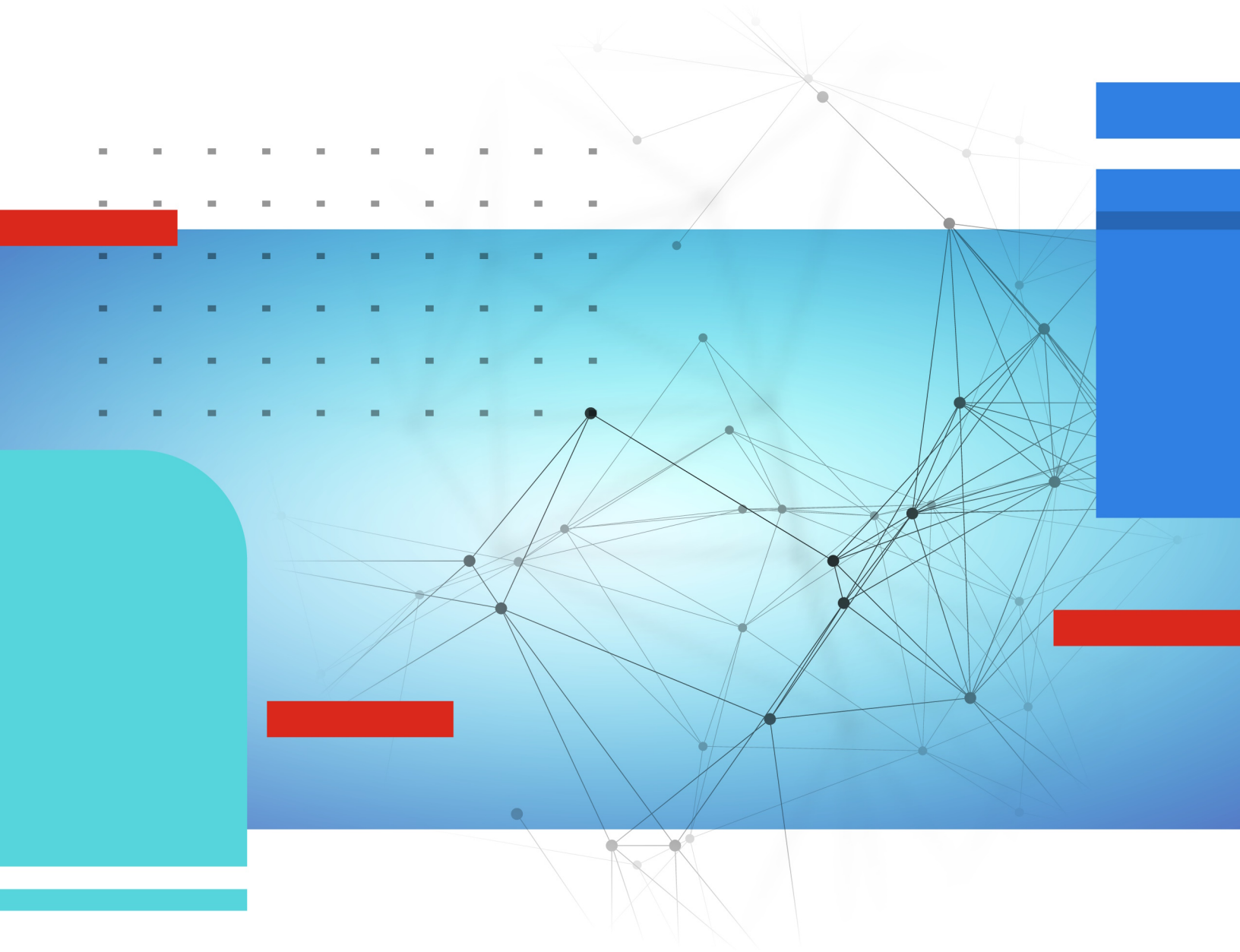
Release Notes

FortiOS 7.6.0



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

June 16, 2025
FortiOS 7.6.0 Release Notes
01-760-1019331-20250616

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-07-25	Initial release.
2024-07-30	Updated New features or enhancements on page 15, Resolved issues on page 47, and Known issues on page 78.
2024-08-06	Updated Special notices on page 9, Resolved issues on page 47, and Known issues on page 78.
2024-08-14	Updated New features or enhancements on page 15, Resolved issues on page 47 and Known issues on page 78.
2024-08-15	Updated Virtualization environments on page 43.
2024-08-16	Updated Resolved issues on page 47 and Known issues on page 78.
2024-08-26	Updated Resolved issues on page 47 and Known issues on page 78.
2024-09-03	Updated New features or enhancements on page 15, Resolved issues on page 47, and Known issues on page 78.
2024-09-12	Updated New features or enhancements on page 15, Resolved issues on page 47, and Known issues on page 78.
2024-09-16	Updated Known issues on page 78.
2024-09-18	Updated Known issues on page 78.
2024-09-19	Updated Resolved issues on page 47 and Known issues on page 78.
2024-09-23	Updated Resolved issues on page 47.
2024-10-02	Updated Resolved issues on page 47 and Known issues on page 78.
2024-10-15	Updated Resolved issues on page 47 and Known issues on page 78.
2024-10-24	Updated Fortinet Security Fabric upgrade on page 37.
2024-10-28	Updated New features or enhancements on page 15, Resolved issues on page 47, and Known issues on page 78.
2024-11-01	Updated SSL VPN removed from 2GB RAM models for tunnel and web mode on page 9.
2024-11-11	Updated New features or enhancements on page 15, Resolved issues on page 47, and Known issues on page 78.
2024-11-27	Added Default setting of cp-accel-mode is changed to none on 2GB memory models on page 40. Updated New features or enhancements on page 15, Resolved issues on page 47, and Known issues on page 78.
2024-11-28	Updated New features or enhancements on page 15.

Date	Change Description
2024-12-10	Updated Virtualization environments on page 43, New features or enhancements on page 15, and Known issues on page 78.
2024-12-19	Updated Special notices on page 9.
2024-12-23	Updated New features or enhancements on page 15, Resolved issues on page 47, and Known issues on page 78.
2025-01-02	Updated Introduction and supported models on page 8.
2025-01-15	Updated Resolved issues on page 47.
2025-01-20	Updated Resolved issues on page 47.
2025-02-04	Updated Resolved issues on page 47 and Known issues on page 78.
2025-02-18	Updated Resolved issues on page 47 and Known issues on page 78.
2025-03-03	Updated Changes in default behavior on page 13, Resolved issues on page 47, and Known issues on page 78.
2025-03-17	Updated Resolved issues on page 47 and Known issues on page 78.
2025-03-31	Updated Resolved issues on page 47 and Known issues on page 78.
2025-04-17	Updated Changes in CLI on page 11, Resolved issues on page 47, and Known issues on page 78.
2025-04-28	Updated Resolved issues on page 47 and Known issues on page 78.
2025-05-13	Updated Resolved issues on page 47 and Known issues on page 78.
2025-05-27	Updated Resolved issues on page 47 and Known issues on page 78.
2025-06-05	Updated Changes in CLI on page 11.
2025-06-06	Updated Resolved issues on page 47 and Known issues on page 78.
2025-06-12	Updated Known issues on page 78.
2025-06-16	Updated Resolved issues on page 47.

Introduction and supported models

This guide provides release information for FortiOS 7.6.0 build 3401.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.6.0 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60F, FG-61F, FG-70F, FG-71F, FG-80F, FG-80F-BP, FG-80F-DSL, FG-80F-POE, FG-81F, FG-81F-POE, FG-100F, FG-101F, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-400F, FG-401F, FG-500E, FG-501E, FG-600E, FG-601E, FG-600F, FG-601F, FG-800D, FG-900D, FG-900G, FG-901G, FG-1000D, FG-1000F, FG-1001F, FG-1100E, FG-1101E, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3000F, FG-3001F, FG-3100D, FG-3200D, FG-3200F, FG-3201F, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3700F, FG-3701F, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-4800F, FG-4801F, FG-5001E, FG-5001E1, FG-6000F, FG-7000E, FG-7000F
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60F, FWF-61F, FWF-80F-2R, FWF-80F-2R-3G4G-DSL, FWF-81F-2R, FWF-81F-2R-3G4G-DSL, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-60F, FGR-60F-3G4G, FGR-70F, FGR-70F-3G4G
FortiFirewall	FFW-1801F, FFW-2600F, FFW-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-OPC, FG-VM64-RAXONDEMAND, FG-VM64-XEN

FortiGate 6000 and 7000 support

FortiOS 7.6.0 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

Hyperscale incompatibilities and limitations

See Hyperscale firewall incompatibilities and limitations in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 7.6.0 features.

FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 7.6.0 features.

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

SSL VPN removed from 2GB RAM models for tunnel and web mode

On FortiGate models with 2GB of RAM or below, the SSL VPN web and tunnel mode feature will no longer be 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-60F/FWF-60F

- FGT-61F/FWF-61F
- FGR-60F and variants (2GB and 4GB versions)

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 have SSL VPN web and tunnel mode support.

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

As part of improvements to enhance performance and optimize memory usage on FortiGate models with 2 GB RAM or less, starting from version 7.4.4, FortiOS no longer supports proxy-related features.

This change impacts the FortiGate 40F and 60F series devices, along with their variants. See Proxy-related features no longer supported on FortiGate 2 GB RAM models for more information.

FortiGate VM memory and upgrade

FortiGate virtual machines (VMs) are not constrained by memory size and will continue to support all available features after upgrading to FortiOS 7.6.0. However, it is recommended to setup VMs with at least 4 GB of RAM for optimal performance.

Hyperscale NP7 hardware limitation

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

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

Changes in CLI

Bug ID	Description
974985	Before 7.6.0, the adv-interval accepted values from 1 to 255 seconds. Starting with FortiOS 7.6.0, adv-interval accepts values in milliseconds, ranging from 250 to 255000. This change allows for quicker VRRP failovers. For more information, see Configure the VRRP hello timer in milliseconds.
995885	Removed the `set security-rating-result-submission` setting under `system.global`.
1002468	Before the update, users were required to manually specify the FortiManager (FMG) serial number under the system central-management. Starting with the new release, FortiGate devices can now automatically retrieve the FortiManager serial number by establishing a connection with FortiManager. Manually specifying the serial number will result in an error if the connection to FortiManager has not yet been established. For more information, see Automatic Serial Number Retrieval with FortiManager.
1009740	Renamed the server-type setting's `iot-query` option to `vpatch-query`. `config system central-management` `  config server-list` `  edit <id>` `  set server-type {update|rating|vpatch-query|iot-collect}` `  set server-address <x.x.x.x>` `  next` `  end` `end`

Changes in GUI behavior

Bug ID	Description
834860	Users are allowed to create a policy using IP or MAC addresses directly from the FortiView pages and Log Viewer. This feature streamlines the policy creation process, making it more efficient and user-friendly.
969758	Added GUI support for creating Internet Service Group. This allows users to create and manage Internet Service Groups more intuitively and efficiently, providing a more user-friendly experience.
976480	Added GUI support for creating local-in policies. This allows users to create local-in policies more intuitively and efficiently, providing a more user-friendly experience.
987210	GUI Enhancement for Firewall Policy Management. Users have the option to apply logical and operations among various policy objects within the GUI, providing a more detailed level of control over the configuration of firewall policies.

Changes in default behavior

Bug ID	Description
1028017	Change the default value of `cert-probe-failure` in `firewall ssl-ssh-profile` to `allow`.
1041367	FortiGate VMs, regardless of the number of vCPUs, now receive the IPS full extended database. The previous restriction of a minimum of eight cores is no longer applicable.

Changes in table size

Bug ID	Description
1012680	On entry-level FortiGate models, with the exception of the 40F model, increase the number of static routes and static routes6 from 100 to 250.
1032057	On entry-level FortiGate models, increase the number of VIP and VIP6 from 512 to 4096.
1038357	On high-end FortiGate models, increase the number of static routes and static routes6 from 10000 to 20000.

New features or enhancements

More detailed information is available in the New Features Guide.

Cloud

See Public and private cloud in the New Features Guide for more information.

Feature ID	Description
997374	High availability (HA) failover is now supported for IPv6 networks on GCP. The *NextHopInstance route* table attribute is used during an HA failover event.
1032254	FortiGate-VM on IBMCloud supports virtual network interfaces. This interface type is selected by default.
1081155	FortiGate-VM supports the AWS r8g instance family.

GUI

See GUI in the New Features Guide for more information.

Feature ID	Description
875308	The Advanced Threat Protection Statistics security widget has been enhanced to provide per-VDOM functionality, more data source options, and enhanced user interactivity. It now uses FortiView stats for data, allows timeframe selection, offers expanded views with antivirus logs, and supports log device settings. This provides users with more detailed and customizable threat protection statistics.
877680	Enhancement to IPsec GUI. The process of creating and editing IPsec tunnels is now more logical. The wizard supports setting the IKE version for both Hub and Spoke and Site-to-Site configurations, along with other transport-related fields for Site-to-Site tunnels. Additionally, security posture tags can be added to FortiClient Remote Access tunnels. These updates aim to make the process more intuitive and efficient.

Feature ID	Description
984655	The Security Rating Display & Integrations have been enhanced for a more streamlined user experience. The *Security Rating* page now showcases *Security Controls* and *Vulnerabilities* tabs, with reorganized and categorized controls for improved navigation. Details on *PSIRT Advisory/Outbreak* detection are now presented in a dedicated card. A new feature, *Security Rating Insights*, provides immediate access to crucial security information. Simply hover over any tested object to reveal a tooltip with more information about any non-conformance to best practices or industry standards. Additionally, *Security Rating* checks are now run on-demand when relevant configuration changes are made, addressing previous performance issues. An overview of *Security Rating Insights* on each page offers a quick filter for items failing certain criteria.
1030693	The FortiOS GUI has been enhanced to display a more modern style, including new icons, updated widget and button shapes, and increased spacing between fields and content. Tables have been adjusted to reduce the width to enclose the table within the page, update the table design, and hide action buttons, such as Edit and Delete, until an entry checkbox is selected. Furthermore, when creating and editing entries in the GUI, the configuration fields now display in a pane instead of a new page.
1035775	Improvements to device upgrade. This enhancement streamlines the upgrade process for all supported devices, including FortiGates, FortiAPs, FortiSwitches, and FortiExtenders. It offers a unified and consistent approach, empowering customers to manage and monitor the upgrade progression effortlessly through an intuitive interface. Moreover, it simplifies the upgrade journey, ensuring a smooth and seamless user experience.
1043027	Enhanced Logging for Threat Feed Updates. Two new fields have been added to the *Threat Feed System* event log. These fields display the total number of entries and the number of invalid entries in the *Threat Feed*. The additional information from these new fields can aid in detecting configuration errors and setting up alerts to spot significant and potentially abnormal changes in the size of the threat feed.

LAN Edge

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

Feature ID	Description
919714	Users can now use FortiSwitch event log IDs as triggers for automation stitches. This allows for automated actions like console alerts, script execution, and email notifications in response to events, such as switch group modifications or location changes. This boosts automation and system management efficiency.
947945	FortiOS WiFi controller allows customers to generate MPSK keys using the FortiGuest self-registration portal. This addition empowers customers to independently create and assign MPSK keys to their devices, streamlining the process and enhancing security.

