Release Notes

FortiOS 7.2.11

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

February 12, 2025
FortiOS 7.2.11 Release Notes
01-7211-1114580-20250212

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-02-12	Initial release.

Introduction and supported models

This guide provides release information for FortiOS 7.2.11 build 1740.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.2.11 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-DSL, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-90G, FG-91E, FG-91G, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-120G, FG-121G, 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-80F-2R-3G4G-DSL, FWF-81F-2R, FWF-81F-2R-3G4G-DSL, 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

Special branch supported models

The following models are released on a special branch of FortiOS 7.2.11. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1740.

FGT-30G	is released on build 6542
FWF-30G	is released on build 6542

FortiGate 6000 and 7000 support

FortiOS 7.2.11 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.

FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 7.2.11 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 7.2.11 features.

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.

Hyperscale NP7 hardware limitation

Because of an NP7 hardware limitation, for CGN traffic accepted by a hyperscale firewall policy that includes an overload with port block allocation (overload PBA) IP Pool, only one block is allocated per client. The setting of the hyperscale firewall policy `cgn-resource-quota` option is ignored.

Because of this limitation, under certain rare conditions (for example, only a single server side IP address and port are being used for a large number of sessions), port allocation may fail even if the block usage of the client is less than its quota. In cases such as this, if the client has traffic towards some other servers or ports, additional port allocation can become successful. You can also work around this problem by increasing the IP Pool block size (`cgn-block-size`).

Changes to NP7 traffic shaping

The following known issues for the Queuing based Traffic Management (QTM) module on NP7 are fixed:

- Incorrect checksum for fragments after QTM.
- Packets longer than 6000 bytes cause QTM to hang.
- Refreshing causes QTM to hang.
- MTU is not honored after QTM, so the packet is not fragmented.

As a result of these changes, you can no longer use the following command to change QoS type used for traffic shaping for sessions offloaded to NP7 processors:

```
config system npu
    set default-qos-type {policing | shaping}
end
```

Instead, `default-qos-type` can only be set to `policing`.

For NP7 sessions, policy traffic shaping, per-IP shaping, and regular port shaping (outbandwidth enabled on an interface without a shaping profile) always use the NP7 accounting and traffic shaping module (called the TPE module). This is the same as changing the `default-qos-type` to `policing`.

For NP7 sessions, shaping profiles on interfaces now only use QTM for traffic shaping (equivalent to setting `default-qos-type` to `shaping`). Shaping profiles on interfaces are also called Multiclass shaping (MCS). The interface can be a physical interface, LAG interface, and VLAN interface (over physical or LAG). The FortiGate supports shaping profiles on a maximum of 100 interfaces.

Changes in default behavior

Bug ID	Description
1063233	The BIOS security level is updated from levels 0/1/2 to levels Low and High. Level High will correspond to previous behaviors in level 2, and level Low will correspond to behaviors in level 1. BIOS that still uses levels 0 will now behave like level 1/Low.

New features or enhancements

More detailed information is available in the New Features Guide.

Feature ID	Description
1061119	This enhancement reduces ipshelper CPU usage during the database update process, optimizing system performance and ensuring smoother operations.

Upgrade information

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

Multiple upgrade methods are available for individual FortiGate devices and multiple FortiGate devices in a Fortinet Security Fabric:

FortiGate	Upgrade option	Details
Individual FortiGate devices	Manual update	Use the procedure in this topic. See also Upgrading individual devices in the FortiOS Administration Guide.
	Automatic update based on FortiGuard upgrade path	See Enabling automatic firmware updates in the FortiOS Administration Guide for details
Multiple FortiGate devices in a Fortinet Security Fabric	Manual, immediate or scheduled update based on FortiGuard upgrade path	See Fortinet Security Fabric upgrade on page 14 and Upgrading Fabric or managed devices in the FortiOS Administration Guide.

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

FortiAnalyzer	• 7.2.10
FortiManager	• 7.2.10
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 16
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 7.2.11. When Security Fabric is enabled in FortiOS 7.2.11, all FortiGate devices must be running FortiOS 7.2.11.

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 7.2.11:

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 7.2.11 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. Check the *Cluster Status* dashboard widget or use the `diagnose sys confsync status` command to confirm that all components are synchronized and operating normally.

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.

FortiGates with ULL ports may expereince status down on active ports

After upgrading to FortiOS version 7.2.9, FortiGate platforms with ultra-low-latency (ULL) ports like 600F and 901G models may experience link status down on active ULL ports if the following conditions are met:

- The ULL port is set to 25G mode
- Forward error correcting (FEC) is enabled on the port
- Forward error correcting (FEC) is disabled on the connecting switch

This behaviour change is due to a fix in FortiOS 7.2.9 version for an issue where FEC feature was disabled even though it was enabled in the CLI. This allowed the FortiGate ULL port to still connect to the switch with FEC disabled. After the fix, FEC is activated on the ForitGate and caused a mismatch with the switch.

Workaround: User can disable FEC feature on the FortiGate ULL port to match with the connecting switch, or they can enable FEC feature on the switch to match with the FortiGate side.

```
config system interface
    edit <ULL port>
        set forward-error-correction disable
    next
end
```

SLBC FG-5001E primary blade fails to install image

For FG-5001E in a session-aware load balanced cluster (SLBC), all secondary blades install the image successfully. However, the primary blade fails, showing a `sync timeout` error, even with `graceful-upgrade` disabled.

Product integration and support

The following table lists FortiOS 7.2.11 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 0319 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	• 6.00303
IPS Engine	• 7.00357

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

Anti Spam

Bug ID	Description
1050805	When spam mail is received from the server, POP connection times out.

Anti Virus

Bug ID	Description
1068321	MMDB and AVAI DBs are unsigned after upgrading from version 7.0.15 to version 7.2.9.
1073326	Entry-level FortiGate's with 2GB of memory encounter a memory usage issue and do not operate as expected caused by the scanunit initiating an AV engine restart.
1078882	The scanunit tries to scan with no payload, resulting in an error message from FortiNDR and generating an error on FortiGate.

