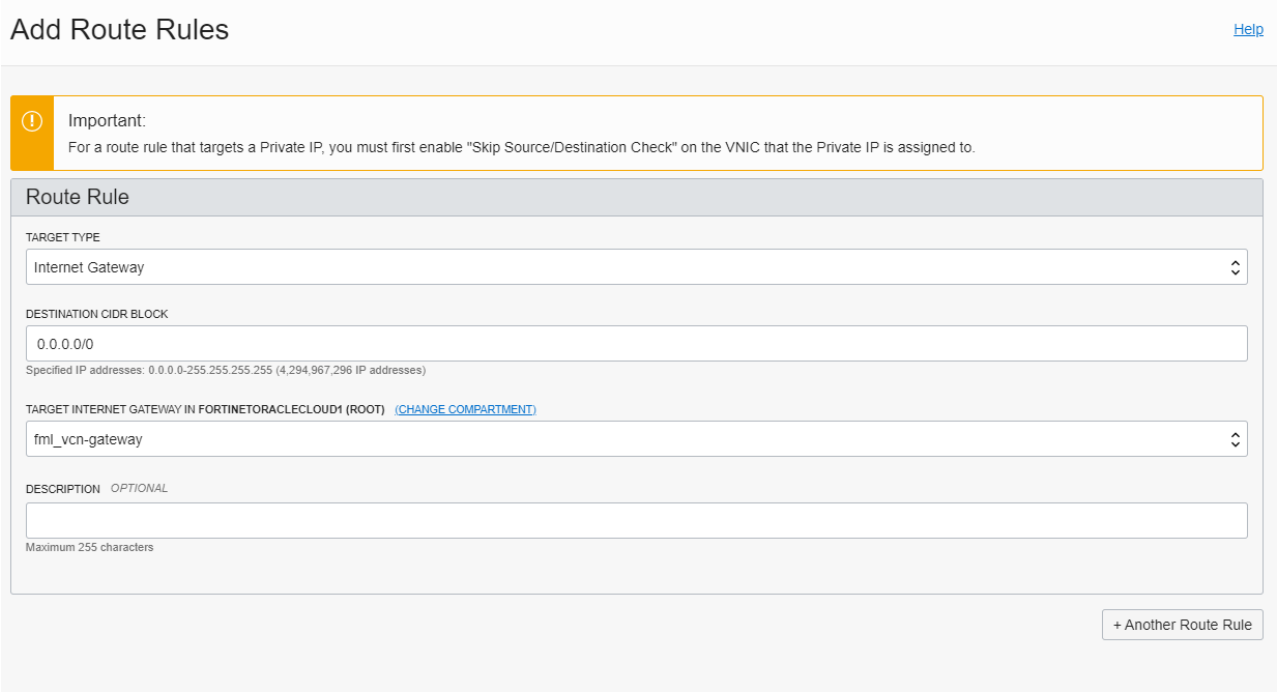




7. Add a **Route Rule** for the **Default Route Table**.

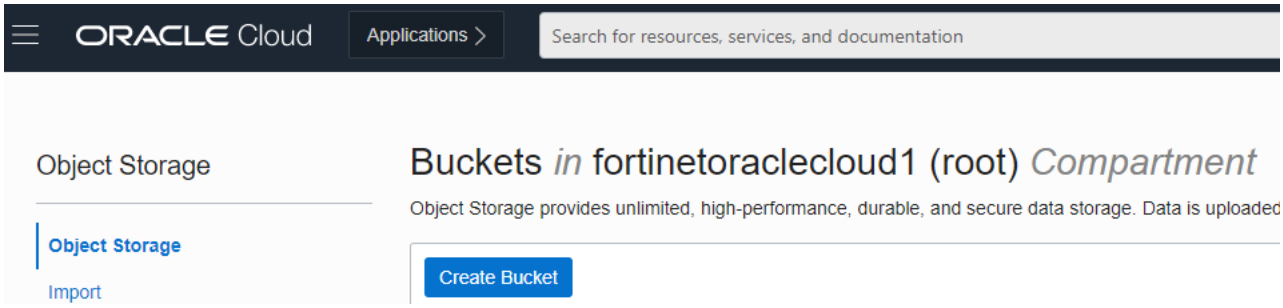


8. Choose **TARGET TYPE** as **Internet Gateway**, and choose the gateway you just created, and you can set **DESTINATION CIDR BLOCK** as **0.0.0.0/0** for all.

