FortiAuthenticator - AWS Deployment Guide

Version 6.2.0

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

July 6, 2021
FortiAuthenticator 6.2.0 AWS Deployment Guide
23-620-657460-20210706

TABLE OF CONTENTS

Change log

Date	Change Description
2020-09-16	Initial release.
2021-07-06	Updated: • Configuring a Virtual Private Cloud on page 7 • Launching FortiAuthenticator-VM from AWS Marketplace on page 10 • Launching FortiAuthenticator-VM from EC2 Console on page 12 • Connecting to FortiAuthenticator on page 14 • Installing a valid license on page 16 • Upgrading FortiAuthenticator firmware on page 17

About FortiAuthenticator on AWS

Overview

FortiAuthenticator is designed specifically to provide authentication services for firewalls, SSL and IPsec VPNs, wireless access points, switches, routers, and servers. FortiAuthenticator includes RADIUS and LDAP server authentication methods, and SAML, which is used for exchanging authentication and authorization data between an Identity Provider and a Service Provider. Authentication servers are an important part of an enterprise network, controlling access to protected network assets, and tracking users' activities to comply with security policies.

FortiAuthenticator is not a firewall; it requires a FortiGate appliance to provide firewall-related services. Multiple FortiGate units 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 FSSO Agent on a Windows AD network.

FortiAuthenticator for AWS delivers centralized, secure two-factor authentication for a virtual environment, with a stackable user license for the greatest flexibility. Supporting from 100 to 1 million+ users, FortiAuthenticator for AWS supports the widest range of deployments, from small enterprise right through to the largest service provider.

AWS instance type support

FortiAuthenticator-VM supports the following AWS instance types. Note that supported instance types in the AWS Marketplace listing can change without notice.

- t2.micro, t2.small, t2.medium, t2.large, t2.xlarge, t2.2xlarge
- m3.medium, m3.large, m3.xlarge, m4.large, m4.xlarge, m4.2xlarge
- c3.large, c3.xlarge, c3.2xlarge, c3.4xlarge, c4.large, c4.xlarge, c4.2xlarge

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

Recommended AWS instance types:

FortiAuthenticator-VM License	AWS Instance Type
FAC-VM-100-UG	t2.medium, m3.medium
FAC-VM-1000-UG	t2.large, m3.large, m4.large, c3.large, c4.large
FAC-VM-10000-UG	t2.xlarge, m3.xlarge, m4.xlarge, c3.xlarge, c3.2xlarge, c4.xlarge, c4.2xlarge
FAC-VM-100000-UG	t2.2xlarge, m4.2xlarge, c3.4xlarge

Licensing

FortiAuthenticator for AWS supports the bring your own license (BYOL) model. Licenses can be obtained through any Fortinet partner. If you don't have a partner, contact awssales@fortinet.com for assistance in purchasing a license. 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 AWS

Overview

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

- Configuring a Virtual Private Cloud on page 7
- Deploying FortiAuthenticator-VM to AWS on page 10
- Connecting to FortiAuthenticator on page 14
- Installing a valid license on page 16
- Upgrading FortiAuthenticator firmware on page 17

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'd operate in your own data center.

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

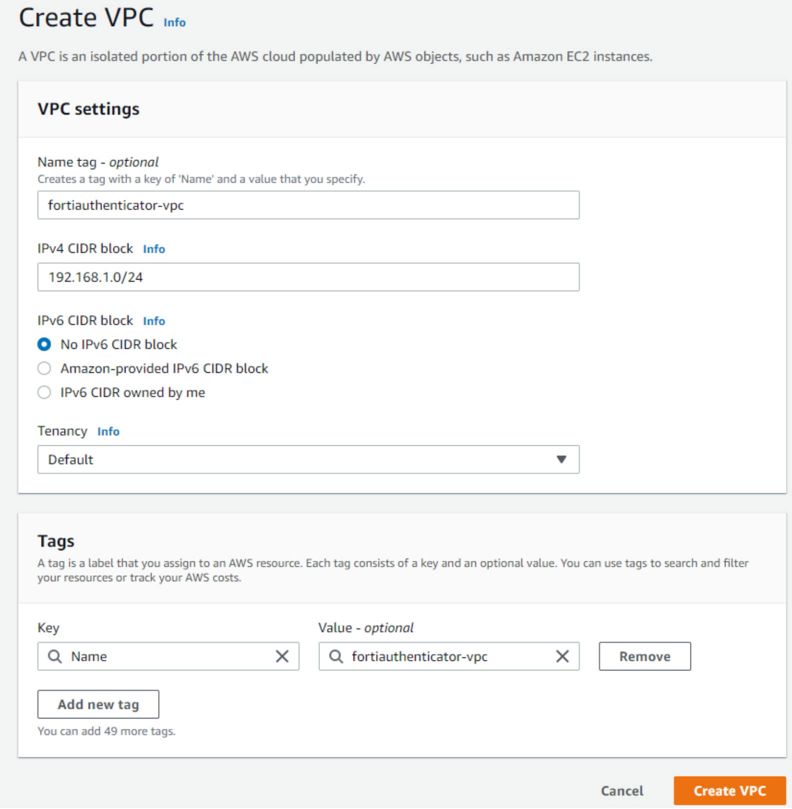
This section describes how to set up a VPC with a single public subnet, attach the VPC to the internet gateway, and then create a routing table and associate the subnet.