Application Control

Bug ID	Description
1015616	Packets may be dropped by the anti-reply function due to it being partially offloaded.

DNS Filter

Bug ID	Description
1100282	Chrome flex OS cannot access glowscotland.sharepoint.com when using FortiGate DNS servers.

Explicit Proxy

Bug ID	Description
1015722	WAD auto-tuning is not working ideally for various cases, resulting in throughput for single file downloads not reaching the ideal speed when `tcp-window-type` is set to `auto-tuning`.
1067291	Applications do not connect over explicit proxy if deep-inspection profile is applied.
1079152	Socks Proxy Traffic is not logged in Forward Traffic log.

File Filter

Bug ID	Description
1011320	Adding File Filter to a flow-based firewall policy may impact performance.

Firewall

Bug ID	Description
910946	`diffserv-forward` does not work well for IPv6 TCP/UDP offloaded traffic.
923715	DSCP in packet is removed for TCP/UDP NAT66 IPv6 traffic when NPU offloaded.
951422	Corner case: failure to download file from web server with Proxy mode inspection and AV/IPS enabled.
966466	On an FG-3001F NP7 device, packet loss occurs even on local-in traffic.
985508	When `allow-traffic-redirect` is enabled, redirect traffic that ingresses and egresses from the same interface may incorrectly get dropped if the source address of the incoming packet is different from the FortiGate's interface subnet and there is no firewall policy to allow the matched traffic.
992610	The source interface displays the name of the VDOM and local out traffic displays as forward traffic.
996622	On FortiGate, the IPv6 real server shown as DOWN by the health check but it is considered UP in the kernel.
1025078, 1086315	Some customers observed a memory usage increase and issues with client sessions not disconnecting when using virtual servers.
1028356	Reordering the DNAT policies in the central NAT causes a false hit count.
1050864	No route is found when the FTP server connects back to FTP client in FTP active mode.
1050906	sflowd daemon killed every minute, and improper netflow data seen on scrutinizer.

Bug ID	Description
1059989	Modifying the shaping profile, whether it is assigned to an interface or not, results in IPsec tunnels going down.
1060452	FortiGate in policy-based mode showing the incorrect policy ID in forward traffic logs.
1068393	Incorrect matching of zones and SD-WAN zones occurs where interfaces do not exist.

1078662	If an interface on an NP7 platform has the `set inbandwidth XXX`, `set outbandwidth XXX`, and `set egress-shaping-profile XX` settings, the following issues may occur:
	• Fragment packet checksum is incorrect.
	• MTU is not honored when sending packets out.
	• QTM hangs and blocks traffic when packet size is larger than 6000 bytes.
	Workaround:
	`config system interface`
	`    edit xx`
	`        unset egress-shaping-profile`
	`    next`
	`end`

1079590	Intermittent reply traffic is not sent out of FortiGate.
1081542	On FortiGate, packets are dropped when ASIC offloading is enabled.
1088507	ICMP responses do not follow the incoming interface for traffic directed to FortiGate when virtual-patch is enabled.
1098208	After FortiGate exits conserve mode, some policies failed to install into the kernel at the same time.
1101301	Monitor API firewall/address-fqdns6 returns 0 count and empty resolved IP.
1103748	A threat feed configured as a source cannot match security policy in a policy-based FortiGate.
1104208	loadbalancer real server IP address exposed to internet.
1106112	Small platforms cannot remove FFDB shared memory files.
1112628	External connector for IP database is not working in security policy.

FortiGate 6000 and 7000 platforms

Bug ID	Description
949175	During FIM failover from FIM2 to FIM1, the NP7 PLE sticks on a cache invalidation, stopping traffic.
976521	On FortiGate 6000 models, a CPU usage issue occurs in the node process when navigating a policy list with a large number (+7000) of policies in a VDOM.
1057499	FIM interfaces are DOWN after restoring the root VDOM configuration due to a speed issue.
1060619	CSF is not working as expected.

Bug ID	Description
1081015, 1086953	The secondary 7K slot 3 (FPM) has no ISDB database and will not update.
1086889	FIM encounters a split-brain scenario after rebooting.
1088402	On FortiGate 6K/7K FGSP clusters, the configuration does not synchronize properly with `standalone-config-sync` enabled.
1095936	Different sensors appear in the list of FIM1 and FIM2.
1097428	Unable to see the Security Profile menu in the global VDOM in the GUI. The CLI is not impacted.
1098811	Process crashing on slot2.
1102481	Local-in remote access issues due to incorrect destination address.
1103739	The cmdsvr process is monopolizing the CPU, and FPCs are out of synchronization with MBD on primary and secondary devices.
1103958	Some autoupdate DB versions are not updated properly causing the blades to go out of synchronization.
1105009	`execute load-balance slot manage <slot-id>` does not work as expected.
1109415	New SNMP MIB table for chassis sensor.

GUI

Bug ID	Description
937939	Unable to disable automatic patch upgrade in the setup wizard on some FortiGate models or on FortiGates managed by FortiManager.
941723	An error occurred when attempting to perform interface migration from a physical interface containing a VLAN interface to an aggregate interface.
985287	The Interface Bandwidth widget for PPPoE interfaces does not show current details.
1019750	The available interfaces list is slow in configurations with many IPsec tunnel connections.
1035356	The WAN interface is accessible in the GUI under certain interface configurations even though it is not allowed in the configuration file.
1044745	On the *Dashboard* > *User & Devices* page on a VDOM, the *Address* column shows multiple devices with the FortiGate VLAN gateway instead of the Client IP.
1047963	High Node.js memory usage when building FortiManager in Report Runner fails. Occurs when FortiManager has a slow connection, is unreachable from the FortiGate (because FMG is behind NAT), or the IP is incorrect.
1092475	On the *Policy & Objects* > *Firewall Policy* page, in the *Edit Policy* dialog, the GTP-profile do not display in the GUI when Central SNAT is enabled.

