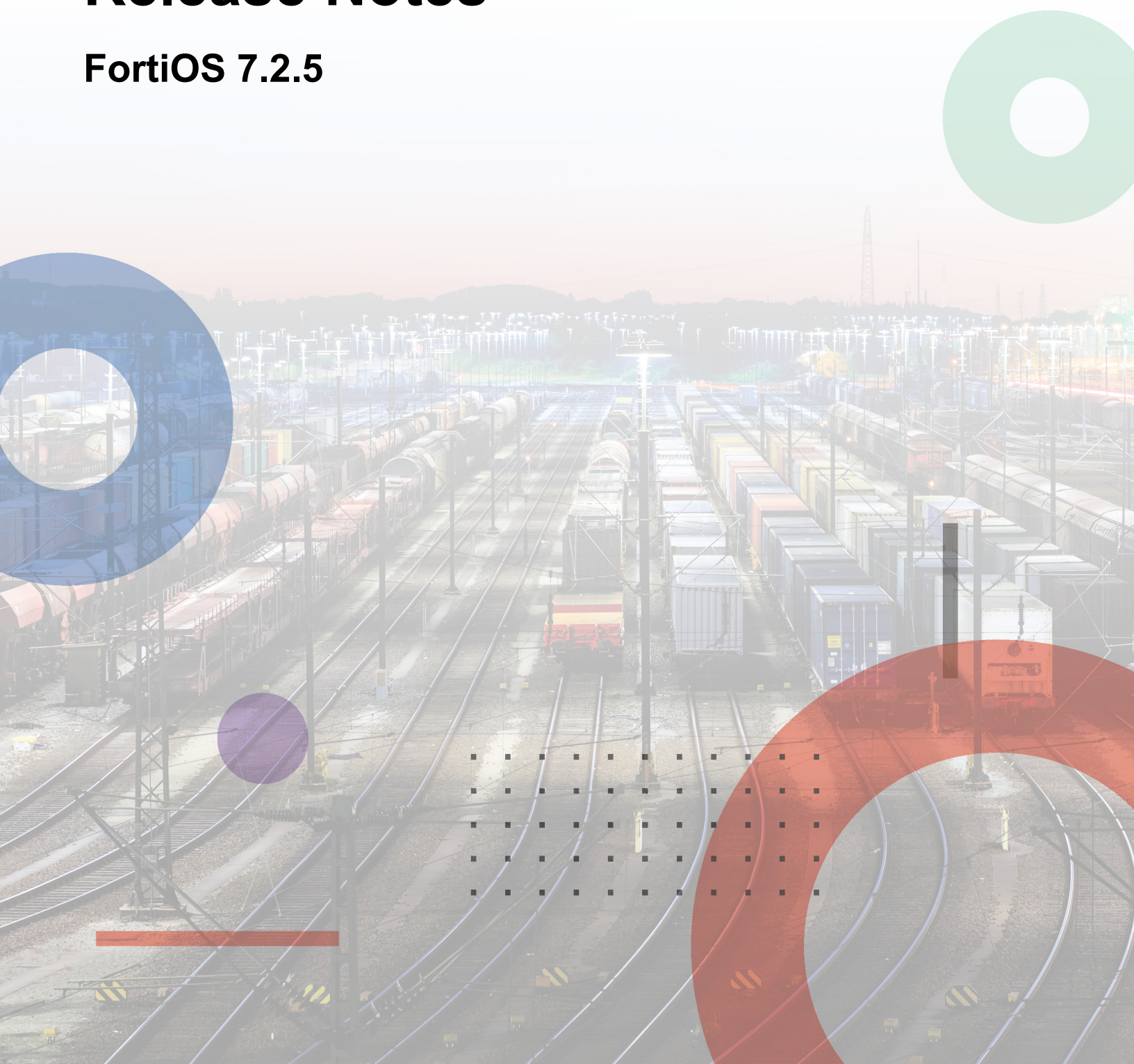
FORTINET

Release Notes

FortiOS 7.2.5



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

FORTINET TRAINING 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

June 8, 2023
FortiOS 7.2.5 Release Notes
01-725-857839-20230608

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-06-08	Initial release.

Introduction and supported models

This guide provides release information for FortiOS 7.2.5 build 1517.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.2.5 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-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-3000F, FG-3001F, 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, 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-3980E, 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 7.2.5 supports the following FG-6000F, FG-7000E, and FG-7000F models:

FG-6000F	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

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.

FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 7.2.5 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 7.2.5 features.

Changes in GUI behavior

Bug ID	Description
742365	Prior to this enhancement, a ZTNA configuration required configuring: • An EMS connection and EMS tags • A ZTNA server configuration • A ZTNA rules (proxy policy) • An authentication scheme and rules (optional) In this enhancement, there are now two ways to configure the ZTNA rule in the GUI. 1. Full ZTNA policy: under *System* > *Feature Visibility*, enable *Explicit Proxy*. Under *Policy & Objects* > *Proxy Policy*, create a policy with the *ZTNA* type. 2. Simple ZTNA policy: a regular *Firewall Policy* is used for policy management. When creating a new *Firewall Policy*, configure a ZTNA policy with *ZTNA* mode. As a result, the *Policy & Objects* > *ZTNA* > *ZTNA rules* tab has been removed. Existing ZTNA rules now appear in *Policy & Objects* > *Proxy Policy* after upgrade.

Changes in default behavior

Bug ID	Description
837048	In the following scenarios, creating a matching address object for an interface is enabled automatically and cannot be disabled: • When creating a new interface with the LAN role. • When an interface role is changed from a non-LAN role to a LAN role. Once the address object is created, it cannot be deleted unless the interface role is changed to a non-LAN role.
841712	On FortiGates licensed for hyperscale firewall features, the `config system setting` options `nat46-force-ipv4-packet-forwarding` and `nat64-force-ipv6-packet-forwarding` now also apply to NP7-offloaded traffic. The `config system npu` option `nat46-force-ipv4-packet-forwarding` has been removed.

Changes in table size

Bug ID	Description
870538	Increase `firewall.address`, `firewall.service.group`, and `firewall.policy` table size for FG-600F and FG-601F. The new sizes are 4000, 4000, and 30000 respectively.
883103	Increase `firewall.address` from 40,000 to 50,000 for FG-1000D, FG-1100E, and FG-1101E. Increase `firewall.address` from 65,000 to 100,000 for FG-1200D, FG-1500D, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, and FG-2500E. Increase `firewall.address` from 65,000 to 150,000 for FG-2600F and FG-2601F.

New features or enhancements

More detailed information is available in the New Features Guide.

Feature ID	Description
727383	Add GUI support for IPv6 addresses in Internet Service Database (ISDB), and allow them to be configured in firewall policies.
745172	The information pane, which is located in the right-side gutter of many GUI pages, is enhanced to display the top three contextually appropriate questions as hyperlinks under the *Hot Questions at FortiAnswers* heading. • Clicking a link takes the user to the related questions and answer page on the FortiAnswers website. • The number of answers, votes, and views is displayed for each question. • Clicking the *See more* link takes the user to the related topic page on FortiAnswers. The existing documentation related links have been renamed: • The *Documentation* section header is renamed to *Online Guides*. • The *Online Help* link is renamed to *Relevant Documentation*.
749989	FortiGates, FortiSwitches, FortiAPs, and FortiExtenders can download an EOS (end of support) package automatically from FortiGuard during the bootup process or by using manual commands. Based on the downloaded EOS package files, when a device passes the EOS date, a warning message is displayed in the device's tooltip, and the device is highlighted in the GUI. The End-of-Support security rating check rule audits the EOS of FortiGates and Fabric devices. This allows administrators to have clear visibility of their Security Fabric, and help prevent any security gaps or vulnerabilities that may arise due to any devices that are past their hardware EOS date.
753177	Display IoT devices with known vulnerabilities on the *Security Fabric* > *Asset Identity Center* page's *Asset* list view. Hovering over the vulnerabilities count displays a *View IoT Vulnerabilities* tooltip, which opens the *View IoT Vulnerabilities* table that includes the *Vulnerability ID*, *Type*, *Severity*, *Reference*, *Description*, and *Patch Signature ID*. Each entry in the *Reference* column includes the CVE number and a link to the CVE details. The *Security Fabric* > *Security Rating* > *Security Posture* report includes *FortiGuard IoT Detection Subscription* and *FortiGuard IoT Vulnerability* checks. The *FortiGuard IoT Detection Subscription* rating check will pass if the *System* > *FortiGuard* page shows that the *IoT Detection Service* is licensed. The *FortiGuard IoT Vulnerability* rating check will fail if any IoT vulnerabilities are found. To detect IoT vulnerabilities, the FortiGate must have a valid IoT Detection Service license, device detection must be configured on a LAN interface used by IoT devices, and a firewall policy with an application control sensor must be configured.
766158	Introduce a multi-tiered approach to determining the action taken on a video. The channel filter is checked first, and if the video's channel matches a configuration entry, the corresponding action is taken. If not, the FortiGuard category filter is checked and the corresponding action is taken if the video's category matches a configuration entry. If neither of these conditions are met, the default action specified in the video filter profile is used. Logging is also enabled by default.