Feature ID	Description
952124	Users connected to a WiFi Access Point in a FortiExtender can now access the internet, even when the FortiGate is in LAN-extension mode. This ensures seamless internet connectivity for WiFi clients using the FortiGate LAN-extension interface.
952927	The FortiOS WiFi controller has been enhanced to support both TCP and TLS protocols for Radius communication during the 802.1X authentication of WiFi stations. This solves an issue for customers who require stable and secure authentication processes, particularly in complex network infrastructures where UDP might not be sufficient.
965485	Added GUI support for wireless data rates and sticky client removal thresholds. This provides a more intuitive and efficient management of client thresholds and rate controls, enhancing the user experience for accessibility and ease of use.
975075	The FortiAP K series now supports IEEE 802.11be, also known as Wi-Fi 7, for these models: FAP-441K, FAP-443K, FAP-241K, and FAP-243K. This expands device compatibility, boosts network performance, and enhances user experience.
976646	FortiOS extends captive portal support to newer wireless authentication methods, such as OWE and WPA3-SAE varieties. This ensures that users can benefit from the most advanced and secure authentication methods available.
987762	Support OpenRoaming Standards for FortiAP. This boosts Wi-Fi management and user experience by automating guest Wi-Fi onboarding, enabling secure roaming between Wi-Fi and LTE/5G networks, and providing businesses with insightful customer analytics.
990058	FortiOS supports managing the USB port status on compatible FortiAP models. `conf wireless-controller wtp-profile` `  edit <name>` `  set usb-port {enable | disable}` `  next` `end`
997048	FortiOS supports beacon protection, improving Wi-Fi security by protecting beacon frames. This helps devices connect to legitimate networks, reducing attack risks. `config wireless-controller vap` `  edit <name>` `  set beacon-protection {enable | disable}` `  next` `end`
997571	There is added support for 802.11mc protocol in FortiAP, enabling FortiAP radio to operate in 802.11mc responder mode, allowing a mobile device to measure its distance to the AP using the Wi-Fi Round Trip Time (RTT) feature within 802.11mc. `conf wireless-controller wtp-profile` `  edit FAP433G-default` `  config radio-1` `  set 80211mc [enable | disable]`

Feature ID	Description
	`` end next end ``` The FortiAP device must be running firmware version 7.6.0 to support this feature.
999971	Supports receiving the NAS-Filter-Rule attribute after successful WiFi 802.1X authentication. These rules can be forwarded to FortiAP to create dynamic Access Control Lists (dACLs) for the WiFi station, enhancing network access control and security.
1000358	The Bonjour profile supports micro-location, ensuring mDNS traffic originating from one location remains isolated from other locations. This bolsters both network management and security. ``` config wireless-controller bonjour-profile edit <name> set micro-location {enable | disable} end ```
1006398	Enhanced device matching logic based on DPP policy priority. Users can now utilize the CLI to dictate the retention duration of matched devices for dynamic port or NAC policies, allowing greater control over device management.
1006607	FortiOS WiFi controllers MPSK feature now includes both WPA2-Personal and WPA3-SAE security modes. This provides customers with more versatile security options, leveraging the MPSK feature with the latest WPA3-SAE security mode.
1006722	Support for local LAN segregation for FortiAP. When enabled, both wired clients on the LAN port and wireless stations on the SSID remain within the same layer-2 bridge. However, their local traffic is segregated from the FAP's WAN side. This provides users with enhanced control over network traffic, improving security and network management. ``` config wireless-controller vap edit <name> set local-lan-partition {enable | disable} next end ```
1012115	Support fast failover for FortiExtender. This enhancement ensures that FortiGate can swiftly recover data sessions in the event of a failover, reducing downtime and enhancing reliability.
1017160	Support Static RADIUS NAS-ID in Stand-Alone mode. This feature allows the FortiOS WiFi controller to push the `nas-id-type` setting to a managed FortiAP. Consequently, the FortiAP can adhere to this setting and include the NAS-Identifier value in Access-Request packets when authenticating a WiFi station with a remote RADIUS server. This enhancement provides more flexibility and control over the authentication process, thereby improving the overall network security.

Feature ID	Description
1030088	The FortiAP sniffer includes improved packet detection, capturing all frame types across specified channel bandwidths ranging from 320 MHz to 20 MHz. This is vital for in-depth network analysis and troubleshooting, ensuring comprehensive wireless traffic examination for better network management and security.
1039228	Added support for VLANs over a FortiExtender configured as a LAN extension. VLAN support is configured on the FortiGate Access Controller using the GUI or using these CLI commands: `config extension-controller extender-profile` `edit <FortiExtender Profile>` `set extension lan-extension` `config lan-extension` `config downlinks` `edit <id>` `set type port` `set port <port>` `set pvid <vlanid>` `next` `end` `end` `next` `end` Where `port` is the VLAN interface added to the FortiExtender interface and `vlanid` is the desired VLAN ID.
1039878	Support for IKEv2 in FortiAP IPsec VPN. The addition of IKEv2 offers improved performance when FortiAP establishes an IPsec VPN tunnel with FortiGate. This enhancement addresses the need for more secure and efficient VPN connections, preventing potential security risks and ensuring a smoother user experience.

Log & Report

See Logging in the New Features Guide for more information.

Feature ID	Description
974975	FortiOS logs MAC address flapping events. The log provides comprehensive details about the event, such as the specific MAC address involved, the ports where the flapping occurred, and the exact time of the event. This enhancement assists network administrators in quickly identifying and addressing related issues, thereby enhancing network stability and performance.

Feature ID	Description
975413	Support the logging of the MessageId field. By logging the MessageId, FortiAnalyzer (FAZ) can effectively trace unwanted emails back to their origin, which is instrumental in network monitoring and analyzing email traffic. This is beneficial in intricate network setups where several FortiGates are integrated with FortiMail along the network's outbound trajectory, with FAZ for logging.
975414	Introducing log messages for Packet Capture and TCP Dump Operations. A system event log is generated each time a packet capture operation is started or stopped using the GUI, and for the start and stop events of CLI sniffer operations. This enhancement provides users with a clear audit trail of packet capture and tcpdump activities, thereby improving transparency and control.
988670	FOS now offers the ability to set the source interface for syslog/netflow settings. This enhancement allows syslog and NetFlow to utilize the IP of the specified interface as source when sending the messages out. This enables changing the source IP easier, making the process more efficient and less time-consuming, especially when the customer is managing thousands of remote locations. `config log syslogd setting` `  set status enable` `  set source-ip-interface <name>` `end` `config system netflow` `  config collectors` `  edit <id>` `  set source-ip-interface <name>` `  next` `  end` `end`
992606	FortiOS now permits logs from non-management VDOMs to be sent to both global and *vdom-override syslog* servers. Previously, configuring an *override syslog* server under a non-management VDOM would halt the transmission of logs to the *global syslog* server. This ensures uninterrupted log transmission to the global server, enhancing the log management experience. `config syslog override-setting` `  set use-management-vdom {enable | disable}` `end`
1002502	Supports the generation of duplicate IP logs. This enhances the system's ability to detect and log IP conflicts, improving network management and troubleshooting for users. `config system global` `  set ip-conflict-detection {enable | disable}` `end`

Feature ID	Description
1002503	Support Local traffic logging per local-in policy. This allows for logging to be configured per local-in policy, enabling more precise and targeted logging. This resolves the over-generalized logging for users, providing the ability to focus on specific local-in policies that are most relevant to their needs. `config log setting` `  set local-in-policy-log {enable | disable}` `end` `config firewall local-in-policy` `  edit <id>` `  set logtraffic {enable | disable}` `  end` `end`

Network

See Network in the New Features Guide for more information.

Feature ID	Description
652281	Disable all proxy features on FortiGate models with 2 GB of RAM or less by default. Mandatory and basic mandatory category processes start on 2 GB memory platforms. Proxy dependency and multiple workers category processes start based on a configuration change on 2 GB memory platforms.
805896	FortiOS supports sending SNMP traps when a MAC is added, moved, or removed from a FortiSwitch port. This enhances FortiGate's network monitoring capabilities, enabling network administrators to monitor MAC address changes in real-time, strengthening overall network security.
888417	Internal Switch Fabric (ISF) Hash Configuration Support for NP7 Platforms. This provides a new level of flexibility and control to NP7 platform users, allowing them to fine-tune network settings for optimal performance and security. These NP7 FortiGate models support this feature: FG-1800F, FG-2600F, FG-3500F, FG-4200F, and FG-4400F. Use the following command to configure NPU port mapping: `config system npu-post` `  config port-npu-map` `  edit <interface-name>` `  set npu-group <group-name>` `  next` `  next` `end`

Feature ID	Description
	Use the following command to configure the load balancing algorithm used by the ISF to distribute traffic received by an interface to the interfaces of the NP7 processors in your FortiGate: `config system interface` `  edit <interface>` `  set sw-algorithm {l2 | l3 | eh | default}` `  next` `end`
928885	Added GUI support for IPv6 address in explicit-web proxy forwarding server. This enhancement allows users to create and manage IPv6 forward-server more intuitively and efficiently, providing a more user-friendly experience.
961141	The DHCPv6 server/client can accommodate multiple DHCP options. Support for Option 16, also known as the Vendor Class Option, is added for DHCPv6. This allows IP-Pools and Options assignment based on VCI Match for DHCPv6 server and client.
972774	BGP prefixes can be configured utilizing firewall addresses (`ipmask` and `interface-subnet` `types`) and groups. This streamlines the configuration processing, allowing users to leverage their existing firewall addresses and groups when configuring BGP network prefixes.
973481	Socks proxy now supports UTM scanning, authentication, and forward server, making it more versatile. This is beneficial for customers who require these functionalities for their operations.
973573	You can now specify a tagged VLAN for users to be assigned to when the authentication server is unavailable. Previously, you could only specify an untagged VLAN. This feature is available with 802.1x MAC-based authentication. It is compatible with both Extensible Authentication Protocol (EAP) and MAC authentication bypass (MAB).
974985	FortiOS allows the hello timer for the Virtual Router Redundancy Protocol (VRRP) to be configured in milliseconds. This timer dictates the rate at which VRRP advertisements are sent. With this enhanced control, users can ensure quick failover and high availability where necessary.
974986	The OSPF protocol now allows for the customization of the Link State Advertisement (LSA) refresh interval, providing enhanced flexibility and control over the timing parameters within the network. Furthermore, OSPFs capabilities have been expanded to include fast link-down detection on VLAN interfaces, boosting the networks responsiveness and dependability. `config router ospf` `  set lsa-refresh-interval <integer>` `  config ospf-interface` `  edit <name>` `  set interface <string>` `  set linkdown-fast-failover {enable | disable}` `  next` `  end` `end`

Feature ID	Description
975923	FortiOS supports Network Prefix Translation (NPTv6), ensuring end-to-end connectivity and one to one address mapping for address independence. This improves network scalability and facilitates efficient IPv6 network management.
977097	A new CLI option allows users to choose to discard or permit IPv4 SCTP packets with zero checksums on the NP7 platform. `config system npu` `config fp-anomaly` `set sctp-csum-err {allow | drop | trap-to-host}` `end` `end`
978974	Users can upgrade their LTE modem firmware directly from the FortiGuard. This eliminates the need for manual downloading and uploading and provides users flexibility to schedule the upgrade.
982226	FortiOS now incorporates Netflow sampling support. This enhancement enables the FortiGate to maintain a count of the packets or bytes that have been sampled for a particular interface. If the packet count for a session surpasses the threshold set by the `netflow-sample-rate` for either transmitted or received traffic on a NetFlow-enabled interface, a NetFlow report is exported. This process effectively reduces the load on the collector. `config system interface` `edit <name>` `set netflow-sampler {tx | rx | both}` `set netflow-sample-rate <integer>` `set netflow-sampler-id <integer>` `next` `end`
985285	Enhancement to Packet Capture Functionality. This feature adds the capability to store packet capture criteria, allowing for the re-initiation of packet captures multiple times using the same parameters such as interface, filters, and more, thereby streamlining packet capture management. Additionally, this feature incorporates diagnostic commands to list, initiate, terminate, and remove GUI packet captures, enhancing the level of control users have over their packet capture operations.
990092	There is added support for UDP-Lite (IP protocol number 136) traffic in the traffic log and session log output, CLI configuration of IPv4 and IPv6 policy routes, custom session TTL, custom firewall service settings, and GUI configuration of custom firewall services on the *Policy & Objects > Services* page. UDP-Lite traffic is supported by HA session synchronization for connectionless sessions when enabled and strict header checking when enabled to silently drop UDP-Lite packets with invalid header format or wrong checksum errors.
990096	FortiOS allows multiple remote Autonomous Systems (AS) to be assigned to a single BGP neighbor group using AS path lists. This enhancement offers increased flexibility and efficiency in managing BGP configurations, especially in intricate network environments.

Feature ID	Description
990893	Supports the inclusion of a group set in PIM join/prune messages, per RFC 4601. FortiGate can send PIM join/prune messages containing a group set, reducing the number of messages sent to the router. This improvement addresses the issue of router overload in extensive multicast environments, ensuring greater stability and efficiency in network operations.
992604	When a FortiGate is acting as an IPv4 BGP neighbor and using stateful DHCPv6, it learns BGP routes with the IPv6 next-hop belonging to an on-link prefix, and this prefix is advertised using RA. By default, a learned kernel route (currently only RA routes) has a distance of 255 and does not interfere with current route selection. To make the RA route usable by BGP, using a new CLI command `set kernel-route-distance`, set the distance to less than 255 such as 254 or below: `config router setting` `set kernel-route-distance <1-255> (with default of 255)` `end` If there are other user space routes with the same prefix, the best route will be chosen based on distance.
992605	FOS includes a filtering mechanism for netflow sampling. User can apply exclusion filters to their netflow sampling based on various criteria such as source IP, source port, destination IP, destination port, and IP protocol. The addition of this feature enhances the relevance of the data collected, streamlines data management processes, and minimizes superfluous network traffic. `config system netflow` `  config exclusion-filters` `  edit <id>` `  set source-ip  <IP_address>` `  set destination-ip <IP_address>` `  set source-port <port>` `  set destination-port <port>` `  set protocol <protocol_ID>` `  next` `end`
1000356	FOS now supports being configured as a recursive DNS resolver. As a resolver, the FortiGate can directly interact with root name servers, Top-Level Domain (TLD) name servers, and finally authoritative name servers to resolve DNS queries. Furthermore, FortiOS also adds support for prioritizing root name servers. You may choose root servers from the list of default servers, or you can configure your own custom root name server.
1002403	FTP Session-Helper Support for 464XLAT Environment. This enhancement enables FortiOS to support both passive and active modes in a 464XLAT environment.

Feature ID	Description
1006904	Allow customers to use interface names, not just IP addresses, for defining source IPs in RADIUS, LDAP, and DNS configurations. This caters to dynamic IP changes, such as those governed by SD-WAN rules. FortiOS will use the interfaces current IP as the source IP, enhancing network flexibility and resolving potential connectivity issues.
1019490	Automatic LTE Connection Establishment. This enhancement automates the process of LTE connection establishment. When a SIM card is inserted, FortiOS (FOS) can obtain the Mobile Country Code (MCC) and Mobile Network Code (MNC) from the service providers radio tower. FOS then uses these codes to look up the appropriate APN for the SIM card in a predefined table and automatically creates a wireless profile. This eliminates the need for manual configuration by the user, simplifying the process of establishing an LTE connection.
1029730	Introducing IPv6/64 prefix session quota and an IPv4 prefix session quota for both software and hardware sessions with Hyperscale. This new feature allows for more precise control over session limits.  This feature only works for no-NAT polices. To configure global session quotas for IPv6 sessions: `config system npu` `set ipv6-prefix-session-quota {disable | enable}` `set ipv6-prefix-session-quota-high <high-threshold>` `set ipv6-prefix-session-quota-low <low-threshold>` `end` To configure session quotas for IPv4 sessions accepted by firewall policies with NAT disabled: `config system npu` `set ipv4-session-quota {disable | enable}` `set ipv4-session-quota-high <high-threshold>` `set ipv4-session-quota-low <low-threshold>` `end`

Policy & Objects

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

Feature ID	Description
967654	FortiOS allows internet service as source addresses in the local-in policy. This allows more flexibility and control in managing local traffic, enhancing network security and efficiency.

