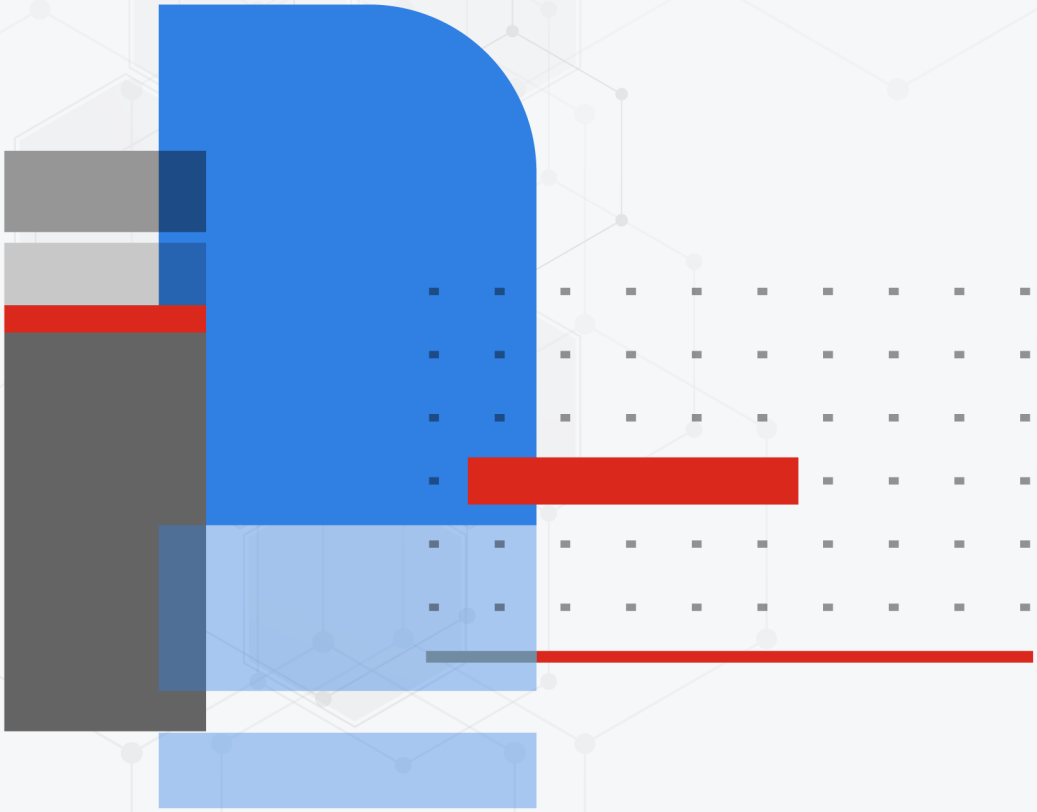
Release Notes

FortiOS 7.4.2



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

January 22, 2024
FortiOS 7.4.2 Release Notes
01-742-951009-20240122

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-12-20	Initial release.
2023-12-21	Updated New features or enhancements on page 15, Known issues on page 55, and Built-in IPS Engine on page 63.
2023-12-27	Updated Resolved issues on page 36, Known issues on page 55, and Built-in IPS Engine on page 63.
2024-01-02	Updated Resolved issues on page 36 and Known issues on page 55.
2024-01-03	Added Remote access with write rights through FortiGate Cloud on page 11 to the Special Notices.
2024-01-09	Updated New features or enhancements on page 15, Resolved issues on page 36, and Known issues on page 55.
2024-01-22	Updated Known issues on page 55.

Introduction and supported models

This guide provides release information for FortiOS 7.4.2 build 2571.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.4.2 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-70F, FG-71F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100F, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-400F, FG-401F, FG-500E, FG-501E, FG-600E, FG-601E, FG-600F, FG-601F, FG-800D, FG-900D, FG-900G, FG-901G, FG-1000D, FG-1000F, FG-1001F, FG-1100E, FG-1101E, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3000F, FG-3001F, FG-3100D, FG-3200D, FG-3200F, FG-3201F, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3700F, FG-3701F, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-4800F, FG-4801F, FG-5001E, FG-5001E1, FG-6000F, FG-7000E, FG-7000F
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-60F, FGR-60F-3G4G, FGR-70F, FGR-70F-3G4G
FortiFirewall	FFW-1801F, FFW-2600F, FFW-3980E, FFW-4200F, FFW-4400F, FFW-4401F, FFW-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 7.4.2 supports the following FG-6000F, FG-7000E, and FG-7000F models:

FG-6000F	FG-6300F, FG-6301F, FG-6500F, FG-6501F
FG-7000E	FG-7030E, FG-7040E, FG-7060E
FG-7000F	FG-7081F, FG-7121F

Special notices

Hyperscale incompatibilities and limitations

See Hyperscale firewall incompatibilities and limitations in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 7.4.2 features.

FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 7.4.2 features.

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

Remove OCVPN support

The IPsec-based OCVPN service has been discontinued and licenses for it can no longer be purchased as of FortiOS 7.4.0. GUI, CLI, and license verification support for OCVPN has been removed from FortiOS. Upon upgrade, all IPsec phase 1 and phase 2 configurations, firewall policies, and routing configuration previously generated by the OCVPN service will remain. Alternative solutions for OCVPN are the Fabric Overlay Orchestrator in FortiOS 7.2.4 and later, and the SD-WAN overlay templates in FortiManager 7.2.0 and later.

Remove WTP profiles for older FortiAP models

Support for WTP profiles has been removed for FortiAP B, C, and D series models, and FortiAP-S models in FortiOS 7.4.0 and later. These models can no longer be managed or configured by the FortiGate wireless controller. When one of these models tries to discover the FortiGate, the FortiGate's event log includes a message that the FortiGate's wireless controller `can not be managed because it is not supported`.

IP pools and VIPs are now considered local addresses

In FortiOS 7.4.1 and later, all IP addresses used as IP pools and VIPs are now considered local IP addresses if responding to ARP requests on these external IP addresses is enabled (`set arp-reply enable`, by default). For these cases, the FortiGate is considered a destination for those IP addresses and can receive reply traffic at the application layer.

Previously in FortiOS 7.4.0, this was not the case. For details on the history of the behavior changes for IP pools and VIPs, and for issues and their workarounds for the affected FortiOS versions, see Technical Tip: IP pool and virtual IP behavior changes in FortiOS 6.4, 7.0, 7.2, and 7.4.

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

In FortiOS 7.4.0 and later, users should use the built-in Fortinet_GUI_Server certificate or SHA-256 and higher certificates for the web management interface. For example:

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

Number of configurable DDNS entries

Starting in FortiOS 7.4.0, the number of DDNS entries that can be configured is restricted by table size. The limits are 16, 32, and 64 entries for lentry-level, mid-range, and high-end FortiGate models respectively.

After upgrading to FortiOS 7.4.0 or later, any already configured DDNS entries that exceed the limit for the FortiGate model in use will be deleted. For example, if a user has 20 DDNS entries before upgrading to 7.4.0 and is using a entry-level FortiGate model, the last four DDNS entries will be deleted after upgrading.

In such instances where the number of DDNS entries exceeds the supported limit for the FortiGate model in use, users have the option to upgrade their FortiGate model to one that supports a higher number of DDNS entries.

FortiGate models with 2 GB RAM can be a Security Fabric root

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

As part of improvements to reducing memory usage on FortiGate models with 2 GB RAM, FortiOS 7.4.2 and later can authorize up to five devices when serving as a Fabric root.

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

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).

Admin and super_admin administrators cannot log in after a prof_admin VDOM administrator restores the VDOM configuration and reboots the FortiGate

When a VDOM administrator using the prof_admin profile is used to restore a VDOM configuration and then reboot the FortiGate, an administrator using the super_admin profile (including the default admin administrator) cannot log in to the FortiGate.

Therefore, in FortiOS 7.4.1, a prof_admin VDOM administrator should not be used to restore a VDOM configuration (FortiOS 7.4.2 and later are not affected).

Workarounds:

1. If a prof_admin VDOM administrator has already been used to restore a VDOM configuration, then **do not reboot**. Instead, log in using a super_admin administrator (such as default admin), back up the full configuration, and restore the full configuration. After the full configuration restore and reboot, super_admin administrators will continue to have the ability to log into the FortiGate.

   After this workaround is done, the FortiGate is **still susceptible to the issue** if the backup and restore is performed again by the prof_admin VDOM administrator. A FortiOS firmware upgrade with this issue resolved will be required to fully resolve this issue.

2. To recover super_admin access after having restored a VDOM configuration and performing a FortiGate reboot, power off the device and boot up the FortiGate from the backup partition using console access.

SMB drive mapping with ZTNA access proxy

In FortiOS 7.4.1 and later, SMB drive mapping on a Windows PC made through a ZTNA access proxy becomes inaccessible after the PC reboots when access proxy with TCP forwarding is configured as FQDN. When configured with an IP for SMB traffic, same issue is not observed.

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

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

Remote access with write rights through FortiGate Cloud

Remote access with read and write rights through FortiGate Cloud now requires a paid FortiGate Cloud subscription. The FortiGate can still be accessed in a read-only state with the free tier of FortiGate Cloud. See the FortiGate Cloud feature comparison for more details: https://docs.fortinet.com/document/fortigate-cloud/23.4.0/administration-guide/215425/feature-comparison.

