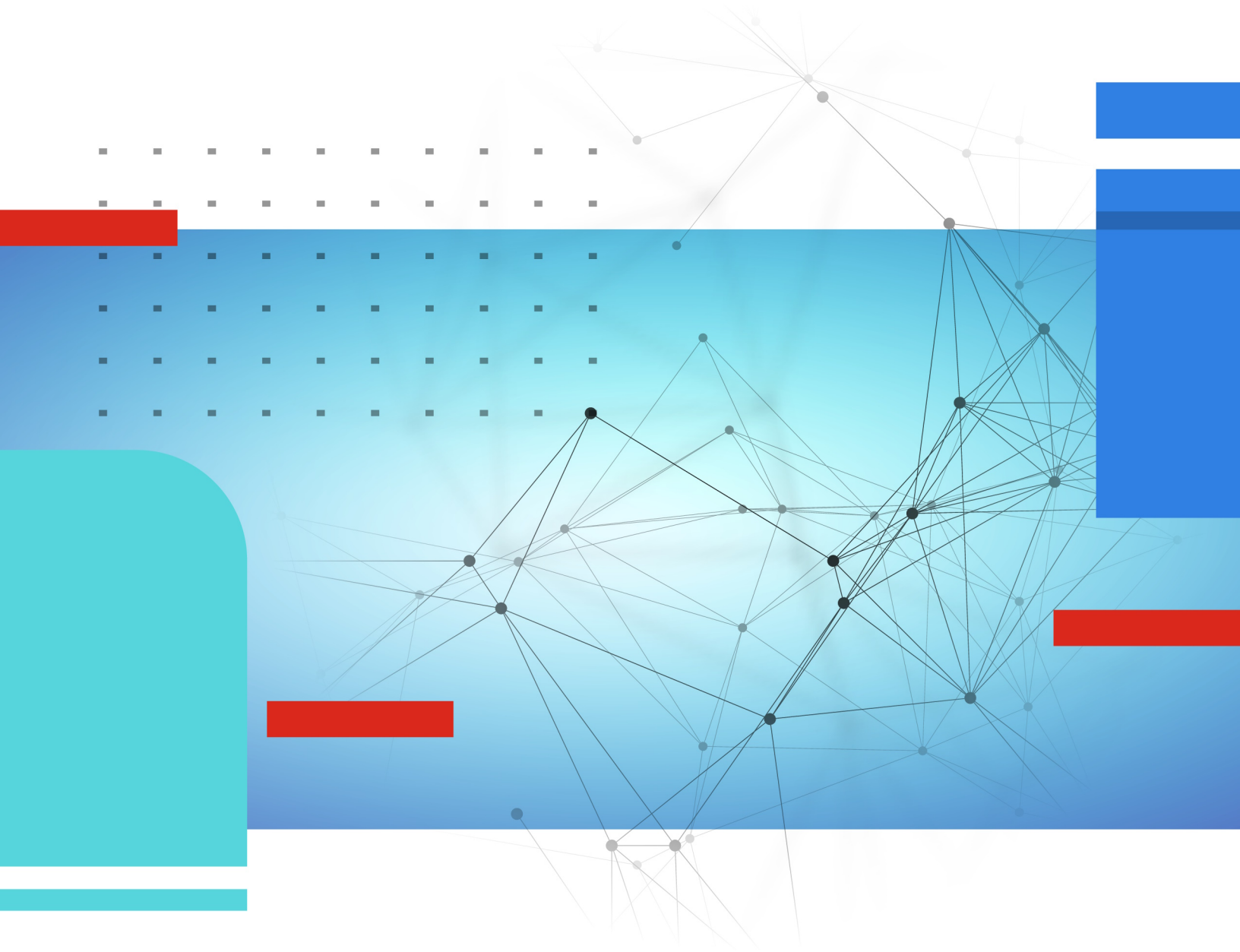
Alibaba Cloud Deployment Guide

FortiMail 7.6.0



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 18, 2024
FortiMail 7.6.0 Alibaba Cloud Deployment Guide
06-760-000000-20241018

TABLE OF CONTENTS

Change Log **4**
Introduction **5**
Region Support **6**
Creating a VPC **7**
Creating a Security Group **10**
Uploading the Image File to Object Storage Service **12**
Creating Custom Images **17**
Creating the FortiMail-VM instance **19**
Connect to FortiMail **22**

Change Log

Date	Change Description
2024-10-18	Initial release of FortiMail 7.6.0 Alibaba Cloud Deployment Guide.

Introduction

This document describes how to deploy FortiMail-VM on the Alibaba Cloud platform. For information about how to configure FortiMail, see the FortiMail Administration Guide.

Region Support

FortiMail-VM is available for purchase in all the regions/datacenters that the Alibaba Cloud global marketplace covers. Available regions are:

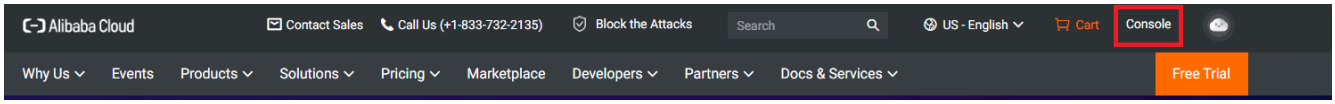
- Hong Kong
- Asia Pacific SE 1 (Singapore)
- US East 1 (Virginia)
- Asia Pacific NE 1 (Tokyo)
- US West 1 (Silicon Valley)
- EU Central 1 (Frankfurt)
- Middle East 1 (Dubai)
- Asia Pacific SE 2 (Sydney)
- Asia Pacific SE 3 (Kuala Lumpur)
- Asia Pacific SOU 1 (Mumbai)
- Asia Pacific SE 5 (Jakarta)
- North China 1
- North China 2
- China North 3 (Zhangjiakou)
- China North 5 (Huhehaote)
- East China 1
- East China 2
- South China 1

Other

- Saudi Arabia via the Saudi Cloud Computing Company. See Alibaba Cloud SCCC Operating Saudi Region.

