Release Notes

FortiOS 7.2.2

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

October 3, 2022
FortiOS 7.2.2 Release Notes
01-722-839376-20221003

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-10-03	Initial release.

Introduction and supported models

This guide provides release information for FortiOS 7.2.2 build 1255.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.2.2 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-500E, FG-501E, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1500D, FG-1500DT, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-5001E, FG-5001E1
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-60F, FGR-60F-3G4G
FortiGate VM	FG-ARM64-AWS, FG-ARM64-KVM, FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VM64-SVM, FG-VM64-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-XEN

Special notices

IPsec phase 1 interface type cannot be changed after it is configured

The IPsec phase 1 interface type cannot be changed after it is configured. This is due to the tunnel ID parameter (`tun_id`), which is used to match routes to IPsec tunnels to forward traffic. If the IPsec phase 1 interface type needs to be changed, a new interface must be configured.

Support for FortiGates with NP7 processors and hyperscale firewall features

FortiOS 7.2.2 includes main branch support for FortiGates with NP7 processors (FG-1800F, FG-1801F, FG-2600F, FG-2601F, FG-3500F, FG-3501F, FG-4200F, FG-4201F, FG-4400F, and FG-4201F). These FortiGates can also be licensed for hyperscale firewall features.

For more information, refer to the Hyperscale Firewall Release Notes.

Upgrade information

Supported upgrade path information is available on the Fortinet Customer Service & Support site.

To view supported upgrade path information:

1. Go to https://support.fortinet.com.
2. From the *Download* menu, select *Firmware Images*.
3. Check that *Select Product* is *FortiGate*.
4. Click the *Upgrade Path* tab and select the following:
   - *Current Product*
   - *Current FortiOS Version*
   - *Upgrade To FortiOS Version*
5. Click *Go*.

Fortinet Security Fabric upgrade

FortiOS 7.2.2 greatly increases the interoperability between other Fortinet products. This includes:

FortiAnalyzer	• 7.2.0
FortiManager	• 7.2.0
FortiExtender	• 4.0.0 and later. For compatibility with latest features, use latest 7.0 version.
FortiSwitch OS (FortiLink support)	• 6.4.6 build 0470 or later
FortiAP **FortiAP-S** **FortiAP-U** **FortiAP-W2**	• See Strong cryptographic cipher requirements for FortiAP on page 10
FortiClient* EMS	• 7.0.3 build 0229 or later
FortiClient* Microsoft Windows	• 7.0.3 build 0193 or later
FortiClient* Mac OS X	• 7.0.3 build 0131 or later
FortiClient* Linux	• 7.0.3 build 0137 or later
FortiClient* iOS	• 7.0.2 build 0036 or later
FortiClient* Android	• 7.0.2 build 0031 or later
FortiSandbox	• 2.3.3 and later for post-transfer scanning • 4.2.0 and later for post-transfer and inline scanning

* If you are using FortiClient only for IPsec VPN or SSL VPN, FortiClient version 6.0 and later are supported.

When upgrading your Security Fabric, devices that manage other devices should be upgraded first. Upgrade the firmware of each device in the following order. This maintains network connectivity without the need to use manual steps.

1. FortiAnalyzer
2. FortiManager
3. Managed FortiExtender devices
4. FortiGate devices
5. Managed FortiSwitch devices
6. Managed FortiAP devices
7. FortiClient EMS
8. FortiClient
9. FortiSandbox
10. FortiMail
11. FortiWeb
12. FortiADC
13. FortiDDOS
14. FortiWLC
15. FortiNAC
16. FortiVoice
17. FortiDeceptor
18. FortiAI
19. FortiTester
20. FortiMonitor

⚠ If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.2.2. When Security Fabric is enabled in FortiOS 7.2.2, all FortiGate devices must be running FortiOS 7.2.2.

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- admin user account
- session helpers
- system access profiles

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download > Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

Strong cryptographic cipher requirements for FortiAP

FortiOS 7.0.0 has removed 3DES and SHA1 from the list of strong cryptographic ciphers. To satisfy the cipher requirement, current FortiAP models whose names end with letter E or F should be upgraded to the following firmware versions:

- FortiAP (F models): version 6.4.3 and later
- FortiAP-S and FortiAP-W2 (E models): version 6.2.4, 6.4.1, and later
- FortiAP-U (EV and F models): version 6.0.3 and later
- FortiAP-C (FAP-C24JE): version 5.4.3 and later

If FortiGates running FortiOS 7.0.1 need to manage FortiAP models that cannot be upgraded or legacy FortiAP models whose names end with the letters B, C, CR, or D, administrators can allow those FortiAPs' connections with weak cipher encryption by using compatibility mode:

```
config wireless-controller global
    set tunnel-mode compatible
end
```

FortiGate VM VDOM licenses

FortiGate VMs with one VDOM license (S-series, V-series, Flex-VM) have a maximum number or two VDOMs. An administrative type root VDOM and another traffic type VDOM are allowed in 7.2.0. After upgrading to 7.2.0, if the VM previously had split-task VDOMs enabled, two VDOMs are kept (the root VDOM is an administrative type).