Bug ID	Description
1097263	Antivirus and webfilter profiles cannot be selected in a policy in the GUI. Affected platforms: FGT-30G and FWF-30G.
1099309	Security Rating endpoint will serve temporary files as they are being written to the file system.
1102404	VDOM search function does not work properly if VDOM has uppercase letters.
1110382	Admin can log in to GUI (HTTPS) with password, even when *admin-https-pki-required* is enabled.
1114658	Improve Node.js health check from forticron to use IPC server in Node.js rather than HTTP server.

HA

Bug ID	Description
830538	FGCP FortiGates go out-of sync when the certificates used for IPsec are updated using SCEP.
908490	When a peer joins an FGSP group, existing sessions on the primary unit will not auto-sync to the backup unit.
965217	In an HA configuration, FortiGate may experience intermittent heartbeat loss causing unexpected failover to the secondary unit.
965813, 1007917	Authorizing a FortiExtender causes FortiOS HA out-of-sync and inability to connect to secondary FGT after failover.
982081	After changing the status to down on the ha1 and ha2 ports, setting the status back to up does not bring up the ports. **Workaround:** Reboot the FortiGate.
985967	Session synced with FGSP does not allow immediate failover when UTM is enabled in flow mode.
996977	A factory reset 6KF device became out-of-sync after composed the HA due to a rule.fmwp mismatch.
998004	When the HA management interface is set a LAG, it is not synchronized to newly joining secondary HA devices.
1047094	The HA Secondary unit cannot communicate with FortiGate Cloud when it uses *standalone-mgmt-vdom* using the HA Primary unit.
1054041	On FortiGate's in an HA environment, DHCP clients can not get an IPv4 address from the server with vcluster.
1056138	On FortiGate 120G and 121G models in an HA cluster, if the `ha` or `mgmt` interface is used as the heartbeat interface, the HA cluster may not synchronize and the GUI HA page may not load.
1060006	The `standalone-config-sync` conf-member kept out-of-synchronization after an upgrade and configuration change.

Bug ID	Description
1060023	FortiGate in an HA environment encounters a CPU usage issue on FGSP cluster members with more than 200000 session running.
1062433	SASE FortiGate's go out of synchronization after `HTTP.Chunk.Length.Invalid` was removed in the new FMWP package.
1084662	FFDB signatures keep flapping on all blades except the master FIM of the primary chassis.
1088956, 1101490	>Logs for one arm sniffer interface are sent to FAZ from both HA cluster members.
1091189	The passive member in an A-A HA sends traffic with the virtual mac.
1095786	No GARPs are sent out for associated active hosts' MAC addressess in a VWP when an A-P HA failback.
1100177	In an FGSP setup, on asymmetric TCP flow during SYN/ACK packet on the other member, the TCP MSS value is not adjusted according to the firewall policy.
1101456	Aggregate interface status is not consistent with the configured admin status.

ICAP

Bug ID	Description
1072282	ICAP may encounter a *400 Bad Request* error with certain websites due to an absent reason-phrase when converting from HTTP/2 to HTTP/1.

Intrusion Prevention

Bug ID	Description
1061119	ipshelper CPU usage reduced during the database update process, optimizing system performance and ensuring smoother operations.
1090134	IPS engine re-initialization after receiving a threat feed update from an external resource.
1107445	Remove IPS diagnose command `diagnose ips cfgscript run`.

IPsec VPN

Bug ID	Description
930571	SD-WAN health-check on ADVPN shortcut does not work after HA failover.
942618	Traffic does not pass through an `vpn-id-ipip` IPsec tunnel when wanopt is enabled on a firewall policy.
951667	A crash might happen during the rekey of the initiator.
1002345	IKE daemon randomly does not operate as expected during phase1 rekeying depending on soft rekey margin, timing, and packet ordering.
1018749	IPsec inserted SA's are not deleted successfully after flushing all tunnels.
1023871	IPSec IKEv2 with SAML cannot match the Entra ID group during EAP due to a buffer size issue.
1027537	On the SOC4 platform, L2TP & ETHERIP traffic does not traverse through an IPSec tunnel with NP offload enabled.
1031985	IPSec VPN tunnel does not go down when the VPN peer route is removed from the routing table.
1033154	FortiGate does not unregister the `net_device` causing the unit to encounter a performance issue.
1039988	When performing a SAML authentication, authd gets stuck in a loop due to a CPU usage issue.
1042324	The Phase1 monitor BGP remains active when the tunnel is DOWN.
1042465	VPN interface error counter increases, traffic intermittent when NPU acceleration is enabled globally.
1054440	Incrementing TX and RX errors on VPN interface.
1059778	IPsec does not work as expected when the traffic path is `spoke dialup` to `hub1`, then from `hub1` to another site using a site-to-site tunnel.
1061925	IPsec tunnels are flushed when unrelated changes are made in the system.
1071769	L2TP/IPsec connection FortiGate-Windows Native VPN client breaks after the Windows client initiates the ISAKMP SA renegotiation.
1073670	An `IkEd` crash on secondary causes IPsec client to reconnect.
1076636	Unexpected behavior in IKED occurs when a peer attempts to negotiate with two different gateway profiles simultaneously.
1080164	The `tcp-mss` setting on the tunnel interface does not take effect for IPv6 traffic.
1082624	EAP doe snot work as expected for local users inherited from the policy. RADIUS users can authenticate and the tunnel can be established.
1093588	Issue with deleting an IPsec tunnel created automatically when FX is connected to FortiGate.

Log & Report

Bug ID	Description
871142	SAML SSO administrator login with post-login banner enabled does not have a login event.
1001583	On the *Log & Report* > *Forward Traffic* page, the GUI experiences a performance issue and reverts to the last input when multiple ports are added to a filter for destination ports.
1008626	ReportD does not function as expected when event logs have message fields over 2000 bytes.
1024570	The SSH deep-inspection with `unsupported-version bypass > log information` is not showing.
1031342	On the *Security Traffic Log* > *Security* tab, the *Details* page displays data with a *1/500 log fetched* prompt.
1045253	FortiGate logs are not transferred into FortiGate Cloud Log server.
1060204	When the threat feed download times out, a system event log is not generated.
1083537	The FortiAnalyzer serial number disappears from the FortiGate configuration when the OFTP session disconnects.
1084934	Firewall logs show *Object Object* in GUI and `dstintf="unknown-0"` in raw logs.
1088385	FortiGate intermittently loses the FortiAnalyzer serial number and is required to verify again the FortiAnalyzer serial number and certificate.
1091064	Forward traffic does not contain the `poluuid` and `policyname` fields.

