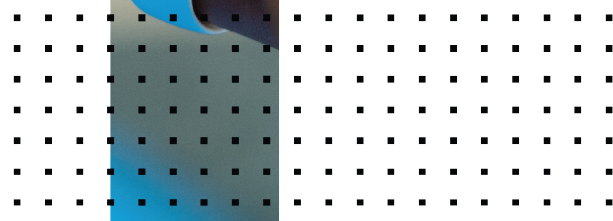
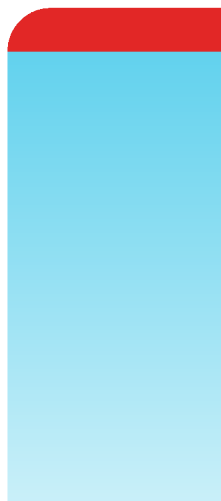


# OCI Administration Guide

FortiAuthenticator 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/support-and-training/training.html>

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



August 5, 2021

FortiAuthenticator 6.4.0 OCI Administration Guide

23-640-734921-20210805

# TABLE OF CONTENTS

<b>Change log</b> .....	<b>4</b>
<b>About FortiAuthenticator on OCI</b> .....	<b>5</b>
OCI instance type support .....	5
Licensing .....	6
<b>Deploying FortiAuthenticator on OCI</b> .....	<b>7</b>
Preparing for a deployment .....	7
Creating an instance by importing an image .....	7
Obtaining the deployment image and placing it in your bucket .....	7
Importing the image .....	10
Launching the FortiAuthenticator-VM instance .....	12
Connecting to FortiAuthenticator-VM .....	16

# Change log

Date	Change Description
2021-08-05	Initial release.

# About FortiAuthenticator on OCI

FortiAuthenticator is designed specifically to provide authentication services for firewalls, SSL and IPsec VPNs, wireless access points, switches, routers, and servers. FortiAuthenticator includes Remote Authentication Dial-In User Service (RADIUS) and Lightweight Directory Access Protocol (LDAPv3) server authentication methods, and Security Assertion Markup Language (SAML), which is used for exchanging authentication and authorization data between an Identity Provider (IdP) and a Service Provider (SP). Authentication servers are an important part of an enterprise network, controlling access to protected network assets, and tracking user activity to comply with security policies.

FortiAuthenticator is not a firewall; it requires either a FortiGate-VM "virtual" or FortiGate "hardware" appliance to provide firewall-related services. Multiple FortiGate appliances can use a single FortiAuthenticator appliance for Fortinet Single Sign-On (FSSO) and other types of remote authentication, two-factor authentication, and FortiToken device management. This centralizes authentication and FortiToken maintenance.

FortiAuthenticator provides an easy-to-configure remote authentication option for FortiGate users. Additionally, it can replace the Fortinet Single Sign-On (FSSO) Agent on a Windows Active Directory (AD) network.

## OCI instance type support

FortiAuthenticator-VM supports the following OCI compute shapes. For up-to-date information on each instance type, see [OCI Compute Shapes](#).

When selecting an instance type for your deployment, consider your use case for FortiAuthenticator and the requirements to support it.

Compute shape	OCPUs	Max VNIC	FortiAuthenticator-VM license
VM.Standard2.1	1	2	FAC-VM-100-UG
VM.Standard2.2	2	2	FAC-VM-100-UG or FAC-VM-1000-UG
VM.Standard2.4	4	4	FAC-VM-100-UG, FAC-VM-1000-UG or FAC-VM-10000-UG
VM.Standard2.8	8	8	FAC-VM-10000-UG or FAC-VM-100000-UG
VM.Standard2.16	16	16	FAC-VM-100000-UG
VM.Standard2.24	24	24	FAC-VM-100000-UG
VM.Standard1.1	1	2	FAC-VM-100-UG
VM.Standard1.2	2	2	FAC-VM-100-UG or FAC-VM-1000-UG
VM.Standard1.4	4	4	FAC-VM-100-UG, FAC-VM-1000-UG or FAC-VM-10000-UG
VM.Standard1.8	8	8	FAC-VM-10000-UG or FAC-VM-100000-UG
VM.Standard1.16	16	16	FAC-VM-100000-UG

## Licensing

FortiAuthenticator for OCI supports the bring your own license (BYOL) model.