Creating a VPC and subnet

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

1. From the **AWS Management Console**, go to **Services > Network & Content Delivery**, click **VPC**.
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. For the **Name tag** field, enter a name for your VPC.
   b. For the **IPv4 CIDR block** field, specify an IPv4 address range for your VPC.

   c. From the **Tenancy** dropdown, select **Default**.



Create VPC Info

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.
fortiauthenticator-vpc

IPv4 CIDR block Info
192.168.1.0/24

IPv6 CIDR block Info
● No IPv6 CIDR block
○ Amazon-provided IPv6 CIDR block
○ IPv6 CIDR owned by me

Tenancy Info
Default

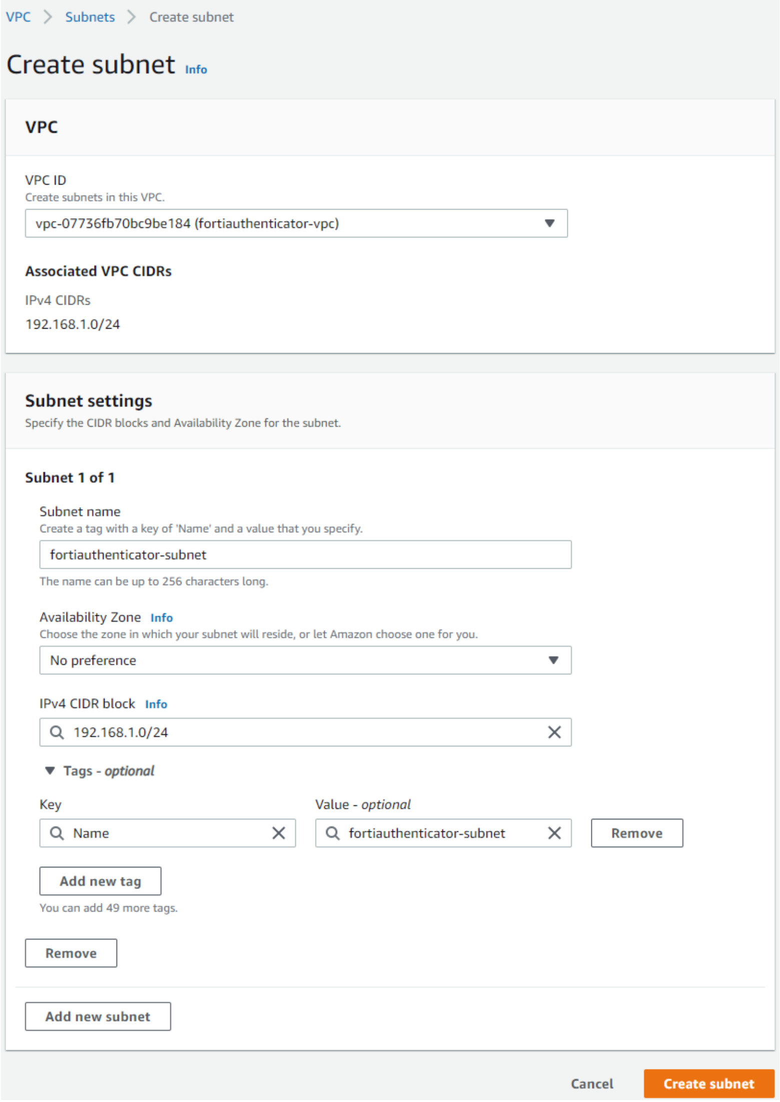
Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*	
Name	fortiauthenticator-vpc	Remove

Add new tag
You can add 49 more tags.

