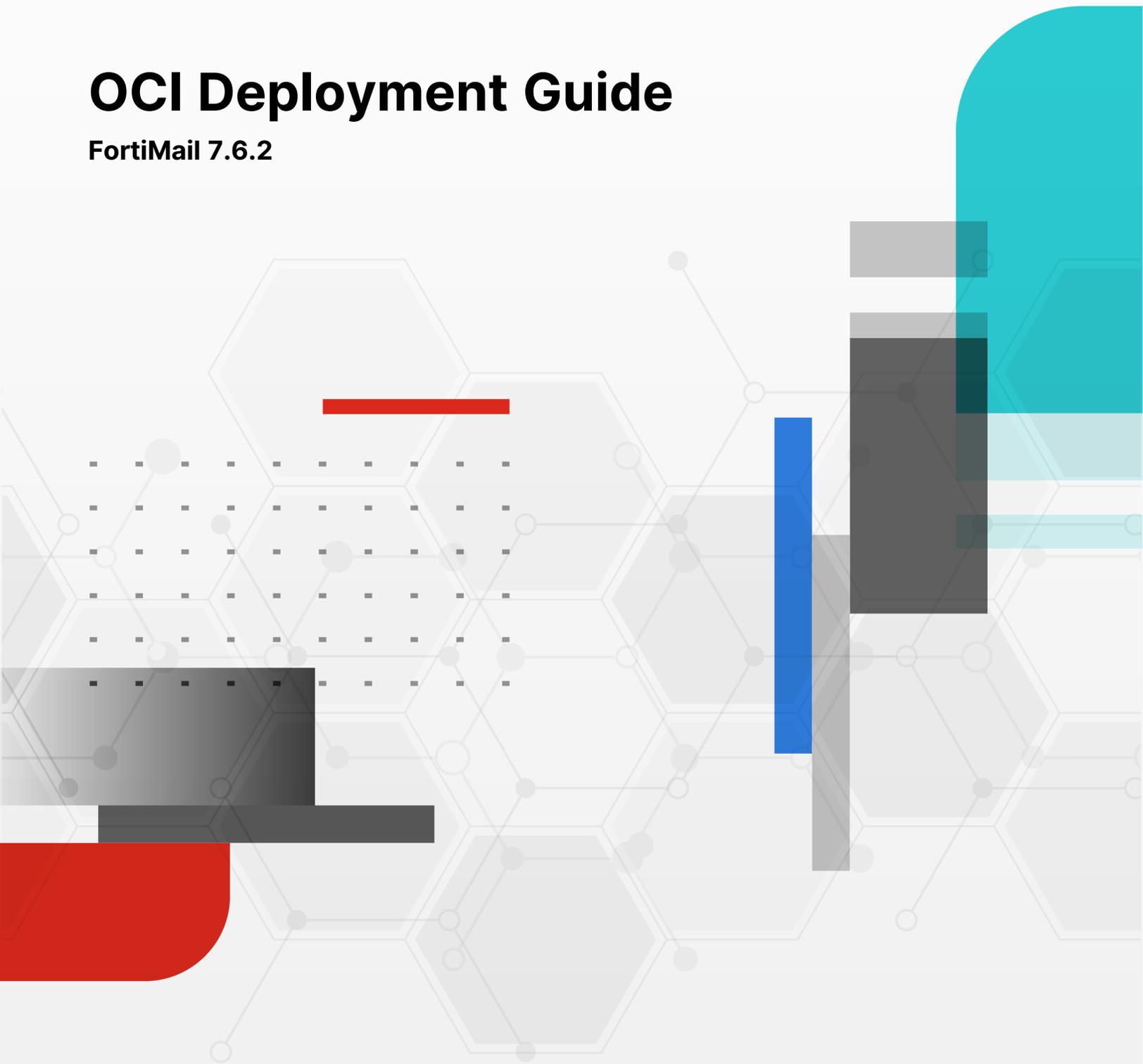


# OCI Deployment Guide

FortiMail 7.6.2



**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](mailto:techdoc@fortinet.com)



April 09, 2025

FortiMail 7.6.2 OCI Deployment Guide

06-762-000000-20250409

# TABLE OF CONTENTS

<b>Change Log</b> .....	<b>4</b>
<b>Introduction</b> .....	<b>5</b>
<b>Creating a Virtual Cloud Network and Public-facing Subnet</b> .....	<b>6</b>
<b>Creating a FortiMail-VM Instance</b> .....	<b>12</b>
<b>Attaching Storage to FortiMail-VM</b> .....	<b>18</b>
<b>Accessing FortiMail-VM</b> .....	<b>20</b>

# Change Log

Date	Change Description
2025-04-09	Initial release of the FortiMail 7.6.2 OCI Deployment Guide.

# Introduction

This document describes how to deploy FortiMail-VM on Oracle Cloud Infrastructure (OCI).

FortiMail-VM supports Oracle Dedicated Region Cloud.

