Alibaba Cloud Administration Guide

FortiAuthenticator 6.5.0

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/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

February 13, 2023
FortiAuthenticator 6.5.0 Alibaba Cloud Administration Guide
23-650-779559-20230213

TABLE OF CONTENTS

Change log

Date	Change Description
2023-02-13	Initial release.

About FortiAuthenticator on Alibaba Cloud

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 Alibaba Cloud 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 Alibaba Cloud supports the widest range of deployments, from small enterprise right through to the largest service provider.

Instance type support

FortiAuthenticator for Alibaba Cloud can be deployed as VM instances. Supported machine types may change without notice.

Licensing

FortiAuthenticator for Alibaba Cloud supports the bring your own license (BYOL) model. Licenses can be obtained through any Fortinet partner. If you don't have a partner, contact alisales@fortinet.com for assistance in purchasing a license. This license model is stackable, allowing you to expand your VM solution as your environment expands.

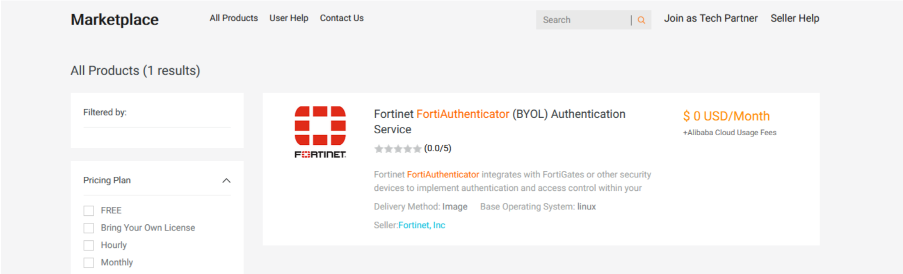
For additional information on the FortiAuthenticator stackable license model, see the FortiAuthenticator datasheet.

Deploying FortiAuthenticator on Alibaba Cloud

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

Deploying FortiAuthenticator from the Alibaba Cloud Marketplace

1. Log in to the Alibaba Cloud Marketplace with your account and search for FortiAuthenticator in your search box.
2. Select the *Fortinet FortiAuthenticator BYOL Authentication Service* option in the results page .



Fortinet FortiAuthenticator (BYOL) Authentication Service

(0.0/5)

$ 0 USD/Month

+Alibaba Cloud Usage Fees

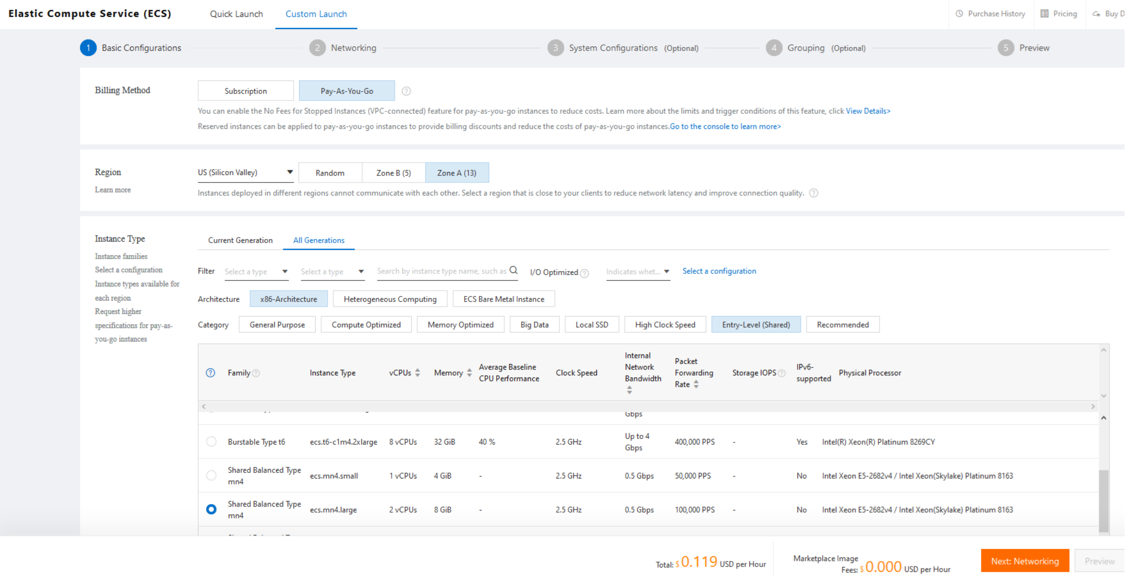
Fortinet FortiAuthenticator integrates with FortiGates or other security devices to implement authentication and access control within your