5. Click **Create VPC**.
   The VPC is created. Take note of the Name and VPC ID as they will be needed later in the deployment process.
6. Click **Close**.
7. In the navigation pane, under **Virtual Private Cloud**, click **Subnets**.
8. Click **Create subnet**.
9. In the **Subnets** tab, under **VPC** pane, select a VPC from the **VPC ID** dropdown.
10. Under the **Subnet settings** pane, set the following attributes for your subnet:
    a. For the **Subnet name** field, enter a name.
    b. From the **Availability Zone** dropdown, select **No Preference**.

c. For the **IPv4 CIDR block** field, specify an IPv4 address range.



Create subnet

VPC

VPC ID
Create subnets in this VPC.
vpc-07736fb70bc9be184 (fortiauthenticator-vpc)

Associated VPC CIDRs
IPv4 CIDRs
192.168.1.0/24

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
fortiauthenticator-subnet
The name can be up to 256 characters long.

Availability Zone
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
No preference

IPv4 CIDR block
192.168.1.0/24

Tags - *optional*

Key	Value - *optional*
Name	fortiauthenticator-subnet

You can add 49 more tags.

11. Click **Create subnet**.
    The subnet is created. Take note of the subnet name and subnet ID.
12. Click **Close**.
13. From the list of subnets, select the newly created subnet.
14. Click **Actions**, and then click **Modify auto-assign IP settings**.
15. Select **Enable auto-assign public IPv4 address**, and then click **Save**.

Attaching the VPC to the internet gateway

This section shows you how to connect your VPC to the internet gateway. Note that if you are using the default VPC, the internet gateway should already exist.

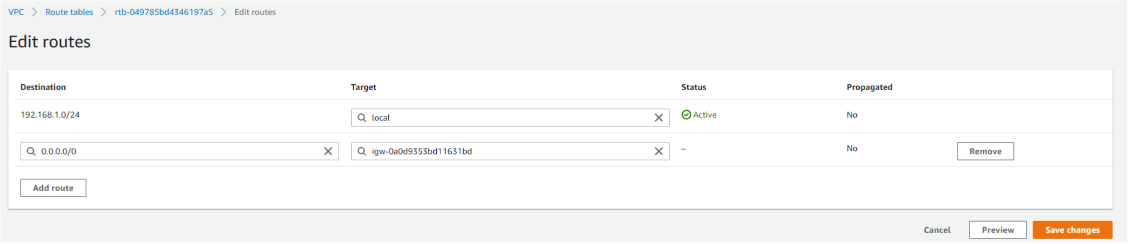
1. In the navigation pane, under **Virtual Private Cloud**, click **Internet Gateways**.
2. Click **Create internet gateway**.
3. In the **Name tag** field, enter a name for the internet gateway, and then click **Create internal gateway**.
   The internet gateway is created.

4. Click **Close**.
   Note that the state of the internet gateway you created is detached.
5. From 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, from the **VPC** dropdown, select your VPC.
8. Click **Attach internal gateway**.
   The state of the internet gateway changes to attached. Your VPC is attached to the internet gateway.

Creating a routing table

This section shows you how to create a route to allow all outbound traffic from the FortiAuthenticator to use the selected internet gateway.

1. In the navigation pane, under **Virtual Private Cloud**, click **Route Tables**.
2. From the list of route tables, select the route table associated with the your VPC.
3. Click the **Routes** tab, and then click **Edit routes**.
   Add another route to allow all outbound traffic to use the selected gateway. You can also enter a particular IP/Mask combination to restrict outgoing traffic to a specific value.
4. Click **Add route**.
5. In the **Destination** field, enter `0.0.0.0/0`.
6. Click the **Target** field, click **Internet Gateway**, and then click your gateway to select it for this route.



