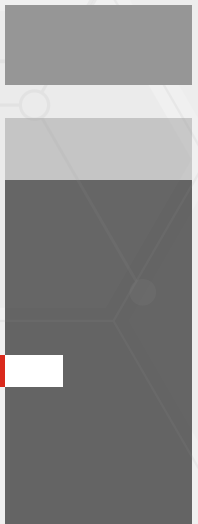
FORTINET

Release Notes

FortiOS 8.0.1





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



September 21, 2026
FortiOS 8.0.1 Release Notes

TABLE OF CONTENTS

Change Log **6**
Introduction and supported models **7**
Supported models 7
FortiGate 6000 and 7000 support 8
Special notices **9**
FortiManager support for updated FortiOS private data encryption key 9
Hyperscale incompatibilities and limitations 10
FortiGate 6000 and 7000 incompatibilities and limitations 11
Agentless VPN (formerly SSL VPN web mode) not supported on some FortiGate series models 11
2 GB RAM FortiGate models no longer support most FortiOS proxy-related features 12
2 GB RAM FortiGate models no longer support Security Rating and Security Fabric topology 12
Policy check required for hairpin traffic 12
FortiGate WiFi controller support with FortiOS 8.0.0 13
FortiLink split interface with LLDP neighbor detection mode 13
Changes in CLI **14**
Changes in default behavior **15**
Changes in default values **17**
Changes in table size **18**
New features or enhancements **19**
FortiGate 6000 and 7000 platforms 19
GUI 19
HA 20
Hyperscale 21
LAN Edge 21
Log & Report 24
Network 24
Operational Technology 26
Policy & Objects 26
SD-WAN 26
Security Fabric 28
Security Profiles 28
System 29
User & Authentication 30
VPN 31
WiFi Controller 32
ZTNA 32
Upgrade information **33**
Fortinet Security Fabric upgrade 33
Downgrading to previous firmware versions 35

Firmware image checksums ... 35
FortiGate 6000 and 7000 upgrade information ... 35
Password policy enforcement ... 36
FortiGate VM upgrade requirement ... 37
Product integration and support ... 38
Virtualization environments ... 39
Language support ... 39
Agentless VPN support ... 40
Resolved issues ... 41
Agentless VPN ... 41
AntiVirus ... 41
Application Control ... 42
Data Leak Prevention ... 42
DNS Filter ... 42
Endpoint Control ... 43
Explicit Proxy ... 43
Firewall ... 44
FortiGate 6000/7000 Platform ... 46
FortiView ... 46
GUI ... 46
HA ... 49
HyperScale ... 51
Intrusion Prevention ... 52
IPsec VPN ... 53
Log and Report ... 54
Proxy ... 55
REST API ... 57
Routing ... 57
SD-WAN ... 58
Security Fabric ... 58
Switch Controller ... 59
System ... 60
Upgrade ... 64
User and Authentication ... 65
VM ... 66
VoIP ... 67
Web Application Firewall ... 68
Web Filter ... 68
WiFi Controller ... 68
ZTNA ... 69
Known issues ... 70
New known issues ... 70
FortiGate 6000/7000 Platform ... 70
Upgrade ... 70

Existing known issues ... 70
AntiVirus ... 71
FortiGate 6000/7000 Platform ... 71
GUI ... 71
HA ... 72
HyperScale ... 72
IPsec VPN ... 72
REST API ... 73
Routing ... 73
User and Authentication ... 73
Built-in AV Engine ... **74**
Resolved engine issues ... 74
Built-in IPS Engine ... **75**
Limitations ... **76**
Citrix XenServer limitations ... 76
Open source XenServer limitations ... 76

Change Log

Date	Change Description
2026-09-15	Initial release of 8.0.1.
2026-09-16	Updated Introduction and supported models on page 7.
2026-09-17	Updated Built-in IPS Engine on page 75 and Changes in default behavior on page 15.
2026-09-21	Updated New features or enhancements on page 19, Resolved issues on page 41, and Known issues on page 70.

Introduction and supported models

This guide provides release information for FortiOS 8.0.1 build 0245.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 8.0.1 supports the following models.

FortiGate	FG-30G, FG-31G, FG-40F, FG-40F-3G4G, FG-50G, FG-51G, FG-50G-5G, FG-51G-5G, FG-50G-SFP, FG-50G-DSL, FG-50G-SFP-POE, FG-51G-SFP-POE, FG-60F, FG-61F, FG-70F, FG-71F, FG-70G, FG-71G, FG-70G-POE, FG-71G-POE, FG-80F, FG-80F-BP, FG-80F-DSL, FG-80F-POE, FG-81F, FG-81F-POE, FG-90G, FG-91G, FG-100F, FG-101F, FG-120G, FG-121G, FG-200E, FG-200F, FG-200G, FG-201E, FG-201F, FG-201G, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-400F, FG-401F, FG-400G, FG-401G, FG-500E, FG-501E, FG-600E, FG-601E, FG-600F, FG-601F, FG-700G, FG-701G, FG-800D, FG-900D, FG-900G, FG-901G, FG-1000D, FG-1000F, FG-1001F, FG-1100E, FG-1101E, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000F, FG-3001F, FG-3000G, FG-3001G, FG-3200F, FG-3201F, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3500G, FG-3501G, FG-3600E, FG-3601E, FG-3700F, FG-3701F, FG-3800G, FG-3801G, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-4800F, FG-4801F, FG-6000F, FG-7000E, FG-7000F
FortiWiFi	FWF-30G, FWF-31G, FWF-40F, FWF-40F-3G4G, FWF-50G, FWF-50G-5G, FWF-50G-SFP, FWF-50G-DSL, FWF-51G, FWF-60F, FWF-61F, FWF-70G, FWF-71G, FWF-70G-POE, 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-50G-5G, FGR-60F, FGR-60F-3G4G, FGR-60G, FGR-60G-M12, FGR-60G-5G, FGR-70F, FGR-70F-3G4G, FGR-70G, FGR-70G-5G, FGR-70G-5G-Dual
FortiFirewall	FFW-1801F, FFW-2600F, FFW-3001F, FFW-3501F, 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-XEN

Starting with FortiOS 7.6.1, New deployments on Azure Marketplace use Generation 2 (Gen2) VM images and no longer support Azure F-series, Fs-series, Standard Dv2, and Standard Dsv2 instance types, or similar instance families, which require Gen1 images. Existing FortiGate VMs deployed on F-series or Fs-series instance types can continue to operate and be upgraded to FortiOS 7.6.1 or later. Upgrade to newer instance families for better and more stable performance. See Instance type support for details.

FortiGate 6000 and 7000 support

FortiOS 8.0.1 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

- FortiManager support for updated FortiOS private data encryption key on page 9
- Hyperscale incompatibilities and limitations on page 10
- FortiGate 6000 and 7000 incompatibilities and limitations on page 11
- Agentless VPN (formerly SSL VPN web mode) not supported on some FortiGate series models on page 11
- 2 GB RAM FortiGate models no longer support most FortiOS proxy-related features on page 12
- 2 GB RAM FortiGate models no longer support Security Rating and Security Fabric topology on page 12
- Policy check required for hairpin traffic on page 12
- FortiGate WiFi controller support with FortiOS 8.0.0 on page 13
- FortiLink split interface with LLDP neighbor detection mode on page 13

FortiManager support for updated FortiOS private data encryption key

With the introduction of FortiOS 7.6.1, Fortinet has updated the private-data-encryption key feature. Administrators are no longer required to manually input a 32-digit hexadecimal `private-data-encryption` key. Instead administrators simply enable the command, and a random `private-data-encryption` key is generated.

How FortiManager 8.0.0 works with FortiOS private data encryption keys has changed. This topic covers the changes. See FortiManager behavior on page 10.

Previous FortiOS CLI behavior

```
config system global
    set private-data-encryption enable
end
Please type your private data encryption key (32 hexadecimal numbers):
1234567890123456789012345678 9abc
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
1234567890123456789012345678 9abc
Your private data encryption key is accepted.
```

New FortiOS CLI behavior

```
config system global
    set private-data-encryption enable
end
This operation will generate a random private data encryption key!
Previous config files encrypted with the system default key cannot be restored after this
operation!
```

```
Do you want to continue? (y/n)y
Private data encryption key generation succeeded!
```

FortiManager behavior

FortiManager 8.0.0 can centrally manage FortiGates with the private-data-encryption setting enabled, with the following limitations:

- FortiManager can import objects that include the password type attribute.

  When FortiManager imports objects that include a password-type attribute, the administrator will be prompted to specify the password used by the object during the import process.
- FortiManager cannot be used to create NAT and transparent VDOMs.

This applies to FortiGates with private keys that are manually configured in FortiOS 7.6.0 and earlier and private keys that are randomly generated in FortiOS 7.6.1 and later.

FortiManager does not require you to verify the private key of the FortiGate when adding it to FortiManager.

FortiGates that require the protection of private data encryption and need to be managed by FortiManager should follow these procedures on a fresh install.

1. On the FortiGate, enable `private-data-encryption`.
2. On the FortiManager, add the FortiGate to the Device Manager. FortiManager will not be required to provide the key for PDE, as it will not be importing any password-related settings.
3. Make all configuration changes directly on the FortiManager.
4. Push and install the changes to the FortiGate.

If you require the use of NAT or Transparent VDOMs, you should perform this additional step before the steps above.

1. Enable `multi-vdom` mode on the FortiGate.
2. Add the VDOMs that you will use on the FortiGate.
3. Follow the above steps to enable `private-data-encryption` and manage the FortiGate from the FortiManager.

For more information, see the FortiManager Administration Guide.

Hyperscale incompatibilities and limitations

See Hyperscale firewall incompatibilities and limitations in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 8.0.1 features.

FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 8.0.1 features.

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

Agentless VPN (formerly SSL VPN web mode) not supported on some FortiGate series models

On the following FortiGate models, the Agentless VPN (formerly SSL VPN web mode) feature is no longer available from the GUI or CLI. Settings will not be upgraded from previous versions.

The affected models include:

- FGT-40F/FWF-40F and variants
- FGT-50G/FWF-50G and variants
- FGT-60F/FWF-60F
- FGT-61F/FWF-61F
- FGR-60F and variants (2GB versions only)
- FGT-70G/FWF-70G and variants
- FGT-90G and FGT-91G

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

On these FortiGate models, consider migrating to using IPsec Dialup VPN for remote access.

See SSL VPN to IPsec VPN Migration for more information.

FortiGate models not listed above will continue to support Agentless VPN (formerly SSL VPN web mode). However, SSL VPN tunnel mode is not longer supported on any models.

2 GB RAM FortiGate models no longer support most FortiOS proxy-related features

As part of improvements to enhance performance and optimize memory usage on FortiGate models with 2 GB RAM or less, FortiOS no longer supports most proxy-related features.

However FortiOS 7.6.5 brings back proxy-based inspection for email protocols on FortiGate models with 2 GB RAM. This covers the following services:

- SMTP(s)
- POP3(s)
- IMAP(s)
- NNTP

Firewall policies can once again support proxy-based inspection mode when users select one or more of the above services in the firewall policy.

This change impacts the FortiGate 40F, 60F, and 50G series devices, along with their variants.

See Proxy-related features no longer supported on FortiGate 2 GB RAM models for more information.

2 GB RAM FortiGate models no longer support Security Rating and Security Fabric topology

To enhance the stability of physical FortiGate devices devices with 2 GB RAM, the Security Rating feature and Security Fabric topology visibility have been removed. These changes prioritizes device stability and mitigate potential performance issues. For more information, see Optimizations for physical FortiGate devices with 2 GB RAM.

Policy check required for hairpin traffic

In FortiOS 7.6.5, the default setting for `allow-traffic-redirect` and `ipv6-allow-traffic-redirect` changed from `enable` to `disable`:

```
config system global
  set allow-traffic-redirect disable
  set ipv6-allow-traffic-redirect disable
end
```

Upon upgrade, both of these settings will be changed to `disable`, even if they were enabled before.

Disabling this setting ensures that hairpin traffic arriving at an interface and redirected out on the same interface requires a firewall policy to explicitly allow the traffic. If you want to redirect traffic without the need for a policy based only on routing decision, then manually enable these settings.

FortiGate WiFi controller support with FortiOS 8.0.0

FortiGate WiFi Controller running FortiOS 8.0.0 no longer supports FortiAP-C, FortiAP-U E-series, and FortiAP-W2 E-series models, except for FAP-221E, 223E, 421E and 423E.

FortiLink split interface with LLDP neighbor detection mode

When FortiLink neighbor detection mode is set to LLDP and the FortiLink split interface is enabled, one FortiLink member port remains in the up/active state, while the other remains in the down/standby state.

Changes in CLI

Bug ID	Description
895242	For the FortiGate-6000 and 7000 platforms, the default HA upgrade mode has been changed to from simultaneous to uninterruptible.

