

Release Notes

Container FortiOS 7.2.2



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<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>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



June 10, 2025

Container FortiOS 7.2.2 Release Notes

87-722-1155912-20250610

TABLE OF CONTENTS

Change Log	4
Introduction	5
New features	5
System requirements	6
Special Notices	7
No GUI for administration	7
Logging to FortiAnalyzer through syslog	7
Resolved Issues	8
Known Issues	9

Change Log

Date	Change Description
2025-06-10	Initial release.

Introduction

Container FortiOS is a cloud-native FortiOS designed for deployment into a containerized environment.

The following features are supported:

- Security features:
 - Application control
 - Antivirus
 - Intrusion prevention
 - Botnet
 - Web filtering
 - IPAM
- Network security features:
 - Firewall/NGFW
 - Segmentation
 - IPsec VPN
- Networking features:
 - Static routing
 - sNAT and Central NAT
 - VIP and DNAT
- Policy and automation engine
- Logging and reporting
- REST API

This document provides information about Container FortiOS version 7.2.2, build 265. It includes the following sections:

- [New features on page 5](#)
- [System requirements on page 6](#)
- [Special Notices on page 7](#)
- [Resolved Issues on page 8](#)
- [Known Issues on page 9](#)

New features

This release contains the following new features and enhancements:

- Support for deployment as IPSEC dialup VPN server.
- Adds `peer` and `peergrp` to IPSEC phase1 interface to support certificate-based authentication.
- Support for FQDN firewall addresses.
- Access proxy VIP supports UDP protocol.
- Antivirus improvements to match FortiOS flow-mode antivirus detection capability.

System requirements

Container FortiOS can be deployed into the following container platforms:

- Linux Containers (LXC)
- Docker
- Kubernetes

CPU	<ul style="list-style-type: none">• x86-64• ARMv7• ARMv8
RAM	400 MB
Disk	100 MB
I/O	Any container hypervisor supported vNIC

Special Notices

- No GUI for administration on page 7
- Logging to FortiAnalyzer through syslog on page 7

No GUI for administration

Container FortiOS does not include a GUI. All administration and configuration must be done through the CLI or REST API.

Logging to FortiAnalyzer through syslog

Container FortiOS can be configured to send logs to FortiAnalyzer through `syslogd`.

To configure logging to FortiAnalyzer:

In the Container FortiOS CLI enter the following command:

```
config log syslogd setting
    set status enable
    set server <FortiAnalyzer IP address>
end
```

Resolved Issues

The following issues have been fixed in 7.2.2. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
963766	HTTP/HTTPS traffic to VIP address cannot pass when service on firewall policy is not ALL.
973816	VIP configured on Container FortiOS will not reach the firewall policy engine and traffic passes through.
1002122	Operation with multiple dataplanes fails (multus).
1026239	When configuration restoration fails, the previous configuration is not kept. Instead the default configuration is loaded.
1027392	Container FortiOS fails to block FortiGuard sample files using deep packet inspection and antivirus.
1029815	Container FortiOS IPSEC does not support deployment as a dial-up server.
1035055	<code>config router static</code> is not accessible in restricted mode.
1047210	In Kubernetes, a deny-all policy can unintentionally block INPUT/OUTPUT traffic due to shared iptables chains with FORWARD.
1057603	Container FortiOS Firewall VIP access-proxy does not allow UDP traffic.
1099796	IPsec VPN does not support certificate based authentication.
1122223	Missing diagnose command to force IPsec VPN re-authentication.
1125786	FortiGuard Operational Technology Security Service does not work correctly in Container FortiOS.

Known Issues

The following issues have been identified in Container FortiOS 7.2.2. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Bug ID	Description
766577	SSL profile in server cert replace mode, address exempt does not work.
766932	NGFW policy mode: application match is failed until <code>ipsmonitor restart</code> .
767061	HTTP POST is not blocked according to webfilter profile config in NGFW policy mode.
803998	HTTP traffic with non-default port is blocked by wildcard policy with <code>enforce-default-app-port</code> enabled.
805909	WebFilter remote URL category match fails.
824457	Replacement message and AV log show file quarantined when quarantine feature is not supported.
843686	IPS and traffic log have <code>srcintf/dstintf</code> exchanged.
846255	<code>set logtraffic all</code> does not log non-security events.
850619	Interface name in packet sniffer output is always <code>wan</code> .
876660	Facebook and Instagram are not blocked when action for <code>Social.Media</code> is set to <code>block</code> in application list.
877408	With <code>other-application-log</code> enabled, sometimes <code>utmaction</code> in traffic log is <code>allow</code> when Twitter is blocked.
925802	Only the first VIP in firewall policy <code>dstaddr</code> works.
939520	With static NAT VIP configured, EICAR in HTTPS download is not blocked by antivirus.
941912	Site to site VPN traffic does not trigger Container FortiOS to bring up the tunnel after manually bringing it down from FortiGate.
947623	Custom application control replacement message group does not take effect.
966694	<code>iptables v1.8.7 (legacy): multiple -p flags not allowed error in Docker container startup log</code> .
977762	Container FortiOS does not learn settings in <code>config system dns</code> .
1013833	In NGFW policy mode, sometimes the URL category rating is not set for traffic which should be blocked by implicit deny policy.
1017298	Add schedule to <code>config firewall policy</code> in NGFW profile mode.
1020326	Adding a new IPsec phase1 interface entry brings established tunnel down and up.
1023047	<code>dia test application restapi 127.0.0.1 443</code> returns <code>ERROR: Error: socket</code>

Bug ID	Description
	hang up.
1025710	Container FortiOS does not translate VIP when utm-status is enabled but without any feature set on firewall policy.
1027058	Status in <code>config system autoupdate schedule</code> is ignored.
1028069	Virtual IPs that use the Container FortiOS <code>eth0</code> interface address as the <code>extip</code> do not work
1046436	Deny rule does not block traffic to VIP.
1113029	NAT is not taking place for ICMP and HTTPS traffic on Container FortiOS running in a Docker environment.
1116880	<code>ipset</code> table is full when configuring multiple large destination subnets in a firewall policy which causes the firewall policy to not work.
1145105	Wrong source IP is used when Container FortiOS sends packets to FortiAnalyzer as syslog server.
1149090	Certificate inspection: No block page after webfilter URL category block for some websites. <code>ERR_SSL_PROTOCOL_ERROR</code> shown instead.
1149174	After YouTube is blocked by <code>appctrl</code> , <code>ERR_SSL_PROTOCOL_ERROR</code> is shown instead of a block page.
1151084	Enabling UTM profiles on a policy sometimes blocks traffic completely.



www.fortinet.com

Copyright© 2025 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 Chief Legal Officer, 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.