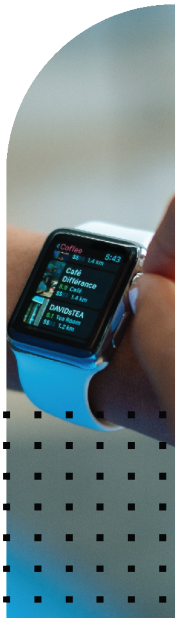
AWS Deployment Guide

FortiVoice 5.3



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/training-certification

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

January 6, 2022
FortiVoice 5.3 AWS Deployment Guide
26-530-588144-20220106

TABLE OF CONTENTS

Change log

Date	Change description
2019-10-25	Initial release.
2021-04-30	Minor formatting changes for the migration of this document to a new location on the Fortinet Documentation Library.
2022-01-06	Updated AWS instance type support on page 5.

Introduction

The FortiVoice Enterprise phone system enables you to completely control your organization's telephone communications. Easy to use and reliable, the FortiVoice Enterprise phone system delivers everything you need to handle calls professionally, control communication costs, and stay connected everywhere.

The FortiVoice Enterprise phone system includes all the fundamentals of enterprise-class voice communications, with no additional cards to install. Auto attendants, voice messaging, ring groups, conferencing and much more are built-in. In addition, the FortiVoice personal web portal lets your staff view their call logs, configure and manage their own messaging, and access other features, such as the operator console and the agent console.

This document describes how to deploy FortiVoice-VM on a virtual server instance in the cloud with Amazon Web Services (AWS). Using Amazon Elastic Compute Cloud (EC2) eliminates the need to invest in hardware to deploy FortiVoice-VM and allows you to rapidly control computing resources by adding or scaling server instances.

After launching the FortiVoice-VM instance from the EC2 Management Console, you can connect to the FortiVoice-VM instance, load a valid license, and start managing your FortiVoice-VM instance.

This section includes the following topics:

AWS instance type support

It is recommended to deploy FortiVoice-VM on an AWS instance type with a minimum of 1 vCPU and a memory size of 2 GB or larger. When selecting an instance type for your deployment, consider your use case for FortiVoice and the requirements to support it.

For up-to-date information on each instance type, see Amazon EC2 Instance Types.

For details about FVE-VM features, see the FortiVoice Enterprise Phone Systems Data Sheet.

The following table provides information on general purpose instance types:

FortiVoice VM license	AWS instance type
VM-50	m3.medium, c3.large, c4.large
VM-100	m3.medium, c3.large, c4.large
VM-200	m3.large, c3.xlarge, c4.xlarge
VM-500	m3.xlarge, m4.large
VM-2000	m4.xlarge, c3.2xlarge, c4.2xlarge
VM-5000	m3.2xlarge, m4.2xlarge

Supported operating system

The operating system of FortiVoice-VM in AWS is Linux/Unix.

Licensing

FortiVoice for AWS supports the bring your own license (BYOL) model.

To place an order to purchase a FortiVoice for AWS license, you can contact a local Fortinet partner or send an email to awssales@fortinet.com.

After placing an order, Fortinet sends a license registration code to the email address used in the order form. Use this code to register your Fortinet FortiVoice for AWS product with Fortinet Support (see Installing a valid license on page 13).

Configuring a Virtual Private Cloud

Amazon Virtual Private Cloud (VPC) allows you to define a virtual network into which you deploy your instances. This virtual network closely resembles a traditional network that you would operate in your own data center.

Like a traditional network, your VPC can support multiple subnets that can be configured to have internet access and a VPN connection back to your existing data center, thus extending your physical network into a cloud.

This section describes how to set up a VPC with a single public subnet, attach the VPC to the internet gateway, and then create a routing table and associate the subnet.

Prerequisite

Prior to performing procedures in this section, make sure to sign up for AWS and follow the instructions to create an AWS account.

Creating a VPC and subnet

This section shows you how to create an AWS VPC and a subnet. When applicable, choose settings specific to your own environment.

1. Go to the Amazon VPC Management Console and log in to your AWS account.
2. In the navigation pane, under **Virtual Private Cloud**, click **Your VPCs**.
3. Click **Create VPC**.
4. On the **Create VPC** page, set the following attributes for your VPC:
   a. In the **Name tag** field, enter a name for your VPC.
   b. In the **IPv4 CIDR block** field, specify an IPv4 address range for your VPC.
   c. In the **Tenancy** drop-down list, select **Default**.
5. Click **Create**.
   The VPC is created.
6. Take note of the **Name** and **VPC ID** as they are needed later in the deployment process.
7. Click **Close**.
8. In the navigation pane, under **Virtual Private Cloud**, click **Subnets**.
9. Click **Create subnet**.
10. On the **Create subnet** page, set the following attributes for your subnet:
    a. In the **Name tag** field, enter a name.
    b. In the **VPC** drop-down list, select your VPC.
    c. In the **Availability Zone** drop-down list, select **No preference**.
    d. In the **IPv4 CIDR block** field, specify an IPv4 address range.
11. Click **Create**.
    The subnet is created.
12. Take note of the subnet name and subnet ID.
13. Click **Close**.
14. In the list of subnets, select the newly created subnet.