1256819	Renamed the update-server-location setting to fortiguard-server-location under config system fortiguard. The setting description has also been updated to reflect FortiGuard services instead of FortiGuard updates. Applicable to all platforms.
	CLI changes
	`config system fortiguard`
	`  set fortiguard-server-location <location>`
	`end`
	Previous CLI
	`config system fortiguard`
	`  set update-server-location <location>`
	`end`

1266730	The arp-reply CLI option is now supported for IPv4 and IPv6 firewall VIPs. The arp-reply option is enabled by default and you can use the following command to disable ARP replies for a firewall VIP:
	`config firewall vip`
	`  edit new-vip`
	`  set arp-reply disable`
	`  end`

1271740	Removed tenant-extraction configuration from the Inline CASB custom application CLI and GUI. Previously, tenant information could be extracted from JSON traffic using user-defined JQ filters for granular SaaS application control. This functionality has been removed to reduce security risks associated with running custom JQ scripts and to simplify maintenance.
1294499	Expands the supported block size range for Port block allocation IP pools from 644096 to 164096.
1295515	The "intra-vap-privacy" setting is added for local-bridging VAP.

Changes in default behavior

Bug ID	Description
1073893	When a large TCP packet enters an IPsec tunnel, the FortiGate no longer adjusts the TCP MSS value automatically. Instead, it sends an ICMP message (ICMP_FRAG_NEEDED) to notify the sender of the correct MTU size. The sender can then adjust the TCP MSS and subsequent packet sizes accordingly.
1223618	The configuration export commands have been restructured to give administrators explicit control over how secrets in exported configuration files are protected. Previously, when a user did not specify the password option, FortiGate encrypted all configuration secrets using a static key. This enhancement requires the user to either provide a password to encrypt sensitive information or the entire configuration file, in which case the exported secrets can be restored and reversed only with that same password, or to mask all secrets, which cannot be restored or reversed at all. The new execute export commands replace the network-server-targeted execute backup commands and require the administrator to explicitly select how secrets are protected before a configuration file is exported. The legacy execute backup config command remains available, but its scope has been reduced to local and management-station targets only. To perform a configuration backup: `execute export config {standard | full | yaml} {encrypted | obfuscated | secrypt} {ftp | scp | sftp | tftp | usb} <filename> <server> [<password>]` For more information, see Encrypted configuration export.
1238339	1. Enable the dedicated host queue by default to carry critical traffic. This secures critical connections like BFD, BGP, LACP, even under extreme background load. 2. NP7 DSWH profile changed to improve the buffer performance. 3. Don't return e_busy at the NP7 driver to prevent CPU exhaustion under intense retry. 4. Enable the `dedicated-management-cpu` by default to prevent regular traffic from running on CPU0, which is also used for processing critical traffic on lower-end NP7 platforms. * To maximize the CPS performance, you can disable this feature. 5. Regular host queues now drop packets at DSWH under extreme load, instead of doing backpressure to DSW. This helps to show which CPU core is busy during debugging and prevents bigger issues like CG_FULL.
1266783	The default hostname format now includes a short serial number hash to improve device identification. Newly generated hostnames use the product name and a unique serial-based hash instead of only the product name. Previous format FortiGate-71F New format FortiGate-71F-XEZOKB

Bug ID	Description
1275491	The default outbound firewall policy is no longer preconfigured on newly deployed desktop models and the FG-100F/200F series. Administrators can optionally create the default outbound firewall policy during the initial setup wizard, helping meet compliance requirements while preserving a streamlined deployment experience.
1288059	On FortiGate 20xG models, port1 and port2 are removed from the virtual switch and configured for DHCP by default after a factory reset or outofbox initialization to support Zero Touch Provisioning (ZTP) over these ports.

Changes in default values

Bug ID	Description
1248524	The default MTU for IPsec tunnel interfaces has been changed from 1420 to 1402 across all FortiGate models.
1248566	The default value for system.global.log-daemon-cpu-threshold has changed from 0 to 75. The valid range has also been updated from 0-99 to 50-99. This setting controls the CPU usage threshold at which the syslog daemon spawns a new child process.

Changes in table size

Bug ID	Description
1132879	Increase extension-controller.extender size for FortiGate-200G and higher end to 512 to support more lan-extension connections.
1261899	The maximum length for firewall policy names has been increased from 35 to 255 characters to allow for more descriptive naming conventions.

New features or enhancements

More detailed information is available in the New Features Guide.

FortiGate 6000 and 7000 platforms

Feature ID	Description
1116827	Enhances the IPS engine to correctly detect and inspect GTPv2 Tunnel IDs by extending support beyond GTPv1. This enables accurate analysis of GTP U payloads and faster identification and isolation of compromised subscriber devices.

GUI

See GUI in the New Features Guide for more information.

Feature ID	Description
1170580	Added a Notification Center that consolidates hardware and operational alerts under a header bell, now split into General and Event Alerts sections. Admins can view logs, diagnose with FortiAI, create automation triggers, dismiss alerts, and choose which alert types to show.
1228572	Feature Visibility has been redesigned to align with the FortiGate navigation structure, simplifying feature discovery and configuration through improved search, organization, and change review.
1236143	The FortiView Applications and AI Applications dashboards now use an interactive, chart-driven view instead of a flat table. Applications are presented by classification sanctioned, unsanctioned, and unclassified so administrators can spot shadow IT, GenAI usage, and risk patterns at a glance, then filter and drill down into the applications that need investigation.
1250068	The FortiView AI widgets can now use FortiAnalyzer as a data source for GenAI traffic analysis and reporting.
1254298	Adds GUI support for monitoring 5G modem status and performing firmware upgrades, improving visibility and streamlining maintenance workflows.

Feature ID	Description
1275491	Adds an Initial Firewall Policy Setup wizard to the first-boot experience on desktop models and the FG-100F/200F series, enabling one-click deployment of a default outbound firewall policy on newly deployed FortiGate devices. This replaces preconfigured default outbound policy to support compliance requirements and is available only when no firewall policies exist.

HA

Feature ID	Description
1205727	You may be able to reduce FGCP HA failover times by changing the NP7 link scan interval. The NP7 link scan interval is the amount of time that a FortiGate with NP7 processors waits between scans to determine if a link has failed. A shorter NP7 link scan interval can cause the FortiGate to send gratuitous ARP packets sooner after an HA failover has occurred. config system npu set np-linkscan-interval <milliseconds> end The `np-link-scan-interval` range is 50 to 1000ms. The default NP7 link scan interval is 1000 milliseconds (ms). If your FGCP HA cluster experiences longer than expected HA failover delays (for example a 2-second interval for a failover to occur) reducing the NP7 link scan interval may reduce HA failover delays.
1249137	FortiGate FGSP HA synchronizes IPsec VPN state between cluster members so that tunnels are synchronized after a member failure or planned reboot. This enhancement ensures that the configured traffic interfaces are not brought operationally up until IPsec synchronization has finished. The synchronization sequence uses IKE, rather than the HA process, to signal when IPsec state synchronization is complete.

1277890	Added FGCP HA high memory utilization failover protection for the FortiGate 6000 and 7000 platforms.
	New CLI options:
	`config system ha`
	`set memory-based-failover {enable | disable}`
	`set memory-failover-threshold <memory-usage-threshold>`
	`set memory-failover-monitor-period <seconds>`
	`set memory-failover-sample-rate <seconds>`
	`set memory-failover-flip-timeout <minutes>`
	`set memory-failover-board-failure-tolerance <tolerance>`
	`end`
	You can use `memory-failover-board-failure-tolerance` to set the tolerance for how many FIMs or FPMs/FPCs reach the high memory utilization threshold before a failover occurs.

Hyperscale

Feature ID	Description

1236578	SCTP traffic processing behavior can now be configured on SoC4 and SoC5 platforms. New NPU settings control SCTP offloading and whether SCTP control packets are forwarded to the host for processing.
	CLI changes
	`config system npu`
	`set sctp-offload {enable | disable}`
	`set sctp-ctrlpkt-to-host {enable | disable}`
	`end`

1280968	Added the ipv4-option setting under config system npu>config fp-anomaly to control how IPv4 packets containing IP options are processed.
	CLI changes
	`config system npu`
	`config fp-anomaly`
	`set ipv4-option {allow | trap-to-host}`
	`end`
	`end`

1286440	This enhancement extends NP7 CGN logging so that RSSO user and group information from RADIUS accounting is appended to NAT64 EIF per-session syslogs.
1288373	Introduces NPU offload support for IPsec over VNE interfaces on SoC5/NP7Lite and NP7 platforms, enabling hardware acceleration at the driver level, improving performance and throughput.
1298417	Adds support for the match-vip option in deny firewall policies within hyperscale VDOM. This enhancement ensures VIP traffic is correctly matched and blocked after DNAT, improving policy enforcement consistency.

LAN Edge

See LAN Edge in the New Features Guide for more information.

Feature ID	Description
1164734	Enhances RSPAN and ERSPAN configuration by allowing settings to be applied at the individual FortiSwitch stack level instead of all switches under a FortiLink interface. This provides more granular traffic monitoring control and greater deployment flexibility.

Feature ID	Description
1198560	A new Voice Controller lets FortiGate discover and authorize FortiVoice appliances and FortiFone phones over FortiLink, following the same model as the Switch Controller. Previously, FortiGate could only forward voice traffic; now, common settings such as extension numbers, ring groups, and PBX location can be configured for managed FortiVoice from a single FortiGate, simplifying deployment in FortiGate-centric environments.

1213241	Added the emac-vlan-mode setting under config system npu to control EMAC VLAN operating behavior. The setting allows prioritizing either full functionality or session offloading, depending on deployment requirements.
	CLI changes
	`config system npu`
	`  set emac-vlan-mode {functionality | offloading}`
	`end`
	This applies to NP6 platforms only.

1244041	Added support for transmitting DHCP relay packets over the 5G modem. A new dhcp-relay option under config system cellular-modem enables or disables DHCP relay traffic over the modem connection. Supported on all 5G units.
	CLI changes
	`config system cellular-modem`
	`  config modem1`
	`  set dhcp-relay {enable | disable}`
	`  end`
	`end`

1254611	Wildcard VLAN handling and VLAN filtering are now supported on software switches (switch-interface) when intra-switch-policy is set to explicit. These options enable policy matching for VLAN-tagged traffic and allow restriction of permitted VLAN ranges.
	CLI changes
	`config system switch-interface`
	`  edit <name>`
	`  set wildcard-vlan {enable | disable}`
	`  set vlan-filter <vlan-range-list>`
	`  next`
	`end`

1280876	FortiExtender profiles can now operate in Wi-Fi WAN mode, allowing a Wi-Fi radio to function as a client and connect to external wireless networks for WAN connectivity. Support includes Wi-Fi network definitions, enterprise authentication settings, radio mode selection, and profile persistence. CLI changes `config extension-controller extender-vap`