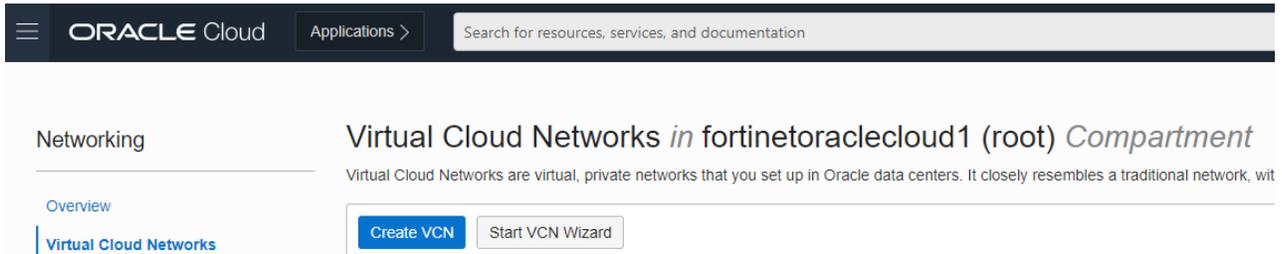
Oracle Dedicated Region Cloud (ODRC) provides all Oracle Cloud Infrastructure (OCI) public cloud services (IaaS/PaaS/SaaS) in a physical location of the customer's choosing. For more information, see the [OCI Dedicated Region website](#).

For details about how to use FortiMail, see the [FortiMail Administration Guide](#).

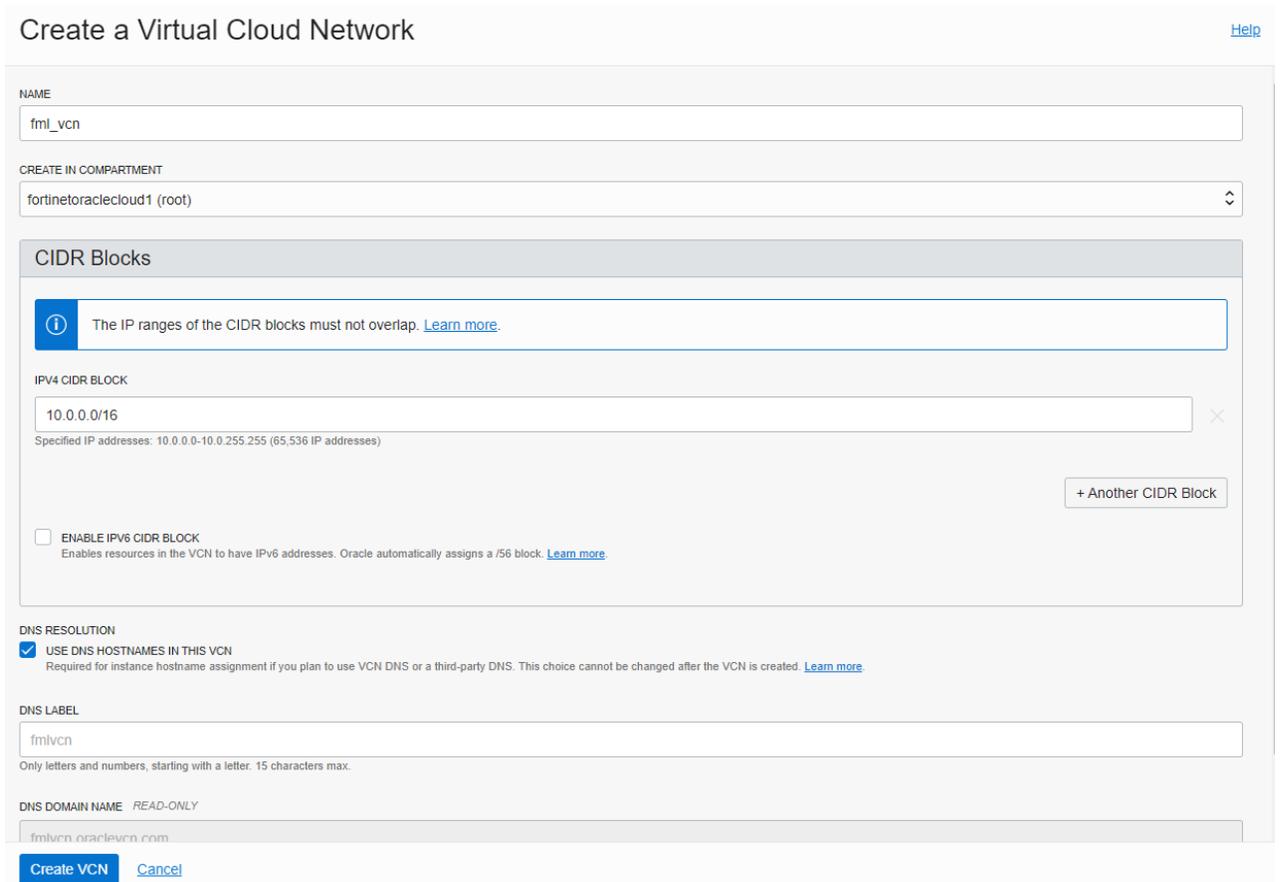
# Creating a Virtual Cloud Network and Public-facing Subnet

1. Log into OCI.

Go to *Networking > Virtual Cloud Networks*, and click *Create Virtual Cloud Network*.



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



3. In the virtual cloud network details, create a public-facing subnet.

## Creating a Virtual Cloud Network and Public-facing Subnet

Networking » Virtual Cloud Networks » Virtual Cloud Network Details



AVAILABLE

### fml\_vcn

[Move Resource](#) [Add Tags](#) [Terminate](#)

VCN Information [Tags](#)

**Compartment:** fortinetoraclecloud1 (root)  
**Created:** Wed, Apr 21, 2021, 06:11:07 UTC  
**IPv4 CIDR Block:** 10.0.0.0/16  
**IPv6 CIDR Block:** No Value

**OCID:** ...5qr4sa [Show](#) [Copy](#)  
**DNS Resolver:** [fml\\_vcn](#)  
**Default Route Table:** [Default Route Table for fml\\_vcn](#)  
**DNS Domain Name:** fmlvcn.oraclevcn.com

Resources

**Subnets (0)**

[CIDR Blocks \(1\)](#)

[Route Tables \(1\)](#)

[Internet Gateways \(0\)](#)

### Subnets *in* fortinetoraclecloud1 (root) *Compartment*

[Create Subnet](#)

Name	State	IPv4 CIDR Block	Subnet Access
No items found.			