Licenses can be obtained through any Fortinet partner. If you don't have a reseller partner, you can find a local Fortinet reseller partner by visiting the [Find a Partner](#) portal and performing a search in the following regions:

- Asia Pacific, Australia, and New Zealand
- EMEA (Europe, Middle East, and Africa)
- Latin America and Caribbean
- North America
- North America: US Federal

This license model is stackable, allowing you to expand your VM solution as your environment expands. For additional information on the FortiAuthenticator stackable license model, see the [FortiAuthenticator datasheet](#).

# Deploying FortiAuthenticator on OCI

This guide provides step-by-step instructions for successful deployment and initial configuration of FortiAuthenticator for OCI:

- [Preparing for a deployment on page 7](#)
- [Creating an instance by importing an image on page 7](#)
- [Connecting to FortiAuthenticator-VM on page 16](#)

## Preparing for a deployment

The deployment section in this guide assumes that you have already created a Virtual Cloud Network (VCN) and relevant network resources, such as route tables and subnets. You must also configure a Security List so that you can access FortiAuthenticator over the Internet while closing unnecessary ports. At a minimum, you must open TCP port 443 and 22 to allow incoming access to the FortiAuthenticator management GUI and SSH console for initial configuration. See the *Ports and Protocols* document on the [Fortinet Document Library](#).

You can obtain the deployment image, import the file into the OCI portal, and then launch the FortiAuthenticator-VM instance. See [Creating an instance by importing an image on page 7](#).

## Creating an instance by importing an image

This guide provides step-by-step instructions for successful deployment and initial configuration of FortiAuthenticator for OCI:

- [Obtaining the deployment image and placing it in your bucket on page 7](#)
- [Importing the image on page 10](#)
- [Connecting to FortiAuthenticator-VM on page 16](#)

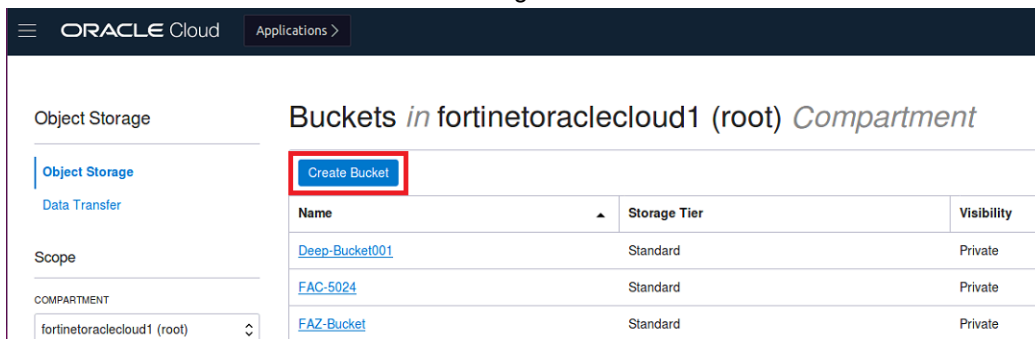
## Obtaining the deployment image and placing it in your bucket

1. Go to <https://support.fortinet.com>.
2. In the top menu, navigate to *Download > Firmware Images*.
3. From the *Select Product* dropdown list, select *FortiAuthenticator*, then click the *Download* tab.
4. Navigate to the desired firmware release.
5. Download the *FAC\_VM\_OPCVX-buildXXXX-FORTINET.out.opc.zipfile*.

