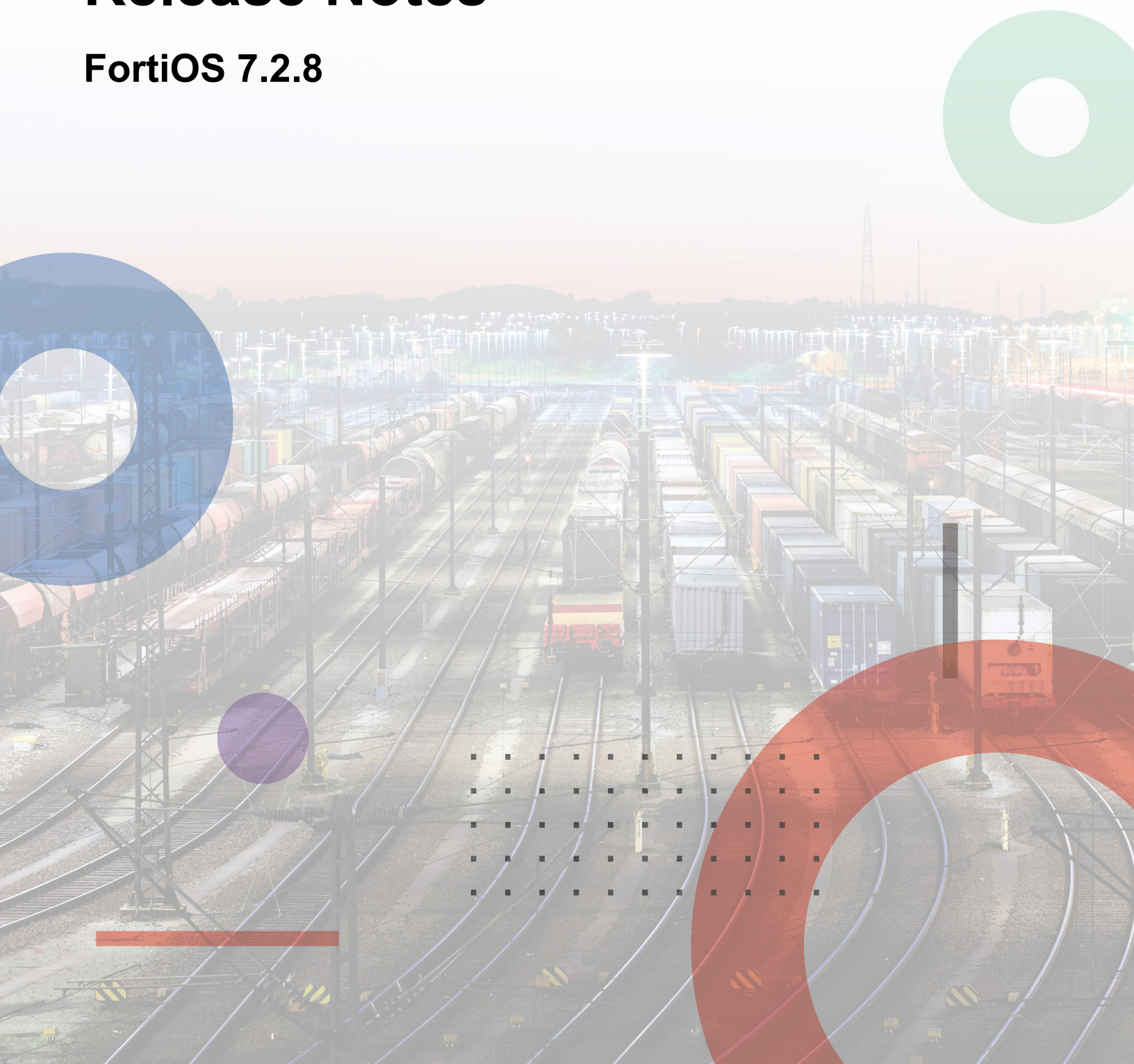
FORTINET

Release Notes

FortiOS 7.2.8



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

March 14, 2024
FortiOS 7.2.8 Release Notes
01-728-1004347-20240314

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-03-14	Initial release.

Introduction and supported models

This guide provides release information for FortiOS 7.2.8 build 1639.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.2.8 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-70F, FG-71F, 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-400F, FG-401F, FG-500E, FG-501E, FG-600E, FG-601E, FG-600F, FG-601F, FG-800D, FG-900D, FG-900G, FG-901G, FG-1000D, FG-1000F, FG-1001F, 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-3000F, FG-3001F, FG-3100D, FG-3200D, FG-3200F, FG-3201F, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3700F, FG-3701F, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-4800F, FG-4801F, FG-5001E, FG-5001E1, FG-6000F, FG-7000E, FG-7000F
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, FGR-70F, FGR-70F-3G4G
FortiFirewall	FFW-1801F, FFW-2600F, FFW-3980E, FFW-4200F, FFW-4400F, FFW-4401F, FFW-4801F, FFW-VM64, FFW-VM64-KVM
FortiGate VM	FG-ARM64-AWS, FG-ARM64-AZURE, FG-ARM64-GCP, FG-ARM64-KVM, FG-ARM64-OCI, 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

FortiGate 6000 and 7000 support

FortiOS 7.2.8 supports the following FG-6000F, FG-7000E, and FG-7000F models:

FG-6000F	FG-6001F, FG-6300F, FG-6301F, FG-6500F, FG-6501F

FG-7000E	FG-7030E, FG-7040E, FG-7060E
FG-7000F	FG-7081F, FG-7121F

Special notices

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

In FortiOS 7.2.0 and later, 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.

IP pools and VIPs are now considered local addresses

In FortiOS 7.2.6 and later, all IP addresses used as IP pools and VIPs are now considered local IP addresses if responding to ARP requests on these external IP addresses is enabled (`set arp-reply enable`, by default). For these cases, the FortiGate is considered a destination for those IP addresses and can receive reply traffic at the application layer.

Previously in FortiOS 7.2.0 to 7.2.5, this was not the case. For details on the history of the behavior changes for IP pools and VIPs, and for issues and their workarounds for the affected FortiOS versions, see Technical Tip: IP pool and virtual IP behavior changes in FortiOS 6.4, 7.0, 7.2, and 7.4.

FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 7.2.8 features.

- FortiGate 6000 incompatibilities and limitations
- FortiGate 7000E incompatibilities and limitations
- FortiGate 7000F incompatibilities and limitations

Hyperscale incompatibilities and limitations

See Hyperscale firewall incompatibilities and limitations in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 7.2.8 features.

Remove support for SHA-1 certificate used for web management interface (GUI)

Starting in FortiOS 7.2.5, users should use the built-in Fortinet_GUI_Server certificate or SHA-256 and higher certificates for the web management interface. For example:

```
config system global
    set admin-server-cert Fortinet_GUI_Server
end
```

SMB drive mapping with ZTNA access proxy

In FortiOS 7.2.5 and later, SMB drive mapping on a Windows PC made through a ZTNA access proxy becomes inaccessible after the PC reboots when access proxy with TCP forwarding is configured as FQDN. When configured with an IP for SMB traffic, same issue is not observed.

One way to solve the issue is to enter the credentials into Windows Credential Manager in the form of `domain\username`.

Another way to solve the issue is to leverage the KDC proxy to issue a TGT (Kerberos) ticket for the remote user. See ZTNA access proxy with KDC to access shared drives for more information. This way, there is no reply in Credential Manager anymore, and the user is authenticated against the DC.

Console error message when FortiGate 40xF boots

In FortiOS 7.2.5 and later, FortiGate 400F and 401F units with BIOS version 06000100 show an error message in the console when booting up.

The message, `Write I2C bus:3 addr:0xe2 reg:0x00 data:0x00 ret:-121.`, is shown in the console, and the FortiGate is unable to get transceiver information.

The issue is fixed in BIOS version 06000101.

FortiGate models with 2 GB RAM cannot be a Security Fabric root

A Security Fabric topology is a tree topology consisting of a FortiGate root device and downstream devices within the mid-tier part of the tree or downstream (leaf) devices at the lowest point of the tree.

As part of improvements to reducing memory usage on FortiGate models with 2 GB RAM, this version of FortiOS no longer allows these models to be the root of the Security Fabric topology or any mid-tier part of the topology. Therefore, FortiGate models with 2 GB RAM can only be a downstream device in a Security Fabric or a standalone device.

The affected models are the FortiGate 40F, 60E, 60F, 80E, and 90E series devices and their variants.

FortiGate models with 2 GB RAM running FortiOS 7.4.2 or later can be used as the Security Fabric root. See FortiGate models with 2 GB RAM can be a Security Fabric root.

To confirm if your FortiGate model has 2 GB RAM, enter `diagnose hardware sysinfo conserve` in the CLI and check that the total RAM value is below 2000 MB (1000 MB = 1 GB).

In the GUI on the *Security Fabric* > *Fabric Connectors* page when editing the *Security Fabric Setup* card, the *Security Fabric role* can only be configured as *Standalone* or *Join Existing Fabric*.