In **SUBNET TYPE**, select *Regional*. In **SUBNET ACCESS**, select *Public Subnet*.

## Create Subnet

NAME

fml\_vcn\_public\_sub

CREATE IN COMPARTMENT

fortinetoraclecloud1 (root)

SUBNET TYPE

**Regional (Recommended)**

Instances in the subnet can be created in any availability domain in the region. Useful for high availability. ✓

**Availability Domain-specific**

Instances in the subnet can only be created in one availability domain in the region.

**CIDR Block**

CIDR BLOCK

10.0.0.0/24

Specified IP addresses: 10.0.0.0-10.0.0.255 (256 IP addresses)

ROUTE TABLE COMPARTMENT IN FORTINETORACLECLOUD1 (ROOT) [\(CHANGE COMPARTMENT\)](#)

Default Route Table for fml\_vcn

SUBNET ACCESS

**Private Subnet**

Prohibit public IP addresses for Instances in this Subnet

**Public Subnet**

Allow public IP addresses for Instances in this Subnet ✓

Leave the default **ROUTE TABLE**, **DHCP OPTIONS**, and **SECURITY LIST**. You will modify them later.

DNS LABEL

Only letters and numbers, starting with a letter. 15 characters max.

DNS DOMAIN NAME READ-ONLY

DHCP OPTIONS COMPARTMENT IN FORTINETORACLECLOUD1 (ROOT) [\(CHANGE COMPARTMENT\)](#)

**Security Lists**

You can associate up to 5 network security lists with the subnet.

SECURITY LIST COMPARTMENT IN FORTINETORACLECLOUD1 (ROOT) [\(CHANGE COMPARTMENT\)](#)

[+ Another Security List](#)

[Show Tagging Options](#)

[Create Subnet](#) [Cancel](#)

- To access FortiMail-VM with HTTPS, add an ingress rule in the security list. There are three default rules, including port 22 for SSH access. More ports are needed for later deployment and testing, such as port 25 for SMTP. You can add or modify these rules later.

Networking > Virtual Cloud Networks > fml\_vcn > Security List Details Subnet provisioning successfully initiated.



### Default Security List for fml\_vcn

Instance traffic is controlled by firewall rules on each Instance in addition to this Security List

[Move Resource](#) [Add Tags](#) [Terminate](#)

Security List Information Tags

OCID: ...3xwjq [Show](#) [Copy](#) Compartment: fortinetoraclecloud1 (root)

Created: Wed, Apr 21, 2021, 06:11:07 UTC

Resources

- [Ingress Rules \(3\)](#)
- [Egress Rules \(1\)](#)

**Ingress Rules**

[Add Ingress Rules](#) [Edit](#) [Remove](#)

<input type="checkbox"/>	Stateless	Source	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allows
<input type="checkbox"/>	No	0.0.0.0/0	TCP	All	22		TCP traffic for ports: 22 SSH Remote Login Protocol
<input type="checkbox"/>	No	0.0.0.0/0	ICMP			3, 4	ICMP traffic for: 3, 4 Destination Unreachable: Fragmentation Needed and Don't Fragment was Set
<input type="checkbox"/>	No	10.0.0.0/16	ICMP			3	ICMP traffic for: 3 Destination Unreachable

0 Selected

Click *Add Ingress Rule*. In *IP PROTOCOL*, select *TCP*. In *DESTINATION PORT*, enter 443.

Ingress Rule 1

Allows TCP traffic 443 HTTPS

STATELESS ⓘ

SOURCE TYPE: CIDR

SOURCE CIDR: 0.0.0.0/0  
Specified IP addresses: 0.0.0.0-255.255.255.255 (4,294,967,296 IP addresses)

IP PROTOCOL ⓘ: TCP

SOURCE PORT RANGE OPTIONAL ⓘ: All  
Examples: 80, 20-22

DESTINATION PORT RANGE OPTIONAL ⓘ: 443  
Examples: 80, 20-22

DESCRIPTION OPTIONAL

Maximum 255 characters

The default egress rules allow all traffic for all ports. No modification is required.

Resources

Egress Rules

[Add Egress Rules](#) [Edit](#) [Remove](#)

<input type="checkbox"/>	Stateless	Destination	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allows	Description
<input type="checkbox"/>	No	0.0.0.0/0	All Protocols				All traffic for all ports	

0 Selected Showing 1 item < 1 of 1 >

5. In the virtual cloud network, click *Create Internet Gateway*.

Networking » Virtual Cloud Networks » Virtual Cloud Network Details » Internet Gateways



fml\_vcn

[Move Resource](#) [Add Tags](#) [Terminate](#)

VCN Information Tags

**Compartment:** fortinetoraclecloud1 (root)  
**Created:** Wed, Apr 21, 2021, 06:11:07 UTC  
**IPv4 CIDR Block:** 10.0.0.0/16  
**IPv6 CIDR Block:** No Value

**OCID:** ...5qr4sa [Show](#) [Copy](#)  
**DNS Resolver:** [fml\\_vcn](#)  
**Default Route Table:** [Default Route Table for fml\\_vcn](#)  
**DNS Domain Name:** fmlvcn.oraclevcn.com

Resources

Subnets (1)  
 CIDR Blocks (1)  
 Route Tables (1)  
**Internet Gateways (0)**  
 Dynamic Routing Gateways (0)

Internet Gateways in fortinetoraclecloud1 (root) Compartment

[Create Internet Gateway](#)

Name	State	Created
No items found.		