Delivery Method: Image Base Operating System: linux

Seller:Fortinet, Inc

3. On the FortiAuthenticator *Service* page, click *Choose Your Plan*.
   You will be directed to the *Basic Configurations* page.
4. Configure the following on the *Basic Configurations* page.
   a. In *Billing Method*, select your preferred billing method.
   b. In *Region*, choose the region where you want to deploy your VM.
   c. In *Instance Type*, select *X86-Architecture* as the architecture type, any category that matches your need, and an instance family.
      FortiAuthenticator will not run on under 1GB of RAM, so it at least 2GB of RAM is recommended. (Although FortiAuthenticator will run on 1GB of RAM, it may encounter performance issues when many users are

present).



Billing Method: Subscription | Pay-As-You-Go

You can enable the No Fees for Stopped Instances (VPC-connected) feature for pay-as-you-go instances to reduce costs. Learn more about the limits and trigger conditions of this feature, click View Details>

Reserved instances can be applied to pay-as-you-go instances to provide billing discounts and reduce the costs of pay-as-you-go instances.Go to the console to learn more>

Region: US (Silicon Valley) | Random | Zone B (5) | Zone A (13)

Learn more

Instances deployed in different regions cannot communicate with each other. Select a region that is close to your clients to reduce network latency and improve connection quality.

Instance Type: Current Generation | All Generations

Instance families
Select a configuration
Instance types available for each region
Request higher specifications for pay-as-you-go instances

Filter: Select a type | Select a type | Search by instance type name, such as | I/O Optimized | Indicates whet... | Select a configuration

Architecture: x86-Architecture | Heterogeneous Computing | ECS Bare Metal Instance

Category: General Purpose | Compute Optimized | Memory Optimized | Big Data | Local SSD | High Clock Speed | Entry-Level (Shared) | Recommended

	Family	Instance Type	vCPUs	Memory	Average Baseline CPU Performance	Clock Speed	Internal Network Bandwidth	Packet Forwarding Rate	Storage IOPS	IPv6-supported	Physical Processor
○	Burstable Type t6	ecs.t6-c1m4.2xlarge	8 vCPUs	32 GiB	40 %	2.5 GHz	Up to 4 Gbps	400,000 PPS	-	Yes	Intel(R) Xeon(R) Platinum 8269CY
○	Shared Balanced Type mn4	ecs.mn4.small	1 vCPUs	4 GiB	-	2.5 GHz	0.5 Gbps	50,000 PPS	-	No	Intel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163
●	Shared Balanced Type mn4	ecs.mn4.large	2 vCPUs	8 GiB	-	2.5 GHz	0.5 Gbps	100,000 PPS	-	No	Intel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163

Total: $0.119 USD per Hour

Marketplace Image Fees: $0.000 USD per Hour

d. In *Image*, select *Marketplace Image*.

e. In *Storage*, click *Add Disk* to add a data disk. A disk is required in order for the FortiAuthenticator-VM to boot successfully. The example below includes a 60 GB data disk, but smaller disk sizes are supported.
If you require regular backups of FortiAuthenticator, you can configure the *Snapshots* sections accordingly.

f. Click *Next: Networking*.

5. Configure the following on the *Networking* page:

   a. In *Network Type*, either use an existing VPC or create a new one by clicking on the link for the VPC console.