Feature ID	Description

	`config videofilter profile`
	`edit <name>`
	`set default-action {allow | monitor | block}`
	`set log {enable | disable}`
	`next`
	`end`

767570	Add the Fabric Overlay Orchestrator, which is an easy-to-use GUI wizard within FortiOS that simplifies the process of configuring a self-orchestrated SD-WAN overlay within a single Security Fabric without requiring additional tools or licensing. Currently, the Fabric Overlay Orchestrator supports a single hub architecture and builds upon an existing Security Fabric configuration. This feature configures the root FortiGate as the SD-WAN overlay hub and configures the downstream FortiGates (first-level children) as the spokes. After configuring the Fabric Overlay, you can proceed to complete the SD-WAN deployment configuration by configuring SD-WAN rules.

769722	Allow a managed FortiSwitch ID to be edited and store the device serial number as a new read-only field.
	`config switch-controller managed-switch`
	`edit <id>`
	`set sn <serial_number>`
	`next`
	`end`
	The device ID can be configured to a maximum of 16 alphanumeric characters, including dashes (-) and underscores (_).
	Some related `config`, `execute`, and `diagnose` commands have been modified to configure and display user-definable FortiSwitch IDs accordingly. The system data and daemons have been modified to use the new switch serial number field to ensure the existing switch controller and dependent features still work.

780571	Add *Logs Sent Daily* chart for remote logging sources (FortiAnalyzer, FortiGate Cloud, and FortiAnalyzer Cloud) to the *Logging & Analytics Fabric Connector* card within the *Security Fabric* > *Fabric Connectors* page and to the *Dashboard* as a widget for a selected remote logging source.
805867	Increase the number of supported NAC devices to 48 times the maximum number of FortiSwitch units supported on that FortiGate model.
812329	Support DVLAN mode 802.1ad and 802.1Q on NP7 platforms, which provides better performance and packet processing.

812993	Support the blocking of a discovered FortiExtender device on a FortiGate configured as a FortiExtender controller using *Reject Status* in the GUI and `set authorized disable` in the CLI.
	`config extension-controller extender`
	`edit <name>`
	`set id <string>`
	`set authorized disable`
	`next`
	`end`

Feature ID	Description
819508	A FortiGate can allow single sign-on (SSO) from FortiCloud and FortiCloud IAM users with administrator profiles inherited from FortiCloud or overridden locally by the FortiGate. Similarly, users accessing the FortiGate remotely from FortiGate Cloud can have their permissions inherited or overridden by the FortiGate.
819583	Add guards to Node.JS log generation and move logs to `tmpfs` to prevent conserve mode issues. Node.JS logs only last a calendar day and will store up to 5 MB of logs. Once this limit is exceeded, the log file is deleted and a new file is created. A delete option has been added to the Node.JS debug command. `# diagnose nodejs logs {list | show <arg> | show-all | delete <arg>}`

827464	The FortiGate device ID is carried by the IKEv2 message NOTIFY payload when it is configured.
	`config vpn ipsec phase1-interface`
	`edit <name>`
	`set dev-id-notification enable`
	`set dev-id <string>`
	`next`
	`end`
	This device ID configuration is required when the FortiGate is configured as a secure edge LAN extension for FortiSASE, and allows FortiSASE to distribute IKE/IPsec traffic according to the FortiGate device ID to achieve load balancing.

829478	Improve replacement message displayed for YouTube videos blocked by video filtering. When a user visits a video directly by URL, a full-page replacement message is displayed. When a user loads a video from YouTube, the page will load but the replacement message will display in the video frame.
836287	Support adding YAML to the file name when backing up the config as YAML, and detecting file format when restoring the configuration. The `execute restore yaml-config` command has been removed and `execute restore config` should be used. In the GUI, the *File format* field has been removed from the *Restore system Configuration* page.

836653	On FortiGates licensed for hyperscale firewall features, the following commands display summary information for IPv4 or IPv6 hardware sessions.
	`# diagnose sys npu-session list-brief`
	`# diagnose sys npu-session list-brief6`

838363	Internet Service Database (ISDB) on-demand mode replaces the full-sized ISDB file with a much smaller file that is downloaded onto the flash drive. This file contains only the essential entries for Internet Services. When a service is used in a firewall policy, the FortiGate queries FortiGuard to download the IP addresses and stores them on the flash drive. The FortiGate also queries the local MAC Database (MADB) for corresponding MAC information.
	`config system global`
	`set internet-service-database on-demand`
	`end`

Feature ID	Description
839877	FortiPolicy can be added to the Security Fabric. When FortiPolicy joins the Security Fabric and is authorized in the *Security Fabric* widget, it appears in the Fabric topology pages. A FortiGate can grant permission to FortiPolicy to perform firewall address and policy changes. Two security rating tests for FortiPolicy have been added to the *Security Posture* scorecard.

849515	Add `auto-discovery-crossover` option under `config vpn ipsec phase1-interface` to block or allow (default) the set-up of shortcut tunnels between different network IDs.
	`config vpn ipsec phase1-interface`
	`edit <name>`
	`set auto-discovery-crossover {allow | block}`
	`next`
	`end`
	When `auto-discovery-crossover` is set to `block` on the auto-discovery sender:
	• In a single hub case, the hub knows the network ID of all the shortcut endpoints.
	• The shortcut offer trigger will be suppressed if IKE detects that the ingress tunnel and egress tunnel have different network IDs.
	When `auto-discovery-crossover` is set to `block` on the auto-discovery receiver:
	• In a multi-hub case, the hub may not know the network ID of the endpoint where traffic is forwarded.
	• Peers will exchange information on whether the shortcut cross-over is allowed.
	• The shortcut initiator will send its network ID and cross-over setting to the shortcut responder in the shortcut query message.
	• The shortcut responder will then send back its own network ID and any error status.
	• If cross-over is not allowed on any side:
	  • The shortcut responder will not allocate a phase 1 and sets the error status in the shortcut reply.
	  • The shortcut initiator will not initiate the shortcut connection if it receives an error in the shortcut reply.
	When `auto-discovery-crossover` is set to `allow`:
	• The cross-over shortcut connection will be initialized with network ID of 0.
	• The non-cross-over shortcut connection will use the configured network ID number.

849771	Support Shielded and Confidential VM modes on GCP where the UEFI VM image is used for secure boot, and data in use is encrypted during processing.
854704	FortiGate VMs with eight or more vCPUs can be configured to have a minimum of eight cores to be eligible to run the full extended database (DB). Any FortiGate VM with less than eight cores will receive a slim version of the extended DB. This slim-extended DB is a smaller version of the full extended DB, and it is designed for customers who prefer performance.
855520	Harden REST API and GUI access.
855561	Use API endpoint domain name from instance metadata to support FortiOS VM OCI DRCC region.
855684	Allow users to configure the RADIUS NAS-ID as a custom ID or the hostname. When deploying a wireless network with WPA-Enterprise and RADIUS authentication, or using the RADIUS MAC authentication feature, the FortiGate can use the custom NAS-ID in its Access-Request.