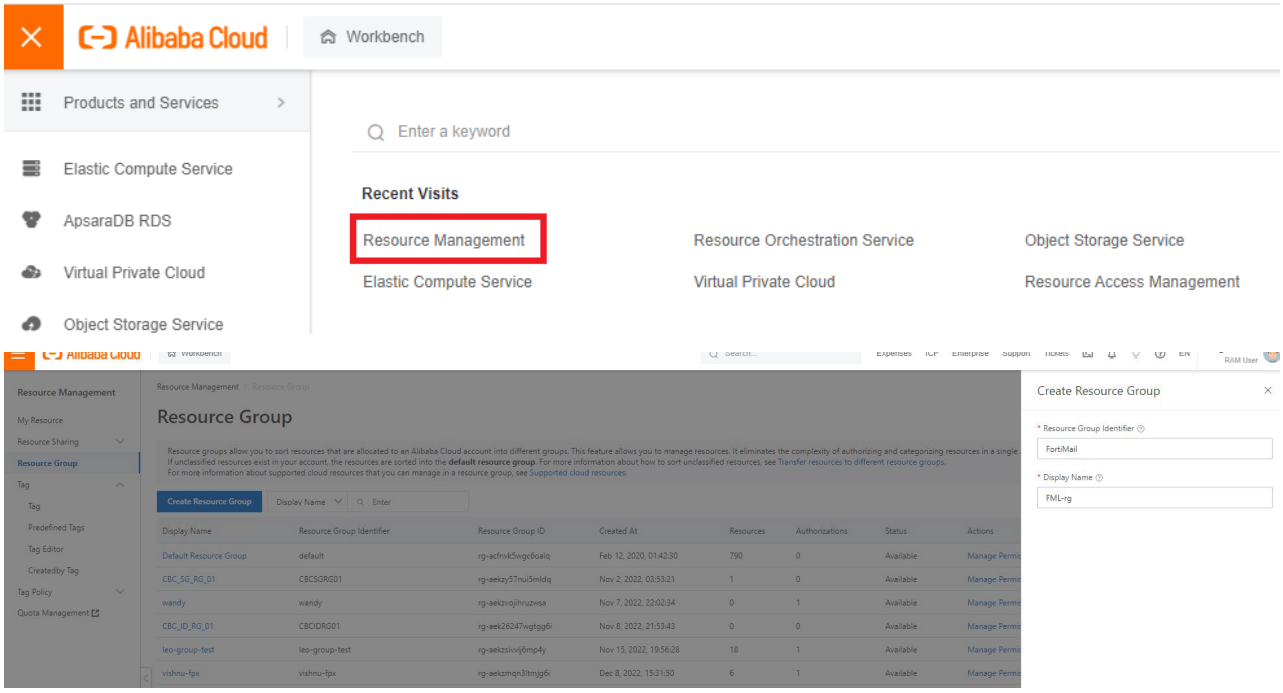
Creating a VPC

To deploy FortiMail, you first need to create a resource group and a virtual private cloud (VPC) on Alibaba Cloud.



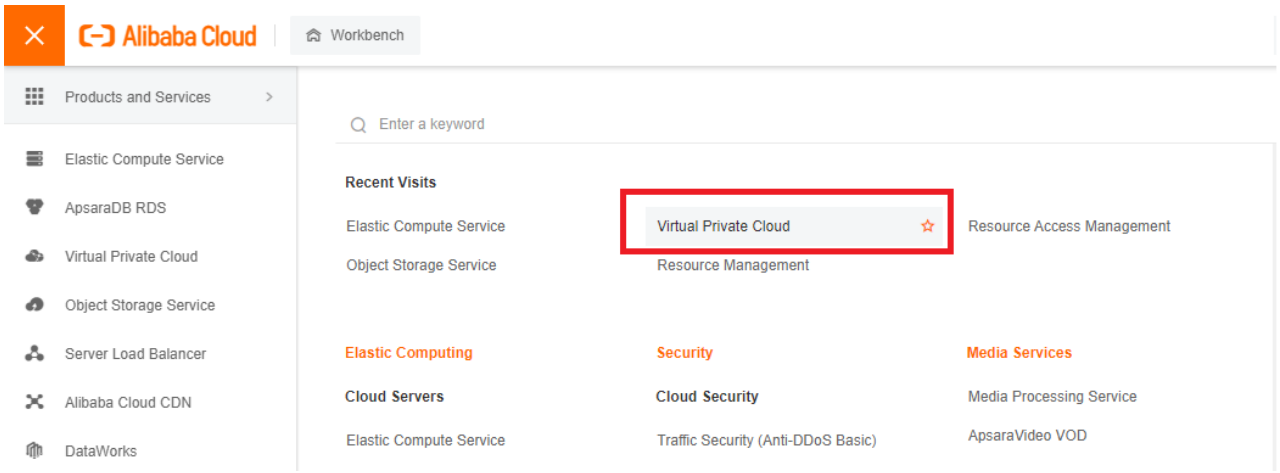
To create a resource group:

1. Log on to Alibaba Cloud.
2. Go to *Products and Services* > *Resource Management* > *Resource Group*.
3. Click *Create Resource Group*.
4. Enter the *Resource Group Identifier* and *Display Name*.

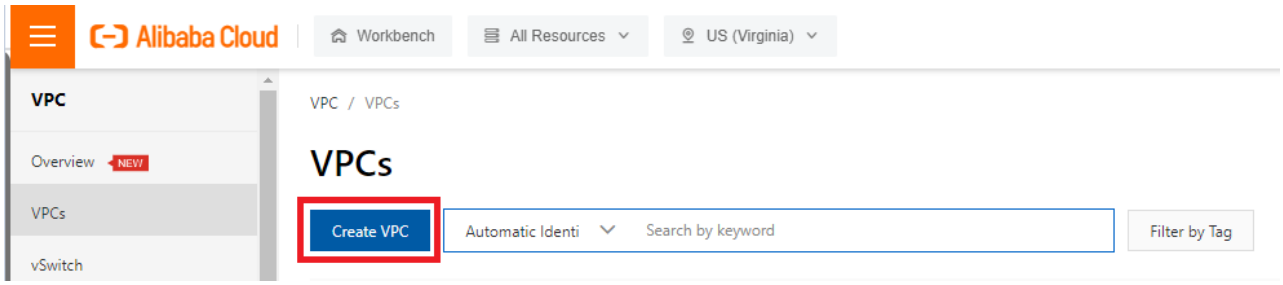


To create a VPC:

1. Log on to Alibaba Cloud web portal and go to *Products and Services* > *Virtual Private Cloud*.

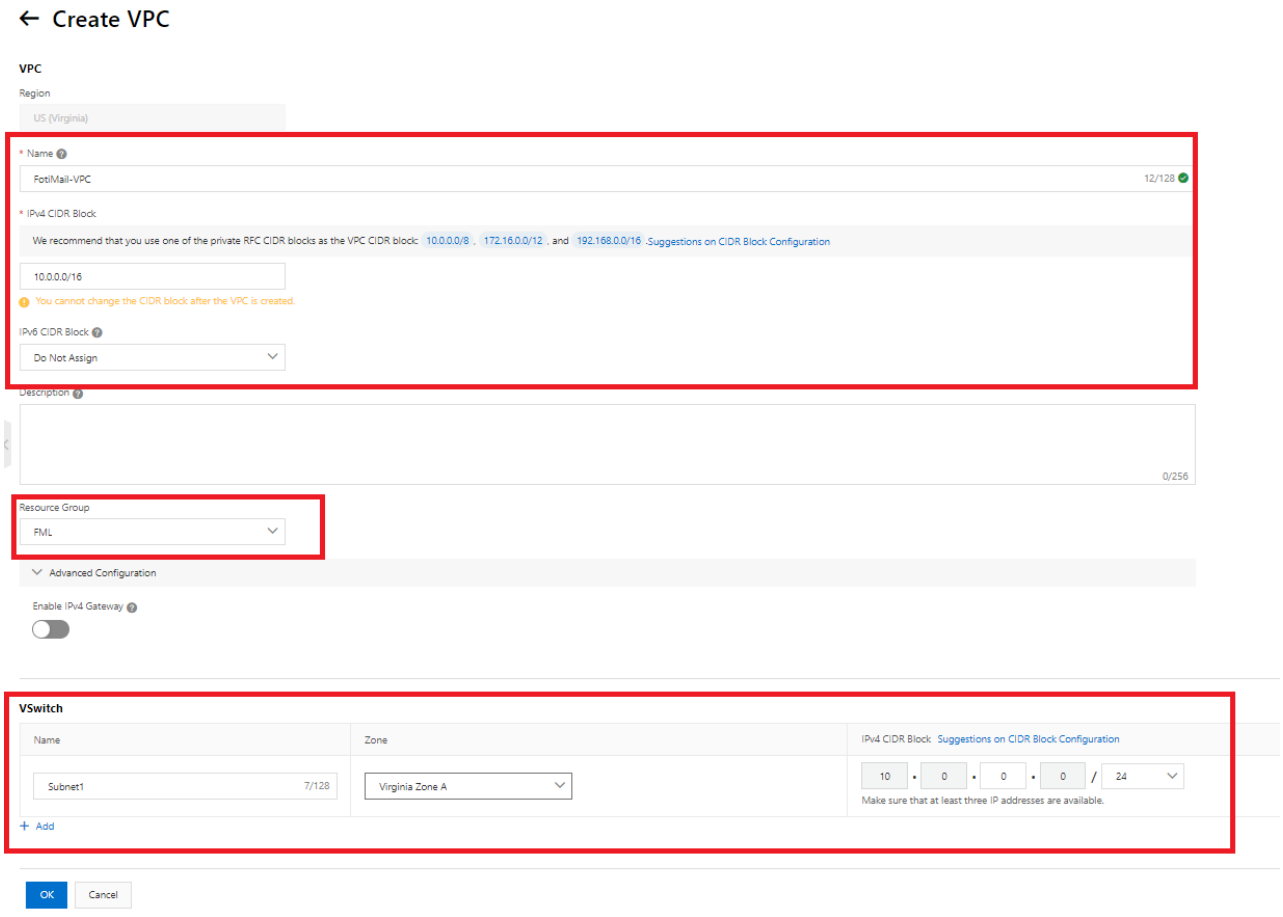


2. Click Create VPC.



3. Configure the following settings:

VPC	
Name	Enter a name for the VPC.
IPv4 CIDR Block	Specify the IPv4 CIDR Block for this VPC.
Resource Group	Select the resource group for the VPC.
VSwitch	
Name	Enter a name for the VSwitch.
Zone	Select the zone of the VSwitch. Later, it is recommended to deploy FortiWeb-VM in the same zone.
IPv4 CIDR Block	Specify the IPv4 CIDR Block for this VSwitch. It should be a subnet of the VPC.



Creating a Security Group

A security group is a set of firewall rules that control the traffic for your VM instances. When you create a VPC, a default security group protects instances within it. It's recommended to add inbound rules so that the traffic will be allowed to flow on the specified ports.

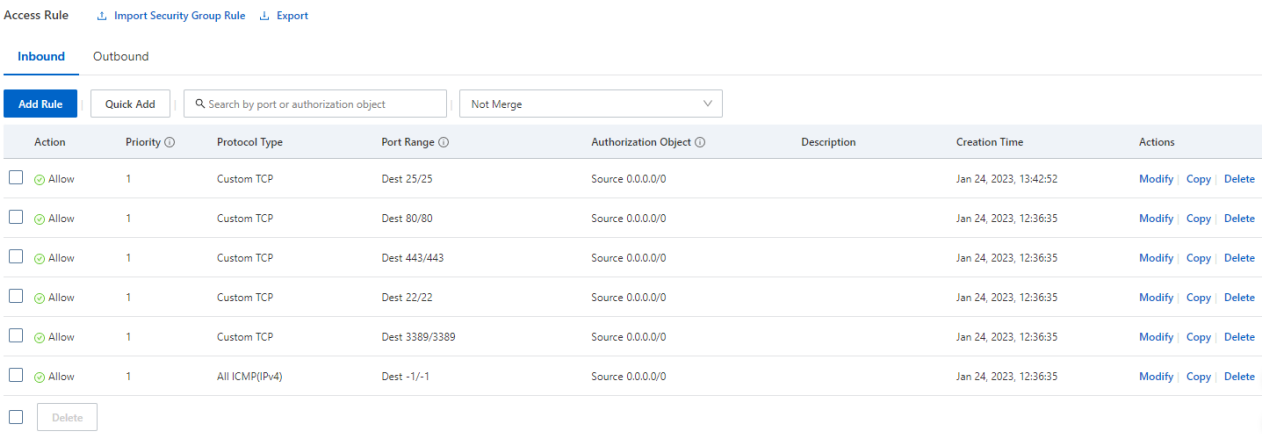
To create a security group:

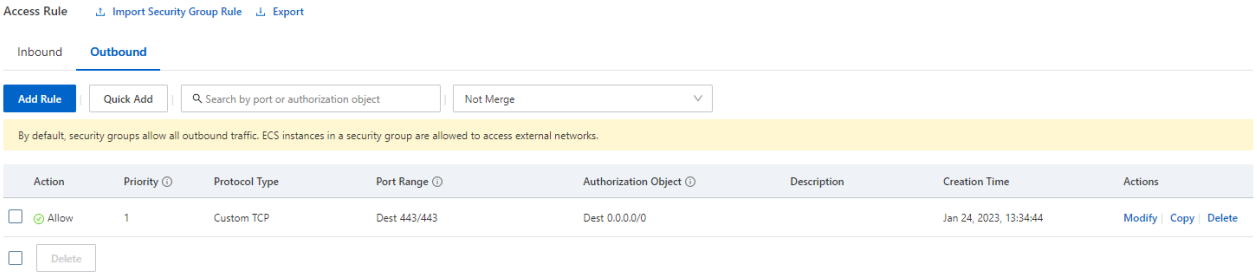
1. In the Alibaba Cloud web portal, select *Elastic Compute Service*.
2. Select *Network & Security* > *Security Groups*, then click *Create Security Group*.
3. Configure the *Basic Information*:

Security Group Name	Enter a name for the Security Group.
Network	Select the VPC you have created.
Security Group Type	Select **Basic Security Group** or **Advanced Security Group** as desired.
Resource Group	Select the resource group for the security group.

4. Configure Access Rule. Manually add rules to allow ports according to your own needs, in addition to the default ports 80, 443, and 22.

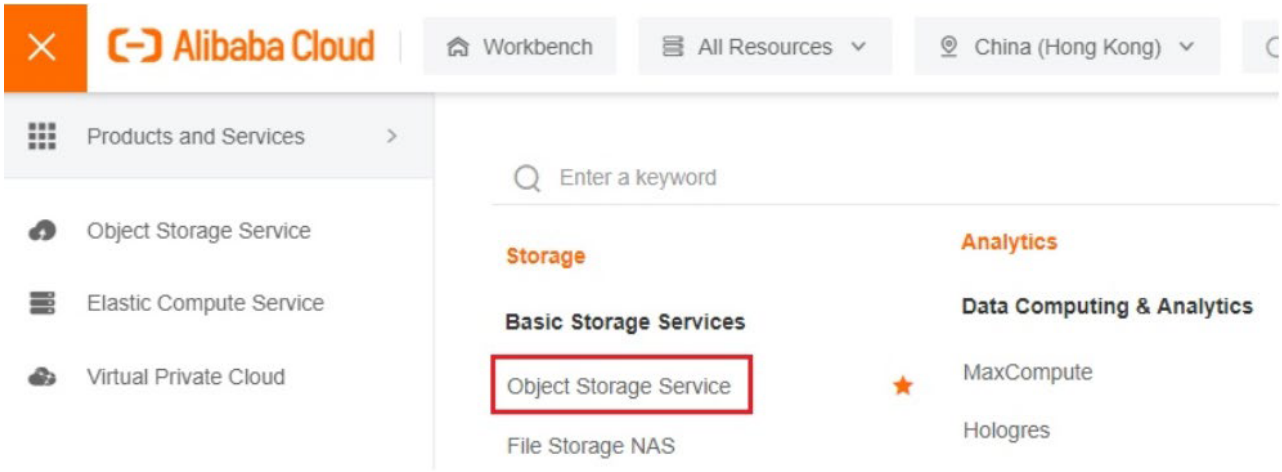
   It is recommended to add the following inbound and outbound rules as shown below in order for FortiMail-VM to connect and run properly.
5. Set the protocol type and port range as shown in the table, and set the source as 0.0.0.0/0 or ::/0 to allow access to the specified ports from all IPv4 or IPv6 addresses.