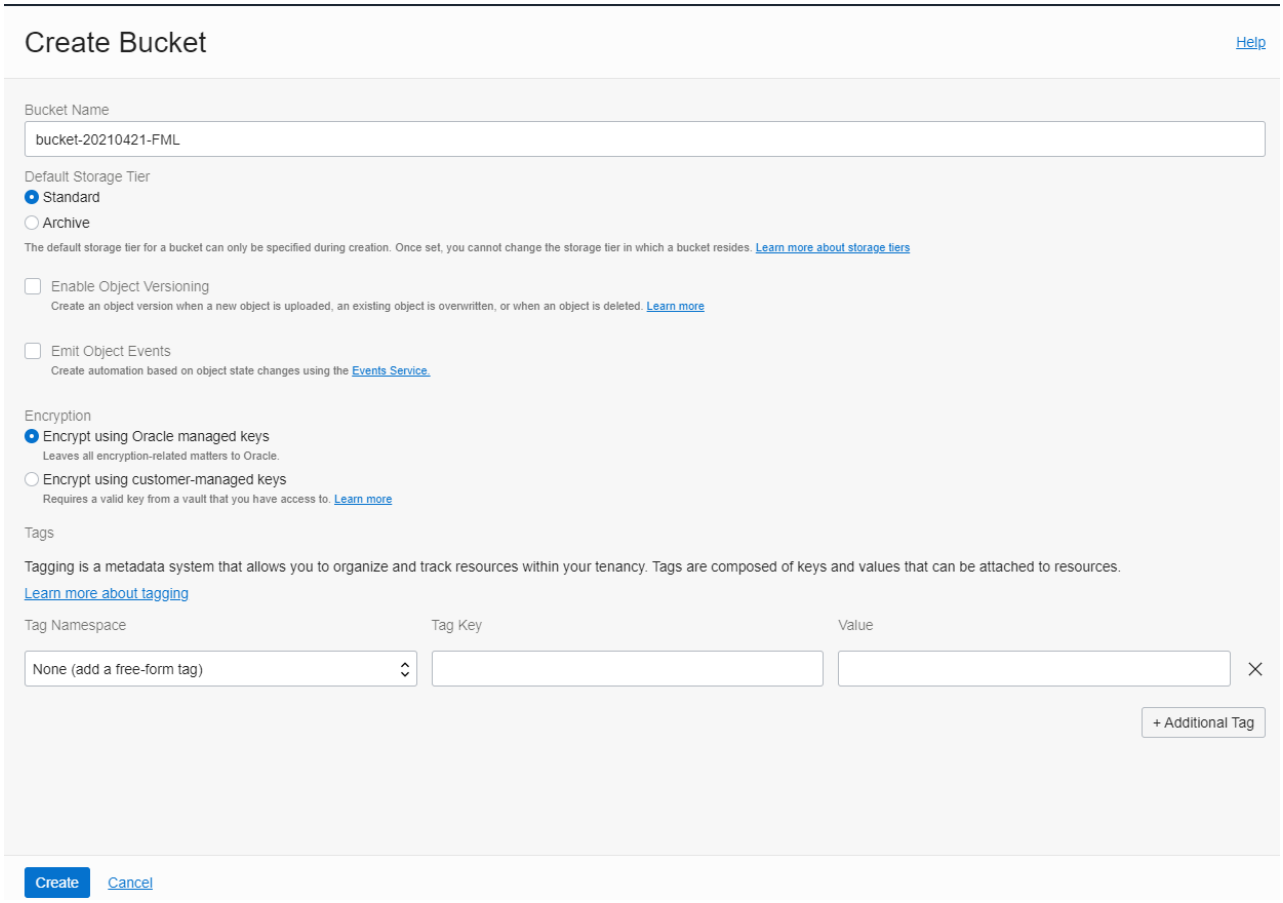


Creating a FortiMail-VM Instance

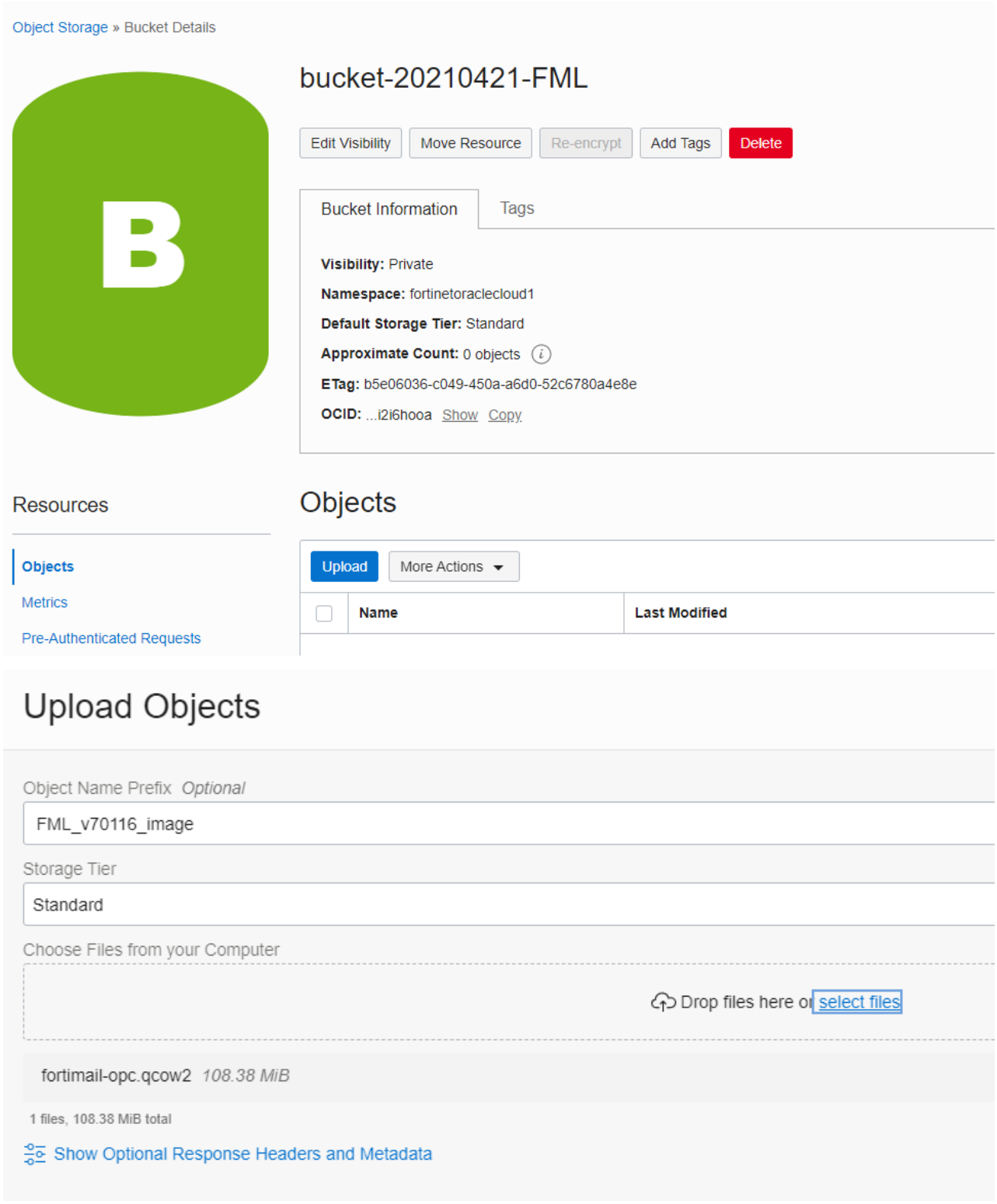
1. Go to https://support.fortinet.com and download the FortiMail VM image FML_VMOC-64-vxx-build0xxx-FORTINET.out.openxen.zip file. Unzip it to get the 'fortimail-opc.qcow2' file, which is needed to deploy FortiMail on OCI.
2. On OCI, go to **Object Storage**, then click **Create Bucket** to create a standard storage bucket.



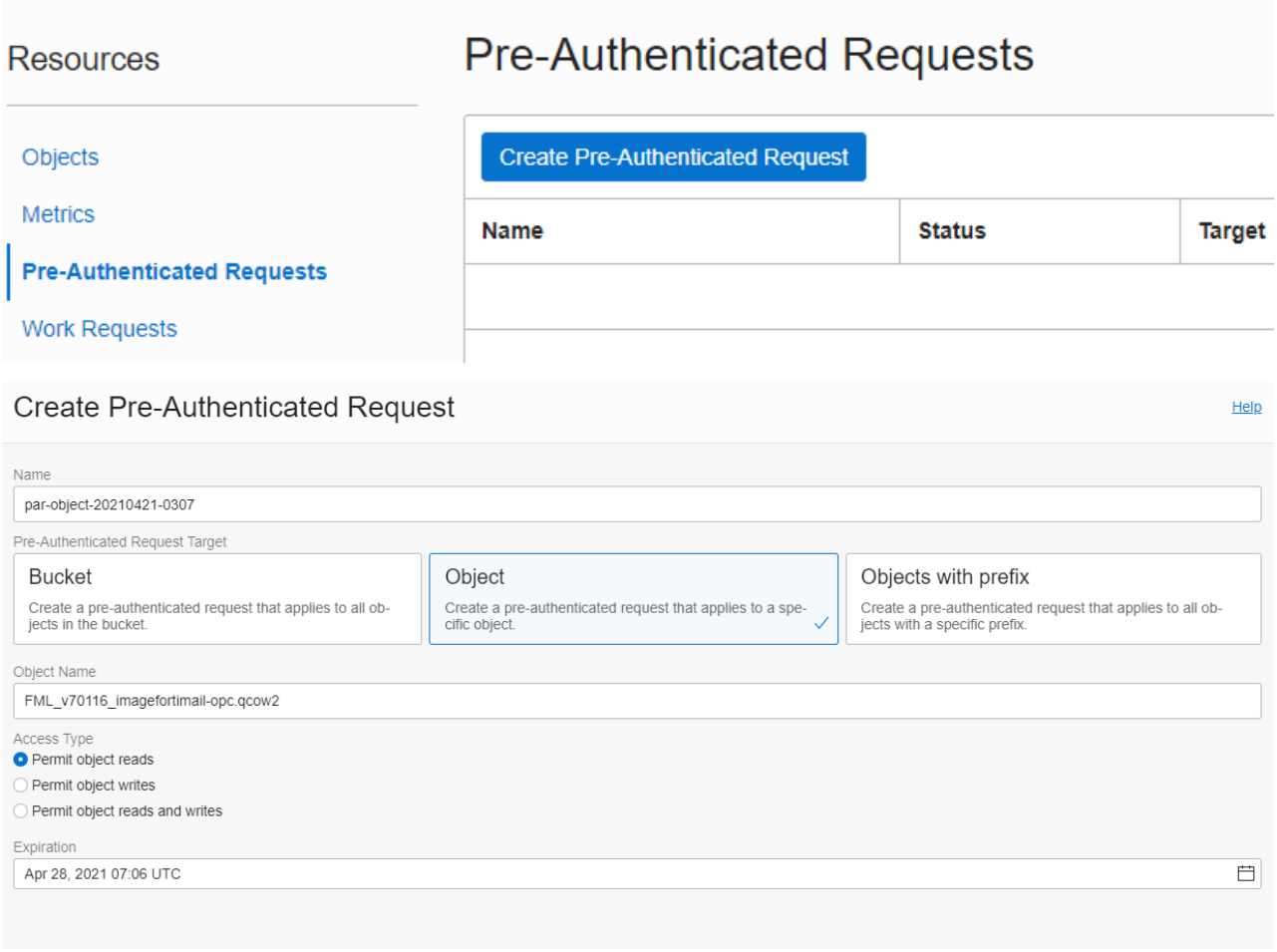
You can create the bucket with default settings.