Feature ID	Description

	`config user radius`
	`edit <name>`
	`set nas-id-type {legacy | custom | hostname}`
	`set nas-id <string>`
	`next`
	`end`

858786	When configuring a CGN IP pool for a hyperscale firewall, exclude IP addresses within this IP pool from being used for source NAT (`excludeip`). This allows users to remain secure and mitigate attacks by ensuring that global IP addresses within a CGN IP pool that are being targeted by external attackers are not re-used by other users of the hyperscale firewall.
	`config firewall ippool`
	`edit <name>`
	`set type cgn-resource-allocation`
	`set startip <IPv4_address>`
	`set endip <IPv4_address>`
	`set excludeip <IPv4_address>, <IPv4_address>, <IPv4_address> ...`
	`next`
	`end`
	This option is currently not supported with a fixed allocation CGN IP pool (when `set cgn-fixedalloc enable` is configured).

860965	Support the AWS T4g instance family with the FG-ARM64-AWS firmware image. Support the AWS C6a and C6in instance families with the FG-VM64-AWS firmware image.

866174	The `wtp-profile` of FAP-432F, FAP-433F, FAP-U432F, and FAP-U433F models can set external antenna parameters when the corresponding external antenna is installed.
	`config wireless-controller wtp-profile`
	`edit <name>`
	`config radio-1`
	`set optional-antenna {none | FANT-04ABGN-0606-O-R | FANT-04ABGN-0606-P-R}`
	`end`
	`next`
	`end`

868164	Implement BIOS-level signature and file integrity checking for important system files and executables. Warn users of failed integrity checks, or prevent the system from booting depending on the severity and BIOS verification level. Kernel and userspace processes can also periodically verify the integrity of AV and IPS engine files, and other important system files and executables. FortiOS firmware and each release of an AV or IPS engine file are dually-signed by Fortinet CA and third-party CAs.
868592	Support Saudi Cloud Computing Company (SCCC) and alibabacloud.sa domain (a standalone cloud backed by AliCloud).

Feature ID	Description
869198	Make the health check sensitive enough to detect small amounts of packet loss by decreasing the link monitor check interval and probe timeout minimum limit down to 20 ms, which will significantly impact VOD/voice.
881186	Support deploying VMware FortiGate VMs directly as a Zero Trust Application Gateway using the OVF template (.vapp). ZTNA related parameters such as EMS server, external and internal interface IPs, and application server mapping can be configured during OVF deployment. ZTNA policies, authentication schemes, rules, and user groups are also bootstrapped.
894191	Improve GUI memory consumption for FortiGates with 2 GB of RAM or less.

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

FortiAnalyzer	• 7.2.3
FortiManager	• 7.2.3
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 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. 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. FortiNAC
13. FortiVoice
14. FortiDeceptor
15. FortiNDR
16. FortiTester
17. FortiMonitor
18. FortiPolicy

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.2.5. When Security Fabric is enabled in FortiOS 7.2.5, all FortiGate devices must be running FortiOS 7.2.5.

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, FortiFlex) 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).

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 7.2.5:

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 7.2.5 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

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 firewall policy`
`  edit 1`
`  set voip-profile "ips_voip_filter"`
`  next`
`  edit 2`
	`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`
	`  edit 1`
	`  set ips-voip-filter "ips_voip_filter"`
	`  next`
	`  edit 2`

Before upgrade	After upgrade

`set voip-profile "sip_alg_profile"`
`next`
`end`
	`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 and 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 7.2.5 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 03011 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	• 6.00288
IPS Engine	• 7.002314

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 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 7.2.5. To inquire about a particular bug, please contact Customer Service & Support.

Anti Spam

Bug ID	Description
857911	The *Anti-Spam Block/Allow List Entry*dialog page is not showing the proper *Type* values in the dropdown.
877613	*Mark as Reject* can be still chosen as an *Action* in an *Anti-Spam Block/Allow List* in the GUI.

Anti Virus

Bug ID	Description
818092	CDR archived files are deleted at random times and not retained.
849020	FortiGate enters conserve mode and the console prints a `fork()` failed message.
851706	Nothing is displayed in the *Advanced Threat Protection Statistics* dashboard widget.
863461	Scanunit displays unclear warnings when AV package validation fails.
869398	FortiGate sends too many unnecessary requests to FortiSandbox and causes high resource usage.
895950	Critical log message, `Fortigate mmdb signature is missing`, is generated on a unit without an AVDB contract.

Application Control

Bug ID	Description
857632	Unable to access to some websites when application control with deep inspection is enabled.

DNS Filter

Bug ID	Description
871854	DNS UTM log still presents unknown FortiGuard category even when the DNS proxy received a rating value.
878674	Forward traffic log is generated for allowed DNS traffic if the DNS filter is enabled but the policy is set to log security events only.

Explicit Proxy

Bug ID	Description
842016	Client gets 304 response if a cached object has varying headers and is expired.
849794	Random websites are not accessible with proxy policy after upgrading to 6.4.10.
865135	Multipart boundary parsing failed with CRLF before the end of boundary 1.
875736	The `proxy-re-authentication-mode` option has been removed in 7.2.4 and is replaced with `proxy-keep-alive-mode re-authentication`. The new `proxy-re-authentication-time` timer is associated with this re-authentication mode. There are two unresolved issues: • After upgrading, the previously configured `proxy-auth-timeout` value for the absolute re-authentication mode is not preserved in the new `proxy-re-authentication-time`. • The new `proxy-re-authentication-time` is currently configured in seconds, but it should be configured in minutes to be consistent with other related authentication timers (such as `proxy-auth-timeout`).
880361	Transparent web proxy policy has no match if the source or destination interface is the same and member of SD-WAN.
901239	Multiple WAD crashes after upgrading firmware to 7.2.4.
901614	Firewall schedule does not work as expected with a proxy policy.

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.

Bug ID	Description
770541	Within the *Policy & Objects* menu, the firewall, DoS, and traffic shaping policy pages take around five seconds to load when the FortiGate cannot reach the FortiGuard DNS servers.
804603	An httpsd singal 6 crash occurs due to `/api/v2/monitor/license/forticare-resllers`.
816493	The `set sub-type ems-tag` option is blocked in HA diff installation.
835413	Inaccurate sFlow interface data reported to PRTG after upgrading to 7.0.
840689	Virtual server aborts connection when `ssl-max-version` is set to `tls-1.3`.
851212	After traffic flow changes to FGSP peer from owner, iprope information for synchronized sessions does not update on the peer side.
854901	Full cone NAT (`permit-any-host enable`) causes TCP session clash.
856187	Explicit FTPS stops working with IP pool after upgrading.
860480	FG-3000D cluster kernel panic occurs when upgrading from 7.0.5 to 7.0.6 and later.
861990	Increased CPU usage in softirq after upgrading from 7.0.5 to 7.0.6.
864612	When the service protocol is an IP with no specific port, it is skipped to be cached and causes a `protocol/port` service name in the log.
865661	Standard and full ISDB sizes are not configurable on FG-101F.
872744	Packets are not matching the existing session in transparent mode.
875565	The policy or other cache lists are sometimes not freed in time. This may cause unexpected policies to be stored in the cache list.
884578	Virtual server stops working after upgrading to 7.2.4.
895962	Virtual server with the HTTP HOST method is crashing WAD.
897849	*Firewall Policy* list may show empty sequence grouping sections if multiple policies are sharing the same `global-label`.
912740	On a FortiGate managed by FortiManager, after upgrading to 7.4.0, the *Firewall Policy* list may show separate sequence grouping for each policy because the `global-label` is updated to be unique for each policy.

FortiGate 6000 and 7000 platforms

Bug ID	Description
838036	Merge FortiGate 6000 and 7000 series platforms.
888873	The FortiGate 7000E and 7000F platforms do not support GTP and PFCP load balancing.
902545	Unable to select a management interface LAG to be the direct SLBC logging interface.

Bug ID	Description
905692	On a FortiGate 6000 or 7000, the active worker count returned by the output of `diagnose sys ha dump-by group` can be incorrect after an FPC or FPM goes down.
905788	Unable to select a management interface LAG to be the FGSP session synchronization interface.

