# 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

| 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

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** | • x86-64<br>• ARMv7<br>• ARMv8 |
| **RAM** | 400 MB |
| **Disk** | 100 MB |
| **I/O** | Any container hypervisor supported vNIC |

# Special Notices



## 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 inquires 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 | `config router static` 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 `ipsmonitor restart`. |
| 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 `enforce-default-app-port` 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 `srcintf`/`dstintf` exchanged. |
| 846255 | `set logtraffic all` does not log non-security events. |
| 850619 | Interface name in packet sniffer output is always `wan`. |
| 876660 | Facebook and Instagram are not blocked when action for `Social.Media` is set to `block` in application list. |
| 877408 | With `other-application-log` enabled, sometimes `utmaction` in traffic log is `allow` when Twitter is blocked. |
| 925802 | Only the first VIP in firewall policy `dstaddr` 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 | `iptables v1.8.7 (legacy): multiple -p flags not allowed` error in Docker container startup log. |
| 977762 | Container FortiOS does not learn settings in `config system dns`. |
| 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 `config firewall policy` in NGFW profile mode. |
| 1020326 | Adding a new IPsec phase1 interface entry brings established tunnel down and up. |
| 1023047 | `dia test application restapi 127.0.0.1 443` returns `ERROR: Error: socket` |

| 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 `config system autoupdate schedule` is ignored. |
| 1028069 | Virtual IPs that use the Container FortiOS `eth0`interface address as the `extip` 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 | `ipset` 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 FortiOSsends packets to FortiAnalyzer as syslog server. |
| 1149090 | Certificate inspection: No block page after webfilter URL category block for some websites. ERR_SSL_PROTOCOL_ERROR shown instead. |
| 1149174 | After YouTube is blocked by `appctrl`, ERR_SSL_PROTOCOL_ERROR is shown instead of a block page. |
| 1151084 | Enabling UTM profiles on a policy sometimes blocks traffic completely. |

www.fortinet.com