Create Internet Gateway [Help](#) [Cancel](#)

---

NAME

fml\_vcn-gateway

CREATE IN COMPARTMENT

fortinetoraclecloud1 (root)

Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values that can be attached to resources.

[Learn more about tagging](#)

TAG NAMESPACE TAG KEY VALUE

None (add a free-form tag)   ×

[+ Additional Tag](#)

[Create Internet Gateway](#) [Cancel](#)

6. In the route table, click *Add Route Rules*.

[Networking](#) » [Virtual Cloud Networks](#) » [fml\\_vcn](#) » Route Table Details



AVAILABLE

## Default Route Table for fml\_vcn

[Move Resource](#) [Add Tags](#) [Terminate](#)

Route Table Information Tags

**OCID:** ...s7666q [Show](#) [Copy](#)

**Created:** Wed, Apr 21, 2021, 06:11:07 UTC

Resources

[Route Rules \(0\)](#)

### Route Rules

[Add Route Rules](#) [Edit](#) [Remove](#)

	Destination	Target Type
<input type="checkbox"/>		

0 Selected

In **TARGET TYPE**, select *Internet Gateway*. In **DESTINATION CIDR BLOCK**, select `0.0.0.0/0`. In **TARGET INTERNET GATEWAY**, select the gateway that you just created.

### Add Route Rules

[Help](#)

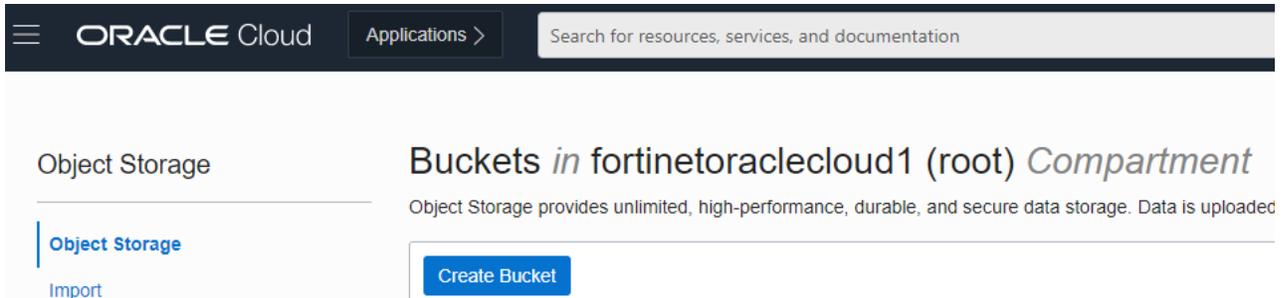
**Important:**  
For a route rule that targets a Private IP, you must first enable "Skip Source/Destination Check" on the VNIC that the Private IP is assigned to.

Route Rule
<b>TARGET TYPE</b> Internet Gateway
<b>DESTINATION CIDR BLOCK</b> 0.0.0.0/0 <small>Specified IP addresses: 0.0.0.0-255.255.255.255 (4,294,967,296 IP addresses)</small>
<b>TARGET INTERNET GATEWAY IN FORTINETORACLECLOUD1 (ROOT)</b> <a href="#">(CHANGE COMPARTMENT)</a> fml_vcn-gateway
<b>DESCRIPTION</b> <small>OPTIONAL</small>  <small>Maximum 255 characters</small>