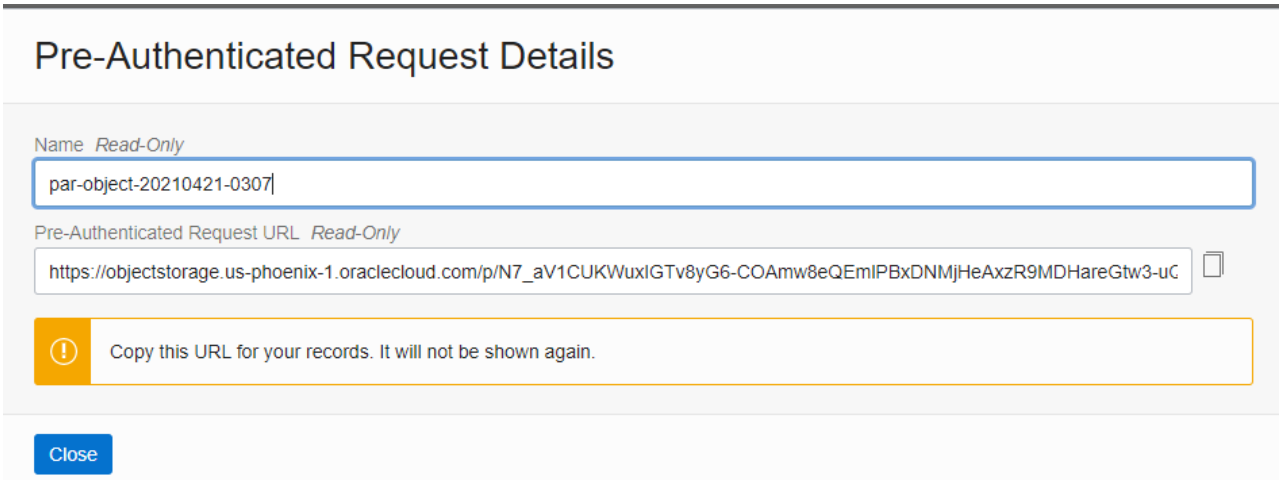
3. Click into the bucket you just created and upload the `*.qcow2` file to **Objects**.



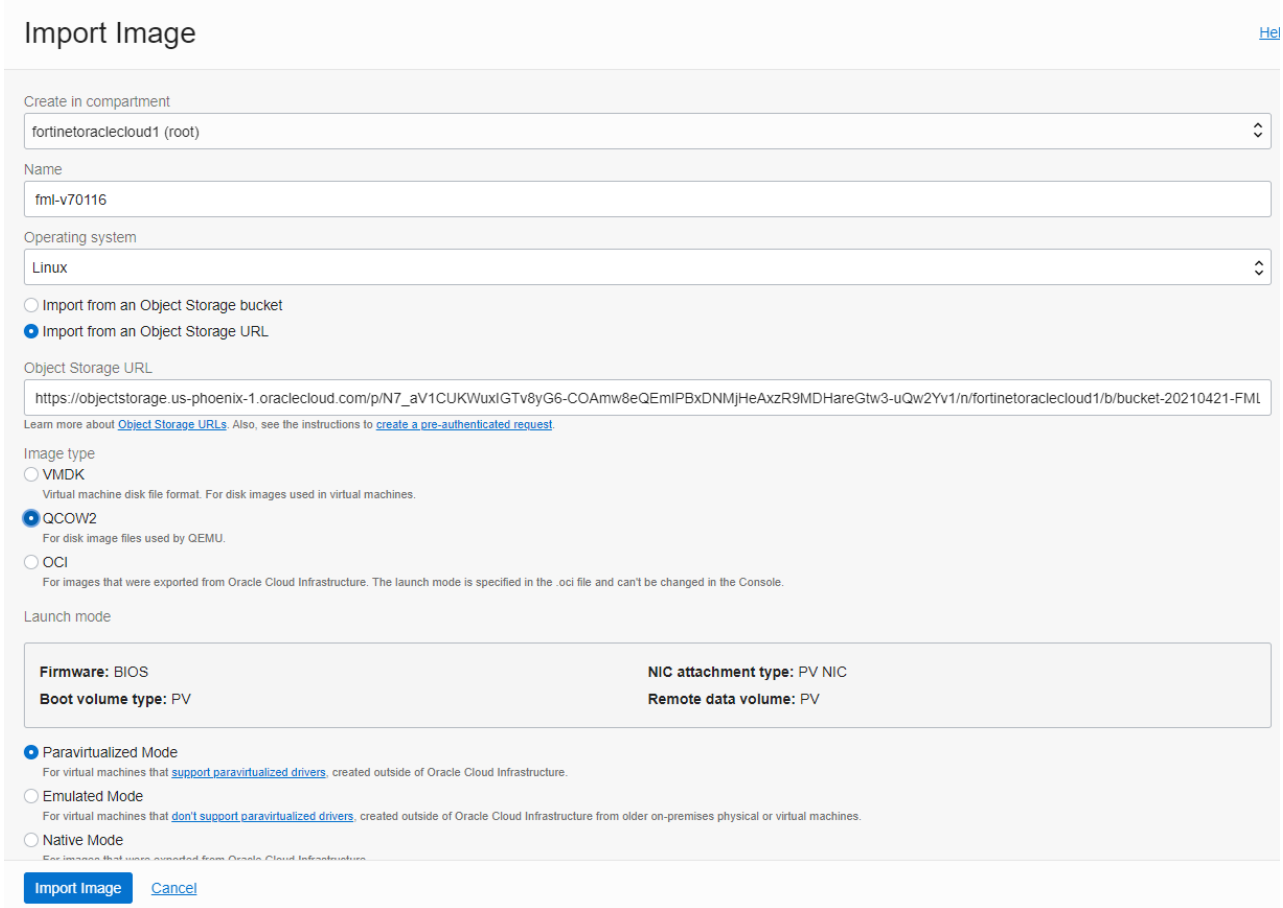
4. After the image file is uploaded, create a **Pre-Authenticated Request**.