FortiView

Bug ID	Description
838652	The *FortiView Sessions* monitor displays VDOM sessions from other VDOMs.
892798	WAD is crashing and CPU memory is spiking when loading FortiView.

GUI

Bug ID	Description
440197	On the *System* > *FortiGuard* page, the override FortiGuard server for *AntiVirus & IPS Updates* shows an *Unknown* status, even if the server is working correctly. This is a display issue only; the override feature is working properly.
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.
699508	When an administrator ends a session by closing the browser, the administrator timeout event is not logged until the next time the administrator logs in.
722358	When a FortiGate local administrator is assigned to more than two VDOMs and tries logging in to the GUI console, they get a command parse error when entering VDOM configuration mode.
753328	Incorrect shortcut name shown on the *Network* > *SD-WAN* > *Performance SLAs* page.
807197	High `iowait` CPU usage and memory consumption issues caused by report runner.
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.
821030	Security Fabric root FortiGate is unable to resolve firewall object conflicts in the GUI.
821734	*Log & Report* > *Forward Traffic* logs do not show the *Policy ID* if there is no *Policy Name*.
822991	On the *Log & Report* > *Forward Traffic* page, using the filter *Result : Deny(all)* does not work as expected.

Bug ID	Description
827893	Security rating test for *FortiCare Support* fails when connected to FortiManager Cloud or FortiAnalyzer Cloud.
829736	Incorrect information is being displayed for the HA role on the *System* > *HA* page.
829773	Unable to load the *Network* > *SD-WAN* > *SD-WAN Rules* table sometimes due to a JavaScript error.
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.
837048	Unable to delete the LAN interface's addresses without switching it back to a none-LAN role.
842079	On the *System* > *HA* page, a *Failed to retrieve info* caution message appears when hovering over the secondary unit's *Hostname*. The same issue is observed on the *Dashboard* > *Status* > *Security Fabric* widget.
845513	On G-model profiles, changing the platform mode change from single 5G (dedicated scan enabled) to dual 5G is not taking effect.
853414	Policy and dashboard widgets do not load when the FortiGate manages a FortiSwitch with tenant ports (exported from root to other VDOM).
854529	The local standalone mode in a VAP configuration is disabled when viewing or updating its settings in the GUI.
861466	The *Active Administrator Sessions* widget shows the incorrect interface when accessing the firewall through the GUI.
862474	IPsec tunnel interface *Bandwidth* widget inbound is zero and outbound value is lower than the binding interface.
865956	On the *Network* > *Policy Routes* page, entries cannot be copied and pasted above or below.
866790	*System* > *Firmware & Registration* menu is not visible for administrator accounts without read-write permissions for the `sysgrp-permission` category.
867802	GUI always displays *Access denied* error after logging in.
869138	Unable to select addresses in *FortiView* monitors.
869828	An httpsd crash occurs when the GUI fails to get the disk log settings from the FortiGate.
870675	CLI console in GUI reports *Connection lost.* when the administrator has more than 100 VDOMs assigned.
874502	An access privilege prompt is not displayed when logging in to the GUI of a FortiGate managed by a FortiManager with `post-login-banner` enabled. The user is logged in with read-only permissions.
881678	On the *Network* > *Routing Objects* page, editing a prefix list with a large number of rule entries fails with an error notification that *The integer value is not within valid range*.
889647	CLI console disconnects and has `'/tmp/daemon_debug/node_...'` crash.
890531	Node.JS boots earlier than autod, which leads to a Node.JS crash.

Bug ID	Description
890683	GUI being exposed to port 80 on the interfaces defined in the ACME settings, even if administrative access is disabled on the interface.
891895	When remotely accessing the FortiGate from FortiGate Cloud, the web GUI console displays `Connection lost. Press Enter to start a new session.`
897004	On rare occasions, the GUI may display blank pages when the user navigates from one menu to another if there is a managed FortiSwitch present.
899434	A `super_admin` login is logged in the console logs when remotely logging in to a FortiGate with the FortiCloud portal using a `prof_admin` profile.

HA

Bug ID	Description
662978	Long lasting sessions are expired on HA secondary device with a 10G interface.
795443	The `execute reboot` script does not work in HA due to a HA failover before the script running is done.
826790	DHCP over IPsec is not working in an FGSP cluster.
843837	HA A-P virtual cluster information is not correctly presented in the GUI and CLI.
852308	New factory reset box failed to synchronize with primary, which was upgraded from 7.0.
853900	The administrator `password-expire` calculation on the primary and secondary returns a one-second diff, and causes HA to be out-of-sync.
854445	When adding or removing an HA monitor interface, the link failure value is not updated.
855841	In an HA A-P environment, an old administrator user still exists in the system after restoring the backup.
856004	Telnet connection running ping fails during FGSP failover for virtual wire pair with VLAN traffic.
856643	FG-500E interface stops sending IPv6 RAs after upgrading from 7.0.5 to 7.0.7.
860497	Output of `diagnose sys ntp status` is misleading when run on a secondary cluster member.
864226	FG-2600F kernel panic occurs after a failover on both members of the cluster.
868622	The session is not synchronized after HA failover by detecting monitored interface as down.
869557	Upgrading or re-uploading an image to the HA secondary node causes the OS to be `un-certified`.
870367	FGCP A-P devices get out of HA synchronization periodically due to FortiTokens being added and deleted.
872431	Primary FortiGate synchronizes the changing HA command to the secondary.

Bug ID	Description
874823	FGSP `session-sync-dev` ports do not use L2 Ethernet frames but always use UDP, which reduces the performance.
876178	hasync crashing with signal 6 after upgrading to 7.2.3 from 7.0.7.
878173	When downloading the speed test server list, the HA cluster gets and stays out-of-sync.
885245	Unexpected failover occurs due to uptime, even if the uptime difference is less than the `ha-uptime-diff-margin`.
885844	HA shows as being out-of-sync after upgrading due to a checksum mismatch for `endpoint-control fctems`.

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 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.
807523	On NP7 platforms the `config system npu` option for `nat46-force-ipv4-packet-forwarding` is missing.
810366	Unrelated background traffic gets impacted when changing a policy where a hyperscale license is used.
824733	IPv6 traffic continues to pass through a multi-VDOM setup, even when the static route is deleted.
835697	Interface routes under DHCP mode remain in LPMD after moving the interface to another VDOM.
837270	Allowing intra-zone traffic is now supported in hyperscale firewall VDOMs. Options to block or allow intra-zone traffic are available in the GUI and CLI.
841712	On FortiGates licensed for hyperscale firewall features, the `config system setting` options `nat46-force-ipv4-packet-forwarding` and `nat64-force-ipv6-packet-forwarding` now also apply to NP7-offloaded traffic. The `config system npu` option `nat46-force-ipv4-packet-forwarding` has been removed.
877696	Get KTRIE invalid node related error and kernel panic on standby after adding a second device into A-P mode HA cluster.

Intrusion Prevention

Bug ID	Description
839170	IPS engine may crash (`SIGALRM`) when the system is busy because it might not receive enough run time.
842073	High CPU usage for more than 20 minutes and cmdb deadlock after FortiGuard update.
856837	When flow mode AV is enabled, IPS engine memory usage is higher with a large number of flow mode AV requests.
883600	Under `config ips global`, configuring `set exclude-signatures none` does not save to backup configuration.

IPsec VPN

Bug ID	Description
699973	IPsec aggregate shows down status on *Interfaces*, *Firewall Policy*, and *Static Routes* configuration pages.
726326, 745331	IPsec server with NP offloading drops packets with an invalid SPI during rekey.
788751	IPsec VPN Interface shows incorrect TX/RX counter.
797342	Users cannot define an MTU value for the aggregate VPN.
798045	FortiGate is unable to install SA (`failed to add SA, error 22`) when there is an overlap in configured selectors.
810833	IPsec static router gateway IP is set to the gateway of the tunnel interface when it is not specified.
812229	A random four-character peer ID is displayed in the GUI and CLI when a VPN tunnel is formed using IKEv2 if the peer ID is not configured.
828933	iked signal 11 crash occurs once when running a VPN test script.
842571	If `mode-cfg` is used, a race condition can result in an IP conflict and sporadic routing problems in an ADVPN/SD-WAN network. Connectivity can only be restored by manually flushing the IPsec tunnels on affected spokes.
848014	ESP tunnel traffic hopping from VRF.
849515	ADVPN dynamic tunnel is picking a tunnel ID that is within another VPN interface IP range.
852868	Issues with synchronization of the route information (using `add-route` option) on spokes during HA failover that connect to dialup VPN.
855705	NAT detection in shortcut tunnel sometimes goes wrong.