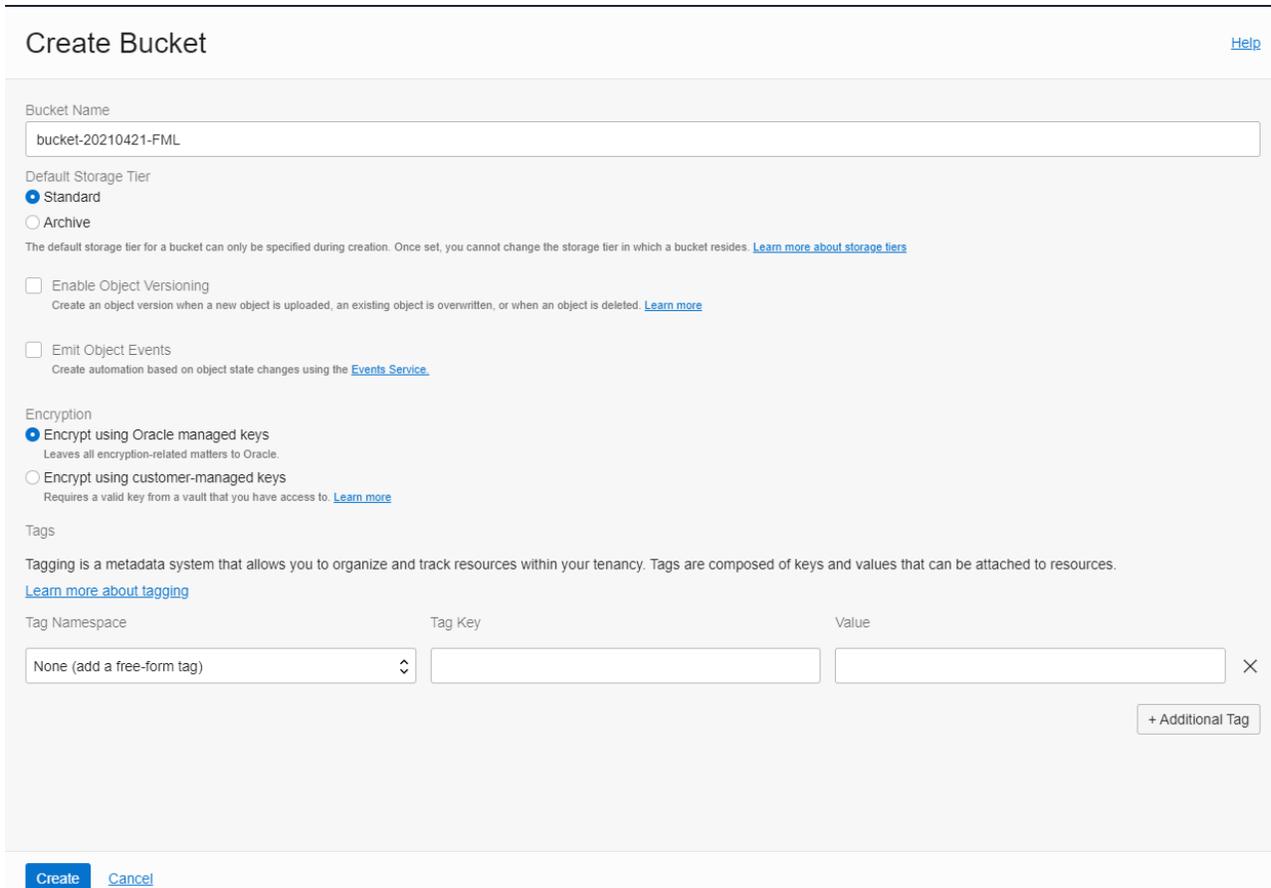
+ Another Route Rule

# Creating a FortiMail-VM Instance

1. Go to [Fortinet Support](#) 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. Log into OCI.
3. Go to *Object Storage*, then click *Create Bucket* to create a standard storage bucket.



You can create the bucket with default settings.



4. Click on the bucket that you just created and upload the \*.qcow2 file to *Objects*.

[Object Storage](#) » Bucket Details



## bucket-20210421-FML

[Edit Visibility](#) [Move Resource](#) [Re-encrypt](#) [Add Tags](#) [Delete](#)

Bucket Information [Tags](#)

**Visibility:** Private  
**Namespace:** fortinetoraclecloud1  
**Default Storage Tier:** Standard  
**Approximate Count:** 0 objects ⓘ  
**ETag:** b5e06036-c049-450a-a6d0-52c6780a4e8e  
**OCID:** ...i2i6hooa [Show](#) [Copy](#)

### Resources

**Objects**

[Metrics](#)

[Pre-Authenticated Requests](#)

### Objects

[Upload](#) [More Actions](#) ▾

<input type="checkbox"/>	Name	Last Modified
--------------------------	------	---------------

## Upload Objects

Object Name Prefix *Optional*

FML\_v70116\_image

Storage Tier

Standard

Choose Files from your Computer

Drop files here or [select files](#)

fortimail-opc.qcow2 108.38 MiB

1 files, 108.38 MiB total

[Show Optional Response Headers and Metadata](#)

5. After the image file is uploaded, create a pre-authenticated request.

### Resources

- Objects
- Metrics
- Pre-Authenticated Requests
- Work Requests

## Pre-Authenticated Requests

Create Pre-Authenticated Request

Name	Status	Target

---

### Create Pre-Authenticated Request [Help](#)

Name

Pre-Authenticated Request Target

**Bucket**

Create a pre-authenticated request that applies to all objects in the bucket.

**Object**

Create a pre-authenticated request that applies to a specific object. ✓

**Objects with prefix**

Create a pre-authenticated request that applies to all objects with a specific prefix.

Object Name

Access Type

Permit object reads

Permit object writes

Permit object reads and writes

Expiration

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

## Pre-Authenticated Request Details

Name *Read-Only*

Pre-Authenticated Request URL *Read-Only*

! Copy this URL for your records. It will not be shown again.

Close

- 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*. In *Launch mode*, select *Paravirtualized Mode* or *Emulated Mode*. Native mode is not supported.

## Import Image [Help](#)

Create in compartment

fortinetoraclecloud1 (root)

Name

fml-v70116

Operating system

Linux

Import from an Object Storage bucket  
 Import from an Object Storage URL

Object Storage URL

https://objectstorage.us-phoenix-1.oraclecloud.com/p/N7\_av1CUKWuXlGTv8yG6-COAmw8eQEmlPBxDNMjHeAxzR9MDHareGtw3-uQw2Yv1n/fortinetoraclecloud1/b/bucket-20210421-FML

Learn more about [Object Storage URLs](#). Also, see the instructions to [create a pre-authenticated request](#).

Image type

VMDK  
 Virtual machine disk file format. For disk images used in virtual machines.

QCOW2  
 For disk image files used by QEMU.

OCI  
 For images that were exported from Oracle Cloud Infrastructure. The launch mode is specified in the .oci file and can't be changed in the Console.

Launch mode

**Firmware:** BIOS

**Boot volume type:** PV

**NIC attachment type:** PV NIC

**Remote data volume:** PV

Paravirtualized Mode  
 For virtual machines that [support paravirtualized drivers](#), created outside of Oracle Cloud Infrastructure.

Emulated Mode  
 For virtual machines that [don't support paravirtualized drivers](#), created outside of Oracle Cloud Infrastructure from older on-premises physical or virtual machines.

Native Mode  
 For images that were exported from Oracle Cloud Infrastructure.