CLI system permissions

Starting in FortiOS 7.4.2, the usage of CLI diagnostic commands (`cli-diagnose`), previously named `system-diagnostics`, is disabled by default, with the exception of super_admin profile users. Users can now exercise more granular control over the CLI commands. See CLI system permissions for more information.

When the user upgrades to FortiOS 7.4.2 or later, the following settings for CLI options will be applied, irrespective of whether `system-diagnostics` was enabled or disabled in FortiOS 7.4.1 or earlier.

CLI option	Status
`cli-diagnose`	Disabled
`cli-get`	Enabled
`cli-show`	Enabled
`cli-exec`	Enabled
`cli-config`	Enabled

To enable permission to run CLI diagnostic commands after upgrading:

```
config system accprofile
    edit <name>
        set cli-diagnose enable
    next
end
```

Many diagnostic commands have privileged access. As a result, using them could unintentionally grant unexpected access or cause serious problems, so understanding the risks involved is crucial.

Changes in GUI behavior

Bug ID	Description
907058	Improve the visibility of OT vulnerabilities and virtual patching signatures: • Add a *Security Profiles* > *Virtual Patching Signatures* page that displays all OT virtual patching signatures. • In the *Assets* widget (*Dashboard* > *Assets & Identities*), display a tooltip for detected IoT and OT vulnerabilities when hovering over the *Vulnerabilities* column. • Add the *View IoT/OT Vulnerabilities* option per device to drill down and list the IoT and OT vulnerabilities. • Display the OT Security Service entitlement status and OT package versions in the right-side gutter of a virtual patching profile page.
915481	Optimize the *Policy & Objects* pages for loading large datasets. For example, instead of loading an entire dataset of address objects on the *Addresses* page or within the address object dialog inside a firewall policy, data is lazily-loaded. Different types of address objects are loaded separately. Enhancements include: • Add a tabbed design for firewall object list pages. • Lazily- load the firewall address list and introduce sub-tabs for each type of address object. • Update the *Address* dialog page. • Update the *Policy* dialogs and use new address dialogs with a lazy-load selection widget.
954319	On the *Policy & Objects* > *Firewall Policy*, *Proxy Policy*, and *ZTNA* pages, *ZTNA Tag* references are renamed *Security Posture Tag*.
955294	To reduce the number of clicks to configure a ZTNA server object, the settings to create a new *Server/service mapping* are condensed. Real server mappings can be configured directly in the *Service/Server Mapping* pane. To display additional real servers or load balancing options in the GUI, create a second real server first in the CLI.

Changes in default behavior

Bug ID	Description
938115	Enhance the QUIC option by introducing a tri-state selection: bypass, block, or inspect. The default setting for QUIC is inspect. This enhancement provides more granular control over QUIC traffic. `config firewall ssl-ssh-profile` `  edit <name>` `  config https` `  set quic {inspect | bypass | block}` `  end` `  config dot` `  set quic {inspect | bypass | block}` `  end` `  next` `end`
959084	On FortiGate VMs that are using the FortiFlex license, once the expiration date is reached, an automatic three-day grace period offered by FortiGuard will start. Afterwards, the VM license will become expired, and all firewall functions stop working.

Changes in table size

Bug ID	Description
823373	Increase the number of VRFs per VDOM from 64 to 252.
938320	Adjust the number of firewall policies from 5000 to 2000 on FortiGate models with 2 GB RAM (40F, 60E, and 60F series devices) to improve memory usage.
945604	On FortiGate 4K models and larger, increase the table size for the system.zone VDOM limit from 500 to 1000.

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
737947	When configuring a FortiGate VM as a network virtual appliance (NVA) as part of the Azure vWAN solution, the FortiGate can make API calls and send health metrics to Azure for integration with Azure Monitor.
839076	Add GUI support for configuring various AWS resource addresses using an AWS SDN connector.
952335	Add GUI support to apply a FortiFlex token on the *FortiGate VM License* page. • For newly deployed or expired VM instances: when the license pop-up appears. • For already licensed VM instances: from the *Virtual Machine* dashboard widget or the *System* > *FortiGuard* page.

FortiGate 6000 and 7000 platforms

Feature ID	Description
814242	The FortiGate 7000F platform supports setting a custom load balancing method for an individual VDOM. All of the traffic destined for that VDOM will be distributed to FPMs by the NP7 load balancers according to the following setting: `config system settings` `set dp-load-distribution-method {derived | to-primary | src-ip | dst-ip | src-dst-ip | src-ip-sport | dst-ip-dport | src-dst-ip-sport-dport}` `end` The default load balancing method, `derived`, means traffic for that VDOM uses the global load balancing method set by the `dp-load-distribution-method` option of the global `config load-balance` setting command.

GUI

See GUI in the New Features Guide for more information.

Feature ID	Description
926533	The FortiOS GUI indicates when users are running the STS (Special Technical Support) build (formerly known as TOP3). It is more apparent that the user is using this specific build, and the associated risks are highlighted after users log in.

Hyperscale

Feature ID	Description
875141	Support the transmission of logs using TCP. This is a significant improvement from the previous version, which only supported UDP. TCP provides a more reliable connection, ensuring no logs are lost during transmission. This is beneficial for carrier customers who require a robust and dependable logging system.
920148	IPv4 or IPv6 IP address threat feeds can be added to hyperscale firewall policies as source or destination addresses.
921750	Support NetFlow version 9 for session logging in hyperscale VDOMs. By integrating NetFlow version 9 for session logging, the hyperscale software offers users a more comprehensive and precise view of network traffic data. This leads to enhanced network monitoring, troubleshooting, and planning capabilities.
968801	Add `enforce-seq-order` hyperscale hardware logging option to enable or disable sending hyperscale VDOM software session logs in order by sequence number.

LAN Edge

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

Feature ID	Description
834550	Introduce FortiSwitch management using the HTTPS protocol. This new capability supports all the same FortiLink features, offering users a simpler alternative to the more complex CAPWAP protocol.
866172	The local radio of FortiWiFi 8xF, 6xF, and 40F models when operating in client mode and connecting with a third-party SSID can be configured in the GUI to use either *WPA3 SAE* or *Opportunistic Wireless Encryption (OWE)* security mode.
866174	When a specific Fortinet external antenna is installed, the FortiAP profiles of FAP-432F, FAP-433F, FAP-U432F, and FAP-U433F models can be configured using the `optional-antenna` setting by choosing from a list of supported Fortinet external antenna models. For example, for the FAP-433F: `config wireless-controller wtp-profile` `edit "FAP433F"` `config radio-1`

Feature ID	Description
	`set optional-antenna {none | FANT-04ABGN-0606-O-R | FANT-04ABGN-0606-P-R}` `end` `next` `end` This setting can be configured in the GUI for supported FortiAP profile in the *Radio* section. Enable *External antenna* and select the external antenna model from the list of defined values. This setting allows antenna gains that are specific to the Fortinet external antenna model and the Wi-Fi band (2.4 GHz or 5 GHz) being used to be taken into consideration by the FortiGate wireless controller to set transmit power properly for a managed FortiAP device.
933260	Support RADIUS accounting interim updates on roaming for WPA-Enterprise security. The enhancement is specifically designed to resolve compatibility issues with Cisco's Identity Services Engine (ISE) session stitching feature with improved interoperability between devices and networks, leading to a more seamless and secure wireless connectivity experience. This is beneficial for organizations that rely on Cisco ISE for network access control, as it ensures their security protocols align with industry standards. `config wireless-controller vap` `edit <name>` `set security wpa2-only-enterprise` `set roaming-acct-interim-update {enable | disable}` `next` `end`
939229	Support the Hunting-and-Pecking (HnP) Only authentication method for WPA3-SAE SSIDs. This setting is disabled by default. `config wireless-controller vap` `edit <name>` `set ssid <name>` `set security wpa3-sae` `set pmf enable` `set sae-hnp-only {enable | disable}` `next` `end`
940562	When a third-party external antenna is installed, the FortiAP profiles of selected models can be configured with `set optional-antenna custom` and `set optional-antenna-gain <integer>` (in dBi, 0 - 20, default = 0). Supported FortiAP models include: FAP-432F, FAP-432FR, FAP-433F, FAP-233G, FAP-432G, FAP-433G, FAP-U432F, and FAP-U433F. For example: `config wireless-controller wtp-profile` `edit "FP433G"` `config platform` `set type 433G` `end`

Feature ID	Description
	`` config radio-2 set optional-antenna custom set optional-antenna-gain "10" end next end ``` These settings can be configured in the GUI for supported FortiAP profile in the *Radio* section. Enable *External antenna*, select *Custom* from the dropdown, and enter a value for *External antenna gain (dB)*.
940905	Support WPA3 options when the radio mode is set to Fortinet's SAM (Service Assurance Manager). This includes WPA3-SAE and WPA3 OWE. In also includes support for WPA2/WPA3-Enterprise with certificate authentication, encompassing both PEAP and EAP-TLS. ``` config wireless-controller wtp-profile edit <name> config radio-1 set mode sam set sam-ssid <string> set sam-security-type {wpa-enterprise |wpa3-sae | owe} end next end ```
960883	Support individual control of the 802.11k and 802.11v protocols. In previous FortiOS versions, these protocols were jointly controlled with the `voice-enterprise` option. ``` config wireless-controller vap edit <name> set 80211k {enable | disable} set 80211v {enable | disable} next end ```
962880	Simplify the Bonjour profile provisioning and failover mechanism. • Users can set the Bonjour profile in the WTP configuration and WTP profile. ``` config wireless-controller wtp-profile edit <name> set bonjour-profile <name> next end ``` • To ensure uninterrupted service, introduce a new election procedure among the APs. This provides a failover mechanism or redundancy if the Bonjour gateway goes down.
962881	Support hitless rolling AP upgrades. This feature smartly upgrades APs by not upgrading all APs at once. It queues some APs and considers the reachability of neighboring APs and their locations. This prevents service drops during simultaneous upgrades, ensuring uninterrupted WiFi service.