Feature ID	Description
998367	MAP-E has been enhanced to support multiple VNE interfaces within the same VDOM, allowing for a more versatile network setup.
998789, 998790	Users can configure custom port ranges for both Port Block Allocation (PBA) and Fixed Port Range (FPR) types of IPPools. This provides users with the flexibility to specify port ranges from 1024 to 65535, enhancing user control and adaptability in network configurations. `config firewall ippool` `edit <name>` `set type {fixed-port-range | port-block-allocation}` `set startport <integer>` `set endport <integer>` `next` `end`
998792	Support for NAT64 has been added within the Fixed-Port-Range IP pool. Internal IPv6 ranges can be configurated in the NAT64 Fixed Port Range IP pool. This addition is significant because it allows for prefix-based restrictions, providing greater control and security over network traffic management.
1000366	Support HTTP Transaction Logging. This enables HTTP transaction details in a new type of traffic log when HTTP traffic is routed through a proxy, ensuring comprehensive logging of HTTP interactions for improved monitoring and analysis.
1002499	Introducing the 7-Day Policy Hit Counter for NGFW Policies. This feature offers a rolling tally of the number of times a policy has been triggered over the previous seven days. Users are empowered with a more comprehensive and dynamic insight into their policy usage patterns over time, enhancing user experience and promoting efficient resource management.
1017162	Support for the Full Cone Network Address Translation (NAT) (similar to Endpoint Independent Filtering (EIF)) has been added for Fixed Port Range IP Pool. This allows all external hosts to send packets to internal hosts through a mapped external IP address and port, enhancing connectivity and communication efficiency. `config firewall ippool` `edit <name>` `set type fixed-port-range` `set permit-any-host {enable | disable}` `next` `end`

SD-WAN

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

Feature ID	Description
939700	A new gutter section added to the *Fabric Overlay Orchestrator* page if the FortiSASE SPA license is active. From this section the user can open a slide that will generate a FortiSASE SPA easy configuration key based on the current FOO configuration which can be used in SPA setup of FortiSASE.
951494	In this enhancement, support for a new FortiGuard SLA Database (SLA Database), which includes popular SaaS and Internet destinations and recommended settings that can be selected as probe servers for SD-WAN Performance SLA configuration in the GUI using the *Performance SLA* and *SLA Target* fields in the *New Performance SLA* page and in the CLI using these commands: `config system sdwan` `  config health-check` `  edit <health-check name>` `  set fortiguard enable` `  set fortiguard-name <target-name-from-SLA-Database>` `  next` `  end` `end` The FortiGate requires a valid SD-WAN Network Monitor (SWNM) entitlement to be applied for the FortiGuard SLA Database to be downloaded or updated.
987765	Enhancements have been added to improve overall ADVPN 2.0 operation for SD-WAN, including: • The local spoke directly sends a shortcut-query to a remote spoke to trigger a shortcut after ADVPN 2.0 path management makes a path decision. • ADVPN 2.0 path management can trigger multiple shortcuts for load-balancing SD-WAN rules. Traffic can be load-balanced over these multiple shortcuts to use as much of the available WAN bandwidth as possible without wasting idle links if they are healthy. The algorithm to calculate multiple shortcuts for the load-balancing service considers transport group and in-SLA status for both local and remote parent overlays. • Spokes can automatically deactivate all shortcuts connecting to the same spoke when user traffic is not observed for a specified time interval. This is enabled by configuring a shared idle timeout setting in the IPsec VPN Phase 1 interface settings for the associated overlays.
992608	Allows IPv6 Multicast traffic to be steered by SD-WAN rules. In the event of an SD-WAN member falling out of SLA, the multicast traffic is designed to failover to another member. Once the original member recovers and meets the SLA again, the multicast traffic will switch back, ensuring optimal network performance and reliability. `config router multicast6` `  config pim-sm-global` `  set pim-use-sdwan {enable | disable}` `  end` `end`

Feature ID	Description
1001819	Embed SD-WAN SLA status (within SLA or out of SLA) for IPsec overlays and matching SLA priorities in ICMP probes for the best path selection that works with BGP on loopback designs. It consists of these parts: 1. Embed Spokes SLA status (within SLA or out of SLA) for IPsec overlays in the ICMP probes that Spokes send to Hub when Spokes `config health-check` entries are configured with embed-measured-health enabled, the new CLI command `sla-id-redistribute <id>` configured with the `<id>` of the SLA setting, and the SLA setting is matched. 2. Embed Spokes within SLA and out of SLA priorities when new CLI commands `set priority-in-sla` and `set priority-out-sla` are configured in Spokes config members for IPsec overlays. 3. On the Hub, if the `set detect-mode remote` is configured and the Hubs health check sla-id-redistribute matches an SLA setting with `set link-cost-factor remote`, then the received SLA status is used to mark the SLA status of the IPSec tunnel, and the matching SLA priority is applied to the routes associated with the IPSec overlay where the ICMP packet comes in. This feature also supports the Spoke-initiated speed test case, where the test link is set out of SLA and the out-of-SLA priority is sent to the Hub, which causes traffic to use other routes during the speed test. To ease the migration process, in case many Spokes are deployed, the Hub can work in a hybrid mode where if `set sla-id-redistribute` is not configured on the Spoke the Hub would use its own SLA settings to determine the route priority.
1016452	To ensure FortiGate spoke traffic remains uninterrupted when configuration is orchestrated from the SD-WAN Overlay-as-a-Service (OaaS), there is added support for an OaaS agent on the FortiGate. The OaaS agent communicates with the OaaS controller in FortiCloud, validates and compares FortiOS configuration, and applies FortiOS configuration to the FortiGate as a transaction when it has been orchestrated from the OaaS portal. If any configuration change fails to be applied, the OaaS agent rolls back all configuration changes that were orchestrated. Secure communication between the OaaS agent and the OaaS controller is achieved using the FGFM management tunnel. The new CLI command `get oaas status` displays the detailed OaaS status.

Security Fabric

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

Feature ID	Description
892477	FortiOS can now email CLI script action output results in an attachment when the output exceeds 64K characters.

Feature ID	Description
972642	The external resource entry limit is now global. Additionally, file size restrictions now adjust according to the device model. This allows for a more flexible and optimized use of resources, tailored to the specific capabilities and requirements of different device models.
1000836	Before this enhancement, a FortiGate can only connect to the FortiClient Cloud instance that is registered under the root FortiCloud account. FortiGate now supports connecting to a FortiClient Cloud instance registered under a sub-OU in FortiCloud. Furthermore, a FortiGate can override FortiClient Cloud access key setting on a per-vdom basis. With these enhancements, a FortiGate can support FortiClient Cloud in multi-tenancy scenarios.
1002148	FortiOS allows the application of threat feed connectors as source addresses in central SNAT. This enhancement allows for more dynamic and responsive network security configuration.
1012620	A FortiGate full fabric upgrade now performs upgrades by groups in the following order: **1.** PoE PD (Powered Devices) **2.** PSE (Power Source Equipment) and non-POE devices **3.** FortiGate itself  Group 2 (PSE and non-POE devices) must wait until Group 1 (PoE PD) finishes and upgraded to new firmware before starting its upgrade. Once all upgrades are complete and the FortiGate is back up, it will verify all devices are in the new firmware version.

Security Profiles

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

Feature ID	Description
937180	FortiOS antivirus now supports Microsoft OneNote files through its CDR feature. FortiGate sanitizes these files by removing active content, such as hyperlinks and embedded media, while preserving the text. This feature provides an additional tool for network administrators to protect users from malicious documents.
939342	GUI support for Exact Data Match (EDM) for Data Loss Prevention. This optimizes data management and minimizes false positives.
962889	FortiOS Carrier has enhanced its management capabilities for GTPv0 traffic. This provides the flexibility to either allow or restrict GTPv0 traffic, ensuring a more secure and adaptable strategy for managing their GTPv0 traffic. This option is set to deny by default, blocking all GTTPv0 traffic when creating a new GTP profile. You can allow or block all GTPv0 traffic in a GTP profile using this command:

Feature ID	Description
	config firewall gtp edit <name> set gtpv0 {allow | deny} next end
968303	Add support to control TLS connections that utilize Encrypted Client Hello (ECH), with options to block, allow, or force the client to switch to a non-ECH TLS connection by modifying DoH responses. This increases control and flexibility for managing TLS connections.
974035	Support DNS Filtering for Proxy Policy. This enhancement added the ability to apply DNS Filtering to proxy policies. This addition enhances security by providing an extra layer of protection for clients operating behind a proxy. This is particularly beneficial in scenarios where client applications are configured to use DoH and DoT protocols and require the added security of DNS Filtering.
977002	FortiOS offers stream-based scanning for HTML and Javascript files in flow mode. This allows the AV engine to determine the necessary amount of file payload to buffer and to scan the partial buffer in certain instances, eliminating the need to cache the entire file and potentially leading to an improvement in memory usage.
981912	Improvements to the webfilter UTM logs allow the incorporation of endpoint device data, including hostname and MAC address, enhancing network activity insights. config log setting set extended-utm-log {enable | disable} end
989087	Enhancement to the FortiGuard-managed DLP dictionaries. Users now have the flexibility to select a FortiGuard dictionary with varying confidence levels based on their specific needs. High level offers maximum precision, medium-level balances match quantity and precision, and low level captures most matches with the potential for false positives. This feature aims to balance data traffic precision and volume, enhancing the user experience.
1007937	Support the Zstandard (zstd) compression algorithm for web content. This enhancement enables FortiOS to decode, scan, and forward zstd-encoded web content in a proxy-based policy. The content can then be passed or blocked based on the UTM profile settings. This ensures a seamless and secure browsing experience.
1012626	In this enhancement, a hash of all executable binary files and shared libraries are taken during image build time. The file containing these hashes, called the executable hash, is also hashed and as a result signed. The signature for this hash is verified during bootup to ensure integrity of the file. After validation, the hashes of all executable and share libraries can be loaded into memory for real-time protection.
1014842	Introducing Domain Fronting Protection for both explicit proxy and proxy-based firewall policies. This feature empowers FortiGate to confirm if the domain of the request matches the actual host domain in the HTTP header. Security is enhanced by preventing unauthorized access that could result from domain mismatches.

Feature ID	Description
	config firewall profile-protocol-options edit protocol config http set domain-fronting {allow | block | monitor} next end end
1025233	DNS over TLS (DoT) and DNS over HTTPS (DoH) are now supported in DNS inspection for both proxy and flow mode.
1036025	DNS translation now supports Service (SRV) records over the DNS Filter profile, offering broader coverage and finer control for network administrators.

System

See System in the New Features Guide for more information.

Feature ID	Description
754783	Added GUI support for GTPv2 options for FortiOS Carrier. There are now separate filters for GTPv0/v1 and GTPv2, along with individualized settings for managing their message rate limits. Furthermore, support for an IE allow list configuration has been added. This feature grants users more precise control over GTP profiles, enhancing the overall usability.
955835	Previously, when `auto-upgrade` was disabled, users would receive a warning advising them to execute `exec federated-upgrade cancel` in order to remove any scheduled upgrades. However, with the new update, the system is now capable of autonomously canceling any pending upgrades, eliminating the need for manual user action.
957562	New hyperscale feature to control the rate at which NP7 processors generate ICMPv4 and ICMPv6 error packets to prevent excessive CPU usage. This feature is enabled by default, and you can use the following options to change the configuration if required for your network conditions: config system npu config icmp-error-rate-ctrl set icmpv4-error-rate-limit {disable | enable} set icmpv4-error-rate <packets-per-second> set icmpv4-error-bucket-size <token-bucket-size> set icmpv6-error-rate-limit {disable | enable} set icmpv6-error-rate <packets-per-second> set icmpv6-error-bucket-size <token-bucket-size> next end

Feature ID	Description
962887	FGSP Support for Packet Forwarding Control Protocol (PFCP) in the FOS Carrier. FortiCarriers robustness and reliability is bolstered by ensuring consistent PFCP session information across all FGSP peers. It also facilitates the smooth synchronization of PFCP session information to newly integrated peers. This feature improves the systems scalability by enabling effortless integration of new peers into the FGSP cluster, and augments network flexibility and efficiency through the support for asymmetric routing.
971546	GUI support added to control the use of CLI commands in administrator profiles.
974976	Support for synchronizing RSSO (Radius Single Sign-On) authenticated user logon information between FGSP peers. This ensures a consistent user experience across all FGSP peers.
975021	FortiGate now supports 3 methods of VMAC definition to increase the number of HA virtual MAC addresses beyond the number HA group-ids. These methods are: **1.** Manual VMAC per interface **2.** Auto VMAC assignment **3.** Group-id based assignment (existing) Manual VMAC can be configured on a physical, EMAC or FortiExtender interface, which will override other VMAC assignment options. Auto VMAC assignment utilizes the hardware MAC address of the primary unit with the locally administered bit (U/L bit) changed to 1. For example, 00:xx:xx:xx:xx:xx becomes 02:xx:xx:xx:xx:xx. This option is only supported on physical interfaces. `config system ha` `  set auto-virtual-mac-interface <interface list>` `end` `config system interface` `  set virtual-mac <mac address>` `end`
983862	Dynamic Source Port for GTP-U Packets is now supported on NP7 Platforms. This feature establishes two sessions for bidirectional traffic, regardless of the source ports. By reducing the number of sessions, it significantly decreases memory usage. This is particularly beneficial for customers handling high volumes of GTP-U traffic, offering a memory-efficient and streamlined solution. `config system global` `  set gtpu-dynamic-source-port {enable | disable}` `end`
985440	Session Failover is now supported for asymmetric traffic. FortiGate can now continue sessions on the active FGSP peer if the original FGSP peer, which initially received the sessions first packet, becomes unavailable. Once the original FGSP peer is back online, the session will switch back to it. This enhancement ensures continuity and reliability of the network sessions, even in the event of a device failure.

Feature ID	Description
988090	Streamlines timezone updates with a downloadable database. Previously, the IANA timezone database was embedded within the image, necessitating a FOS image upgrade for any updates. Now, it is conveniently downloadable from the FortiGuard server, enabling FortiGate to automatically refresh its timezone database seamlessly. This advancement eliminates customers' need to wait for the next image release to access new or updated timezones.
988573	An FGCP HA split-brain scenario may occur when heartbeat interfaces are down or there is extreme latency or congestion, leading to the secondary unit promoting itself to primary. To prevent this situation, this enhancement introduces the backup heartbeat interface which is a dedicated interface used only when a secondary unit detects no heartbeats from the primary through the regular heartbeat interfaces. `config system ha` `  set backup-hbdev <interface list>` `end`
992630	FortiOS can restrict local admin logins through the console when the remote authentication server is reachable. This provides more extensive control over local admin logins, improving the system's security. `config system global` `  set admin-restrict-local {all | non-console-only | disable}` `end`
1000200	This enhancement enables SNMP clients to query the BIOS security level of a FortiGate using the new OID 1.3.6.1.4.1.12356.101.4.1.38.
1000361	Security enhancement for closed-network VM licenses. The CMS signature is now verified immediately after the license is loaded. This ensures the license is from Forticare and confirms the authenticity of its contents and contracts, enhancing license integrity and customer trust.
1000364	Configuration files are now encrypted in the eCryptfs file system when a system reboots or shuts down, and decrypted when the system boots up and is required to load the configs to CMDB. The eCryptfs encryption key is generated and stored on the TPM the same way as the private-data-encryption key, if TPM is supported on the device model. Otherwise, it is generated by CSPRNG and stored on disk.
1000368	FortiOS allows the `delay-tcp-npu-session` enable option to be applied globally, eliminating the need to set the command for each firewall policy, conserving resources. `config system global` `  set delay-tcp-npu-session {enable | disable}` `end`
1002103	FortiOS supports the Ethernet Statistics Group for Remote Network Monitoring (RMON), which provides detailed statistics about the traffic that passes through the Ethernet interface, such as drop events and collisions.
1007419	The `print tablesize` command has been updated to show object usage, aiding administrators in monitoring limits and improving system management.

Feature ID	Description
1007570	Support for interface selection method for SNMP traps. This enhancement enables SNMP traps to leverage SD-WAN rules. This feature is especially advantageous in larger SD-WAN environments, where routing SNMP traps via the most efficient SD-WAN path has previously posed a challenge.
1013511	This enhancement requires the kernel to verify the signed hashes of important file-system and object files during bootup. This prevents unauthorized changes to file-systems to be mounted, and other unauthorized objects to be loaded into user space on boot-up. If the signed hash verification fails, the system will halt.
1025442	Allow non-management vdoms to perform queries using SNMPv3. This enhancement expands the query capabilities of non-management vdoms, improving the systems versatility. `config system snmp sysinfo` `  set non-mgmt-vdom-query {enable | disable}` `end`

User & Authentication

See Authentication in the New Features Guide for more information.

Feature ID	Description
848357	FortiOS allows users to specify the sequence that authentication methods are executed in when both 802.1x and MAC Authentication Bypass (MAB) are enabled. Users can prioritize one method over the other based on their specific network security requirements.
951626	Support for client certificate validation and EMS tag matching has been added to the explicit proxy policy, improving user experience and security.
966534	Support for SCIM server on FortiGate. This enhancement allows FortiGate to communicate with an IdP using the SCIM 2.0 protocol, enabling automatic provisioning of users and groups on FortiGate.
972434	Support is added for a customizable password reuse threshold applicable to both system and user password policies. This empowers users to determine the frequency of password reuse, bolstering password management and enhancing security.
972636	Expand the range of protocols that can trigger RADIUS authentication, now including DNS and ICMP queries. This improvement provides our customers with a more flexible solution.
974984	FortiOS now preserves authentication sessions even after a Firewall reboot. This feature enhances the user experience by eliminating the need for re-authentication after a Firewall reboot. `config system global` `  set auth-session-auto-backup {enable | disable}`

Feature ID	Description
	set auth-session-auto-backup-interval {1min | 5min | 15min | 30min | 1hr} end

VPN

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

Feature ID	Description
845078	Incorporates a global installation of the OpenSSL FIPS provider at startup. This enhancement ensures that any OpenSSL application is automatically compliant with FIPS regulations. Additionally, the system now defaults to the more secure TLS1.2 and TLS1.3 protocols. Furthermore, only Diffie-Hellman parameters of 2048 bits or higher are permitted. This ensures a robust security posture and aligns with industry standards.
969747	Support Post-Quantum Cryptography (PQC) for IPsec key exchange, enhancing security with algorithms that protect against quantum computer attacks. This update ensures future-proof encryption and addresses vulnerabilities in traditional methods, aligning with upcoming security standards.
976976	In IPsec dial-up VPN config, an option is added to enforce ZTNA security posture tag matching before establishing an IKEv2 VPN tunnel. The following settings have been added: config vpn ipsec phase1-interface edit <name> set ike-version 2 set remote-gw-match {any | ipmask | iprange | geography | ztna} set remote-gw-ztna-tags <IPv4 ZTNA posture tags> next end When `set remote-gw-match ztna` is enabled, `remote-gw-ztna-tags` can be configured.
976999	FortiOS now offers the capability for users to enable automatic selection mechanism for the IPSec tunneling protocol. IKE will initially employ UDP encapsulation. If UDP establishment does not succeed within the set threshold, the transport layer protocol seamlessly switches to TCP to ensure optimal performance and reliability. config vpn ipsec phase1-interface edit <name> set ike-version 2 set transport {auto | udp | tcp} set auto-transport-threshold <integer> next end

Feature ID	Description
996136	FortiOS now supports session resumptions for IPSec tunnel version 2. This enhances the user experience by maintaining the tunnel in an idle state, allowing uninterrupted usage even after a client resumes from sleep or when connectivity is restored after a disruption. It also removes the necessity for re-authentication when reconnecting, making the process more efficient.
1006448	Enhanced SSL VPN security by restricting and validating HTTP messages that are used only by web mode and tunnel mode.