Feature ID	Description
	``` edit <name> set type wifi-network set security {WPA-Personal | WPA-Enterprise | WPA-WPA2-Enterprise} set identity <string> set password <string> next end config extension-controller extender-profile edit <name> config wifi config radio-1 set mode {AP | Client} set persistence {enable | disable} set wifi-networks <vap1>,<vap2>,... end end next end ```
1291807	Add Layer 3 Intra-Controller Roaming support for Bridge mode SSIDs, allowing WiFi clients roaming between FortiAPs to retain their original IP address and network path. This enables uninterrupted application sessions and seamless mobility, even when the client associates with a roaming FortiAP that provides access to a different VLAN or subnet.
1293688	Added support for WPA3 transition mode SSIDs on 6 GHz radios, enabling a single SSID to operate across 2.4 GHz, 5 GHz, and 6 GHz bands. This simplifies wireless deployments while maintaining compatibility with legacy clients and supporting WPA3 on 6 GHz devices.
1296905	Added configurable wireless client authentication lockout to temporarily suppress authentication attempts after a defined number of failed logins. This feature helps mitigate PSK brute-force and dictionary attacks and is supported in Tunnel, Bridge, and Local Standalone deployments.
1306258	Added STP Root Guard support for interfaces participating in a virtual switch with STP enabled. STP Root Guard prevents a port from accepting superior BPDUs that could cause an unintended device to become the root bridge. CLI changes ``` config system interface edit <interface> set stp-root-guard {enable | disable} next end ```

Log & Report

See Logging in the New Features Guide for more information.

Feature ID	Description
1270732	This feature introduces optional LUKS-based full-disk encryption for the log disk (varlog). When enabled via `execute formatlogdisk encrypt`, the log disk is formatted with a LUKS header and transparently encrypted using dm-crypt. The encryption key can be stored in TPM (if available) or on the local filesystem.
1281517	A reason field is added to IPsec event logs for tunnel negotiation failures and tunnel-down events, so administrators can identify the root cause of a disconnected IPsec tunnel from the logs alone.
1301863	FortiGate generates new system event logs that record device-level and account-level contract and license changes. These logs provide visibility into contract state changes that determine a FortiGate's eligibility for automatic upgrades.

Network

See Network in the New Features Guide for more information.

Feature ID	Description
1122263	FortiOS now supports IPv6 PCP for DNAT46, enabling inbound PCP MAP requests in NAT64 deployments. This enhancement allows FortiGate to dynamically manage IPv6-to-IPv4 mappings via PCP, improving compatibility with CLAT-based CPEs.
1149106	FortiOS now supports upstream SSL for HTTPS virtual servers. When enabled, FortiGate converts incoming HTTP traffic to HTTPS between itself and the HTTPS server, improving security for trusted internal deployments with resource-constrained devices.
1192303	On FortiGates with NP7 processors, the following new option is available to enable or disable VLAN accounting: config system npu set vlan-accounting {disable | enable} end VLAN accounting is enabled by default. VLAN accounting on a busy FortiGate with a large number of VLANs can generate large numbers of VLAN lookup (SPV/TPV) messages. In some cases these messages can cause CG-FULL conditions or packet drops, especially on very busy systems. You can use the following command to reduce the number of VLAN accounting massages that are generated by increasing the VLAN accounting interval. config system npu set vlan-acct-interval <milliseconds> end The default VLAN accounting interval is 200 milliseconds. The range is 100 to 10000 milliseconds.

Feature ID	Description
1198563	Adds support to manually configure MAC addresses for VLAN and software switch interfaces independently of their parent interfaces.
1223026	Added support for reordering Virtual IP (VIP) entries in the GUI when central NAT is disabled, including inline Insert Above and Insert Below creation options. Security Rating now automatically detects and highlights overlapping or shadowed VIPs, helping administrators identify and resolve VIP ordering conflicts.
1248322	A new enhancement introduces support for an optional client certificate during firmware upgrades via URL. This allows users to specify a client certificate when connecting to mTLS-enabled servers. `execute restore image url <url> [Enter|<cert_name>]`
1252369	Enhances SIP ALG to support 1:1 NAT mapping per voice server using a dedicated VIP range during SIP 302 redirect processing. By assigning a unique external IP to each server, the system ensures precise SIP header translation and robust NAT tracking. This architecture significantly improves scalability and reliability in load-balanced VoIP environments.
1261566	Enhance VRF configuration by adding support for user-defined names alongside VRF IDs, allowing routing commands to display names instead of only numeric identifiers for improved clarity and manageability in multi-VRF environments.
1262907	Allow unaddressed IPsec tunnel interfaces to be used as PIM interfaces by borrowing the IP address of a loopback interface. config router multicast config interface edit ""p1"" set update-source ""lo1"" next end end
1273072	FortiGate now supports the Captive Portal API defined in RFC 8908, giving client devices a standardized, secure way to detect and interact with a captive portal using the URL advertised in DHCP option 114.
1273080	Introduces the link-sync-group feature to enable bidirectional interface state synchronization, ensuring all member interfaces transition collectively based on link status. This enhancement addresses limitations of unidirectional fail-detect by preventing interface flapping loops and improving resiliency in LACP and telco deployments.
1281516	Enhanced SNMP monitoring with new OIDs for VPN tunnel, Proxy ID, and IPsec SA statistics, enabling administrators to remotely monitor key IPsec VPN metrics without direct access to the FortiGate
1283986	Enhances VLAN pooling by allowing configuration of network IP per VLAN, enabling wireless clients with static IP addresses to be mapped to the corresponding VLAN based on subnet. This enhancement improves segmentation and deployment flexibility in L2 environments by aligning VLAN assignment with client network addressing.
1285651	Extends GTP-U dynamic source port support to IPv6 traffic on NP7 platforms. By reducing session creation to just two sessions per bidirectional flow, this feature significantly lowers memory consumption for carrier environments handling large volumes of GTP-U traffic.

Feature ID	Description
1295481	Multicast packets are now forwarded to the incoming interface when switch-controller-access-vlan (intra-VLAN blocking) is enabled on that interface and a matching multicast policy exists. This allows multicast applications to keep working for clients on the same access VLAN without disabling intra-VLAN blocking
1303461	FortiGate now supports DHCP Lease Query (RFC 4388) to retrieve a client's MAC address from the DHCP server's lease database internal or external when the client is not on the same Layer 2 network. This enables features such as MAC Authentication Bypass (MAB) for clients on remote subnets, where the MAC address is otherwise unavailable in the local neighbor table.

Operational Technology

See Operational Technology in the New Features Guide for more information.

Feature ID	Description
1284382	Adds out-of-band serial management via USB-to-serial cable on FGR-70F/70G Series platforms, which lack a DB9 port. Enables `execute obm-console` to connect to up to 4 controlled devices for remote control.

Policy & Objects

See Policy and objects in the New Features Guide for more information.

Feature ID	Description
1105204	Adds support for using SCIM groups directly in firewall policies, eliminating the need for local group mapping, simplifying identity-based access control. Additionally enables IPsec VPN authorization by matching certificate SAN fields with SCIM user attributes, ensuring consistent and streamlined user authentication and policy enforcement.
1252371	Weighted random early detection (WRED) queuing within traffic shaping is now supported on the 4.19 kernel.

SD-WAN

See SD-WAN in the New Features Guide for more information.

Feature ID	Description

1249436	The new spillover load-balance is added to explicit SD-WAN service rules. When a member exceeds its configured egress or ingress threshold, new sessions are spilled over to the next eligible member that is still within SLA, while existing sessions stay on the saturated link until usage drops below the configured spillover threshold.
	
	`config system sdwan`
	`  config service`
	`  edit <service_id>`
	`  set hash-mode spillover`
	`  next`
	`  end`
	`end`

1249437	Add SD-WAN Weight-based-spillover Load-balancing Algorithm Support in SD-WAN Policy (Explicit Rules). This mode ensures traffic is distributed based on "weight" to interfaces with used bandwidth below a defined spillover threshold, preventing overload on saturated links.
1273077	This feature allows SD-WAN to consume a FortiExtender's (FEX) cellular signal strength and data-quota utilization as SLA metrics. Two new health-check metrics: `signal-strength` and `quota-usage` can now be added to a health-check SLA rule's cost factors.

1277091	Enable assigning route priority to the routes that FortiGate dynamically installs for a tunnel through the `add-route` mechanism. This feature is necessary to prevent suboptimal routing and loops, in complex, multi-hub SD-WAN architectures.
	
	`config vpn ipsec phase1-interface`
	`  edit`
	`  set priority <integer>`
	`  next`
	`end`

1284610	Add support for RPKI (Resource Public Key Infrastructure) so FortiGate may confirm an AS originating a route announcement is actually authorized to do so. A new daemon, rpkid, is created to maintain a Route Origin Authorization (ROA) table, and interacts with the BGP daemon to validate BGP routes.
1288984	Adds support for BGP large communities (RFC 8092), a 12-byte attribute designed to address the scaling limitations of legacy community formats in 4-byte Autonomous System Number (ASN) environments, while improving policy control and interoperability in modern BGP deployments.
1306553	Add MTU awareness to SD-WAN health checks that use the ICMP (ping) protocol. Administrators can now configure the probe packet size for ICMP health checks and can set the "Don't Fragment" (DF) flag on probes. This enables health checks to accurately detect MTU mismatches or path limitations along an SD-WAN member's link.
1306554	Add support to SD-WAN health-checks for IPv6 to allow HTTPS as a probe protocol alongside the existing http-get, http-agent, and http-match options.

Security Fabric

See Security Fabric in the New Features Guide for more information.

Feature ID	Description
1145865	Downstream Security Fabric members may now be authorized based on the certificate issuer's CN and the devices subject CN. As long as the issuer is a trusted CA, or one of the CAs in the hierarchy of signing chain is a trusted CA, downstream devices will maintain authorization, even if certificates are renewed, reducing admin reauthorization frequency.
1159462	FortiGate now supports centralized FortiTelemetry Agent image upgrades, enabling administrators to deploy upgrades for supported FT100G, Windows agents and macOS agents directly from the FortiGate.
1250637	External feeds can now support hashed URL and hashed SNI lists, which can then be used in a Web Filter profile to enforce policy. This allows customers such as ISPs, regulators, and enterprises that receive block lists only in hashed form to apply the required filtering at scale, without FortiGate accessing or storing the plaintext URLs.
1314093	Added support for focusing on a selected FortiGate and its subtree in the Security Fabric Topology page. Added topology view switching between Assets, Vulnerable Assets, Security Rating, and End of Support, with progressive search results for improved responsiveness.

Security Profiles

See Security profiles in the New Features Guide for more information.

Feature ID	Description
1168592	Adds Optical Character Recognition (OCR) support to Data Loss Prevention (DLP), enabling inspection of text embedded in images, screenshots, and scanned documents. OCR-extracted content is evaluated against DLP policies to detect and block sensitive information in visual content that would otherwise bypass traditional text-based inspection.
1214967	The proxy-based Web Filter profile can now inspect actual image content by submitting images to the FortiGuard Image Classification cloud service, which returns content categories with confidence scores. Administrators set per-category log/block thresholds to allow, monitor, or block images that URL and category filtering alone cannot detect.
1220356	Enhances FortiTelemetry by allowing administrators to define custom telemetry applications and include them in telemetry profiles alongside predefined public applications. This extends monitoring support to private enterprise applications and is supported on FortiTelemetry Windows and macOS agents.

Feature ID	Description
1241726	Support for hashed Exact Data Matching (EDM) is now available, enabling secure data ingestion on FortiGate without exposing sensitive plaintext. Additionally, the new edm-csv2json FNDN tool converts typed CSV datasets into a hashed format. This output can be imported and utilized within your EDM templates, providing a privacy-focused alternative to traditional CSV-based detection.
1249939	Adds support for TLS key exchange translation between PQC and classical algorithms in SSL Deep Inspection (proxy mode). This enables seamless interoperability between PQC-enabled and legacy services while preserving full inspection and supporting gradual adoption of quantum-safe cryptography without service disruption.
1270148	The signature hold timer, previously available for IPS signatures only, now extends to Application Control signatures. When a new application signature arrives in an APDB package update, FortiGate places it on hold for the configured period instead of applying it immediately. This gives administrators a window to review newly added application signatures before they can affect production traffic.
1278557	Introduced a customizable application classification framework for application signatures, expanding classification beyond the built-in sanctioned and unsanctioned model. Custom classifications, scopes, and rule-based assignment provide granular application categorization and filtering in application control overrides.
1294840	Added support for ML-DSA post-quantum signature algorithms (ml-dsa-44, ml-dsa-65, and ml-dsa-87) in TLS deep inspection when using flow-based inspection. This enhancement enables TLS connections that require post-quantum authentication while protecting against quantum-era threats.
1296887	Adds support for FortiGate-triggered FortiAP firmware upgrades from external FTP, TFTP, SFTP, SSH, and HTTP(S) servers. This provides a flexible upgrade path for deployments with limited bandwidth, large firmware images, or unreliable connectivity between FortiGate and FortiAP.
1308265	Added risk level classification and filtering for SaaS applications in the Inline CASB GUI, enabling administrators to quickly identify and prioritize higher-risk applications using FortiGuard-provided risk ratings.

System

See System in the New Features Guide for more information.

Feature ID	Description
1081074	Add support for automatically generating and assigning a unique, strong administrator password when authorizing a FortiAP that does not already have one configured. Password retention or reset during deauthorization is configurable.

Feature ID	Description
1173951	FortiGate now supports the Technical Report 069 (TR-069) CPE WAN Management Protocol, enabling remote management via an ACS server (e.g., GenieACS). This lets administrators manage FGT as a CPE device, including configuration, firmware push, and remote reboot/factory-reset.

1269583	A configurable timeout is now available for manually initiated disk scans. If an execute disk scan operation does not complete within the configured timeout period, the FortiGate terminates the scan and reboots. The default timeout is 7200 seconds (2 hours).
	CLI changes
	`config system global`
	`set disk-scan-timeout <0-86400>`
	`end`

1275588	Web-proxy now supports multiple certs to enable higher performance while keeping compatibility. For example, using EDDSA+RSA.
	`config web-proxy global`
	`set ssl-cert ""cert1"" ""cert2""`
	`set proxy-fqdn ""default.fqdn""`
	`end`

1288991	Firmware release RSS feed now supports FIPS/FIPS-CC firmware release.
1299497	Automation email notifications now use enhanced email templates by default for improved readability. The updated notifications replace plain-text formatting, remove raw log content from messages, and include additional event information where applicable.

User & Authentication

See Authentication in the New Features Guide for more information.

Feature ID	Description
1244920	Adds the ability to enable both Dynamic VLAN and VLAN Pooling simultaneously when configuring a VAP with RADIUS authentication. This enhancement expands flexibility in enterprise deployments by allowing VLAN assignment from RADIUS or, when absent, falling back to the local VLAN pool for seamless segmentation.

1280307	Added support for including interfaces configured as DHCP clients in IPAM automatic conflict resolution check. This option is disabled by default.
	`config system ipam`
	`set dhcp-intf-conflict-check {enable | disable}`
	`end`

Feature ID	Description
	If `set automatic-conflict-resolution` and `set dhcp-intf-conflict-check` are enabled simultaneously, an error message prevents this invalid configuration from being applied.

VPN

See IPsec and SSL VPN or Agentless VPN in the New Features Guide for more information.

Feature ID	Description

1095246	MCS shaping support is now available for IPsec dialup tunnels, providing a scalable traffic shaping solution for deployments with large numbers of tunnels. New NPU settings allow selection of the default IPsec MCS mode and enable TPE-based shaping for host traffic on IPsec interfaces.
	CLI changes
	`config system npu`
	`  set default-ipsec-mcs-type {policy | shaping}`
	`  set mcs-host-packet-tpe-shaping {enable | disable}`
	`end`

1235059	IPsec multipath allows encrypted tunnel traffic to be distributed across multiple sub-tunnels and CPU queues simultaneously. By grouping these sub-tunnels into a single logical super tunnel, FortiGate can utilize multiple CPU cores in parallel, significantly increasing VPN throughput without requiring changes to the overall tunnel design or addressing plan.
	To enable:
	`config vpn ipsec phase1-interface`
	`  edit <name>`
	`  set multipath <integer>`
	`  next`
	`end`

1277068	The VPN wizard for creating remote access and SIA tunnels now extends IPAM-based addressing to IPv6. Previously, only the IPv4 client range could be auto-assigned from IPAM -- the IPv6 range had to be entered manually. Administrators can now define an IPv6 pool in IPAM and have a block of addresses automatically assigned to the tunnel for dual-stack VPN clients.
1296910	The IPsec VPN Wizard is reorganized to separate FortiClient and native operating system clients into dedicated top-level template options. This change allows admins to more clearly pick the VPN configurations by the type of client, then drill down to specific supported configurations for that client.

WiFi Controller

See Wireless in the New Features Guide for more information.

Feature ID	Description
1299648	The WiFi Controller now automatically triggers an initial DARRP once 90% of managed FAPs have been online for 30 minutes, and runs DARRP for each newly joined FAP after 30 minutes online. Scheduled DARRP continues as configured thereafter.

ZTNA

See Zero Trust Network Access in the New Features Guide for more information.

Feature ID	Description
1303517	A ZTNA reverse-connector can now register itself as a relay node with the upstream ZTNA Edge, allowing traffic to be routed through it as part of a multi-hop relay chain.

Upgrade information

Supported upgrade path information is available through the Upgrade Path Tool on the Fortinet Document Library.

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 33 and Upgrading all devices in the FortiOS Administration Guide.

To view supported upgrade path information:

1. Go to the Fortinet Document Library at https://docs.fortinet.com/product/fortigate.
2. From the right side-bar, go to *Tools & Resources* and select *Upgrade Path Tool*.
3. Check that *Choose a product* is *FortiGate / FortiOS*.
4. In the *Product Model* list, select your model.
5. In the *Current Version* list, select the FortiOS version you are currently running.
6. In the *Target Upgrade Version* list, select the target FortiOS version for the upgrade.
7. Click *Go* to view the upgrade path.

Fortinet Security Fabric upgrade

FortiOS 8.0.1 is verified to work with these Fortinet products. This includes:

FortiAnalyzer	• 8.0.1
FortiManager	• 8.0.1
FortiExtender	• 7.4.0 and later
FortiSwitch OS (FortiLink support)	• 6.4.6 build 0470 and later

FortiAP	• 7.2.2 and later
FortiAP-U	• 6.2.5 and later
FortiAP-W2	• 7.2.2 and later
FortiClient EMS	• 7.0.3 build 0229 and later
FortiClient Microsoft Windows	• 7.0.3 build 0193 and later
FortiClient Mac OS X	• 7.0.3 build 0131 and later
FortiClient Linux	• 7.0.3 build 0137 and later
FortiClient iOS	• 7.0.2 build 0036 and later
FortiClient Android	• 7.0.2 build 0031 and 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, 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 8.0.0, use FortiClient 8.0.0.

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. FortiNDR
16. FortiTester
17. FortiMonitor

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 8.0.1. When Security Fabric is enabled in FortiOS 8.0.1, all FortiGate devices must be running FortiOS 8.0.1.

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*.

FortiGate 6000 and 7000 upgrade information

To make sure a FortiGate 6000 or 7000 firmware upgrade is successful, before starting the upgrade, Fortinet recommends you use health checking to make sure the FIMs and FPMs are all synchronized and operating as expected.

If you are following a multi-step upgrade path, you should re-do health checking after each upgrade step to make sure all components are synchronized before the next step.

You should also perform a final round of health checking after the firmware upgrade process is complete.

For recommended health checking commands, see the Fortinet community article:Technical Tip: FortiGate-6000/7000 Chassis health check commands.

Both management boards and all of the FPCs in a FortiGate 6000 FGCP HA cluster run the same firmware image. You upgrade the firmware from the primary FortiGate 6000 management board.

All of the FIMs and FPMs in a FortiGate 7000 FGCP HA cluster also run the same firmware image. You upgrade the firmware from the primary FIM in the primary FortiGate 7000.

A graceful firmware upgrade of a FortiGate 6000 or 7000 FGCP cluster only causes minimal traffic interruption. Use the following command to enable graceful upgrade.

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

To improve session synchronization during a graceful upgrade, you can also enable `session-pickup`:

```
config system ha
   set session-pickup enable
end
```



For the FortiGate 7000F platform, enabling session pickup requires using the `session-sync-dev` option to select one or more interfaces to use for session synchronization. The recommended session synchronization configuration is to add two 100Gbps FIM management interfaces to a LAG and configure the HA `session-sync-dev` option to use this LAG for session synchronization. The recommended interfaces to use for this LAG are the M1 interface of the FIM in slot 1 and the M1 interface of the FIM in slot 2. You should use a switch to connect the LAGs in the two chassis. To support graceful upgrade with session synchronization:

```
config system ha
   set upgrade-mode uninterruptible
   set session-syn-dev <lag>
   set session-pickup enable
end
```

During a graceful firmware upgrade the secondary FortiGate 6000 or 7000 upgrades its firmware first, traffic then fails over to the secondary FortiGate 6000 or 7000 and then the primary FortiGate 6000 or 7000 firmware is upgraded. 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.

Normally, you would want to enable `uninterruptible-upgrade` to minimize traffic interruptions. But `uninterruptible-upgrade` does not have to be enabled. In fact, if a traffic interruption is not going to cause any problems, you can disable `uninterruptible-upgrade` so that the firmware upgrade process takes less time.

As well, some firmware upgrades may not support setting `upgrade-mode` to `uninterruptible`. Make sure to review the release notes before running a firmware upgrade to verify whether or not setting `upgrade-mode` to `uninterruptible` is supported to upgrade to that version.

Password policy enforcement

After upgrade to FortiOS 7.6.5 or later, the password policy is enforced, and your password must meet the requirements before you can log in to FortiOS. Passwords must contain:

- 1 uppercase letter
- 1 lowercase letter

- 1 special character
- 1 number (0-9)
- A minimum length of 12 characters

If your password meets the requirements, you can log in to FortiOS after upgrade.

If your password does not meet the requirements, you must change your password before you can log in to the GUI or CLI.

FortiGate VM upgrade requirement

Starting in FortiOS 8.0.1, FortiGate VM models support signatures in CMS (Cryptographic Message Syntax) format, and the support introduces a required intermediate upgrade step.

For FortiOS 8.0, you must upgrade the FortiGate VM to 8.0.1 before you can upgrade to 8.0.2 or later.

Product integration and support

The following table lists FortiOS 8.0.1 product integration and support information:

FortiManager and FortiAnalyzer	See the FortiOS Compatibility Tool for information about FortiOS compatibility with FortiManager and FortiAnalyzer.
Web browsers	• Microsoft Edge 135 • Mozilla Firefox version 138 • Google Chrome version 136 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 135 • Mozilla Firefox version 138 • Google Chrome version 136 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 0335 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
	  • Novell eDirectory 8.8

AV Engine	• 8.0018
IPS Engine	• 8.0048

See also:

- Virtualization environments on page 39
- Language support on page 39
- Agentless VPN support on page 40

Virtualization environments

The following table lists hypervisors and recommended versions.

Hypervisor	Recommended versions
Citrix Hypervisor	• 8.2 Express Edition, CU1
Linux KVM	• Ubuntu 22.04.3 LTS • Red Hat Enterprise Linux release 9.4 • SUSE Linux Enterprise Server 12 SP3 release 12.3
Microsoft Windows Server	• Windows Server 2022
Windows Hyper-V Server	• Microsoft Hyper-V Server 2022
Open source XenServer	• Version 3.4.3 • Version 4.1 and later
VMware ESXi	• Versions 6.5, 6.7, 7.0, 8.0, and 9.0.

Language support

The following table lists language support information.

Language support

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

Agentless VPN support

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

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 138 Google Chrome version 136
Microsoft Windows 10 (64-bit)	Microsoft Edge 135 Mozilla Firefox version 138 Google Chrome version 136
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 138 Google Chrome version 136
macOS Ventura 13.1	Apple Safari version 18 Mozilla Firefox version 137 Google Chrome version 136
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 8.0.1. To inquire about a particular bug, please contact Customer Service & Support.

Agentless VPN

Bug ID	Description
1272872	WAD blocks file uploads to an SSL VPN web app when SSL VPN traffic is processed by WAD.
1297439	GET /api/v2/monitor/vpn/ssl generates multiple subsessions for a single SSL VPN user when the API response uses different session matching conditions than the CLI.
1309910	Security vulnerability occurs when connecting to a malicious SSH server with crafted packets.

AntiVirus

Bug ID	Description
1125299	HTTP logs are missing HTTP method and agent information when uploading files using HTTP POST/PUT.
1260804	Zip file download is blocked when Antivirus profile is configured in Proxy mode and scanned by stream scan.
1281140	Fields are missing from Message ID 8195 when using multipart/form-data Content-Type
1307986	Server response is sent to FSA for scanning when FortiGate has FSA inline scanning enabled and client performs an HTTP POST to upload a file.

Application Control

Bug ID	Description
1264508	Application control fails to block small files through WeChat when using proxy inspection mode
1274897	Unknown app and appcat fields occur when IoT and OT rules are from different tables.
1283464	Video application signatures are not detected when QUIC protocol is used by browser
1285724	Inconsistency in Risk Score Display occurs when using CLI and GUI on FortiGate

Data Leak Prevention

Bug ID	Description
1279965	DLP keyword blocking fails when using keyword type with UTF8 encoded characters on Gemini and Claude.

DNS Filter

Bug ID	Description
1214371	DNS filtering over TLS is bypassed when SSL deep inspection is enabled and DNSfilter profile is in proxy mode.
1254420	High CPU usage occurs in dnsproxy when handling DNS requests for IPv6-only domains.
1254680	DNS-over-TLS fails when configured on FortiGate 201E with FortiOS 7.4.10
1265529	Wildcard FQDNs starting with '*.' do not match base domains when learning resolved IPs from DNS queries.
1278174	Safe search enforcement issues occur for bing.com when using IPv6 proxy policies
1294339	Excessive DNS queries occur when FortiSLB integration is disabled
1295373	SRV records are redirected to the mgmt interface instead of the VWP interface when a DNS filter profile is applied in the policy
1309271	Server failed message occurs when SRV type requests are blocked by DNS filter
1313580	Error condition in dnsproxy occurs when allocating DNS relay connections

Endpoint Control

Bug ID	Description
1285871	The fcnacd daemon fails to auto-update EMS connector fields in the FortiManager ADOM when the endpoint-control fctems-override configuration is updated.
1299308	ZTNA destinations are blocked with Implicit Deny when the FortiGate loses connection with the EMS server due to SSL verification failure.

Explicit Proxy

Bug ID	Description
1253730	Intermittent HTTPS request timeouts occur when proxy-based UTM inspection is enabled on a Virtual Server VIP.
1281206	Captive portal fails to appear when IPS is enabled on the proxy policy
1291974	Error condition occurs when FortiGate is configured with explicit web proxy and forwarding server using FQDN that resolves to both IPv4 and IPv6 addresses without an IPv6 interface
1292536	PAC file data is cleared when deleting a VDOM named 'root'
1292842	Unintended space is inserted when add-option append in web-proxy.profile.headers is used.
1298780	SSL websites fail to load in Firefox when FortiGate restarts
1303255	FortiGate presents Fortinet_CA_Untrusted certificate to clients when accessing HTTP Virtual Server on port 8080
1305730	Explicit proxy policy matches IPv4 destination when configured with IPv6 FQDN object and DNS server resolves only to an A record
1309716	Proxy Address Group trims members to a maximum of 10 when editing or cloning the group in the GUI.
1311271	Explicit or web proxy policies stop WAD from responding when a request attached to a 1way origin server is answered locally.
1319389	FortiGate does not respond properly to PAC file requests when a client sends an HTTP GET request after restoring configuration on a freshly installed device.
1321351	WAD drops FIN packets to the server on proxy-created IP sessions.
1322804	Explicit web proxy fails to load vdom-scoped configuration when a new vdom reuses the index of a deleted vdom.

Firewall

Bug ID	Description
1104208	NAT is not correctly applied to traffic when a single SYN packet is sent to a VIP without an acknowledgment or reset.
1225460	Traffic offload failure occurs when using back-to-back EMAC VLAN interfaces for inter-VDOM traffic
1232145	Traffic is blocked when auto-asic-offload is enabled on firewall policy with back-to-back EMAC VLAN and Inter-VDOM Link topology.
1234453	VXLAN traffic fails when offloading is enabled
1236578	SCTP COOKIE-ECHO packets are dropped when ASIC offloading is disabled on FortiGate.
1238766	SCTP traffic forwarding issue occurs when using the hardware switch on FortiGate-80F
1254325	Internet-service-database in on-demand mode downloads ffdb_on_demand files repeatedly during automatic updates if the ffdb version remains unchanged.
1254541	IPsec tunnels and offloaded sessions restart when a QoS profile is configured
1257907	NTurbo offload fails when using inter-VDOM links on FortiGate.
1270066	Shaping statistics unavailable when UTM is enabled in policy on SOC5 platform
1270494	Egress shaping-profile cannot accurately limit maximum-bandwidth on VLAN interface when configured on its parent interface on SoC5 models.
1270575	Traffic fragmentation issues occur when passing through multiple VDOMs on FortiGate
1271340	L2TPv3 packets are discarded when protocol 115 is not included as a known protocol on FortiGate
1274475	Fragmented packets are forwarded to different LAG member ports when LAG hashing uses both L3 and L4 fields.
1275753	Traffic is allowed by incorrect firewall policy when NAT64 rules are evaluated incorrectly with multiple policies configured.
1276696	Interface bandwidth shaping fails to enforce aggregate limits on NP7 models during parallel streams.
1277509	Unexpected behavior related to the QTM module when egress-shaping-profile is configured on the parent interface of a VLAN interface.
1279396	TLS_AES_256_GCM_SHA384 cipher suite is not advertised when using an EC384 certificate on a VIP
1280020	COS marking is removed when traffic is accelerated over a hardware switch
1280836	Installation failure occurs when setting a large number of address objects in firewall policy

Bug ID	Description
1281193	FTP passive mode fails when FortiGate is not performing NAT after firmware upgrade from 7.4.9 to 7.6.6
1283427	Traffic disruption occurs when offloading is enabled in the firewall policy
1283624	Address range comparison issues occur when using debug flow filters
1286715	After a firewall address is renamed, duplicate addresses can be accepted in a firewall policy without errors from the CLI.
1286869	Session offloading fails when sflow configuration is removed
1291290	SNAT session persistence occurs when route changes with snat-route-change enabled
1292043	Session count increase occurs when asymmetric ECMP return traffic is combined with auxiliary-session handling after upgrading the connected router.
1293223	NetFlow packets are sent as Template 259 when carrying IPv4 information
1295481	Multicast packets are forwarded to the incoming interface when switch-controller-access-vlan is enabled on that interface.
1298800	Source addresses are removed from firewall policies when upgrading to FortiOS 8.0
1299325	A reboot resets diffservcode values to 00000 when diffservcode-rev 000011 and diffservcode-forward are set in a firewall policy.
1301104	VIP health check failure occurs when backend servers are reachable through a non-default VRF
1308113	An error condition occurs in the SSL configuration when setting ssl-server-algorithm custom twice with ssl-server-min-version set to client
1308123	PRP/MMS/SNMP packets are blocked when PRP NPU attributes are enabled for a transparent vdom on FortiGate Rugged 70F
1308568	Inconsistent Round-Trip Time behavior occurs when using the Least RTT load balancing method with Ping health checks
1309219	SNAT issues occur when VRFs route leaking and SSL Deep Inspection FQDN Exemption are configured with flow-based inspection
1314405	Fragmentation drops COS marking on outgoing packets.
1316379	Configuring 221 or more srcaddr objects in a local-in policy causes FortiGate to reboot unexpectedly.
1321678	Traffic logs display an incorrect custom service name when multiple services match a flow.
1326219	MAC-type dynamic fabric addresses fail to match security policies when configured as source or destination addresses in NGFW policy mode.
1335398	Virtual Server generates HTTP 504 Gateway Timeout errors when the backend server requires rsa_pkcs1_sha256/384/512 for TLS 1.2 handshakes.