VPC > Route tables > rtb-049785bd4346197a5 > Edit routes

Edit routes

Destination	Target	Status	Propagated	
192.168.1.0/24	local	Active	No	
0.0.0.0/0	igw-0a0d9353bd11631bd	-	No	Remove

7. Click **Save changes**.
8. Click **Close**.

Deploying FortiAuthenticator-VM to AWS

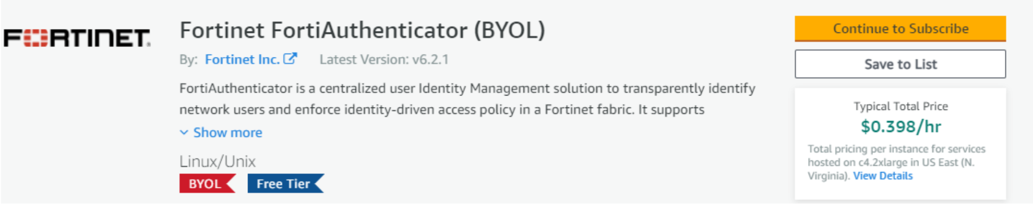
You can deploy the FortiAuthenticator-VM in one of two ways:

- Launching FortiAuthenticator-VM from AWS Marketplace on page 10
- Launching FortiAuthenticator-VM from EC2 Console on page 12

Launching FortiAuthenticator-VM from AWS Marketplace

This section details how to launch FortiAuthenticator from AWS Marketplace. Before proceeding, ensure that you have configured a virtual private cloud (VPC) to use with the FortiAuthenticator-VM.

1. Navigate to the **AWS Marketplace: Fortinet FortiAuthenticator (BYOL)** page.



Fortinet FortiAuthenticator (BYOL)

By: Fortinet Inc. Latest Version: v6.2.1

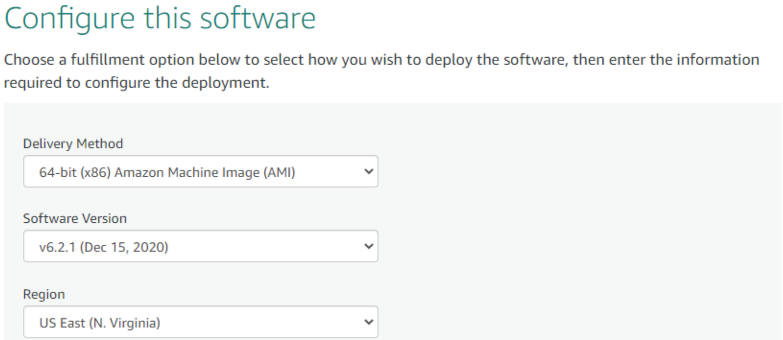
FortiAuthenticator is a centralized user Identity Management solution to transparently identify network users and enforce identity-driven access policy in a Fortinet fabric. It supports

Linux/Unix

Typical Total Price $0.398/hr

Total pricing per instance for services hosted on c4.2xlarge in US East (N. Virginia). View Details

2. Click **Continue to Subscribe**, and then click **Continue to Configuration**.
3. Under **Configure this software**, select a **Delivery Method**, **Software Version**, and **Region**.



Configure this software

Choose a fulfillment option below to select how you wish to deploy the software, then enter the information required to configure the deployment.

Delivery Method: 64-bit (x86) Amazon Machine Image (AMI)

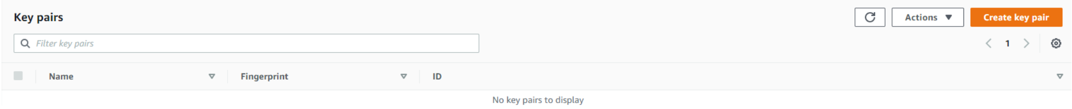
Software Version: v6.2.1 (Dec 15, 2020)

Region: US East (N. Virginia)

4. Click **Continue to Launch**.
5. Under **Launch this software**, configure the following attributes:
   a. From the **Choose Action** dropdown, select **Launch from Website**.
   b. From the **EC2 Instance Type** dropdown, select an instance type that supports your deployment scenario.
   c. From the **VPC Settings** dropdown, select your VPC.
   d. From the **Subnet Settings** dropdown, select the subnet associated to your VPC.
   e. For **Security Group Settings**, click **Create New Based On Seller Settings**. Provide a name and description for your security group and then click **Save**.
   f. For **Key Pair Settings**, select an existing key pair from the dropdown list or create a key pair. See To create a key pair.
6. Click **Launch**.

To create a key pair:

1. Under **Launch this software** from step 5, go to the **Key Pair Settings** pane, and select **Create a key pair in EC2**.
   The **Key pairs** tab opens.