ZTNA

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

Feature ID	Description
945605	With this enhancement, FortiGate can share ZTNA information such as ZTNA VIP address and application specifics like application address and port via the EMS connector. On FortiClient EMS, the configured ZTNA TCP and SaaS applications are pulled into the ZTNA application catalog. These apps can be applied to ZTNA Destinations without any additional configurations.
975010	Support for UDP traffic destinations is added for ZTNA. On a supported FortiClient endpoint (7.4.1 and above), when UDP traffic to a destination is detected, FortiClient will form a UDP connection over QUIC to the FortiGate ZTNA gateway. After authentication, security posture check and authorization, a connection with the destination will be formed and the end to end UDP traffic will pass through. `config firewall vip` `edit < ZTNA VIP >` `set type access-proxy` `set h3-support {enable | disable}` `next` `end`
1011594	Added GUI support for specifying SaaS applications within the service/server mapping inside a ZTNA server object. This enhancement allows users to create and manage ZTNA server with service type SaaS more intuitively and efficiently, providing a more user-friendly experience.

Upgrade information

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

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 37 and Upgrading all devices in the FortiOS Administration Guide.

To view supported upgrade path information:

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

Fortinet Security Fabric upgrade

FortiOS 7.6.0 is verified to work with these Fortinet products. This includes:

FortiAnalyzer	• 7.6.1
FortiManager	• 7.6.1
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 or SSL VPN, FortiClient version 6.0 and later are supported.

When upgrading your Security Fabric, devices that manage other devices should be upgraded first.

When using FortiClient with FortiAnalyzer, you should upgrade both to their latest versions. The versions between the two products should match. For example, if using FortiAnalyzer 7.6.0, use FortiClient 7.6.0.

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 7.6.0. When Security Fabric is enabled in FortiOS 7.6.0, all FortiGate devices must be running FortiOS 7.6.0.

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

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

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

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

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

To perform a graceful upgrade of your FortiGate 6000 or 7000 to FortiOS 7.6.0:

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

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

When upgrading from FortiOS 7.4.1 to a later version, use the following command to enable uninterruptible upgrade:

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

2. Download the FortiOS 7.6.0 FG-6000F, FG-7000E, or FG-7000F firmware from https://support.fortinet.com.
3. Perform a normal upgrade of your HA cluster using the downloaded firmware image file.
4. When the upgrade is complete, verify that you have installed the correct firmware version.
   For example, check the FortiGate dashboard or use the `get system status` command.
5. Check the *Cluster Status* dashboard widget or use the `diagnose sys confsync status` command to confirm that all components are synchronized and operating normally.

Default setting of cp-accel-mode is changed to none on 2GB memory models

This change disables CP acceleration to lower system memory usage thus can prevent some unexpected behavior due to lack of memory.

Previous FortiOS CLI behavior:

```
config ips global
    set cp-accel-mode advanced
end
```

New FortiOS CLI behavior after upgrade:

```
config ips global
    set cp-accel-mode none
end
```

This change will cause performance impact as CPU will do the pre-match (pattern match) inside IPS (CPU) instead of hardware engine (cp module in SOC4). Some customers could expect an increase in CPU utilization as a result.

FortiGate and FortiWiFi 4xF/6xF families are affected by this change.

Product integration and support

The following table lists FortiOS 7.6.0 product integration and support information:

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 0316 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	• 7.00030
IPS Engine	• 7.01014

See also:

- Virtualization environments on page 43
- Language support on page 43
- SSL VPN support on page 44
- FortiExtender modem firmware compatibility on page 44

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, and 8.0.

Language support

The following table lists language support information.

Language support

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

SSL VPN support

SSL VPN web mode

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

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 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.

FortiExtender modem firmware compatibility

The following table lists the modem firmware file name and version for each FortiExtender model and its compatible geographical region.

FortiExtender model	Modem firmware image name	Modem firmware file on Support site	Geographical region
FEX-101F-AM	FEM_EM06A-22-1-1	FEM_EM06A-22.1.1-build0001.out	America

FortiExtender model	Modem firmware image name	Modem firmware file on Support site	Geographical region
FEX-101F-EA	FEM_EM06E-22-01-01	FEM_EM06E-22.1.1-build0001.out	EU
	FEM_EM06E-22.2.2	FEM_EM06E-22.2.2-build0002.out	EU
FEX-201E	FEM_06-19-0-0-AMEU	FEM_06-19.0.0-build0000-AMEU.out	America and EU
	FEM_06-19-1-0-AMEU	FEM_06-19.1.0-build0001-AMEU.out	America and EU
	FEM_06-22-1-1-AMEU	FEM_06-22.1.1-build0001-AMEU.out	America and EU
	FEM_06-22-1-2-AMEU	FEM_06-22.1.2-build0001-AMEU.out	America and EU
FEX-201F-AM	FEM_07A-22-1-0-AMERICA	FEM_07A-22.1.0-build0001-AMERICA.out	America
	FEM_07A-22-2-0-AMERICA	FEM_07A-22.2.0-build0002-AMERICA.out	America
FEX-201F-EA	FEM_07E-22-0-0-WRLD	FEM_07E-22.0.0-build0001-WRLD.out	World
	FEM_07E-22-1-1-WRLD	FEM_07E-22.1.1-build0001-WRLD.out	World
FEX-202F-AM	FEM_07A-22-1-0-AMERICA	FEM_07A-22.1.0-build0001-AMERICA.out	America
	FEM_07A-22-2-0-AMERICA	FEM_07A-22.2.0-build0002-AMERICA.out	America
FEX-202F-EA	FEM_07E-22-1-1-WRLD	FEM_07E-22.1.1-build0001-WRLD.out	World
FEX-211E	FEM_12-19-1-0-WRLD	FEM_12-19.1.0-build0001-WRLD.out	World
	FEM_12-19-2-0-WRLD	FEM_12-19.2.0-build0002-WRLD.out	World
	FEM_12-22-1-0-AMEU	FEM_12-22.0.0-build0001-AMEU.out	America and EU
	FEM_12-22-1-1-WRLD	FEM_12-22.1.1-build0001-WRLD.out	World
FEV-211F_AM	FEM_12_EM7511-22-1-2-AMERICA	FEM_12_EM7511-22.1.2-build0001-AMERICA.out	America

FortiExtender model	Modem firmware image name	Modem firmware file on Support site	Geographical region
FEV-211F	FEM_12-22-1-0-AMEU	FEM_12-22.1.0-build0001-AMEU.out	World
FEX-211F-AM	FEM_12_EM7511-22-1-2-AMERICA	FEM_12_EM7511-22.1.2-build0001-AMERICA.out	America
FEX-212F	FEM_12-19-2-0-WRLD	FEM_12-19.2.0-build0002-WRLD.out	World
	FEM_12-22-1-1-WRLD	FEM_12-22.1.1-build0001-WRLD.out	World
FEX-311F	FEM_EM160-22-02-03	FEM_EM160-22.2.3-build0001.out	World
	FEM_EM160-22-1-2	FEM_EM160-22.1.2-build0001.out	World
FEX-511F	FEM_RM502Q-21-2-2	FEM_RM502Q-21.2.2-build0003.out	World
	FEM_RM502Q-22-03-03	FEM_RM502Q-22.3.3-build0004.out	World
	FEM_RM502Q-22-04-04-AU	FEM_RM502Q-22.4.4-build0005_AU.out	Australia
	FEM_RM502Q-22-1-1	FEM_RM502Q-22.1.1-build0001.out	World
	FEM_RM502Q-22-2-2	FEM_RM502Q-22.2.2-build0002.out	World

The modem firmware can also be uploaded manually by downloading the file from the Fortinet Customer Service & Support site. The firmware file names are listed in the third column of the table.

To download the modem firmware:

1. Go to https://support.fortinet.com/Download/FirmwareImages.aspx.
2. From the *Select Product* dropdown, select *FortiExtender*.
3. Select the *Download* tab.
4. Click *MODEM-Firmware*.
5. Select the FortiExtender model and image name, then download the firmware file.

Resolved issues

The following issues have been fixed in version 7.6.0. To inquire about a particular bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
948197	Large file downloads may intermittently stall when flow-based UTM and SSL deep inspection are enabled.
977634	FortiOS *High Security Alert* block page reference URL is incorrect.
981757	An error is displayed when downloading a file from a browser with FortiSandbox `scan-mode default` enabled using an antivirus profile.
993785	When logged in as an administrator with Security Fabric access permissions set to none, trying to create a new antivirus profile on the *Security Profiles* > *Antivirus* page shows an error.
1028114	FortiGate cannot connect to FortiSandboxCloud when `inline content block scan mode` is set to default in an antivirus profile.
1031084	When FortiGate is in HA AA mode, the secondary unit does not connect to all FSA types for inline scanning.
1042358	A memory usage issue in the WAD process prevents the AV Engine from loading properly.

Application Control

Bug ID	Description
982147	Remote TACACS+ administrators cannot edit application control profiles using the GUI due to transaction failure. **Workaround**: TACACS+ administrators can make changes to the application control using the CLI or local administrators can make changes using the GUI.
1015616	Packets may be dropped by the anti-reply function due to it being partially offloaded.

Data Loss Prevention

Bug ID	Description
980995	DLP Reference check slide window is empty on Global level.
1007202	An upgrade issue may prevent the upload or download of large files using HTTP2.
1012922	When a DLP policy is set to block the upload or download of test PDF documents, the policy does not function as expected.
1036260	The DLP blocks all traffic with deep packet inspection and displays an error page.

DNS Filter

Bug ID	Description
804790	DNS server latency increases by 15 seconds when a request times out. This increase may give a perception that this server is unreachable or has a latency value that doesn't reflect real-world conditions.
1010464	When the DNS filter is enabled with `external-ip-blocklist`, the IPS Engine remains in D status for an extended period of time and the DNS session ends.
1025233	Support Encrypted ClientHello (ECH) in flow mode.
1026058	When IP is not resolved or does not exist, the DNS alters the response for the domain and results in a performance issue on the client device.
1048289	DNS requests with uppercase characters in the domain name are not blocked when the policy is in flow mode with an external *Domain* threat feed.

Endpoint Control

Bug ID	Description
987456	FortiOS experiences a CPU usage issue in the daemon when connecting to an EMS that has a large amount of EMS tags.
1007809	On FortiGate, anonpages and active(anon) pages frequently use a high amount of memory, causing FortiGate to enter into conserve mode.

Explicit Proxy

Bug ID	Description
775882	The WAD does not function as expected due to a memory allocation issue.
830418	Website content does not load properly when using an explicit proxy.
890776	The GUI-explicit-proxy setting on the *System* > *Feature Visibility* page is not retained after a FortiGate reboot or upgrade.
893935	HTTP requests are forwarded to the server through a web proxy even when `forward-server group-down` is set to block.
894557	In some cases, the explicit proxy policy list can take a long time to load due to a delay in retrieving the proxy statistics. This issue does not impact explicit proxy functionality.
983897	Traffic that should not be matching a policy is incorrectly matching an allow policy or a deny policy.
990643	FortiGate blocks pages when browsing websites though a transparent proxy-redirect policy on SD-WAN.
991106	Traffic logs and security events cannot be viewed in the SASE portal caused by the WAD not functioning as expected.
1001700	If explicit webproxy uses SAML authentication and the PAC file is enabled at the same time, the browser will report a too many redirects error when trying to visit any websites.
1006362	Debug daemon may be blocked while handling client connection and increases the GUI load time.
1011209	The proxy policy does not work as expected when the session-ttl value is greater than the global session-ttl value.
1014477	Files do not get uploaded on webmail applications with antivirus, app control, or IPS enabled on an explicit proxy policy.
1021643	The WAD may not forward HTTP requests through an explicit web proxy.
1021710	The `server-down-option-block` command does not work as expected when creating a connection to a forward proxy server.
1025974	When FortiGate is configured as a downstream proxy with an FQDN type, browsing traffic may encounter a gateway timeout error.
1026362	Web pages do not load when `persistent-cookie` is disabled for `session-cookie-based authentication` with *captive-portal*.
1042125	FortiGate generates a replacement error message when the `message-upon-server-error` option is disabled.
1048194	FortiGate blocks traffic if a `onetime` schedule is configured in an explicit proxy policy and the schedule has not expired.

File Filter

Bug ID	Description
1004198	.exe files in ZIP archives are not blocked by file-filter profiles during CIFS file transfers.

Firewall

Bug ID	Description
807191	On FortiGate, the `diagnose netlink interface list` command shows no traffic running through the policy, even with NP offload enabled or disabled.
815333	Local-in policy does not deny IKE UDP 500/4500.
819274	On the *Query > Routing Menu* page in FortiManager, the routing table does not include the static or BGP types in `get router info routing-table all`.
837866	On the NP7 platform, traffic is blocked when `egress-shaping-profile` and `outbandwidth` are enabled on a VLAN parent interface.
892774	On FortiGate 7000 models, the hit counter on the FortiManager GUI does not display the correct values.
951422	Corner case: failure to download file from web server with Proxy mode inspection and AV/IPS enabled.
966466	On an FG-3001F NP7 device, packet loss occurs even on local-in traffic.
985419	On the *Policy & Objects > Firewall Policy* page, the *Log violation traffic* checkbox displays as being unchecked when the policy is configured and reopened for editing. This purely a GUI display issue and does impact system operation.
991961	On the *Policy & Objects > Addresses* page, address objects are not sorted in alphabetical order for address group or firewall policies.
992610	The source interface displays the name of the VDOM and local out traffic displays as forward traffic.
996876	Adding IPv6 address group memberships to a policy using FortiGate REST API does not work as expected.
998699	On the *Policy & Objects > Firewall Policy* page, the *Firewall/Network* options are missing in the GUI when enabling a security profile group in a policy.
1002269	When a schedule is added to a firewall policy, the schedule is not activated at the time configured in the policy.

Bug ID	Description
1004267	On the *Policy & Objects* > *Firewall Policy* page, when searching for an address object with a comment keyword, no results are displayed.
1008680	On FortiOS, the *Dashboard* > *FortiView Destination Interfaces*, *Dashboard* > *FortiView Source Interfaces* pages, and *Policy & Objects* > *Firewall Policy* > *Edit Policy* page display incorrect bandwidth units.
1008863	SNAT `type port-block-allocation` does not work as expected in NAT64.
1010037	When editing object address on the *Policy & Objects* > *Addresses* page, the GUI does not function as expected if the address being edited contains a slash character.
1010824	FortiGate creates dummy destination IP logs when pinging a FortiGate VIP.
1011438	On the *Policy & Objects* > *Firewall Policy List* page, the *Interface Pair View* does not display policies alphanumerically and by interface alias.
1012239	When creating a new policy using the GUI in TP mode, NAT is automatically enabled.
1013488	On the *Policy & Objects* > *Firewall Policy* page, searching for service port numbers in the *Firewall Policy* list does not return any results.
1014584	On the *Policy & Objects* > *Firewall Policy* page, firewall policies with FQDN show as *unresolved* in the table.
1016893	On the *Policy & Objects* > *Firewall Policy* page, when hovering over addresses in the *Source* or *Destination* columns, the *tooltip* window does not scroll when there are a large number of addresses.
1022116	After editing a policy on the *Interface Pair View* window on the *Policy & Objects* > *Firewall Policy* page, the display order changes.
1034378	SMTP traffic does not egress from the same interface when a UTM profile is used in a proxy-based policy.