15. Click **Actions**, and then click **Modify auto-assign IP settings**.
16. Select **Enable auto-assign public IPv4 address**, and then click **Save**.

Attaching the VPC to the internet gateway

This section shows you how to create an internet gateway and attach the VPC to that internet gateway. Note that if you are using the default VPC, the internet gateway should already exist.

1. In the navigation pane of the VPC Dashboard, under **Virtual Private Cloud**, click **Internet Gateways**.
2. Click **Create internet gateway**.
3. In the **Name tag** field, enter a name for the internet gateway, and then click **Create**.
   The internet gateway is created.
4. Click **Close**.
   Note that the State of the internet gateway you created is *detached*.
5. In the list of internet gateways, select the newly created internet gateway.
6. Click **Actions**, and then click **Attach to VPC**.
7. On the **Attach to VPC** page, in the **VPC** drop-down list, select your VPC.
8. Click **Attach**.
   The State of the internet gateway changes to *attached*. Your VPC is attached to the internet gateway.

Adding a route to the route table

This section shows you how to add a route to the route table to allow all outbound traffic from the FortiVoice-VM to use the selected internet gateway.

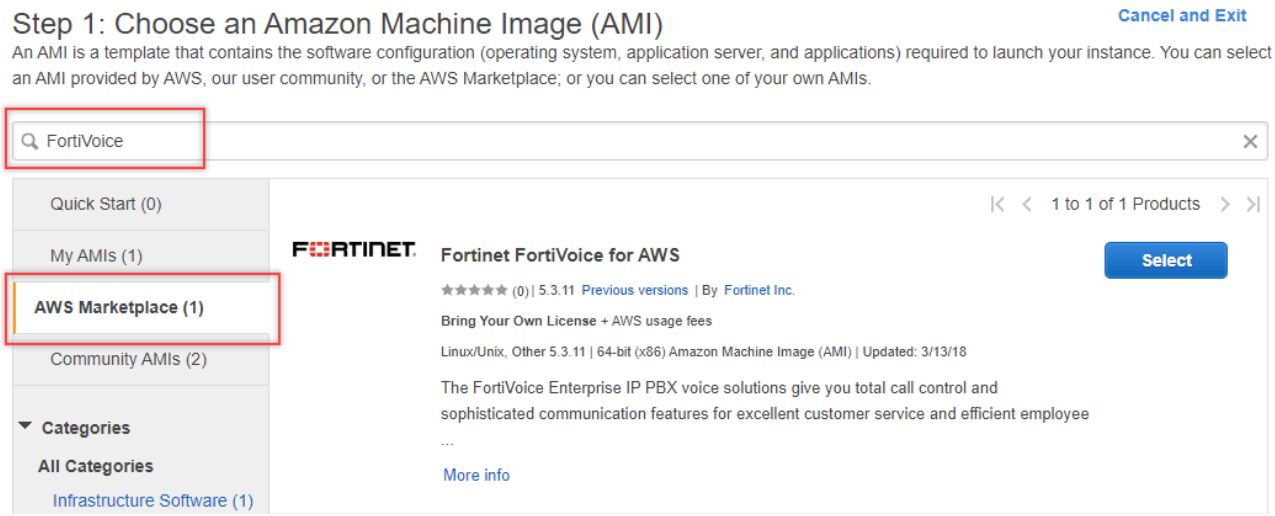
1. In the navigation pane of the VPC Dashboard, under **Virtual Private Cloud**, click **Route Tables**.
2. From the list of route tables, select the route table associated with your VPC ID.
3. Click the **Routes** tab, and then click **Edit routes**.
4. Add another route to allow all outbound traffic to use the selected gateway.
   a. Click **Add route**.
   b. In the **Destination** field, type `0.0.0.0/0`. However, if you want to restrict outgoing traffic to a specific value, then enter the required IP/Mask combination.
   c. Click the **Target** field, click **Internet Gateway**, and then click your gateway to select it for this route.
   d. Click **Save routes**.
   e. Click **Close**.

Launching FortiVoice-VM from EC2 Console

This section describes how to launch a FortiVoice-VM from the EC2 Management Console.