Key pairs

Name	Fingerprint	ID

No key pairs to display

2. In the **Key pairs** tab, select **Create key pair**.
3. In the **Create key pair** tab:
   a. Enter a name for this key pair.
   b. Select either the **pem** or **ppk** file format depending on whether you want to use OpenSSH or PuTTY respectively to connect to the FortiAuthenticator-VM.

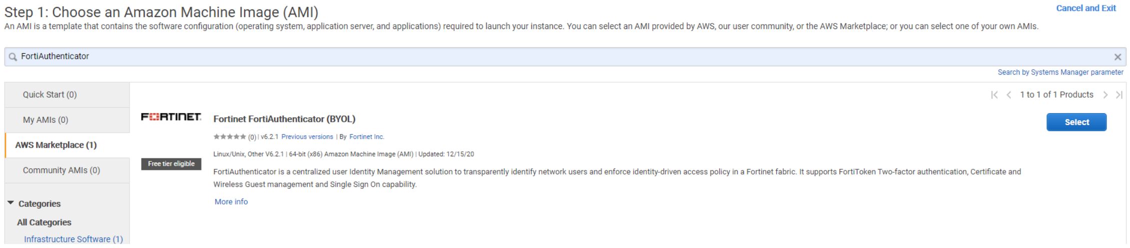
4. Click **Create key pair**.
   The created key pair is downloaded on your computer.

The instance of FortiAuthenticator deploys on EC2. The process can take several minutes to complete. You can view the status of the deployment process from the EC2 console. When the deployment process is finished and the FortiAuthenticator-VM is provisioned and powered up, access the FortiAuthenticator-VM to complete the post-deployment setup. See Connecting to FortiAuthenticator on page 14.

Launching FortiAuthenticator-VM from EC2 Console

This section details how to launch FortiAuthenticator-VM from the EC2 Management Console. Before proceeding, ensure that you have configured a virtual private cloud (VPC) to use with the FortiAuthenticator-VM and that a key pair has been created and can be assigned to your instance. To create and download a key pair, from the **EC2 Management Console**, under **Network & Security**, click **Key Pairs**.

1. From the **AWS Management Console**, go to **Services > EC2**.
2. From the **EC2 Management Console**, under **Launch instance** dropdown, click **Launch instance**.
3. For **Step 1: Choose an Amazon Machine Image (AMI)**, click **AWS Marketplace**, and in the **Search** field, type `FortiAuthenticator` and press Enter.
4. To the right of **Fortinet FortiAuthenticator (BYOL)**, click **Select**.



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

FortiAuthenticator

Fortinet FortiAuthenticator (BYOL)

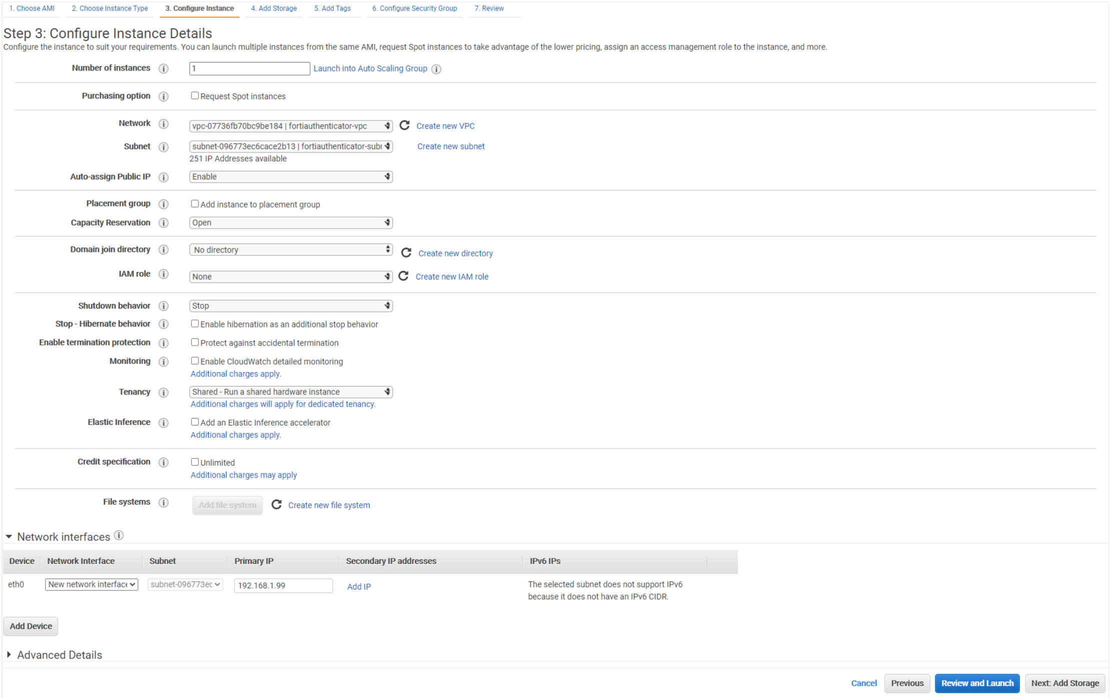
★★★★★ (0) | v6.2.1 Previous versions | By Fortinet Inc.