Access Rule
Import Security Group Rule
Export
Inbound
Outbound
Add Rule
Quick Add
Search by port or authorization object
Not Merge
Action
Priority
Protocol Type
Port Range
Authorization Object
Description
Creation Time
Actions
Allow 1 Custom TCP Dest 25/25 Source 0.0.0.0/0 Jan 24, 2023, 13:42:52 Modify | Copy | Delete
Allow 1 Custom TCP Dest 80/80 Source 0.0.0.0/0 Jan 24, 2023, 12:36:35 Modify | Copy | Delete
Allow 1 Custom TCP Dest 443/443 Source 0.0.0.0/0 Jan 24, 2023, 12:36:35 Modify | Copy | Delete
Allow 1 Custom TCP Dest 22/22 Source 0.0.0.0/0 Jan 24, 2023, 12:36:35 Modify | Copy | Delete
Allow 1 Custom TCP Dest 3389/3389 Source 0.0.0.0/0 Jan 24, 2023, 12:36:35 Modify | Copy | Delete
Allow 1 All ICMP(IPv4) Dest -1/-1 Source 0.0.0.0/0 Jan 24, 2023, 12:36:35 Modify | Copy | Delete
Delete


Access Rule
Import Security Group Rule
Export
Inbound
Outbound
Add Rule
Quick Add
Search by port or authorization object
Not Merge
By default, security groups allow all outbound traffic. ECS instances in a security group are allowed to access external networks.
Action
Priority
Protocol Type
Port Range
Authorization Object
Description
Creation Time
Actions
Allow 1 Custom TCP Dest 443/443 Dest 0.0.0.0/0 Jan 24, 2023, 13:34:44 Modify | Copy | Delete
Delete

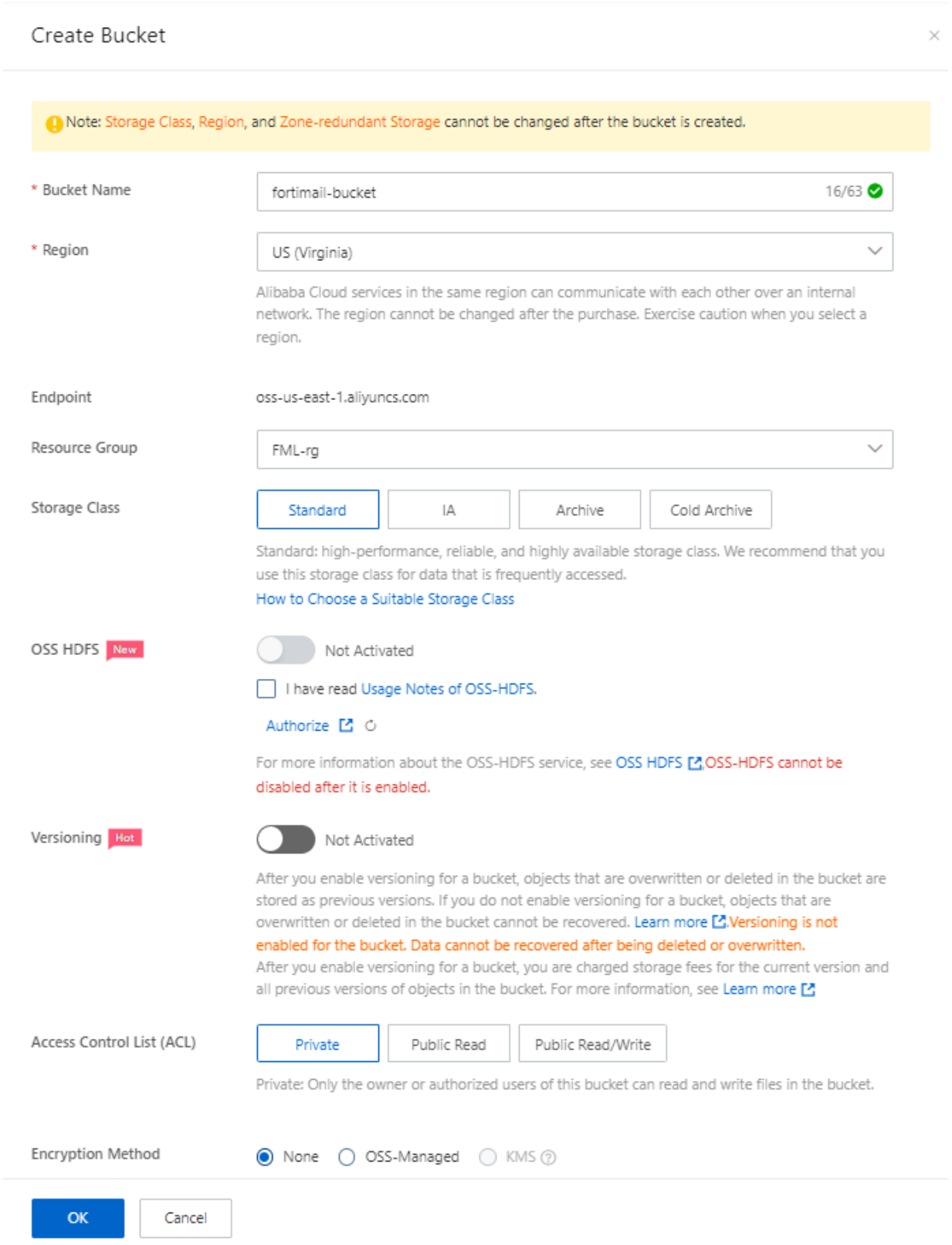
Uploading the Image File to Object Storage Service

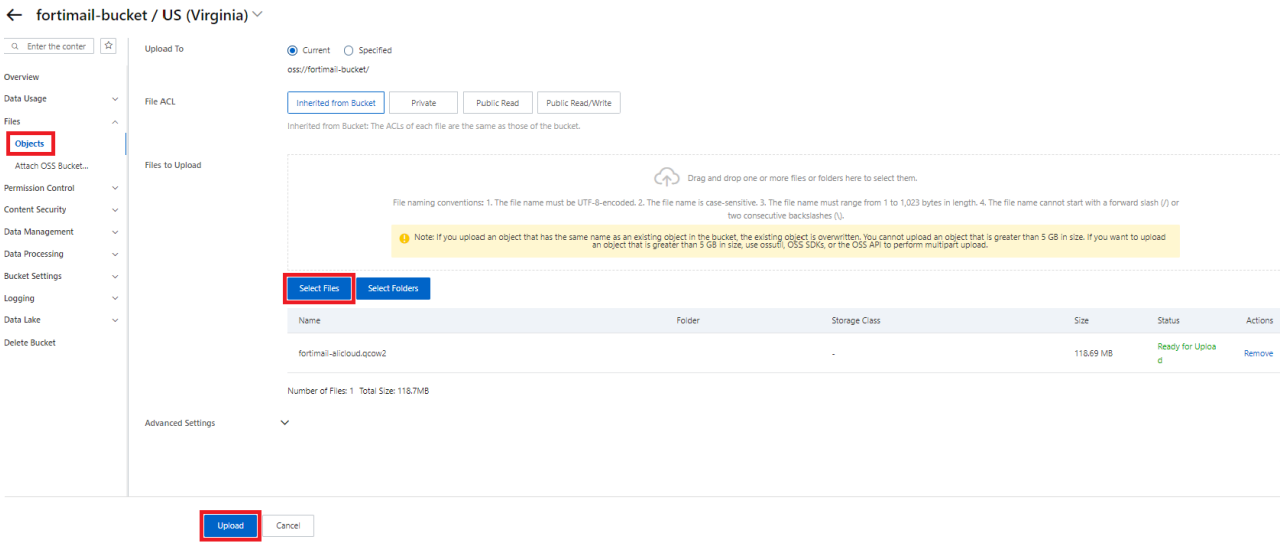
1. Select *Object Storage Service*.



2. Select *Buckets* and click *Create Bucket*.
   - Enter a name for the bucket.
   - Select the region where this bucket will be located.