Proxy

Bug ID	Description
894755	WAD daemons memory increases when a firewall policy configuration changes.
914128	In protecting server SSL profile, cannot change server certificate order.
916178	FortiGate encounters an issue with the WAD daemon when deep inspection and SSL exemption are enabled while visiting a server with an expired certificate.
983997	If two root CA have the same information in Subject and Issuer but different public key and SN, FortiGate cannot validate.
988473	On FortiGate 61E and 81E models, a daemon WAD issue causes high memory usage.
1008079	Memory usage increase for WAD process.
1018780	FortiGate encounters a memory usage issue caused by the WAD process after an upgrade.
1020828	An HTTP2 stream issue causes an error condition in the WAD.

Bug ID	Description
1023127	WAD crashes on the FortiGates with signal 11.
1039006	Some websites cannot open subpages when the HTTP2 header value exceeds 16MB.
1042055	On FortiGate, an interruption occurs in the WAD process when in proxy-mode causing the unit to go into memory conserve mode.
1047441	On FortiGate, the WAD process may not work as expected with H2 traffic when creating UTM logs.
1048296	FortiGate experiences an HTTP2 framing error when accessing websites using proxy mode with deep inspection configured due to a frame sizing issue in the WAD process.
1051875	The IP SNI check for `strict sni-server-cert-check` is skipped due to a WAD process issue.
1064758	The *Protocol* option tcp window size in a proxy policy does not work as expected.
1066113	Some websites not loading when inspection mode is proxy.
1067942	An error occurs in the WAD process when DoH traffic is sent to a transparent proxy after enabling HTTP policy redirect, and without having a transparent proxy configured.
1096728	For FortiGate in Azure environments, WAD crash affects some VIP traffic.

REST API

Bug ID	Description
984499	REST API query `/api/v2/monitor/system/ha-peer` does not return the primary attribute of an HA cluster member.
989677	Update JavaScripts to the latest Long Term Support version.
1074529	FortiGate is unable to rename the `Address` object with API `cmdb/firewall/address/` and Workspace mode transactions.
1081018	Monitor API firewall/address-fqdns6 returns 0 count and empty resolved IP (CLI is okay).

Routing

Bug ID	Description
885362	If SD-WAN set `tie-break` as `fib-best-match`, increase the size of candidate path for ECMP.
935297	Probe server `aws.amazon.com` is listed in SD-WAN default health-check list.
952140	DNS over TCP local-out traffic can match SD-WAN rule with specifying UDP protocol.

Bug ID	Description
988498	Multicast traffic flow is not functioning as expected when static-join is used.
1031394	On the *Network* > *Routing Objects* page, the *Set AS path* on the *Edit Rule* pane does not allow the use of the full range AS numbers.
1048338	On FortiGate in an HA setup the secondary HA passive device generates unexpected logs.
1049721	When BGP enables local-as-replace-as and there is a network loop condition, the NLRI's as-path is increased indefinitely.
1057135	The gateway/offload value of offloaded one-way UDP sessions is reset when unrelated routing changes are made.
1057474	FortiGate does not generate a PIM register after stopping and starting a multicast stream.
1057504	FortiGate encounters a multicast routing issue in a VRRP environment.
1058700	SD-WAN rule in load-balance mode limited to 8 active SD-WAN members.
1069060	Routes are not displayed correctly when the BGP configuration is in a specific order.
1072311	L2P TPE drops, triggering BGP sessions flap.
1084907	IPv6 routes are inactive when dual stack BFD is configured.
1085271	An IGMP membership report with a `0.0.0.0` source does not work as expected in kernel 4.19.13.
1119119	Application bgpd crashes with signal 11 due to freeing appling routemaps.

Security Fabric

Bug ID	Description
940489	Issue with importing endpoint groups from Cisco ACI Management Tenant with FortiManager direct connector.
987531	Threat Feed connectors in different VDOMs cannot use the source IP when using internal interfaces.
1037951	The Security Fabric widget shows the serial number instead of the hostname.
1040700	The external connector only allows users to specify the interface in the root vdom and not the vdom it is configured in.
1041855	kubed crashed with signal 6 (Aborted) when testing kubernetes sdn connector during robot auto test.
1056262	With a FortiGate configured with a `root-vdom` and a `mgmt-vdom`, when an automation stitch is configured for a compromised host with IP-Ban action, the IP is banned from the `mgmt-vdom`.
1057862	On the *Security Fabric* > *Automation* page, webhook requests use the same `Content-Type: application/json` in HTTP headers for all requests, even if it has a custom header.

Bug ID	Description
1082980	The AZURE type dynamic firewall address takes longer than normal to resolve itself, even with the correct filter value in the robot test bed.
1103566	In a Security Fabric with 70 downstream FortiGates, fabric management fails to load due to long FAP and FSW firmware API.
1113463	FortiGate Azure connector fails to retrieve AKS information on AKS 1.29.5.

SSL VPN

Bug ID	Description
888149	When `srcaddr6` contains `addrgrp6`, sslvpnd crashes after dual-stack tunnel is established.
937704	FortiGate encounters a memory usage issue when bringing down multiple SSL VPN tunnels with multiple RADIUS users.
993822	After a SAML user is connected to SSL VPN, an incorrect Framed-IP-Address is set in the radius accounting packet.
1000674	When generating function backtrace in crash logs for ARM32, SSL VPN frequently crashes due to segmentation faults.
1012486	SSL VPN OS checklist does not include minor version numbers of macOS 13 and 14.
1077157	FortiGate sends out expired server certificate for a given SSL VPN realm, even when the certificate configured in `virtual-host-server-cert` has been updated.
1078149	Internal resources cannot be accessed using FortiClient after a network disruption.
1082427	The OS checklist for SSL VPN in FortiOS does not include macOS Sequoia 15.0.
1101837	Insufficient session expiration in SSL VPN using SAML authentication.