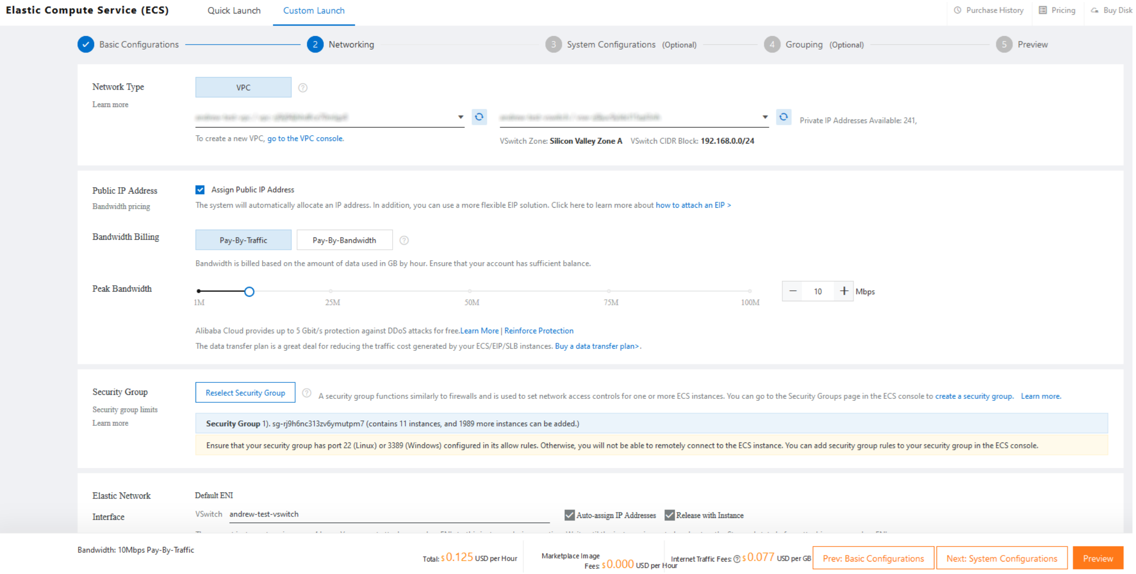
   b. In *Public IP Address*, you **must enable the Public IP Address** field or else FortiAuthenticator will not be reachable from any public network.

   c. In *Bandwidth Billing*, select whether you want to *Pay-By-Traffic* or *Pay-By-Bandwidth*.

   d. In *Security Group*, add security groups to the instance to limit the type of traffic that can access the instance.

   e. All remaining configuration options can be left to the default settings.

   f. Click *Next: System Configurations*.



Network Type: VPC

Learn more

[redacted] | [redacted] | Private IP Addresses Available: 241,

To create a new VPC, go to the VPC console.

VSwitch Zone: **Silicon Valley Zone A** VSwitch CIDR Block: **192.168.0.0/24**

Public IP Address: ☑ Assign Public IP Address

Bandwidth pricing

The system will automatically allocate an IP address. In addition, you can use a more flexible EIP solution. Click here to learn more about how to attach an EIP >

Bandwidth Billing: Pay-By-Traffic | Pay-By-Bandwidth

Bandwidth is billed based on the amount of data used in GB by hour. Ensure that your account has sufficient balance.

Peak Bandwidth: 1M 25M 50M 75M 100M − 10 + Mbps

Alibaba Cloud provides up to 5 Gbit/s protection against DDoS attacks for free.Learn More | Reinforce Protection

The data transfer plan is a great deal for reducing the traffic cost generated by your ECS/EIP/SLB instances. Buy a data transfer plan>.

Security Group: Reselect Security Group

Security group limits
Learn more

A security group functions similarly to firewalls and is used to set network access controls for one or more ECS instances. You can go to the Security Groups page in the ECS console to create a security group. Learn more.

Security Group 1). sg-rj9h6nc313zv6ymutpm7 (contains 11 instances, and 1989 more instances can be added.)

Ensure that your security group has port 22 (Linux) or 3389 (Windows) configured in its allow rules. Otherwise, you will not be able to remotely connect to the ECS instance. You can add security group rules to your security group in the ECS console.