FortiGate 6000 and 7000 platforms

Bug ID	Description
638799	The DHCPv6 client does not work with vcluster2.
694958	On FortiGate 7000 models, the *Power Supply* status displays as *Normal* in the GUI when there is a logged power failure.
819274	On the *Query* > *Routing Menu* page in FortiManager, the routing table does not include the static or BGP types in `get router info routing-table all`.
885205	IPv6 ECMP is not supported for the FortiGate 6000F and 7000E platforms. IPv6 ECMP is supported for the FortiGate 7000F platform.

Bug ID	Description
892774	On FortiGate 7000 models, the hit counter on the FortiManager GUI does not display the correct values.
940541	A permanent MAC address is used instead of an HA virtual MAC address during automation.
946399	On the *Policy & Objects > Firewall Policy* page, address entries cannot be edited using the *Edit* button from the *tooltip* pop-up window.
983236	Under normal conditions, a FortiGate 6000 or 7000 may generate event log messages due to a known issue with a feature added to FortiOS 7.2 and 7.4. The feature is designed to create event log messages for certain DP channel traffic issues but also generates event log messages when the DP processor detects traffic anomalies that are part of normal traffic processing. This causes the event log messages to detect false positives that don't affect normal operation. For example, *DP channel 15 RX drop detected!* messages can be created when a routine problem is detected with a packet that would normally cause the DP processor to drop the packet. Similar discard message may also appear if the DP buffer is full.
1003879	Incorrect SLBC traffic-related statistics may be displayed on the FortiGate 6000 or FortiGate 7000 GUI (for example, in a dashboard widgets). This can occur if an FPC or FPM is not correctly registered for statistic collection during startup. This is purely a GUI display issue and does not impact system operation.
1005227	Full-cone NAT support for 7KF.
1013046	On FortiGate 6000 and 7000 models, interested traffic cannot trigger the IPsec tunnel.
1018594	On FortiGate 7000, if `gtp-mode` is enabled and then disabled, after disabling *gtp-enhanced mode* and rebooting the device, traffic is disrupted on the FIM and cannot be recovered.
1022499	IPv6 routes are not fully synchronized between HA primary and secondary units.
1025926	After a firmware upgrade, the configuration does not synchronize because the SDN connector password is unmatched.
1028313	On FortiGate 7000E and 7000F models in an HA cluster, FortiGate experiences a split brain scenario between the primary and secondary units when the primary unit is rebooted.
1029415	On FortiGate 6000 models in an HA cluster, the secondary unit does not send out logs when an interface is configured.
1030917	FortiGate displays an erroneous error for high/low warning alarms. SFP data transfer functions as expected.
1033050	On FortiGate 6000 models in an HA cluster, the secondary unit does not send out automated stitch emails for certain events.
1047553	HA remote access does not work as expected when `ha-port-dtag-mode` is double-tagging.

FortiView

Bug ID	Description
941521	On the *Dashboard > FortiView Websites* page, the *Category* filter does not work in the Japanese GUI.
945448	On the *Asset Vulnerability Monitor* page, filtering by FortiClient user does not show any results.

GUI

Bug ID	Description
896008	On wide resolution screens, the GUI-based CLI console widget has text overlap display issues on very wide screens.
946521	On the *System > Interfaces* page, the *set monitor-bandwidth* setting is not automatically disabled set when the interface bandwidth monitor for a port is deleted.
957441	On the *Firmware & Registration* page, the GUI displays a *Cannot determine mkey for cmdb source entry*. error message. This is purely a GUI display issue and does not impact system function.
964386	GUI dashboards show all the IPv6 sessions on every VDOM.
970528	The `hsts-max-age` is not enforced as set under `config system global`.
974988	FortiGate GUI should not show a license expired notification due to an expired device-level FortiManager Cloud license if it still has a valid account-level FortiManager Cloud license (function is not affected).
978716	On the *Security Profiles > Inline-CASB* page, when a SaaS application is added to a CASB profile, the option is not grayed out and the SaaS application can be added again.
981244	On the FortiGate GUI, IPsec or GRE configurations are missing when using `set type tunnel`.
983422	A GTP profile cannot be applied to policy using the GUI.
992346	`Node.JS` restarts and causes a `kill ESRCH` error after an upgrade.
993890	The `Node.JS` daemon restarts with a `kill ESRCH` error on FortiGate after an upgrade.
994915	The CLI GUI console is disconnected after creating a new VDOM.
996845	When saving a packet capture, the file name saves as a generic file name with no identifiable information.
998155	The `Node.JS` restarts and causes a `Cannot read properties of undefined (reading 'on')` error on FortiGate after an upgrade.

Bug ID	Description
1006079	When changing administrator account settings, the `trusthost10` setting is duplicated.
1006868	On the *FortiGuard* page, when setting a schedule using the *Scheduled updates* option on the GUI, the CLI displays the wrong value.
1007934	FortiGate may experience a memory usage issue with the node daemon once a connection is closed.
1013455	On the FortiGate GUI, inter-VDOM links are not available for packet capture.
1013866	The category action change is not saved if the category number is the same as the existing entry ID.
1017181	The `Node.JS` restarts and causes an `Error: The socket was closed while data was being compressed` error.

HA

Bug ID	Description
825380	When workspace configuration save mode is set to *manual* in the *System > Settings*, configuration changes made on the primary unit and then saved do not synchronize with the secondary unit when one of the cluster units are rebooted or shutdown after the change.
962525	In HA mode, FortiGate uses `ha-mgmt-interface` as the portal for the DNS resolver, even if this port may not be able to reach the DNS server.
985601	When configuring VDOMs in an HA cluster, the VDOM assigned to the VDOM link in vcluster2 active on the secondary unit is incorrect.
985967	Session synced with FGSP does not allow immediate failover when UTM is enabled in flow mode.
988944	On the *Fabric Management* page, the HA Secondary lists both primary and secondary FortiGate units.
992758	When uploading certificates, HA can go out of synchronization.
993849	After restoring a VDOM configuration, the HA is not synchronized.
995340	An issue with `hasync` in the secondary unit may cause FortiGate to enter into conserve mode.
998004	When the HA management interface is set a LAG, it is not synchronized to newly joining secondary HA devices.
1000001	A secondary HA unit may go into conserve mode when joining an HA cluster if the FortiGate's configuration is large.
1000808	FortiGate in an HA setup has an unnecessary primary unit selection when a new member joins or reboots one member in the VC cluster when the VC has more than 2 units.

Bug ID	Description
1002682	The VMware SDN connector does not respect the `ha-direct` setting and uses the management interface, causing traffic to be dropped.
1004215	Local out traffic from the primary HA unit uses the wrong interface when SNMP points to the secondary HA unit.
1005596	Using RADIUS login on the secondary unit does not work as expected when trying to login to the primary and secondary units at the same time.
1007395	When downgrading to a 7.2.x firmware version, an error message displays on the primary HA device and does not get removed when the device is rebooted.
1013152	After a factory reset, the FortiGate HA cluster may remain out of synchronization between the primary and secondary units.
1015950	When upgrading a FortiGate VM Analyzer, a CPU usage issue causes the auto scale cluster to go out of synchronization.
1017177	A WAD processing issue causes the SNMP to not respond in an HA cluster.
1018937	In a FortiGate HA configuration, the tunnel connection to FortiManager is disrupted due to a mismatched serial number and local certificate issue.
1024535	In an FGSP cluster configuration running in TP mode, reply traffic in asymmetric flow is not offloaded to NP.
1025585	Network traffic may be disrupted due to a linking issue with upstream routers.
1027149	When creating a new VDOM in an HA configuration, FortiGate may not operate as expected due to an `hasync` issue.
1029441	In an HA cluster on the SCO4 platform, the secondary unit enters a continuous rebooting cycle due to an interruption in the kernel after a firmware upgrade.
1032415	On the *System > HA* page, all HA vcluster device roles display as *Primary* in the *Role* column.
1033083	HA sessions are not synchronized properly causing a high number of sessions on the primary unit and the standby unit enters into conserve mode.
1033626	During a firewall failover, the multicast traffic is not forwarded within an appropriate time frame.
1034326	In a HA cluster using FGSP mode, the primary and secondary units cannot synchronize the lease agreements due to a synchronization issue with the DHCP server.

Hyperscale

Bug ID	Description
817562	lpmd fails to correctly handle different VRFs, treating all as vrf 0, causing improper route management and affecting network traffic isolation.

Bug ID	Description
994019	Harpin traffic may not work due to a rare situation caused by a race condition.
961684	When DoS policies are used and the system is under stress conditions, BGP might go down.
967017	TCP or UDP timer profiles configured using `config-system npu` may not work as intended.
975220	The Gentree Compiler is enabled by default on all NP7 platforms for threat feed support.
976972	New primary can get stuck on failover with HTTP CC sessions.
993343	In a Hyperscale VDOM, an interruption in the kernel occurs with `set nat46-generate-ipv6-fragment-header` enabled.
1016478	When modifying existing policies with a BOA loaded configuration, NPD is not working as expected.
1024274	When Hyperscale logging is enabled with multicast log, the log is not sent to servers that are configured to receive multicast logs.
1024313	The template for the netflow v9 log packets is not included in the configuration.
1024902	After FTP traffic passes, the `npu-session stat` does not display the accurate amount of actual sessions on FortiGate.
1032471	When rebooting the secondary unit in an FGSP setup, the session information is not visible in the secondary unit.
1034100	The NPD process is interrupted in a Hyperscale VDOM configuration after an upgrade and sessions are not setup on hardware.

ICAP

Bug ID	Description
1022247	In an ICAP profile, the `set request-failure bypass` option does not work as expected resulting in traffic being blocked.

Intrusion Prevention

Bug ID	Description
810783	The number of IPS sessions is higher than kernel sessions, which causes the FortiGate to enter conserve mode.
910267	In an FGSP setup running emix traffic, nTurbo values run in the negative.

Bug ID	Description
916175	In rare cases, the IPS engine may not handle buffer overflow.
968464	nTurbo passes the wrong ID to the IPS engine when the `set vrf` value is above 32.
979586	When applying an IPS profile with offloading enabled, WLAN authentication does not function as expected caused by EAP transaction timeouts.
995997	ISDB is shown in 'diag test app ipsmonitor 1' output when IPS/AppCtrl feature are not enabled.
1000223	HTTPS connections to a Virtual IP (VIP) on TCP port 8015 are incorrectly blocked by the firewall, displaying an IPS block page even when no packet from the outside to TCP port 8015 should reach the internal VIP address.
1008064	The IPS DB is not preserved when upgrading to 7.2.5 or later.
1008107	Because of how IPS handles long-lived nTurbo sessions, throughput capacity may be reduced after an FGCP HA failover. Once all failed-over nTurbo sessions have been completed, throughput will return to normal.
1011702	FortiGate experiences a CPU usage issue which may lead to an interruption in the kernel when dos-policy is enabled.
1013666	When a FGT device on a closed network uses FMG as the vulnerability lookup server, the lookups fail because the IPS engine does not honor the override server setting.
1026354	On FortiGate, the softirq experiences a CPU usage issue with the IPS engine when traffic hits a firewall policy without an IPS profile.

IPsec VPN

Bug ID	Description
564920	IPsec VPN fails to connect if `ftm-push` is configured.
787673	IPsec VPN types are not saved to the configuration when edited using the GUI.
942618	Traffic does not pass through an `vpn-id-ipip` IPsec tunnel when wanopt is enabled on a firewall policy.
950445	After a third-party router failover, traffic traversing the IPsec tunnel is lost.
966085	IKEv2 authorization with an invalid certificate can cause tunnel status mismatch.
968055	After an upgrade, L2TP/IPsec connections using the RIP protocol do not function as expected.
968376	Changes to the IPsec tunnel type from a static to dialup user on the GUI does not change the actual configuration.
974648	Editing existing IPsec aggregate members does not update in the bundle list.

Bug ID	Description
978243	Unable to send all prefixes through FortiClient using dial-up IPsec VPN split tunnel to macOS devices.
986756	VPN traffic does not pass between VDOMs through intervdom links.
989570	On FortiGate, firewall address groups created using the VPN wizard cannot be edited.
994115	When ASIC offload is enabled and packet size is larger than 1422, FortiGate does not generate an *ICMP Type 3, Code 4* error message.
996625	Unable to create a FortiClient dial-up VPN with certificate authentication because a peer CA certificate cannot be selected.
998229	Traffic loss is experienced on inter-region ADVPN tunnels after phase 2 rekey.
999619	A peername conflict error occurs when users configure static tunnels and then dynamic tunnels. There is no conflict when done in the reverse order.
1001602	Using IPSec over back to back EMAC VLAN interfaces does not work as expected with NPU offload enabled.
1001996	The iked does not function as expected due to a misplaced object being created in the secondary HA during failover.
1003830	IPsec VPN tunnel phase 2 instability after upgrading to 7.4.2 on the NP6xlite platform.
1004272	On NP7 platforms that are used a hub in a hub and spoke configuration, traffic packets are dropped on IPsec tunnel spokes due to an anti-replay error.
1006110	When an ipip tunnel over IPsec is configured, the configuration may cause running traffic to access the deleted SA.
1007043	Iked may experience an interruption in operation resulting in all VPN tunnels going down.
1009732	If there are more than 2000 dialup IPsec tunnel interfaces used in multiple FGT firewall polices, and IKE policy update may not able to complete before IKE watchdog timeout.
1014026	On the *VPN > IPsec Tunnels* page, after creating an IPsec tunnel in phase 2, the *Named Address* field does not show any results.
1019269	On the *VPN > IPsec Tunnels* page, when language setting on FortiOS is set to anything other than English, the *Status* column displays active (green up arrow) when the tunnel is inactive.
1020250	A second IPsec tunnel cannot be added on different IP versions that use the same *peerid*.
1025202	After a peer-side interface shutdown and reboot, the `dpd status` does not return to `OK`, even when the peer-interface is up and SA renegotiated.
1029262	IPsec VPN traffic does not pass over the tunnel when the HA heartbeat cable is reconnected.
1031985	IPSec VPN tunnel does not go down when the VPN peer route is removed from the routing table.
1033154	FortiGate does not unregister the `net_device` causing the unit to encounter a performance issue.

Bug ID	Description
1041019	When QKD dialup is enabled, IKE SA cannot establish a connection and generates an error.
1047148	FortiGate prematurely switches ports when IKE fragmented packets are not delivered from FortiClient to FortiOS.

Log & Report

Bug ID	Description
872493	Disk logging files are cached in the kernel, causing high memory usage.
925649	An interruption may occur in the daemon locallogd when the system is in memory conserve mode.
957130	On the *Log & Report > Forward Traffic* page, when running version 7.2.3 of FortiGate, log retrieval speed from FortiAnalyzer is slow.
960661	FortiAnalyzer report is not available to view for the secondary unit in the HA cluster on the *Log & Report > Reports* page.
973673	The `monitor-failure-retry-period` is not working as expected when the log daemon restarts the next oftp connection after a connection timeout.
993476	On FortiGate, the locallogd process encounters a CPU usage issue for a few minutes after a reboot or a restart.
998215	Frequent API queries to add and remove objects can result in a memory usage issue on FortiGate.
1000600	When a log output is generated, the position of the *rawdata* field is not consistent, causing some information to be missing.
1002502	Add log when duplicate IP detected.
1005171	After upgrading to version 7.0.14, the system event log generates false positives for individual ports that are not used in any configuration.
1006611	FortiOS may not function as expected when the miglogd application attempts to process logs.
1008626	ReportD does not function as expected when event logs have message fields over 2000 bytes.
1010074	The miglogd does not function as expected due to a CPU usage issue.
1010244	When uploading the log file to the FTP server, some parts of the log files are not included in the upload.
1010428	On the *Log & Report > System Events* page, the log displays an *FortiGate has experienced an unexpected power off* error message when an interruption occurs in the kernel.
1011172	The miglogd does not forward log packages to FortiAnalyzer due to a memory usage issue.

Bug ID	Description
1012862	User equipment IP addresses are not visible in traffic logs.
1018392	A memory usage issue in the fgtlogd daemon causes FortiGate to enter into conserve mode.
1021195	The IPS engine sends a high frequency of IoT device queries even when the device identification is set to disabled.
1025797	The `appcat` field location is inconsistently placed in the system log.
1028167	A system log message is not generated when `syslogd setting` is enabled or disabled in the GUI or CLI.
1028309	On FortiGate, a CPU usage issue occurs in the locallogd.
1040678	The first character `User-Agent` information is not included in the web filter log.