In the CLI, the following error messages are displayed when attempting to configure a FortiGate model with 2 GB RAM as a Security Fabric root:

```
config system csf
    set status enable
end

...

2GB-RAM models cannot be a Security Fabric root.
Please set the upstream.
object set operator error, -39, roll back the setting
Command fail. Return code -39
```

FortiGuard Web Filtering Category v10 update

Fortinet has updated its web filtering categories to v10, which includes two new URL categories for AI chat and cryptocurrency websites. To use the new categories, customers must upgrade their Fortinet products to one of the versions below:

- FortiManager - Fixed in 6.0.12, 6.2.9, 6.4.7, 7.0.2, 7.2.0, 7.4.0.
- FortiOS - Fixed in 7.2.7 and 7.4.1.
- FortiClient - Fixed in Windows 7.2.3, macOS 7.2.3, Linux 7.2.3.
- FortiClient EMS - Fixed in 7.2.1.
- FortiMail - Fixed in 7.0.7, 7.2.5, 7.4.1.
- FortiProxy - Fixed in 7.4.1.

Please read the following CSB for more information to caveats on the usage in FortiManager and FortiOS: https://support.fortinet.com/Information/Bulletin.aspx

FortiAP-W2 models may experience bootup failure during automatic firmware and federated upgrade process if they are powered by a managed FortiSwitch's PoE port

Disable automatic firmware upgrades and the federated upgrade feature if you have FortiAP-W2 devices that are exclusively powered by a PoE port from a FortiGate or FortiSwitch.

The federated upgrade feature starts the upgrades of managed FortiSwitch and FortiAP devices start at approximately the same time. Some FortiAP-W2 devices take a longer time to upgrade than the FortiSwitch devices. When the FortiSwitch finishes upgrading, it reboots, and can disrupt the PoE power to the FortiAP devices. If a FortiAP device is still upgrading when the power is disrupted, it can cause the FortiAP device to experience a bootup failure.

Both automatic firmware upgrade and manually triggering federated upgrade can cause this issue.

For more information about federated upgrade and automatic firmware upgrades, see Upgrading all device firmware by following the upgrade path (federated update) and Enabling automatic firmware updates.

To disable automatic upgrade:

```
config system fortiguard
    set auto-firmware-upgrade disable
end
```

Remote access with write rights through FortiGate Cloud

Remote access with read and write rights through FortiGate Cloud now requires a paid FortiGate Cloud subscription. The FortiGate can still be accessed in a read-only state with the free tier of FortiGate Cloud. Alternatively, you can access your FortiGate through its web interface.

Please contact your Fortinet Sales/Partner for details on purchasing a FortiGate Cloud Service subscription license for your FortiGate device.

For more information see the FortiGate Cloud feature comparison and FortiGate Cloud Administration guide FAQ.

Changes in default behavior

Bug ID	Description
959084	On FortiGate VMs that are using the FortiFlex license, once the expiration date is reached, an automatic three-day grace period offered by FortiGuard will start. Afterwards, the VM license will become expired, and all firewall functions stop working.

Changes in table size

Bug ID	Description
823373	Increase the number of VRFs per VDOM from 64 to 252.

New features or enhancements

More detailed information is available in the New Features Guide.

Feature ID	Description
480717	Add `config system dedicated-mgmt` to all FortiGate models with mgmt, mgmt1, and mgmt2 ports.
685910	Add SoC4 driver support for the IEEE 802.1ad, which is also known as QinQ. When the OID is used up, it is forbidden to create a new QinQ interface.
743804	Add a RADIUS option to allow the FortiGate to set the RADIUS accounting message group delimiter to a comma (,) instead of a plus sign (+) when using RSSO. The default delimiter is still a plus sign.

789237	FortiOS supports customizing the source IP address and the outgoing interface for communication with the upstream FortiGate in the Security Fabric:
	`config system csf`
	`set source-ip <class_ip>`
	`set upstream-interface-select-method {auto | sdwan | specify}`
	`end`

838535	Support matching by destination port when matching a central NAT rule if the protocols are TCP, UDP, or SCTP.
846399	Add 100G speed option for FG-180xF for ports 37, 38, 39, and 40. Upon firmware upgrade, existing port speed configurations are preserved.

883606	FortiOS allows customers to enable or disable the INDEX extension that appends the VDOM or interface index in RFC tables.
	`config system snmp sysinfo`
	`set append-index {enable | disable }`
	`end`

884375	Add support for FAP-234G management.
886560	Support switching to an alternate FortiAnalyzer if the main FortiAnalyzer is unavailable. Once the connectivity is restored, it will automatically fall back to the primary FortiAnalyzer.
886564	This enhancement changes to the Internet Key Exchange (IKE) protocol to bolster the security measures and improve the performance of IPsec VPN. The three key changes include EMS SN Verification, IPsec SAML-based authentication, and IPsec Split DNS.

906370	Support EMS serial number checking per IPsec phase 1 interface.
	`config vpn ipsec phase1-interface`
	`edit <name>`
	`set ems-sn-check {enable | disable}`
	`next`
	`end`

Feature ID	Description
915879	Add two FortiGuard web filter categories: • Artificial intelligence technology (category 100): sites that offer solutions, insights, and resources related to artificial intelligence (AI). • Cryptocurrency (category 101): sites that specialize in digital or virtual currencies that are secured by cryptography and operate on decentralized networks.
930522	Remote access with read and write rights through FortiGate Cloud now requires a paid FortiGate Cloud subscription. The FortiGate can still be accessed in a read-only state with the free tier of FortiGate Cloud. Alternatively, you can access your FortiGate through its web interface. Please contact your Fortinet Sales/Partner for details on purchasing a FortiGate Cloud Service subscription license for your FortiGate device.
931953	FortiOS supports Automatic Firmware Modification Attempt Reporting. This enhancement improves upon the Real-time file system integrity checking feature by implementing an automatic reporting mechanism in the event of an unauthorized firmware modification attempt.
934273	Support the BGP graceful restart helper-only mode. This ensures that during a FortiGate HA failover, the neighboring router that only supports BGP graceful restart helper mode retains its routes.

938066	FortiOS supports customizing retry times and intervals for token activation for FortiFlex/Flex-VM licenses.
	`execute vm-license-options count <integer>`
	`execute vm-license-options interval <integer>`

965990	FortiOS supports up to six NetFlow collectors. This enhancement extends to multi-VDOM environments where a maximum of six NetFlow collectors can be used globally or on a per-VDOMs basis.
976152	FortiOS supports source IP address anchoring in dial-up IPsec tunnels. This allows the gateway to match connections based on the IPv4/IPv6 gateway address parameters, such as the subnet, address range, or country.

977097	Choose whether to discard or permit IPv4 SCTP packets with zero checksum on the NP7 platform:
	`config system npu`
	`  config fp-anomaly`
	`  set sctp-csum-err {allow | drop | trap-to-host}`
	`  next`
	`end`

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

FortiAnalyzer	• 7.2.5
FortiManager	• 7.2.5
FortiExtender	• 7.4.0 and later
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 19
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.

When using FortiClient with FortiAnalyzer, you should upgrade both to their latest versions. The versions between the two products should match. For example, if using FortiAnalyzer 7.2.0, use FortiClient 7.2.0.

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. FortiGate devices
4. Managed FortiExtender devices
5. Managed FortiSwitch devices
6. Managed FortiAP devices
7. FortiClient EMS
8. FortiClient
9. FortiSandbox
10. FortiMail
11. FortiWeb
12. FortiNAC
13. FortiVoice
14. FortiDeceptor
15. FortiAI
16. FortiTester
17. FortiMonitor
18. FortiPolicy

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.2.8. When Security Fabric is enabled in FortiOS 7.2.8, all FortiGate devices must be running FortiOS 7.2.8.

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, go to *Support* > *Firmware Image Checksums* (in the *Downloads* section), enter the image file name including the extension, and click *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 and later 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, FortiFlex) have a maximum number or two VDOMs. An administrative type root VDOM and another traffic type VDOM are allowed in 7.2.0 and later. After upgrading to 7.2.0 and later, if the VM previously had split-task VDOMs enabled, two VDOMs are kept (the root VDOM is an administrative type).

VDOM link and policy configuration is lost after upgrading if VDOM and VDOM link have the same name

Affected versions:

- FortiOS 6.4.9 and later
- FortiOS 7.0.6 and later
- FortiOS 7.2.0 and later

When upgrading to one of the affected versions, there is a check within the set `vdom-links` function that rejects `vdom-links` that have the same name as a VDOM. Without the check, the FortiGate will have a kernel panic upon bootup during the upgrade step.

A workaround is to rename the `vdom-links` prior to upgrading, so that they are different from the VDOMs.

FortiGate 6000 and 7000 upgrade information

Upgrade FortiGate 6000 firmware from the management board GUI or CLI. Upgrade FortiGate 7000 firmware from the primary FIM GUI or CLI. The FortiGate 6000 management board and FPCs or the FortiGate 7000 FIMs and FPMs all run the same firmware image. Upgrading the firmware copies the firmware image to all components, which then install the new firmware and restart. A FortiGate 6000 or 7000 firmware upgrade can take a few minutes, the amount of time depending on the hardware and software configuration and whether DP or NP7 processor software is also upgraded.

On a standalone FortiGate 6000 or 7000, or an HA cluster with `uninterruptible-upgrade` disabled, the firmware upgrade interrupts traffic because all components upgrade in one step. These firmware upgrades should be done during a quiet time because traffic can be interrupted for a few minutes during the upgrade process.

Fortinet recommends running a graceful firmware upgrade of a FortiGate 6000 or 7000 FGCP HA cluster by enabling `uninterruptible-upgrade` and `session-pickup`. A graceful firmware upgrade only causes minimal traffic interruption.