Elastic Network Interface: Default ENI

VSwitch: andrew-test-vswitch ☑ Auto-assign IP Addresses ☑ Release with Instance

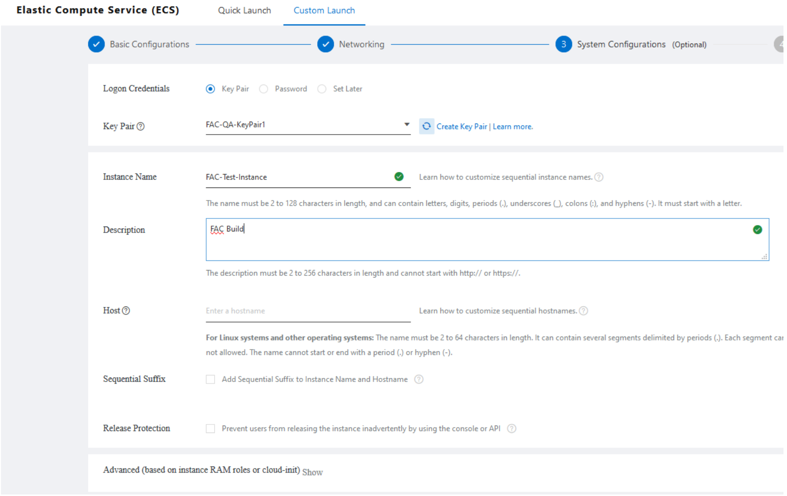
Bandwidth: 10Mbps Pay-By-Traffic

Total: $0.125 USD per Hour

Marketplace Image Fees: $0.000 USD per Hour

Internet Traffic Fees: $0.077 USD per GB

6. On the *System Configurations* page, you can create a key pair to access FortiAuthenticator via VNC (or use an existing key pair), and you can give your instance a custom name and description.



Elastic Compute Service (ECS)   Quick Launch   Custom Launch

✓ Basic Configurations — ✓ Networking — 3 System Configurations (Optional)

Logon Credentials: ● Key Pair ○ Password ○ Set Later

Key Pair: FAC-QA-KeyPair1 — Create Key Pair | Learn more.

Instance Name: FAC-Test-Instance — Learn how to customize sequential instance names.

The name must be 2 to 128 characters in length, and can contain letters, digits, periods (.), underscores (_), colons (:), and hyphens (-). It must start with a letter.

Description: FAC Build

The description must be 2 to 256 characters in length and cannot start with http:// or https://.

Host: Enter a hostname — Learn how to customize sequential hostnames.

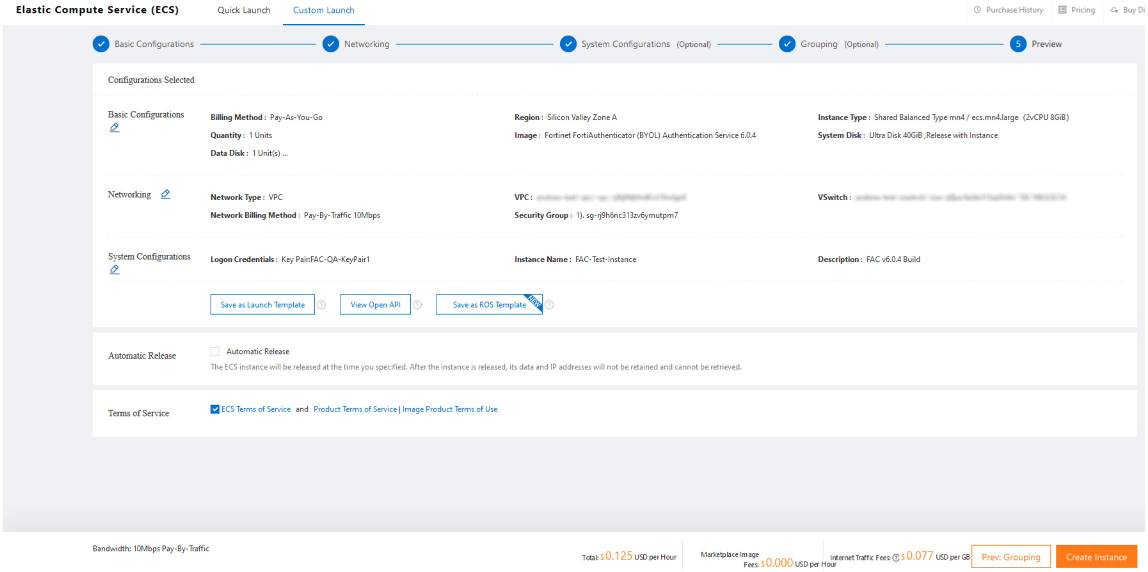
For Linux systems and other operating systems: The name must be 2 to 64 characters in length. It can contain several segments delimited by periods (.). Each segment car not allowed. The name cannot start or end with a period (.) or hyphen (-).