Proxy

Bug ID	Description
871273	When the kernel API tries to access the command buffer, the device enters D state due to a kernel interruption.
900546	DNS proxy may resolve with an IPv4 address, even when `pref-dns-result` is set to IPv6, if the IPv4 response comes first and there is no DNS cache.
918652	FortiGate experiences a CPU usage issue and halts traffic when there are a large amount of addresses and external resource is updated frequently.
922093	CPU usage issue in WAD caused by source port exhaustion when using WAN optimization.
933502	When a forward server with proxy authorization is configured with certain traffic, a memory usage issue in the WAD process interrupts to operation of FortiGate.
949464	On FortiGate, a memory usage issue in the WAD may cause the unit to enter into conserve mode.
956481	On FortiGate 6000 models, when an explicit proxy is configured, the TCP 3-way handshake does complete as expected.
979361	After an upgrade, FortiOS encounters an error condition in the application daemon wad caused by an SSL cache error.
982553	After upgrading from version 6.4.13 to version 7.0.12 or 7.0.13, FortiGate experiences a memory usage issue.
983997	Certificate validation fails on FortiGate/FortiProxy when using root CAs with identical subjects but distinct public keys and serial numbers.
987483	On FortiGate, the WAD daemon does not work as expected due to a NULL pointer issue.

Bug ID	Description
987655	RPM files could not be blocked in HTTP downloading on Box Cloud website in proxy mode.
988473	On FortiGate 61E and 81E models, a daemon WAD issue causes high memory usage.
994101	SSL Logs show *certificate-probe-failed* error when web profile is enabled.
999118	TCP connections are not distributed properly when `src-affinity-exempt` is enabled.
1000653	The proxy policy does not validate IP addresses in the XFF when an HTTP address is sent by AGW.
1001598	When proxy-based policies are enabled, HTTP2 resources cannot be accessed.
1003481	FortiGate may not work as expected due to an error condition in the daemon WAD.
1008079	Memory usage increase for WAD process.
1010718	The proxy inspection mode policy is deleted from the configuration without notification after an upgrade.
1012965	Deep inspection and web filter for an explicit proxy policy do not work if `profile-protocol-options` has additional ports for HTTP.
1016970	High memory usage in WAD causes FortiGate to enter into conserve mode.
1019230	On FortiGate, a memory usage issue in the WAD causes the unit to enter into conserve mode.
1020828	An HTTP2 stream issue causes an error condition in the WAD.
1021346	Starting from version 7.4.4, FortiOS no longer supports proxy-related features for FortiGate models with 2 GB RAM or less. When upgrading from FOS 7.4.3 or earlier to later versions, the UTM profile feature set was not properly changed from proxy to flow.
1021699	When some regex objects do not match the policy, it can result in all other objects in the same policy to not match.
1028017	Change the default value of `cert-probe-failure` in `firewall ssl-ssh-profile` to `allow`.
1033729	An IMAP connection to an external application email server is not established in a proxy mode policy with DPI enabled.
1036201	A memory usage issue occurs in the WAD daemon process for `wad-config-notify`.
1039006	Some websites cannot open subpages when the HTTP2 header value exceeds 16MB.

REST API

Bug ID	Description
859680	In an HA setup with vCluster, a CMDB API request to the primary cluster does not synchronize the configuration to the secondary cluster.

Bug ID	Description
984499	REST API query `/api/v2/monitor/system/ha-peer` does not return the primary attribute of an HA cluster member.
1026195	When importing a certificate using API, it is not visible on FortiOS despite displaying that the import was successful.

Routing

Bug ID	Description
779825	In SD-WAN with `interface-select-method` enabled, if link performance is affected, local out traffic continues on the same link.
792512	The dashboard Session widget cannot display the correct IPv6 session count per VDOM.
923994	On the *Network* > *Static Routes* page, VRF information does not display in the VRF column.
924693	On the *Network* > *SD-WAN* > *SD-WAN Rules* page, member interfaces that are down are incorrectly shown as up. The tooltip on the interface shows the correct status.
966681	FortiGate cannot ping an IPv6 loopback address.
978683	The `link-down-failover` command does not bring the BGP peering down when the IPsec tunnel is brought down on the peer FortiGate.
987360	SD-WAN health checks are not deleted after all related references are removed when applied over ADVPN.
989012	The `ICMP_TIME_EXCEEDED` packet does not follow the original ICMP path displays the incorrect traceroute from the user.
990211	On the *Network* > *BGP* > *Neighbor Groups* page, an error message is shown under *IPv4 Filtering* for routes that are already have in and out routes configured in the GUI.
993843	On FortiGate 1800F models, the VXLAN tunnel on a Loopback interface does not match SD-WAN rules.
995972	When accessing the ZebOS in chroot, the ospfd does not work as expected.
1000433	The IPv6 route with dynamic gateway enabled cannot be configured after an upgrade and reboot.
1001556	VXLAN does not match SD-WAN rule when a service is specified.
1002132	A BGP neighbor over GRE tunnel does not get established after upgrading due to anti-spoofing not functioning as expected.
1002721	Existing `dcerpc` sessions do not follow SD-WAN rules for routing tables.
1002851	BGP Stale routes do not function as expected in an HA configuration.

Bug ID	Description
1004249	FortiGate routes traffic to an interface with a physical status of DOWN.
1006703	OSPF logs for neighbor status are not generated when using multiple VRFs.
1006753	When renewing the LTE WWAN IP, some packets are sent using the old IP address causing traffic to drop.
1007163	In a hub and spoke configuration, the spoke cannot resolve BGP routes to HUB when a shortcut is established.
1008818	The default configuration of the Fabric Overlay Orchestrator causes concurrent disconnects with the BGP.
1009907	The OSPF daemon does not function as expected causing routing to stop working after an HA cluster failover.
1011263	FortiGate does not advertise default route to its EBGP neighbor when `capability-default-originate` is enabled.
1012321	When modifying an address in VDOM DAF, the session is routed to the default static route instead of the policy routing.
1012895	The `set-regexp` command does not function as expected in the `extcommunity-list`.
1013773	FortiGate does not automatically add the set LTE dynamic route to the routing table.
1013940	After an HA failover and the SD-WAN neighbor role is selected as the primary, the SD-WAN service with role set as primary is disabled.
1017950	The OSPF process encounters a CPU usage issue when there are a high number of prefixes and `redistribute bgp` is enabled.
1019166	On the *Network* > *Routing Objects* page, route map objects cannot be edited and saved.
1020474	In a hub and spoke configuration, the IPsec SA MTU calculation does not match with the `vpn-id-ipip` encapsulation resulting in a fragmentation issue.
1021666	When adding a route using SD-WAN zone, there is no overlap check on existing gateway IP addresses which prevents routes from being added.
1022665	When the SNAT does not match the outgoing interface during failover from the secondary to the primary, SD-WAN traffic does not failover back to the primary WAN.
1023878	SD-WAN SLA shows intermittent disruptions of packet loss on all links simultaneously, even though there is no actual packet loss.
1025201	FortiGate encounters a duplication issue in a hub and spoke configuration with `set packet-duplication force` enabled on a spoke and `set packet-de-duplication` enabled on the hub.
1031394	On the *Network* > *Routing Objects* page, the *Set AS path* on the *Edit Rule* pane does not allow the use of the full range AS numbers.
1042487	When setting a prefix using the set prefix option, the prefix entry is created using a default route instead of the desired configuration.

Bug ID	Description
1042848	BGP multipath routing does not work as expected in a BGP confederation setup.
1044403	HTTPS/SSH traffic fails on the interface when policy routing is enabled due to incorrect ARP requests from cached routes.
1050992	IKE-SAML reply traffic does not egress from the same interface as ingress traffic when the route is present in the routing table.

Security Fabric

Bug ID	Description
899585	When running a security rating check, the security rating endpoints do not use the latest endpoint data.
907452	On FortiOS, GUI access can be prevented when requesting a security rating over CSF from FortiAnalyzer.
948322	After deauthorizing a downstream FortiGate from the *System > Firmware & Registration* page, the page may appear to be stuck to loading.
958429	On the *Security Fabric > Automation* page, the webhook request header does not contain `Content-type: application/json` when using the JSON format. This causes Microsoft Teams to reject the request.
968621	Erroneous memory allocation resulting in unexpected behavior in csfd after upgrading.
972921	On the *Security Fabric > External Connectors* page, the comments are not working as expected in the threat feed list for the domain threat feed.
984127	FortiGate shows the wrong notification to setup an upstream device that is not a FortiGate to the Security Fabric.
987531	Threat Feed connectors in different VDOMs cannot use the source IP when using internal interfaces.
989184	The Security Fabric root device takes longer than expected to synchronize with downstream secondary HA devices in an HA configuration.
990703	In certain scenarios, dynamic addresses managed by the Azure SDN connector may be removed leading to potential network interruptions.
991462, 993279	When automation stitch is configured with the once schedule, the stitch is not synchronized to the downstream FortiGates.
994167	An issue with the csfd results in FortiGate being disconnected from the Security Fabric.
1000880	When renaming an existing address name on a downstream FortiGate from the root FortiGate, a new address is created on the downstream FortiGate with the updated name.

Bug ID	Description
1003503	During a full fabric upgrade where a PoE powered device (PD) connected to a Power Sourcing Equipment (PSE) are upgraded, the upgrade of the PD may be interrupted if the PSE finishes upgrading first, causing a boot loop on the PD. This behavior is now avoided by performing upgrades on PDs first before upgrading PSEs and the FortiGate itself.
1008901	STIX threat feeds cannot download properly due to a JSON parsing issue.
1014961	The SDN Connector for nutanix does not return all the entries.
1023998	On the *System > Firmware & Registration* page, the firmware information for the secondary device is not shown when the *Security Fabric* is enabled in the GUI.
1026700	Internal REST API requests are routed through the httpsd CSF proxy, leading to issues with chunked encoding for large responses and blocking behavior.
1041855	kubed crashed with signal 6 (Aborted) when testing kubernetes sdn connector during robot auto test.

SSL VPN

Bug ID	Description
905050	Intermittent behavior in samld due to an absent crucial parameter in the SP login response may lead to SSL VPN users experiencing disconnections.
947536	SSL VPN crashes on corporate FortiGate due to watchdog timeout when a single connection enters an infinite loop of read iterations and the worker process becomes unresponsive to new connections
982705	When editing a security policy, the custom signature is removed from the policy.
983513	The `two-factor-fac-expiry` command is not working as expected for remote RADIUS users with a remote token set in FortiAuthenticator.
999378	When the GUI tries to write a QR code for the SSL VPN configuration to the file system to send in an email, it tries to write it in a read-only folder.
999661	When changing SSL VPN access in the *Restrict Access* field to *Allow access from any host* and enabling the *Negate Source* option on the *VPN > SSL VPN* page, the changes made in the GUI are not reflected in the CLI.
1000674	When generating function backtrace in crash logs for ARM32, SSL VPN frequently crashes due to segmentation faults.
1001272	The SAML DB Insert does not function as expected and causes a CPU usage issue.
1003672	When RDP is accessed through SSL VPN web mode, keyboard strokes on-screen lag behind what is being typed by users.
1004633	FortiGate does not respond to ARP packets related to SSL VPN client IP addresses.

Bug ID	Description
1012486	SSL VPN OS checklist does not include minor version numbers of macOS 13 and 14.
1018928	A CPU usage issue occurs in the tvc daemon when the vpn server cannot be reached.
1022439	SAMLD encounters a memory usage issue, preventing successful login attempts on SSL VPN.
1024584	The SSL VPN IP pool may get exhausted when `tunnel-connect-without-reauth` is enabled.
1024837	OneLogin SAML does not work with SSL VPN after upgrading to 7.0.15 or 7.4.3.
1026102	SSL VPN encounters a CPU usage issue in the daemon after updating the language from the GUI.
1027863	NAS-IP per SSL-VPN realm does not work as expected under the `config vpn ssl web realm` after upgrading firmware.
1036542	When using an SSL VPN quick connection in web mode, web page images are distorted.
1041202	SSL VPN does not work as expected if an LDAP user UPN exceeds 35 characters.

Switch Controller

Bug ID	Description
688724	A non-default LLDP profile with a configured `med-network-policy` cannot be applied on a switch port.
899414	On the *WiFi & Switch Controller > WiFi maps* page *Diagnostics and Tools* panel, and on the *WiFi & Switch Controller > FortiSwitch Clients* page, the status of the LACP interface is incorrectly shown as down when it is up. This is a GUI issue that does not affect the operations of the LACP interface. To view the correct status of the LACP interface, go to the *WiFi & Switch Controller > FortiSwitch* Ports page, or use the CLI.
944975	After configuring the `switch-controller lldp-profile`, the changes are not reflected in the CLI when the `show switch-controller lldp-profile` command is run.
960240	On the *WiFi & Switch Controller > Managed FortiSwitches* page, ISL links do not display as solid connections.
984404	On the *System > Firmware & Registration* page, after upgrading the version 7.4.2, the FortiSwitch shows as *not registered* in the GUI.
991855	The `access-mode` and `storm control policy` commands are not visible in FortiGate clusters causing them to go out of synchronization and does not send updated configurations to the FortiSwitch.
995518	On the *WiFi & Switch Controller > Managed FortiSwitches > Upgrade* page, the *FortiGuard* option is not available to upgrade when new firmware is available.

Bug ID	Description
1000663	The switch-controller managed-switch ports' configurations are getting removed after each reboot.
1023888	On the *WiFi & Switch Controller > FortiSwitch Ports* page, changes made to the *Allowed VLANs* and *Native VLAN* columns are not saved when edited on the GUI.
1032105	FortiGate in an HA configuration goes out of synchronization due to a split-port interface on FortiSwitch.
1033874	FortiGate does not work as expected due an issue with a null variable in the `cu_acd`.

System

Bug ID	Description
860534	VDOM settings are removed after rebooting FortiGate in TP mode with multiple VDOMs enabled.
880611	FortiGate enters into conserve mode due to a memory usage issue.
901721	In a certain edge case, traffic directed towards a VLAN interface could cause an kernel interruption.
910364	CPU usage issue in miglogd caused by constant updates to the ZTNA tags.
916172	GRE traffic is still allowed to flow through when the GRE interface is disabled.
917886	On FortiGate, fragmented packets with specific flow types are not forwarded to the correct ports on a LAG interface.
925554	On the *Network > Interfaces* page, hardware and software switches show VLAN interfaces as down instead of up. The actual status of the VLAN interface can be verified using the command line.
932002	Possible infinite loop can cause FortiOS to become unresponsive until the FortiGate goes through a power cycle.
935158	The FortiGate console prints `check_gui_redir_file: No such file or directory` after rebooting.
938475	A memory usage issue occurs when multiple threads try to access VLAN group.
946393	On FortiGate, the software switch does not send an ARP reply from OIF.
947398	When an EMAC VLAN interface is set up on top of a redundant interface, the kernel may encounter an error when rebooting.
948875	The passthrough GRE keepalive packets are not offloaded on NP7 platforms.
952284	A FortiGate with 2 GB of memory enters conserve mode when a node uses 20% of the memory.

Bug ID	Description
953547	SCTP traffic does not get forwarded by a connected hardware switch on FortiGate.
956697	On NP7 platforms, the FortiGate maybe reboot twice when upgrading to 7.4.2 or restoring a configuration after a factory reset or burn image. This issue does not impact FortiOS functionality.
959660	The `private-data-encryption` configuration does not use the configured private key.
964465	Administrators with read-write permission for WiFi and read permission for network configuration cannot create SSIDs on the *System > Administrator Profiles* page.
964820	Traffic forwarding on Dialup VPN IPSec does not work as expected when `npu-offload` is enabled.
966237	On NP7 platforms, egress shaping on a physical interface is not enforced on traffic according to the shaping profile definition.
966384	On FortiGate 401F and 601F models, the CR mediatype option on x5-x8 ports is not available.
967436	DAC cable between FortiGate and FortiSwitch stops working after upgrading from 7.2.6 to 7.2.7.
968134	FortiGate 200F experiences a performance issue due to Marvell switch HOL mode.
970053, 1006324	When a different transceiver type is added to FortiGate, the new transceiver information does not update in the GUI or CLI.
972170	On FortiGate 80F models, the 100FULL speed option is not available for the SPF port.
974740	FortiGate 2600F does not set 10G ports to 100G.
975496	FortiGate 200F experiences slow download and upload speeds when traversing from a 1G to a 10G interface.
975778, 1004883	VLAN traffic is stopped when created on LACP with `split-port-mode` configured.
976314	After upgrading FortiGate and not changing any configuration details, the output of `s_duplex` in `get hardware nic port` command displays `Half` instead of `Full`. This is purely a display issue and does not affect system operation.
978122	FortiGate experiences packet drop when `egress-shaping-profile` is applied to a LAG interface.
979645	TCP traffic is classified as ip-frag and dropped when HPE entries are incorrectly configured in FortiOS versions prior to the fix.
981433	The ipmcsensord does not work as expected when executing sensor-related commands before the high-end device sensor finishes booting up.
986713	When restoring a FortiGate from a backup configuration, the device enters into system maintenance mode and is not accessible.
986926	On the FortiGate 90xG models, the ULL interfaces for x5 - x8 are down after being set to 25G speed.