Bug ID	Description
855772	FortiGate IPsec tunnel role could be incorrect after rebooting or upgrading, and causes negotiation to be stuck when it comes up.
858681	When upgrading from 6.4.9 to 7.0.6 or 7.0.8, the traffic is not working between the spokes on the ADVPN environment.
858697	Native IPsec iOS authentication failure using LDAP account with two-factor authentication.
858715	IPsec phase 2 fails when both HA cluster members reboot at the same time.
861195	In IPsec VPN, the fnbamd process crashes when the password and one-time password are entered in the same *Password* field of the VPN client.
869166	IPsec tunnel does not coming up after the upgrading firmware on the branch FortiGate (FG-61E).
873097	Phase 2 not initiating the rekey at soft limit timeout on new kernel platforms.
876795	RADIUS server will reject new authentication if a previous session is missing ACCT-STOP to terminate the session, which causes the VPN connection to fail.
882483	ADVPN spoke does not delete the BGP route entry to another spoke over IPsec when the IPsec VPN tunnel is down.
885818	If a tunnel in an IPsec aggregate is down but its DPD link is on, the IPsec aggregate interface may still forward traffic to a down tunnel causing traffic to drop.
887800	In an L2TP configuration, `set enforce-ipsec enable` is not working as expected after upgrading.
891462	The *Peer ID* field in the *IPsec* widget should not show a warning message that *Two-factor authentication is not enabled*.
892699	In an HA cluster, static routes via the IPsec tunnel interface are not inactive in the routing table when the tunnel is down.
899822	IPsec dialup interface does not appear in the *Interface* dropdown when adding an *Interface Bandwidth* widget.

Log & Report

Bug ID	Description
755632	Unable to view or download generated reports in the GUI if the report layout is custom.
795272	Local out DNS traffic is generating forward traffic logs with `srcintf "unknown-0"`.
823183	FortiGates are showing *Logs Queued* in the GUI after a FortiAnalyzer reboot, even tough the queued logs were actually all uploaded to FortiAnalyzer and cleared when the connection restores.
825318	*Archived Data* tab is missing from intrusion prevention and application control log *Details* pane once `log-packet` is enabled.

Bug ID	Description
828211	Policy ID filter is not working as expected.
829862	On the *Log & Report* > *ZTNA Traffic* page, the client's *Device* ID is shown as *[object Object]*. The Log Details pane show the correct ID information.
836846	Packet captured by firewall policy cannot be downloaded.
838357	A deny policy with log traffic disabled is generating logs.
839601	When log pages are scrolled down, no logs are displayed after 500 lines of logs.
850519	*Log & Report* > *Forward Traffic* logs do not return matching results when filtered with *!<application name>*.
857573	Log filter with negation of destination IP display all logs.
858304	When FortiGate Cloud logging is enabled, the option to display *7 days* of logs is not visible on the *Dashboard* > *FortiView* pages.
858589	Unable to download more than 500 logs from the FortiGate GUI.
860141	Syslog did not update the time after daylight saving time (DST) adjustment.
860264	The miglogd process may send empty logs to other logging devices.
860459	Unable to back up logs (FG-201E).
860487	Incorrect time and time zone appear in the forward traffic log when `timezone` is set to `18` (GMT-3 Brasilia).
861567	In A-P mode, when the link monitor fails, the event log displays a description of `ha state is changed from 0 to 1`.
864219	A miglogd crash occurs when creating a dynamic interface cache on an ADVPN environment.
872181	On the *Log & Report* > *Log Settings* > *Local Logs* page, the *Local reports* and *Historical FortiView* settings cannot be enabled.
872326	FortiGate cannot retrieve logs from FortiAnalyzer Cloud. Results are shown rarely.
873987	High memory usage from miglogd processes even without traffic.
879228	FortiAnalyzer override settings are not taking effect when `ha-direct` is enabled.
906888	Free-style filter not working as defined under `config fortianalyzer override-filter`.

Proxy

Bug ID	Description
707827	The video filter does not display the proper replacement message when the user redirects to a blocked video from the YouTube homepage or video recommendation list.
746587	WAD crashes during traffic scan in proxy mode.

Bug ID	Description
766158	Video filter FortiGuard category takes precedence over allowed channel ID exception in the same category.
781613	WAD crash occurs four times on FG-61F during stress testing.
796150	WAD crashed many times on FG-61F during stress testing.
818371	WAD process crashes with some URIs.
823078	WAD user-info process randomly consumes 100% CPU of one core.
825977	WAD crash occurs on FG-101F during stress testing.
834387	In a firewall proxy policy, the SD-WAN zone assigned to interface is not checked.
835745	WAD process is crashing after upgrading to FortiOS 7.2.1.
843318	If a client sends an HTTP request for a resource which is not yet cached by the FortiGate and the request header contains `Cache-Control: only-if-cached`, then the WAD worker process will crash with signal 11.
853864	FortiGate out-of-band certificate check issue occurs in a proxy mode policy with SSL inspection.
854511	Unable to make API calls using Postman Runtime script after upgrading to 7.2.0.
855853	WAD crashes frequently and utilizes high CPU.
855882	Increase in WAD process memory usage after upgrading.
856235	The WAD process memory usage gradually increases over a few days, causing the FortiGate to enter into conserve mode.
857368	WAD crashed while parsing a Huffman-encoded HTTP header.
857507	WAD crash with signal 11 occurs after to upgrading.
858148	Memory leak in WAD user info history daemon.
870151	WAD memory leak occurs on TCP port and HTTP tunnel session port.
870554	WAD crash occurs with explicit proxy when IPv6 is enabled.
874563	WAD has signal 11 crash when attempting to merge user information attributes.
880712	WAD crashed with signal 11.
885674	Unable to send logs from FortiClient to FortiAnalyzer when deep inspection is enabled on firewall policy.
886284	Application WAD signal 11 crash occurs.

REST API

Bug ID	Description
725048	Improve performance for `/api/v2/monitor/system/available-interfaces` (phase 2).
847526	Able to add incomplete policies with empty mandatory fields using the REST API.
849273	`/api/v2/monitor/system/certificate/download` can still download already deleted CSR files.
864393	High CPU usage of httpsd on FG-3600E HA system.
886012	Setting the MTU fails when a port is defined by the API.
892237	Updating the HA monitor interface using the REST API PUT request fails and returns a -37 error.

Routing

Bug ID	Description
708904	`No IGMP-IF for ifindex` log points to multicast enabled interface.
724468	Router policy destination address not take effect when `internet-service-id` is configured.
821149	Early packet drop occurs when running UTM traffic on virtual switch interface.
827565	Using `set load-balance-mode weight-based` in SD-WAN implicit rule does not take effect occasionally.
893603	GUI does not show gateway IP on the routing table page if VDOM mode is transparent.
846107	IPv6 VRRP backup is sending RA, which causes routing issues.
848310	IPsec traffic sourced from a loopback interface does not follow the policy route or SD-WAN rules.
850778	Spoke-to-spoke communication randomly breaks. The BGP route to reach the spoke subnet points to the main ADVPN tunnel instead of the shortcut tunnel.
850862	When creating a new rule on the *Network* > *Routing Objects* page, the user cannot create a route map with a rule that has multiple similar or different AS paths in the GUI.
860075	Traffic session is processed by a different SD-WAN rule and randomly times out.
862165	FortiGate does not add the route in the routing table when it changes for SD-WAN members.
862418	Application VWL crash occurs after FortiManager configuration push causes an SD-WAN related outage.
862573	SD-WAN GUI does not load, and the lnkmtd process crashes frequently.
863318	Application forticron signal 11 (Segmentation fault) received.