Switch Controller

Bug ID	Description
960240	On the *WiFi & Switch Controller > Managed FortiSwitches* page, ISL links do not display as solid connections.
1063144	FortiGate 101F default FortiLink interface has no members.
1064814	Random CPU spikes and for cu_acd process
1113465	The VLAN is randomly not getting assigned on FSW port using DPP policy.

System

Bug ID	Description
860460	On a redundant interface, traffic may drop with some NPU-offload enabled policies when the interface is not initialized properly.
880629	System unresponsive when running traffic while stopping IPS and nturbo.
897520	Application newcli signal 11.
900686	newcli crash when executing debug commands followed by TAC report.
900936	fnbamd heap corruption causes crashes in several different places.
901721	In a certain edge case, traffic directed towards a VLAN interface could cause a kernel interruption.
907752	On FortiGate 1000D models, the SFP 1G port randomly experiences flapping during operation.
910551	System unresponsive during SSL VPN test.
916940	Cannot enable monitoring bandwidth for more than 23 interfaces.
920320	FortiGate encounters increasing `Rx_CRC_Errors` on SFP ports on the NP6 platform when an Ethernet frame contains carrier extension symbols to Cisco devices.
932077	Connection issue between SOC4 platform and Hirschmann GRS 105 switches since SOC4 doesn't support certain carrier extension signals.
944744	TCP traffic failed on FortiGate 4800F when going through emac-vlan.
948875	The passthrough GRE keepalive packets are not offloaded on NP7 platforms.
955998	The traffic is dropped when `auto-asic-offload` is enabled and passing through a VLAN associated with a 10G redundant interface.
960707	Egress shaping does not work on NP when applied on the WAN interface.
975895	FortiGate locks when *Configuration save mode* is set to *Manual* and triggers a reboot.
983467	FortiGate 60F and 61F models may experience a memory usage issue during a FortiGuard update due to the ips-helper process. This can cause the FortiGate to go into conserve mode if there is not enough free memory.
984696	Network usage is not accurately reported by the `get system performance status` command.
992323, 1056133, 1075607, 1082413, 1084898	Traffic interrupted when traffic shaping is enabled on 9xG and 12xG.
997001	Threat feed received "400 Bad Request" when fetching the external resource file through IPV6.
999816	FortiGate 100 models may become unresponsive and prevent access to the GUI, requiring a reboot to regain access due to an issue with the SOC3.

Bug ID	Description
1006685	FortiGate enters a loop cycle and generates a large number of LCAP packets when FortiGate does not receive LCAP packets from a peer device.
1008022	After a restarting FortiGate from the GUI, the `auto-nego` SFP port settings are not reflected in FortiGate.
1012577	Traffic on WAN interface is dropped when `policy-offload-level` (under `config system setting`) is set to `dos-offload`.
1013010	On some FortiGates, 25 GB transceivers are displayed as 10 GB transceivers in the `get system interface transceiver` command.
1015736	On FortiWiFi 60/61F models, the STATUS LED light does not turn on after rebooting the device.
1017446	Some TTL exceeded packets are not forwarded on their destination and an error message is not always generated.
1017941	On the FortiGate 220xE and 330xE, the GUI interface bandwidth show terabyte spike for gigabyte interface.
1018843	When FortiGate experiences a memory usage issue and enters into conserve mode, the system file integrity check may not work as expected and cause the device to shutdown.
1020921	When configuring an SNMP trusted host that matches the management *Admin* trusted host subnet, the GUI may give an incorrect warning that the current SNMP trusted host does not match. This is purely a GUI display issue and does not impact the actual SNMP traffic.
1025114	Insufficient free memory on entry-level Fortigate devices with 2 GB RAM may cause unexpected behavior in the IPS engine.
1025576	Passthrough GRE traffic using Transparent Ethernet Bridging packets as the protocol type are not offloaded on NP7 platforms.
1025927	In an HA configuration, FortiGate cannot access the GUI after a firmware upgrade due to a certificate matching issue.
1029447	FortiGate encounters increasing `Rx_CRC_Errors` on SFP ports on the NP6 platform when an Ethernet frame contains carrier extension symbols to Cisco devices.
1032018	The SFP+ port LED does not illuminate and displays a speed 10Mbps even though the link status up and speed is set to 1000Mbps.
1032602	FortiGate encounters a memory usage issue on DNS proxy, resulting in FortiGate going into conserve mode.
1041165	The MAC Authentication Bypass (MAB) does not initiate on a virtual switch due a kernel configuration issue.
1044178	FortiGate does not return an ICMP message with type *unreachable* and code `packet too big` with the vne-tunnel.
1048496	On FortiGate, the `snmp` daemon does not work as expected resulting in the SNMP queries timing out.
1048684	Vmalloc size is not enough on 100E model.