Sequential Suffix: □ Add Sequential Suffix to Instance Name and Hostname

Release Protection: □ Prevent users from releasing the instance inadvertently by using the console or API

Advanced (based on instance RAM roles or cloud-init) Show

7. Click on the *Preview* button to preview the setup and then click on the *Create Instance* button to deploy the instance after accepting the terms of service.



Elastic Compute Service (ECS)   Quick Launch   Custom Launch   Purchase History   Pricing   Buy Di

✓ Basic Configurations — ✓ Networking — ✓ System Configurations (Optional) — ✓ Grouping (Optional) — 5 Preview

Configurations Selected

Basic Configurations

Billing Method: Pay-As-You-Go
Quantity: 1 Units
Data Disk: 1 Unit(s) ...
Region: Silicon Valley Zone A
Image: Fortinet FortiAuthenticator (BYOL) Authentication Service 6.0.4
Instance Type: Shared Balanced Type mn4 / ecs.mn4.large (2vCPU 8GiB)
System Disk: Ultra Disk 40GiB ,Release with Instance

Networking

Network Type: VPC
Network Billing Method: Pay-By-Traffic 10Mbps
VPC: [redacted]
Security Group: 1). sg-rj9h6nc313zv6ymutpm7
VSwitch: [redacted]

System Configurations

Logon Credentials: Key Pair:FAC-QA-KeyPair1
Instance Name: FAC-Test-Instance
Description: FAC v6.0.4 Build

Save as Launch Template   View Open API   Save as ROS Template

Automatic Release: □ Automatic Release
The ECS instance will be released at the time you specified. After the instance is released, its data and IP addresses will not be retained and cannot be retrieved.

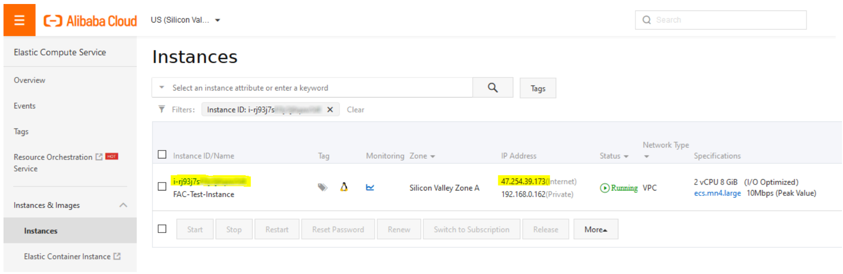
Terms of Service: ☑ ECS Terms of Service and Product Terms of Service | Image Product Terms of Use

Bandwidth: 10Mbps Pay-By-Traffic

Total: $0.125 USD per Hour   Marketplace Image Fees: $0.000 USD per Hour   Internet Traffic Fees: $0.077 USD per GB   Prev: Grouping   Create Instance

Deployment will take approximately 10-15 minutes to complete depending on the number of CPUs and the size of the data disk selected. Once complete, you can access the FortiAuthenticator through its public IP. The default credentials are:

- Username: admin
- Password: *<instance ID>*



Alibaba Cloud   US (Silicon Val...   Search

Elastic Compute Service
Overview
Events
Tags
Resource Orchestration Service
Instances & Images
Instances
Elastic Container Instance