Bug ID	Description
865914	When BSM carries multiple CRPs, PIM might use the incorrect prefix to update the mroute's RP information.
870983	Unable to set `local-as` in BGP confederation configuration.
883918	Delay in joining `(S,G)` in PIM-SM.
884372	All BGP routes in dual ADVPN redundant configuration are not getting updated to the correct WAN interface post-rollback to WAN failover.
890379	After upgrading, SD-WAN is unable to fail over the traffic when one interface is down.
897940	Link monitor's probe timeout value range is not appropriate when the user decreases the minimum interval.

Security Fabric

Bug ID	Description
753177	IoT device vulnerabilities should be included in security ratings.
809106	*Security Fabric* widget and *Fabric Connectors* page do not identify FortiGates properly in HA.
814796	The threat level threshold in the compromised host trigger does not work.
819192	After adding a Fabric device widget, the device widget does not appear in the dashboard.
825291	Security rating test for *FortiAnalyzer* fails when connected to FortiAnalyzer Cloud.
832015	Root FortiGate cannot finish the security rating with a large Fabric topology (more than 25 to 30 devices) because the REST API is not limited to the local network.
844412	When a custom LLDP profile has `auto-isl` disabled, the security rating test, *Lockdown LLDP Profile*, fails.
848822	The *FortiAP Firmware Versions* and *FortiSwitch Firmware Versions* security rating tests fail because the firmware version on the FortiAPs and FortiSwitches is not recognized correctly.
851656	Sessions with `csf_syncd_log` flag in a Security Fabric are not logged.
852340	Various places in the GUI do not show the secondary HA device.
862532	Unable to load topology pages for a specific Security Fabric topology on the root and downstream FortiGates.
867313	*Error triggering automation stitch* message appears when the license expiry notification type is *FortiGuard Web Filter*.
868701	In a simple cluster, the primary unit failed to upgrade to 7.2.3.
870527	FortiGate cannot display more than 500 VMs in a GCP dynamic address.

Bug ID	Description
875100	Unable to remove external resource in a certain VDOM when the external resource has no reference in that VDOM.
880011	When the Security Fabric is enabled and `admin-https-redirection` is enabled on a downstream FortiGate, the following GUI features do not work for the downstream FortiGate when the administrator manages the downstream FortiGate using the root FortiGate's GUI: • Web console access • Diagnostic packet capture • GUI notification when a new device joins or leaves the Security Fabric • GUI notification if a configuration on the current page changes These features still work for the root FortiGate's GUI.
885810	The gcpd daemon constantly crashes (signal 11 segmentation fault).
887967	Fabric crashes when synchronizing objects with names longer than 64 characters.
907172	Automation stitch with FortiDeceptor Fabric connector event trigger cannot be triggered.

SSL VPN

Bug ID	Description
710657	The `dstaddr`/`dstaddr6` of an SSL VPN policy can be set to `all` when split tunnel mode is enabled and only the default portal is set.
719740	The *No SSL-VPN policies exist* warning should not be shown in the GUI when a zone that has ssl.root as a member is set in an SSL VPN policy.
746440	When sending the SSL VPN settings email (*VPN* > *SSL-VPN Settings* > *Send SSL-VPN Configuration*), the *Email* template only includes a hyperlink to the configuration, which is not supported by Gmail and Fortinet email.
748085	Authentication request of SSL VPN realm can now only be sent to user group, local user, and remote group that is mapped to that realm in the SSL VPN settings. The authentication request will not be applied to the user group and remote group of non-realm or other realms.
787768	The `web-mode` setting should not be enabled when the portal is mapped in an SSL VPN policy where a VIP is applied.
808107	FortiGate is not sending Accounting-Request packet that contains the Interim-Update AVP when two-factor authentication is assigned to a user (defined on the FortiGate) while connecting using SSL VPN.
810239	Unable to view PDF files in SSL VPN web mode.
819754	Multiple DNS suffixes cannot be set for the SSL VPN portal.
828194	SSL VPN stops passing traffic after some time.

Bug ID	Description
839261	On the *VPN* > *SSL-VPN Settings* page, when the `source-address-negate` option is enabled for an address in the CLI, the GUI does not display an exclamation mark against that address entry in the *Hosts* field. This is cosmetic and does not affect on the FortiGate functionality or operation. The `source-address-negate` option being enabled can be confirmed in the CLI.
850898	OS checklist for the SSL VPN in FortiOS does not include macOS Ventura (13).
852566	User peer feature for one group to match to multiple user peers in the authentication rules is broken.
854143	Unable to access Synology NAS server through SSL VPN web mode.
854642	Internal website with JavaScript is proxying some functions in SSL VPN web mode, which breaks them.
856316	Browser displays an *Error, Feature is not available* message if a file larger than 1 MB is uploaded from FTP or SMB using a web bookmark, even though the file is uploaded successfully. There are no issues with downloading files.
856554	SSL VPN web mode top-right dropdown button (user profile menu) does not work.
859115	SSL VPN bookmark not accessible.
863860	RDP over SSL VPN web mode to a Windows Server changes the time zone to GMT.
864096	EcoStruxure Building Operations 2022 does not render using SSL VPN bookmark.
864417	In the second authentication of RADIUS two-factor authentication, the `acct-update-interval` returned is `0`. SSL VPN uses the second return and not send RADIUS `acct-interim-update` packet.
867182	RDP/VNC host name is not encrypted when URL obscuration is enabled.
870061	Kernel does not delete original route after address assigned to the client changes.
873313	SSL VPN policy is ignored if no user or user group is set and the FSSO group is set.
873995	Problem with the internal website using SSL VPN web mode.
877896	When accessing the VDOM's GUI in SSL VPN web mode, policies are only shown for a specific VDOM instead of all VDOMs.
884860	SSL VPN tunnel mode gets disconnected when SSL VPN web mode is disconnected by `limit-user-logins`.
890876	One of the speed-connect website JavaScript files has trouble with host process.

Switch Controller

Bug ID	Description
730472	FortiSwitch enabled VLANs with VLAN and proxy ARP access have large latencies on initial ARP resolutions.

Bug ID	Description
762615, 765283	FortiSwitches managed by FortiGate go offline intermittently and require a FortiGate reboot to recover.
769722	Support FortiLink to recognize a FortiSwitch based on its name and not just by serial number.
853718	Layer 3 FortiLink does not come up after upgrading.
854104	FortiLink daemon keeps pushing the configuration to FortiSwitch for a long time when the FortiSwitch is deleted and re-discovered.
857778	Switch controller managed switch port configuration changes do not take effect on the FortiSwitch.
858113	On the *WiFi & Switch Controller* > *Managed FortiSwitches* page, when an administrator with restricted access permissions is logged in, the *Diagnostics and Tools* page for a FortiSwitch cannot be accessed.
876021	FortiLink virtually managed switch port status is not getting pushed after the FortiGate reboots.
886887	When a MAC VLAN appears on the same MCLAG trunk, continuous event logs are received on FortiGate and FortiAnalyzer.

System

Bug ID	Description
550701	WAD daemon signal 11 causes cmdbsvr deadlock.
649729	HA synchronization packets are hashed to a single queue when `sync-packet-balance` is enabled.
666664	Interface belonging to other VDOMs should be removed from interface list when configuring a GENEVE interface.
700621	The forticron daemon is constantly being restarted.
709679	Get `can not set mac address(16)` error message when setting a MAC address on an interface in HA that is already set.
713951	Not all ports are coming up after an LAG bounce on 8 × 10 GB LAG with ASR9K. Affected platforms: FG-3960E and FG-3980E.
722273	SA is freed while its timer is still pending, which leads to a kernel crash.
724085	Traffic passing through an EMAC VLAN interface when the parent interface is in another VDOM is blocked if NP7 offloading is enabled. If `auto-asic-offload` is disabled in the firewall policy, then the traffic flows as expected.
729912	DNS proxy does not transfer the DNS query for IPv6 neighbor discovery (ND) when client devices are using random MAC addresses, so one device can configure many IPv6 addresses.
748496	Wrong IP displayed in GUI widget if FortiGuard anycast AWS is used.