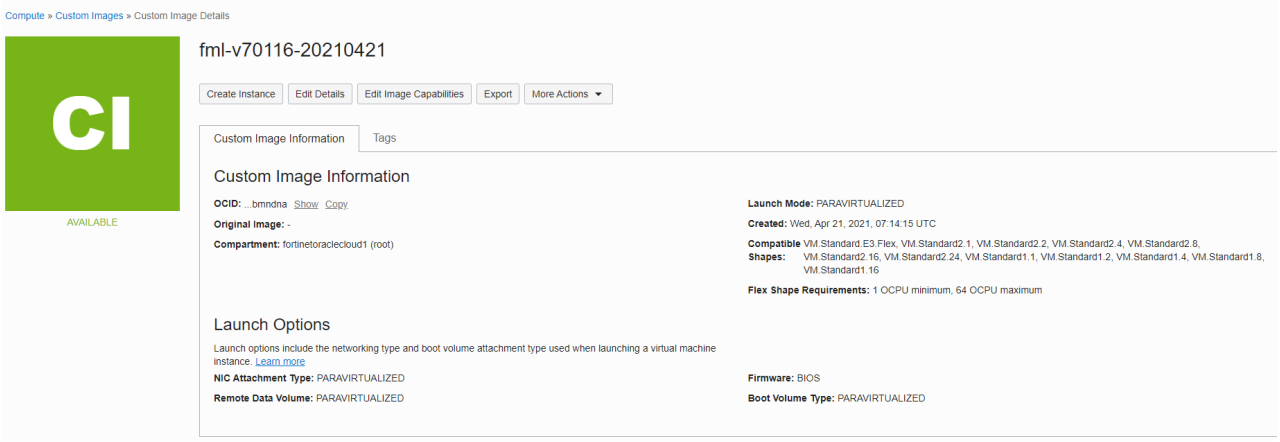
5. After the request is created, you will see the details window. Copy and save this URL, which will be used in later steps.



6. Go to **Compute > Custom Images**. Click **Import Image**. Choose **Import from an Object Storage URL** and paste the previous URL. Under **IMAGE TYPE**, select **QCOW2**. Under **LAUNCH MODE**, select **PARAVIRTUALIZED MODE** or **EMULATED MODE**. Native mode is not supported.



7. From the newly imported image, click **Create Instance**. Take note of the **Compatible Shapes**, and make sure to choose a shape from this list in later steps.



8. You can choose either **Availability domain** and keep the advanced options as default.

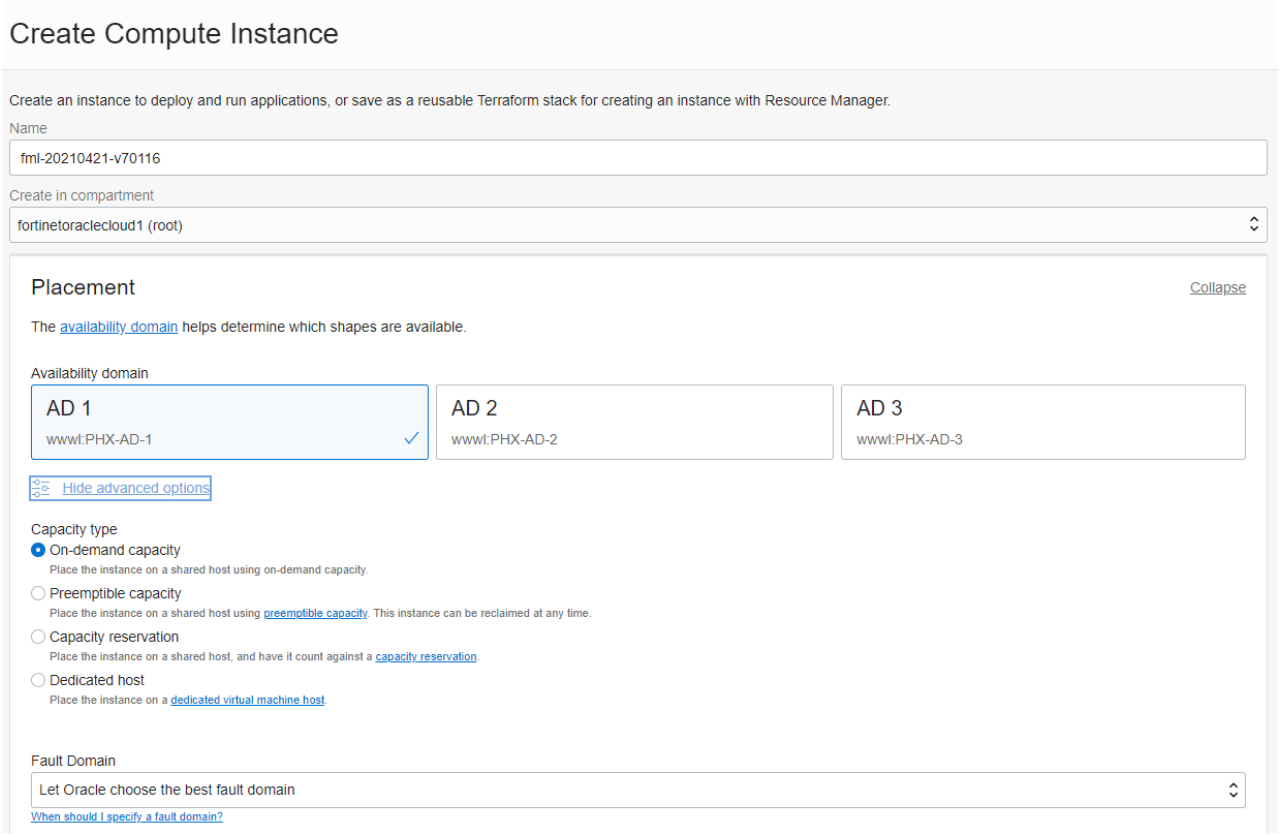
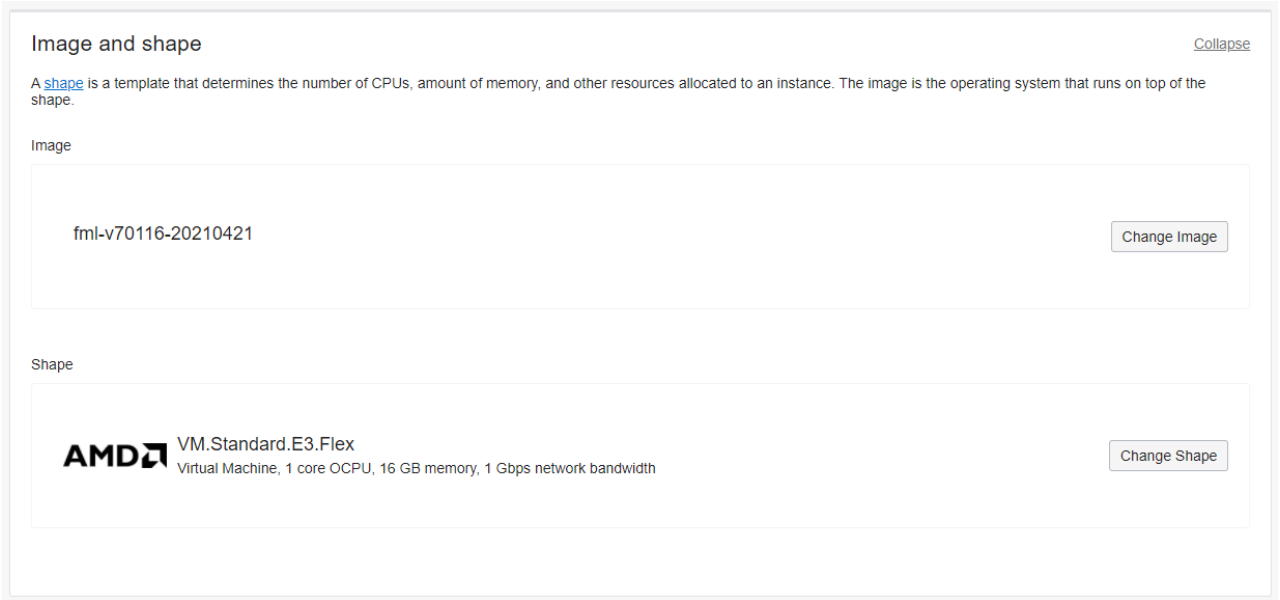
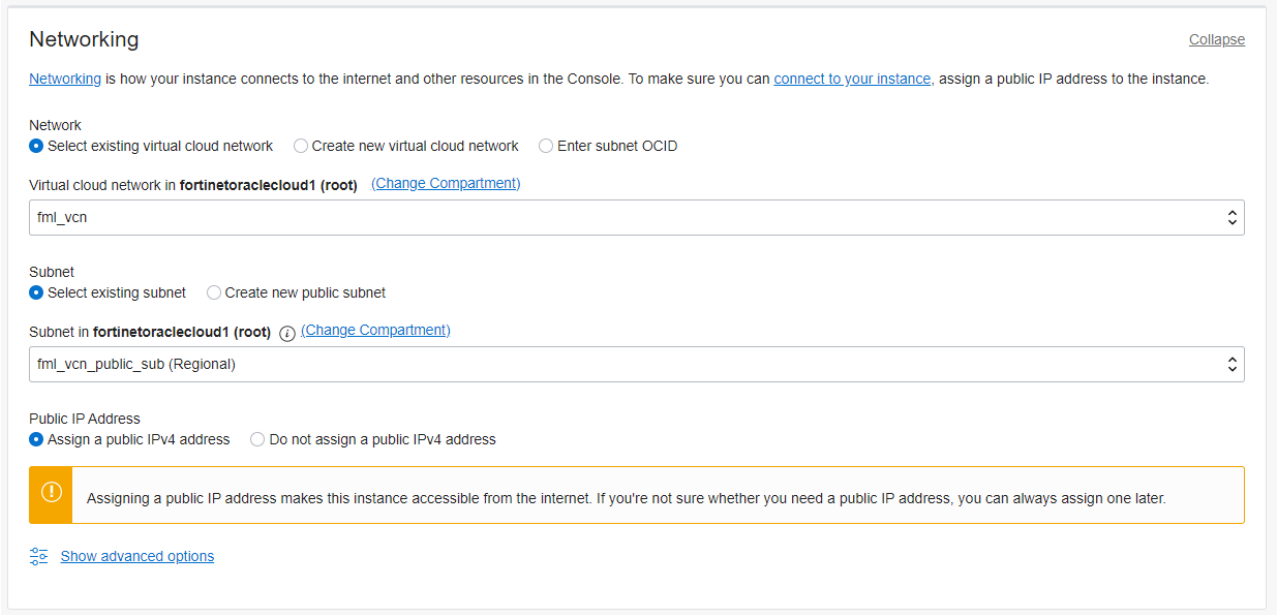