Fortinet recommends that you review the services provided by your FortiGate 6000 or 7000 before a firmware upgrade and then again after the upgrade to make sure that these services continue to operate normally. For example, you might want to verify that you can successfully access an important server used by your organization before the upgrade and make sure that you can still reach the server after the upgrade and performance is comparable. You can also take a snapshot of key performance indicators (for example, number of sessions, CPU usage, and memory usage) before the upgrade and verify that you see comparable performance after the upgrade.

To perform a graceful upgrade of your FortiGate 6000 or 7000 to FortiOS 7.2.8:

1. Use the following command to enable `uninterruptible-upgrade` to support HA graceful upgrade:

   ```
   config system ha
       set uninterruptible-upgrade enable
   end
   ```

2. Download the FortiOS 7.2.8 FG-6000F, FG-7000E, or FG-7000F firmware from https://support.fortinet.com.
3. Perform a normal upgrade of your HA cluster using the downloaded firmware image file.
4. When the upgrade is complete, verify that you have installed the correct firmware version.
   For example, check the FortiGate dashboard or use the `get system status` command.
5. Confirm that all components are synchronized and operating normally.

For example, go to *Monitor* > *Configuration Sync Monitor* to view the status of all components, or use `diagnose sys confsync status` to confirm that all components are synchronized.

IPS-based and voipd-based VoIP profiles

Starting in FortiOS 7.2.5, the new IPS-based VoIP profile allows flow-based SIP to complement SIP ALG while working together. There are now two types of VoIP profiles that can be configured:

```
config voip profile
    edit <name>
        set feature-set {ips | voipd}
    next
end
```

A voipd-based VoIP profile is handled by the voipd daemon using SIP ALG inspection. This is renamed from proxy in previous FortiOS versions.

An ips-based VoIP profile is handled by the IPS daemon using flow-based SIP inspection. This is renamed from flow in previous FortiOS versions.

Both VoIP profile types can be configured at the same time on a firewall policy. For example:

```
config firewall policy
    edit 1
        set voip-profile "voip_sip_alg"
        set ips-voip-filter "voip_sip_ips"
    next
end
```

Where:

- `voip-profile` can select a `voip-profile` with `feature-set voipd`.
- `ips-voip-filter` can select a `voip-profile` with `feature-set ips`.

The VoIP profile selection within a firewall policy is restored to pre-7.0 behavior. The VoIP profile can be selected regardless of the inspection mode used in the firewall policy. The new `ips-voip-filter` setting allows users to select an IPS-based VoIP profile to apply flow-based SIP inspection, which can work concurrently with SIP ALG.

Upon upgrade, the `feature-set` setting of the `voip profile` determines whether the profile applied in the firewall policy is `voip-profile` or `ips-voip-filter`.

Before upgrade	After upgrade

`config voip profile`
`  edit "ips_voip_filter"`
`  set feature-set flow`
`  next`
`  edit "sip_alg_profile"`
`  set feature-set proxy`
`  next`
`end`
	`config voip profile`
	`  edit "ips_voip_filter"`
	`  set feature-set ips`
	`  next`
	`  edit "sip_alg_profile"`
	`  set feature-set voipd`
	`  next`
	`end`
	
	`config firewall policy`

Before upgrade	After upgrade
config firewall policy edit 1 set voip-profile "ips_voip_filter" next edit 2 set voip-profile "sip_alg_profile" next end	edit 1 set ips-voip-filter "ips_voip_filter" next edit 2 set voip-profile "sip_alg_profile" next end

Upgrade error message

The FortiGate console will print a `Fail to append CC_trailer.ncfg_remove_signature:error in stat` error message after upgrading from 7.2.4 to 7.2.5 or later. Affected platforms include: FFW-3980E, FFW-VM64, and FFW-VM64-KVM. A workaround is to run another upgrade to 7.2.5 or later.

Product integration and support

The following table lists FortiOS 7.2.8 product integration and support information:

Web browsers	• Microsoft Edge 114 • Mozilla Firefox version 113 • Google Chrome version 114 Other browser versions have not been tested, but may fully function. Other web browsers may function correctly, but are not supported by Fortinet.
Explicit web proxy browser	• Microsoft Edge 114 • Mozilla Firefox version 113 • Google Chrome version 114 Other browser versions have not been tested, but may fully function. 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 0314 and later (needed for FSSO agent support OU in group filters)
	  • Windows Server 2022 Standard
	  • Windows Server 2022 Datacenter
	  • 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	• 6.00297
IPS Engine	• 7.00336

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, 7.0, and 8.0.

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 113 Google Chrome version 113
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 113 Google Chrome version 113
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 113 Google Chrome version 113
macOS Ventura 13	Apple Safari version 15 Mozilla Firefox version 113 Google Chrome version 113
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 7.2.8. To inquire about a particular bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
879946	An incorrect warning is shown for antivirus flow: *Setting a proxy profile in a flow policy. Proxy features will not work*.
948182	FortiSandbox side panel statistics only shows only statistics for root/management VDOM.
961077	*Advanced Threat Protection Statistics* dashboard is not increasing counters (AV).
993785	When changing the antivirus profile settings, the GUI shows an access denied error message.

Application Control

Bug ID	Description
820481	For firewall policies using proxy-based inspection mode, some HTTP/2 sessions may be incorrectly detected as unknown applications.
952307	FG-400F sees increased packet loss when using an application list in the policy.

Data Loss Prevention

Bug ID	Description
893697	DLP is not blocking VME video files.
914533	The DLP sensor does not block EXE files.
926592	Outlook cannot connect to the Exchange server once the DLP profile protocol is set to MAPI.

DNS Filter

Bug ID	Description
907365	DNS proxy caches DNS responses with only one CNAME record.

Endpoint Control

Bug ID	Description
979811	The ZTNA channel is not cleaned when overwriting old lls entries.

Explicit Proxy

Bug ID	Description
901627	Explicit proxy and SD-WAN fail to match a policy if the destination has multiple zones set.
909328	Forward matching is applied to check the group name for SAML Authentication with Proxy Policy.
926178	Post-upgrade, explicit proxy policies may mismatch when an HTTP CONNECT request or TLS SNI of a HTTPS session partially matches to a policy with deep inspection enabled.
942612	Web proxy forward server does not convert HTTP version to the original version when sending them back to the client.
978473	Explicit proxy policy function issues when matching external-threat feed categories.
980752	Applications on the BOX cannot be started through proxy.
983897	Traffic that should not be matching a policy is incorrectly matching an allow policy or a deny policy.
997787	When accessing multiple destinations, received ERR_TOO_MANY_REDIRECTION error.

Firewall

Bug ID	Description
667201	Moving a policy and then changing the view page will cause a blank grouping label to be displayed.
838535	Support matching by destination port when matching a central NAT rule if the protocols are TCP, UDP, or SCTP.

Bug ID	Description
850175	When the UTM is enabled, NP7 NTurbo is not set properly, which causes the shaper to not guarantee the SIP traffic based on the class ID.
888957	The one-time schedule pre-expiration event log button is always set to disable.
898938	NAT64 does not recover when the interface changes.
907763	The `diffserv-copy` option in the `config firewall policy` command cannot be configured.
921658	SD-WAN IPsec egress traffic shaping is not working when traffic offloading is enabled on an NP7 unit.
925630	Unable to unset `http-supported-max-version` to start using HTTP/2.
950889	Session clashes occur when incoming traffic matches an expected session and undergoes SNAT, but the SNAT port is already occupied by another session.
951373	Traffic shaping does not match the correct queue for outbound traffic when the `class-id` range exceeds the [2, 7] limit, which applies to egress shaping.
952552	When using HTTP1, the TLS handshake from the proxy to the real server does not include the SNI.
953907	Virtual wire pair interface drops all packet if the `prp-port-in`/`prp-port-out` setting is configured under `system npu-setting prp` on FG-101F.
958311	Firewall address list may show incorrect error for an unresolved FQDN address. This is purely a GUI display issue; the FQDN address can be resolved by the FortiGate and traffic can be matched.
963071	Drops in multicast traffic, caused by a change in multicast routing (PIM), may occur at the start of multicast communication after upgrading.
969255	Firewall administrators with read-write access can create new Service entries, but cannot delete them.
970179	Unrelated route changes will cause the existing session to be marked dirty.
972473	WAD crashes when using load balancing with SSL offloading.
973388	TCP state of a session was not updated properly.
976713	A *Hello Retry Request* message is not sent from the FortiGate during an SSL offload by `config firewall ssl-server`.
977641	In transparent mode, multicast packets are not forwarded through the bridge and are dropped.
987397	The GUI does not allow a range member and a subnet member to be in the same source filter of a VIP.

FortiGate 6000 and 7000 platforms

Bug ID	Description
787604	Transceiver information in unavailable for FPM/FIM2 ports in the GUI.