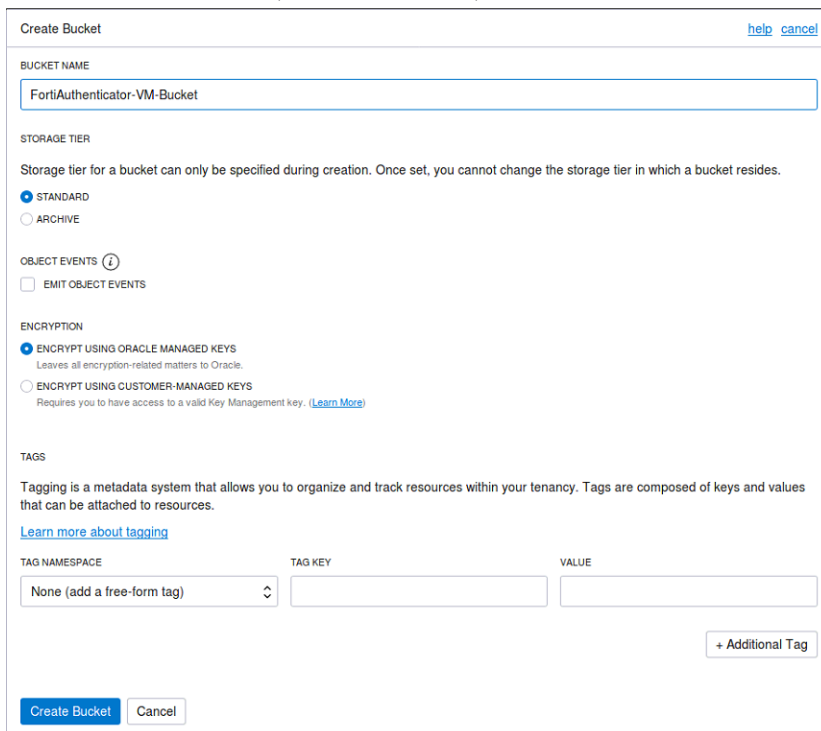


- XXX is the build number.
  - Ensure the file name includes the OPC.
-

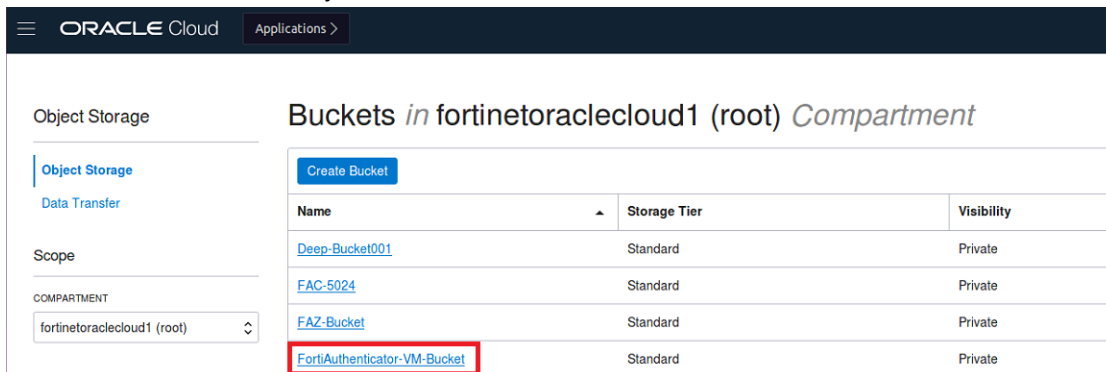
6. After you extract the zip the file, locate the *fackvm.qcow2* file. You will need this file to deploy FortiAuthenticator on OCI.
7. In OCI, go to *Core Infrastructure > Object Storage > Object Storage*.
8. Click *Create Bucket* to create a standard storage bucket.



9. In the *Bucket Name* field, name the bucket, then click *Create Bucket*.



10. Click the name of the bucket you created to edit it.





11. Click *Upload Objects*.

Object Storage - Bucket Details

### FortiAuthenticator-VM-Bucket

Edit Visibility Move Resource Add Tags Delete

Bucket Information Tags

Visibility: Private  
 Namespace: fortinetoraclecloud1  
 Storage Tier: Standard  
 Approximate Count: 0 objects  
 ETag: 2133328a-aa50-4e0d-bd17-de8ec8cf0387

Encryption Key: Oracle managed key [Assign](#)  
 Created: Mon, Sep 23, 2019, 16:28:36 UTC  
 Compartment: [fortinetoraclecloud1](#)  
 Approximate Size: 0 bytes  
 Emit Object Events: Disabled [Edit](#)

Resources

- Objects
- Metrics
- Pre-Authenticated Requests
- Work Requests
- Lifecycle Policy Rules

### Objects

Upload Objects Restore Delete Search by prefix

Name	Size	Status	Created
No items found.			