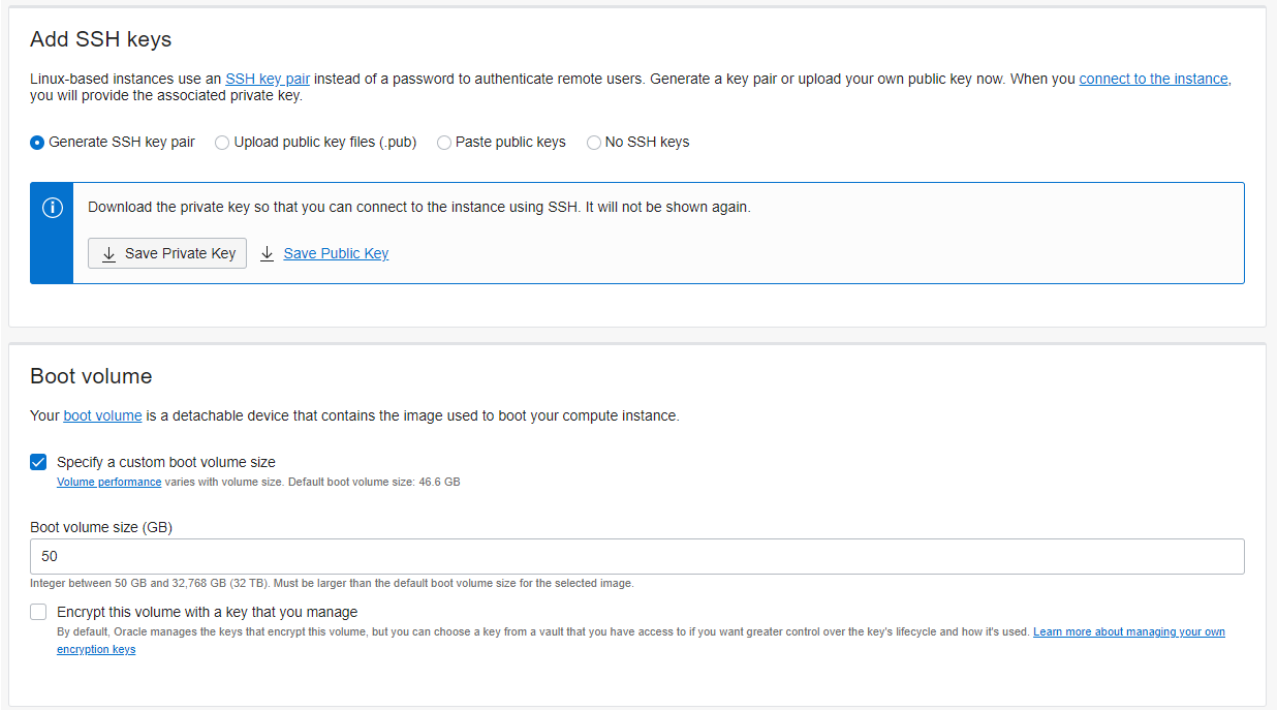
Image and shape are chosen automatically. You can modify the shape as desired.



9. Choose your VCN and its public subnet. For public access to FortiMail, you must assign a public IPV4 address.



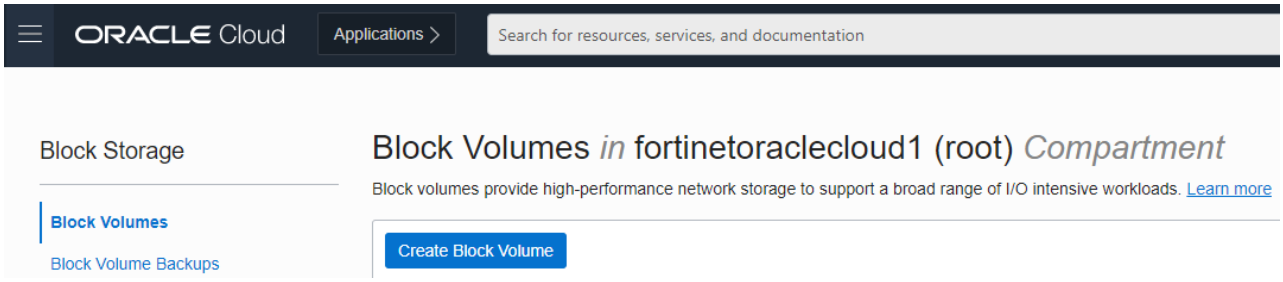
10. Click **Generate SSH key pair** and **Save Private Key**. The private key will be used for SSH accessing. You can also paste your own SSH public key or skip this step for now. Specify the customer boot volume size as minimum 50 GB.