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

Compute > Custom Images > Custom Image Details

CI

AVAILABLE

fml-v70116-20210421

Custom Image Information Tags

---

**Custom Image Information**

**OCID:** `..bmrndna` [Show](#) [Copy](#)

**Original Image:** -

**Compartment:** fortinetoraclecloud1 (root)

**Launch Mode:** PARAVIRTUALIZED

**Created:** Wed, Apr 21, 2021, 07:14:15 UTC

**Compatible:** VM.Standard.E3.Flex, VM.Standard2.1, VM.Standard2.2, VM.Standard2.4, VM.Standard2.8

**Shapes:** VM.Standard2.16, VM.Standard2.24, VM.Standard1.1, VM.Standard1.2, VM.Standard1.4, VM.Standard1.8, VM.Standard1.16

**Flex Shape Requirements:** 1 OCPU minimum, 64 OCPU maximum

**Launch Options**

Launch options include the networking type and boot volume attachment type used when launching a virtual machine instance. [Learn more](#)

**NIC Attachment Type:** PARAVIRTUALIZED

**Remote Data Volume:** PARAVIRTUALIZED

**Firmware:** BIOS

**Boot Volume Type:** PARAVIRTUALIZED

9. Either select an *Availability domain* or keep the default advanced options.

## Create Compute Instance

Create an instance to deploy and run applications, or save as a reusable Terraform stack for creating an instance with Resource Manager.

Name  
fml-20210421-v70116

Create in compartment  
fortinetoraclecloud1 (root)

**Placement** [Collapse](#)

The [availability domain](#) helps determine which shapes are available.

Availability domain

AD 1 www1:PHX-AD-1 ✓	AD 2 www1:PHX-AD-2	AD 3 www1:PHX-AD-3
-------------------------	-----------------------	-----------------------

[Hide advanced options](#)

Capacity type

- On-demand capacity  
Place the instance on a shared host using on-demand capacity.
- Preemptible capacity  
Place the instance on a shared host using [preemptible capacity](#). This instance can be reclaimed at any time.
- Capacity reservation  
Place the instance on a shared host, and have it count against a [capacity reservation](#).
- Dedicated host  
Place the instance on a [dedicated virtual machine host](#).

Fault Domain  
Let Oracle choose the best fault domain

[When should I specify a fault domain?](#)

Image and shape are chosen automatically. You can modify the shape if required.

**Image and shape** [Collapse](#)

A [shape](#) is a template that determines the number of CPUs, amount of memory, and other resources allocated to an instance. The image is the operating system that runs on top of the shape.

Image

fml-v70116-20210421 [Change Image](#)

Shape

**AMD** VM.Standard.E3.Flex  
Virtual Machine, 1 core OCPU, 16 GB memory, 1 Gbps network bandwidth [Change Shape](#)

10. Select your virtual cloud network and its public subnet. For public access to your FortiMail-VM, you must assign a public IPV4 address.

### Networking [Collapse](#)

[Networking](#) is how your instance connects to the internet and other resources in the Console. To make sure you can [connect to your instance](#), assign a public IP address to the instance.

Network  
 Select existing virtual cloud network    Create new virtual cloud network    Enter subnet OCID

Virtual cloud network in **fortinetoracled1 (root)** [\(Change Compartment\)](#)

fml\_vcn

Subnet  
 Select existing subnet    Create new public subnet

Subnet in **fortinetoracled1 (root)** [\(Change Compartment\)](#)

fml\_vcn\_public\_sub (Regional)

Public IP Address  
 Assign a public IPv4 address    Do not assign a public IPv4 address

! Assigning a public IP address makes this instance accessible from the internet. If you're not sure whether you need a public IP address, you can always assign one later.

[Show advanced options](#)

11. 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.

### Add SSH keys

Linux-based instances use an [SSH key pair](#) instead of a password to authenticate remote users. Generate a key pair or upload your own public key now. When you [connect to the instance](#), you will provide the associated private key.

Generate SSH key pair    Upload public key files (.pub)    Paste public keys    No SSH keys

i Download the private key so that you can connect to the instance using SSH. It will not be shown again.

[Save Private Key](#)
[Save Public Key](#)

### Boot volume

Your [boot volume](#) is a detachable device that contains the image used to boot your compute instance.

Specify a custom boot volume size  
[Volume performance](#) varies with volume size. Default boot volume size: 46.6 GB

Boot volume size (GB)

50

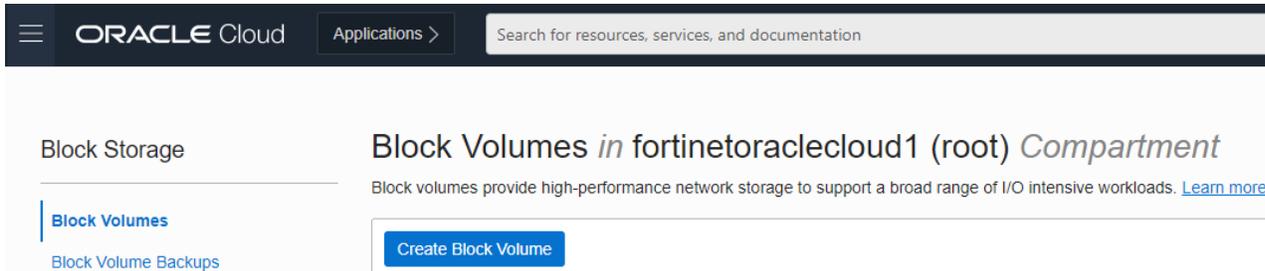
Integer between 50 GB and 32,768 GB (32 TB). Must be larger than the default boot volume size for the selected image.