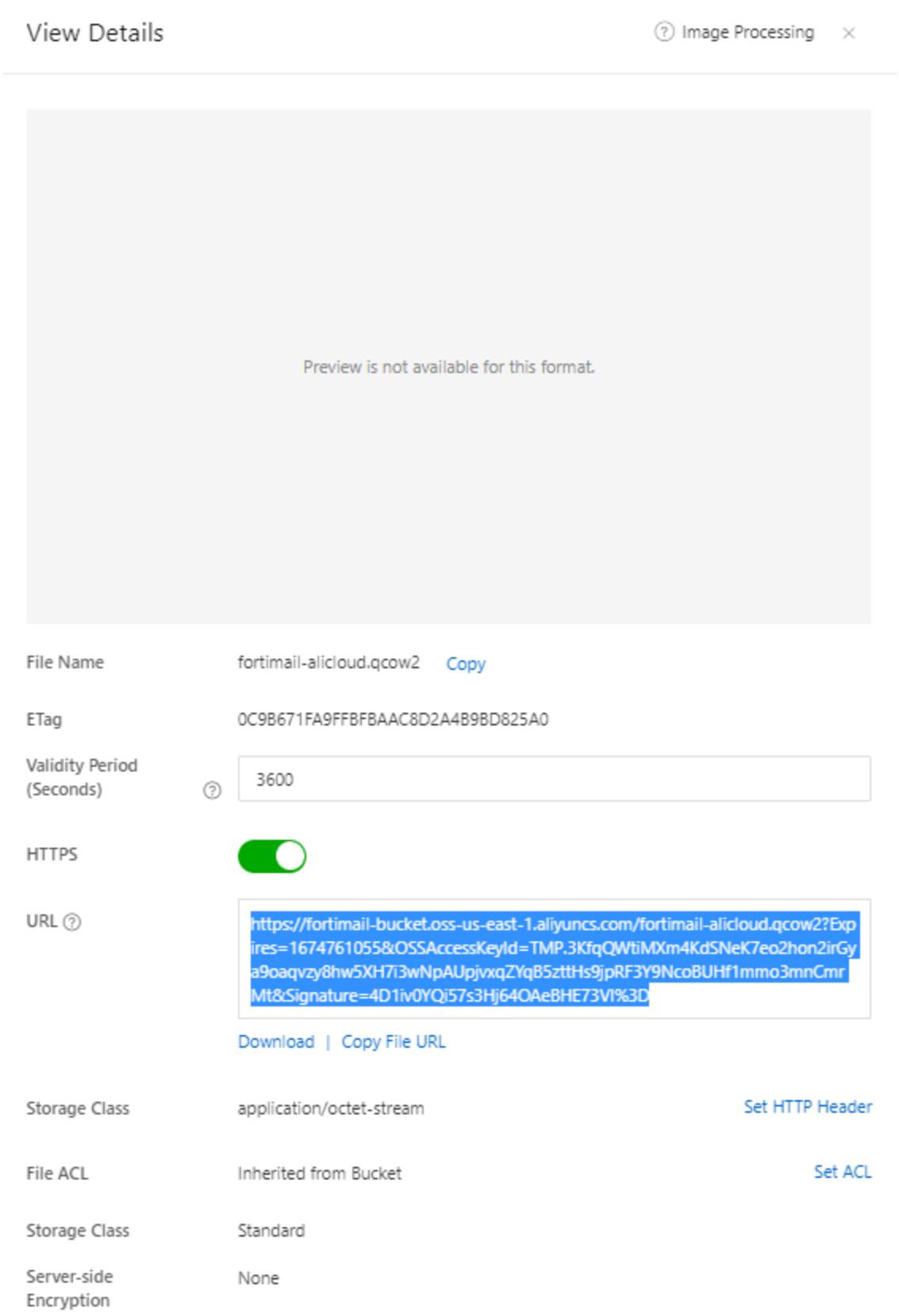
- Configure the *Storage Class*, *Access Control List*, and *Encryption Method* as shown below.



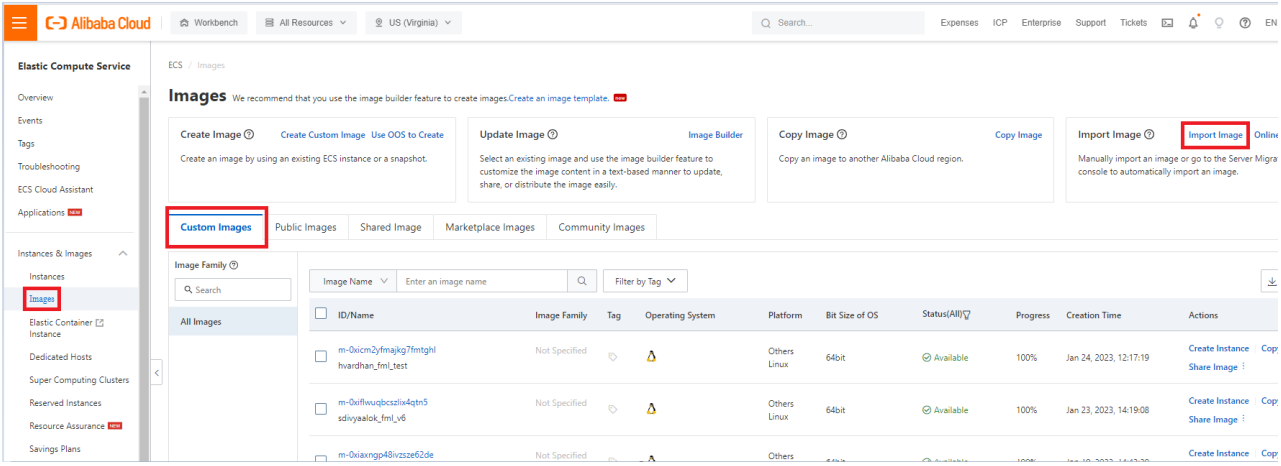


3. Click *OK*. The bucket will appear in the bucket list in the navigation menu.
4. Select the bucket you just created, then click the *Files Tab*. Click the *Upload* button to upload the image file.
5. Select *Current* for the Upload to directory, inherited from Bucket as the File ACL, then *Select Files* to upload the (qcow2) image file.