Bug ID	Description
886287	The IPsec ESP error log is generated with the wrong interface.
887946	UTM traffic is blocked by an FGSP configuration with asymmetric routing.
892600	IPv6 static route is removed from the management VDOM.
907695	The FortiGate 6000 and 7000 platforms do not support IPsec VPN over a loopback interface or an NPU inter-VDOM link interface.
910824	On the FortiGate 7000F platform, fragmented IPv6 ICMP traffic is not load balanced correctly when the `dp-icmp-distribution-method` option under `config load-balance` is set to `dst-ip`. This problem may also occur for other `dp-icmp-distribution-method` configurations.
910883	The FortiGate 6000s or 7000s in an FGSP cluster may load balance FTP data sessions to different FPCs or FPMs. This can cause delays while the affected FortiGate 6000 or 7000 re-installs the sessions on the correct FPC or FPM.
933541	IPV4 DNS/ICMP fragment traffic testing issues even when ip-reassembly diabled on the NPU.
937879	FortiGate-7000F chassis with FIM-7941Fs cannot load balance fragmented IPv6 TCP and UDP traffic. Instead, fragmented IPv6 TCP and UDP traffic received by the FIM-7941F interfaces is sent directly to the primary FPM, bypassing the NP7 load balancers. IPv6 ICMP fragmented traffic load balancing works as expected. Load balancing fragmented IPv6 TCP and UDP traffic works as expected in FortiGate-7000F chassis with FIM-7921Fs.
938475	Memory usage issue occurs when multiple threads try to access a VLAN group.
939119	Statistics displayed in the *Session Rate* dashboard widget do not match the statistics displayed from the command line.
939171	The Global Sessions does not match the CLI output.
941944	CPU usage data displayed in the FortiGate 6000 GUI is actually CPU usage data for the management board. CPU usage data displayed in the FortiGate 7000 GUI is actually the CPU usage for the primary FIM.
941971	Dashboard widgets for *CPU*, *Memory*, *Session*, and *Session Rate* show usage as 0% on root and non-root VDOMs.
946943	On 6K and 7K platforms, the management VDOM GUI should not show the *WiFi & Switch Controller* menu.
947570	In an FGCP cluster, the secondary unit cannot reply to the SNMP query while using the management IP.
948750	When EMAC VLAN interfaces are removed spontaneously from the configuration, TCP traffic through their underlying VLAN interface fails.
949175	On the FortiGate 7121F, with FIM2 as the primary FIM, making FIM1 the primary causes NP7 PLE invalidation.
949240	SLBC special ports do not match the local-in policy's management path.

Bug ID	Description
954862	Graceful upgrade from 7.0.12 to 7.2.6 or 7.2.7, or from 7.0.12 to 7.4.2 or 7.4.3 will fail on the FortiGate 6501F/6500F, FortiGate 7060E with slot6 occupied, and FortiGate 7121F with slot12 occupied.
973407	FIM installed NPU session causes the SSE to get stuck.
978241	FortiGate does not honor worker port partition when SNATing connections using a fixed port range IP pool.

FortiView

Bug ID	Description
941524	On the *FortiView Web Sites* page, the *Category* filter does not work in the Japanese GUI.

GUI

Bug ID	Description
848660	Read-only administrator may encounter a *Maximum number of monitored interfaces reached* error when viewing an interface bandwidth widget for an interface that does not have the monitor bandwidth feature enabled.
872063	The VLAN ID cannot be changed in the GUI.
894499	The FortiGate GUI displays only the most recent 100 entries on CRL view.
930960	GUI pages that use the security rating fail to load on an iPhone.
934644	When the FortiGate is in conserve mode, node process (GUI management) may not release memory properly causing entry-level devices to stay in conserve mode.
943949	The GUI does not allow parentheses, (), to be used in the interface description.
945221	The GUI does not show any transceiver information until running `get system interface transceiver` in the CLI.
954356	When connected to the FortiGate GUI on a mobile phone, the table content on some pages like *Network* > *Interfaces*, *Policy & Objects* > *Firewall Policy*, and *WiFi & Switch Controller* > *Managed FortiSwitches* is cut off.
955836	The firewall users widget is missing the *Show all FSSO Logons* button.
961576	GUI issue when moving a policy between groups.
963028	The Forward Traffic page does not show device inventory information.

Bug ID	Description
964386	GUI dashboards show all the IPv6 sessions on every VDOM.
969101	Managed FortiAP-s page is not loading for non super-admin users.
972887	The interface firewall object created automatically is not found by a firewall policy search with IP address.
975403	FortiGate removes the `?` from custom replacement messages.

HA

Bug ID	Description
871636	HA configuration synchronization packets (Ethertype 0x8893) are dropped when going through VXLAN.
904117	When walking through the session list to change the `ha_id`, some dead sessions could be freed one more time.
912665	FGCP primary-secondary cluster only uses one `session-sync-dev`, in spite of having multiple `session-sync-dev`.
916286	The `execute ha failover set <vcluster number>` command only support two vclusters, even when mutiple vclusters exist.
922435	Interfaces for the root VDOM are displayed in the GUI when different VDOM is selected on the HA secondary.
924671	FG-200F in HA's management interface is not responding after a reboot.
925269	Configuration is out-of sync when external feed connectors are applied to a policy.
931965	Do not automatically enable LLDP transmission on an HA management port with LLDP reception enabled.
937246	An error condition occurred while forwarding over a VRRP address, caused by the creation of a new VLAN.
949352	The user.radius checksum is the same in both HA units, but the GUI shows a different checksum on the secondary and the HA status is out of sync.
950868	Traffic is not forwarded on L2 peer to keep FGSP with an available L2 connection.
951292	Newly added webfilter profiles are not visible in the GUI of the secondary HA device.
953167	Access to console and SSH is lost due to a specific configuration.
954098	The `set auto-firmware-upgrade disable` setting is not synchronized between FGCP members.
955555	Unexpected traffic flow occurs after FGSP is enabled between clusters.

Bug ID	Description
962491	Some long lasting TCP established sessions expire on the HA secondary unit earlier than on the primary unit.
962681	In a three member A-P cluster, the dhcp lease list (`execute dhcp lease-list`) might be empty on secondary units.
971075	The last interface belonging to the management VDOM (not root VDOM) is not displayed when accessing `ha-mgmt-interface`.
972163	Under heavy traffic, some sessions are not fully synchronized to the FGCP secondary unit.
972896	No configuration error when restoring a configuration with incorrect `config firewall wildcard-fqdn custom` entries, resulting in an `HA-unsync` status.
974749	TCP/SCTP sessions count mismatch in an HA pair in A-P mode.
985237	Output is missing from the `diagnose sys ha vlan-hb-monitor` command.

Hyperscale

Bug ID	Description
949188	With NAT64 HS policy, ICMP reply packets are dropped by FortiOS.
950582	Traffic not passing across the VDOM link.
958066	Observed TCP sessions timing out with a single hyperscale VDOM configuration after loading image from BIOS.
984852	The HA/AUX ports are not enabled on boot up when using the NPU path option.

Intrusion Prevention

Bug ID	Description
782966	IPS sensor GUI shows *All Attributes* in the filter table when IPS filters with default values are selected in the CLI.
862830	`[?Q?ci_" sekret=]` causes the parser to create a new field, `"sekret=`".
882593	HTTPS traffic slows when IPS with NTurbo is used over a virtual wire pair.
907259	High CPU usage due to the IPS engine, causing high latency on the network.
923393	IPS logs show incorrect source and destination IP addresses and policy IDs, and the ports are zeros.
949662	Interface policy logs show the external facing IP instead of the actual source.

IPsec VPN

Bug ID	Description
564920	IPsec VPN fails to connect if `ftm-push` is configured.
852051	Unexpected condition in IPsec engine on SoC4 platforms leads to intermittent IPsec VPN operation.
897867	IPsec VPN between two FortiGates (100F and 60F) experiences slow throughput compared to the available underlay bandwidth.
898757	Support IKEv2 split DNS mode-cfg (RFC 8598).
898961	`diagnose trafficte st` issues with dynamic IP addresses and loopback interfaces.
914418	File transfer stops after a while when offloading is enabled.
920725	IPsec tunnels that have external DHCP services for IP assignment have an extra selector added after upgrading to 7.0.11.
922064	Firewall becoming unresponsive to DPD/IKE messages, causing IPsec VPNs to drop.
926002	Incorrect traffic order in IPsec aggregate redundant member list after upgrade.
942495	IKEv2 connection issue related to the order of policies using different user groups.
945367	Disabling `src-check` (RPF) on the parent tunnel is not inherited by ADVPN shortcuts.
945873	Inconsistency of `mode-cfg` between phase 1 assigned IP address and destination selector addition.
950012	IPsec tunnels stuck on NP6XLite spoke drop the ESP packet.
950445	After a third-party router failover, traffic traversing the IPsec tunnel is lost.
951765	Shortcut created from parent tunnel interface does not inherit MSS value and may face fragmentation.
954911	IPv6 firewall address IP prefix object is invisible on accessible networks in the GUI.
957412	Authentication fails since the EAP proxy cannot get groups by the hostname of FortiGate in the NAS-ID RADIUS attribute.
960212	IPsec traffic is unidirectional when `vpn-id-ipip` and offloading are enabled, and the tunnel VRF is greater than 63.
961305	FortiGate is sending ESP packets with source MAC address of port1 HA virtual MAC address.
965915	After an HA failover, static gateway IPsec routing fails.
966085	IKEv2 authorization with an invalid certificate can cause tunnel status mismatch.
968218	When the IPsec tunnel destination MAC address is changed, tunnel traffic may stop.
982599	When a NAT port is changed between two static IPsec endpoints, the new port cannot be applied on the tunnel.
996625	Unable to create a FortiClient dial-up VPN with certificate authentication because a peer CA certificate cannot be selected.

Limitations

Bug ID	Description
961992	The buffer and description queue limitation of Marvell switch ports causes a performance limitation.