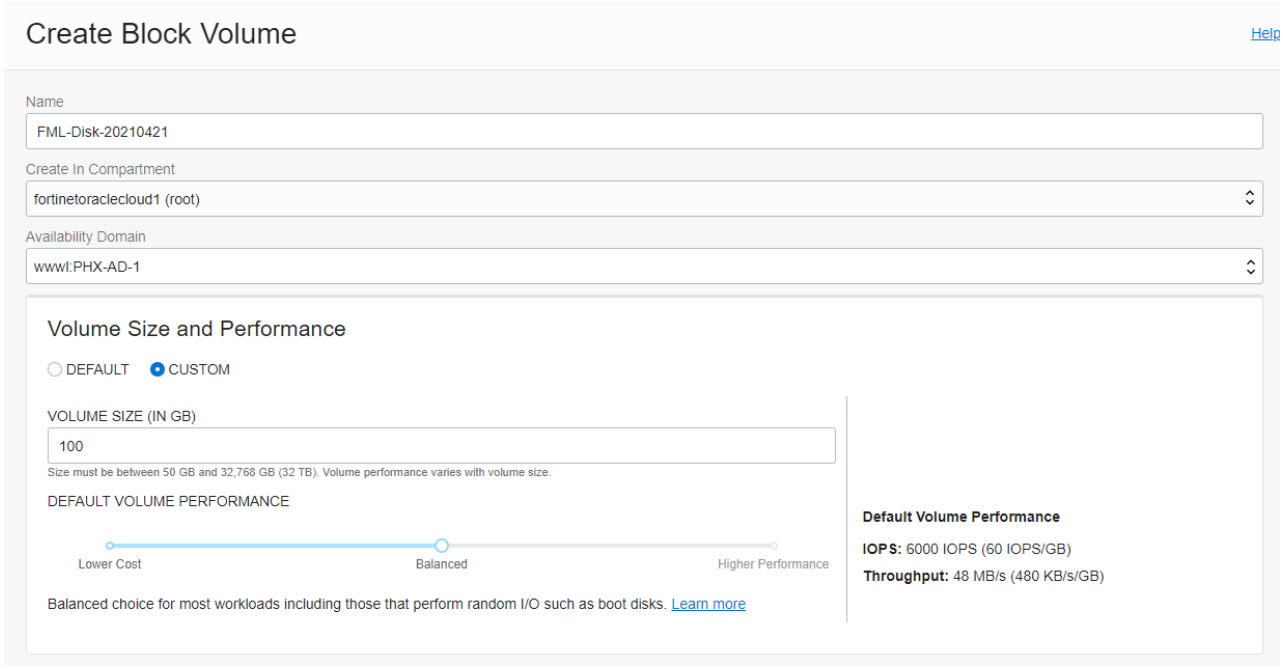
At this stage, the deployment is not complete yet. You also need to add a storage volume as a system log disk and attach it to the FortiMail instance. If you want FortiMail to run inline across two or multiple subnets, you will also need to add one or more virtual network interfaces and attach them to the FortiMail instance.

Attaching Storage to FortiMail

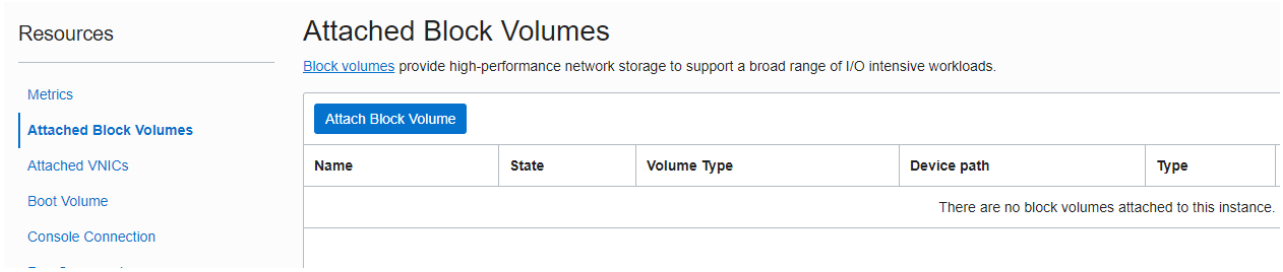
1. On OCI, go to **Storage > Block Volumes > Create Block Volume**.



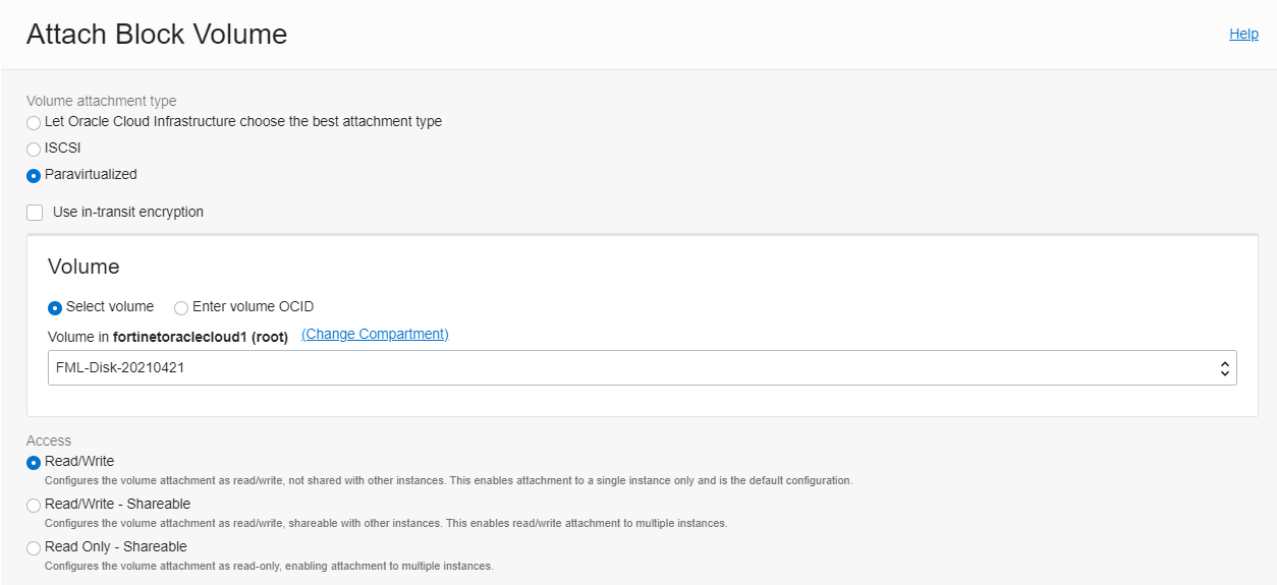
Make sure the **Availability Domain** is the same as your instance, and customize a smaller volume size, for example, 100 GB. Keep other settings as default.