0 Selected Showing 0 Items Page 1

12. Upload the objects:

- (Optional) Edit the *Object Name Prefix*.
- Upload the deployment image *fackvm.qcow2* file that you downloaded.
- Click *Upload Objects*.

Upload Objects [help](#) [cancel](#)

OBJECT NAME PREFIX *OPTIONAL*

FortiAuthenticator-VM

CHOOSE FILES FROM YOUR COMPUTER

Drop files here or [select files](#)

fackvm.qcow2 70.54 MiB

1 files, 70.54 MiB total

Upload Objects Cancel

13. Select *View Object Details* for the newly uploaded object.

Object Storage - Bucket Details

### FortiAuthenticator-VM-Bucket

Edit Visibility Move Resource Add Tags Delete

Bucket Information Tags

Visibility: Private  
 Namespace: fortinetoraclecloud1  
 Storage Tier: Standard  
 Approximate Count: 0 objects  
 ETag: 2133328a-aa50-4e0d-bd17-de8ec8cf0387

Encryption Key: Oracle managed key [Assign](#)  
 Created: Mon, Sep 23, 2019, 16:28:36 UTC  
 Compartment: [fortinetoraclecloud1](#)  
 Approximate Size: 0 bytes  
 Emit Object Events: Disabled [Edit](#)

Resources

- Objects
- Metrics
- Pre-Authenticated Requests
- Work Requests
- Lifecycle Policy Rules

### Objects

Upload Objects Restore Delete Search by prefix

Name	Size	Status	Created
FortiAuthenticator-VMfackvm.qcow2	70.54 MiB	Available	Mon, Sep 23, 2019, 16:34:04 UTC

0 Selected Showing 1 Item Page 1

14. Save the URI of the object.



This file is required in a subsequent step.

Object Details [close](#)

**Name:** FortiAuthenticator-VMfackvm.qcow2

**URL Path (URI):** <https://objectstorage.us-ashburn-1.oraclecloud.com/n/fortinetoraclecloud1/b/FortiAuthenticator-VM-Bucket/o/FortiAuthenticator-VMfackvm.qcow2>

**Storage Tier:** Standard

**Size:** 70.54 MiB

**Accept-Ranges:** bytes

**Content Length:** 73961472

**Etag:** 695ec2a9-534a-4509-8379-49b930e68bc0

**Last Modified:** Mon, Sep 23, 2019, 16:34:04 UTC

**opc-multipart-md5:** Aa03lpwGT+T6ObHjvtqhsQ==2

**x-api-id:** native

[Download](#)

## Importing the image

1. In OCI, go to *Core Infrastructure > Compute > Custom Images*, and click *Import Image*.

The screenshot shows the Oracle Cloud console interface. On the left sidebar, under 'Compute', the 'Custom Images' option is selected. In the main content area, the 'Import Image' button is highlighted with a red box. Below the button, a table lists existing custom images. The table has columns for image name, OCID, original image, and creation date. Two images are visible: 'FACE-5024-PV' and 'fmg1166-pv'. Both are marked as 'AVAILABLE'.

2. On the *Import Image* page:
  - a. *Name* the image.
  - b. Set the *Image Type* to *QCOW2*.
  - c. Set the *Launch Mode* to *Paravirtualized Mode*.
  - d. Click *Import Image* and wait for the image status to become *Available*.

**Import Image** [help](#) [cancel](#)

---

**CREATE IN COMPARTMENT**  
 fortinetoraclecloud1 (root)

**NAME**  
 FortiAuthenticator-VM

**OPERATING SYSTEM**  
 Linux

**OBJECT STORAGE URL**  
 https://objectstorage.us-ashburn-1.oraclecloud.com/n/fortinetoraclecloud1/b/FortiAuthenticator-VM-Bucket/o/FortiAuthenticator-VMfackvm.qcow2

See [Object Storage URLs](#) for more information. See [instructions](#) for creating a pre-authenticated request.

**IMAGE TYPE**

VMDK

QCOW2

OCI  
Select OCI for .oci files exported from Oracle Cloud Infrastructure. The launch mode setting is specified in the .oci file and cannot be changed in the Console.