Log & Report

Bug ID	Description
864111	An internal error occurs on the FortiCloud Report page when a Japanese report name is too long.
903841	When an administrator login fails, the event log shows that the login was successful.
920376	Content disarm and reconstruction (CDR) files are not consistent in the log view.
929269	After disabling an event under the event filter, the system events summary page still shows event logs for that event.
932537	If Security Rating is enabled to run on schedule (every four hours), the FortiGate can unintentionally send local-out traffic to fortianalyzer.forticloud.com during the Security Rating run.
945287	Cloud logging settings are not retained when the FortiGate language setting is Japanese.
950768	When a GUI login fails due to `exceed_limit`, `logged in successfully` appears in the system event log.
952509	The UUID is used instead of the external resource name in the `Threat feed updated` system event log.
954565	Although there is enough disk space for logging, IPS archive full message is shown.
960661	FortiAnalyzer report is not available to view for the secondary unit in the HA cluster.
961244	Icons in logs evaluations and policies are no longer displayed.
965247	FortiGate syslog format in reliable transport mode is not compliant with RFC 6587.
967692	The received traffic counter is not increasing when the traffic is HTTPS with webfilter.
987261	In the webfilter content block UTM log in proxy inspection mode, `sentbyte` and `rcvdbyte` are zero.

Proxy

Bug ID	Description
727629	An error case occurs in WAD while handling the HTTP requests for an explicit proxy policy.

Bug ID	Description
790426	An error case occurs in WAD while redirecting the web filter HTTPS sessions.
806556	Unexpected behavior in WAD when the ALPN is set to `http2` in the `ssl-ssh-profile`.
828917, 919781	Unexpected behavior in WAD when there are multiple LDAP servers configured on the FortiGate.
837095	WAD daemon runs high with many child processes and is not coming down after configuring 250 CGN VDOMs.
845361	A rare error condition occurred in WAD caused by compounded SMB2 requests.
863132	Proxy mode inspection is slow when testing a single TCP stream from fast.com, which causes bandwidth slowness on FG-100F and FG-200F devices.
901296	An error case occurs in WAD while handling the HTTP requests for an explicit proxy policy.
940149	Inadvertent traffic disruption caused by WAD when it receives an HTTP2 data frame payload on a dead stream.
947814	Too many redirects on TWPP after the second KRB keytab is configured.
954104	An error case occurs in WAD when WAD gets the external authenticated users from other daemons.
965966	An error condition occurred in WAD due to heavy HTTP video traffic when using a video filter profile with deep inspection enabled.
915404	Proxyd did not account for all RFC-compliant SMTP pipelining cases.
922286	WAD traffic to globalvideoquery.fortinet.net does not follow the FortiGuard interface-select-mode.
955990	Captive portal reappears repeatedly in the browser after importing user credentials.

REST API

Bug ID	Description
944723	The `/firewall/vip` API does not recognize custom SSL cipher suites.
951384	API responses for PBR provides incorrect value if address groups are used in PBR.
951411	Inconsistent handling of web filter profile actions in API transactions.
964424	REST API GET `/ips/sensor/{name}` adds extra space to `locations`, `severity`, `protocol`, `os`, and `application` field values.

Routing

Bug ID	Description
792512	The dashboard Session widget cannot display the correct IPv6 session count per VDOM.
852498	BGP packets are marked with DSCP CS0 instead of CS6.
888210	The GUI takes three minutes to load 4000 TWAMP health-checks.
890954	The change of an IPv6 route does not mark sessions as dirty nor trigger a route change.
897666	Issue with SD-WAN rule for FortiGuard.
926525	`Routing information changed` log is being generated from secondary in an HA cluster.
928152	FortiGate generates two OSPF stub entries for the same prefix after upgrading from 6.4 to 7.0.
930749	IPv6 traffic was no longer forwarded according to route list and neighbor-cache list after upgrading from 7.2.4 to 7.2.5.
932092	API call returns recursive next-hop for the gateway address.
934273	Support GR helper mode (peer) for BGP.
934803	Synchronized kernel VPNv4 routes are not used in an HA failover.
935370	SD-WAN performance SLA `tcp-connect` probes clash with user sessions.
935886	SD-WAN packet duplication feature in force mode suddenly stops duplicating and starts to duplicate again once the FortiGate is rebooted.
938500	Status of OSPF adjacency is `Loading` on spokes while `Full` on the hub side.
943333	When SD-WAN health-check is configured, the IPv6 interface IP address of shortcut fails to be pinged.
952908	Locally originated type 5 and 7 LSAs' forward address value is incorrect.
954100	Packet loss status in SD-WAN health check occur after an HA failover.
957627	Learned BGP through routes are not withdrawn on the spoke after the EBGP neighborship is down between the hub and third party device.
964182	IPsec traffic with `vpn-id-ipip` is egressing with the wrong VRF when offloading is enabled.
965752	After HA monitored interface fails over, SD-WAN intermittently does not follow `route-map-preferable`.
969671	GRE tunnel is stuck using a non-existing devindex.
974921	Configuring the *Set weight* on the route map to *0* in the GUI does not save this setting in the CLI configuration.
977215	SD-WAN health check with state = dead moves between 100% and 0% packet loss while the state stays the same.
978204	BFD/BGP dropping when outbandwidth is applied.
985539	SD-WAN health check logs are not generated for ADVPN shortcuts.

Bug ID	Description
989840	Issue with PIM neighborship over an IPSec tunnel with NP offload.

Security Fabric

Bug ID	Description
876588	External Connectors can cause a FortiGate internal error when the configuration name has invalid characters.
902344	When there are over 30 downstream FortiGates in the Security Fabric, the root FortiGate's GUI may experience slowness when loading the *Fabric Management* page and prevents the user from upgrading firmware in the GUI.
907819	Advanced GCP connector does not resolve if one element does not exist.
908489	When one of the downstream FortiGate VM's license is invalid, the root FortiGate will be automatically logged out from accessing the *Firmware & Registration* page.
920391	Non-management VDOM is not allowed to set a `source-ip` for `config system external-resource`.
938980	HTTP 400 errors observed using SDN connector to query AKS clusters if local administrator is disabled.
947634	*Security Fabric* widget shows the serial number instead of the hostname for a secondary FortiGate in HA.
950624	Renaming conflicted Fabric objects on the root FortiGate does not synchronize the changed Fabric objects to the downstream FortiGate.
956423	In HA, the primary unit may sometimes show a blank GUI screen.
966740	Security rating *Last Ran* displays incorrect values.
968585	The automation stitch triggered by the FortiAnalyzer event handler does not work as expected.
968621	Erroneous memory allocation resulting in unexpected behavior in csfd after upgrading.
968749	The GUI is slow when editing or trying to authorize devices in the Security Fabric section.
975393	Security Fabric messages change after upgrading.
976049	The external threat feed connection status is Unavailable in a non-VDOM enabled FortiGate.
980595	When loading the fabric connector pages when there are many extension devices connected to the fabric, the page becomes unresponsive.
985198	The IP address threat feed connection status indicates an *Other Error*.
988526	Address object changes from the CLI of the root FortiGate in Security Fabric are not synchronized with downstream devices.

SSL VPN

Bug ID	Description
821240	SSLVPNVD 11 signal failure due to attempt to read out of bounds memory.
830068	SSL VPN stops listening on IPv6 interface after a reboot.
879329	Destination address of SSL VPN firewall policy may be lost after upgrading when `dstaddr` is set to `all` and at least one authentication rule has a portal with split tunneling enabled.
896492	When using RDP bookmarks in SSL web mode, some keys stopped working.
898889	The internal website does not load completely with SSL VPN web mode.
926612	The SSL VPN log shows users having been disconnected from SSL VPN for unknown reason.
929001	An invalid user name entered in FortiClient could cause two factor PKI user login to crash sslvpnd after the client certificate checking passed.
930275	Firewall policy is not allowing the all destination address with a split-tunneling portal.
950157	SSL VPN connected/disconnected endpoint event log can be in the wrong sequence.
952860	During a handshake when FortiClient sends a larger-than-MTU hello message, the packet is fragmented by IP layer and dropped by the FortiGate.
957406	OS checklist for SSL VPN in FortiOS does not include macOS Sonoma 14.
965482	FortiGate 200F experiences poor performance due to Marvell switch HOL mode.
981310	Multiple VPNSSL disconnections triggered by sslvpnd failure.

Switch Controller

Bug ID	Description
703374	Long DAC-type cable is added to default media type on 10G port on FG-100F.
816790	Console printed DSL related error messages when disconnecting the managed FortiSwitch and connecting to the FortiGate again.
818116	When changing the FortiSwitch FortiLink port status, the configuration is not applied to the FortiSwitch.
899414	The *WiFi Maps* and *FortiSwitch Clients* menus in the GUI show the LACP interface with red down arrows when the LACP interfaces are up.
904834	FortiGate and FortiManager have different definitions for the value of `poe-detection-type` on S108EF platform.
911232	The security rating shows an incorrect warning for unregistered FortiSwitches on the *Managed FortiSwitches* page.

Bug ID	Description
	Workaround: navigate to the *Diagnostics & Tools* pane of the FortiSwitch to see the correct registration status.
937065	An exported FortiSwitch port is not correctly showing up/down status.
949377	NAC policy cannot match the MAC address with a specific VLAN. The NAC policy needs to be deleted and re-createed for it to work again.
950379	The diagnostics of online FortiAPs shows *Link Down* in the trunk port *Connected Via* field when the FortiAP has an LACP connection to a FortiSwitch.
984404	After upgrading the version 7.4.2, the FortiSwitch shows as *not registered* in the GUI.
989015	The SWC switch port does not have all of the speed options compared to FortiSwitch.