Bug ID	Description
776646	On the *Network* > *Interfaces* page, configuring a delegated interface to obtain the IPv6 prefix from an upstream DHCPv6 server fails with an error notification (*CLI internal error*).
784169	When a virtual switch member port is set to be an alternate by STP, it should not reply with ARP; otherwise, the connected device will learn the MAC address from the alternate port and send subsequent packets to the alternate port.
790595	Improve dnsproxy process memory management.
799570	High memory usage occurs on FG-200F.
805122	In FIPS-CC mode, if `cfg-save` is set to `revert`, the system will halt a configuration change or certificate purge.
807629	NP7 `dos-offload` triggers an established TCP session to have synproxy process issues.
810137	Scheduled speed test crash is caused by adding the same object to a list twice.
810879	DoS policy ID cannot be moved in GUI and CLI when multiple DoS policies are enabled.
812957	When setting the `speed` of 1G SFP ports on FG-180xF platforms to `1000full`, the interface does not come up after rebooting.
813607	LACP interfaces are flapping after upgrading.
815937	FCLF8522P2BTLFTN transceiver is not working after upgrade.
818897	The value of SNMP OID IP-MIB (RFC 4293) is inaccurate.
820268	VIP traffic access to the EMAC VLAN interface uses incorrect MAC address on NP7 platform.
826490	NP7 platforms may reboot unexpectedly when unable to handle kernel null pointer de-reference.
827240	FortiGate in HA may freeze and reboot. Before the reboot, softIRQ may be seen as high. This leads to a kernel panic.
828129	A disabled EMAC VLAN interface is replying to a ping.
836409	When deleting a non-existing entry, the error code returned is not appropriate.
838933	DoS anomaly has incorrect threshold after loading a modified configuration file.
840960	When kernel debug level is set to `>=KERN_INFO` on NP6xLite platforms, some tuples missing debug messages may get flooded and cause the system to get stuck.
845736	After rebooting the FortiGate, the MTU value on the VXLAN interface was changed.
847314	NP7 platforms may encounter random kernel crash after reboot or factory reset.
850683	Console keeps displaying `bcm_nl.nr_request_drop ...` after the FortiGate reboots because of the `cfg-save revert` setting under `config system global`. Affected platforms: FG-10xF and FG-20xF.
850688	FG-20xF system halts if setting `cfg-save` to `revert` under `config system global` and after the `cfg-revert-timeout` occurs.
852562	Huge configuration files cause delays during the booting process.

Bug ID	Description
853144	Network device kernel null pointer is causing a kernel crash.
853794	Issue with the `server_host_key_algorithm` compatibility when using SSH on SolarWinds.
853811	Fortinet 10 GB transceiver LACP flapping when shut/no shut was performed on the interface from the switch side.
854388	Configuring `set src-check disable` is not persistent in the kernel after rebooting for GRE interfaces.
855573	False alarm of the PSU2 occurs with only one installed.
855775	Time zone for Kyiv, Ukraine is missing.
856202	Random reboots and kernel panic on NP7 cluster when the FortiGate sends a TCP RST packet and IP options are missing in the header.
859717	The FortiGate is only offering the `ssh-ed25519` algorithm for an SSH connection.
859795	High CPU utilization occurs when relay is enabled on VLAN, and this prevents users from getting an IP from DHCP.
860052	The 40G/100G port goes down on FG-260xF when upgrading to 7.2.
860385	IPv6 BGP session drops when passing through a FortiGate configured with VRF.
862941	GUI displays a blank page if `vdom-admin` user has partial permissions.
867435	FG-400E-BP has crash at `initXXXXXXXXXXX[1]: segfault at 3845d5a` after package validation fails.
867978	Subnet overlap error occurs when configuring the same IPv4 link-local addresses on two different interfaces.
868225	After a cold reboot (such as a power outage), traffic interfaces may not come up with a possible loss of VLAN configurations.
868821	`execute ssh-regen-keys` should be global-level command.
869599	Forticron memory is leaking.
870381	Memory corruption or incorrect memory access when processing a bad WQE.
875868	HQIP test fails on FG-2201E.
876853	No output of `execute sensor list` is displayed after rebooting.
876874	The *Dashboard* > *Status* > *Sensor Information* widget does not load.
877039	On the *Network* > *BGP* page, creating or editing a table entry increases memory consumption of the FortiGate to 99%.
877154	FortiGate with new kernel crashes when starting debug flow.
877240	Get `zip conf file failed -1` error message when running a script configuring the FortiGate.

Bug ID	Description
878400	When traffic is offloaded to an NP7 source MAC, the packets sent from the EMAC VLAN interface are not correct.
880290	NP7 is not configured properly when the ULL ports are added to LAG interface, which causes accounting on the LAG to not work.
881094	FG-3501F NP7 is dropping all traffic after it is offloaded.
882187	FortiGate enters conserve mode in a few hours after enabling UTM on the policies.
883071	Kernel panic occurs due to null pointer dereference.
887772	High CPU usage after upgrade to 7.2.4, WAD crashes continuously.
889634	Unable to configure IPv6 setting on system interface (FWF-81F-2R-POE).
891841	Unable to handle kernel NULL pointer dereference at `0000000000000000` for NP7 device; the device keeps rebooting.
899884	FG-3000F reboots unexpectedly with NULL pointer dereference.
909345	Kernel panic occurs when receiving ICMP redirect messages.

Upgrade

Bug ID	Description
850691	The `endpoint-control fctems` entry `0` is added after upgrading from 6.4 to 7.0.8 when the FortiGate does not have EMS server, which means the `endpoint-control fctems` feature was not enabled previously. This leads to a FortiManager installation failure.
892647	Static route configurations were lost upgrading from 7.0.7 to 7.2.3.
900761	FG-601E crashes randomly after upgrading to 7.0.8 and 7.0.11.

User & Authentication

Bug ID	Description
751763	When MAC-based authentication is enabled, multiple RADIUS authentication requests may be sent at the same time. This results in duplicate sessions for the same device.
823884	Searching in *User & Authentication* > *User Definition* shows results from other groups.
843528	RADIUS MAC authentication using ClearPass is intermittently using old credentials.
846545	LDAPS connectivity test fails with old WinAD after OpenSSL was upgraded to 3.0.2.

Bug ID	Description
853793	FG-81F 802.1X MAC authentication bypass (MAB) failed to authenticate Cisco AP.
855898	All devices are detected as *Other identified device* in the *Device Inventory* widget.
856370	The EAP proxy worker application crashes frequently.
857438	SSL VPN group matching does not work as expected for Azure auto login.
858961	Client's firewall authentication session timeout is set to 900 when it passes MAC authentication bypass by ping.
859845	In some cases, the proper hostnames are not showing up when looking at APs on the FortiSwitch ports screen.
864703	ACME client fails to work with some CA servers.
865166	A cid scan crash occurs when device detections happen in a certain order.
867225	ARP does not trigger FortiGuard device identification query.

VM

Bug ID	Description
740796	IPv6 traffic triggers `<interface>: hw csum failure` message on CLI console.
856645	Session is not crated over NSX imported object when traffic starts to flow.
859165	Unable to enable FIPS cipher mode on FG-VM-ARM64-AWS.
859589	VPNs over Oracle Cloud stop processing traffic.
860096	CPU spike observed on all the cores in a GCP firewall VM.
868698	During a same zone AWS HA failover, moving the secondary IP will cause the EIP to be in a disassociated state.
869359	Azure auto-scale HA shows certificate error for secondary VM.
878074	FG-ARM64-GCP and FG-ARM64-AZURE have HA synchronization issue with internal IP after failover.
881728	Kernel hangs on FG-VM64-AZURE.
883203	FG-AWS SDN is unable to retrieve EKS cluster information, even thought its role is trusted by the EKS role.
883896	Backup virtual server not working as expected (`ERR_EMPTY_RESPONSE`).
885829	Azure SDN connector stopped processing when Azure returned `NotFound` error for VMSS interface from an AD DS-managed subscription.
890278	FG-VM Rackspace On-Demand upgrade from 7.2.3 to 7.2.4 breaks the pay-as-you-go license, and reverts it to an evaluation license.