6. The file will be displayed in the table on the *Upload* page if it is uploaded successfully. Click *View Details*.

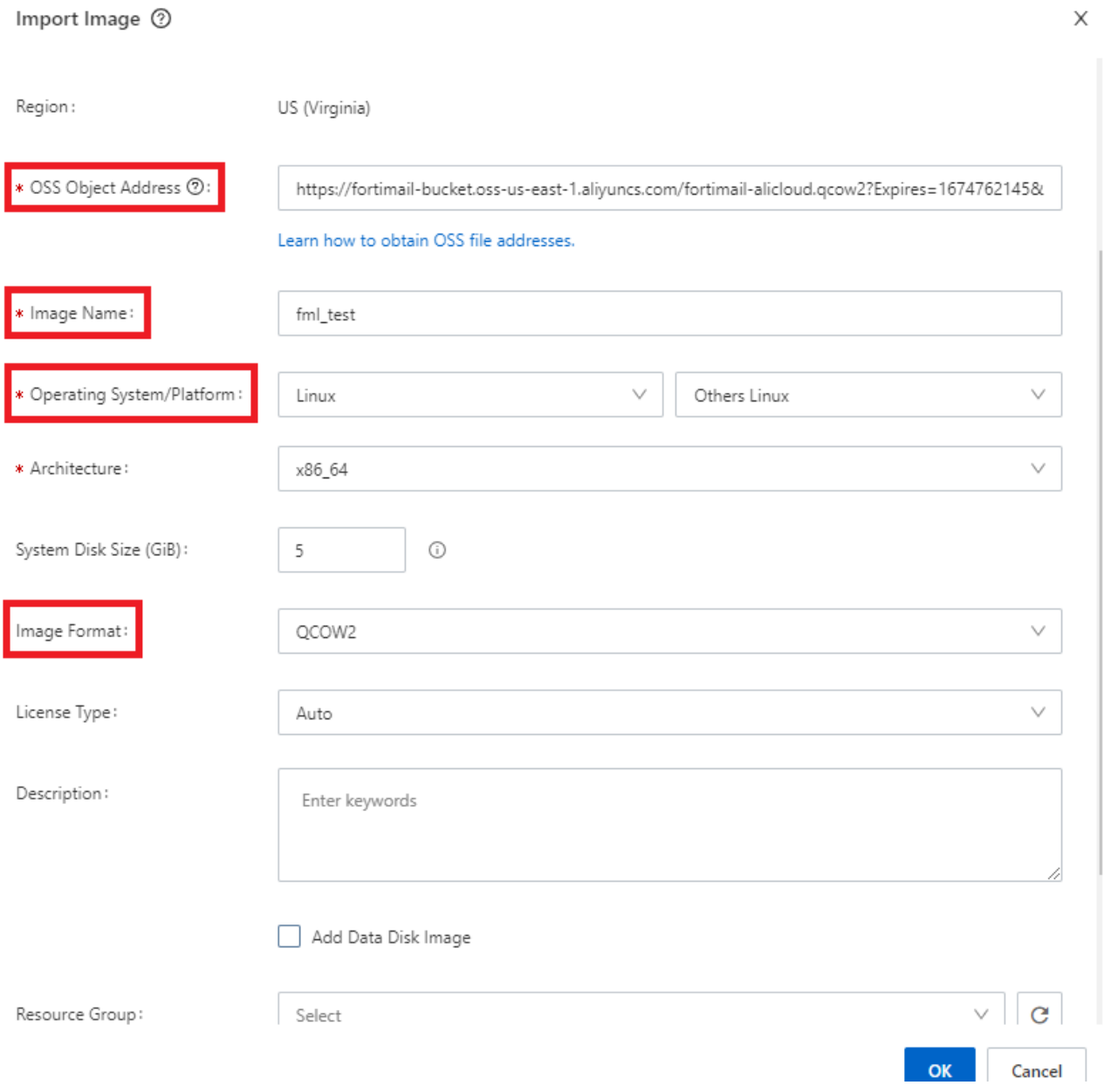

View Details
Image Processing
Preview is not available for this format.
File Name
fortimail-alicloud.qcow2
Copy
ETag
0C9B671FA9FFBFBAAC8D2A4B9BD825A0
Validity Period (Seconds)
3600
HTTPS
URL
https://fortimail-bucket.oss-us-east-1.aliyuncs.com/fortimail-alicloud.qcow2?Expires=1674761055&OSSAccessKeyId=TMP.3KfqQWtiMXm4KdSNeK7eo2hon2irGya9oaqvzy8hw5XH7i3wNpAUpjvxqZYqB5zttHs9jpRF3Y9NcoBUHf1mmo3mnCmrMt&Signature=4D1iv0YQi57s3Hj64OAeBHE73Vl%3D
Download | Copy File URL
Storage Class
application/octet-stream
Set HTTP Header
File ACL
Inherited from Bucket
Set ACL
Storage Class
Standard
Server-side Encryption
None

7. Click *Copy File URL*. You will use this URL later when creating a custom image.



Creating Custom Images

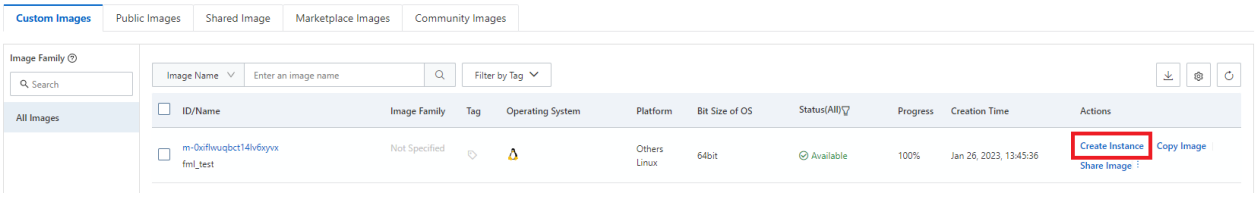
1. Select *Elastic Compute Service*.
2. Select *Instances & Images* > *Images* > *Custom Images*, then click the *Import Image* button.



3. Configure the image settings.
   - *OSS Object Address*: Enter the File URL you have copied in the last step when uploading image file to Object Storage Service.
   - *Image Name*: Enter a name for the image.

For other settings, please configure them as shown below.

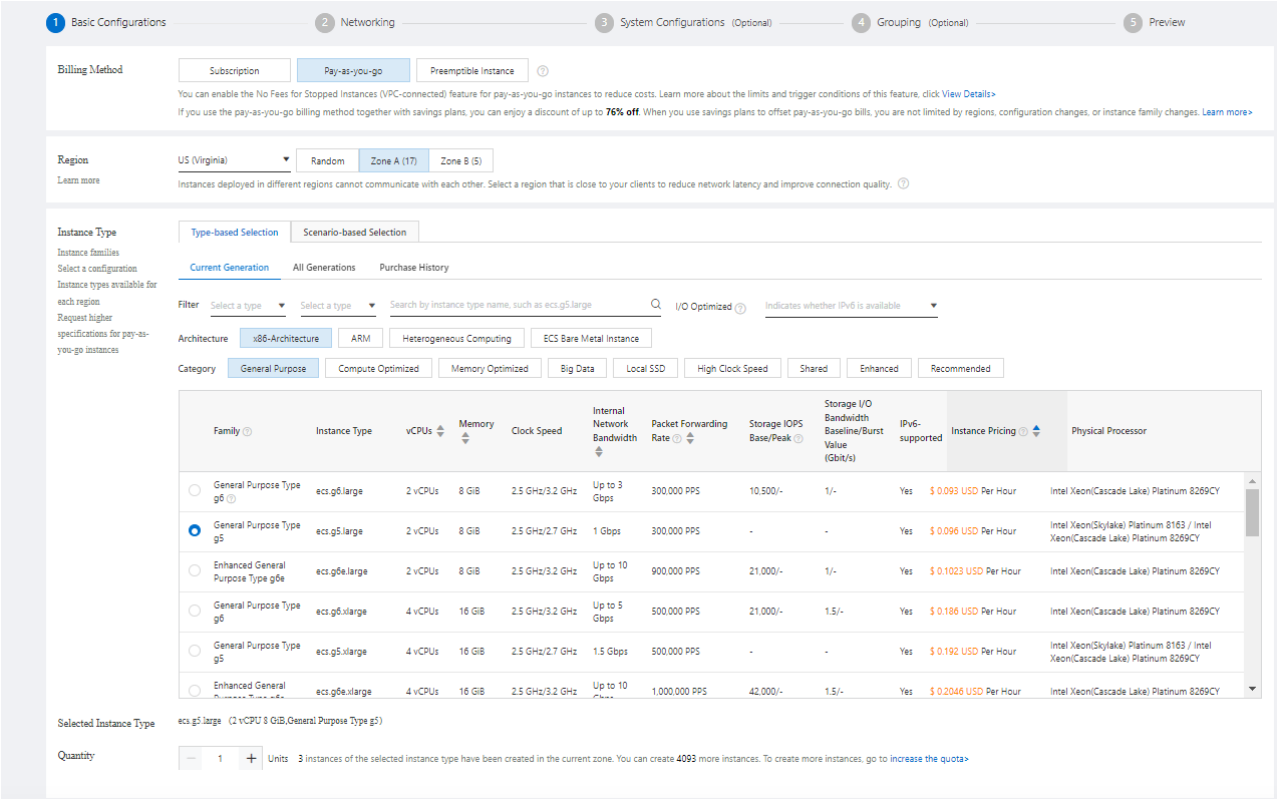
4. Click *OK*.
5. You will see the image listed on the *Custom Images* tab if it is created successfully.
6. Click *Create Instance* to create a FortiMail instance.