Feature ID	Description
963851	Enhance CAPWAP management over NAT to provide a stability boost for Fortinet APs that operate behind a NAT device. This allows users to set the frequency of keep-alive messages, thereby improving connectivity. `config wireless-controller timers` `  set nat-session-keep-alive <integer>` `end`
967663	Support the generation of a private key, a crucial component for SAE-PK authentication. This enhancement is significant as it offers an integrated mechanism for key generation, eliminating the need for third-party tools. This makes the FortiGate a more self-sufficient and secure system for SAE-PK authentication. `# execute wireless-controller create-sae-pk`
969387	Support the automated reboot functionality for APs. This automatically reboots an AP stuck in a discovery loop, a state that disrupts network service. This smart feature reduces network downtime, and eliminates the need for manual intervention, thus saving time and resources. It ensures a resilient and seamless network experience. `config wireless-controller timers` `  set ap-reboot-wait-interval <integer>` `  set ap-reboot-wait-time <hh:mm>` `  set ap-reboot-wait-interval2 <integer>` `end`

Log & Report

See Logging in the New Features Guide for more information.

Feature ID	Description
975411	Modify the log fields for long-lived sessions by adding three new log fields to the long-lived session log: duration delta (`durationdelta`), sent packet delta (`sentpktdelta`), and received packet delta (`rcvdpktdelta`). The fields enhance the granularity and accuracy of session logs, providing a more detailed view of long-lived sessions. This aids in troubleshooting and analysis.

Network

See Network in the New Features Guide for more information.

Feature ID	Description
685910	Add SoC4 driver support for the IEEE 802.1ad, which is also known as QinQ. When the OID is used up, it is forbidden to create a new QinQ interface.
881823	BGP now incorporates the advanced security measures of the TCP Authentication Option (TCP-AO). This integration bolsters the security of BGP connections and enhances the reliability of these connections, thereby contributing to the overall security of the internet. • Add `cmac-aes128` option in the `router key-chain` settings: `config router key-chain` `edit <name>` `config key` `edit <id>` `set algorithm cmac-aes128` `next` `end` `next` `end` • Add `auth-options` for BGP `neighbor` and `neighbor-group` settings: `config router bgp` `config neighbor` `edit <ip>` `set auth-options <key-chain>` `end` `next` `config neighbor-group` `edit <name>` `set auth-options <key-chain>` `end` `next` `end` • Add debug command for `tcp-auth-options`: `# diagnose sys tcp-auth-options`
890574	Support port mirroring with NP7 offloaded traffic. Offloaded packets are copied to a mirroring port, which can be linked to an external device for in-depth analytics.
921795	Simplify the configuration of the FortiGate LAN extension feature by automatically configuring a VDOM link between a traffic VDOM, by default, the root VDOM and the LAN extension VDOM. After connecting to the FortiGate Controller, the following settings are automatically configured on the FortiGate Connector: • VDOM link interface in the LAN extension VDOM is a part of the LAN extension software switch • VDOM link interface in the traffic VDOM is dynamically assigned an IP address, which has been obtained from the FortiGate Controller This feature is required to support the FortiGate Secure Edge use case for FortiSASE.

Feature ID	Description
925668	FortiOS can be configured with a maximum of three sFlow collectors. This also applies to multi-VDOM environments where a maximum of three sFlow collectors can be used globally and/or on a per-VDOMs basis. This feature enables up to a maximum of three unique parallel sFlow streams or transmissions per sFlow sample to three different sFlow collectors. The sFlow collector configuration can only be configured in the CLI.
934273	Support the BGP graceful restart helper-only mode. This ensures that during a FortiGate HA failover, the neighboring router that only supports BGP graceful restart helper mode retains its routes.
941347	Enhance FortiOS packet capture. If the browser is closed or refreshed, users can return at a later time to view, stop, restart, or download the capture. The number of captures that can be stored on FortiGate is determined by the device's capabilities. REST APIs have been introduced for starting, stopping, deleting, and downloading packet captures.

Policy & Objects

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

Feature ID	Description
875309	Add GUI support for port block allocation (PBA) IP pools for NAT64 traffic.
886571	Support IPS inspection for multicast UDP traffic.
941072	The handling of virtual patch local-in traffic is optimized by identifying the type of traffic early based on its port number and protocol. The IPS engine will tag the local-in sessions for services, including SSL VPN and web GUI. If a tagged session does not have any vulnerability signatures for the FortiOS version, then IPS will bypass scanning the session. This optimizes performance by only scanning and dropping the sessions that are exploiting a vulnerability.

SD-WAN

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

Feature ID	Description
884084	Update SD-WAN with ADVPN to version 2.0 with major changes to ADVPN design and operation, namely, introducing edge discovery and path management for ADVPN spokes. ADVPN 2.0 incorporates intelligence into the spokes to ensure shortcut tunnels, known as shortcuts, are established using underlays available on both spokes and chosen based on matching certain link health criteria.

Feature ID	Description
	ADVPN 2.0 provides a more flexible SD-WAN solution than the original ADVPN to achieve resiliency against underlay outages or degraded underlay performance that is no longer dependent on specific BGP routing designs or mechanisms.
900197	Add IPv6 support for SD-WAN segmentation over a single overlay. This allows seamless communication between IPv6 devices within virtual routing and forwarding (VRF) overlay networks, benefiting organizations transitioning to IPv6 or operating in a dual-stack environment.
936294	Enhance the SD-WAN hub and spoke speed test feature as follows: • Allow the speed test server to be deployed on the hub. Speed tests can be initiated from the spokes in cases when a spoke is behind NAT. • Support uploading and downloading tests. • Support TCP and UDP. • Allow users to apply an egress shaping profile (`update-shaper`) to an IPsec tunnel (`none`, `local`, `remote`, or `both`). • Support configuring custom speed test ports.

Security Fabric

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

Feature ID	Description
815483	FOS now supports configurable Purdue levels for Fortinet Fabric devices, specifically: FortiGate, managed FortiSwitch, and FortiAP. This means that users have the flexibility to adjust the Purdue levels of these devices according to their specific needs and preferences, enhancing the adaptability and functionality of their Fabric devices.

Security Profiles

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

Feature ID	Description
744954	Support Punycode encoding in the `url` and `hostname` fields in flow mode web filter UTM logs. This caters to domain names containing non-ASCII characters, such as internationalized domain names (IDNs). Is also aligns the functionality of flow and proxy modes, offering a more unified and improved user experience. `config webfilter profile` `edit <name>` `set web-flow-log-encoding {utf-8 | punycode}`

Feature ID	Description
	next end
848844	Diameter protocol inspection is supported on the FortiGate. Key features include: • Diameter-based packet forwarding and routing: the FortiGate can forward and route Diameter packets that match a firewall policy with an enabled `diameter-filter profile`. • Packet sanity checking: this feature checks if the packet passing through the FortiGate conforms to the Diameter protocol standards as defined in RFC 3588. • Logging: for network auditing purposes, the traffic for both dropped and forwarded Diameter-based packets can be logged. This is crucial for interfaces used to exchange information with roaming partners over the IPX network.
888411	Enhance customization and control in the video filter profile with two keyword-based filters for video titles and descriptions that offer AND'/'OR logic options. Users can prioritize configured filters, and manage all categories and channels that match the filters using the *Any* option.
959763	The inline IPS feature allows HTTP/HTTPS traffic to be processed directly in WAD for application control and IPS UTM features, reducing reliance on the IPS Engine. The IPS Engine is still required for non-HTTP protocols. This feature is automatically enabled for new devices, but is not enabled if upgrading from FortiOS 7.4.1 or earlier. `config ips settings` `set proxy-inline-ips {enable | disable}` `end`

System

See System in the New Features Guide for more information.

Feature ID	Description
480717	Add `config system dedicated-mgmt` to all FortiGate models with mgmt, mgmt1, and mgmt2 ports.
739200	Add GUI support to prevent FortiGates with an expired support contract from upgrading to a major or minor firmware release.
946205	Enhance IPv6 VRRP to manage and control the VRRP states. Previously, the VRRP states would continue to be primary as long as the IPv6 VRRP destination could be reached by any route, including the default route. `config system interface` `edit <name>` `config ipv6` `config vrrp6` `edit <id>`

Feature ID	Description
	set ignore-default-route {enable | disable} next end end next end
954639	Support SNMP traps for monitoring the free and freeable memory usage on FortiGates. config system snmp sysinfo set trap-free-memory-threshold <integer> set trap-freeable-memory-threshold <integer> end
964697	Support the SNMP trap when power is restored to the power supply unit (PSU) in a FortiGate. When the PSU regains power after an outage, an SNMP trap should be triggered. This enhances the monitoring capabilities of the FortiGate.