Bug ID	Description
1050883	Backing up a configuration using SFTP with the domain username does not work when characters @ and \ are in the username.
1050908	In some scenarios, when FortiGate as a DHCP client sends out `DHCP-REQUEST` packets, the SRC IP address is set in the IP header.
1053195	FortiGate is locked up when manual mode is configured and the config revert is triggered.
1054294	FortiGate reboots after a connected HA heartbeat cable is connected, or running the `diag hardware deviceinfo nic ha` command.
1056174	FortiOS processes packets on a non-active port of a redundant link.
1057131	A FortiGuard update can cause the system to not operate as expected if the FortiGate is already in conserve mode. Users may need to reboot the FortiGate.
1057625	FortiGate does not work as expected due to an interruption in the kernel.
1058740	Unexpected behavior observed in entry-level FortiGate models, including FortiGate VMs with less than 2 GB of RAM, during system updates due to memory allocation issue.
1061334	FortiGate returns a string with a *%* sign for the OID *1.3.6.1.4.1.12356.101.4.8.2.1.8* (*fgLinkMonitorPacketLoss*).
1061413	`EXPIRE` dates are not displayed properly when executing the `get sys fortiguard-service status` command due to a formatting issue.
1061796	Inaccurate inbound and outbound traffic values on the *Bandwidth* widget for the EMAC VLAN interface.
1062698	DNSproxy CPU is running high.
1063017	FortiGate factory reset via script from FortiManager not working.
1064241	FortiGate 100E series models sometimes get unresponsive.
1065553	FortiGate 80F-DSL models display the incorrect connected route.
1068150	The DHCP relay uses the wrong interface to send DHCP offer packets to the client.
1075032	On FortiGate, NP7 offloaded traffic does not use the MAC address of a new default gateway to forward traffic using the EMAC-VLAN interface.
1075116	Admin user is logged out unexpectedly from the console when using a configuration tool.
1076883	When the top application bandwidth feature is disabled, the GUI process still performs the initial check for application bandwidth, which may cause FortiCron to experience high CPU usage.
1078568	SN in get message does not match the subject CN or SAN in the peer's certificate.
1080641	With FortiGate Cloud central management with public DNS server, when configuring FortiGate Cloud as central management for the FortiGate, the GUI shows a misleading message saying the FortiGate needs to use FortiGuard DNS. This is inaccurate, as the FortiGate Cloud service can work with any public DNS server.
1082838	System unresponsive triggered by CPU profiling across all cores.

Bug ID	Description
1090372	Cannot create more than seven access profile entries on a FortiGate 40F.
1095834	Memory usage of node process continues to increase.
1096409	EXPIRE dates cannot be displayed properly when displaying the output of `get sys fortiguard-service status`.
1104410	1G SFP port does not come up on the FortiGate 120G.

Upgrade

Bug ID	Description
1102990	SLBC FortiGate 5001E primary blade failed to install image, even though graceful-upgrade was disabled.

User & Authentication

Bug ID	Description
1003373	FortiGate experiences a gradual memory usage issue in the fnbamd process.
1004258	The Strict-SNI SSL Profile might block TCP connections if the SNI cannot be verified due to an active probe failure.
1009884	FortiGate encounters a CPU usage issue in the `authd` process after a firmware upgrade.
1018846	When SCEP is used with SSL connections, some TLS connections are missing the SNI extension on FortiGate.
1042326	On FortiGate, the `two-factor-email-expiry` setting in the `config system global` command is not applicable for administrators.
1043222	CMPv2 IR does not work as expected due to server certification validation error conditions.
1044084	On the *Dashboard > Firewall User Monitor* page, the *Search* field does not display in the GUI when there are a large number (+1000) FSSO user logos.
1045753	An ACME certificate enrollment error is generated without detailed error message information.
1075627	On the *User & Authentication > RADIUS Servers* page, the *Test Connectivity* and *Test User Credentials* buttons may incorrectly return a *Can't contact RADIUS server* error message when testing against a RADIUS server that requires the `message-authentication` attribute in the access request from the FortiGate. This is a GUI display issue as the actual RADIUS connection does send the `message-authentication` attribute.

Bug ID	Description
1080234	For FortiGate (versions 7.2.10 and 7.4.5 and later) and FortiNAC (versions 9.2.8 and 9.4.6 and prior) integration, when testing connectivity/user credentials against FortiNAC that acts as a RADIUS server, the FortiGate GUI and CLI returns an *invalid secret for the server* error. This error is expected when the FortiGate acts as the direct RADIUS client to the FortiNAC RADIUS server due to a change in how FortiGate handles RADIUS protocol in these versions. However, the end-to-end integration for the clients behind the FortiGate and FortiNAC is not impacted.
1080510	When using SCEP, the auto renewal certificate is not initiated.
1111303	Cannot see any LLDP neighbors on the FortiGate 90G.

1112718	When RADIUS server has the require-message-authenticator setting disabled, The GUI RADIUS server dialogs *Test connectivity* and *Test user credentials* still check for the message-authenticator value and incorrectly fail the test with *missing authenticator* error message.
	`config user radius`
	`    edit <radius server>`
	`        set require-message-authenticator disable`
	`    next`
	`end`
	This is only a GUI display issue and the end-to-end integration with RADIUS server should still work.

VM

Bug ID	Description
1001940	A new created FGT-VM64 could not configure the vapp options settings.
1012000	When unicast HA setup has a large number of interfaces, FGT Hyper-V takes a long time to boot up.
1012927	When FortiGate returns an *ICMP TTL-EXCEEDED* message, the `geneve` option field header is missing.
1042973	Multiple cores reporting high CPU on GCP.
1054244	FortiToken does not work as expected after moving a FortiGate-VM license to a new VM with the same serial number.
1072695	The VLAN interface is not reachable on a FortiGate VM running KVM with Intel 10G NIC (10Gb ethernet card).
1082197	The FortiGate-VM on VMware ESXi equipped with an Intel E810-XXV network interface card (NIC) using SFP28 transceivers at 25G speed is unable to pass VLAN traffic when DPDK is enabled.
1085482	On FGT-VM-AZURE, dpdk@mlx4 is not supported anymore but needs graceful processing.
1107962	OCI Dynamic addresses are being removed/added every few seconds.

Web Filter

Bug ID	Description
1026023	The webfilter and traffic logs show the incorrect realserver IP address due to a WAD process issue.
1038995	Content filtering is not working when ALPN HTTP/2 is enabled with SSL deep inspection.
1054334	Clone default webfilter profile via GUI does not copy action settings properly for some categories.
1099818	Output of `diagnose webfilter fortiguard cache dump` command shows the message "Cache is not enabled".