Bug ID	Description
902816	Azure kernel panic occurs after a failover on the cluster.
912184	`RIP: 0010:storvsc_queuecommand+0x57d/0x` is observed after deploying an FG-VM64-AZURE in Standard_DS4_v2 size.

VoIP

Bug ID	Description
757477	PRACK will cause voipd crashes when the following conditions are met: `block-unknown` is disabled in the SIP profile, the PRACK message contains SDP, and PRACK fails to find any related previous transactions (this is not a usual case).

Web Filter

Bug ID	Description
766126	Block replacement page is not pushed automatically to replace the video content when using a video filter.
856793	In flow mode, URL filter configuration changes cause a spike in CPU usage of the IPS engine process.
863728	The urlfilter process causes a memory leak, even when the firewall policy is not using the web filter feature.
878442	FortiGuard block page image (logo) is missing when the `Fortinet-Other` ISDB is used.

WiFi Controller

Bug ID	Description
807605	FortiOS exhibits segmentation fault on hostapd on the secondary controller configured in HA.
821320	FG-1800F drops wireless client traffic in L2 tunneled VLAN with `capwap-offload` enabled.
825182	The 6 GHz channel lists should be updated according to the latest WiFi country region channels map.
828901	Connectivity loss occurs due to switch and FortiAPs (hostapd crash).
831736	Application hostapd crash found on FG-101F.

Bug ID	Description
834644	A hostapd process crash is shown in device crash logs.
835783	CAPWAP traffic is not offloaded when re-enabling `capwap-offload`.
837130	Wireless client shows portal related webpage while doing MAC authentication with MAB mode.
846730	*Dynamic VLAN assignment* is disabled in the GUI when editing an SSID with `radius mac-auth` and `dynamic-vlan` enabled.
856038	The `voice-enterprise` value changed after upgrading.
856830	HA FortiGate encounters multiple hostapd crashes.
857084	Hostapd segmentation fault signal 6 occurs upon HA failover.
857140	Hostapd segmentation fault signal 11 occurs upon RF chamber setup.
857975	The cw_acd process appears to be stuck, and is sending several access requests for MAC authentication.
858653	Invalid wireless MAC OUI detected for a valid client on the network.
861552	Wireless client gets disconnect from WiFi if it is connected to a WPA2 SSID more than 12 hours.
865260	Incorrect source IP used in the self-originating traffic to RADIUS server.
868022	Wi-Fi clients on a RADIUS MAC MPSK SSID get prematurely de-authenticated by the secondary FortiGate in the HA cluster.
882551	FortiWiFi fails to act as the root mesh AP, and leaf AP does not come online.
891625	Quarantined STA connected to a long interface name VAP is not moved to quarantined VLAN 4093.
892575	MPSK SSID with `mpsk-schedules` stopped working after the system time was changed due to daylight saving time.

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.
859421	ZTNA server (access proxy VIP) is causing all interfaces that receive ARP request to reply with their MAC address.
863057	ZTNA real server address group gets unset once the FortiGate restarts.

Bug ID	Description
865316	Adding an EMS tag on the *Policy & Objects* > *Firewall Policy* edit page for a normal firewall policy forces NAT to be enabled.
875589	WAD crash observed when a client EMS tag changes.
887307	WAD crashes after upgrading to 7.2 (build 1336 and later).

Known issues

The following issues have been identified in version 7.2.5. To inquire about a particular bug or report a bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
908706	On the *Security Profiles* > *AntiVirus* page, a VDOM administrator with a custom administrator profile cannot create or modify an antivirus profile belonging to the VDOM. **Workaround**: set the VDOM administrator profile to *super_admin*.

Explicit Proxy

Bug ID	Description
817582	When there are many users authenticated by an explicit proxy policy, the *Firewall Users* widget can take a long time to load. This issue does not impact explicit proxy functionality.
877337	HTTPS requests over IPv6 are not matched sometimes to the proxy policy when the IPv6 Internet Service Database is applied in the proxy policy.

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`

Firewall

Bug ID	Description
843554	If the first firewall service object in the service list (based on the order in the command line table) has a protocol type of *IP*, the GUI may incorrectly modify its protocol number whenever a new firewall service of the same protocol type *IP* is created in the GUI.

Bug ID	Description

	This silent misconfiguration can result in unexpected behavior of firewall policies that use the impacted service. For example, some 6K and 7K platforms have firewall service *ALL* (protocol type *IP*) as the first service, and this can cause the *ALL* service to be modified unexpectedly.
	Workaround: create a new service in the CLI, or move a non-IP type services to the top of the firewall service list. For example, if `ALL` is the first firewall service in the list:
	`config firewall service custom`
	`edit "unused"`
	`set tcp-portrange 1`
	`next`
	`move "unused" before "ALL"`
	`end`

FortiGate 6000 and 7000 platforms

Bug ID	Description
909163	Local logging support is needed on all SLBC models.

GUI

Bug ID	Description
825598	A `Node exiting due to unhandled rejection: TypeError [ERR_INVALID_URL]: Invalid URL` error message appears in the debug crash log for the node process. This error does not impact the GUI operation.
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.
898902	In the *System* > *Administrators* dialog, when there are a lot of VDOMs (over 200), the dialog can take more than one minute to load the *Two-factor Authentication* toggle. This issue does not affect configuring other settings in the dialog. **Workaround**: use the CLI to configure `two-factor-authentication` under `config system admin`.

HA

Bug ID	Description
818432	When private data encryption is enabled, all passwords present in the configuration fail to load and may cause HA failures.

Hyperscale

Bug ID	Description
802182	A `cmdb_txn_cache_data(query=log.npu-server,leve=1) failed` error is seen after editing an interface's VLAN ID.
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.

IPsec VPN

Bug ID	Description
916260	The IPsec VPN tunnel list can take more than 10 seconds to load if the FortiGate has large number of tunnels, interfaces, policies, and addresses. This is a GUI display issue and does not impact tunnel operation.

Log & Report

Bug ID	Description
860822	When viewing logs on the *Log & Report* > *System Events* page, filtering by *domain\username* does not display matching entries. **Workaround**: use a double backslash (*domain\\username*) while filtering or searching by username only without the domain.

Proxy

Bug ID	Description
837724	WAD crash occurs.

Routing

Bug ID	Description
907386	BGP neighbor group configured with password is not working as expected.

SSL VPN

Bug ID	Description
795381	FortiClient Windows cannot be launched with SSL VPN web portal.

Switch Controller

Bug ID	Description

904640	When a FortiSwitch port is reconfigured, the FortiGate may incorrectly retain old detected device data from the port that results in an unexpected number of detected device MACs for the port. Using `diagnose switch-controller mac-cache show` to check the device data can result in the *Device Information* column being blank on the *WiFi & Switch Controller* > *FortiSwitch Ports* page or in the *Assets* widget.
	Workaround: disable the device retention cache to remove old device data.
	`config switch-controller global`
	`  set mac-retention-period 0`
	`end`

911232	Security rating shows an incorrect warning for unregistered FortiSwitches on the *WiFi & Switch Controller* > *Managed FortiSwitches*. **Workaround**: select a FortiSwitch and use the *Diagnostics & Tools* tooltip to view the correct registration status.

System

Bug ID	Description
884023	When a user is logged in as a VDOM administrator with restricted access and tries to upload a certificate (*System* > *Certificates*), the *Create* button on the *Create Certificate* pane is greyed out.
887940	Status light is not showing on the FortiGate 60F or 100F after a cold reboot.

Web Filter

Bug ID	Description
885222	HTTP session is logged as HTTPS in web filter when VIP is used.

WiFi Controller

Bug ID	Description
814541	When there are extra large number of managed FortiAP devices (over 500) and large number of WiFi clients (over 5000), the *Managed FortiAPs* page and *FortiAP Status* widget can take a long time to load. This issue does not impact FortiAP operation.
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.
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.
904349	Unable to create FortiAP profile in the GUI for dual-5G mode FortiAP U231F/U431F models. **Workaround**: use the CLI to update the profile to dual-5G mode.

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