Encrypt this volume with a key that you manage  
By default, Oracle manages the keys that encrypt this volume, but you can choose a key from a vault that you have access to if you want greater control over the key's lifecycle and how it's used. [Learn more about managing your own encryption keys](#)

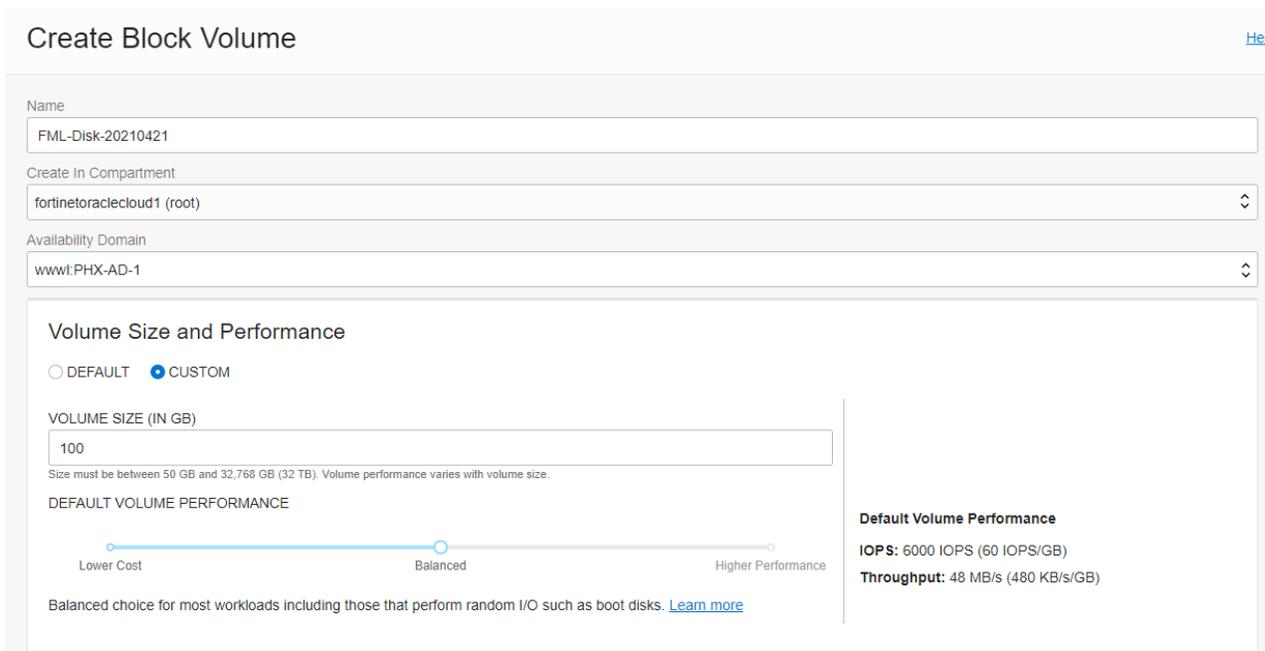
At this time, the deployment is not complete yet. You also need to add a storage volume as a system log disk and attach it to the FortiMail-VM instance. If you want FortiMail-VM to run inline across multiple subnets, you also need to add one or more virtual network interfaces and attach them to the FortiMail-VM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

# Attaching Storage to FortiMail-VM

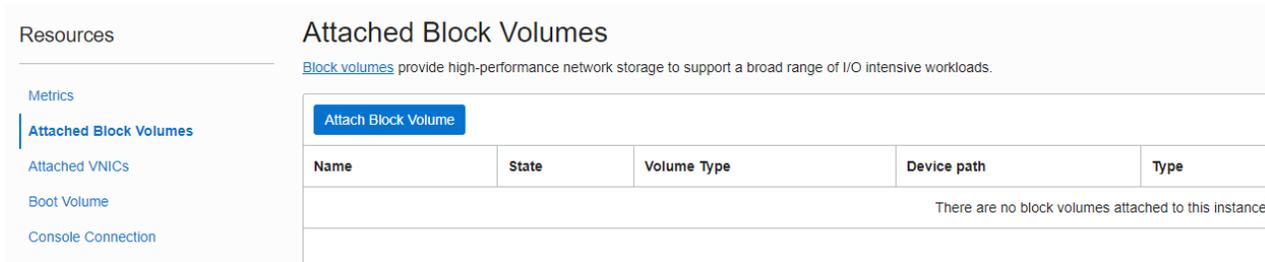
1. On OCI, go to *Storage > Block Volumes > Create Block Volume*.



*Availability Domain* should be the same as your instance, and customize a smaller volume size such as 100 GB. Keep other default settings.



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



3. Select the block volume that you created earlier. In *Volume attachment type*, select *Paravirtualized*.

### Attach Block Volume [Help](#)

Volume attachment type

Let Oracle Cloud Infrastructure choose the best attachment type

iSCSI

Paravirtualized

Use in-transit encryption

#### Volume

Select volume  Enter volume OCID

Volume in **fortinetoraclecloud1 (root)** [Change Compartment](#)

FML-Disk-20210421

Access

Read/Write  
Configures the volume attachment as read/write, not shared with other instances. This enables attachment to a single instance only and is the default configuration.