VPN

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

Feature ID	Description
780297	Rename the `mdst-addr6` IKE debug filter option to `mrem-addr6`.
879452	Add the ability to rename their IPsec tunnels. Once a tunnel name is changed, all references to that tunnel, such as routing and policies, are automatically updated to reflect the new name. This ensures consistency and saves users the trouble of manually updating each reference. config vpn ipsec phase1-interface rename <string> to <string> end
887173	IPsec tunnels between HA members use manual keys to encrypt and authenticate, which may not be sufficient for some internal security policies. The IKE daemon has been updated to use auto-negotiation for the IPsec tunnel key, and to establish and maintain the tunnel. config system ha set ipsec-phase2-proposal <option> end
905804	Support IPsec key retrieval with a quantum key distribution (QKD) system using the ETSI standardized API. This eliminates negotiation, simplifies the process, and enhances efficiency in IPsec key management.

Feature ID	Description
923120	Introduce a proprietary solution to support the encapsulation of Encapsulating Security Payload (ESP) packets within Transmission Control Protocol (TCP) headers. This allows ESP packets to be assigned a port number, which enables them to traverse over carrier networks where direct IPsec traffic is blocked or impeded by carrier-grade NAT. The TCP port for IKE/IPsec traffic is configured in the global settings: `config system settings` `  set ike-tcp-port <integer>` `end` The phase 1 interface settings include options for ESP encapsulation: `config vpn ipsec phase1-interface` `  edit <name>` `  set ike-version 2` `  set transport {udp | udp-fallback-tcp | tcp}` `  set fortinet-esp {enable | disable}` `  set fallback-tcp-threshold <integer>` `  next` `end`

ZTNA

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

Feature ID	Description
865016	Introduce Fabric integration between the FortiGate and FortiGSLB, which allows a FortiGate to publish custom host and domain names directly to FortiGSLB. This enables external IPs on VIPs used in ZTNA server objects to be published with the host and domain names directly to FortiGSLB, where its DNS service can provide nameserver lookups for the FQDNs.
897240	The *Any*/*All* GUI selector for ZTNA tags is added back to the simple and full ZTNA policy configuration page. The setting is defaulted to *Any*.

Upgrade information

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

To view supported upgrade path information:

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

Fortinet Security Fabric upgrade

FortiOS 7.4.2 greatly increases the interoperability between other Fortinet products. This includes:

FortiAnalyzer	• 7.4.2
FortiManager	• 7.4.2
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 7.4.0, use FortiClient 7.4.0.

Upgrade the firmware of each device in the following order. This maintains network connectivity without the need to use manual steps.

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

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.4.2. When Security Fabric is enabled in FortiOS 7.4.2, all FortiGate devices must be running FortiOS 7.4.2.

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 7.4.2:

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

IPS-based and voipd-based VoIP profiles

In FortiOS 7.4.0 and later, the new IPS-based VoIP profile allows flow-based SIP to complement SIP ALG while working together. There are now two types of VoIP profiles that can be configured:

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

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

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

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

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

Where:

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

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

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

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

Product integration and support

The following table lists FortiOS 7.4.2 product integration and support information:

Web browsers	• Microsoft Edge 112 • Mozilla Firefox version 113 • Google Chrome version 113 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 112 • Mozilla Firefox version 113 • Google Chrome version 113 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 0313 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	• 7.00021
IPS Engine	• 7.00524

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 8.4 • SUSE Linux Enterprise Server 12 SP3 release 12.3
Microsoft Windows Server	• Windows Server 2019
Windows Hyper-V Server	• Microsoft Hyper-V Server 2019
Open source XenServer	• Version 3.4.3 • Version 4.1 and later
VMware ESXi	• Versions 6.5, 6.7, 7.0, and 8.0.

Language support

The following table lists language support information.

Language support

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

SSL VPN support

SSL VPN web mode

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

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 113 Google Chrome version 112
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 113 Google Chrome version 112
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 113 Google Chrome version 112
macOS Ventura 13.1	Apple Safari version 16 Mozilla Firefox version 103 Google Chrome version 111
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
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

FortiExtender model	Modem firmware image name	Modem firmware file on Support site	Geographical region
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
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

FortiExtender model	Modem firmware image name	Modem firmware file on Support site	Geographical region
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 7.4.2. To inquire about a particular bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
827497	Unsupported file samples are submitted to FortiSandbox for analytics.
845954	Flow AV does not have a limit of how much memory it can use when buffering files for scanning.
911872	When connecting to FortiGate Cloud Sandbox, the connection status takes a long time to update and shows as unreachable.
921175	Make improvements to the AV engine when handling outbreak prevention queries.
948182	FortiSandbox side panel statistics only shows only statistics for root/management VDOM.
948371	Scanunit should no longer submit known infected files to FortiSandbox.
961077	*Advanced Threat Protection Statistics* dashboard is not increasing counters (AV).
962261	*Send Files to FortiSandbox for Inspection* AV profile setting does not work as expected.

Application Control

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

Data Leak Prevention

Bug ID	Description
911830	DLP file type "AND" sensor cannot block the file when it is a DOCX file.

Bug ID	Description
922311	DLP sensor cannot block MS-Office XML files, but can block MS-Office files when setting the profile type as message.
926592	Outlook cannot connect to the Exchange server once the DLP profile protocol is set to MAPI.

Explicit Proxy

Bug ID	Description
782713	Value overflow in destination interface of WAD traffic log.
926178	Post-upgrade, explicit proxy policies may mismatch when an HTTP CONNECT request or TLS SNI of a HTTPS session partially matches to a policy with deep inspection enabled.
942612	Web proxy forward server does not convert HTTP version to the original version when sending them back to the client.

Firewall

Bug ID	Description
665662	Using the append command to add entries to a policy object that mixes the use of wildcard and regular entries can result in an error to the policy during reboot. This applies to interface, address, and service policy objects.
786317	The `service` field in the traffic log shows the configured custom service name, even for traffic that does not match the FQDN configured in the custom service.
865137	After enabling the `ssl-http-location-conversion` option in the virtual server, it does not take effect.
875309	Support port block allocation (PBA) IP pools for NAT64 traffic.
921658	SD-WAN IPsec egress traffic shaping is not working when traffic offloading is enabled on an NP7 unit.
924588	Unable to access a real server using VIP with a custom cipher.
925630	Unable to unset `http-supported-max-version` to start using HTTP/2.
929109	Exported firewall policy is missing the negate option for source, destination, and service fields.
939734	When there are two to seven thousand addresses on the *Policy & Objects* > *Virtual IPs* page, clicking *Suggestions* in the *Map to* field makes the GUI unresponsive.
940360	FortiGate adds deleted `tcp-portrange` and `udp-portrange` after a reboot.

Bug ID	Description
942605	FortiGate accepts the `ha-mgmt-intf-only` local-in policy from FortiManager, even though the `ha-mgmt-status` is not enabled.
948393	Policy lookup should not get result with `policy_action: deny` for non-TCP protocols and non-80/443 TCP ports.
950775	Traffic matches incorrect central SNAT rule when performing NAT46 in NGFW policy mode.
950889	Session clashes occur when incoming traffic matches an expected session and undergoes SNAT, but the SNAT port is already occupied by another session.
951373	Traffic shaping does not match the correct queue for outbound traffic when the `class-id` range exceeds the [2, 7] limit, which applies to egress shaping.
951684	The maximum size of the server certificate for virtual server should be displayed.
952552	When using HTTP1, the TLS handshake from the proxy to the real server does not include the SNI.
952761	BGP and other traffic is getting dropped when IPv4 and IPv6 access lists are applied.
953907	Virtual wire pair interface drops all packet if the `prp-port-in`/`prp-port-out` setting is configured under `system npu-setting prp` on FG-101F.
953921	GUI does not display the configured parameters for traffic shaping policies when editing a policy with an SD-WAN zone.
957749	An `action=accept` should not be shown in a traffic log when UDP traffic dropped by IPS. The `utmaction` field is also missing in this scenario.
962984	Server load balancing health monitor does not work with Patroni (PostgreSQL cluster) when content matching is configured.
963071	Drops in multicast traffic, caused by a change in multicast routing (PIM), may occur at the start of multicast communication after upgrading.
967205	Changing the destination in the policy replaces applied services with service, ALL.

FortiGate 6000 and 7000 platforms

Bug ID	Description
891642	FortiGate 6000 and 7000 platforms do not support managing FortiSwitch devices over FortiLink.
892600	IPv6 static route is removed from the management VDOM.
896758	Virtual clustering is not supported by FortiGate 6000 and 7000 platforms.
905450	SNMP walk failed to get the BGP routing information.
907140	Authenticated users are not synchronized to the secondary FortiGate 6000 or 7000 chassis when the secondary chassis joins a primary chassis to form an FGCP cluster.