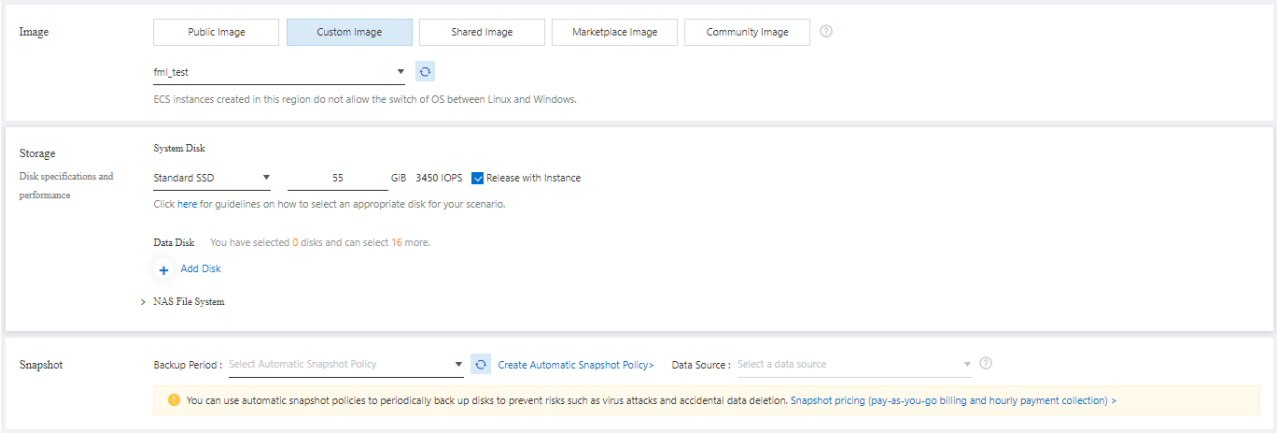


Creating the FortiMail-VM instance

1. Select the *Custom Launch* tab.
2. Set *Basic Configurations*.

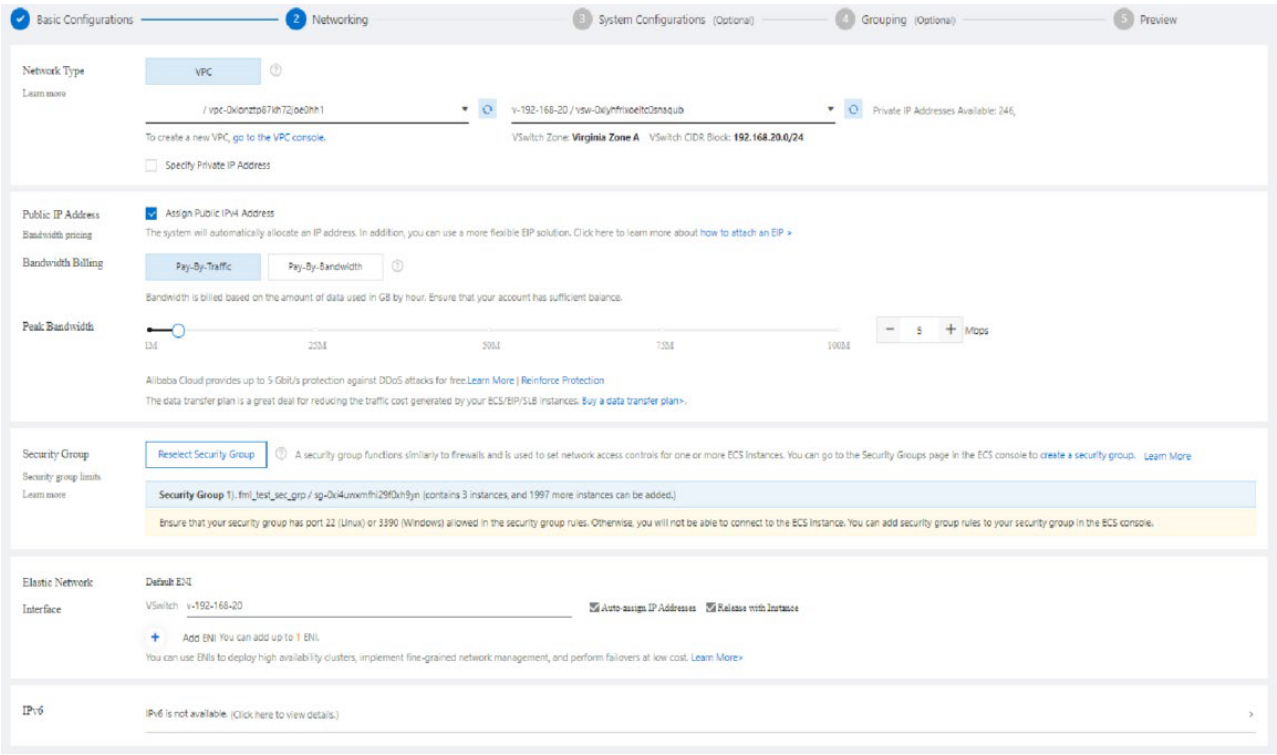
Billing Method	Choose the desired billing method. If you plan to use FortiWeb for a long time, **Subscription** is the most economical choice.
Region	Select the region and zone where the VSwitch is located.
Instance Type	Select the instance type with at least 2 vCPU and 8 GB memory.





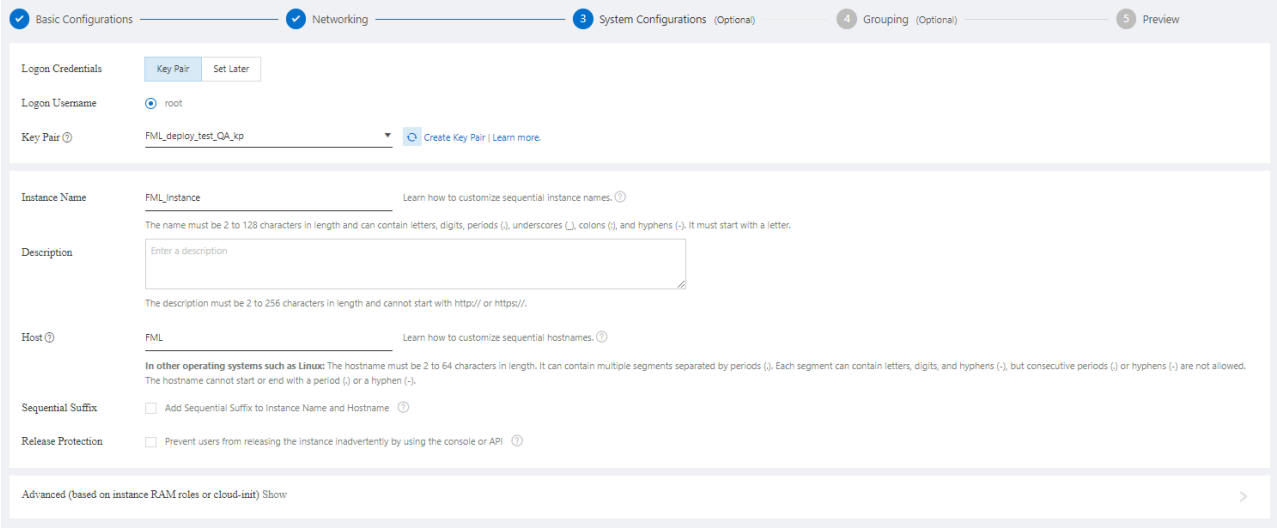
3. Configure *Networking*.