Instances

Select an instance attribute or enter a keyword   Tags

Filters: Instance ID: i-rj93j7s[redacted] ✕ Clear

□	Instance ID/Name	Tag	Monitoring	Zone	IP Address	Status	Network Type	Specifications

□	i-rj93j7s[redacted]
	FAC-Test-Instance
				Silicon Valley Zone A	47.254.39.173(Internet)
					192.168.0.162(Private)
						Running	VPC	2 vCPU 8 GiB (I/O Optimized)
								ecs.mn4.large 10Mbps (Peak Value)

□ Start   Stop   Restart   Reset Password   Renew   Switch to Subscription   Release   More

Connecting to FortiAuthenticator

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

Reviewing the FortiAuthenticator instance state

After launching the FortiAuthenticator-VM instance from the Alibaba Cloud Marketplace, 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_IP>
   ```

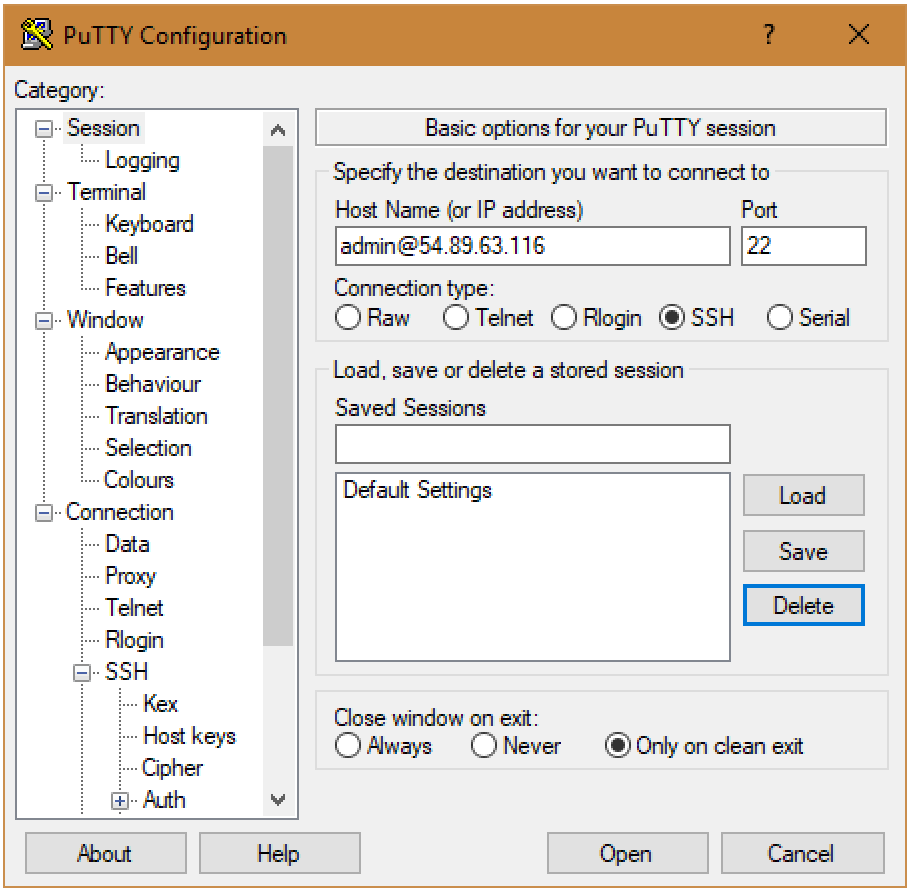
For additional information on connecting to your instance from a Linux environment, see Connecting to Your Linux Instance Using SSH.

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. 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@<ip_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>
```

Connect to FortiAuthenticator UI

1. In a web browser, navigate to https://<AC-FAC-Public_IP>.
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_IP>.
3. On the **Login** page, for **Username**, enter **admin**. For **Password**, enter the Alibaba Cloud instance ID.
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 FortiCloud 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 FortiCloud.

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 **Upload** 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 Alibaba Cloud 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 **FortiCloud** 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 **Upload**.

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.

www.fortinet.com