



FortiAuthenticator - Alibaba Cloud Deployment Guide

Version 6.1.0



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://fortiguard.com/

END USER LICENSE AGREEMENT https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK Email: techdoc@fortinet.com



September 24, 2020 FortiAuthenticator 6.1.0 Alibaba Cloud Deployment Guide 23-610-621024-20200924

TABLE OF CONTENTS

About FortiAuthenticator on Alibaba Cloud	4
Overview	. 4
Instance type support	
Licensing	. 4
Deploying FortiAuthenticator on Alibaba Cloud	
Overview	. 5
Deploying FortiAuthenticator from the Alibaba Cloud Marketplace	. 5
Connecting to FortiAuthenticator	. 8
Reviewing the FortiAuthenticator instance state	8
Connecting to FortiAuthenticator using SSH and key pair from a Linux environment	9
Connecting to FortiAuthenticator using SSH and key pair from a Windows environment	9
Change the FortiAuthenticator administrator password	10
Connect to FortiAuthenticator UI	10
Installing a valid license	10
Registering and downloading your license	10
Upload the license file to FortiAuthenticator-VM	11
Upgrading FortiAuthenticator firmware	11

About FortiAuthenticator on Alibaba Cloud

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 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

Overview

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 on page 5
- Connecting to FortiAuthenticator on page 8
- Installing a valid license on page 10
- Upgrading FortiAuthenticator firmware on page 11

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 .

Marketplace	All Products	User Help Contact Us		Search	Q	Join as Tech Partner	Seller Help
All Products (1 results)							
Filtered by:		FURTIDET	Fortinet FortiAuthenticator (BYC Service ***** (0.0/5)	IL) Authentication		\$ 0 USD/Montl +Alibaba Cloud Usage F	
Pricing Plan	^		Fortinet FortiAuthenticator integrates wit devices to implement authentication and				
FREE			Delivery Method: Image Base Operation	g System: linux			
Bring Your Own License			Seller:Fortinet, Inc				
Monthly							

- **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 ar	e present).	•											
Elastic Compute Service (E	CS) Quick Launch	Custom Launch									③ Purchase History	Pricing	Ga Buy D
1 Basic Configu	rations	2 Networking			3 System Cor	figurations (Optional)	4 0	Grouping	g (Optional)	5 Pre	view	
Billing Method		Pay-As-You-Go							his feature	n, click View Details>			
Region Learn more													
Instance Type Current Generation All Generations Instance Type and Selet a configuration Fair Selet a type Search by instance type name, such at Q VO Optimized Indicates whet. ▼ Selet a configuration Instance Type and Archaecture Selet a type Search by instance type name, such at Q VO Optimized Indicates whet. ▼ Selet a configuration Request higher exchanging Archaecture Meterogeneous Computing (CS Bare Metal Instance exchanging							ecommended						
	🕜 🛛 Family 🔿	Instance Type vCPU	Js 🕆 Memory 🕆	Average Baseline CPU Performance	Clock Speed	Internal Network Bandwidth ‡	Packet Forwarding Rate ≑	Storage IOPS 🕥	IPv6- support	Physical Processor ed			•
	·					Gops							>
	Burstable Typ	e tó ecs.t6-c1m4.2xlarge 8 vCl	PUs 32 GiB	40 %	2.5 GHz	Up to 4 Gbps	400,000 PPS		Yes	Intel(R) Xeon(R) Platinum 8269CY			
	Shared Balan mn4	ced Type ecs.mn4.small 1 vCl	PUs 4 GiB		2.5 GHz	0.5 Gbps	50,000 PPS		No I	Intel Xeon E5-2682v4 / Intel Xeon(Sky	(lake) Platinum 8163		1.1
	O Shared Balan mn4	ced Type ecs.mn4.large 2 vCl	PUs 8 GiB		2.5 GHz	0.5 Gbps	100,000 PPS		No	Intel Xeon E5-2682v4 / Intel Xeon(Sky	(lake) Platinum 8163		4.
		-				Tota	al: \$ 0.119 (JSD per Hour	Marketpl	lace Image Fees: \$ 0.000 USD per Hou	Next: Netv	rorking	Preview

- 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.