**LAUNCH MODE**

PARAVIRTUALIZED MODE  
 Select this option for virtual machines that [support paravirtualized drivers](#), created outside of Oracle Cloud Infrastructure.  
[Show Launch Options](#)

EMULATED MODE  
 Select this option for virtual machines that [do not support paravirtualized drivers](#), created outside of Oracle Cloud Infrastructure from your older on-premise physical or virtual machines.  
[Show Launch Options](#)

NATIVE MODE  
 Select this option for images exported from Oracle Cloud Infrastructure.  
[Show Launch Options](#)

**TAGS**  
 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: None (apply a free-form tag) | TAG KEY: | VALUE: | [+ Additional Tag](#)

VIEW DETAIL PAGE AFTER THIS IMAGE IS IMPORTED

**Import Image**

3. Go to **Core Infrastructure > Block Storage > Block Volumes**, and click **Create Block Volume**.

The screenshot shows the Oracle Cloud console interface. At the top, there's a navigation bar with 'ORACLE Cloud' and 'Applications >'. Below that, the page title is 'Block Storage' and 'Block Volumes in fortinetoraclecloud1 (root) Compartment'. On the left, there's a sidebar with 'Block Volumes' selected. In the main content area, a 'Create Block Volume' button is highlighted with a red box. Below the button is a table listing existing block volumes.

Name	State	Size	Availability Domain
<a href="#">FortiAuthenticator-VM-volume</a>	Provisioning...	50 GB	www1:US-ASHBURN-AD-1
<a href="#">FAC6-5024-BV</a>	Available	50 GB	www1:US-ASHBURN-AD-1
<a href="#">red-BV2</a>	Available	1024 GB	www1:US-ASHBURN-AD-1

4. On the **Create Block Volume** page:

- a. **Name** the volume.
- b. Set the block volume **Size (in GB)**.  
 The FortiAuthenticator-VM is able to run using the minimum 50 GB size, but a larger storage size may be desirable depending on how long of a log history must be preserved and how much activity the VM instance will be subject to.
- c. Click **Create Block Volume**.

Create Block Volume [help](#) [cancel](#)

NAME  
FortiAuthenticator-VM-volume

CREATE IN COMPARTMENT  
fortinetoraclecloud1 (root)

AVAILABILITY DOMAIN  
www.US-ASHBURN-AD-1

SIZE (IN GB)  
50  
Size must be between 50 GB and 32,768 GB (32 TB). Volume performance varies with volume size.

BACKUP POLICY [?](#)  
Select a Backup Policy

ENCRYPTION  
 ENCRYPT USING ORACLE-MANAGED KEYS  
Leaves all encryption-related matters to Oracle.  
 ENCRYPT USING CUSTOMER-MANAGED KEYS  
Requires you to have access to a valid Key Management key.

TAGS  
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](#)

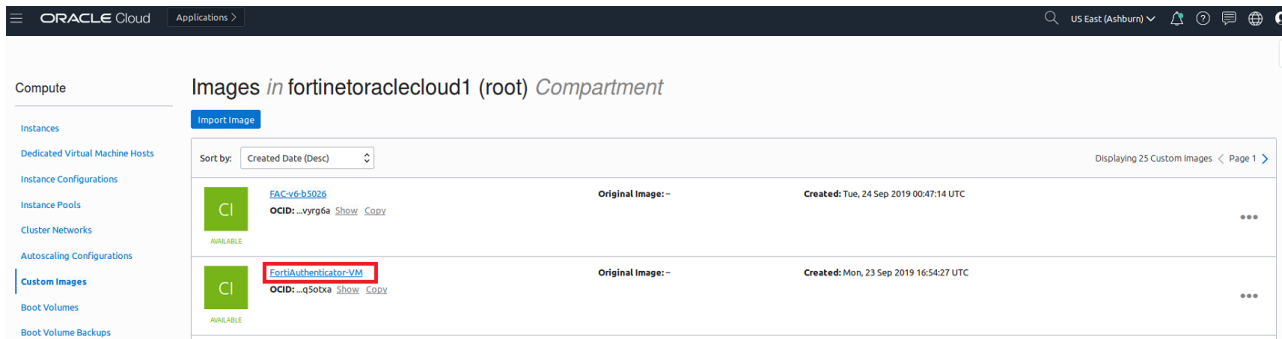
TAG NAMESPACE TAG KEY VALUE  
None (add a free-form tag)

VIEW DETAIL PAGE AFTER THIS BLOCK VOLUME IS CREATED

[Create Block Volume](#) [Cancel](#) [+ Additional Tag](#)

## Launching the FortiAuthenticator-VM instance

1. In OCI go to *Core Infrastructure > Compute > Custom Images*, and click the previously imported image. See [Importing the image on page 10](#).