System

Bug ID	Description
733096	FG-100F HA secondary's unused ports flaps from down to up, then to down.
754970	HPE does not enforce a limit on fragmented packets sent to the CPU when ip-reassembly is enabled.
763739	On FG-200F, the *Outbound* bandwidth in the *Bandwidth* widget does not match outbandwidth setting.
801481	Download speed issue through WAN configured with PPPoE on FortiGate.
828557	FortiGate as DHCP relay is not showing a DHCP decline in the debugs when there is an IP conflict in the network.
846399	Add 100G speed option for FG-180xF for ports 37, 38, 39, and 40. Upon firmware upgrade, existing port speed configurations are preserved.
855515	Hardware csum failure message keeps repeating on Azure 7.0.8.
859393	SNMP poll for fgExplicitProxyRequests returns 0.
861661	SNMP OID 1.3.6.1.2.1.4.32 ipAddressPrefixTable is not available.
861962	When configuring an 802.3ad aggregate interface with a 1 Gbps speed, the port's LED is off and traffic cannot pass through. Affected platforms: 110xE, 220xE, 330xE, 340xE, and 360xE.
867428	Add check to skip invalid names when creating a VDOM.
880271	Aggregate interface (LAG) dropping traffic.
882131	PPPoE interface with SFP does not recover after a connectivity failure.
882187	FortiGate enters conserve mode in a few hours after enabling UTM on the policies.

Bug ID	Description
883606	FortiOS allows customers to enable or disable the INDEX extension that appends the VDOM or interface index in RFC tables.
885057	Add 100G speed option on the FortiGate 1800F.
887940	Status light is not showing on the FortiGate 60F or 100F after a cold and warm reboot.
888941	Some sessions are still reported as offloaded when `auto-asic-offload` is disabled.
892478	Interface release from cmdb and iprope keep updating when DHCP client renewal fails.
893143	SFP interfaces that are set to 1000auto are not negotiating on the secondary device.
907657	FortiGate does not perform a disk scan automatically when `autorun-log-fsck` is enabled.
910364	CPU usage issue in miglogd caused by constant updates to the ZTNA tags.
910651	On FG-600F, all members are up but the LACP status is showing as down after upgrading.
910829	Degraded traffic bandwidth for download passing from 10G to 1G interfaces.
911906	Enable auto-upgrade by default on the FortiGate 40F and 40G.
912092	FortiGate does not send ARP probe for UDP NP-offloaded sessions.
915585	Optimize memory usage, which causes the SLAB memory to increase, in kernel 4.19.
916493	Fail detection function does not work properly on X1 and X2 10G ports.
917827	Delay sending LACPDU in kernel 4.19.
919901	For FIPS-CC mode, the strict check for basic constraints should be removed for end entity certificates.
920349	Connectivity was lost after creating new VDOM and NPU_VLINK.
923473	Sometimes, the configuration cannot be backed up to an FTP server.
925647	Memory usage issue caused by repetitive log messages. Affected platforms: FG-100xF.
926817	Review the temperature sensor for the SoC4 system.
929135	Interactive CLI commands, like `purge`, cannot be cut and pasted into the console and exits the script. The purge command in a console puTTy session stops and waits for a `y` confirmation.
929896	Unable to configure a 9600 baud-rate on DNP3-Proxy.
930803	Unable to monitor DSL parameters and the `get sys dsl status` command shows errors.
931167	IPv6 suffixes configured on an interface are not reflected after a reboot.
931299	When the URL filter requests the FortiGuard (FGD) rating server address using DNS, it will try to get both A (IPv4) and AAAA (IPv6) records.
931604	The FortiGate checksum changes and the FortiManager Backup Mode device status becomes out-of-sync.

Bug ID	Description
937982	High CPU usage might be observed on entry-level FortiGates if the cache size reaches 10% of the system memory.
938174	ARP issue with VXLAN over IPsec and Soft Switch.
938449	In the 4.19 kernel, when a neighbor's MAC is changed, the session and IPsec tunnel cannot be flushed from the NPU.
938981	The virtual server http-host algorithm is redirecting requests to an unexpected server.
939935	High CPU usage caused by DHCP packets.
939947	FG-1100E SFP interface of port 23 and 24 with transceiver status is down after upgrading.
940504	Loading of the Toss Bank application is delayed or gets stuck on iPhones with hyperscale CGNAT (NAT64).
943033	Enabling `vdom-dns` causes the VDOM DNS certificate to be blank instead of the default value.
943090	Buffer and description queue limitation of Marvell switch port will cause a performance limitation.
943615	When cmdbsvr receives a request to update the version number, it also receives a copy of the query, but this copy is not freed.
943948	FortiGate as L2TP client is not working with Cisco ASR as L2TP server.
945426	FortiGate ports are not in a configured state after the connected switch reboots.
945871	DNAT does not work on software switch in explicit mode.
946413	Temperature sensor value missing for FG-180xF, FG-420xF, and FG-440xF platforms.
946714	Unexpected reboot caused by a rare error condition for FG-VM.
947127	Kernel TCP sessions do no timeout after receiving a legitimate RST and the system goes into conserve mode.
947240	FortiGate is not able to resolve ARPs of few hosts due to their ARP replies not reaching the primary FPM.
948460	Enabling NP7 offloading is causing packet drops when using a shaping profile.
948490	Changing address object setting triggers a 30 second CPU usage spike.
949481	The `tx_collision_err` counter in the FortiOS CLI keeps increasing on both 10G SFP+ X1 and X2 interfaces.
950010	Alarm observed for high PECI temperature despite less CPU activity.
952284	A FortiGate with 2G of memory enters conserve mode when a node uses 20% of the memory.
954529	The `diagnose npu sniffer stop` command can lead to a traffic outage.
955021	When signal 11 is sent to httpsd process using `diagnose sys kill 11 <PID>`, httpsd does not restart. The GUI displays a *Service unavailable* message. GUI access can be restored by rebooting the device.

Bug ID	Description
955074	MSS clamping is not working on VXLAN over IPsec after upgrading.
955798	Interface LED from panel indicates the wrong status.
956391	On FG-10xE, when using ports 13 to 16 as virtual switch LAN ports, auto speed is not supported.
956413	FG-1101E ports with AVAGO AFBR-5710PZ transceiver failed to come up after upgrading.
957147	FortiGate as DNS server does not resolve domains in the local database on new VDOM.
957714	Memory usage issue occurs when multiple threads try to access a VLAN group.
957846	High CPU usage caused by DHCP packets.
958157	The GeoIP file should close appropriately after opening or using mmap to share memory.
960563	An error condition occurred in the kernel caused by a rare condition while using the GRE tunnels.
960643	IP addresses with an expired quarantine period might not be removed from quarantine.
960707	Egress shaping does not work on NP when applied on the WAN interface.
962153	A port that uses a copper-transceiver does not update the link status in real-time.
963597	Multiple configuration settings are missing after restoring the VDOM.
963600	SolarWinds unable to negotiate encryption, no matching host key type found.
964465	Administrator with read-write permission for WiFi and read permission for network configuration cannot create SSIDs.
966187	Unable to set a static ARP entry on the EMAC VLAN interface.
966761	SNMP OID 1.3.6.1.2.1.4.34.1.5 ipAddressPrefix is not fully implemented.
967171	The `speed 1000auto` setting on ports X1 to X4 disappears after upgrading from 7.2.5 to 7.2.6. Affected platforms: FG-40xF and FG-60xF.
968134	FortiGate 200F experiences poor performance due to Marvell switch HOL mode.
969230	FEC does not take effect on X5 - X8 ports when running at 25G ULL mode on FG-601F.
971404	Session expiration does not get updated for offloaded traffic between a specific host range.
975496	FortiGate 200F slow download and upload speeds when traversing from a 1G to a 10G interface.
977231	An error condition occurred in fgfm caused by an out-of-band management configuration.
977740	Transparent-mode VDOM system switch-interface and Firewall policies deleted after a power cycle.
981685	On the FortiGate 4400F, high CPU usage by random CPU cores in the system space.
982200	FortiGate enters into conserve mode due to excessive memory usage by Slabs.
982651	Security mode 802.1X authentication happens every hour on a hardware switch on with 7.2 code.
986698	The NP7 should use the updated MAC address from the ARP table to forward traffic to the destination server.

Bug ID	Description
988528	With NGFW mixed traffic, the CPU usage goes to 99%.
995395	Typo in the `set ipv6-allow-local-in-slient-drop` command.
995965	Ports 15 and 16 are directly connected but are unable to ping each other.

Upgrade

Bug ID	Description
871181	FG-3401E link is not coming up using DAC cables after upgrading.
896937	Port channel is down after upgrading the FG-1101E.
939011	All transparent VDOMs cannot synchronize because of `switch-controller.auto-config.policy`.
940126	Upgrading a FGT-3401E generates BPDUs, which cause the switch to disable the port.
1003503	Optimizing federated auto-firmware upgrade with FortiGate, FortiSwitch, and FortiAP.