FortiGate 6000/7000 Platform

Bug ID	Description
895242	The default setting of "uninterruptible-upgrade" is inconsistent between SLBC and regular FortiGate platforms.
947982	Audio cutouts occur when CG_FULL errors are high on NP7 models
1241479	IVS related DCE counters do not work as expected on SoC5 platforms.
1275854	Merge occurs when FortiGate-400G and 401G models are integrated into FortiOS 7.x
1277890	HA memory-based-failover support based on FPM memory utilization is not supported on 6K/7K platforms.
1280968	IGMP join issues occur on interfaces configured in virtual switch on FortiGate.
1283535	fragmented IKE packet drop
1307574	License sync issue occurs when VDOM license is added to the FIM through the GUI
1314590	FGCP HA is not supported for HA between an AC powered and a DC powered FortiGate 6000F, FortiGate 7000E or FortiGate 7000F chassis.
1322916	Setting ipsec-tunnel-slot to auto on SLBC platforms limits scalability by assigning IPsec ESP workers based on a gateway hash.

FortiView

Bug ID	Description
1158855	An error condition in FortiGate occurs when generating a query after using the Fortinet Support Tool for GUI capture.
1310841	FortiView displays the firewall policy instead of the proxy policy when "Show in FortiView" is selected for a proxy policy.

GUI

Bug ID	Description
463029	Tooltip display issues occur when address or service groups have long names
981278	Devices are not displayed on the OT view page when a large number of devices are detected

Bug ID	Description
1027218	The "clients" link on the Diagnostics page of any FAP opens one type of client (any of 2.4GHz, 5GHz, or 6GHz bands) and then becomes unresponsive.
1040164	Interface X1/X2 does not display on the GUI-Network-Interface page faceplate for FortiGate-90G Gen2.
1058668	Export to CSV/JSON file fails when policy number exceeds 700 due to non-existent application id
1145907	The bandwidth widget reports traffic incorrectly on a backup VLAN interface on FortiGate NP6 platform models when fast-path processing is disabled.
1194766	Search functionality issue occurs when viewing threat feed entries from the GUI.
1194972	Devices are not visible on Asset & Identities > OT view when API response from /api/v2/monitor/user/device/query retrieves devices without sufficient information.
1200390	An error condition in httpsd occurs when processing requests with invalid JSON filter parameters.
1212624	Memory usage issues caused by the V8 JavaScript engine
1217015	Faceplate loading issue occurs when hovering over WAN interface in multi-vdom mode
1223774	Firewall policy GUI page shows 'no-inspection' for SSL when profile group is applied.
1225806	Memory usage issues caused by V8 ExternalPointerTable leak
1228030	GUI displays the wrong help message when changing the guest-admin password after login with guest-admin.
1228366	Network interfaces are displayed in incorrect order when accessing Network>Interfaces on FortiGate 30G.
1229180	Unknown status occurs when loading config with 9k+ tunnels across VDOMs
1229684	The FortiGate VM License page is not displayed in the GUI when the FortiGate VM is unlicensed
1231257	GUI policy match tool generates "Policy match failed due to internal error" when intrazone traffic is enabled on a WAN interface.
1246460	Incorrect interface information appears when hovering over SFP icon on FGR-70F-3G4G
1249113	FortiClient-managed devices with network interfaces connecting to different VDOMs may create multiple interface entries in the user-device-store causing memory usage issues.
1249651	No interface bandwidth is displayed when traffic passes through virtual-switch interfaces
1257351	Viewing or refreshing the Replacement Messages page causes the GUI to lose connection temporarily.
1260292	Print button is not visible when using prof_admin profile after FortiOS upgrade
1261256	FortiGate displays the upgrade page instead of restarting the FortiAP when clicking Restart and OK on the FortiAP edit page.

Bug ID	Description
1261462	Error saving request object to CLI occurs when editing copied ISDB policies with FQDN address in destination
1262347	Multiple clicks are required to configure wildcard URL filters from the GUI
1264166	GUI CLI console generates "Connection lost. Press Enter to start a new session." under FIPS-CC mode.
1265960	Incorrect bandwidth values occur when configuring LAG interfaces for inbound and outbound traffic
1267983	The GUI custom creation page displays IKE proposals and DH groups that do not match the default CLI recommended list.
1271369	SAN format options are not available in GUI when creating a CSR on FortiGate
1274070	File name does not update with CLI console name when renamed
1274994	Duplicate policy entry occurs when numerous policies are configured with implicit policy enabled
1276291	Firewall Users Method and User Group graph disappears when using FortiGate v7.4.11
1277699	Incorrect display of device and hostname with Korean characters occurs when device detection is enabled and Windows computer name contains Korean characters.
1277938	Log application health metrics cannot be saved when auto-asic-offload is enabled in CLI
1277951	Packet capture file download fails when session ID exceeds the maximum value.
1278004	Having 5500 security policies causes the Security Policy page to stop responding.
1278206	HTTPS GUI access fails when using a Low Encryption license after upgrading to FortiOS 7.4.11
1278887	Application Sensor Clone fails to save modifications when cloning an existing sensor.
1279207	Changing the accprofile setting of a remote admin generates "Empty values are not allowed..FortiToken is invalid" error.
1280043	FortiGate GUI hides srcaddr6 and dstaddr6 fields when nat46 is enabled.
1280868	The FortiSwitch Ports page displays no results when filtering the Device Info column by MAC address.
1282020	Duplicate policies occur when sections share the same global-label
1282578	An error condition occurs in httpsd when receiving an unexpected signal.
1285288	FortiSwitch Clients search for MAC address displays 'No Results' in a multi-VDOM environment where the switch and its connected endpoints are not in the same VDOM.
1291013	An error condition occurs when accessing FortiAI settings from FortiGate
1291914	An error condition occurs in the service creation process when using ICMP protocol.
1292309	Slow scrolling occurs on the policy page with a large number of policies

Bug ID	Description
1293641	Systems events memory log page appears grey or blank when navigating to Log & Report Event Log
1300025	Admin session termination occurs when using Chrome or Edge browsers for login.
1301041	An error condition in httpsd occurs when serving error responses through Apache ErrorDocument sub-requests
1304918	Automation Stitch edit page displays the wrong HA cluster destination in a CSF fabric with multiple FortiGate HA clusters.
1306049	A blank page appears when accessing the GUI after upgrading to v7.6.7
1307573	Multiple categories appear for the same user group in Sequence Grouping View after upgrading to FortiOS 7.6.7
1308729	Changing DNS settings to specify on a FortiClient IPsec VPN tunnel causes the GUI OK button to spin and fail to apply changes.
1309235	Address object search issues occur when filtering by IP address in the GUI
1310172	GUI restore generates 413 Content Too Large when restoring a configuration with 200K policies.
1310806	Fast scrolling on the Firewall Policy and Address Objects pages displays a blank white page.
1311656	Editing an existing SD-WAN member displays blank Interface and Zone fields.
1312045	FortiSwitch Ports search generates ERR_HTTP2_SERVER_REFUSED_STREAM and disconnects the GUI user.
1312386	FortiGate fails to load the Interfaces page in the GUI for the root VDOM in multi-VDOM mode.
1312573	Read-only users fail to add dashboard widgets when a FortiGate is centrally managed by FortiManager.
1313617	The GUI allows unsetting the mandatory manageip on Transparent mode VDOMs.
1315353	Unable to add address objects occurs when self-reference is set in exclude-members
1316392	The dashboard Administrators widget stops httpsd from responding when an admin session contains a NULL field.
1317062	Hit count is not visible in the GUI for SNAT policies when Central SNAT is configured
1320690	The GUI hides the dedicated management interface when configured in dedicated-mgmt.

HA

Bug ID	Description
1031043	Incorrect information appears on the HA page when the HA cluster is in MVC mode

Bug ID	Description

1205727	You may be able to reduce FGCP HA failover times by changing the the NP7 link scan interval. The NP7 link scan interval is the amount of time that a FortiGate with NP7 processors waits between scans to determine if a link has failed. A shorter NP7 link scan interval can cause the FortiGate to send gratuitous ARP packets sooner after an HA failover has occurred.
	
	`config system npu`
	`  set np-linkscan-interval <milliseconds>`
	`end`
	
	The np-link-scan-interval range is 50 to 1000ms. The default NP7 link scan interval is 1000 milliseconds (ms). If your FGCPHA cluster experiences longer than expected HA failover delays (for example a 2-second interval for a failover to occur)reducing the NP7 link scan interval may reduce HA failover delays.

1226122	System > HA: There is no "upgrade" button on secondary GUI page when HA in "local-only" or "secondary-only" MVC upgrade mode
1233776	FSSO user list disappearance occurs when HA failover happens twice.
1258325	FortiToken Mobile push fails when private-data-encryption is enabled after a full HA cluster shutdown
1260236	Unexpected power off events occur in FortiGate 70G when configured in HA Active/Passive mode with wireless traffic.
1265113	Return traffic occurs when virtual cluster failover happens
1265208	High CPU usage issues observed during high session setup rates on secondary units.
1267616	FGSP session synchronization issues occur when FGSP links experience high latency.
1270605	HA cluster sync fails when adding a new VDOM in HA primary
1271356	Link down condition occurs on FortiGate 4801F when media type is set to SR and forward error correction is set to CL74-FC-FEC at 25G speed
1271911	Virtual MAC address is not set correctly when override-wait-time is enabled and secondary device is configured before timeout.
1273323	5G interface fails to reacquire an IP address after HA failover when in HA active-passive mode.
1275263	An error condition occurs in FGSP cluster when adding new nodes.
1278733	On HA setup, getting error 'Failed to load data.' when tried to configure new interface in GUI on 70G, 91G121G3001F, 4201F, 4801F.
1281897	Missing start time occurs when running diagnose sys ha dump-by group after upgrading to 7.6.6
1285215	TCP/135 traffic fails when DCE-RPC session helper is enabled with asymmetric traffic in FGSP-transparent mode

Bug ID	Description
1286934	Authentication issues occur in FortiCloud SSO during HA failover due to serial mismatch
1289905	DPD settings are added to some tunnels on secondary when type is dynamic
1291963	Traffic disruption occurs when duplicate joined ports are formed after HA switchover
1292078	High CPU usage issues observed during high-rate non-offloaded GRE traffic
1292621	A SCIM database exceeding 16MB leaves HA out of sync across secondary nodes.
1293476	BFD flaps occur when there is a FGCP or FGSP failover
1294331	HA synchronization issues occur when engine-id-type is set to hex
1294432	HA synchronization issue occurs when running auto-script to modify SDWAN member order in SDWAN rule
1296191	HA failover occurs twice within the same second when a secondary unit leaves the cluster with override disabled.
1296784	Session synchronization issues occur when FGSP is configured over FGCP cluster environment.
1298467	High CPU consumption occurs when policy package is pushed from FortiManager
1309304	Adding, removing, or renaming a FortiSwitch leaves the HA cluster out of sync.
1309845	Per-packet load balancing loops QUIC traffic in FGSP environments.
1310679	Creating a new local user on the primary unit leaves an HA cluster out-of-sync until a re-sync process completes.
1311587	HA cluster synchronization issues occur when private-data-encryption is enabled
1311938	Failover occurs when probe-response is added to port1 interface
1312803	Session sync packets from an unknown FGSP peer stop the sessionsync daemon from responding.
1317118	Adding a switch leaves the HA configuration out of sync because the event triggers a CMDB update only on the primary unit.
1323497	An IKE NAT port change blocks traffic after HA failover.

HyperScale

Bug ID	Description
1141632	The system fails to send new syslog packets when a highavailability failover occurs on FortiGate models.
1219541	Traffic disruption occurs when changing an interface's vdom

Bug ID	Description
1284721	BFD sessions drop when running diagnose firewall ippool list pba
1285581	A performance drop may occur on specific FortiGate model when processing TCP PBA NAT-overload and HTTP CPS traffic
1288505	Traffic disruption occurs when session sync between FGCP peers uses layer2 RLT packet
1290329	Packet loopback occurs when flapping a member of a LAG as hardware session sync device
1291520	DNS traffic drops occur when BGP to router 2 goes down

Intrusion Prevention

Bug ID	Description