astic Compute Service (ECS)	Quick Launch	Custom Launch					🛇 Purchase History 🔳 Pri	cing 💪 Buy Disk
Basic Configurations -		2 Networking		3 System Configurations	(Optional)	4 Grouping (Optional)	5 Preview	
Network Type Learn more	VPC		• 0	VSwitch Zone: Silicon Valley Zone A VSwitch		O Private IP Addresses Available: 241,		
Public IP Address Bandwidth pricing	Assign Public IP A The system will automa		on, you can use a more flexil	ole EIP solution. Click here to learn more about t	ow to attach an EIP >			
Bandwidth Billing	Pay-By-Traffic Bandwidth is billed bas	Pay-By-Bandwidth (ount has sufficient balance.				
Peak Bandwidth		25M 25M : up to 5 Gbit/s protection against DDo s a great deal for reducing the traffic c		25M 1 Reinforce Protection P/SLB instances. Buy a data transfer plan>.	0 100M	- 10 + Mbps		
Security Group Security group limits Learn more		sg-rj9h6nc313zv6ymutpm7 (contains 1	1 instances, and 1989 more i	instances can be added.)		o the Security Groups page in the ECS console to		
Elastic Network Interface	Default ENI VSwitch andrew-test-	vswitch		Auto-assign IP Addresses	Release with Instance			
Bandwidth: 10Mbps Pay-By-Traffi	ic		Total: \$ 0.125 USD pe	r Hour Marketplace Image Fees \$0.000 USD pe	Internet Traffic Fees () \$ 0.07	7 USD per GB Prev: Basic Configurations	Next: System Configurations	Preview

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.

Basic Configurations		3 System Configurations (Optional)
Logon Credentials	Key Pair Password Set Later	
Key Pair 🕲	FAC-QA-KeyPeir1	O Create Key Peir Learn more.
Instance Name	FAC-Test-Instance	Learn how to customize sequential instance names. $$
Description	The name must be 2 to 128 characters in length, and can con	tain letters, digits, periods (), underscores (), colons (), and hyphens (). It must start with a letter.
Host 🗇		Learn how to customize sequential hostnames. ① must be 2 to 64 characters in length. It can contain several segments delimited by periods (), Each segment can
Sequential Suffix	not allowed. The name cannot start or end with a period (.) or Add Sequential Suffix to Instance Name and Hostname	
Release Protection	Prevent users from releasing the instance inadvertently b	y using the console or API ①
Advanced (based on insta	nce RAM roles or cloud-init) $_{\rm Show}$	

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 Compu	ite Service (ECS)	Quick Launch Custom Launch		🕓 Purchase History 🔠 Pricing 🖙 Buy Di
	Basic Configurations	Vetworking	System Configurations (Optional)	– 🕑 Grouping (Optional) — 5 Preview
	Configurations Selected			
	Basic Configurations	Billing Method: Pay-Ac-You-Go Quantify: 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 mod / ecc.mnklarge (2xCPU 8GB) System Disk: Ubra Disk 40GB /helesse with Instance
	Networking 🖉	Network Type : VPC Network Billing Method : Pay-By-Traffic 10Mbps	VPC : Security Group : 1), sg-rj8h6nc313zx6ymutpm7	VSwitch :
	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 T	emplate 🗞 🕐	
	Automatic Release	Automatic Release The ECS instance will be released at the time you specified. After the instance is release	ed, its data and IP addresses will not be retained and cannot be retrieved.	
	Terms of Service	CCS Terms of Service and Product Terms of Service Image Product Terms of Use		
	Bandwidth: 10Mbps Pay-By-Traf	ffic	Total: \$ 0.125 USD per Hour Marketplace Image Free \$	0.000 USD per Hote

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>

i accinera:		
E C-) Alibaba Cloud	US (Silicon Val 👻	Q Search
Elastic Compute Service	Instances	
Overview	 Select an instance attribute or enter a keyword Tags 	
Events	▼ Filters: Instance ID: i-rj93j7s X Clear	
Tags		Network Type
Resource Orchestration 🖸 📧	Instance ID/Name Tag Monitoring Zone - IP Address Status -	✓ Specifications
Instances & Images	Ing23g1s Ing23g1s	g VPC 2 vCPU 8 GiB (I/O Optimized) ecs.mn4.large 10Mbps (Peak Value)
Instances	Start Stop Restart Reset Password Renew Switch to Subscription Release More.	
Elastic Container Instance 🖾		