Product integration and support

The following table lists FortiOS 7.2.2 product integration and support information:

Web browsers	• Microsoft Edge • Mozilla Firefox version 98 • Google Chrome version 99 Other web browsers may function correctly, but are not supported by Fortinet.
Explicit web proxy browser	• Microsoft Edge 44 • Mozilla Firefox version 74 • Google Chrome version 80 Other web browsers may function correctly, but are not supported by Fortinet.
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
Fortinet Single Sign-On (FSSO)	• 5.0 build 0308 and later (needed for FSSO agent support OU in group filters) • Windows Server 2019 Standard • Windows Server 2019 Datacenter • Windows Server 2019 Core • Windows Server 2016 Datacenter • Windows Server 2016 Standard • Windows Server 2016 Core • Windows Server 2012 Standard • Windows Server 2012 R2 Standard • Windows Server 2012 Core • Windows Server 2008 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 Core (requires Microsoft SHA2 support package) • Novell eDirectory 8.8
AV Engine	• 6.00276
IPS Engine	• 7.00234

Virtualization environments

The following table lists hypervisors and recommended versions.

Hypervisor	Recommended versions
Citrix Hypervisor	• 8.1 Express Edition, Dec 17, 2019
Linux KVM	• Ubuntu 18.0.4 LTS • Red Hat Enterprise Linux release 8.4 • SUSE Linux Enterprise Server 12 SP3 release 12.3
Microsoft Windows Server	• 2012R2 with Hyper-V role
Windows Hyper-V Server	• 2019
Open source XenServer	• Version 3.4.3 • Version 4.1 and later
VMware ESXi	• Versions 6.5, 6.7, and 7.0.

Language support

The following table lists language support information.

Language support

Language	GUI
English	✓
Chinese (Simplified)	✓
Chinese (Traditional)	✓
French	✓
Japanese	✓
Korean	✓
Portuguese (Brazil)	✓
Spanish	✓

SSL VPN support

SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 98 Google Chrome version 99
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 98 Google Chrome version 99
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 98 Google Chrome version 99
macOS Monterey 12.2	Apple Safari version 15 Mozilla Firefox version 98 Google Chrome version 99
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

Resolved issues

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

Common Vulnerabilities and Exposures

Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE references
846234	FortiOS 7.2.2 is no longer vulnerable to the following CVE Reference: • CVE-2022-40684
846854	FortiOS 7.2.2 is no longer vulnerable to the following CVE Reference: • CVE-2022-40684

Known issues

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

Anti Virus

Bug ID	Description
800731	Flow AV sends HTML files to the FortiGate Cloud Sandbox every time when HTML is not configured in file list.
818092	CDR archived files are deleted at random times and not retained.

Application Control

Bug ID	Description
804138	Application icon is missing when FortiGuard anycast is set to AWS (unable to resolve globalproductapi2.fortinet.net).

Firewall

Bug ID	Description
719311	On the *Policy & Objects* > *Firewall Policy* page in 6.4.0 onwards, the IPv4 and IPv6 policy tables are combined but the custom section name (global label) is not automatically checked for duplicates. If there is a duplicate custom section name, the policy list may show empty for that section. This is a display issue only and does not impact policy traffic. **Workaround**: rename the custom section to unique name between IPv4 and IPv6 policies.
770541	There is a delay opening firewall, DoS, and traffic shaping policies in the GUI.
824091	Promethean Screen Share (multicast) is not working on the member interfaces of a software switch.

FortiView

Bug ID	Description
798427	Change the sandbox PDF report query to be on-demand.

GUI

Bug ID	Description
651648	When a large number of addresses is present (~17000), searching for an object takes 20 to 30 seconds to display results on the *Policy & Objects* > *Addresses* page.
677806	On the *Network* > *Interfaces* page when VDOM mode is enabled, the *Global* view incorrectly shows the status of IPsec tunnel interfaces from non-management VDOMs as up. The VDOM view shows the correct status.
685431	On the *Policy & Objects* > *Firewall Policy* page, the policy list can take around 30 seconds or more to load when there is a large number (over 20 thousand) of policies. **Workaround**: use the CLI to configure policies.
749843	*Bandwidth* widget does not display traffic information for VLAN interfaces when a large number of VLAN interfaces are configured.
780832	*WiFi & Switch Controller* > *Managed FortiAPs* list does not load if there is an invalid or unsupported FortiAP configured.
820909	On the *Policy & Objects* > *Schedules* page, when the end date of a one-time schedule is set to the 31st of a month, it gets reset to the 1st of the same month. **Workaround**: use CLI to set schedules with an end date of 31st.
831439	On the *WiFi & Switch Controller* > *SSIDs* page, multiple DHCP servers for the same range can be configured on an interface if the interface name contains a comma (,) character.
831885	Unable to access GUI via HA management interface of secondary unit.