1049160	IPSA self test failure occurs when upgrading to FortiOS 7.6.0 build 3388 with debug image.
1123425	OT signatures are not displayed after FortiGate reboot
1197659	An error condition in IPS engine occurs when processing HTTP traffic
1259235	An error condition in ipsengine occurs during upgrade to 7.4.11
1263949	An error condition in IPS Engine occurs when switching packet layer modes
1267456	A ClientHello packet larger than the MSS generates an SSL error when retransmitted to the server.
1268468	UDP fragmentation bypasses IPS when NP is enabled in IPsec tunnel
1273729	Error condition in IPS occurs when handling high volumes of application traffic through FortiGate
1301558	An error condition in IPS engine occurs when upgrading to 7.6.7.
1301803	High memory usage occurs when running IPS engine version 8.0.34
1304696	HTTP2 traffic consumes excessive memory and leaves FortiGate in conserve mode.
1310986	When Application Control is enabled without enabling an IPS sensor, updating of OT threat definitions (ISDB) is incorrectly skipped.
1324330	Assets displays devices with an empty MAC address when IPS detects IoT devices.
1328188	Certificate inspection blocks TLS 1.0 connections when IPS engine is updated to 7.01196.

IPsec VPN

Bug ID	Description
1073893	When a large TCP packet enters an IPsec tunnel, the FortiGate no longer adjusts the TCP MSS value automatically. Instead, it sends an ICMP message (ICMP_FRAG_NEEDED) to notify the sender of the correct MTU size. The sender can then adjust the TCP MSS and subsequent packet sizes accordingly.
1103754	Failed HTTP sessions occur when passing through nTurbo due to improper handling of fragmented packets
1113625	Traffic disruption occurs when FortiExtender or LAN Extension sessions are offloaded on the FortiGate side.
1201323	The copy-dscp feature drops traffic with an original IPv4 checksum of 0xffff on NP7 models.
1206506	Traffic disruption occurs when IPsec tunnel manager write sequence issue happens
1222252	VLAN CoS marking fails when traffic goes through an IPSec tunnel
1236634	Renewing expired certificates in ipsec.phase1-interface causes iked to restart unexpectedly.
1243205	High CPU softirq usage occurs when using EMAC-VLAN interface with IPsec VPN on SoC5 platforms.
1246587	Traffic forwarding issues occur when NPU offload is enabled for IPSEC VPN
1248524	File download fails when FortiGate encounters IPSec VPN with set encapsulation vpn-id-ipip and AV proxy and NAT-T
1254266	IPsec dial-up VPN connection fails when username case sensitivity does not match for RADIUS users.
1263848	IKEv2 CERTREQ matching failure occurs when FortiGate acts as a common VPN server for multiple vendors with multiple CA certificates.
1266053	vpn-id-ipip encapsulation stops IPsec VPN traffic on FortiGate 50G.
1268238	Peer SNs are not exchanged when exchange-FortiGate-device-id is enabled
1272584	IPv4 multicast traffic over IPsec fails on FortiGate-6501F when configured on v8.0.0 and v7.6.7.
1273353	VPN tunnels experience intermittent disruption when IPSec VPN server certificates are renewed via SCEP
1273969	High memory usage occurs when VWL triggers shortcut-offer for existing shortcut tunnels in SD-WAN ADVPN deployment on FortiGate-40F and FortiGate-60F.
1276932	Site-to-site VPN establishment fails when using DDNS with duplicate DNS resolved remote gateway IP.
1278723	Traffic forwarding issues occur when MTU constraints are not properly configured for IPsec tunnels

Bug ID	Description
1278940	Unexpected behavior occurs in the system when receiving IPsec VPN traffic with large ICMP packets and NPU offload enabled
1283050	An error condition in IKE daemon occurs when using DDNS with specific network conditions.
1286310	Web traffic disruption occurs when ASIC offload is enabled on FortiGate with IPSec traffic and UTM inspection.
1287274	Loopback-asymroute option is not configurable when transport is set to auto.
1288373	IPsec phase2-rekey drops traffic and BGP neighbors on NP7 and NP7lite models when IPsec over VNE is configured with offloading enabled.
1293470	Data transmission issues occur in IPsec VPN tunnels when npu-offload is enabled on FortiGate.
1296071	Duplicate packets occur when offloading is enabled on NP7
1297016	FortiGate 50G drops ICMP packets over IPsec tunnels when NPU-offloading is enabled.
1304588	Intermediate CA is not sent in certificate payload for IKEv2 signature-based authentication when send-cert-chain is enabled on phase 1 settings.
1311512	An error condition occurs in IKEv1 when setting negotiate-timeout to 15 or lower.
1314786	IPsec VPN with vpn-id-ipip fails to offload some sessions on NP7 models.
1318272	Enabling system.settings.ike-policy-route after IPsec tunnel configuration blocks ESP traffic from reaching the egress interface.
1321797	PPTP connection failure occurs when Compression Control Protocol negotiation happens on FortiGate 120G
1328024	Tunnel gateway switching leaves the negotiation timeout outdated, which expires the tunnel negotiation before 2FA completes.

Log and Report

Bug ID	Description
1209432	Traffic logs display a wildcard custom service name instead of the preset service when both match a flow.
1237774	Log field information loss occurs when the URL or Referrer header exceeds a certain character limit
1241256	Failure to send OT information to FortiAnalyzer occurs when a large number of IoT/OT vulnerabilities are generated.
1250247	Authentication issues occur when FortiSASE VPN users connect over SPA site-to-site

Bug ID	Description
1261240	Repeated DNS resolution attempts occur when related functionality is disabled on FortiGate
1265088	Syslog packets are sent when syslog-override is enabled
1266492	Secondary unit logs are not received by FortiAnalyzer Cloud when running FortiOS 7.4.9 and above in a FortiGate HA cluster
1269067	Synchronization fails when generating a large number of IoT/OT vulnerabilities
1269332	FortiGate loses FortiAnalyzer serial number during failover from primary to secondary FortiAnalyzer
1278983	FortiSM violation logs are generated in error on hypervisor VM platforms due to SNMP lacking read access to the VM licensing information.
1281143	IPS archive logging fails after firmware upgrade to v7.6.6 due to incorrect folder permissions. Affects only FortiGates which have been upgraded from a version earlier than 6.4.2.
1281704	Anomaly category is unavailable when viewing log filter categories
1281906	Traffic logs are generated when logging is disabled on proxy policies after upgrading to FortiOS 7.6.6
1292012	An error condition occurs in FortiGate when accessing shared memory files.
1294193	Memory usage issues caused by logging connection disruptions to FortiAnalyzer
1308114	CEF format generates duplicate duser fields when logs contain both to and user fields.
1316969	Disk log cleanup deletes IPS PCAP archives when other UTM log categories are missing log files for the same roll number.
1321626	Concurrent DNS queries for the same FQDN generate "fgfm connection to device is down" logs without corresponding connection up logs.

Proxy

Bug ID	Description
1107714	An error condition in WAD occurs when the server's certificate key type mismatches the ServerKeyExchange signature type
1224454	SSL deep inspection blocks or bypasses traffic when the first ClientHello TCP segment payload is 1024B or less.
1244955	An error condition occurs in WAD during peer port validation.
1252579	High CPU usage occurs when proxy-based inspection mode is enabled and udp-not-quic traffic is allowed
1269317	An error condition in WAD occurs when upgrading FortiGate VM to FortiOS 7.6.6

Bug ID	Description
1276917	Phantom UDP/443 traffic occurs when UDP/443 traffic is redirected to WAD for QUIC handling and the packet is not QUIC on FortiGate 120G.
1280944	Traffic is blocked when the unsupported-ssl-version allow setting is enabled and the min-allowed-ssl-version is set to TLS 1.1
1281435	SSL deep inspection is bypassed when Firewall Policy is configured with WAF and proxy-based inspection.
1282767	FortiGate generates "secappdomain=WAD Violation: process-[wad_worker]" log messages at bootup.
1286767	Certificate selection issue occurs when multiple certificates are defined in an SSL profile in replace mode
1286815	CPU usage issues observed during high WAD worker process load
1287399	An error condition in WAD occurs when an unexpected VM failure or shutdown happens.
1291005	Connections are dropped when Implicit Deny is triggered due to an error condition in WAD caused by malformed LDAP objectSid attribute
1292478	The ech-outer-sni setting is not created when changing the SSL/SSH Inspection profile from deep-inspection to certificate-inspection on the first attempt
1294129	An error condition in WAD occurs when configuring VIP with HTTP3 support enabled and passing a large number of QUIC packets
1296246	FortiGate responds with TLS 1.1 and 1.0 when ssl-min-proto-version is set to TLSv1.2
1297169	Memory usage issues caused by proxy-inline-ips being enabled
1303431	An error condition in WAD occurs when validating certificates after upgrade from v7.6.6 to v7.6.7
1305726	TLS handshake failure occurs when TLS-AES-256-GCM-SHA384 is the only configured SSL cipher suite
1307625	Proxy-based mode in VWP policy slows website loading when NPU is enabled.
1322838	Enabling the WebSocket protocol causes the WAD daemon to consume increasing memory over time.
1323515	An FSSO identity lookup that returns no user and matches no proxy-policy stops WAD from responding.
1326200	A blocked WAD event loop consumes excessive memory and triggers Conserve Mode.
1326432	A virtual-server rebuild aborts existing HTTPS server-load-balance HTTP/1.1 keep-alive sessions.

REST API

Bug ID	Description
1159460	Current bandwidth value is not sent to FortiManager for shaping graph when using FortiOS API.
1265839	Group Filter functionality is impacted when a large number of users are authenticated.
1287958	POST /api/v2/monitor/system/firmware/upgrade generates HTTP 500 with API error -28 when upgrading firmware via REST API without the force parameter.
1314746	REST API JSON filtering of policy and address-group lists drops entries or displays incorrect results.

Routing

Bug ID	Description
1104206	AS number is not displayed when BGP is disabled and set to 0 in GUI/CLI
1142955	High CPU usage occurs when link monitor daemon fetches session counts on every interface during REST API calls.
1209642	No SNMP trap is sent when BGP state changes from Active to Idle
1247089	Route advertisement issues occur when using access-list with route-map
1260225	Route swapping issue occurs when injecting IPV6 BGP routes into BGP via redistribution
1267696	BGP network advertisement fails when AS is changed
1272227	Default routes are removed when configuring VIP with an external IP matching the gateway and restarting the routing process
1272281	VRRP failure occurs when using hardware-switch on FortiGate
1273467	Return traffic is not forwarded out of port15 when receiving GRE traffic via port15.
1277091	Suboptimal routing occurs when recursive-inherit-priority is enabled
1277718	Routing tables are incorrectly assigned to VRF 0 when restoring VDOM configuration
1278445	Intermittent BGP disruption occurs when IPsec SA negotiation fails during AUTH exchanges between two spokes.
1279315	Error condition in BGP process occurs when FIM failover sequence happens
1279665	CPU usage issues observed during zebos_launcher process execution on secondary FortiGate in HA A-P

Bug ID	Description
1305218	Route advertisement delay occurs when BGP neighbor comes up with non-zero advertisement-interval configured
1318738	FortiGate fails to delete IPv6 prefix routes when the prefix length is /0.
1324802	BGP delays IPv4 UPDATE messages and End-of-RIB when Graceful Restart is enabled and a BGP peer without the activated address family remains in the connecting state.

SD-WAN

Bug ID	Description
1252011	WAN outage occurs when upgrading FortiGate from 7.6.1 to 7.6.3 or 7.6.5 with SD-WAN and IPsec over VNE WAN links
1273960	Packet loss occurs when upgrading from 7.0.14 to 7.2.10
1279456	Link-Monitor instability occurs when a dead monitor uses the same ICMP ID as a working monitor.
1281211	Traffic disruption occurs when SD-WAN has 'embed-measured health' enabled on the spoke
1290462	VXLAN traffic does not properly behave based on SDWAN rules when SDWAN manual strategy is configured to pass traffic through one tunnel at a time.
1291673	Shortcut flapping occurs when traffic degradation happens on SD-WAN with ADVPN
1293595	Static route remains when health check server FQDN cannot be resolved
1306994	Unstable SDWAN connectivity occurs when Hub withdraws BGP routes
1312550	Packet de-duplication enabled on a receive SD-WAN duplication rule causes FortiGate to terminate TCP sessions shortly after establishment.
1315480	Link-monitor incorrectly collects dynamic BGP peer alive-count.
1323500	Changing DNS server IPs under config system dns stops SD-WAN Performance SLA health check probing for members when set system-dns enable is configured.

Security Fabric

Bug ID	Description
995772	Devices are missing from Asset identity center / OT View when API response from /api/v2/monitor/user/device/query retrieves devices without sufficient information.

Bug ID	Description
1050209	Duplicate security rating entries occur when adding a VDOM