2. Once provisioned, return to the FortiMail instance. Click **Attach Block Volume**.



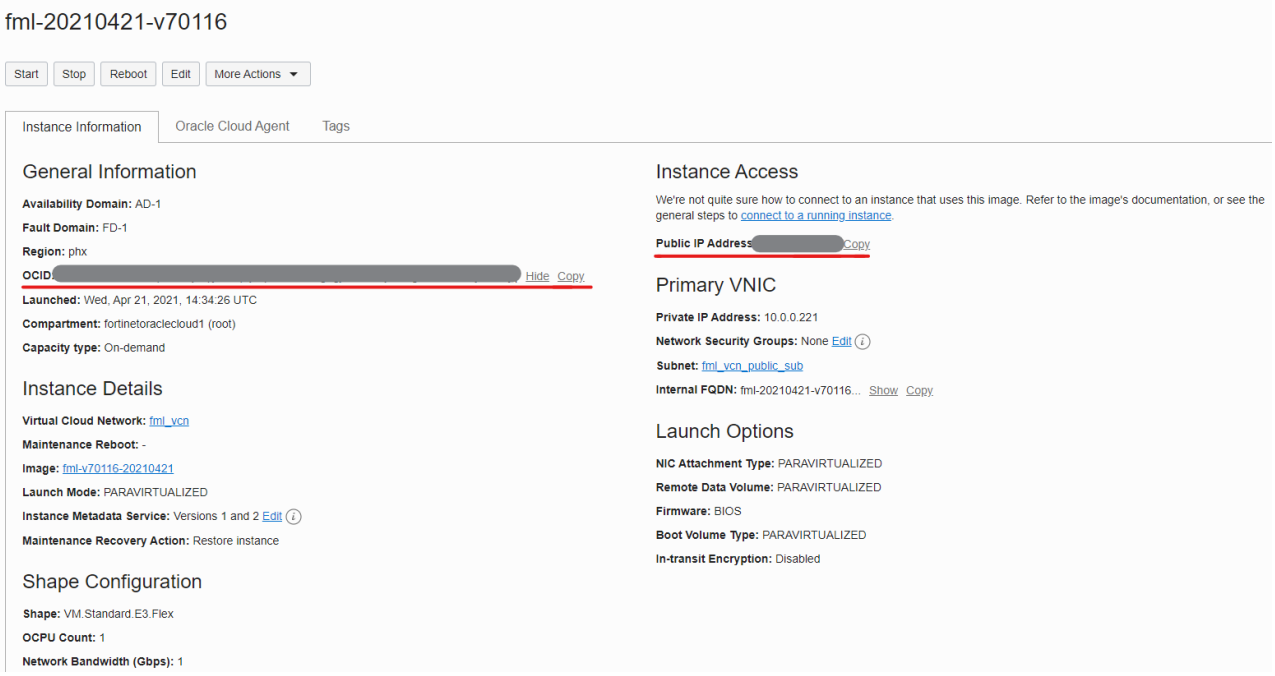
3. Select the block volume that you created earlier and ensure the attachment type is **Paravirtualized**.



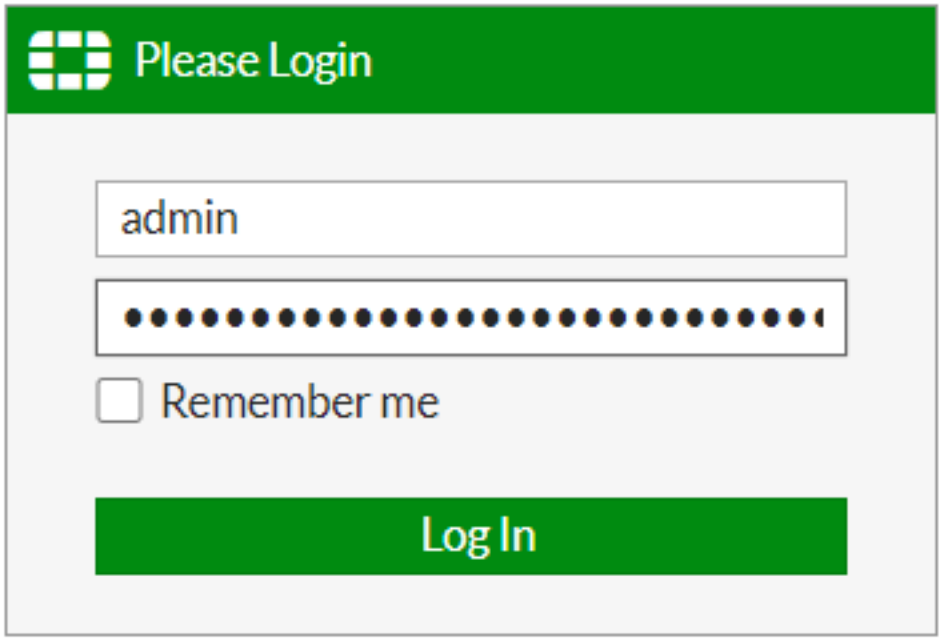
After attaching the block volume, make sure to reboot the FortiMail instance.