Bug ID	Description
907695	The FortiGate 6000 and 7000 platforms do not support IPsec VPN over a loopback interface or an NPU inter-VDOM link interface.
910824	On the FortiGate 7000F platform, fragmented IPv6 ICMP traffic is not load balanced correctly when the `dp-icmp-distribution-method` option under `config load-balance` is set to `dst-ip`. This problem may also occur for other `dp-icmp-distribution-method` configurations.
914273	SNMP query to fgVdEntSesRate returns a 0 value.
937879	FortiGate-7000F chassis with FIM-7941Fs cannot load balance fragmented IPv6 TCP and UDP traffic. Instead, fragmented IPv6 TCP and UDP traffic received by the FIM-7941F interfaces is sent directly to the primary FPM, bypassing the NP7 load balancers. IPv6 ICMP fragmented traffic load balancing works as expected. Load balancing fragmented IPv6 TCP and UDP traffic works as expected in FortiGate-7000F chassis with FIM-7921Fs.
938475	Memory usage issue occurs when multiple threads try to access a VLAN group.
939119	Statistics displayed in the *Session Rate* dashboard widget do not match the statistics displayed from the command line.
941944	CPU usage data displayed in the FortiGate 6000 GUI is actually CPU usage data for the management board. CPU usage data displayed in the FortiGate 7000 GUI is actually the CPU usage for the primary FIM.
941971	Dashboard widgets for *CPU*, *Memory*, *Session*, and *Session Rate* show usage as 0% on root and non-root VDOMs.
946943	On 6K and 7K platforms, the management VDOM GUI should not show the *WiFi & Switch Controller* menu.
947570	In an FGCP cluster, the secondary unit cannot reply to the SNMP query while using the management IP.
947936	On the FortiGate 7060E, only four of six PSUs are shown sometimes.
948750	When EMAC VLAN interfaces are removed spontaneously from the configuration, TCP traffic through their underlying VLAN interface fails.
949175	On the FortiGate 7121F, with FIM2 as the primary FIM, making FIM1 the primary causes NP7 PLE invalidation.
949240	SLBC special ports do not match the local-in policy's management path.

FortiView

Bug ID	Description
941521	On the *FortiView Web Sites* page, the *Category* filter does not work in the Japanese GUI.
950137	FortiView *Application* widget does not show data for explicit proxy traffic.

GUI

Bug ID	Description
651648	When a large number of addresses are present (over 17 thousand), searching for an object on the *Policy & Objects* > *Addresses* page takes around 20 to 30 seconds to display results.
676306, 719694	When there is a connection issue between the FortiGate and a managed FortiSwitch, unexpected behavior might occur in httpsd when navigating between *Switch Controller* related GUI pages.
893560	When private data encryption is enabled, the GUI may become unresponsive and HA may fail to synchronize the configuration.
900818	The GUI should not show the interface speed in the SSL VPN interface tooltip.
904817	Changing the *IPv4*/*IPv6* version in the dropdown of one widget will also impact other *Session Rate* widgets.
924159	A time difference is noticed in the FortiGate GUI and command line when the GUI is refreshed or when logged in on a new tab.
926410	While creating new address from firewall policy, the address slide takes around five seconds to open up.
934644	When the FortiGate is in conserve mode, node process (GUI management) may not release memory properly causing entry-level devices to stay in conserve mode.
940183	No IP results appear when using the search bar of the *Assets & Identities* dashboard.
940592	*Dashboard* > *IPsec Monitor* column selections are not saved across a page refresh.
941723	An error occurred when attempting to perform interface migration from a physical interface containing a VLAN interface to an aggregate interface.
943949	The GUI does not allow parentheses, (), to be used in the interface description.
945221	The GUI does not show any transceiver information until running `get system interface transceiver` in the CLI.
954356	When connected to the FortiGate GUI on a mobile phone, the table content on some pages like *Network* > *Interfaces*, *Policy & Objects* > *Firewall Policy*, and *WiFi & Switch Controller* > *Managed FortiSwitches* is cut off.
973432	When editing an SD-WAN rule with more than one destination, some destinations are automatically removed.

HA

Bug ID	Description
818432	When private data encryption is enabled, all passwords present in the configuration fail to load and may cause HA failures.
902945	Lost management connectivity to the standby node via in-band management.
904117	When walking through the session list to change the `ha_id`, some dead sessions could be freed one more time.
924671	FG-200F in HA's management interface is not responding after a reboot.
925269	Configuration is out-of sync when external feed connectors are applied to a policy.
929156	Asymmetric traffic through one of the FGSP members is allowed, even when the session is in a TCP SYN sent state.
937246	An error condition occurred while forwarding over a VRRP address, caused by the creation of a new VLAN.
940400	SCTP traffic is not forwarded back to the session owner (FGSP asymmetric traffic with IPS , NAT mode, and SCTP).
942504	Temporary network interruption occurs after disabling `standalone-config-sync`.
946878	When configuring an HA management interface, the GUI does not allow the same interface to be used for multiple management interfaces.
949230	Unable to send a file to a remote HA member when synchronizing a configuration.
950868	Traffic is not forwarded on L2 peer to keep FGSP with an available L2 connection.
953167	Access to console and SSH is lost due to a specific configuration.
953202	The hasync process is stuck at 99.9% on one or both cluster members after a failover.
954098	The `set auto-firmware-upgrade disable` setting is not synchronized between FGCP members.
955555	Unexpected traffic flow occurs after FGSP is enabled between clusters.
963951	Unable to modify the `pingserver-flip-timeout` once `vcluster` is enabled.
965938	Standalone configuration synchronization fails to synchronize because of interface subnet firewall address objects.

Hyperscale

Bug ID	Description
936747	Connections per second (CPS) performance of SIP sessions accepted by hyperscale firewall policies with EIM and EIF disabled that include overload with port block allocation (PBA) GCN IP pools is lower than expected.
949188	ICMP reply packets are dropped by FortiOS in a NAT64 hyperscale policy.
950582	Traffic not passing across the VDOM link.
958066	Observed TCP sessions timing out with a single hyperscale VDOM configuration after loading image from BIOS.

Intrusion Prevention

Bug ID	Description
916175	Make improvements to the IPS engine when handling a rare buffer overflow case.
934015	RSH subsession timeout when IPS is enabled.
949662	Interface policy logs show the external facing IP instead of the actual source.
952270	IPS logs for VIP traffic shows external IP as a destination for some signatures.

IPsec VPN

Bug ID	Description
780297	IKE debug log filtering functionality exhibits inaccuracies, resulting in the possibility of displaying unmatched logs when filters are set.
897867	IPsec VPN between two FortiGates (100F and 60F) experiences slow throughput compared to the available underlay bandwidth.
922064	Firewall becoming unresponsive to DPD/IKE messages, causing IPsec VPNs to drop.
926002	Incorrect traffic order in IPsec aggregate redundant member list after upgrade.
926052	For DHCP-over-IPsec, sometimes the client does not send a delete after the DHCP SA.
930278	Setting `loopback-asymroute disable` in the phase 1 configuration pushes down the loopback interface index as tunnel's `bound_if`, causing traffic route lookup failure.
942495	IKEv2 connection issue related to the order of policies using different user groups.

Bug ID	Description
945367	Disabling `src-check` (RPF) on the parent tunnel is not inherited by ADVPN shortcuts.
945873	Inconsistency of `mode-cfg` between phase 1 assigned IP address and destination selector addition.
949086	Policy route is not matching ESP traffic.
950445	After a third-party router failover, traffic traversing the IPsec tunnel is lost.
951765	Shortcut created from parent tunnel interface does not inherit MSS value and may face fragmentation.
954614	IPsec phase 2 negotiation fails with `failed to create dialup instance, error 22` error message.
954911	IPv6 firewall address IP prefix object is invisible on accessible networks in the GUI.
955552	Split DNS not pushed because the split tunnel is not recognized.
957412	Authentication fails since the EAP proxy cannot get groups by the hostname of FortiGate in the NAS-ID RADIUS attribute.
958516	Acct-Output-Octets are wrapped to 32-bit on RADIUS accounting stop.
960212	IPsec traffic is unidirectional when `vpn-id-ipip` and offloading are enabled, and the tunnel VRF is greater than 63.
961305	FortiGate is sending ESP packets with source MAC address of port1 HA virtual MAC address.

Log & Report

Bug ID	Description
850642	Logs are not seen for traffic passing through the firewall caused by numerous simultaneous configuration changes.
903841	When an administrator login fails, the event log shows that the login was successful.
905849	The log settings disk usage graph should show the usage data in the legend's format.
920376	Content disarm and reconstruction (CDR) files are not consistent in the log view.
931924	SSL VPN web mode login history entries are not seen when logs are being sent to FortiAnalyzer.
932537	If Security Rating is enabled to run on schedule (every four hours), the FortiGate can unintentionally send local-out traffic to fortianalyzer.forticloud.com during the Security Rating run.
933650	When the DNS server does not provide the IPv6 (AAAA record) for the NTP server FQDN, FortiGate NTP shows that the IPv6 server is `unresolved -- unreachable`, which is not true.
938396	`The following intrusion was observed:` in the alert mail refera to another field in the anomaly log.

Bug ID	Description
940814	Administrators without read permissions for the threat weight feature cannot see the event log menu.
945287	Cloud logging settings are not retained when the FortiGate language setting is Japanese.
949001	The `quarantine-log enable` setting changed to `disable` after restoring a backup configuration.
950768	When a GUI login fails due to `exceed_limit`, `logged in successfully` appears in the system event log.
952509	The UUID is used instead of the external resource name in the `Threat feed updated` system event log.
953667	Override setting under multi-VDOM mode may cause the FortiGate to stop sending logs to FortiAnalyzer or syslog after switching to non-VDOM mode.
961244	Icons in logs evaluations and policies are no longer displayed.
965247	FortiGate syslog format in reliable transport mode is not compliant with RFC 6587.
967100	When FortiAnalyzer Cloud is chosen as log location, archived data cannot be downloaded for intrusion prevention.
970412	`Virus/Botnet` AV log for machine learning detection hyperlink returns `Object Moved Permanently`.