User & Authentication

Bug ID	Description
868994	FortiGate receives FSSO user in the format of HOSTNAME$.
891068	Guest administration management does not show all groups for multiple VDOMs assigned to a guest administrator account.
915998	FortiToken mobile push with ACME gives an untrusted certificate in iOS application.
932989	In some cases, the HA connection is removed and its memory is freed, but it is still read/written in the following process.
934313	Password and Token concatenation for remote RADIUS users does not work as expected.
967146	Upon expiration, the SSL certificate is removed from GUI but not from the CLI.
971641	Issue sending activation code for FortiToken in a multi-VDOM environment with remote user authentication.
975299	FortiToken serial number is not displayed while searching for it in the GUI.
975689	Unable to print with custom guest user print template.
976338	RADIUS accounting packet with `acct-input-octets` and `acct-output-octets` sometimes shows inconsistent behavior.

Bug ID	Description
1000108	Guest-management administrators cannot see or print guest user passwords in plain text; the password is masked as `ENC XXXX` string.

VM

Bug ID	Description
874559	FortiGate VM HA primary loses connection when setting up secondary unit.
903798	When `send-deny-packet enabled` or `ident-accept disabled`, sending out responding packets (such as TCP RST or ICMP) triggers a restart.
921168	Restore operation overwrite passive configuration in AZURE A-P deployment based on SDN connector.
930381	FortiGate VM heartbeat authentication fails during the upgrade to 7.2.4 or 7.2.5 when HA authentication and encryption is enabled.
932085	In an Azure cluster, the NTP `source-ip6` (IPv6) is synchronized while the `source-ip` (IPv4) is not.
938382	OpenStack Queens FortiGate VM HA heartbeat on broadcast is not working as expected.
951787	On a FortiGate VM on Azure, a deadlock between pci-recovery and mlx5-recovery stalls a number of mlx5-txrxq recovery tasks.
954076	A FortiGate VM on ESXi with FGCP clustering is unable to do VLAN traffic in DPDK mode.
956460	FortiGate cannot detect a log disk in some new Azure instances.
957299	On a FortiGate ARM-OCI, after adding more than one network interface card and rebooting, the interface cards are not kept in order.
957886	GCP OS log in integration issues occur in FortiGate deployment.
959859	FG-VM64-AZURE SDN connector does not retry requests to management.azure.com if they fail.
965668	Interfaces are brought down by azd, and traffic is disrupted until manually disabling and enabling the interfaces on the Azure VM.
967134	An interrupt distribution issue may cause the CPU load to not be balanced on the FG-VM cores.
968740	Unexpected behavior in awsd caused by tags with an empty value on AWS instances while adding a new AWS Fabric connector.
970201	Unexpected reboot caused by a rare error condition for FG-VM.
977271	After enabling DPDK on the VM, return traffic to the VLAN interface is dropped.
983705	The Azure SDN Connector does not retrieve all of the virtual networks if the results are paginated.
999599	On FortiGate AWS, the IPsec configuration goes missing after an upgrade due to an inconsistent table-size.

WAN Optimization

Bug ID	Description
954541	In WANOpt transparent mode, WAN optimization does not keep the original source address of the packets.

Web Filter

Bug ID	Description
915879	Add web filter categories for artificial intelligence technology (category 100) and Cryptocurrency (category 101).
917475	The FortiGuard category threat feed is not working as expected in proxy mode.
929110	The `strict` option for `sni-server-cert-check` is behaving the same as if it is set to `enable`, and logs are not generated upon SNI mismatch with the CN or SAN.
941045	Local rating chooses the wrong category if the URL path falsely matches to a longer local rating URL.
947676	Web filter profile setting changes the order of FortiGuard web filter categories.
982156	The URL local/user category rating result has only one best match category (longest URL pattern match), and other matched local/user categories cannot be chosen even if the category is configured in the profile.
994749	The urlfilter fails to block TP HTTPS traffic with an IP address hostname.

WiFi Controller

Bug ID	Description
883021	Is the FortiGate 100F RFC 2865 compliant and, if yes, why does the FortiGate not always re-authenticated after the Session-Timeout value?
883938	Flooded wireless STA traffic seen in L2 tunneled VLAN (FG-1800F).
896104	An error condtion occured in the kernel when the FortiAP and SSID are in the same software switch.
900605	NAS-ID is not updated immediately after modifying it in the applied RADIUS server when the `wpad-process-count` is set to a non-zero value.
905789	FortiAP 431G is unable to join AC due to no response to cfg_request.

Bug ID	Description
922838	Usage of the cw_acds process increases and drops the FortiAP connection, which forces the FortiAP to restart in an FSM state when FortiAP settings are changed.
923530	Add support for 6 GHz band for DARRP, `wlac -c rf-analysis`, and BG scan period.
926999	An error condition occurred for the EAP proxy while sending the RADIUS Access-Request.
930130	MPSK keys are not loaded completely in the wpad daemon after applying a VAP with an MPSK profile selected on a FortiAP.
931592	CAPWAP offloading does not work with more than 12,000 VAP entries.
938525	Wi-Fi clients failed roaming from one FortiAP to another on the bridge SSID with dynamic VLAN assignment by RADIUS-based MAC authentication.
949857	Captive portal appears each time after a channel change or if roaming performed (Cisco ISE with FortiGate and FortiAP).
951792	Clients connected to certain FortiAPs do not have internet access.
952889	PMKID should be removed when an Android device is disconnected by the RADIUS CoA DM request with Acct-Session-Id.
957543	The collected FortiGate syntax is missing channels for 11AX6.
965695	Join/leave is repeated between FortiAP 421E and FortiGate 100E at multiple sites.
977351	The SASE portal is unable to authorize a FortiAP if it initially connects to a secondary VM.
985265	HA setup hostapd issue during stress test.

ZTNA

Bug ID	Description
888814	Unable to match first group attribute from SAML assertion for ZTNA rule.
945016	When NAT is enabled in a firewall policy ZTNA mode, saving it in GUI will cause NAT to be disabled.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references

Known issues

The following issues have been identified in version 7.2.8. To inquire about a particular bug or report a bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
937375	Unable to delete malware threat feeds using the CLI.

Explicit Proxy

Bug ID	Description
865828	The `internet-service6-custom` and `internet-service6-custom-group` options do not work with custom IPv6 addresses.
890776	GUI-explicit-proxy setting was lost after upgrade.

894557	In some cases, the explicit proxy policy list can take a long time to load due to a delay in retrieving the proxy statistics. This issue does not impact explicit proxy functionality.
	Workaround: restart the WAD process, or update the number of WAD processors.
	`config system global`
	`  set wad-worker-count <integer>`
	`end`

1001700	If explicit webproxy uses SAML authentication and the PAC file is enabled at the same time, the browser will report a too many redirects error when trying to visit any websites.

Firewall

Bug ID	Description
935034	The clock skew tolerance is not reflected.

FortiGate 6000 and 7000 platforms

Bug ID	Description
638799	The DHCPv6 client does not work with vcluster2.
781163	*FortiView Sources* page is unable to display historical data from FortiAnalyzer due to *Fail to retrieve FortiView data* error.
790464	Existing ARP entries are removed from all slots when an ARP query of a single slot does not respond.
885205	IPv6 ECMP is not supported for the FG-6000F and FG-7000E platforms. IPv6 ECMP is supported for the FG-7000F platform.
948388	On the FortiGate 6000s, missing image update command in the CLI: `execute load-balance update image`.
951135	Graceful upgrade of a FortiGate 6000 or 7000 FGCP HA cluster is not supported when upgrading from FortiOS 7.0.12 to 7.2.6. Upgrading the firmware of a FortiGate 6000 or 7000 FGCP HA cluster from 7.0.12 to 7.2.6 should be done during a maintenance window, since the firmware upgrade process will disrupt traffic for up to 30 minutes. Before upgrading the firmware, disable `uninterruptible-upgrade`, then perform a normal firmware upgrade. During the upgrade process the FortiGates in the cluster will not allow traffic until all components (management board and FPCs or FIMs and FPMs) are upgraded and both FortiGates have restarted. This process can take up to 30 minutes.
951193	SLBC for FortiOS 7.0 and 7.2 uses different FGCP HA heartbeat formats. Because of the different heartbeat formats, you cannot create an FGCP HA cluster of two FortiGate 6000s or 7000s when one chassis is running FortiOS 7.0.x and the other is running FortiOS 7.2.x. Instead, to form an FGCP HA cluster, both chassis must be running FortiOS 7.0.x or 7.2.x. If two chassis are running different patch releases of FortiOS 7.0 or 7.2 (for example, one chassis is running 7.2.5 and the other 7.2.6), they can form a cluster. When the cluster is formed, FGCP elects one chassis to be the primary chassis. The primary chassis synchronizes its firmware to the secondary chassis. As a result, both chassis will be running the same firmware version. You can also form a cluster if one chassis is running FortiOS 7.2.x and the other is running 7.4.x. For best results, both chassis should be running the same firmware version, although as described above, this is not a requirement.
954881	Image synchronization failure happened after a factory reset on FortiGate 7000E/F .
994241	On FortiGate 7000F using FGSP and FGCP, when TCP traffic takes an asymmetric path, the TCP ACK and data packets might be dropped in NP7.
1003879	Incorrect SLBC traffic-related statistics may be displayed on the FortiGate 6000 or FortiGate 7000 GUI (for example, in a dashboard widgets). This can occur if an FPC or FPM is not correctly registered for statistic collection during startup. This is purely a GUI display issue and does not impact system operation. To work around this display issue, enter the command `diagnose nodejs process restart` to reset the aggregator. You may need to wait for a few minutes after the system has started up before entering this command to make sure that all systems have fully initialized.