2. Click *Create Instance*.

The screenshot shows the Oracle Cloud console interface for a custom image named 'FortiAuthenticator-VM'. The 'Create Instance' button is highlighted with a red box. The page displays the following information:

- Custom Image Information:** OCID: ...q50bxa, Original Image: -, Compartment: fortinetoracledcloud1 (root), Launch Mode: PARAVIRTUALIZED, Created: Mon, 23 Sep 2019 16:54:27 UTC, Compatible Shapes: VM.Standard2.1, VM.Standard2.2, VM.Standard2.4, VM.Standard2.8, VM.Standard2.16, VM.Standard2.24, VM.Standard1.1, VM.Standard1.2, VM.Standard1.4, VM.Standard1.8, VM.Standard1.16.
- Launch Options:** NIC Attachment Type: PARAVIRTUALIZED, Remote Data Volume: PARAVIRTUALIZED, Firmware: BIOS, Boot Volume Type: PARAVIRTUALIZED.
- Work Requests:** A table with columns: Operation, Status, % Complete, Accepted, Started, Finished. The table is currently empty, showing 'No items found.'

3. On the *Create Compute Instance* page:
- a. In the *Name your instance* field, name the instance.
  - b. In the *Configure networking* section, configure the network.



The *Subnet* must be a public network reachable using an SSH client and web browser.

ORACLE Cloud Applications >

### Create Compute Instance

Name your instance  
FAC-VM-instance-20190923-1356

Choose an operating system or image source ⓘ

FortiAuthenticator-VM Change Image Source

[Hide Shape, Network, Storage Options](#)

Availability Domain

<b>AD 1</b> www1.US-ASHBURN-AD-1 ✓	<b>AD 2</b> www1.US-ASHBURN-AD-2	<b>AD 3</b> www1.US-ASHBURN-AD-3
---------------------------------------	-------------------------------------	-------------------------------------

Instance Type

<b>Virtual Machine</b> A virtual machine is an independent computing environment that runs on top of physical bare metal hardware. ✓	<b>Bare Metal Machine</b> A bare metal compute instance gives you dedicated physical server access for highest performance and strong isolation.
---	---

Instance Shape

**VM.Standard2.1 (Virtual Machine)**  
1 Core OCPU, 15 GB Memory Change Shape

Configure networking

Virtual cloud network compartment  
fortinetoraclecloud1 (root) ▾

Virtual cloud network  
red-VCN1 ▾

Subnet compartment  
fortinetoraclecloud1 (root) ▾

Subnet ⓘ  
Public Subnet www1.US-ASHBURN-AD-1 ▾

Use network security groups to control traffic ⓘ

Boot volume

Default boot volume size: 46.6 GB

Custom boot volume size (in GB)

Choose a key from Key Management to encrypt this volume

Add SSH key ⓘ

Choose SSH key file  Paste SSH keys

Choose SSH key file (.pub) from your computer

Choose Files

[Show Advanced Options](#)