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 Configurati	on		?	×
Category:				
Session	^	Basic options for your PuTTY se		
		Specify the destination you want to conne Host Name (or IP address)	ct to Port	
···· Keyboard ···· Bell		admin@54.89.63.116	22	
Features		Connection type: ◯ Raw ◯ Telnet ◯ Rlogin ◉ SSH	I O Se	erial
Appearance Behaviour		Load, save or delete a stored session Saved Sessions		
···· Translation ···· Selection				
Colours		Default Settings	Load	ł
Data Proxy			Save	e
Telnet			Delet	e
SSH				
···· Kex ···· Host keys ···· Cipher		Close window on exit: Always Never Only on cl	ean exit	
	~			
About	Help	Open	Canc	el

- 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 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. Navigate to FortiCloud and create a new account or log in with an existing account.
- 2. In the toolbar, click Asset > Register/Renew to start the registration process.
- 3. In the **Specify Registration Code** field, enter your license activation code and click **Next** to continue registering the product.
- **4.** Enter the **Support Contract number**, **Product Description**, **Fortinet Partner**, and **IP address**. 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. Click Next.
- 6. 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.
- 7. The Verification page displays. Select the checkbox to indicate that you accept the terms. Click Confirm.
- 8. 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 Choose 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.

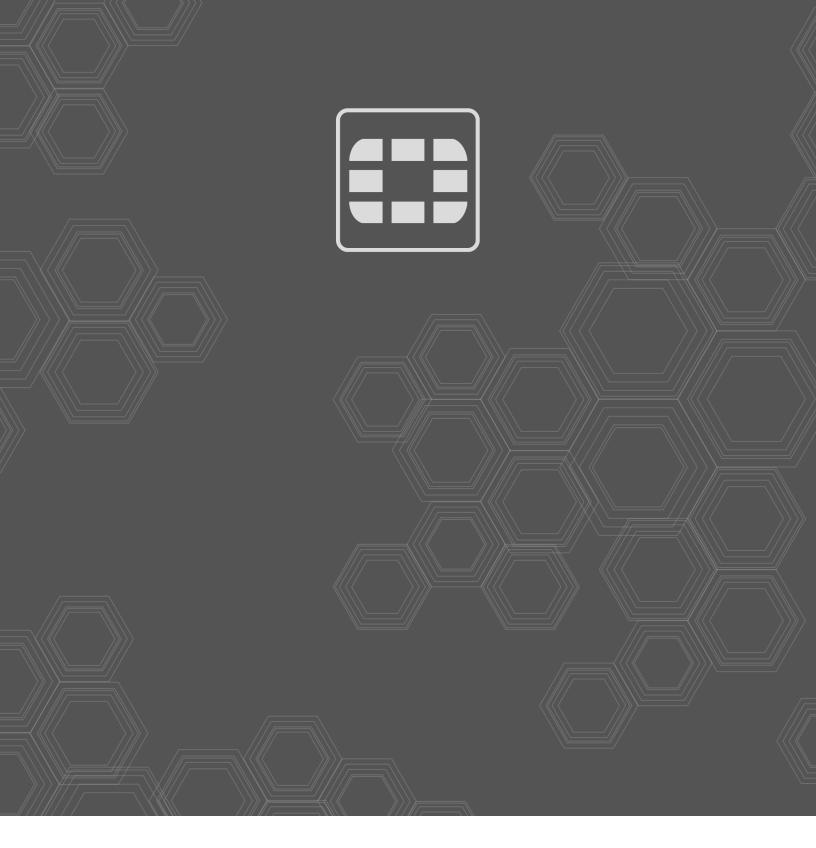
As a part of the license validation process, the IP address of the FortiAuthenticator-VM instance is compared to the IP information in the license file. If a new license has been imported or the IP address has been changed, the FortiAuthenticator-VM must be rebooted in order for the system to validate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

Upgrading FortiAuthenticator firmware

The FortiAuthenticator image available on 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 Choose 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.





Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiGare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.