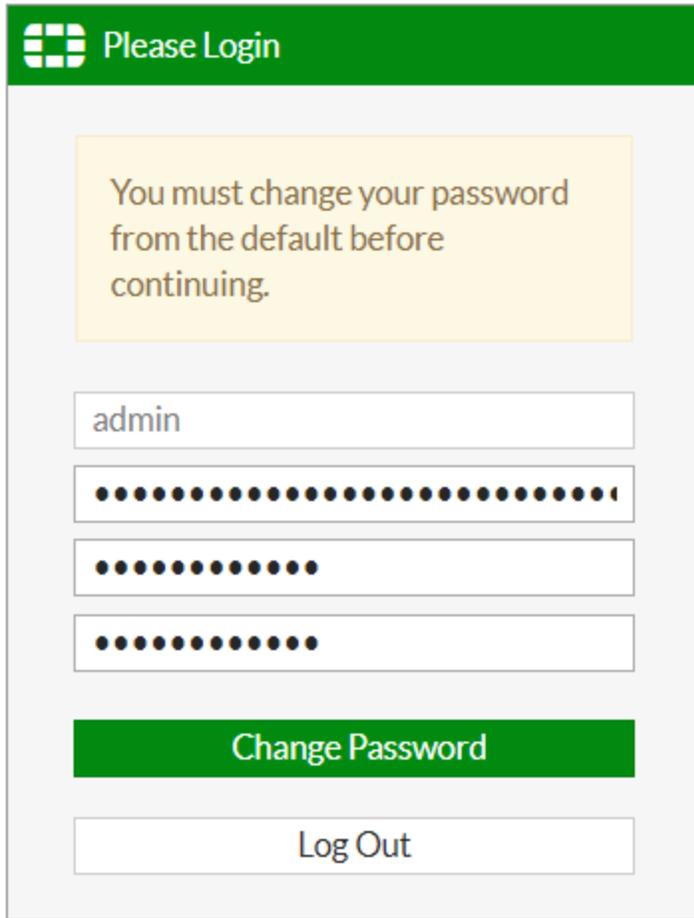
Read/Write - Shareable  
Configures the volume attachment as read/write, shareable with other instances. This enables read/write attachment to multiple instances.

Read Only - Shareable  
Configures the volume attachment as read-only, enabling attachment to multiple instances.



After attaching the block volume, reboot the FortiMail-VM instance.





3. Upload a valid FortiMail-VM license. The FortiMail administrator GUI should appear.

**System Information**

- Serial number: FEVM0200002
- Up time: 0 day(s) 0 hour(s) 26 minute(s) 24 second(s)
- System time: Wed, Apr 21, 2021 11:00:46 PDT
- Reboot time: Wed, Apr 21, 2021 10:34:22 PDT
- Firmware version: v7.0.0, build116, 2021.04.16 [\[Update...\]](#)
- System configuration: [\[Backup...\]](#) [\[Restore...\]](#)
- Operation mode: Gateway
- Current administrator: admin (1 in total) [\[Details...\]](#)
- HA mode: Configured Off, Effective Off
- Log disk: Capacity 19 GB, Used 32 MB (0.17%), Free 19 GB
- Mailbox disk: Capacity 78 GB, Used 276 MB (0.35%), Free 78 GB
- Email throughput: 0 messages per minute (last 26 minutes) Spam: 0, Not Spam: 0 messages per minute

**License Information**

- AntiVirus: **No license**
  - AV definition: Version 1.00000 (Last updated 2018-05-02 11:41:00) [\[Update...\]](#)
  - AV engine: Version 6.00258 (Last updated 2021-03-17 00:40:00)
  - Virus outbreak: Licensed (Expiry date 2022-04-13)
  - AntiSpam: Licensed (Expiry date 2022-04-13)
  - AS definition: Version 1.00001 (Last updated 2007-05-09 17:15:00)
- VM: Registered [\[Update...\]](#)
- FortiSandbox: Disabled [\[Configure...\]](#)
- FortiCloud: Not Activated [\[Activate...\]](#)

**System Resource**

- CPU usage: 0%
- Memory usage: 6%
- System load: 1%
- Log disk usage: 0%

**Statistics History (Count, 30 Days)**

No data!

**Statistics Summary (Today)**

No data!

**Statistics Summary**

Messages		Total	This Year	This Month	This Week	Today	This Hour	This Minute
Not Spam Classified By	Subtotal	0	0	0	0	0	0	0
		0%	0%	0%	0%	0%	0%	0%
Spam Classified By	Subtotal	0	0	0	0	0	0	0
		0%	0%	0%	0%	0%	0%	0%
Virus Classified By	Subtotal	0	0	0	0	0	0	0
		0%	0%	0%	0%	0%	0%	0%
<b>Total</b>		0	0	0	0	0	0	0

**Throughput History (Scan Speed, 30 Days)**

10 KB/s  
8 KB/s  
6 KB/s  
4 KB/s  
2 KB/s

- For further deployment and testing on your FortiMail-VM instance, you may need to add more rules in *Security List* on OCI. For example, a rule to open port 25 is necessary for SMTP testing.

Add Ingress Rules [Cancel](#)

---

Ingress Rule 1

Allows TCP traffic 25 Simple Mail Transfer Protocol (SMTP)

STATELESS ⓘ

SOURCE TYPE: CIDR

SOURCE CIDR: 0.0.0.0/0  
Specified IP addresses: 0.0.0.0-255.255.255.255 (4,294,967,296 IP addresses)

IP PROTOCOL ⓘ: TCP

SOURCE PORT RANGE OPTIONAL ⓘ: All  
Examples: 80, 20-22

DESTINATION PORT RANGE OPTIONAL ⓘ: 25  
Examples: 80, 20-22

DESCRIPTION OPTIONAL

Maximum 255 characters

[+ Another Ingress Rule](#)



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2025 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.