Create Cancel

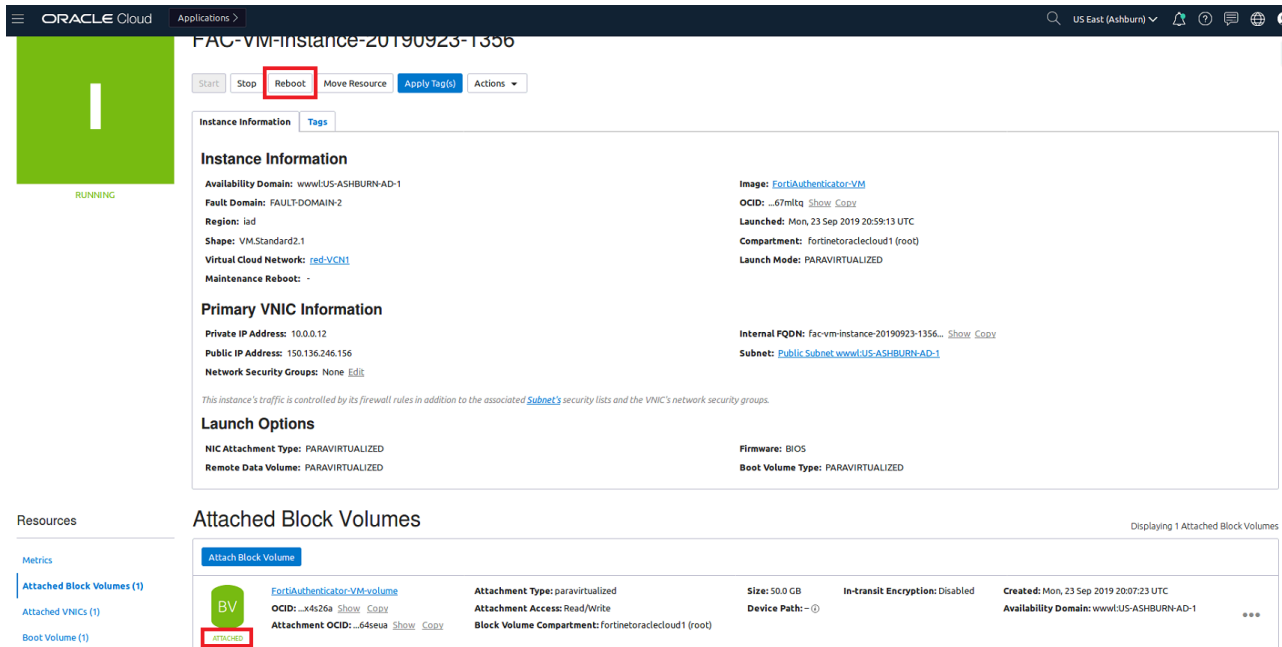
4. Once the instance is *Running*:
  - a. From the side-menu, select *Attached Block Volumes (0)*.
  - b. Click *Attach Block*.

The screenshot shows the Oracle Cloud console interface for a VM instance. The instance name is 'FAC-VM-instance-20190923-1356' and its status is 'RUNNING'. The 'Attached Block Volumes' section is highlighted with a red box, showing 'Attached Block Volumes (0)'. A red box also highlights the 'Attach Block Volume' button in the 'Attached Block Volumes' section.

5. On the *Attach Block Volume* page, select the following options, and click *Attach*:
  - *PARAVIRTUALIZED*
  - *READ/WRITE*
  - The previously created *BLOCK VOLUME*

The screenshot shows the 'Attach Block Volume' configuration page. The 'PARAVIRTUALIZED' radio button is selected under 'Choose how you want to attach your block volume.'. Under 'ACCESS', the 'READ/WRITE' radio button is selected. The 'BLOCK VOLUME COMPARTMENT' dropdown is set to 'fortinetoracled1 (root)' and the 'BLOCK VOLUME' dropdown is set to 'FortiAuthenticator-VM-volume'. The 'Attach' button is visible at the bottom.

- Wait for the block volume to reach the *Attached* state, then click *Reboot* to restart the FortiAuthenticator-VM.



## Connecting to FortiAuthenticator-VM

To access the GUI console of the FortiAuthenticator-VM, log in to its CLI console via SSH, and then connect the public IP address assigned to the instance.

- On OCI, go to *Core Infrastructure > Compute > Instances*, and click the name of the FortiAuthenticator-VM instance that is running.