Bug ID	Description
988528	With NGFW mixed traffic, FortiGate experiences a CPU usage issue.
989473	On FortiGate, the device may not work as expected due to a memory usage issue with the cmdbsvr.
989629	FortiGate does not show additional speed options outside of *auto* on a WAN interface.
990409	After an upgrade on FortiOS, the kernel operation is interrupted and reboots due to a switch command issue.
991264	The locallogd process may cause a CPU usage issue on FortiGate.
995269	On FortiGate, the multicast session walker is rescheduled on the same CPU instead of the next CPU.
995442	FortiGate may generate a *Power Redundancy Alarm* error when there is no power loss. The error also does not show up in the system log.
996893	On FortiWiFi 81F-2R-3G4G-POE models, GPS service cannot be activated.
997563	SNMP *ifSpeed* OID show values as zero on VLAN interfaces in hardware switches.
1000194	FortiGate does not show QoS statistics in the `diagnose netlink interface list` command when offloading is disabled in a firewall policy and IPsec phase 1 tunnel on NP7 platforms.
1000658	After an integrity check, the dates on the hash files do not match causing a false positive error message.
1001133	After an upgrade, FortiGate receives a `PSU RPS LOST` traps error despite not having any RPS connected.
1001498	On FortiGate, TCP and UDP traffic cannot pass through with `dos-offload` enabled.
1001601	A kernel interruption on FortiGate prevents it from rebooting after an upgrade with a specific configuration.
1001722	VLAN/EMAC VLAN traffic is unexpectedly blocked under certain conditions.
1001938	Support Kazakhstan time zone change to a single time zone, UTC+5.
1002323	After restoring a configuration on FortiGate with the interface changed from *aggregate* to *physical*, the interface switches back to *aggregate* and cannot be changed back to *physical*.
1002766	FortiGate prevents select interface a as an option for traceroute, ssl, and telnet services.
1003026	On SoC3/SoC4 platforms, a kernel interruption may occur when running WAD monitoring scripts.
1003349	CPU usage issue in WAD after upgrading from 7.4.1 to 7.4.3 when using address group member.
1003925	After deleting a redundant port on FortiGate, the port does not register as being available and generates an error.
1045701	FGT-80F-BP fails to boot up after burning image, showing error message "cli 161 die in an exception in line 300: end".

Bug ID	Description
1004804	FortiGate running firmware 7.2.7, the device encounters an error condition in the application daemon.
1005573	FortiGate incorrectly sends `set csr` instead of `set certificate` to FortiManager after auto enrolling a certificate using SCEP.
1006024	Administrator accounts using an admin profile with only *FortiGuard Updates* read-write permissions cannot open the *FortiGuard* page.
1006979	FortiGate may encounter a memory usage issue on the flpold process, causing the primary and secondary units to go out of synchronization.
1008049	The I2C bus becomes stuck during an upgrade due to an error in the `switch-config-init` command.
1009278	Traffic does not hit a new policy created in the GUI or CLI due to an `auto-script` command issue.
1009853	Outgoing traffic from EMAC-VLAN uses default cos tag when traffic is not offloaded.
1011229	On FortiGate, a slab memory usage issue causes the device to enter into conserve mode.
1011968	Jumbo frame packets do not pass through all split ports and may cause packets to drop.
1012518	Some FortiGate models on NP6/NP6Lite/NP6xLite platforms experience unexpected behavior due to certain traffic conditions after upgrading to 7.2.8. Traffic may be interrupted momentarily.
1013010	On some FortiGates, 25 GB transceivers are displayed as 10 GB transceivers in the `get system interface transceiver` command.
1015169	On FortiGate, SNMP v3 cannot use `-u <username-pri/sec-SN>` for both IPv4 or IPv6 address queries and SNMP v2 cannot use `-c <comm-SN>` for IPv6 address queries.
1015736	On FortiWiFi 60/61F models, the STATUS LED light does not turn on after rebooting the device.
1017446	Some TTL exceeded packets are not forwarded on their destination and an error message is not always generated.
1018022	On FortiGate, VXLAN traffic is not offloaded properly resulting in some packets being dropped.
1019749	On a VDOM, running `sudo global show` does not return any `system interfaces` information.
1021355	FortiGate encounters a CPU usage issue when there are a high volume of traffic and scripts running on the device which could lead to an issue with performance.
1021542	FortiGate reboots twice after a factory reset when `gtp-enchanced-mode` is enabled.
1021632	FortiGate may experience intermittent traffic loss on an LACP interface in a virtual wire pair with `l2forward` enabled.
1024737	On FortiGate, when `set ull-port-mode` is set to 25G, ports x5-x8 show a status of DOWN.
1025503	On the *Network > Diagnostics* page, FortiGate shows that the packet capture capacity has been reached when there is no captured packet on the device.

Bug ID	Description
1025576	Passthrough GRE traffic using Transparent Ethernet Bridging packets as the protocol type are not offloaded on NP7 platforms.
1025927	In an HA configuration, FortiGate cannot access the GUI after a firmware upgrade due to a certificate matching issue.
1027335	Interface cannot ping out with dos-offloading enabled but no DoS policy.
1029351	The OPC VM does not boot up when in native mode.
1029874	FortiCron does not work as expected due to a memory usage issue in the daemon.
1032018	The SFP+ port LED does not illuminate and displays a speed 10Mbps even though the link status up and speed is set to 1000Mbps.
1034322	FortiGates using a SOC4 platform with a virtual switch configured may continuously reboot when upgrading due to an interruption in the kernel.
1037075	On FortiGate, an interruption occurs in the kernel when running WAD process monitoring scripts.
1037393	FortiGate reboots due to the maximum buffer length difference between nTurbo and NPU HW.
1041457	The kernel 4.19 cannot concurrently reassemble IPv4 fragments for a source IP with more than 64 destination IP addresses.
1041491	FortiGate encounters a memory usage issue in the `node.js` daemon when there is no traffic running through it.
1041669	FortiGate does not upgrade if `private-data-encryption` is enabled and the device is not rebooted.
1043979	An interruption occurs in the kernel resulting in intermittent power disruptions and rebooting of FortiGate.
1048299	User names for some cloud-based services cannot be configured under `config system email-server` that exceed 64 characters.
1052004	FortiGate encounters a memory usage issue when there is no traffic running and the configuration is not fully loaded.

Upgrade

Bug ID	Description
925567	When upgrading multiple firmware versions in the GUI, the *Follow upgrade path* option does not respect the recommended upgrade path.
952828	The automatic patch upgrade feature overlooks patch release with the Feature label. Consequently, a FortiGate running 7.4.2 GA does not automatically upgrade to 7.4.3 GA.

Bug ID	Description
955810	Upgrading FortiOS is unsuccessful due to *unmount shared data partition failed* error.
955835	When `auto-upgrade` is disabled, scheduled upgrades on FortiGate are not automatically canceled. To cancel any scheduled upgrades, `exec federated-upgrade cancel` must be done manually.
977281	After the FortiGate in an HA environment is upgraded using the Fabric upgrade feature, the GUI might incorrectly show the status *Downgrade to 7.2.X shortly*, even though the upgrade has completed. This is only a display issue; the Fabric upgrade will not recur unless it is manually scheduled.
999324	FortiGate Pay-As-You-Go or On-demand VM versions cannot upload firmware using the *System > Firmware & Registration > File Upload* page.
1013821	On FortiGate, an interruption occurs in the kernel in both HA FortiGates when an HA cluster's firmware is upgraded.
1017519	Auto firmware-upgrade may run when a FortiGate is added to a FortiManager that is added behind a NAT.
1025687	After a firmware upgrade, the `config system npu-post` command does not work as expected.
1027462	When restoring an FortiGate, the 7.4.1 config file with deprecated Inline CASB entries displays errors messages and causes the confsyncd to not function as expected.
1031574	During a graceful upgrade, the confsync daemon and updated daemon encounter a memory usage issue, causing a race condition.
1050162	The `auth-pwd` and `private-key` error after upgrading from B2662 when `private-data-encryption` enabled.
1053795	On FortiOS, passwords cannot be changed using the GUI with `password-policy` enabled.
1055486	On the *Firmware and Registration* page, when performing a Fabric Upgrade using the GUI for the whole Fabric topology that includes managed FortiAPs and FortiSwitches, the root FortiGate may use an incorrect recommended image for FortiAP and FortiSwitch due to a parsing issue.

User & Authentication

Bug ID	Description
946191	CPU usage issue in WAD caused by a high number of devices being detected by the device detection feature.
974298	When using the local-in firewall authentication with SAML method, SAML users cannot get access using the authentication portal.

Bug ID	Description
976790	WiFi clients are not authenticated when using the *Use my windows user account* option for LDAP authentication.
988958	When rsso user groups are updated, the session table is not cleared of old sessions and traffic still hits the old policy.
989760	On the *System* > *Certificates* page, error *Unable to create certificate* displays when uploading certificates using the PKCS12 (.pfx) format. The certificates are still uploaded.
1001026	Users are unable to use passwords that contain the *ñ* character for authentication.
1009213	After upgrading firmware on FortiGate, an interruption occurs in the fnbamd resulting in auto-connect not working as expected.
1016112	SSL VPN access is prevented when the LDAP server includes a two-factor authentication filter.
1018846	When SCEP is used with SSL connections, some TLS connections are missing the SNI extension on FortiGate.
1021157	Users are unable to use passwords that contain Polish characters *ńżźćłśąó* for RADIUS authentication.
1023605	Multiple errors observed in the IOTD debug log caused by connection timeouts.
1034898	After a firmware upgrade, FortiToken does not work as expected when using the GUI.
1036265	The `reply-to` option under `config system alertmail` is removed even for `custom mail-servers` with 2-factor authentication after an upgrade.
1039004	The `username-case-sensitive disable` setting is not respected for RSSO when a username has a capital letter.
1039490	FortiGate does not use a policy with deep inspection enabled on SSL profiles for SWG user access.

VM

Bug ID	Description
996389	AWS SDN Connector stops processing caused by the IAM external account role missing the `sts:AssumeRole`value.
998208	The FortiGate-VM system stops after sending an image to the HA secondary during an firmware upgrade due to different Flex-VM CPU license.
999599	On FortiGate AWS, the IPsec configuration goes missing after an upgrade due to an inconsistent table-size.
1001940	A newly created FGT-VM64 could not configure the vapp options settings.
1006570	VPN tunnels go down due to IKE authentication loss after a firmware upgrade on the VM.

Bug ID	Description
1016327	After rebooting, DPDK mode is disabled on a VLAN interface and traffic stops.
1019467	When the underlying interface is removed, the IPsec tunnel interface will still hold a dst reference.
1024011	The SDN connector does not update the correct IP addresses for either the upscale or downscale VMSS.
1025604	The SDN connector does not update the correct IP addresses when using Flexible VMSS.
1030534	On FortiGate, an HA failover does not work as expected when using an OCI environment.
1036917	When a intended policy is configured for interesting traffic subnets, traffic flow hits the implicit deny rule instead of the configured policy.
1040088	In an HA configuration, the secondary unit heartbeat port is accessible even though access to the interface is not allowed on that unit.

VoIP

Bug ID	Description
1004894	VOIPD experiences high memory usage and enters into conserve mode.

WAN Optimization

Bug ID	Description
899377	On FortiGate, an interruption occurs in the WAD causing traffic to stop and large files cannot be downloaded.

Web Filter

Bug ID	Description
634781	Unable to customize replacement message for FortiGuard category in web filter profile.
925801	Custom Images are not seen on Web Filter block replacement page for HTTP traffic in flow mode.

Bug ID	Description
975115	FortiGate prevents adding a regex string to a static URL filter table.
1002266	Web filtering does not update rating servers if there is a FortiGuard DNS change.
1004985	The webfilter cookie override trigger process had no issue observed and an override entry was created in the FortiGate, but client access was kept blocked by the old profile and the client received a replacement message with an override link just like the initial access to trigger the override.

WiFi Controller

Bug ID	Description
908282	On FortiGate, an interruption occurs with the `cw_acd` during failover to the secondary FortiGate.
915715	On a secondary FortiGate in an HA cluster, `user` and `vlan-id` values do not show up when using the `diagnose wireless-controller wlac -d sta online` command in the CLI.
949682	Intermittent traffic disruption observed in cw_acd caused by a rare error condition.
950379	The diagnostics of online FortiAPs shows *Link Down* in the trunk port *Connected Via* field when the FortiAP has an LACP connection to a FortiSwitch.
989929	A kernel interruption occurs on FWF-40F/60F models when WiFi stations connect to SSID on the local radio.
994752	A memory issue on the secondary firewall causes FortiGate to enter into conserve mode.
1001104	FortiAP units repeated joining and leaving FortiGate HA cluster when the secondary FortiGate has stored FortiAP images.
1001672	FortiWiFi reboots or becomes unresponsive when connecting to SSID after upgrading to 7.0.14.
1003070	On FortiGate, the sta count is not accurate when some wireless clients connect to APs managed by FortiGate.
1012433	Guest WiFi clients cannot be removed using RADIUS CoA after FortiGate reboots.
1017238	On the *WiFi & Switch Controller > SSIDs* page, new SSIDs cannot be created with captive portal enabled and a *Portal Type* of *Disclaimer Only* or *Email Collect*.
1018107	Unable to manage FortiAP from FortiGate.
1019680	FortiWiFi cannot access internal FAP consoles due to a login prompt issue in `diagnose sys modem com`.
1035621	Accounting messages are not sent to all accounting servers when `acct-all-servers` enabled.

ZTNA

Bug ID	Description
944772	FortiGate does not use data from FortiClient to send the VPN snapshot to EMS.
998172	When first connecting to the ZTNA server, the EMS websocket can become stuck and an error displays *ZTNA Access Denied - Policy restriction!*.
1008632	When visiting SaaS application web pages using ZTNA, web pages can stall or return an *ERR_CERT_COMMON_NAME_INVALID* error.
1012317	ZTNA intermittently does not match the firewall policy due to missing information in the policy.
1016265	An interruption occurs in the WAD when trying to access the ZTNA server due to map matchers not being present.
1018303	ZTNA does not allow tcp-forwarding SSH traffic to pass through.
1020084	Health check on the ZTNA realserver does not work as expected if a blackhole route is added to the realserver address.
1026930	An interruption occurs in the WAD process causing TCP connections to stop for ZTNA proxy policies.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
980300	FortiOS 7.6.0 is no longer vulnerable to the following CVE Reference: • CVE-2024-26015
997189	FortiOS 7.6.0 is no longer vulnerable to the following CVE Reference: • CVE-2025-47295
998718	FortiOS 7.6.0 is no longer vulnerable to the following CVE Reference: • CVE-2024-26010
998719	FortiOS 7.6.0 is no longer vulnerable to the following CVE Reference: • CVE-2024-26011
999253	FortiOS 7.6.0 is no longer vulnerable to the following CVE Reference: • CVE-2024-50565
1002468	FortiOS 7.6.0 is no longer vulnerable to the following CVE Reference: • CVE-2024-26013
1003801	FortiOS 7.6.0 is no longer vulnerable to the following CVE Reference:

Bug ID	CVE references
	• CVE-2024-36504
1020319	FortiOS 7.6.0 is no longer vulnerable to the following CVE Reference: • CVE-2024-32122
1029403	FortiOS 7.6.0 is no longer vulnerable to the following CVE Reference: • CVE-2024-35279
1052254	FortiOS 7.6.0 is no longer vulnerable to the following CVE Reference: • CVE-2024-48886
1071464	FortiOS 7.6.0 is no longer vulnerable to the following CVE Reference: • CVE-2024-45324

Known issues

Known issues are organized into the following categories:

- New known issues on page 78
- Existing known issues on page 85

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

New known issues

The following issues have been identified in version 7.6.0.

Application Control

Bug ID	Description
990540	FortiGate does not generate traffic logs for established or denied TCP sessions that lack application data.
1060562	The application control profile is missing on the GUI for FortiGate models with 2GB of memory. **Workaround**: Administrators can configure the application control profile using the CLI or using the GUI inline edit option on the policy list if the profile is already configured for the policy.

DNS Filter

Bug ID	Description
1058866	DNS translation does not work as expected when a resolved IP matches the external block list entry.

Endpoint Control

Bug ID	Description
1019658	On FortiGate, not all registered endpoint EMS tags are displayed in the GUI.
1038004	FortiGate may not display the correct user information for some FortiClient instances.

Firewall

Bug ID	Description
990528	When searching for an IP address on the *Firewall Policy* page, the search/filter functionality does not return the expected results.
1007029	On FortiGate, connections are disrupted between client email exchange servers and a virtual server when HTTP2 support is enabled.