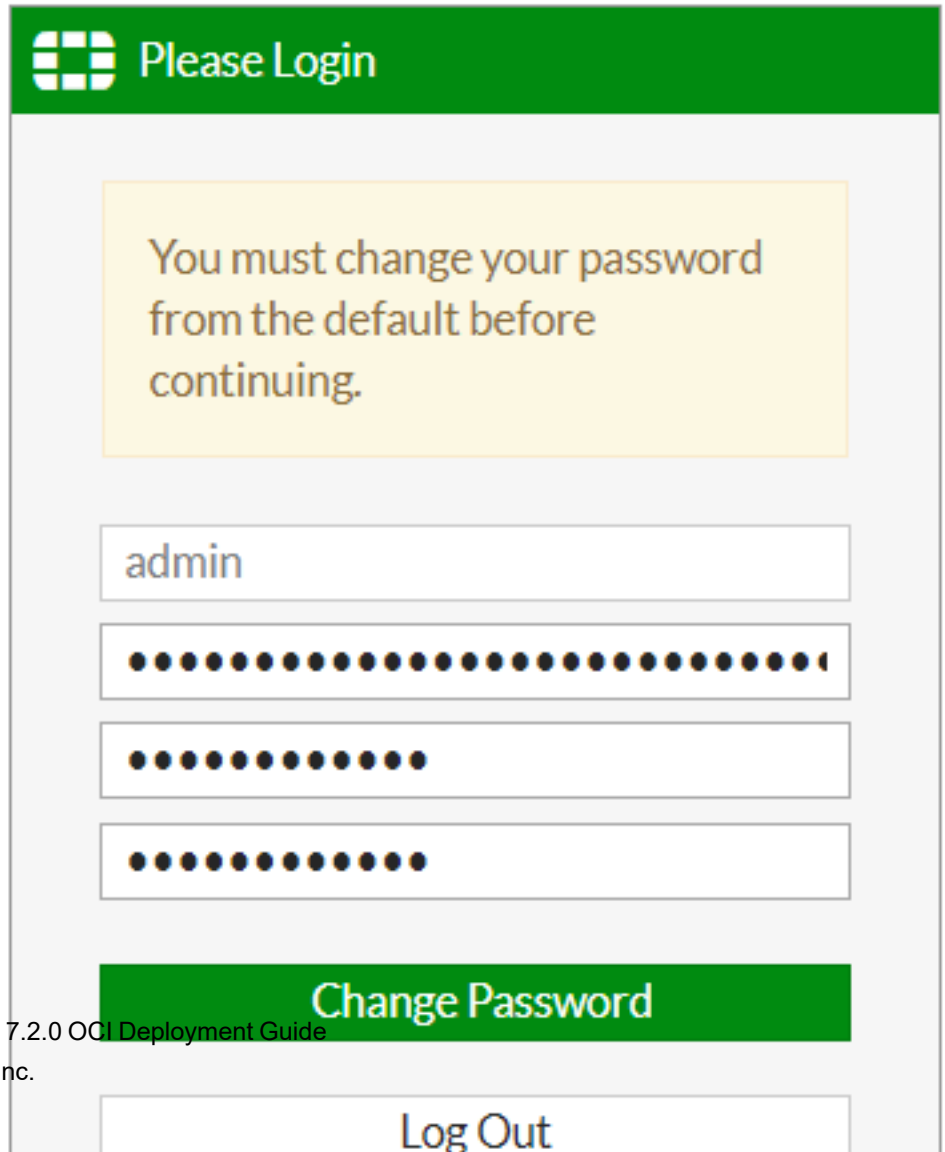
Accessing FortiMail

1. In the FortiMail instance detail page, you will find the public IP address and the OCID. In a web browser, you can access FortiMail with https://<public_IP_address>/admin, and the initial username/password is ‘admin/OCID’.

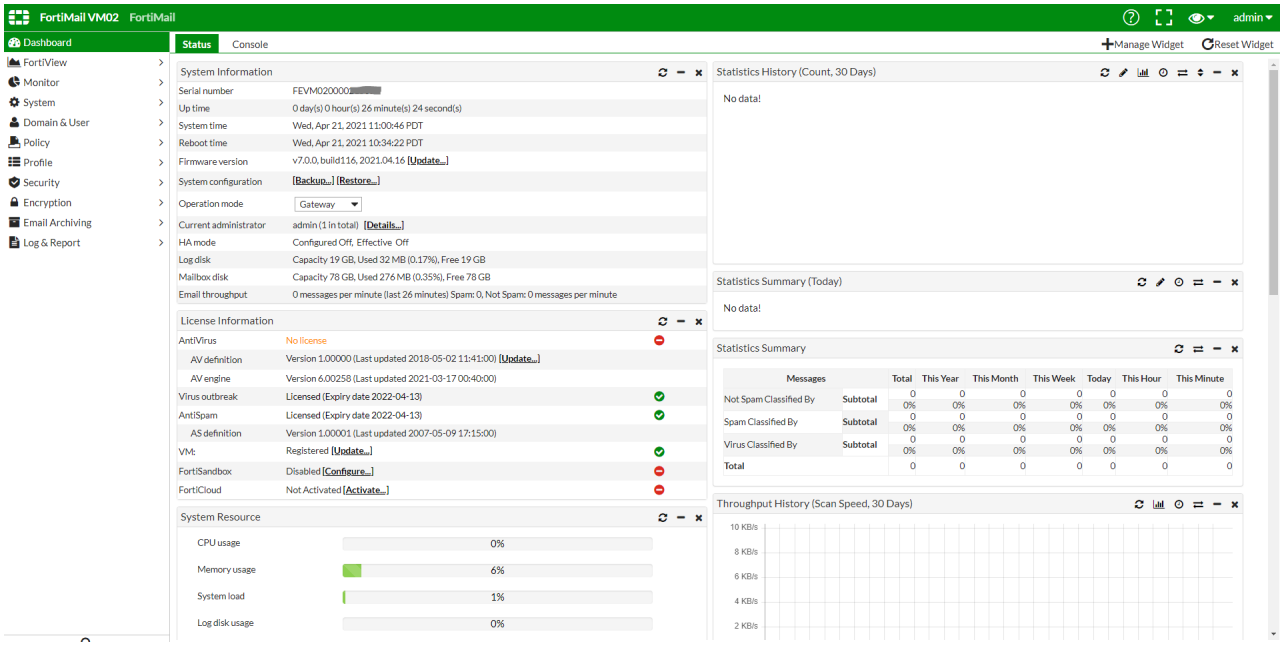


2. At the fist time login, you will be forced to change your password.

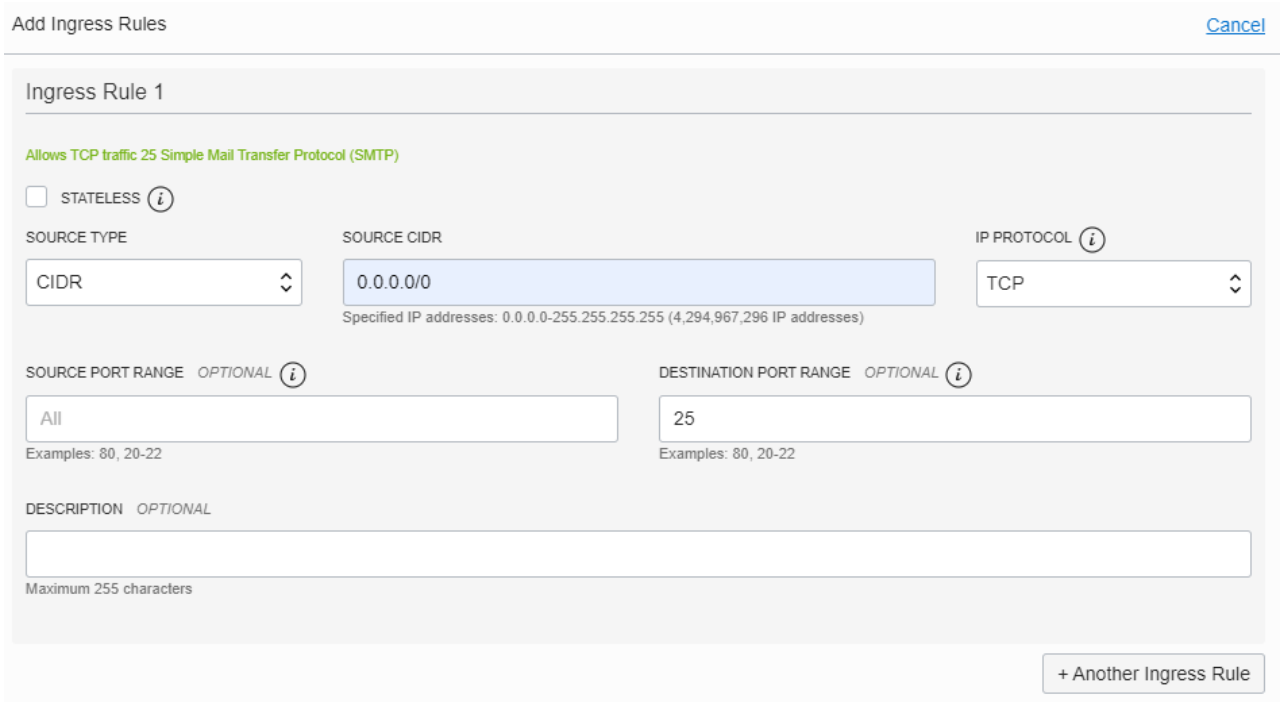

Please Login
admin
Remember me
Log In


Please Login
You must change your password from the default before continuing.
admin
Change Password
Log Out

3. The last step is to upload a valid FML VM license, and then you should be able to see the FortiMail Admin GUI.



4. For further testing on this FortiMail instance, you may need to add more rules in **Security List**. For example, a rule to open port 25 is necessary for SMTP testing.



www.fortinet.com