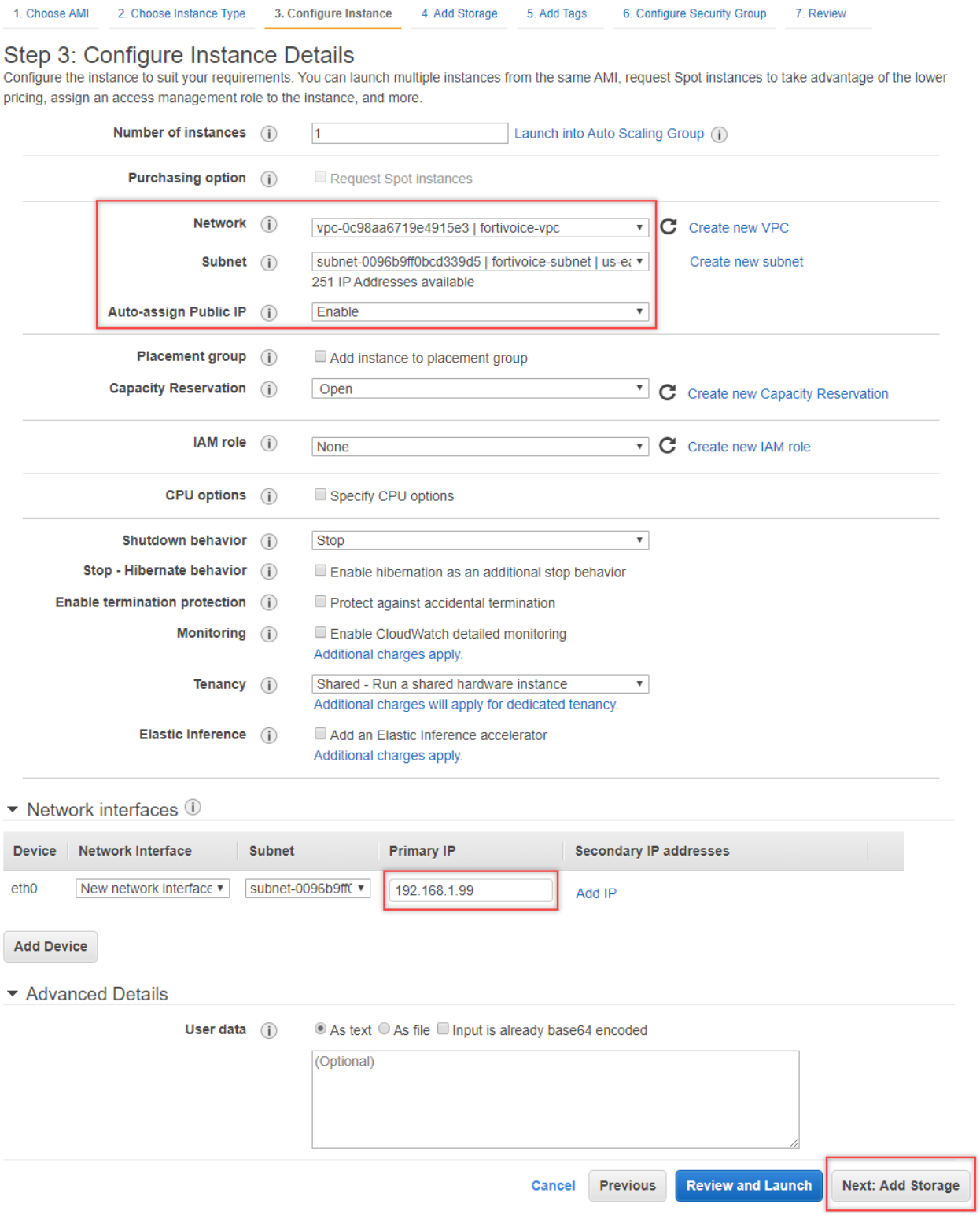
Before proceeding, make sure that you have configured a VPC to use with the FortiVoice-VM. For details, see Configuring a Virtual Private Cloud on page 7.

1. Go to the Amazon EC2 console.
2. From the **EC2 Management Console**, under **Create Instance**, click **Launch Instance**.
3. For **Step 1: Choose an Amazon Machine Image (AMI)**, click **AWS Marketplace**, and in the **Search** field, type `FortiVoice` and press **Enter**.



4. To the right of **Fortinet FortiVoice for AWS**, click **Select**.
5. Review the details of the Fortinet FortiVoice image, and then click **Continue**.
6. For **Step 2: Choose an Instance Type**, select an instance type that is appropriate for your intended usage, and then click **Next: Configure Instance Details**.
7. For **Step 3: Configure Instance Details**, set the attributes for your instance:
   a. In the **Network** drop-down list, select your VPC.
   b. In the **Subnet** drop-down list, select the subnet associated to your VPC.
   c. In the **Auto-assign Public IP** drop-down list, select **Enable**.
8. Under **Network interfaces**, for **Primary IP**, type `192.168.1.99`.