FortiGate 6000 and 7000 platforms

Bug ID	Description
653335	SSL VPN user status does not display on the FortiManager GUI.
936320	When there is a heavy traffic load, there are no results displayed on any *FortiView* pages in the GUI.
950983	*Feature Visibility* options are visible in the GUI on a `mgmt-vdom`.
986845	On FortiOS, the *Security Fabric* widget does not display information on blade status.
998615	When doing a GUI-packet capture on FortiGate, the through-traffic packets are not captured.
1014826	SLBC does not function as expected with IPsec over TCP enabled.
1032573	In an HA configuration, FortiGate does not respond to SNMP queries causing the device to display as being DOWN.
1037965	When applying a script to a configuration, the updated configuration is applied to the FIM but is not fully synchronized on the FPCs.

FortiView

Bug ID	Description
1009287	On the *Dashboard > FortiView Sessions* page, closing a large number of FortiView sessions (+100) can take longer than expected and result in a CPU usage issue.
1034148	The *Application Bandwidth* widget on the *Dashboard > Status* page does not display some external applications bandwidth data.

GUI

Bug ID	Description
1009143	On FortiOS, the time displayed in the CLI and in the GUI do not match.
1018682	When creating a firewall policy, applications groups with custom application signatures cannot be saved using the GUI.
1047146	After a firmware upgrade, a VLAN interface used in IPsec, SSL VPN, or SD-WAN is not displayed on the interface list or the SD-WAN page and cannot be configured in the GUI.
1050865	When updating an administrator password in the GUI, the password expiration date does not update when the new password is created.

HA

Bug ID	Description
851743	When running the `diag sys ha checksum cluster` command, a previous line result is added further down in the output instead of new line result when a FortiGate is configured with several VDOMs .
965217	In an HA configuration, FortiGate may experience intermittent heartbeat loss causing unexpected failover to the secondary unit.
1055336	Using the *Test User Credentials* button from the Radius Server in the GUI does not honor the custom `nas-id-type`.
1070745	Sessions may not fail back to the original FGSP peer that owns the session if either the interface name for the `monitor-interface` or `pingsvr-monitor-interface` is 7 characters or longer.

Hyperscale

Bug ID	Description
1042011	On FortiGate, an login error message displays in the event log after completing an automation.
1042512	On FortiGate, the *CGN Resource Quota* field allows an invalid value to be set.
1093287	Using fixed-allocation IP Pools may cause NP7 NSS/PRP modules to become stuck, potentially disrupting traffic. Other PBA IP pools do not have this issue.

IPsec VPN

Bug ID	Description
735398	On FortiGate, the IKE anti-replay does not log duplicate ESP packets when SA is offloaded in the event log.
995912	After a firmware upgrade, some VPN tunnels experience intermittent signal disruptions causing traffic to be re-routed.
1020690	The *IPsec Aggregate* interface displays as DOWN on the *Network > Interfaces* and the *Policy & Objects > Firewall Policy* pages when the member including the Dialup VPN is actually UP. This is purely a GUI display issue and does affect system operation. The correct status is shown on the *VPN > IPsec Tunnels* page.
1031963	On the *Policy & Objects > Firewall Policy* page, the firewall `hit` and `bytes` counts display values of *0* in a policy-based VPN.
1042371	RADIUS authentication with EAP-TLS does not work as expected through IPsec tunnels.
1054953	If *IKEv2* is selected during the VPN FortiClient Remote Access wizard setup in the GUI, the Extensible Authentication Protocol (EAP) configuration cannot be selected using the GUI.

Log & Report

Bug ID	Description
611460	On FortiOS, the *Log & Report > Forward Traffic* page does not completely load the entire log when the log exceeds 200MB.
1034824	On the *Log & Report > Forward Traffic* page, application icons may not display in the *Application Name* column.
1044092	When filtering forward traffic logs using FortiAnalyzer as a source, data takes longer than expected to load and generates a memory error message.
1053334	The `appcat` log field is not included in the IoT signature logs.

Proxy

Bug ID	Description
1023054	After an upgrade on a 2GB FortiGate device, the firewall policy does not switch from *Proxy-based* to *Flow-based* in the *Inspection mode* field.
1042055	On FortiGate, an interruption occurs in the WAD process when in proxy-mode causing the unit to go into memory conserve mode.
1054052	The WAD process does not load a self-sign certificate when `set admin-server-cert self-sign` is configured in an explicit proxy.

REST API

Bug ID	Description
938349	Unsuccessful API user login attempts do not get reset within the time specified in `admin-lockout-threshold`.
993345	The router API does not include all ECMP routes for SD-WAN included in the `get router info routing-table` command.

Routing

Bug ID	Description
1029460	Creating a BGP IPv4 network prefix or neighbor in the GUI unintentionally creates an empty IPv6 network prefix.
1041812	In a hub and spoke HA configuration, *SD-WAN* pages take longer than expected to load in the GUI when there are a large number of spokes (~350) configured.
1042909	When creating a new static route on the *Network* > *Static Routes* page, the *Priority* field still displays when the *Destination* is switched from *Subnet* to *Internet Service*.

Security Fabric

Bug ID	Description
1007607	When creating a new IPv6 address, SDN connectors cannot be added for dynamic addresses.
1011833	FortiGate experiences a CPU usage issue in the `Node.js` daemon when there multiple administrator sessions running simultaneously.
1019284	When optimizing a security rating, resolving an alert for one rating causes another alert to appear for another rating and the alerts cycle between both ratings continuously.
1019844	In an HA configuration, when the primary FortiGate unit fails over to a downstream unit, the previous primary unit displays as being permanently disconnected.
1040058	The Security Rating topology and results does not display non-FortiGate devices.
1042972	On the *Security Fabric* > *Automation* page, users cannot test an automation stitch that uses the *Schedule* trigger from the GUI.
1054407	The Security Rating report does not show test results for downstream FortiGates when the *All FortiGates* view is selected. **Workaround**: Individual results can still be viewed for each downstream FortiGate by changing the FortiGate selection to the individual FortiGate.
1056262	With a FortiGate configured with a `root-vdom` and a `mgmt-vdom`, when an automation stitch is configured for a compromised host with IP-Ban action, the IP is banned from the `mgmt-vdom`.

Switch Controller

Bug ID	Description
1042390	On the *WiFi & Switch Controller* > *SSID* page, NAC policies using a Wildcard MAC Address cannot be saved using the GUI. **Workaround**: use the CLI to perform the operation.
1054445	When editing a dynamic port policy, saved changes are not shown in the GUI.

System

Bug ID	Description
947982	On NP7 platforms, DSW packets are missing resulting in VOIP experiencing performance issues during peak times.
952104	FortiGate experiences packet loss when using an internal hardware switch.
971466	FortiGateRugged 60 models may experience packet loss when directly connected to Cisco switch.
1003925	After deleting a redundant port on FortiGate, the port does not register as being available and generates an error.
1006685	FortiGate enters a loop cycle and generates a large number of LCAP packets when FortiGate does not receive LCAP packets from a peer device.
1008022	After a restarting FortiGate from the GUI, the `auto-nego` SFP port settings are not reflected in FortiGate.
1020602	After configuring a virtual wire pair (VWP) setting, it is not present in FortiGate after a reboot.
1022935	FortiGate experiences a CPU usage issue when `dedicated-management-cpu` is enabled.
1029353	The SNMP trap is not sent out when a virus is detected on the antivirus scanner.
1041726	Traffic flow speed is reduced or interrupted when the traffic shaper is enabled.
1047085	The FortiOS GUI is unresponsive due to a CPU usage issue with the `csfd` and `node` processes.
1049119	FortiGate encounters an interruption in the kernel due to a NULL pointer issue.
1051961	On FortiGate, IP addresses cannot be assigned within a configured IP range due to a DHCP server issue.
1055392	The traffic shaper does not take effect on the firewall policy when traffic is offloaded to NP7 due to a traffic management issue.
1056578	The DNS server does not operate as expected with `forward-only` mode enabled.
1065969	FortiGate does not boot up after restoring a configuration file containing an invalid string format.

Upgrade

Bug ID	Description
1043815	Upgrading the firmware for a large number (100+) of FortiSwitch or FortiAP devices at the same time may cause performance issues with the GUI and some devices may not upgrade. **Workaround**: pace out the upgrade schedule and upgrade devices in smaller batches.
1056126	FortiGate does not boot up properly after an upgrade when it has a large number (500+) of VDOMs configured.

User & Authentication

Bug ID	Description
1009884	FortiGate encounters a CPU usage issue in the `authd` process after a firmware upgrade.
1021719	On the *System > Certificates* page, the *Create Certificate* pane does not function as expected after creating a new certificate.
1044084	On the *Dashboard > Firewall User Monitor* page, the *Search* field does not display in the GUI when there are a large number (+1000) FSSO user logos.

VM

Bug ID	Description
1012927	When FortiGate returns an *ICMP TTL-EXCEEDED* message, the `geneve` option field header is missing.
1082197	The FortiGate-VM on VMware ESXi equipped with an Intel E810-XXV network interface card (NIC) using SFP28 transceivers at 25G speed is unable to pass VLAN traffic when DPDK is enabled.

Web Filter

Bug ID	Description
1040147	Options set in `ftgd-wf` cannot be undone for a web filter configuration.
1058007	Web filter custom replacement messages in group configurations cannot be edited in FortiGate.

WiFi Controller

Bug ID	Description
1028181	Wi-Fi devices would encounter service delay when roaming over captive-portal SSID with MAC-address authentication.

ZTNA

Bug ID	Description
1053309	An interruption occurs in the WAD when accessing ZTNA TCP-forwarding service through a proxy-policy with a SAML user group and `h2-support` is disabled on the `firewall vip`.

Existing known issues

The following issues have been identified in a previous version of FortiOS and remain in FortiOS 7.6.0.

Firewall

Bug ID	Description
959065	On the *Policy & Objects* > *Traffic Shaping* page, when deleting or creating a shaper, the counters for the other shapers are cleared.
994986	The *By Sequence* view in the Firewall policy list may incorrectly show a duplicate implicit deny policy in the middle of the list. This is purely a GUI display issue and does not impact policy operation. The *Interface Pair View* and *Sequence Grouping View* do not have this issue.
1007566	When the FortiGate has thousands of addresses and hundreds address groups, the GUI can take a few minutes to search for a specific address inside the address group dialog. **Workaround**: User can create the address group in the CLI instead by using the exact address name. User can also perform a search in the CLI using a partial match. For example: `config firewall addrgrp` `edit address_group` `set member <pattern>?` `next` `end`
1057080	On the *Firewall Policy* page, search results do not display in an expanded format.

FortiGate 6000 and 7000 platforms

Bug ID	Description
790464	After a failover, ARP entries are removed from all slots when an ARP query of single slot does not respond.
994241	On FortiGate 7000F using FGSP and FGCP, when TCP traffic takes an asymmetric path, the TCP ACK and data packets might be dropped in NP7.
997161	On FortiGate 6000 FPCs and FortiGate 7000 FPMs the node process may consume large amounts of CPU resources, possibly affecting FPC or FPM performance. (You can run the diagnose sys top command from an FPC or FPM CLI to view CPU usage.) This problem may be caused by security rating result submission. **Workaround**: Use the following commands to disable automatic security rating results submission and to disable running scheduled security ratings checks: `config system global` `set security-rating-result-submission disable` `set security-rating-run-on-schedule disable` `end` Once you have entered these commands, use the following command to restart the node process: `diagnose nodejs process restart`
1006759	After an HA failover, there is no IPsec route in the kernel. **Workaround**: Bring down and bring up the tunnel.
1056894	On the FortiGate 6000 platform, IPv6 VRF routing tables appear under the new and old FPC primary units when the primary FPC slot is changed.
1093412	For an FGSP configuration on the FortiGate 6000 and 7000 platforms, the `encryption` option of the `config system standalone-cluster` command does not encrypt session synchronization traffic. Enabling this option has no effect.

FortiView

Bug ID	Description
1009287	On the *Dashboard > FortiView Sessions* page, closing a large number of FortiView sessions (+100) can take longer than expected and result in a CPU usage issue.
1034148	The *Application Bandwidth* widget on the *Dashboard > Status* page does not display some external applications bandwidth data.

GUI

Bug ID	Description
853352	When viewing entries in slide-out window of the *Policy & Objects > Internet Service Database* page, users cannot scroll down to the end if there are over 100,000 entries.
885427	On the *Network > Interfaces* page, the SFP port is grayed out on the faceplate diagram even though the port is working. This is purely a GUI display issue and does not affect system operation. **Workaround**: View the SFP port information and status using the `interface list` in the CLI.

HA

Bug ID	Description
1054041	On FortiGate's in an HA environment, DHCP clients can not get an IPv4 address from the server with vcluster.

Intrusion Prevention

Bug ID	Description
1117043	After upgrade, event log shows `logdesc="IPSA driver update failed" msg="Fail to update IPSA driver status!"`. This issue only affects physical FortiGate models with the following IPS engine versions: • IPS Engine version: 7.550 - 7.567 • IPS Engine version: 7.1019 - 7.1039 To determine the IPS Engine versions, use the command: `get sys fortiguard-service status | grep 'IPS/FlowAV Engine'` **Workaround**: Power off the FortiGate. Wait 30 seconds, and then power on the FortiGate. **Note**: Reboot using the CLI is not an effective workaround and requires additional steps. After executing `exec shutdown`, unplug the power to the FortiGate. Wait one minute, and the power on the FortiGate.

IPsec VPN

Bug ID	Description
944600	CPU usage issues occurred when IPsec VPN traffic was received on the VLAN interface of an NP7 vlink.
1012615	After upgrade to 7.4.3, IPsec VPN is dropping traffic.

Log & Report

Bug ID	Description
1001583	On the *Log & Report* > *Forward Traffic* page, the GUI experiences a performance issue and reverts the last input when multiple ports are added to a filter for destination ports.
1045253	Log items cannot be created and sent to FortiGate Cloud log server when confirm queue becomes full.

Proxy

Bug ID	Description
1035490	The firewall policy works with proxy-based inspection mode on FortiGate models with 2GB RAM after an upgrade. *Workaround*: After an upgrade, reboot the FortiGate.
1060812	Botnet detection fails in transparent proxy setups caused by implementation error.

Routing

Bug ID	Description
1003756	When creating a rule on the *Network* > *Routing Objects* page, the *Prefix-list* is set to *0.0.0.0 0.0.0.0* when an incorrect format is entered in the *Prefix* field.

Security Fabric

Bug ID	Description
903922	Physical and logical topology is slow to load when there are a lot of managed FortiAP devices (over 50). This issue does not impact FortiAP management and operation.
1057862	FortiGate models with 2GB of memory that manage many extension devices (FortiSwitches and FortiAPs) may enter conserve mode due to the GUI process experiencing a memory usage issue over time. **Workaround**: Avoid loading *Security Fabric* widget, *Security Rating*, and *Topology* pages.

Switch Controller

Bug ID	Description
961142	An interface in FortiLink is flapping with an MCLAG FortiSwitch using DAC on an OPSFPP-T-05-PAB transceiver.

System

Bug ID	Description
901621	On the NP7 platform, setting the interface configuration using set inbandwidth <x> or set outbandwidth <x> commands stops traffic flow. **Workaround**: Change the NP7 `default-qos-type` setting from `shaping` to `policing`. This requires a restart of the device for the configuration to take effect: `config system npu` `  set default-qos-type policing` `end`
1020921	When configuring an SNMP trusted host that matches the management *Admin* trusted host subnet, the GUI may give an incorrect warning that the current SNMP trusted host does not match. This is purely a GUI display issue and does not impact the actual SNMP traffic. **Workaround**: If the trusted host is enabled on all administrative access, make sure the SNMP host IP is included in at least one of these trusted IP/subnets.
1046484	After shutting down FortiGate using the `execute shutdown` command, the system automatically boots up again.
1048496	On FortiGate, the `snmp` daemon does not work as expected resulting in the SNMP queries timing out.
1058256	On FortiGate, interfaces with DAC cables remain down after upgrading to version 7.4.4.

Bug ID	Description
1058397	On FortiGate 900 models, when the baudrate is configured, the changes are not applied and is set to 9600.
1069208	If the DHCP offer contains padding when DHCP relay is used, the DHCP relay deletes the padding before relaying the packet.

VM

Bug ID	Description
1073016	The OCI SDN connector cannot call the API to the Oracle service when an IAM role is enabled.
1082197	VLAN traffic fails to pass through E810-XXV NIC with SFP28 transceiver and 25G speed after enabling DPDK.
1094274	FortiOS becomes unresponsive when sending IPv6 traffic over MLX5 network adapters due to incorrect WQE handling.
1146370	AWS bootstrap is unable to parse IAM role profile properly due to the length.

Built-in AV Engine

AV Engine 7.00030 is released as the built-in AV Engine. Refer to the AV Engine Release Notes for information.

Built-in IPS Engine

IPS Engine 7.001014 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