WiFi Controller

Bug ID	Description
946796	The eap_proxy daemon may keep reloading randomly due to failing to bind a port. This will cause an IKE and WiFi authentication failure.
1001104	FortiAP units repeated joining and leaving FortiGate HA cluster when the secondary FortiGate has stored FortiAP images.
1028181	Wi-Fi devices would encounter service delay when roaming over captive-portal SSID with MAC-address authentication.
1049471	On FortiGate 90G and 120G models, traffic is dropped due to the MAC address of the VAP interface being updated with the old MAC address when HA is enabled.
1050915	On the *WiFi & Switch Controller > Managed FortiAPs* page, when upgrading more than 30 managed FortiAPs at the same time using the *Managed FortiAP* page, the GUI may become slow and unresponsive when selecting the firmware.
1062060	Uzbekistan not in -P, Lower -P 5G power to 20dB EIRP and -P w 6G ch1-93 23dB EIRP not enabled.
1073390	FortiGate generates duplicate WiFi event logs when `set cw_acd multi-core(set acd-process-count)` is enabled.
1075138	On FortiGate, the *Source IP* shown in the system logs is not referenced anywhere in the network.

ZTNA

Bug ID	Description
936353	FortiClient registered on multiple-tenants enabled EMS ztna-tcp-forwarding traffic was sometimes denied when enable user-auth.

Bug ID	Description
1026930	An interruption occurs in the WAD process causing TCP connections to stop for ZTNA proxy policies.
1056179	PPPoE encounters a performance issue after an upgrade.

Known issues

Known issues are organized into the following categories:

- New known issues on page 41
- Existing known issues on page 42

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

New known issues

The following issues have been identified in version 7.2.11.

FortiGate 6000 and 7000 platforms

Bug ID	Description
1062080	SNMP query returns an error when there is a large number of BGP routes.
1078334	Automated backups appending device serial number to file.
1096156	Device is randomly unreachable through GUI.
1108181	confsyncd daemon crash.

FortiView

Bug ID	Description
1123502	FortiView Threats: drilling down to malicious website entry returns *Failed to retrieve FortiView data from disk*.

System

Bug ID	Description

1087270	Unexpected traffic increase over the FortiGate 6000 base backplane.
	Workaround: disable `allow-traffic-redirect` and `ipv6-allow-traffic-redirect`:
	`config system global`
	`    set allow-traffic-redirect disable`
	`    set ipv6-allow-traffic-redirect disable`
	`end`

Existing known issues

The following issues have been identified in a previous version of FortiOS and remain in FortiOS 7.2.11.

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	The GUI-explicit-proxy setting on the *System* > *Feature Visibility* page is not retained after a FortiGate reboot or 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 temporarily disable the WAD debugging process (when FortiGate reboots, this process will need to be disabled again). `diagnose wad toggle` (use direct connect diagnose)
1059899	When setting `sec-default-action` to `accept` on an initial explicit web proxy configuration after a factory reset, incoming traffic does not match the proxy policy and allows all traffic to pass. **Workaround**: set `sec-default-action` to `deny` first in the CLI and then change the setting to `accept`.

Firewall

Bug ID	Description

1117165	Leaving the `apn` field empty in a GTP APN traffic shaping policy means that the policy will not match any traffic. Consequently, APN traffic shaping can only be applied to specific APNs.
	To configure GTP APN traffic shaping:
	`config gtp apn-shaper`
	`    edit <policy-id>`
	`        set apn [<apn-name> <apngrp-name> ...]`
	`        set rate-limit <limit>`
	`        set action {drop | reject}`

Bug ID	Description

	`        set back-off-time <time>`
	`    next`
	`end`

FortiGate 6000 and 7000 platforms

Bug ID	Description
790464	After a failover, ARP entries are removed from all slots when an ARP query of single slot does not respond.
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.
1056894	On the FortiGate 6000 platform, IPv6 VRF routing tables appear under the new and old FPC primary units when the primary FPC slot is changed.

1070365	FGCP HA session synchronization may stop working as expected on a FortiGate 7000F cluster managed by FortiManager. This happens if the HA configuration uses management interfaces as session synchronization interfaces by configuring the `session-sync-dev` option, for example:
	`config system ha`
	`    set session-sync-dev 1-M1 1-M2`
	`end`

Bug ID	Description

	The problem occurs when FortiManager updates the configuration of the FortiGate 7000F devices in the cluster it incorrectly changes to the VDOM of the management interfaces added to the `session-sync-dev` command from `mgmt-vdom` to `vsys_ha` and the interfaces stop working as session sync interfaces.
	You can work around the problem by manually changing the vdom of the management interfaces added to `session-sync-dev` to mgmt-vdom and then retrieving the FortiGate configuration from FortiManager.
	`config system interface`
	`    edit 1-M1`
	`        set vdom mgmt-vdom`
	`    next`
	`    edit 1-M2`
	`        set vdom mgmt-vdom`
	`    next`
	`end`

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.
974988	FortiGate GUI should not 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).
989512	When the number of users in the *Firewall User* monitor exceeds 2000, the search bar, column filters, and graphs are no longer displayed due to results being lazily loaded.
993890	The `Node.JS` daemon restarts with a `kill ESRCH` error on FortiGate after an upgrade.
999972	Edits that are made to *IP Exemptions* in *IPS Signatures and Filters* more than once on the *Security Profiles* > *Intrusion Prevention* page are not saved.
1055197	On FortiGate G series models with dual WAN links, the *Interface Bandwidth* widget may show an incorrect incoming and outgoing bandwidth count where the actual traffic does not match the display numbers.

HA

Bug ID	Description
781171	When performing HA upgrade in the GUI, if the secondary unit takes several minutes to bootup, the GUI may show a misleading error message *Image upgrade failed* due to premature timeout. This is just a GUI display issue and the HA upgrade can still complete without issue.

Bug ID	Description
970316	When adding a new vcluster, the `link-failure` value of the newly added vcluster is not updated, causing the wrong primary unit to be selected.
988944	On the *Fabric Management* page, the HA Secondary lists both primary and secondary FortiGate units.

1072440	Special branch supported models of FortiGate in an HA cluster with an empty HA password, upgrading from a special build GA version (version 7.0.x) to version 7.2.9 and version 7.2.10 GA can cause one of the members to not upgrade.
	Impacted models: Please see a full list of *Special branch supported models* for FortiOS version 7.0.15.
	Workaround: configure a valid HA password for the cluster before the upgrade, or manually upgrade the member that was impacted.
	`config system ha`
	`    set password <new-password>`
	`end`
	Setting the password causes an HA cluster re-election to occur.