1190754	A full tmpfs mount causes forticron to stop responding when updating MAC dynamic addresses in NGFW policy mode.
1210303	APIC device overload occurs when FortiGate logs in multiple times without proper logout.
1275814	Loss of connectivity occurs when AKS cluster provisioning state is not Succeeded
1277653	An error condition in csfd occurs when shared memory allocation fails.
1279316	Downstream FGTs lose firewall policy after root FortiGate upgrade to 8.0.0
1284732	An invalid URI format with protocol in the webhook automation action URI setting prevents the automation action from executing.
1294532	Automation stitch notification emails display truncated content for FortiAnalyzer-event triggers.
1296597	An error condition in Autod occurs when deleting deprecated triggers during upgrade to 7.4.12
1299849	Security Fabric authorization fails for FortiNAC-F when a corrupted CA certificate is present
1301642	An error condition in Autod occurs when using email automation-action
1309335	Duplicate empty VNet objects occur when Azure API returns VNet ID in all lower-case characters

Switch Controller

Bug ID	Description
1187046	FortiGate fails to detect FortiLink-HTTPS tunnel mode when FortiLink interface is enabled
1215775	Communication to management IP fails when a VLAN interface is assigned to a hardware switch in transparent mode
1221779	Device data is missing when querying FortiGate API on FortiOS v7.4
1227202	FortiSwitch configuration is erased when switch-controller fails to add port1 during reboot
1250878	Traffic mirroring issues occur when SPAN is enabled with hardware switch on FortiGate-60F
1254611	Communication fails when intra-switch-policy switches from implicit to explicit.
1269920	Firmware download fails when one firewall attempts to download FortiSwitch firmware from FortiGuard
1269995	An error condition in fltund occurs during upgrade to 7.6.6
1275148	Allowed VLANs are deleted when adding new allowed VLANs on a trunk port.

Bug ID	Description
1290022	Device information fails to load when FortiSwitch has a duplicate prefix name
1290927	Enabling stpforward on a hardware switch causes a network loop on SoC5 platforms.
1293984	FortiSwitch topology hides MCLAG ICL link.
1296864	Sync loss with FortiSwitch occurs when the default admin account is removed
1308243	Security group name changes to 'SSo_Guest_Users' when renaming the user group on FortiGate
1308689	FortiGate displays a FortiSwitch as discovered over CAPWAP when configured for fortilink-https.
1312267	Custom 802.1X security policy cannot be added to pre-provisioned FortiSwitch when authserver-timeout-vlan is enabled
1312703	FortiGate removes RADIUS configuration from a FortiSwitch when the switch is associated with another VDOM as a virtual switch during a reboot.

System

Bug ID	Description
953547	SCTP traffic does not get forwarded by a connected hardware switch on FortiGate.
985028	Link down issue occurs when connecting FGT1001F and Spirent TestCenter with FORTINET 100G DAC 5M cable due to missing mediatype cr4 option
1114381	FortiGate 40x/60xF: Packet loss occurs when congestion happens on FortiGate interfaces
1116876	VDSL connection failure occurs when configured on FortiGate 50G-DSL
1132153	CPU usage issues observed during factory reset on FortiGate-201F
1137047	An error condition occurs when entering FIPS-CC mode
1144387	FortiGate 50G DSL fails to acquire an IP address from a DSL modem
1161211	Memory usage issues caused by polling FortiGate memory usage
1168786	100G ports turn up after reboot when administratively down on platforms with Marvell switch like FortiGate 480xF.
1179827	Hardware switch configuration limitations occur when adding Wan1 and Wan2 on FortiGate
1190222	Incompatibility occurs when using 8G eMMC on 3XG/5XG/7XG/9XG models
1192303	On FortiGates with NP7 processors, the following new option is available to enable or disable VLAN accounting: `config system npu`

Bug ID	Description

	`set vlan-accounting {disable | enable}`
	`end`
	
	VLAN accounting is enabled by default.
	VLAN accounting on a busy FortiGate with a large number of VLANs can generate large numbers of VLAN lookup (SPV/TPV) messages. In some cases these messages can cause CG-FULL conditions or packet drops, especially on very busy systems.
	You can use the following command to reduce the number of VLAN accounting massages that are generated by increasing the VLAN accounting interval.
	
	`config system npu`
	`set vlan-acct-interval <milliseconds>`
	`end`
	
	The default VLAN accounting interval is 200 milliseconds. The range is 100 to 10000 milliseconds.

1193085	Proxy-arp configuration failure occurs when the proxy-arp address group exceeds 256 entries
1198563	FortiOS adds support for MAC address and virtual MAC address configuration for soft-switch and VLAN interfaces.
1208271	Downloading the full Malicious Certificate Database (MCDB) on every update consumes significant network bandwidth.
1213241	Identical bandwidth values occur when multiple EMAC-VLAN interfaces are on the same VLAN
1215120	BLE light blinks blue when FortiGate is set up with FortiZTP without CLI login
1222654	FortiGate-40F fails to display LAN A SPEED and WAN SPEED amber LEDs during the diag hardware test led nic-led.
1227167	Memory usage issues caused by the node process
1229444	TX counters are not displayed for EMAC VLAN interfaces when non-offloaded traffic is present
1229469	Internet connection fails when inserting SIM into FortiGate without manual APN configuration
1232594	NIC copper speed LED test fails when running HQIP on FortiGate-500E
1237876	High CPU utilization occurs when upgrading from FortiOS 7.2.11 to 7.4.9 in large MSSP customer deployments
1238339	Dedicated host queues occur when critical traffic like BFD, BGP, LACP is processed
1242126	Walking the SNMP mib2 ipRouteTable for a specific VDOM stops snmpd from responding when the route cache is large.
1244041	DHCP relay failure occurs when passing through LTE interface

Bug ID	Description
1245329	Configuration loss occurs when FortiGate enters extreme low memory mode
1247647	An error condition in the kernel occurs when VLAN flapping happens on the remote side of a VXLAN configured in one VDOM.
1248631	Intermittent reboot issues occur in FortiWiFi-50G when WiFi clients connect via RADIUS or ax bands
1254396	BLE LED continuously blinks Light Blue when using FortiZTP setup without CLI login
1254702	Unexpected behavior in the kernel occurs when handling IPv6 neighbor traffic within a subnet
1255091	Bluetooth remains active when configured with FortiZTP without CLI login
1259458	Intermittent reboot of FortiGate-71G caused by an error condition in the IPS engine.
1261417	An error condition in cmdbsvr occurs when OpenSSL cleans up resources.
1262407	NP7 models fail to optimize the VLAN hash table size when a large number of VLANs are used in production.
1262639	Bandwidth distribution issue occurs when using LACP after upgrade to 7.4
1264805	Unexpected behavior in the system occurs when upgrading to 7.4.9
1265180	Memory usage issues caused by logging on FortiCarrier-4400F
1265816	SPEED LED blinking occurs when upgrading to FortiOS 7.4.10 on FortiGate FG-40F
1268808	Packet drops occur when querying SNMP OID 1.3.6.1.4.1.12356.101.4.4.2.1.8 for Processor 13
1271259	Transceiver issue occurs when using FR-1 QSFP 100G with FortiGate
1273362	Port LEDs remain solid green when transmitting or receiving data on FortiGate 80F after upgrade to 7.4.11
1273485	25G SFP interface fails to function with Fortinet FN-CABLE-SFP28-5 DAC at 25000full speed
1273973	Backup config via SFTP using box.com fails when keyboard-interactive authentication is required
1275047	Port LEDs fail to illuminate when connected at 100Mbps with auto speed setting
1275741	Memory usage issues caused by np6 ring buffer filling up
1276129	Unexpected behavior in WAD procmgr occurs when mounting chroot jails on FortiOS 7.6.6
1276466	Configuration mismatch occurs when restoring VDOM configuration from a backup file
1276713	Module violation occurs when stress testing with a large number of FAPs and clients
1277460	Speed setting changes to 10000auto when FortiGate-1000F is rebooted after configuring speed auto on port3

Bug ID	Description
1278263	Cleared sessions remain in diagnose sys session stat when an error condition occurs in WAD during client-side read operations
1279864	Auth-cert option is lost when executing config backup on global level in a multi-vdom environment with Captive portal configured on a VDOM-assigned interface
1280307	IPAM fails to de-conflict SASE GCP sites when DHCP-assigned interfaces are excluded from conflict scanning, which blocks SIA traffic.
1281707	Unexpected behavior in reportd and cmdbsvr causes device reboot.
1282367	SNMP bulkget fails to return expected index when non-existing SNMP index and FortiGate interfaces SNMP index are not continuous.
1283702	MTU configuration for VLAN interface is lost after reboot when VLAN is configured over a physical port or LAG.
1289434	LED activity lights do not blink when FortiGate is upgraded to version 7.4.x
1290014	Moving a VM from the root ADOM to customer ADOM fails when changing the vdom-type to admin
1290339	High CPU utilization occurs when FortiCron is running an auto-script
1290942	FortiGate-70G, FortiGate-71G, FortiWall-70G, and FortiWall-71G WAN interface SPEED LED remains lit after reboot when configured as admin-down with no Ethernet cable connected.
1291001	Password change fails for local admins with super_admin privileges when using non-ASCII characters.
1293990	Incorrect IPv6 SNMP interface counters occur when sessions are processed by the CPU.
1294887	LLDP transmission issue occurs when LLDP-MED inventory software revision value exceeds 32 characters
1295619	MTU size changes on WWAN interfaces are not applied when MTU override is enabled on FortiGate 5G models
1296265	FortiManager policy installation generates SNMP trap fgFmTrapConfChange.
1298759	Conserve mode occurs when high memory usage is detected in wad_dev_vuln process
1299330	Third-party CAPWAP fragments are dropped when they pass through NP7 or NP7Lite FortiGate.
1301576	High CPU utilization occurs when forticldd process experiences unlimited retries with no delay after a tcps read fails.
1304395	Traffic drop occurs when one member of an aggregate interface goes down in active mode
1304523	Traffic drop occurs when one LACP member link goes down
1304527	FortiASIC EEI Test generates "ASIC number not correct: expected 2, got 1" on FortiGate-900G, FortiGate-901G, and FortiGate-3700F/3701F.
1304601	Traffic drop occurs when one member of an aggregate interface goes down

Bug ID	Description
1307500	TX packet and byte counters increase when unused ports are in a link down state
1308703	Third-party CAPWAP fragments are dropped when they pass through NP7 or NP7Lite FortiGate.
1309281	Third-party CAPWAP fragments are dropped when they pass through NP7 or NP7Lite FortiGate.
1311807	Reachable value does not update after NTP recovery when NTP communication is restored
1314361	Wake-on-LAN packets are dropped by SOC5 families due to an incorrect checksum.
1314404	UWDB delta updates fail when delta update files contain only the header with no body.
1318095	The deletion of a user session during the execution of convert_k2u_ip_session_minimal_user causes FortiGate to reboot unexpectedly.
1318579	DHCP6C consumes excessive memory on the HA secondary unit when receiving transfer DHCP packets from the primary unit.
1323301	A reboot wipes the configuration installed from FortiManager.
1324050	DHCP relay fails to relay DHCP DISCOVER packets to the DHCP server when the interface index of the VLAN changes.
1324322	The 'show firewall address' command hides the 'associated-interface' attribute after another address object is displayed in the same CLI session.
1324928	Off-network .lic files generated on Windows generate "FortiGate Manual License is invalid" during manual license upload via TFTP.

Upgrade

Bug ID	Description
1270824	Firmware upgrade issues occur when upgrading 648FF via FortiGate GUI
1271250	A forced automatic firmware upgrade occurs when a valid FMWR license is in place and the device is not at EOES in an HA setup.
1277454	Upgrading from 7.6.6 to 7.6.7 may result in the loss of specific `config system global` settings (e.g., hostname, timezone, admin-scp, vdom-mode).
1280589	Upgrade failure occurs when standalone-mgmt-vdom is enabled in HA mode
1283092	Upgrade failure occurs when Private Data Encryption is enabled
1283493	Firmware image transfer delays occur when high latency is present across regions.
1283569	FortiGate force-upg is not automatically cancelled after manually upgrading to a new major.minior

Bug ID	Description
1287363	Boot failure occurs when importing customer configuration after upgrade on FortiGate
1287964	Forced upgrade occurs when FortiGate is configured to use FortiManager as update server and connect to Fortiguard when FortiManager is not available.
1302768	GUI firmware upload generates a signature-validation failure warning when the multipart upload truncates the firmware image.
1302814	The set keytab command is missing after upgrading from v7.6.6 to v7.6.7
1318917	Upgrading to FortiOS 7.6.6 on FortiGate 3200F, 3700F, and 4800F wipes virtual-wire-pair configurations.

User and Authentication