Linux/Unix, Other V6.2.1 | 64-bit (x86) Amazon Machine Image (AMI) | Updated: 12/15/20

FortiAuthenticator is a centralized user Identity Management solution to transparently identify network users and enforce identity-driven access policy in a Fortinet fabric. It supports FortiToken Two-factor authentication, Certificate and Wireless Guest management and Single Sign On capability.

5. Review the details of the Fortinet FortiAuthenticator image, and then click **Continue**.
6. For **Step 2: Choose an Instance Type**, select an instance type 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. From the **Network** dropdown, select your VPC.
   b. From the **Subnet** dropdown, select the subnet associated to your VPC.
   c. From the **Auto-assign Public IP** dropdown, select **Enable**.

8. Under **Network interfaces**, for **Primary IP**, enter `192.168.1.99`.



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances	1 Launch into Auto Scaling Group
Purchasing option	□ Request Spot instances
Network	vpc-07736fb70bc9be184 | fortiauthenticator-vpc Create new VPC
Subnet	subnet-096773ec6cace2b13 | fortiauthenticator-subr Create new subnet 251 IP Addresses available
Auto-assign Public IP	Enable
Placement group	□ Add instance to placement group
Capacity Reservation	Open
Domain join directory	No directory Create new directory
IAM role	None Create new IAM role
Shutdown behavior	Stop
Stop - Hibernate behavior	□ Enable hibernation as an additional stop behavior
Enable termination protection	□ Protect against accidental termination
Monitoring	□ Enable CloudWatch detailed monitoring Additional charges apply.
Tenancy	Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.
Elastic Inference	□ Add an Elastic Inference accelerator Additional charges apply.
Credit specification	□ Unlimited Additional charges may apply
File systems	Add file system Create new file system

Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interfac	subnet-096773ec	192.168.1.99	Add IP	The selected subnet does not support IPv6 because it does not have an IPv6 CIDR.

9. Click **Next: Add Storage**.
10. For **Step 4: Add Storage**, ensure that the size of the second volume is at least 8 GB, and then click **Next: Add Tags**.
11. For **Step 5: Add Tags**, provide any tags that will aid you in managing your FortiAuthenticator VM instance, and then click **Next: Configure Security Group**.
12. For **Step 6: Configure Security Group**, you 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 **Create a new security group** is selected, a security group is generated for you based on recommended settings for the FortiAuthenticator instance.
13. Click **Review and Launch**.
14. 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.
15. From the dropdown, select **Choose an existing key pair**.
16. From the **Select a key pair** dropdown, select a key pair.
    Before proceeding, confirm that you have the private key file for the selected key pair. The private key file can be obtained when a new key pair is created. To create and a key pair, from the **EC2 Management Console**, under **Network & Security**, click **Key Pairs**.
17. Select **I acknowledge that I have access to the selected private key file**.
18. Click **Launch Instances**.

The instance of FortiAuthenticator deploys on EC2. The process can take several minutes to complete. You can view the status of the deployment process from the EC2 console. When the deployment process is finished and the FortiAuthenticator-VM is provisioned and powered up, access the FortiAuthenticator-VM to complete the post-deployment setup. See Connecting to FortiAuthenticator on page 14.

Connecting to FortiAuthenticator

To connect to the FortiAuthenticator-VM instance, you require the instance's elastic IP address, the key pair, and an SSH client.

Reviewing the FortiAuthenticator instance state

After launching the FortiAuthenticator-VM instance from the AWS Marketplace or EC2 Management Console, navigate to the EC2 Management Console and view the list of instances to confirm that the instance is provisioned and powered up. Take note of the instance's public IP address.