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.

Intrusion Prevention

Bug ID	Description
1069190	After upgrading to FortiOS version 7.2.9, FortiGate may experience a CPU usage issue due to IPS engine version 7.00342 when there is a large amount of proxy inspected traffic using the application control and IPS sensor. **Workaround**: downgrade the IPS engine to version 7.00341, or upgrade the device to FortiOS 7.4.6 or later.

IPsec VPN

Bug ID	Description
944600	CPU usage issues occurred when IPsec VPN traffic was received on the VLAN interface of an NP7 vlink.

Proxy

Bug ID	Description
910678	CPU usage issue in WAD caused by a high number of devices being detected by the device detection feature.

REST API

Bug ID	Description
1004136	Unable to fetch more than 1000 logs using an REST API GET request.

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.
924693	On the *Network > SD-WAN > SD-WAN Rules* page, member interfaces that are down are incorrectly shown as up. The tooltip on the interface shows the correct status.
1025201	FortiGate encounters a duplication issue in a hub and spoke configuration with `set packet-duplication force` enabled on a spoke and `set packet-de-duplication` enabled on the hub.

Security Fabric

Bug ID	Description
903922	Security Fabric physical and logical topology is slow to load when there are a lot of downstream devices, including FortiGates, FortiSwitches, FortiAPs, and endpoint device traffic. This is a GUI only display issue and does not impact operations of downstream devices.
1011833	FortiGate experiences a CPU usage issue in the node process when there multiple administrator sessions running simultaneously on the GUI in a Security Fabric with multiple downstream devices. This may result in slow loading times for multiple GUI pages. **Workaround**: disconnect the other concurrent administrator sessions to avoid overloading node process.
1120652	Fabric topology with two devices on different VDOMs but behind the same router show wrong VDOM data on tooltip. **Workaround**: disable `device-identification` on that interface.

SSL VPN

Bug ID	Description
795381	FortiClient Windows cannot be launched with SSL VPN web portal.
941676	Japanese key input does not work correctly during RDP in SSL VPN web mode.

Switch Controller

Bug ID	Description
947351	The FortiSwitch topology is not loading correctly on the GUI.
961142	An interface in FortiLink is flapping with MCLAG with DAC on an OPSFPP-T-05-PAB transceiver.

System

Bug ID	Description
782710	Traffic going through a VLAN over VXLAN is not offloaded to NP7.
882862	On FortiGate 400F, 600F, 900G, 3200F, and 3700F models, LAG interface members are not shutting down when the remote end interface (one member in the LAG) is admin down.
901621	On the NP7 platform, setting the interface configuration using `set inbandwidth <x>` or `set outbandwidth <x>` commands stops traffic flow. **Workaround**: unset the `inbandwidth` and `outbandwidth` in the CLI: `config system interface`

<table>
<tr><th>Bug ID</th><th>Description</th></tr>
<tr><td></td><td><pre>   edit <port>
        unset inbandwidth
        unset outbandwidth
    next
end</pre></td></tr>
<tr><td>921604</td><td>On the FortiGate 601F, the ports (x7) have no cables attached but the link LEDs are green.</td></tr>
<tr><td>1045866</td><td>The <code>node</code> daemon causes a CPU usage and memory usage issue when many interfaces are being edited or created at once.</td></tr>
<tr><td>1078119</td><td>Traffic is intermittently interrupted on virtual-vlan-switch on Soc5 based platforms when a multicast or broadcast packet is received.</td></tr>
<tr><td>1078541</td><td>The FortiFirewall 2600F model may become stuck after a fresh image burn. Upgrading from a previous version stills works.
<b>Workaround</b>: power cycle the unit.</td></tr>
<tr><td>1121548</td><td>Enabling <i>device-identification</i> also gets endpoint information, even though intermediate router exists on FG and endpoints.
<i>Workaround</i>: Disable <code>device-identification</code> on that interface.</td></tr>
</table>

Upgrade

Bug ID	Description
1055486	On the *Firmware and Registration* page, when performing a Fabric Upgrade using the GUI for the whole Fabric topology that includes managed FortiAPs and FortiSwitches, the root FortiGate may use an incorrect recommended image for FortiAP and FortiSwitch due to a parsing issue. **Workaround**: initiate the Fabric Upgrade using the CLI.

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.
1043189	Low-end FortiGate models with 2GB memory may enter conserve mode when processing large user store data with over 5000 user records and each record has a large number of IoT vulnerability data. For example, the *Users and Devices* page or FortiNAC request can trigger the following API call that causes the httpsd process encounter a CPU usage issue and memory usage issue. `GET request /api/v2/monitor/user/device/query`

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.
1094274	FortiGate becomes unresponsive due to an error condition when sending IPv6 traffic.

Web Filter

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

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.
873273	The *Automatically connect to nearest saved network* option does not work as expected when FWF-60E client-mode local radio loses connection.
941691	Managed FortiSwitch detects multiple MACs using the same IP address.

ZTNA

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

Built-in AV Engine

AV Engine 6.00301 is released as the built-in AV Engine. Refer to the AV Engine Release Notes for information.

Built-in IPS Engine

IPS Engine 7.00342 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.

Limitations on HA cluster formation between different FortiGate Rugged 60F and 60F 3G4G models

FortiGate Rugged 60F and 60F 3G4G models have various generations defined as follows:

- Gen1
- Gen2 = Gen1 + TPM
- Gen3 = Gen2 + Dual DC-input
- Gen4 = Gen3 + GPS antenna
- Gen5 = Gen4 + memory

The following HA clusters can be formed:

- Gen1 and Gen2 can form an HA cluster.
- Gen4 and Gen5 can form an HA cluster.
- Gen1 and Gen2 cannot form an HA cluster with Gen3, Gen4, or Gen5 due to differences in the `config system vin-alarm` command.

FORTINET®

www.fortinet.com