Proxy

Bug ID	Description
790426	An error case occurs in WAD while redirecting the web filter HTTPS sessions.
806556	Unexpected behavior in WAD when the ALPN is set to `http2` in the `ssl-ssh-profile`.
919781	Unexpected behavior in WAD when there are multiple LDAP servers configured on the FortiGate.
938502	Original source IP is not preserved for transparent proxy rule after upgrading.
940149	Inadvertent traffic disruption caused by WAD when it receives an HTTP2 data frame payload on a dead stream.
943998	Unble to access website (https://ec***.qu***.com/me***) when using a proxy with DPI.
947359	The newly implemented one-way server will set its port to null when closing.
947814	Too many redirects on TWPP after the second KRB keytab is configured.
954104	An error case occurs in WAD when WAD gets the external authenticated users from other daemons.
955006	SNI check is not working when set to inspect all ports.

Bug ID	Description
958464	Unexpected behavior in WAD when building a debug URL.
971489	When `cloud-communication` is disabled, WAD still connects to productapi.fortinet.com.
974307	An error condition occurs in WAD while coping a file directory.

REST API

Bug ID	Description
944723	The `/firewall/vip` API does not recognize custom SSL cipher suites.
948356	An error condition occurs in HTTPSD when a REST API request is sent with invalid parameters.
951384	API responses for PBR provides incorrect value if address groups are used in PBR.
951411	Inconsistent handling of web filter profile actions in API transactions.

Routing

Bug ID	Description
820407	Auto-link fails if the FortiGate device initiating the FGFM connection is using an interface with a VRF not set to the default, 0.
848270	Reply traffic from the DNS proxy (DNS database) is choosing the wrong interface.
894795	MP-BGP EVPN source address shows 127.0.0.1, while the loopback interface is with a different address.
897918	When the local traffic is using SD-WAN and the reply is coming on a different interface, the reply is ignored.
906896	Make OSPFv3 update the translator role and translated Type-5 LSA when the ASBR table is updated.
926525	`Routing information changed` log is being generated from secondary in an HA cluster.
928152	FortiGate generates two OSPF stub entries for the same prefix after upgrading from 6.4 to 7.0.
934273	Support GR helper mode (peer) for BGP.
935370	SD-WAN performance SLA `tcp-connect` probes clash with user sessions.
935886	SD-WAN packet duplication feature in force mode suddenly stops duplicating and starts to duplicate again once the FortiGate is rebooted.
938500	Status of OSPF adjacency is `Loading` on spokes while `Full` on the hub side.

Bug ID	Description
944351	When using the policy match tool, the *Incoming Interface* dropdown does not list SD-WAN member interfaces.
946783	Unable to set OSPF interface IP in the GUI.
949623	DNS over TCP does not work when `interface-select-method` is set to `sdwan` in the DNS setting, and the corresponding SD-WAN rule is restricted to the TCP protocol only.
951397	Inconsistent GUI output with unusual characters showing up in the SD-WAN rule list settings and the edit SD-WAN rule page.
952543	Reply TCP traffic for inbound local session uses a different egress interface than the originating traffic
952908	Locally originated type 5 and 7 LSAs' forward address value is incorrect.
953744	Connected VLAN routes are getting removed after an HA failover.
954100	Packet loss status in SD-WAN health check occur after an HA failover.
957049	If the router `community-list` type is expanded and changed to `standard`, this causes a `community-list` error.
957627	Learned BGP through routes are not withdrawn on the spoke after the EBGP neighborship is down between the hub and third party device.
963561	When establishing an IPsec tunnel between FortiGate peers using OSPF to exchange routes, the FortiGate sends a stub LSA with a 32-bit netmask.
964182	IPsec traffic with `vpn-id-ipip` is egressing with the wrong VRF when offloading is enabled.
965752	After HA monitored interface fails over, SD-WAN intermittently does not follow `route-map-preferable`.

Security Fabric

Bug ID	Description
902344	When there are over 30 downstream FortiGates in the Security Fabric, the root FortiGate's GUI may experience slowness when loading the *Fabric Management* page and prevents the user from upgrading firmware in the GUI.
907819	Advanced GCP connector does not resolve if one element does not exist.
908489	When one of the downstream FortiGate VM's license is invalid, the root FortiGate will be automatically logged out from accessing the *Firmware & Registration* page.
920391	Non-management VDOM is not allowed to set a `source-ip` for `config system external-resource`.
932935	External connector to VMware 8.0 with `verify certificate` enabled will fail.

Bug ID	Description
938980	HTTP 400 errors observed using SDN connector to query AKS clusters if local administrator is disabled.
947634	*Security Fabric* widget shows the serial number instead of the hostname for a secondary FortiGate in HA.
950624	Renaming conflicted Fabric objects on the root FortiGate does not synchronize the changed Fabric objects to the downstream FortiGate.
958396	The number of log IDs under one automation trigger is limited to 16.

SSL VPN

Bug ID	Description
879329	Destination address of SSL VPN firewall policy may be lost after upgrading when `dstaddr` is set to `all` and at least one authentication rule has a portal with split tunneling enabled.
923518	When SSL VPN web mode is disabled, SAML external browser login requests should be blocked.
930275	Firewall policy is not allowing the all destination address with a split-tunneling portal.
933985	FortiGate as SSL VPN client does not work on NP6 and NP6XLite devices.
941676	Japanese key input does not work correctly during RDP in SSL VPN web mode.
947210	Multiple instances of `*** code requested backtrace ***` for SSL VPN daemon observed during a graceful upgrade (on FG-6000F).
950157	SSL VPN connected/disconnected endpoint event log can be in the wrong sequence.
952860	During a handshake when FortiClient sends a larger-than-MTU hello message, the packet is fragmented by IP layer and dropped by the FortiGate.
957406	OS checklist for SSL VPN in FortiOS does not include macOS Sonoma 14.
958430	If the password renew template is modified with a non-default password renew policy, FortiClient cannot read the HTML page correctly, and returns the error, *Server may not be reachable*.

Switch Controller

Bug ID	Description
703374	Long DAC-type cable is added to default media type on 10G port on FG-100F.
816790	Console printed DSL related error messages when disconnecting the managed FortiSwitch and connecting to the FortiGate again.

Bug ID	Description
818116	When changing the FortiSwitch FortiLink port status, the configuration is not applied to the FortiSwitch.
904834	FortiGate and FortiManager have different definitions for the value of `poe-detection-type` on S108EF platform.
911232	The security rating shows an incorrect warning for unregistered FortiSwitches on the *Managed FortiSwitches* page. **Workaround**: navigate to the *Diagnostics & Tools* pane of the FortiSwitch to see the correct registration status.
931694	Enhance FortiLink event logs for FortiGate-FortiSwitch event log translation.
941673	FortiSwitch event log displays serial number under name when CAPWAP is up or down.
945779	FortiGate CPU VM increases due to the FortiLink process.
949377	NAC policy cannot match the MAC address with a specific VLAN. The NAC policy needs to be deleted and re-createed for it to work again.
953918	FortiGate `nac_segment` is not showing assigned dynamic VLAN on FortiSwitch ports.
961997	Unable to get interface descriptions for the FortiLink ports by using OID 1.3.6.1.2.1.2.2.1.2.

System

Bug ID	Description
656983	MIB OID fgSysLowMemUsage returns value for devices where it is not applicable.
699379	Host protection engine (HPE) enchantments should be applied to NP6XLite platforms.
713951	Not all ports are coming up after an LAG bounce on 8 × 10 GB lag with ASR 9K. Affected platforms: FG-3960E and FG-3980E.
859393	SNMP poll for fgExplicitProxyRequests returns 0.
860460	On a redundant interface, traffic may drop with some NPU-offload enabled policies when the interface is not initialized properly.
861962	When configuring an 802.3ad aggregate setting with 1 Gbps speed, the port's LED light is off and traffic cannot pass through.
899279	NP7 did not offload jumbo packet, but get `NPU INFO: offload=9/9` in the console output.
900663	Refactor the time zone feature to use the IANA time zone database.
900791	The X1 port is always up with FCLF8522P2BTLFTN transceiver.
907657	FortiGate does not perform a disk scan automatically when `autorun-log-fsck` is enabled.

Bug ID	Description
908831	Unable to set upstream interface without setting the delegated IAID first for IPv6 interface under delegated mode.
909225	ISP traffic is failing with the LAG interfaces on upstream switches.
910651	On FG-600F, all members are up but the LACP status is showing as down after upgrading.
910700	Ports are flapping and down on the FortiGate 3980E.
910829	Degraded traffic bandwidth for download passing from 10G to 1G interfaces.
912092	FortiGate does not send ARP probe for UDP NP-offloaded sessions.
913355	GUI and CLI time mismatch for Central America (Mexico) time zone.
915585	Optimize memory usage, which causes the SLAB memory to increase, in kernel 4.19.
916493	Fail detection function does not work properly on X1 and X2 10G ports.
919901	For FIPS-CC mode, the strict check for basic constraints should be removed for end entity certificates.
922458	Administrator with read-only access to management permissions cannot perform a configuration backup in the GUI.
924654	MAC flapping on switch when UDP packets passthrough VWP multiple times with ASIC offload.
925647	Memory usage issue caused by repetitive log messages. Affected platforms: FG-100xF.
926546	ICMP and UDP traffic over GRE is not offloaded on NP7 platforms.
926817	Review the temperature sensor for the SoC4 system.
929904	When L3 or L4 hashing algorithm is used, traffic is not forwarded over the same aggregate member after being offloaded by NP7.
930329	LTE modem is missing after upgrading to 7.4.
931299	When the URL filter requests the FortiGuard (FGD) rating server address using DNS, it will try to get both A (IPv4) and AAAA (IPv6) records.
931604	The FortiGate checksum changes and the FortiManager Backup Mode device status becomes out-of-sync.
934115	Administrator can no longer view or edit the VPN settings in the GUI with `system:none` permissions.
937982	High CPU usage might be observed on entry-level FortiGates if the cache size reaches 10% of the system memory.
938539	The cmdbsvr process is stuck, and is not pushing configurations made in the GUI or CLI.
939110	DHCP server on LAN interface is lost after rebooting or restoring the configuration file.
939411	Multiple spawns of hotplug process consuming high CPU resources.
939935	High CPU usage caused by DHCP packets.
939947	FG-1100E SFP interface of port 23 and 24 with transceiver status is down after upgrading.