Connecting to FortiAuthenticator using SSH and key pair from a Linux environment

1. Using SSH, initiate a connection to the FortiAuthenticator-VM with the following command:

```
ssh -i "<keypair_file_location>" admin@<public_IPv4_Address>
```

Use the following command to set the permissions of your private key file when using an SSH client on a macOS or Linux computer to connect to your Linux instance:

```
chmod 400 my-key-pair.pem
```

This ensures that only you can read the private key file.

If the private key permissions are not set, you cannot connect to your Linux instance using the key pair you have set up. For more information, see Error: Unprotected private key file.

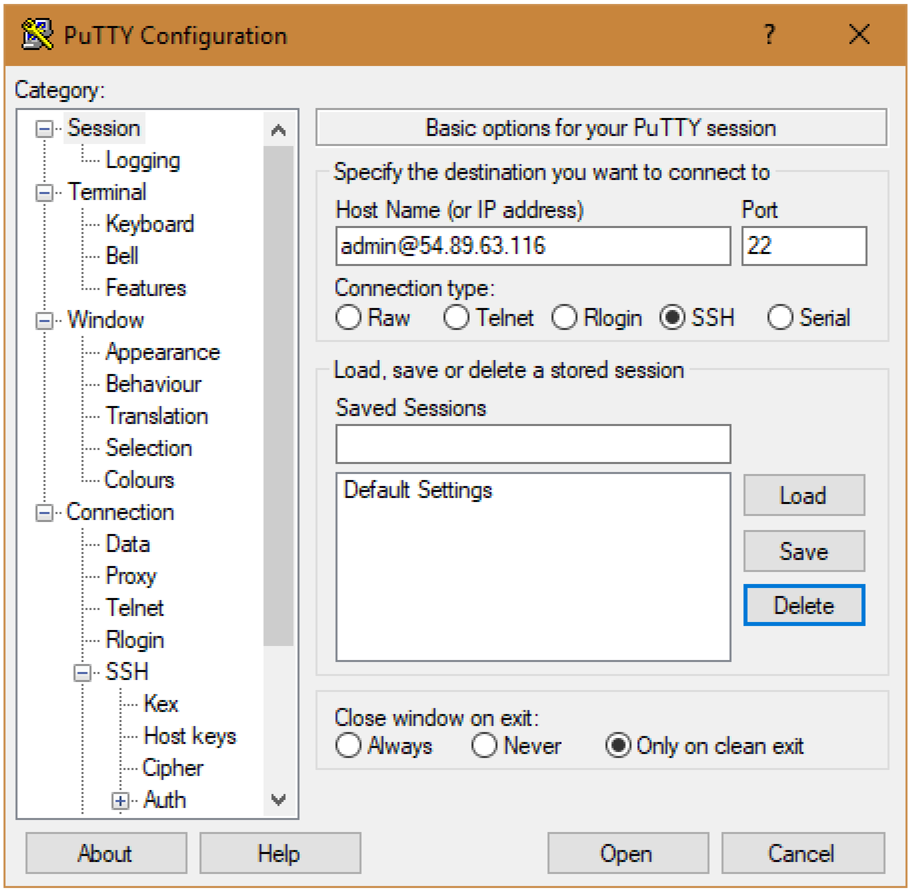
For additional information on connecting to your instance from a Linux environment, see Connecting to Your Linux Instance Using SSH.

Connecting to FortiAuthenticator using SSH and key pair from a Windows environment

This section details how to connect to the FortiAuthenticator-VM using PuTTY, a free SSH client. You can download and install PuTTY from the PuTTY download page. PuTTY does not support the private key format (`.pem`) provided by AWS. Before you can connect to the FortiAuthenticator instance, you must convert your private key to (`.ppk`) format required by PuTTY. For more information, see Convert Your Private Key Using PuTTYgen.

1. Open **PuTTY**.
2. In the **Category** pane, expand **Connection**, expand **SSH**, and then click **Auth**.
3. Click **Browse** , select the `.ppk` file for your key pair, and then click **Open**.
4. In the **Category** pane, click **Session**.
5. For **Host Name (or IP address)**, type `admin@<public_IPv4_Address>`.