2. Copy the *Public IP Address* and *OCID*.

ORACLE Cloud Applications >

Compute » Instances » Instance Details

**FACVMv6b5026**

Start Stop Reboot Move Resource Apply Tag(s) Actions

Instance Information Tags

**Instance Information**

Availability Domain: [www:US-ASHBURN-AD-1](#)  
 Fault Domain: [FAULT-DOMAIN-2](#)  
 Region: [iad](#)  
 Shape: [VM.Standard2.1](#)  
 Virtual Cloud Network: [facqa-vcn-1](#)  
 Maintenance Reboot: -

**Primary VNIC Information**

Private IP Address: [10.0.0.11](#)  
**Public IP Address: [150.136.252.96](#)**  
 Network Security Groups: [None](#) [Edit](#)

Image: [FACVMv6b5026](#)  
**OCID: [...2tkzpq](#)** [Show](#) [Copy](#)  
 Launched: [Wed, 25 Sep 2019 22:04:23 UTC](#)  
 Compartment: [fortinetoraclecloud1 \(root\)](#)  
 Launch Mode: [PARAVIRTUALIZED](#)

Internal FQDN: [facvmv6b5026...](#) [Show](#) [Copy](#)  
 Subnet: [Public Subnet www:US-ASHBURN-AD-1](#)

This instance's traffic is controlled by its firewall rules in addition to the associated [Subnet's](#) security lists and the VNIC's network security groups.

**Launch Options**

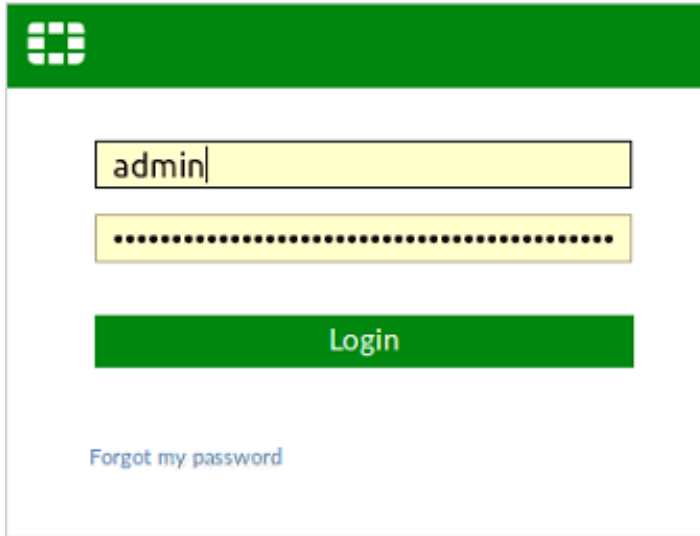
NIC Attachment Type: [PARAVIRTUALIZED](#)  
 Remote Data Volume: [PARAVIRTUALIZED](#)  
 Firmware: [BIOS](#)  
 Boot Volume Type: [PARAVIRTUALIZED](#)

3. Connect to the public IP address using an SSH client.
  - a. Log in with *admin* as the username and the *OCID* as the password.
  - b. Using the CLI, add the public IP address to the `allowed-hosts`. For example:

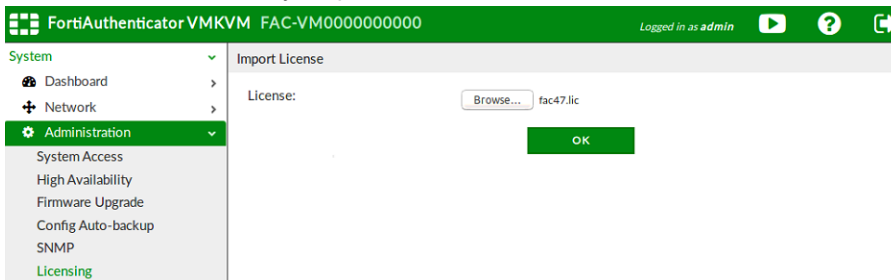
```
> config system global
(global): set allowed-hosts 150.136.252.96
(global): end
>
```

4. In a browser, go to `https://<Public IP Address>`.  
 The browser will display a certificate error message, because the default FortiAuthenticator certificate is self-signed and not recognized by browsers.  
 You can proceed past this message.

5. Log in with *admin* as the username and the *OCID* as the password.



6. Go to *System > Administration > Licensing*.
7. Click *Browse*, and select your purchased FortiAuthenticator-VM license file.



8. Click *OK*.  
The FortiAuthenticator-VM instance is ready to use after the automatic reboot.



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

Copyright© 2021 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 General Counsel, 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.