



Google 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

February 25, 2025

FortiMail 7.6.0 Google Cloud Deployment Guide

06-760-000000-20250225

TABLE OF CONTENTS

Change Log	4
Introduction	5
Creating the FortiMail instance	6
Accessing the FortiMail instance	10

Change Log

Date	Change Description
2025-02-07	Initial release of FortiMail 7.6.0 Google Cloud Deployment Guide.

Introduction

This document describes how to deploy FortiMail VM on Google Cloud, also known as Google Cloud Platform (GCP).
For details about how to use FortiMail, see the FortiMail Administration Guide on <https://docs.fortinet.com>.

Creating the FortiMail instance

FortiMail is available in the Google Cloud Marketplace.

1. Log on to Google Cloud.
2. Go to *Marketplace*, and search for "fortimail".

The screenshot shows the Google Cloud Marketplace interface. At the top left, there is a 'Marketplace' header with a shopping cart icon. To the right is a search bar containing the text 'fortimail' with a magnifying glass icon on the left and a close 'X' icon on the right. Below the search bar, the breadcrumb 'Marketplace > "fortimail"' is visible. On the left side, there is a navigation menu with 'Marketplace home', 'Your products', and 'Your orders'. Below this is a 'Filter' section with a 'Type to filter' input field. The main content area shows '2 results'. The first result is 'Fortinet FortiMail (BYOL) Secure Email Gateway' by Fortinet Inc. It includes the Fortinet logo and a description: 'Fortinet FortiMail-VM is a complete Secure Email solution providing a single solution to protect against malware, as well as outbound threats and data loss with a wide range of top-rated security capabilities including phishing, malware and ransomware protection. Machine learning and outbreak detection techniques are used to detect and block threats.' The second result is 'Fortinet FortiSandbox Zero-Day Threat Protection (BYOL)' by Fortinet Inc. It includes the Fortinet logo and an overview: 'FortiSandbox for GCP enables organizations to defend against Zero-day threats natively in their application, email, endpoint security, and other 3rd party security solutions, or as an extension to their existing security stack. Highlights: AI-powered sandbox malware analysis - Two-stage APT detection - Cloud-native architecture - Scalable and elastic - Leverage cloud elasticity and scale.'

3. Launch the FortiMail instance and configure the boot disk and other parameters as desired.

New Fortinet FortiMail (BYOL) Secure Email Gateway deployment

i Prices don't include private offer discounts

TERRAFORM

COMMAND-LINE DEPLOYMENT

Deployment name *

fortimail-instance1

Deployment Service Account **?**

Existing account

New account

List of available Service Accounts that have the following roles:

- roles/config.agent
- roles/compute.networkAdmin
- roles/compute.admin
- roles/iam.serviceAccountUser
- roles/storage.objectViewer

Select a Service Account

[Redacted]

FortiMail (BYOL)

Image Version

Image Version

7.6.1

Zone

us-central1-b

Machine type

General purpose Compute optimized Memory optimized

Machine types for common workloads, optimized for cost and flexibility

Series
N2

Powered by Intel Cascade Lake and Ice Lake CPU platforms

Machine type
n2-standard-4 (4 vCPU, 2 core, 16 GB memory)



vCPU

4

Memory

16 GB

Boot Disk

Boot disk size in GB
10

Boot disk type
SSD Persistent Disk

Log Disk

Enable Log Disk

Log disk size in GB
80

log disk type
SSD Persistent Disk

Networking

Network interfaces

▼ fml-network1 fml-network1 (10.128.0.0/20)

[ADD A NETWORK INTERFACE](#)

Firewall ?

Add tags and firewall rules to allow specific network traffic from the Internet



Creating certain firewall rules may expose your instance to the Internet. Please check if the rules you are creating are aligned with your security preferences. [Learn more](#)

Allow HTTPS traffic

Source IP ranges for HTTPS traffic

0.0.0.0/0 ?

Allow HTTP traffic

Source IP ranges for HTTP traffic

0.0.0.0/0 ?

Allow TCP port 465 traffic

Source IP ranges for TCP465 traffic

0.0.0.0/0 ?

Allow TCP port 25 traffic

Source IP ranges for TCP25 traffic

0.0.0.0/0 ?

Enable IP Forward ?

DEPLOY

Accessing the FortiMail instance

After booting up the FortiMail instance, you can access it via HTTPS.



The admin password is your FortiMail instance's custom metadata value, as shown below.

[to parent page](#)

DETAILS	OBSERVABILITY	OS INFO	SCREENSHOT
On host maintenance		Migrate VM instance (Recommended)	
Host error timeout		—	
Automatic restart		On (Recommended)	
Customer Managed Encryption Key (CMEK) revocation policy		Do nothing	

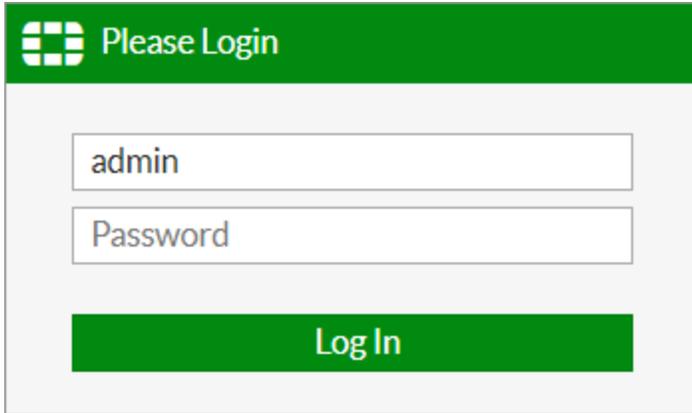
Sole-tenancy	
CPU Overcommit	Disabled

Custom metadata

Key	Value
fortimail_user_password	

To log on to the FortiMail instance, use the following information:

- `https://instance_IP/admin` (FortiMail Instance IP is the instance interface's public IP address. Remember to add /admin at the end.)
- Default user name: `admin`
- Password: (custom metadata value as shown above)



The image shows a login form for FortiMail. It features a green header bar with a white grid icon and the text "Please Login". Below the header, there are two input fields: the first contains the text "admin" and the second is labeled "Password". At the bottom of the form is a green button with the text "Log In".