6. Ensure **Port** is set to **22**.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): admin@54.89.63.116

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

7. Click **Open**.
8. PuTTY displays a security alert that asks whether you trust the host you are connecting to. Click **Yes**.
   The PuTTY SSH terminal window opens.

For additional information on connecting to your FortiAuthenticator-VM instance from a Windows environment, see Connecting to Your Linux Instance from Windows Using PuTTY.

Change the FortiAuthenticator administrator password

Fortinet recommends changing the default admin password after successfully connecting to the FortiAuthenticator-VM. To change the admin password, execute the following command in the open SSH session:

```
execute restore-admin <new_password>
```

Configure FortiAuthenticator to allow UI access

To enable access to the FortiAuthenticator UI, execute the following commands in the open SSH session:

```
config system global
   set allowed-hosts <public_IPv4_Address>
end
```

Connect to FortiAuthenticator UI

1. In a web browser, navigate to https://<public_IPv4_Address>.
2. 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_IPv4_Address>.
3. On the **Login** page, for **Username**, enter **admin**. For **Password**, enter the administrator password selected when you first connected to the FortiAuthenticator-VM.
4. Click **Login**.

Installing a valid license

FortiAuthenticator-VM runs in evaluation mode until it is licensed. Before using the FortiAuthenticator VM you must enter the license file that you download from the Fortinet Support portal upon registration.

Registering and downloading your license

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

Upon registration, download the license file. You will need this file to activate your FortiAuthenticator-VM. You can configure basic network settings from the CLI to complete the deployment. Once the license file is uploaded, the CLI and UI are fully functional.

1. Go to the **FortiCloud** portal and create a new account or log in with an existing account.
2. In *Asset Management*, select *Register Product*, or click the *Register More* button.
3. Provide your registration code:
   a. Enter your product serial number, service contract registration code, or license certificate number.
   b. Choose your end user type as either a government or non-government user.
   c. Click *Next*.
4. Specify your registration information:
   a. If you have purchased a support contract for your product, enter the support contract.
   b. Enter a description to help identify the product.
   c. Enter the IP address of the FortiAuthenticator VM.
   d. Select a **Fortinet Partner**.
   e. Specify the asset group.
   f. Click **Next**.
   As a part of the license validation process, the IP address of the FortiAuthenticator VM instance is compared to the IP information in the license file. If a new license has been imported or the IP address has been changed, the FortiAuthenticator VM must be rebooted in order for the system to validate the change and operate with a valid license.
5. The **Fortinet Product Registration Agreement** page displays. Select the check box to indicate that you have read, understood, and accepted the service contract. Click **Next**.

6. The **Verification** page displays. Select the checkbox to indicate that you accept the terms. Click **Confirm**. Registration is now complete and your registration summary is displayed.
7. On the **Registration Complete** page, download the license file (`.lic`) to your computer. You will upload this license to activate the FortiAuthenticator VM.

Note: After registering a license, Fortinet servers can take up to 30 minutes to fully recognize the new license. When you upload the license file to activate the FortiAuthenticator VM, if you get an error that the license is invalid, wait 30 minutes and try again.

Upload the license file to FortiAuthenticator-VM

1. Log into the FortiAuthenticator-VM from a browser.
2. Navigate to **System** > **Administration** > **Licensing**.
3. Click **Upload a file** and locate the license file (`.lic`) on your computer. Click **OK** to upload the license file.

The VM registration status appears as valid after the license has been validated.

As a part of the license validation process, the IP address of the FortiAuthenticator-VM instance is compared to the IP information in the license file. If a new license has been imported or the IP address has been changed, the FortiAuthenticator-VM must be rebooted in order for the system to validate the change and operate with a valid license.

Upgrading FortiAuthenticator firmware

The FortiAuthenticator image available on AWS Marketplace might not include the latest firmware available for FortiAuthenticator. Upgrade the firmware of your FortiAuthenticator-VM after deployment to ensure that you have the latest features, functionality, and fixes available.

1. Log into the FortiCloud site and download the latest firmware to your local computer.
2. Log into the FortiAuthenticator-VM from a browser.
3. Navigate to **System** > **Administration** > **Firmware Upgrade**.
4. Click **Upload a file**, locate the firmware image on your local computer, and click **Open**.
5. Click **OK**.

The firmware image uploads from your local computer to the FortiAuthenticator-VM, which will then reboot. For a short period of time during this reboot, the FortiAuthenticator-VM is offline and unavailable for authentication.