Hyperscale

Bug ID	Description
804742	After changing hyperscale firewall policies, it may take longer than expected for the policy changes to be applied to traffic. The delay occurs because the hyperscale firewall policy engine enhancements added to FortiOS 7.2.1 may cause the FortiGate to take extra time to compile firewall policy changes and generate a new policy set that can be applied to traffic by NP7 processors. The delay is affected by hyperscale policy set complexity, the total number of established sessions to be re-evaluated, and the rate of receiving new sessions.
824733	IPv6 traffic continues to pass through a multi-VDOM setup, even when the static route is deleted.
829549	DSE entry is being created for ALG sessions, and EIF sessions pass through.
839958	`service-negate` does not work as expected in a hyperscale deny policy.
843197	Output of `diagnose sys npu-session list/list-full` does not mention policy route information.
843305	Get `PARSE SKIP ERROR=17 NPD ERR PBR ADDRESS` console error log when system boots up.

Intrusion Prevention

Bug ID	Description
813727	Custom signatures are not shown in the list when filters (server, client, or critical severity) are applied in an IPS sensor.

IPsec VPN

Bug ID	Description
699973	IPsec aggregate shows down status on *Interfaces*, *Firewall Policy*, and *Static Routes* configuration pages.
761754	IPsec aggregate static route is not marked inactive if the IPsec aggregate is down.
815253	NP7 offloaded egress ESP traffic that was not sent out of the FortiGate.

Log & Report

Bug ID	Description
807661	In a FortiAnalyzer with lots of logs, the log view shows *no result* if the user scrolls down to the bottom of the list.
815150	Negating a range or subnet does not work on in the GUI log display.
820940	On the *Log Settings* page, a VDOM administrator can force a FortiCloud log out of for all VDOMs.
821359	FortiGate appears to have a limitation in the syslogd filter configuration.
826483	The `dstname` log field cannot store more than 66 characters.

Proxy

Bug ID	Description
823247	WAD user_info process leaks memory.

Security Fabric

Bug ID	Description
814796	The threat level threshold in the compromised host trigger does not work.

SSL VPN

Bug ID	Description
795381	FortiClient Windows cannot be launched with SSL VPN web portal.
819296	GUI should not use <server_ip> as a sender to send the SSL VPN configuration (it should use value set in `reply-to`).

System

Bug ID	Description
724085	Traffic passing through an EMAC VLAN interface when the parent interface is in another VDOM is blocked if NP7 offloading is enabled. If the `auto-asic-offload` option is disabled in the firewall policy, traffic flows as expected.
725048	Performance improvements for `/api/v2/monitor/system/available-interfaces` (phase 2).
776646	Configuring a delegated interface to obtain the IPv6 prefix from an upstream DHCPv6 server in the GUI fails with a CLI internal error.
798091	After upgrading from 6.4.9 to 7.0.5, the FG-110xE's 1000M SFP interface may fail to auto-negotiate and cannot be up due to the missed auto-negotiation.
798303	The threshold for conserve mode is lowered.
824464	CMDB checksum is not updated when a certificate is renewed over CMP, causing a FortiManager failure to synchronize with the certificate.

Upgrade

Bug ID	Description
803041	Link lights on the FG-1100E fail to come up and are inoperative after upgrading.

VM

Bug ID	Description
667153	Consume the licensed amount of CPUs without running `execute cpu add` and rebooting when a license is upgraded.
825464	Every time the FortiGate reboots, the certificate setting reverts to `self-sign` under `config system ftm-push`.

Web Filter

Bug ID	Description
766126	Block replacement page is not pushed automatically to replace the video content when using a video filter.

WiFi Controller

Bug ID	Description
688655	Adding an AP results in the cluster going out-of-sync due to different UUID values in the WTP profiles.
789072	Kernel panic on FWF-61F due to `ol_target_failure`, `Target Register Dump Location 0x00401AE0`.
807713	FortiGate is not sending RADIUS accounting message consistently to RADIUS server for wireless SSO.
809623	CAPWAP traffic is dropped when `capwap-offloading` is enabled.
811953	Configuration installation from FortiManager breaks the quarantine setting, and the VAP becomes undeletable.
821803	Wireless multicast traffic causes the cw_acd process to have high CPU usage and triggers a hostapd crash.

ZTNA

Bug ID	Description
832508	The EMS tag name (defined in the EMS server's *Zero Trust Tagging Rules*) format changed in 7.2.1 from `FCTEMS<serial_number>_<tag_name>` to `EMS<id>_ZTNA_<tag_name>`. After upgrading from 7.2.0 to 7.2.1, the EMS tag format was converted properly in the CLI configuration, but the WAD daemon is unable to recognize this new format, so the ZTNA traffic will not match any ZTNA policies with EMS tag name checking enabled. **Workaround**: unset the `ztna-ems-tag` in the ZTNA firewall proxy policy, and then set it again.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

Open source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.

FORTINET®

www.fortinet.com