Bug ID	Description
1186128	Certificate enrollment fails when SCEP server requires HTTP POST
1211983	Certificate chain issues occur when firewall encounters a certificate renewal issue while using EST simplereenroll process
1212700	Authentication failure occurs when system zone name conflicts with VDOM name
1218458	Hardware token activation fails when CMDB write permission is enforced.
1226005	Incorrect FSSO server status appears as connected when password exceeds 16 characters
1233862	Certificate renewal through EST protocol fails when DNS lookup fails
1236839	An error condition in fnbamd occurs when referencing two peer users during certificate authentication
1249801	Certificate renewal fails when ike-tcp-service is enabled on the same interface as ACME
1252114	Tokens cannot be found when using a drift screen size of 1
1257281	TLS negotiation fails when FortiGate initiates a connection to an OpenLDAP server over LDAPS with TLS 1.3 and PQC parameters.
1258884	Password expiry override does not work when configured with unset password-expire
1263909	Certificate enrollment and renewal fails when FortiGate uses HTTP GET instead of HTTP POST for SCEP requests
1266066	Authentication failure occurs when using FortiToken for two-factor authentication after upgrading from FortiOS 7.6.4 to 7.6.5
1271821	Token verification fails when username case sensitivity does not match for LDAP users with 2FA enabled.
1279114	Certificate renewal issues occur with EST when source-ip is enabled

Bug ID	Description
1283430	Firewall auth list is flushed when DHCP client renews its lease
1286569	Authentication failure occurs when primary Radius server connection fails
1286748	A corrupted or missing SCIM database generates "totalResults": -1 in the ListResponse.
1286845	Hardware token activation fails when provisioning via serial number
1287880	Entra ID generates a timeout error during SCIM provisioning when adding a user to an existing group.
1295720	An error occurs when updating a certificate via CLI due to invalid certificate input.
1299410	Network disruption occurs when CMDB edits are made to RSSO related tables
1299861	Renaming a CA certificate causes a PKI user to fail to match the CA of the certificate used.
1302924	Executing "execute vpn certificate local generate" as a FortiManager script with HA enabled generates an invalid certificate.
1304425	An expired or revoked certificate in the certificate chain consumes CPU on FortiGate.
1310424	EAP authentication fails when a SCIM-type group is configured in a firewall policy
1320742	FortiGate fails to authenticate administrators when the password contains a backslash (\) set via CLI.
1325322	Changing authentication configuration during a SAML authentication loop stops WAD from responding.

VM

Bug ID	Description
978021	In FTP passive mode with GWLB setup, Geneve header VNI lengths are zero in syn-ack packets, leading to retransmission issues.
1114866	QAT support occurs when Intel Xeon CPU QAT feature is enabled on FortiGate VM
1115988	Security Fabric Connector and Firmware and Registration pages display incorrect registration status when loading FortiFlex VM license
1188422	FFW_VM License validation fails when FortiManager is configured as a license server
1218373	Auto-scale failure occurs when creating FortiGate-AWS auto scale group with AWS CloudFormation
1240898	DPDK on VM platforms restarts the ipsengine unexpectedly.
1251567	Error messages are printed in the serial console when DPDK is enabled.

Bug ID	Description
1263961	Incomplete subscription retrieval occurs when Azure SDN Connector encounters pagination with more than 50 subscriptions.
1278705	Firewall policy sync fails when system auto-scale is enabled on AWS instance type c5n.xlarge
1279090	An error condition occurs when using the integer option for ibm-region
1282482	Hardware checksum failure occurs when Confidential VM and gvnic features are enabled on GCP VMs
1286979	License issues occur when FortiGate-VM64-OPC obtains FortiCare generated licenses
1288202	Boot failure occurs when Microsoft Secure Boot certificate expires
1294311	SDN connector fails to manage Azure vWAN when deployed in GermanyWestCentral location
1296294	DNS resolution failures occur when update-server-location is set to usa or eu
1297036	Incorrect network interface ordering relative to Azure causes bootstrap failure.
1301244	Upgrade to new open-vm-tools version occurs when using FortiGate_VM64
1303540	Secondary private IP fails to move during HA failover when using OCI SDN Connector with HA support enabled on FortiOS 7.6.7
1306348	LAG creation fails when setting the MAC address on FortiGate-VM with SRIOV interfaces
1311756	Instance token refresh fails when certificate file size exceeds the fixed buffer size in FortiGate VM.
1318073	Azure SDN connector fails to initiate API calls to management.azure.com during HA failover when the connector has not finished initialization.
1323635	Secondary FortiGate fails to validate VM License with FGD when validation with FortiManager fails on VM platforms.
1324904	Live Migration on Azure VMs wipes RPS settings in config system affinity-packet-redistribution.

VoIP

Bug ID	Description
1276335	Memory usage issues caused by voipd daemon with TCP socket connections

Web Application Firewall

Bug ID	Description
1229944	Credit card information is not blocked by WAF profile when mimetype is application/octet-stream

Web Filter

Bug ID	Description
1237517	Slowness occurs when deleting a large number of URL entries pushed from FortiManager to FortiGate

WiFi Controller

Bug ID	Description
1086302	Random users may experience unexpected authentication loss caused by IP address reassignment clearing active sessions for other stations.
1093829	WiFi Channels may appear empty in the FAP K-series profile for Taiwan on the 6GHz radio (Radio2) when the channel bandwidth is set to 320MHz(Wi-Fi 7 channel).
1105433	Running 'diag wireless wlac show all' during debugging causes unexpected AP disconnections in large-scale FAP deployments.
1112629	FAP offline and online again 30 seconds later after FortiGate HA failover
1144969	Inconsistent IP addresses may display between the GUI page and the device column hover popup when WiFi client switch between different SSIDs.
1191416	Multicore generates different WTP session counts between Primary and Secondary FortiGate in large scale setups.
1221706	Captive-portal VAP configuration not syncing to Secondary Firewall
1239578	The secondary unit in HA setup could not show WLAN sessions and client connections when the value of acd-process-count is larger than 1.
1242199	SSID interface is missing in routing table after FortiManager pushed the configuration to FortiGate

Bug ID	Description
1257588	WiFi clients experience random disconnections on WPA3-Enterprise SSID with External RADIUS
1267078	Wifi client moves to another FAP and needs authentication again after authenticated via Cisco ISE
1287896	Status synchronization may fail between FortiGate and FortiAP when multicore processing is enabled.
1301027	FAP unable to Register to FortiGate on VPNv4/VRF segment
1303265	Communication failures occur between the firewall and access points during a failover event triggered by a hostapd process failure.
1306168	Enabling invalid-mac-oui in the WIDS profile consumes excessive cw_acd memory.
1314858	FAP not coming online when managed by a remote FortiGate using PPPoE link
1320951	hard-timeout is not respected in the firewall auth session for radius wsso users flag(110)

ZTNA

Bug ID	Description
1278235	Incorrect keyboard layout occurs when using ZTNA web portal
1280530	Connection failure occurs when outgoing-ip is configured under Explicit Proxy
1295219	An error condition occurs when the server returns a 302 redirect
1300390	UUID becomes all-zero when FortiManager installs policy package with ZTNA EMS tag dynamic address objects on FortiGate
1302743	Load balancing info and preconnection-blob are not added to RDP packets when configuring ZTNA Web Portal with RDP Bookmarks.
1310884	HTTP OPTIONS requests are blocked when using agentless ZTNA.
1321696	ZTNA portal hides the Download FortiClient button when configuring ZTNA agentless web-based application access.

Known issues

Known issues are organized into the following categories:

- New known issues on page 70
- Existing known issues on page 70

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 8.0.1.

FortiGate 6000/7000 Platform

Bug ID	Description
1292637	6000F / 7000F support Multipath IPsec feature #1235059

Upgrade

Bug ID	Description
1343135	Upgrading to 8.0.1 GA.F configuration with names beginning with a period "." will be lost **Workaround**: Before upgrading, rename any configurations whose names begin with a period (.).

Existing known issues

The following issues have been identified in a previous version of FortiOS and remain in FortiOS 8.0.1.

AntiVirus

Bug ID	Description
1307848	Eicar passes when two security policies are configured, first one denies application and second one enables AV scan. **Workaround**: Use wildcard policies to block AV reliably

FortiGate 6000/7000 Platform

Bug ID	Description
1130491	Traffic disruption occurs when WCCP is enabled on FortiGate **Workaround**: Direct all related traffic to master FPC
1131269	UESP packet drop occurs when VPN peer uses different source ports for IKE-NATT and UESP **Workaround**: Add a flow rule to work around the issue
1250240	Traffic disruption occurs when kernel routes are not synchronized across the FPM. **Workaround**: Run diag test application chlbd 3 on the slot that's missing routes to trigger a manual routes redownload.
1336373	7121F-2 (FIM-7941)/b0245: 100G FR transceiver link fails when RS-FEC is enabled on 1-P4, but works with FEC disabled

GUI

Bug ID	Description
1102594	HA status on the Global Dashboard changes unexpectedly during hard refresh
1190683	Fabric Connector status shows as DOWN in GUI after failover on Azure SDN Connector cluster **Workaround**: Logout and login again to the GUI
1205102	Traffic logs cannot be viewed when Resolve unknown applications is enabled **Workaround**: Disable Resolve unknown applications under the global settings of log settings
1232828	Unresponsive GUI occurs when httpd is fully loaded on the forward traffic page **Workaround**: Disable Resolve unknown applications in the log settings
1237136	Dynamic VLANs are not visible on the GUI when a port-security-policy is applied
1249752	Incorrect HA status occurs when switching to mgmt-vdom vdom on FortiGate-6001F
1262047	Connection loss occurs when web-svc-perf is enabled under log settings

Bug ID	Description
	Workaround: Disable web-svc-perf under log setting
1265107	Blank page displays in GUI when vdom_admin logs in but lacks root access
1265177	Display issues occur in FortiView widgets when FIPS-CC mode is enabled **Workaround**: Create another super-admin profile to assign to the new admin.
1265862	On FortiFirewall, GUI displays incorrect log traffic status when firewall policy is configured via CLI **Workaround**: Use set logtraffic all/disable instead of unset logtraffic
1274560	Non-resolvable FQDN objects intermittently show a red box around the object name when filtered by FQDN type in the Policy & Objects section on FortiGate.

HA

Bug ID	Description
1246177	Warning pop-up is not displayed on FGCP cluster members in clusters with more than 2 members
1249251	TCP session failover fails when using NGFW policy-based mode after HA failover.
1273324	SNAT uses incorrect IP address after HA failover **Workaround**: Delete and re-add the secondary IP configuration manually
1285091	Config sync failure occurs when standalone-config-sync is enabled

HyperScale

Bug ID	Description
1200885	Renaming an ippool in a FortiGate setup with VDOMs results in unintended behavior affecting network traffic.
1262881	Hw session sync dev goes out of sync due to the discrepancy in lag driver between primary and secondary

IPsec VPN

Bug ID	Description
1238675	Connection fails to establish when FortiClient VPN Android connects to FortiGate IPsec IKEv1

REST API

Bug ID	Description
1267118	Filters are ignored when using the /firewall/sessions API call

Routing

Bug ID	Description
1260891	BFD packet transmission issues occur when a port member of the aggregate interface is shut down and then brought back up on the switch side. **Workaround**: Change bfd-detect-mult to 7 on both sides.

User and Authentication

Bug ID	Description
1241530	LDAP authentication fails when password is not sent in bind request

Built-in AV Engine

AV Engine 8.0018 is released as the built-in AV Engine.

Resolved engine issues

Bug ID	Description
1003433	In a rare situation, the file filter may mistakenly classify PDF files as BAT files, leading to an undesired blockage of these files.
1215491	DLL files are incorrectly blocked as EXE when both DLL and EXE are configured in proxy mode

Built-in IPS Engine

IPS Engine 8.0048 is released as the built-in IPS Engine. Refer to the IPS Engine Release Notes for information.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

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

Open source XenServer limitations

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



www.fortinet.com

Copyright© 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.