Network Type	Select the VPC and the VSwitch you want to connect to the public IP address.
Public IP Address	Enable *Assign Public IP Address*. You will access FortiWeb's GUI and CLI through this IP address.
Bandwidth Billing	Select *Pay-By-Traffic* or *Pay-By-Bandwidth* as desired.
Security Group	Select the Security Group you have created.
Elastic Network Interface	Select the VSwitch for FortiWeb interfaces to connect to. Click *Add ENI* to add more interfaces on FortiWeb.



4. Configure *System Configurations*.

Select either Key Pair or Set Later for Logon Credentials, and enter an Instance Name. The default username is admin and the password is Instance ID.

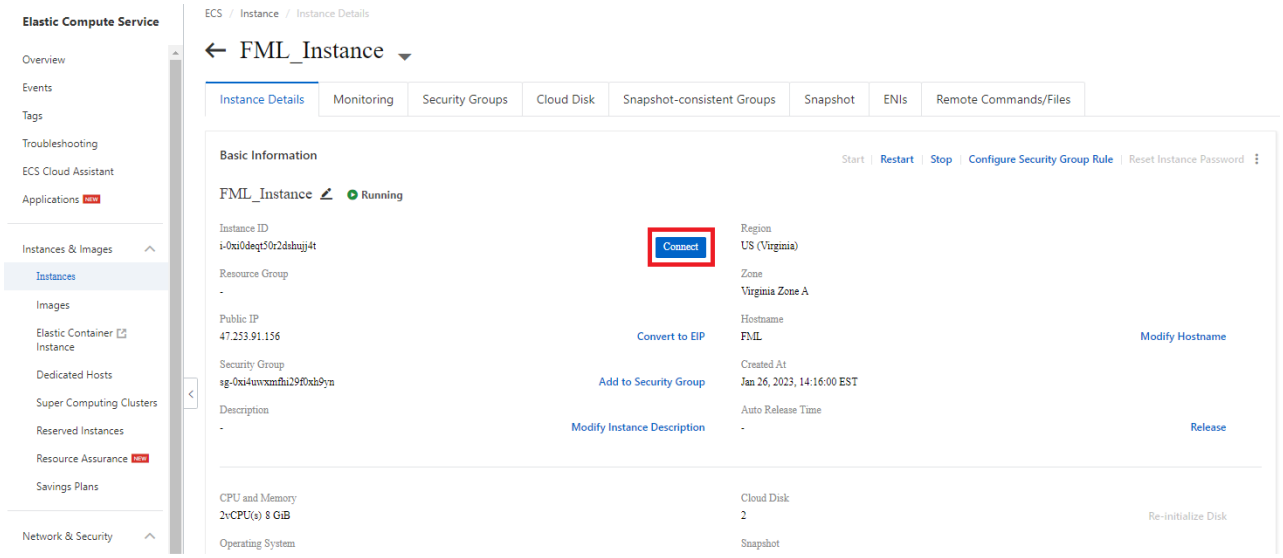


5. Configure *Grouping*. Select Default Resource Group or create a new resource group.
6. Review the instance information. Check ECS Terms of Service and Product Terms of Service Agreement. Click Create Instance.

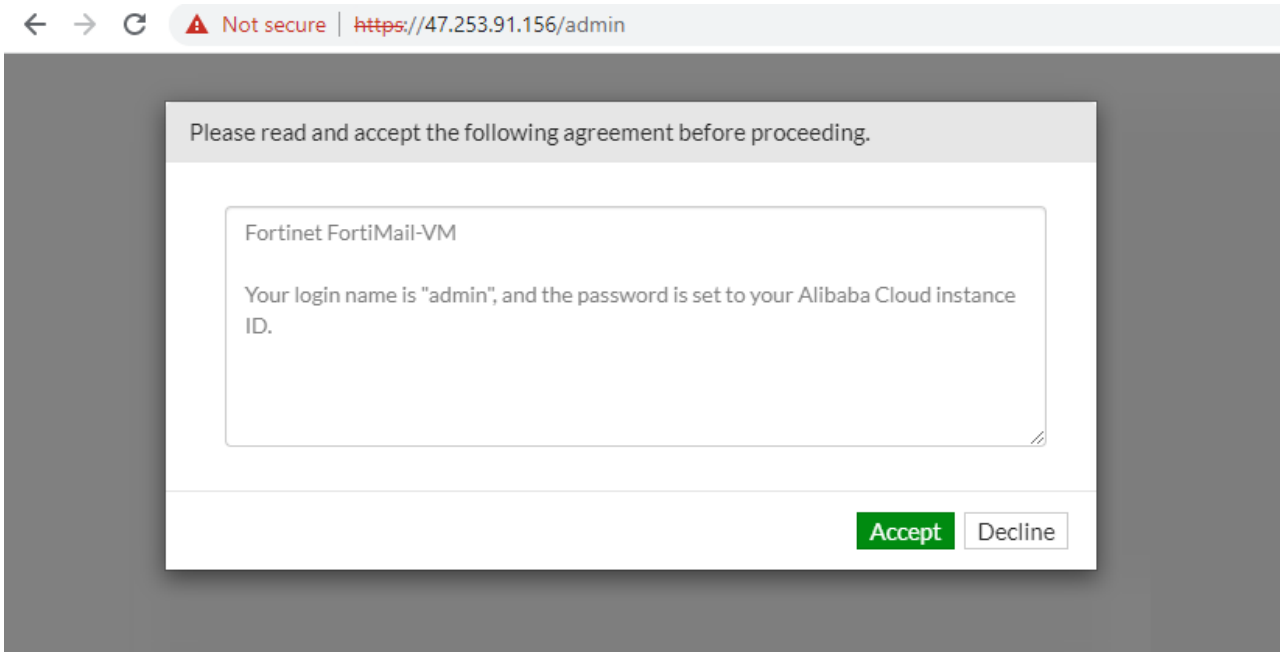
   It may take 1-5 minutes to create the instance.
7. Check the status of the instance. If it's running, you can go ahead to the next step.

Connect to FortiMail

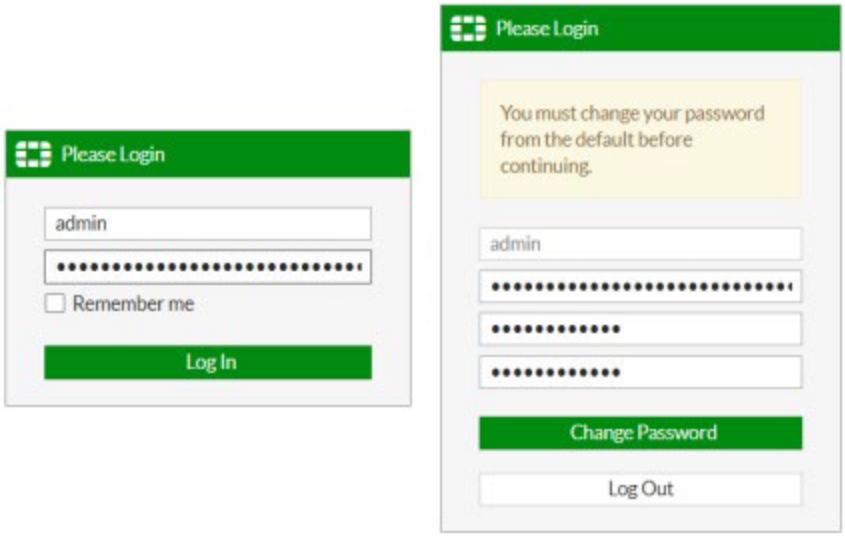
1. Click on Connect. A VNC console will display.



2. Get the public IP address of the instance as shown below. Use this address to access the FortiMail unit's web UI in a web browser or the CLI using an SSH connection.



3. At the first time login, you will be forced to change your password.



4. The last step is to upload a valid FML VM license, and then you should be able to see the FortiMail GUI console. For details about how to configure FortiMail, see the FortiMail Administration Guide.

www.fortinet.com

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.