Bug ID	Description
940504	Loading of the Toss Bank application is delayed or gets stuck on iPhones with hyperscale CGNAT (NAT64).
940752	FortiGate does not allow tagged VLAN 0 packets.
942502	Unexpected behavior occurred in the kernel when creating EMAC VLAN interfaces based on an aggregate interface with the new kernel 4.1.9.
942893	When DHCP IP reservation is edited from the DHCP dashboard widget, the changes are not retained.
943026	Changes to per-IP shaper settings are not reflected on offloaded sessions in NP7 platforms.
943090	Buffer and description queue limitation of Marvell switch port will cause a performance limitation.
943615	When cmdbsvr receives a request to update the version number, it also receives a copy of the query, but this copy is not freed.
943948	FortiGate as L2TP client is not working with Cisco ASR as L2TP server.
945426	FortiGate ports are not in a configured state after the connected switch reboots.
946413	Temperature sensor value missing for FG-180xF, FG-420xF, and FG-440xF platforms.
946714	Unexpected reboot caused by a rare error condition for FG-VM.
947240	FortiGate is not able to resolve ARPs of few hosts due to their ARP replies not reaching the primary FPM.
948448	A super_admin administrator is unable to log in after restoring the VDOM configuration on the admin VDOM and rebooting the FortiGate.
948460	Enabling NP7 offloading is causing packet drops when using a shaping profile.
949481	The `tx_collision_err` counter in the FortiOS CLI keeps increasing on both 10G SFP+ X1 and X2 interfaces.
949975	SNMP value for OID 1.3.6.1.4.1.12356.101.12.2.2.1.5 returns the wrong value.
950010	Alarm observed for high PECI temperature despite less CPU activity.
952279	The TCP handshake is interrupted when any of the UTM profiles are enabled.
954439	SNMP does not respond if a VRF is set on the interface.
955021	When signal 11 is sent to httpsd process using `diagnose sys kill 11 <PID>`, httpsd does not restart. The GUI displays a *Service unavailable* message. GUI access can be restored by rebooting the device.
955074	MSS clamping is not working on VXLAN over IPsec after upgrading.
955798	Interface LED from panel indicates the wrong status.
955998	The traffic is dropped when `auto-asic-offload` is enabled and passing through a VLAN associated with a 10G redundant interface.
956391	On FG-10xE, when using ports 13 to 16 as virtual switch LAN ports, auto speed is not supported.

Bug ID	Description
956413	FG-1101E ports with AVAGO AFBR-5710PZ transceiver failed to come up after upgrading.
956980	Batch lastlog does not show any errors for `password-policy` misconfiguration.
957147	FortiGate as DNS server does not resolve domains in the local database on new VDOM.
957714	Memory usage issue occurs when multiple threads try to access a VLAN group.
957846	High CPU usage caused by DHCP packets.
958157	The GeoIP file should close appropriately after opening or using mmap to share memory.
960563	An error condition occurred in the kernel caused by a rare condition while using the GRE tunnels.
963597	Multiple configuration settings are missing after restoring the VDOM.
966761	SNMP OID 1.3.6.1.2.1.4.34.1.5 ipAddressPrefix is not fully implemented.
969230	FEC does not take effect on X5 - X8 ports when running at 25G ULL mode on FG-601F.

Upgrade

Bug ID	Description
871181	FG-3401E link is not coming up using DAC cables after upgrading.
896937	Port channel is down after upgrading the FG-1101E.
940126	Upgrading a FGT-3401E generates BPDUs, which cause the switch to disable the port.

User & Authentication

Bug ID	Description
823884	When a search is performed on a user *(User & Authentication > User Definition* page), the search results highlight all the groups the user belongs to.
868994	FortiGate receives FSSO user in the format of HOSTNAME$.
907169	WPA2-Enterprise SSID should support EAP-TLS authentication for PKI users that are configured with multi-factor authentication through a RADIUS server.
915998	FortiToken mobile push with ACME gives an untrusted certificate in iOS application.
932989	In some cases, the HA connection is removed and its memory is freed, but it is still read/written in the following process.
939517	On the *System > Replacement Messages* page, the guest user email template cannot restore to the to default value.

Bug ID	Description
943087	After creating a new guest user, the administrator cannot view the user's password in plaintext in the GUI.
946116	On a FortiGate managed by FortiManager, when a guest administrator logs in with read-only permissions, the administrator can still create and edit the guest user.
947299	Global DH parameter does not modify the SSH connection key exchange.
949699	Administrator single sign-on login with SAML does not work after upgrading the firmware 7.4.1 due to the SAML `entity-id` field being incorrectly reset to being empty.
955939	PKI users should pass certificate-based authentication over WPA2-Enterprise SSID.
961496	CPU usage issue caused by signature update for device identification.

VM

Bug ID	Description
903037	A false positive SSL VPN login token error message is generated after a successful connection.
932085	In an Azure cluster, the NTP `source-ip6` (IPv6) is synchronized while the `source-ip` (IPv4) is not.
950235	IPv6 multicast packets are triggering a hardware checksum failure error message on the console.
953760	FG-VM is unable to respond to the load balancer's health probe correctly.
956460	FortiGate cannot detect a log disk in some new Azure instances.
957886	GCP OS log in integration issues occur in FortiGate deployment.
959859	FG-VM64-AZURE SDN connector does not retry requests to management.azure.com if they fail.
965668	Interfaces are brought down by azd, and traffic is disrupted until manually disabling and enabling the interfaces on the Azure VM.
968740	Unexpected behavior in awsd caused by tags with an empty value on AWS instances while adding a new AWS Fabric connector.
970201	Unexpected reboot caused by a rare error condition for FG-VM.

WAN Optimization

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

Web Application Firewall

Bug ID	Description
939380	User cannot set the match *ALL* pattern to deny traffic for the web application firewall profile in the GUI.

Web Filter

Bug ID	Description
887699	Web filter override expiry date in the GUI may be one hour off if daylight saving time (DST) is observed.
923548	Newly added local URL filter entry cannot be moved using drag-and-drop.
929110	The `strict` option for `sni-server-cert-check` is behaving the same as if it is set to `enable`, and logs are not generated upon SNI mismatch with the CN or SAN.
945011	URL filter IP address block is not honored by the enhanced policy lookup tool.
947676	Web filter profile setting changes the order of FortiGuard web filter categories.

WiFi Controller

Bug ID	Description
801730	The `move` function in the CLI does not work for `mpsk-profile` and `mpsk-group`.
891804	After initial packets, FG-101F stops forwarding wired traffic over FAP-23JF LAN tunneled with a dynamic VLAN VAP.
896104	An error condtion occured in the kernel when the FortiAP and SSID are in the same software switch.
938840	Excessive `MEM POOLuse_up_cnt` observed on secondary unit in an HA environment.
941691	Multiple MAC addresses are on one port.
944465	On the *WiFi & Switch Controller* > *Managed FortiAPs* page of a non-management VDOM, the *Register* button is unavailable in the *Device Registration* pane.
945356	FortiOS fails to get all of the configured MAC ACL entries.
946796	The eap_proxy daemon may keep reloading randomly due to failing to bind a port. This will cause an IKE and WiFi authentication failure.
949857	Captive portal appears each time after a channel change or if roaming performed (Cisco ISE with FortiGate and FortiAP).

Bug ID	Description
951792	Clients connected to certain FortiAPs do not have internet access.
952889	PMKID should be removed when an Android device is disconnected by the RADIUS CoA DM request with Acct-Session-Id.
958314	AeroScout agent is not working.
967158	WPA2-Enterprise with a Windows NPS server is not working after upgrading the firmware to FortiOS 7.4.1.
973935	On the *WiFi & Switch Controller* > *Managed FortiAPs* page, there is an error when changing from a single 5G profile to a dual 5G profile on the FortiAP 831F.

ZTNA

Bug ID	Description
918279	Traffic does not match a simple ZTNA firewall policy when the external interface configured on a ZTNA server is a member of a SD-WAN zone being used in the same ZTNA firewall policy.

Known issues

The following issues have been identified in version 7.4.2. To inquire about a particular bug or report a bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
977634	FortiOS *High Security Alert* block page reference URL is incorrect.

Application Control

Bug ID	Description
934197	Selected applications will disappear after searching or filtering for other applications in override.

Firewall

Bug ID	Description
760292	The date in the graph of *Last 7 Days* traffic statistics for the policy is incorrect.
959065	Once a traffic shaper is applied to a traffic shaping firewall policy, the counters should not clear when deleting or creating a traffic shaper.
966466	On an FG-3001F NP7 device, packet loss occurs even on local-in traffic.
981283	NAT64/46 HTTP virtual server does not work as expected in the policy.

FortiGate 6000 and 7000 platforms

Bug ID	Description
781163	*FortiView Sources* page is unable to display historical data from FortiAnalyzer due to *Fail to retrieve FortiView data* error.