9. Click **Next: Add Storage**.



10. For **Step 4: Add Storage**, add additional storage if needed.
11. Click **Next: Add Tags**.

12. For **Step 5: Add Tags**, provide any tags that will aid you in managing your FortiVoice-VM instance, and then click **Next: Configure Security Group**.
13. For **Step 6: Configure Security Group**, define a set of firewall rules that control the traffic for your instance. Select an existing security group or create a new security group. If you select **Create a new security group**, a security group is generated for you based on recommended settings for the FortiVoice instance.
    a. To access the FortiVoice Web UI, add rule types **HTTP** and **HTTPS** to the security group.
    b. To access the FortiVoice CLI, add rule type **SSH** to the security group.

Type	Protocol	Port Range	Source		Description
Custom TCP F	TCP	69	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
Custom UDP I	UDP	5060	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
HTTP	TCP	80	Custom	0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop
HTTPS	TCP	443	Custom	0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop
SSH	TCP	22	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop

14. Click **Review and Launch**.
15. Review the details you have specified, and then click **Launch**.
    The **Select an existing key pair or create a new key pair** dialog box appears.
16. If you have a key pair, select **Choose an existing key pair** in the drop-down list, and then select the key pair.
17. Alternatively, select **Create a new key pair** and perform the following steps:
    a. In the **Key pair name** field, enter a name for the key pair.

Make sure to store the key pair in a secure and accessible location. You will not be able to download the file again after it's created.

You will need to provide the name of your key pair when you launch an instance and the corresponding private key each time you connect to the instance.

    b. Click **Download Key Pair**.
18. Click **Launch Instances**.
    The Launch Status window appears.
    The instance of FortiVoice deploys on EC2. The process can take several minutes to complete.
19. To view the status of the deployment process from the EC2 console, click **View Instances**.
20. When the deployment process is finished and the FortiVoice-VM is provisioned and powered up, access the FortiVoice-VM to complete the post-deployment setup. See Connecting to the FortiVoice-VM instance on page 12.

Connecting to the FortiVoice-VM instance

1. Go to the EC2 Management Console.
2. In the navigation pane, under **Instances**, click **Instances**.
3. Locate your FortiVoice-VM instance in the list and confirm that the instance is provisioned and powered up.
4. Take note of the public IP address and instance ID of the FortiVoice-VM instance.
5. Go to https://<public_IP_address>/admin.
   Where <public_IP_address> is the public IP address of the FortiVoice-VM instance that you want to connect to.
6. When you connect, your web browser might display a security warning related to the certificate not being trusted. This warning is normal and is due to the certificate being self-signed, rather than being signed by a valid certificate authority. Verify and accept the certificate, either permanently or temporarily, and proceed to https://<public_IP_address>/admin.
7. On the FortiVoice login page, for **Name**, enter **admin**. For **Password**, enter the FortiVoice-VM instance ID.
8. Click **Login**.
   The FortiVoice UI window appears.

Installing a valid license

When first deployed, FortiVoice-VM runs in trial mode until it is licensed. The trial mode supports a maximum of 50 active phones for 45 days.

Registering and downloading your license

After placing an order for a FortiVoice-VM license, a license registration code is sent to the email address used in the order form. Use the license registration code provided to register your FortiVoice-VM with Fortinet Support.

Upon registration, download the license file. You need this file to activate your FortiVoice-VM and configure basic network settings.

1. Go to the Fortinet Support portal and create a new account or log in with an existing account.
2. From the Dashboard, click **Register Now**.
3. In the **Registration Code** field, enter your product serial number, service contract registration code or license certificate number.
4. In **End User Type**, choose the type of user as either government or non-government.
5. To continue the product registration, click **Next**.
6. Provide registration details and click **Next**.
7. Read and accept the terms and conditions of the product registration agreement, and click **Next**.
8. On the **Verification** page, review and accept the product entitlement, and click **Confirm**.
9. On the **Registration Complete** page, download the license file `(.lic)` to your computer. You will upload this license to activate the FortiVoice-VM.

After registering a license, Fortinet servers can take up to 30 minutes to fully recognize the new license. If you get an error that the license is invalid while uploading the license file, wait 30 minutes, and then try again.

Uploading the license file to FortiVoice-VM

1. Connect to the FortiVoice VM instance. For details, see Connecting to the FortiVoice-VM instance on page 12.
2. Navigate to **Status** > **Dashboard**.
3. In the **License Information** widget, click **Update license**.
   The Update license dialog box appears.
4. Click **Browse**, locate the license file `(.lic)` you downloaded earlier from Fortinet, and click **Open**.
5. Click **Upload**.
   A message appears stating your license is being authenticated. The authentication process can take several minutes to complete. After the valid license has been processed, a message appears informing you that your license authenticated successfully.
6. Click **OK**.

www.fortinet.com