FortiView

Bug ID	Description
941521	On the *FortiView Web Sites* page, the *Category* filter does not work in the Japanese GUI.

GUI

Bug ID	Description
853352	On the *View/Edit Entries* slide-out pane (*Policy & Objects* > *Internet Service Database* dialog), users cannot scroll down to the end if there are over 100000 entries.
854180	On the policy list page, all policy organization with sequence and label grouping is lost.
925388	After updating, the CMDB may not start up properly. This issue causes problems with both the GUI and CLI.
957441	A *Cannot determine mkey for cmdb source entry* error is received when viewing the *Firmware & Registration* page.
974988	FortiGate GUI should display a license expired notification due to an expired FortiManager Cloud license if it still has a valid account level FortiManager Cloud license (function is not affected).
996379	The address objects page is not loading the content.
999972	IPS profile exemptions are not saved when using the GUI.

HA

Bug ID	Description
825380	In workspace configuration save mode, the save action is not synchronized from the HA primary unit to the secondary unit.
858683	FortiGate in A-P HA mode with `admin-restrict-local` enabled allows the local administrator to log in to the passive host, even if LDAP is available.
929486	When Configuration save mode is set to *Manual*, any firewall policy change will make the cluster out-of-sync.
940400	SCTP traffic is not forwarded back to the session owner (FGSP asymmetric traffic with IPS , NAT mode, and SCTP).
998004	When the HA management interface is set a LAG, it is not synchronized to newly joining secondary HA devices.
1000001	A secondary HA unit may go into conserve mode when joining an HA cluster if the FortiGate's configuration is large.

Hyperscale

Bug ID	Description
802182	After successfully changing the VLAN ID of an interface from the CLI, an error message similar to `cmdb_txn_cache_data(query=log.npu-server,leve=1) failed` may appear.
817562	NPD/LPMD cannot differentiate the different VRF's, considers as VRF 0 for all.
824071	ECMP does not load balance IPv6 traffic between two routes in a multi-VDOM setup.
843197	Output of `diagnose sys npu-session list/list-full` does not mention policy route information.
853258	Packets drop, and different behavior occurs between devices in an HA pair with ECMP next hop.
872146	The `diagnose sys npu-session list` command shows an incorrect policy ID when traffic is using an intra-zone policy.
920228	NAT46 NPU sessions are lost and traffic drops when a HA failover occurs.
936747	Connections per second (CPS) performance of SIP sessions accepted by hyperscale firewall policies with EIM and EIF disabled that include overload with port block allocation (PBA) GCN IP pools is lower than expected. **Workaround**: enter the following command for each NP7 processor to resolve the performance issue. `# diagnose npu np7 setreg <npu_#> nss.nss_thrd_ctrl.thrd_ctrl 0xF` Where `<npu_#>` is the NP7 processor number. NP7 processors are numbered 0, 1, 2, and so on. The configuration changes from entering these diagnose commands are reset if the FortiGate restarts. After a system restart, just re-enter the diagnose commands.
994019	Hairpin is not working.

IPsec VPN

Bug ID	Description
944600	CPU usage issues occurred when IPsec VPN traffic was received on the VLAN interface of an NP7 vlink.
954614	IPsec phase 2 negotiation fails with `failed to create dialup instance, error 22` error message.

Log & Report

Bug ID	Description
938396	`The following intrusion was observed:` in the alert mail refers to another field in the anomaly log.
1001583	The GUI is slow and reverts the input when multiple ports are added to a filter for destination ports.

Proxy

Bug ID	Description
910678	CPU usage issue in WAD caused by a high number of devices being detected by the device detection feature.
922093	CPU usage issue in WAD caused by source port exhaustion when using WAN optimization.

REST API

Bug ID	Description
859680	In an HA setup with vCluster, a CMDB API request to the primary cluster does not synchronize the configuration to the secondary cluster.
920260	SD-WAN interfaces should be denoted in the interface statistics API.
1004136	Unable to retrieve more than 1000 logs using an API call.

Remote Access

Bug ID	Description
837391	FortiClient does not send the public IP address for SAML, resulting in *0.0.0.0* being shown in FortiOS and SASE.

Routing

Bug ID	Description
896090	SD-WAN members can be out-of-sla after some retrieve times.
903444	The `diagnose ip rtcache list` command is no longer supported in the FortiOS 4.19 kernel.
910656	Router information in the BGP summary still shows removed BGP neighbor/peer configuration.
924693	The SD-WAN rule page in the GUI does not show red interfaces if the member is down.
1003756	Prefix-list is set to 0.0.0.0 0.0.0.0 when the wrong input is added using the GUI.

Security Fabric

Bug ID	Description
958429	The webhook request header does not contain `Content-type: application/json` when using the JSON format. This causes Microsoft Teams to reject the request.

SSL VPN

Bug ID	Description
795381	FortiClient Windows cannot be launched with SSL VPN web portal.
905050	SSL VPN users are dropped due the samld process stopping.
941676	Japanese key input does not work correctly during RDP in SSL VPN web mode.
947210	Application sslvpnd `*** code requested backtrace ***` was observed during graceful upgrade.

Switch Controller

Bug ID	Description
947351	The FortiSwitch topology is not loading correctly on the GUI.
951721	The FortiGate GUI shows incorrect port statuses for managed FortiSwitches.
961142	An interface in FortiLink is flapping with MCLAG with DAC on an OPSFPP-T-05-PAB transceiver.
1000663	The switch-controller managed-switch ports' configurations are getting removed after each reboot.

System

Bug ID	Description
782710	Traffic going through a VLAN over VXLAN is not offloaded to NP7.
861144	`execute ping-option interface` cannot specific an interface name of `a`.
882862	LAG interface members are not shutting down when the remote end interface (one member in the LAG) is down.
885189	Control the server host key algorithm in the CLI.
901621	Setting the interface configuration `inbandwidth` or `outbandwidth` commands stops traffic flow.
901721	In a certain edge case, traffic directed towards a VLAN interface could trigger a kernel panic.
913732	Without any traffic, memory usage of FG-1800F keeps increasing slowly over time.
921134	GUI is inaccessible when using a SHA1 certificate as `admin-server-cert`.
921604	On the FortiGate 601F, the ports (x7) have no cables attached but the link LEDs are green.
925554	The GUI shows a VLAN interface of a hardware switch and software switch as down.
939013	SNMP walk of the entire MIB fails when the configuration has split-port and a large number of interfaces.
967436	DAC cable between FortiGate and FortiSwitch stops working after upgrading from 7.2.6 to 7.2.7.

Upgrade

Bug ID	Description

977281	After the FortiGate in an HA environment is upgraded using the Fabric upgrade feature, the GUI might incorrectly show the status *Downgrade to 7.2.X shortly*, even though the upgrade has completed.
	This is only a display issue; the Fabric upgrade will not recur unless it is manually scheduled.
	Workaround: Confirm the Fabric upgrade status to make sure that it is not enabled:
	`config system federated-upgrade`
	`  set status disabled`
	`end`

User & Authentication

Bug ID	Description
667150	When a remote LDAP user with Two-factor Authentication enabled and Authentication type 'FortiToken' tries to access the internet through firewall authentication, the web page does not receive the FortiToken notification or proceed to authenticate the user. **Workaround**: click the *Continue* button on the authentication page after approving the FortiToken on the mobile device.
933622	The FortiGate does not send the user's IP address to the TACACS+ server during an authorization request.
1003405	The Firewall User widget is not displaying users when not expanded to full screen view.

VM

Bug ID	Description
899984	If FGTVM was deployed in UEFI boot mode, do not downgrade to any GA version earlier than 7.2.4.
923061	IPsec tunnels on AWS have TX errors incremented every 30 seconds.

Web Filter

Bug ID	Description
885222	HTTP session is logged as HTTPS in web filter when VIP is used.
1004985	The webfilter cookie override trigger process had no issue observed and an override entry was created in the FortiGate, but client access was kept blocked by the old profile and the client received a replacement message with an override link just like the initial access to trigger the override.

WiFi Controller

Bug ID	Description
869106	The layer 3 roaming feature may not work when the wireless controller is running multiple cw_acd processes (when the value of `acd-process-count` is not zero).
869978	CAPWAP tunnel traffic over tunnel SSID is dropped when offloading is enabled.

Bug ID	Description
873273	The *Automatically connect to nearest saved network* option does not work as expected when FWF-60E client-mode local radio loses connection.
903922	Physical and logical topology is slow to load when there are a lot of managed FortiAP (over 50). This issue does not impact FortiAP management and operation.
938840	Excessive `MEM POOLuse_up_cnt` observed on secondary unit in an HA environment.
941691	Managed FortiSwitch detects multiple MACs using the same IP address.
949682	Intermittent traffic disruption observed in cw_acd caused by a rare error condition.
1001104	Some FortiAP 231F units show join/leave behavior after the FortiGate is upgraded to 7.2.7.

ZTNA

Bug ID	Description
819987	SMB drive mapping made through a ZTNA access proxy is inaccessible after rebooting.

Built-in AV Engine

AV Engine 6.00293 is released as the built-in AV Engine. Refer to the AV Engine Release Notes for information.

Built-in IPS Engine

IPS Engine 7.00326 is released as the built-in IPS Engine. Refer to the IPS Engine Release Notes for information.

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.

www.fortinet.com