Bug ID	Description
787604	Transceiver information in unavailable for FPM/FIM2 ports in the GUI.
790464	Existing ARP entries are removed from all slots when an ARP query of a single slot does not respond.
885205	IPv6 ECMP is not supported for the FortiGate 6000F and 7000E platforms. IPv6 ECMP is supported for the FortiGate 7000F platform.
887946	UTM traffic is blocked by an FGSP configuration with asymmetric routing.
910883	The FortiGate 6000s or 7000s in an FGSP cluster may load balance FTP data sessions to different FPCs or FPMs. This can cause delays while the affected FortiGate 6000 or 7000 re-installs the sessions on the correct FPC or FPM.
911244	FortiGate 7000E IPv6 routes may not be synchronized correctly among FIMs and FPMs.
969530	Blade unexpected reboot occurs on FG-5001D.
973407	FIM installed NPU session causes the SSE to get stuck.
978241	FortiGate does not honor worker port partition when SNATing connections using a fixed port range IP pool.

GUI

Bug ID	Description
848660	Read-only administrator may encounter a *Maximum number of monitored interfaces reached* error when viewing an interface bandwidth widget for an interface that does not have the monitor bandwidth feature enabled. **Workaround**: super_admin users can enable the monitor bandwidth feature on the interface first, then the widget can work for read-only administrators.
853352	When viewing entries in slide-out pan of the *Policy & Objects* > *Internet Service Database* page, users cannot scroll down to the end if there are over 100K entries.
885427	Suggest showing the SFP status information on the faceplate of FGR-60F/60F-3G4G devices.
925388	After updating, the CMDB may not start up properly. This issue causes problems with both the GUI and CLI.
931486	Unexpected behavior in httpsd when the user has a lot of FQDN addresses.
961796	When administrator GUI access (HTTPS) is enabled on SD-WAN member interfaces, the GUI may not be accessible on the SD-WAN interface due to incorrect routing of the response packet. **Workaround**: access the GUI using another internal interface that is not part of an SD-WAN link.
964386	GUI dashboards show all the IPv6 sessions on every VDOM.
966702	List of security profiles it is not displayed correctly in the GUI.

Bug ID	Description
971790	FortiGate models with 2 GB RAM may experience memory usage issues when users access the web GUI, due to a sudden increase in memory consumption in httpsd. **Workaround**: avoid navigating to memory-intensive pages under *Dashboard* with multiple widgets that can cause a spike in memory consumption. Users can create custom dashboards with a single widget to reduce the concurrent load.
972887	The interface firewall object created automatically is not found by a firewall policy search with IP address.
975403	FortiGate removes the `?` from custom replacement messages.
979508	The *Operation Technology* category cannot be turned on or off from the GUI. The option to enable/disable the *Operational Technology* category on application control profiles when hovering the mouse over the category name is missing. **Workaround**: use the CLI to configure it.
983422	A GTP profile cannot be applied to policy using the GUI. **Workaround**: use the CLI to apply the GTP profile.

HA

Bug ID	Description
971075	The last interface belonging to the management VDOM (not root VDOM) is not displayed when accessing `ha-mgmt-interface`.

Hyperscale

Bug ID	Description
817562	NPD/LPMD cannot differentiate the different VRFs, and considers all VRFs as 0.
850252	Restoring a specific VDOM configuration from the GUI does not restore the complete configuration.
896203	The parse error, `NPD-0:NPD PARSE ADDR GRP gmail.com MEMBER ERR`, appears after rebooting the system.
975264	Hyperscale should not support threat feed addresses with the negate option.
976972	New primary can get stuck on failover with HTTP CC sessions.
977376	FG-4201F has a 10% performance drop during a CPS test case with DoS policy.
981918	Hyperscale policy loses the `cgn-log-server-grp` setting with log mode per-mapping when the system reboots.

Intrusion Prevention

Bug ID	Description
782966	IPS sensor GUI shows *All Attributes* in the filter table when IPS filters with default values are selected in the CLI.

IPsec VPN

Bug ID	Description
866413	Traffic over GRE tunnel over IPsec tunnel, or traffic over IPsec tunnel with GRE encapsulation is not offloaded on NP7-based units.
897871	GRE over IPsec does not work in transport mode.
916260	The IPsec VPN tunnel list can take more than 10 seconds to load if the FortiGate has large number of tunnels, interfaces, policies, and addresses. This is a GUI display issue and does not impact tunnel operation.
944600	CPU usage issues occurred when IPsec VPN traffic was received on the VLAN interface of an NP7 vlink.
970703	FortiGate 6K and 7K models do not support IPsec VPN over vdom-link/npu-vlink.

Log & Report

Bug ID	Description
960661	FortiAnalyzer report is not available to view for the secondary unit in the HA cluster. **Workaround**: view the report directly in FortiAnalyzer.

Proxy

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

Bug ID	Description
922093	CPU usage issue in WAD caused by source port exhaustion when using WAN optimization.
933002	Memory usage issue in WAD caused by a rare error condition.
965966	An error condition occurred in WAD due to heavy HTTP video traffic when using a video filter profile with deep inspection enabled.

REST API

Bug ID	Description
964424	REST API GET `/ips/sensor/{name}` adds extra space to `locations`, `severity`, `protocol`, `os`, and `application` field values.

Routing

Bug ID	Description
903444	The `diagnose ip rtcache list` command is no longer supported in the FortiOS 4.19 kernel.
974921	Configuring the *Set weight* on the route map to *0* in the GUI does not save this setting in the CLI configuration.

Security Fabric

Bug ID	Description
948322	After deauthorizing a downstream FortiGate from the *System* > *Firmware & Registration* page, the page may appear to be stuck to loading. **Workaround**: perform a full page refresh to allow the page to load again.
966740	Security rating *Last Ran* displays incorrect values.
968585	The automation stitch triggered by the FortiAnalyzer event handler does not work as expected.
972921	The comments are not working as expected in the threat feed list for the domain threat feed.

SSL VPN

Bug ID	Description
951827	SSL VPN client certificate verification failed after importing the VDOM user peer CA certificate into the global VDOM.

Switch Controller

Bug ID	Description
955550	Unexpected behavior in cu_acd and fortilinkd is causing the CPU to handle the majority of the traffic instead of the NPU.
988335	If a user's network has more than 20 MAC addresses in a NAC environment, it is possible for the CAPWAP to come down.

System

Bug ID	Description
907622	GUI is missing DDNS *Domain* text field box when creating a new DDNS entry.
910364	CPU usage issue in miglogd caused by constant updates to the ZTNA tags.
912383	FGR-70F and FGR-70F-3G4G failed to perform regular reboot process (using `execute reboot` command) with an SD card inserted.
921134	GUI is inaccessible when using a SHA1 certificate as `admin-server-cert`.
921604	The port (x7) has no cables attached, but link LEDs are on the FG- 601F.
953692	SNMP stops working when a second server is added. The FortiGate stops answering SNMP requests to both servers.
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.
964465	Administrators with read-write permission for WiFi and read permission for network configuration cannot create SSIDs. **Workaround**: give read-write permission for network configuration to the administrator.
968618	After the upgrade to 7.4, the NP7 L2P is dropping packets at the L2TI module.
971404	Session expiration does not get updated for offloaded traffic between a specific host range.
971466	FGR 60F faces packet loss with a Cisco switch directly connected to it.
977231	An error condition occurred in fgfm caused by an out-of-band management configuration.

User & Authentication

Bug ID	Description
667150	When a remote LDAP user with Two-factor Authentication enabled and Authentication type 'FortiToken' tries to access the internet through firewall authentication, the web page does not receive the FortiToken notification or proceed to authenticate the user. **Workaround**: click the *Continue* button on the authentication page after approving the FortiToken on the mobile device.
884462	NTLM authentication does not work with Chrome.
967146	Upon expiration, the SSL certificate is removed from GUI but not from the CLI.
972391	RADIUS group is not properly displayed as used.
975689	Unable to print with custom guest user print template.
982573	*Dashboard* > *Assets & Identities* page shows devices and interfaces from all VDOMs.

VM

Bug ID	Description
938382	OpenStack Queens FortiGate VM HA heartbeat on broadcast is not working as expected.
967134	An interrupt distribution issue may cause the CPU load to not be balanced on the FG-VM cores.
977110	Interface disappears after enabling `unicast-status` on HA.
978021	VNI length is zero in the GENEVE header when in FTP passive mode.

Web Filter

Bug ID	Description
634781	Unable to customize replacement message for FortiGuard category in web filter profile.

WiFi Controller

Bug ID	Description
814541	When there are extra large number of managed FortiAP devices (over 500) and large number of WiFi clients (over 5000), the *Managed FortiAPs* page and *FortiAP Status* widget can take a long time to load. This issue does not impact FortiAP operation.
869978	CAPWAP tunnel traffic over tunnel SSID is dropped when offloading is enabled.
883938	Flooded wireless STA traffic seen in L2 tunneled VLAN (FG-1800F).
903922	Physical and logical topology is slow to load when there are a lot of managed FortiAP (over 50). This issue does not impact FortiAP management and operation.
949682	Intermittent traffic disruption observed in cw_acd caused by a rare error condition.
964757	Clients randomly unable to connect to 802.1X SSID when FortiAP has a DTLS policy enabled.
972093	RADIUS accounting data usage is different between the bridge and tunnel VAP.

ZTNA

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

Built-in IPS Engine

IPS Engine 7.00524 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