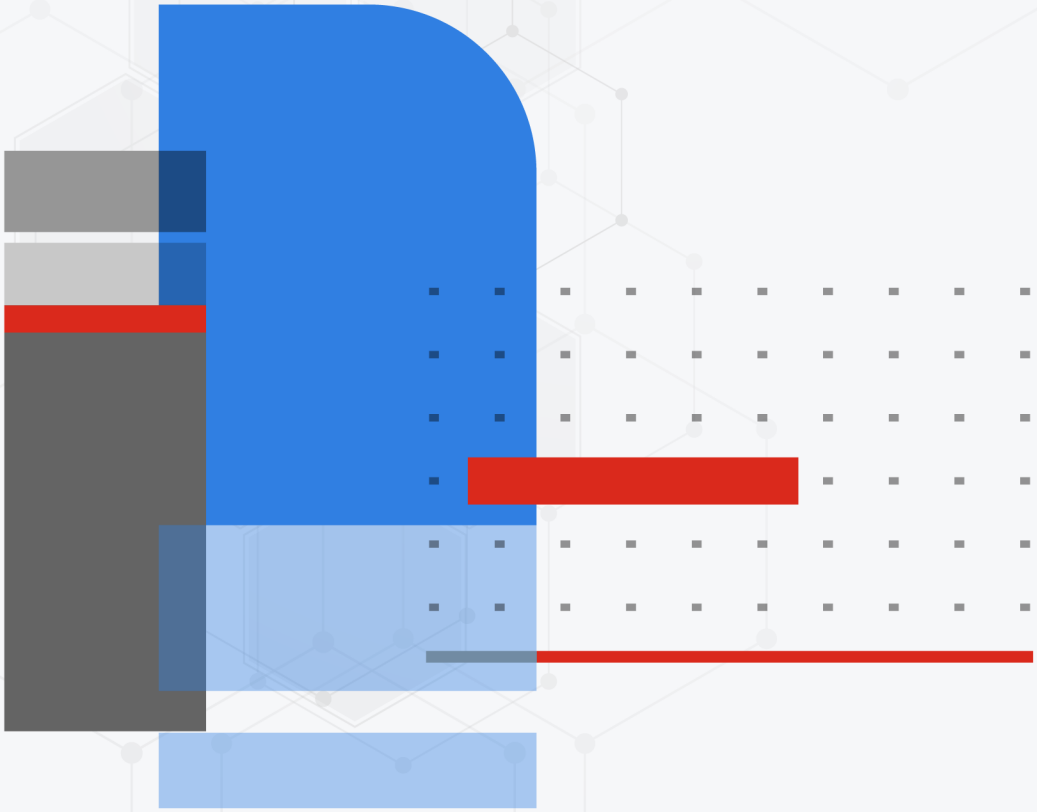
Release Notes

FortiOS 7.4.4



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

May 24, 2024
FortiOS 7.4.4 Release Notes
01-743-986078-20240524

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-05-15	Initial release.
2024-05-16	Updated 2 GB RAM FortiGate models no longer support FortiOS proxy-related features on page 34 and Resolved issues on page 40.
2024-05-17	Updated Introduction and supported models on page 7.
2024-05-24	Updated Changes in default behavior on page 17, New features or enhancements on page 20, Resolved issues on page 40, and Known issues on page 62.

Introduction and supported models

This guide provides release information for FortiOS 7.4.4 build 2662.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.4.4 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-70F, FG-71F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-DSL, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-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-80F-2R-3G4G-DSL, FWF-81F-2R, FWF-81F-2R-3G4G-DSL, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiFirewall	FFW-1801F, FFW-2600F, FFW-3001F, FFW-3980E, FFW-4200F, FFW-4400F, FFW-4401F, FFW-4801F, FFW-VM64, FFW-VM64-KVM
FortiGate VM	FG-ARM64-AWS, FG-ARM64-AZURE, FG-ARM64-GCP, FG-ARM64-KVM, FG-ARM64-OCI, FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VM64-XEN

Special branch supported models

The following models are released on a special branch of FortiOS 7.4.4. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 2662.

FGR-60F	is released on build 6003.
FGR-60F-3G4G	is released on build 6003.

FGR-70F	is released on build 6003.
FGR-70F-3G4G	is released on build 6003.

FortiGate 6000 and 7000 support

FortiOS 7.4.4 supports the following FG-6000F, FG-7000E, and FG-7000F models:

FG-6000F	FG-6001F, FG-6300F, FG-6301F, FG-6500F, FG-6501F
FG-7000E	FG-7030E, FG-7040E, FG-7060E
FG-7000F	FG-7081F, FG-7121F

Special notices

Hyperscale incompatibilities and limitations

See Hyperscale firewall incompatibilities and limitations in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 7.4.4 features.

FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 7.4.4 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.

Default email server available to registered devices with FortiCare

Starting with FortiOS7.4.4, the default email server has been switched from *notification.fortinet.net* to *fortinet-notifications.com*. This default server is only available to registered devices with an active FortiCare support contract. The *reply-to* field in the source email is automatically updated to *DoNotReply@fortinet-notifications.com* for all servers, including custom ones.

Changes in CLI

Bug ID	Description

967017	On a FortiGate with hyperscale firewall enabled, using the `tcp-timeout-profile` or `udp-timeout-profile` options of the `config system npu` command to create TCP or UDP timer profiles and then add them to hyperscale firewall policies using the `tcp-timeout-pid` or `udp-timeout-pid` firewall policy options may not work as intended.
	In FortiOS 7.4.4 `tcp-timeout-profile` and `udp-timeout-profile` are now hidden and Fortinet recommends using `config system global` options such as the following to set TCP and UDP timers:
	`config system global`
	`set early-tcp-npu-session`
	`set reset-sessionless-tcp`
	`set tcp-halfclose-timer`
	`set tcp-halfopen-timer`
	`set tcp-option`
	`set tcp-rst-timer`
	`set tcp-timewait-timer`
	`set udp-idle-timer`
	`end`
	If you have used `tcp-timeout-pid` or `udp-timeout-pid` to add profiles to hyperscale firewall policies, this configuration will still work the same after upgrading to FortiOS 7.4.4 and the profiles that you have added will still be there, but all this configuration will be hidden. To stop using these TCP timeout profiles you can unset the `tcp-timeout-pid` or `udp-timeout-pid` firewall policy options.

968305	The `ssh-xxx-algo` commands have been moved from the `config system global` setting to the `config system ssh-config` setting.
	7.4.3 and earlier:
	`config system global`
	`set ssh-enc-algo`
	`set ssh-hsk-algo`
	`set ssh-kex-algo`
	`set ssh-mac-algo`
	`end`
	7.4.4 and later:
	`config system ssh-config`
	`set ssh-enc-algo`
	`set ssh-hsk-algo`
	`set ssh-kex-algo`
	`set ssh-mac-algo`
	`end`

Bug ID	Description

976646	The captive portal is now an independent setting and separated from the wireless authentication methods.
	7.4.3 and earlier:
	`config wireless-controller vap`
	`edit <name>`
	`set security {captive portal | wpa-personal+captive+portal | wpaonly-personal+captive-portal | wpa2-onlyu-personal+captive-portal}`
	`next`
	`end`
	7.4.4 and later:
	`config wireless-controller vap`
	`edit <name>`
	`set security {open | wpa-personal | wpa2-only-personal | wpa3-sae | wpa3-sae-transition | owe}`
	`next`
	`end`
	Captive portal is disabled when security mode is `wpa2-enterprise/wpa3-enterprise/OSEN`.

999014	The `diagnose sys sdwan service` command is now divided into two separate commands for IPv4 and IPv6.
	IPv4:
	`diagnose sys sdwan service4`
	IPv6:
	`diagnose sys sdwan service6`

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
896277	If a DHCP Interface is added as an SD-WAN Member inside an SD-WAN zone, before `config static route` on SD-WAN zone, FortiOS by default adds a default route with dhcp interface distance in the routing table using the gateway IP information retrieved from the DHCP server. This default route will take precedence over other default routes that have a higher AD.

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 starts. Afterwards, the VM license will expire, and all firewall functions stop working.
975220	The Gentree Compiler is enabled by default on all NP7 platforms for threat feed support.

1005746	As part of a security enhancement, FortiGate-initiated connections to central management using an on-premise FortiManager will have the following requirements:
	1. When initiating the connection from GUI, administrators must validate and accept the FortiManager serial number from the FortiManager certificate before a connection is established.
	2. When initiating the connection from CLI, administrators must configure the FortiManager serial number in central-management before a connection is established.
	`config system central-management`
	`set type fortimanager`
	`set serial-number <FortiManager Serial Number>`
	`set fmg <ip/domain name>`
	`end`

1006011	Starting with 7.4.4, *FMG-Access* is no longer enabled by default on all interfaces. When upgrading from a previous version, if the central management type is not set to *FortiManager*, the FGFM will be disabled across all interfaces.

Changes in default values

Bug ID	Description

1019804	SSL VPN feature visibility is disabled and hidden in factory default, as well as after upgrading from a previous firmware where SSL VPN is not used. Users will not experience any changes when upgrading from a previous firmware where SSL VPN is used.
	To enable SSL VPN feature visibility, configure in the CLI:
	`config system settings`
	`    set gui-sslvpn enable`
	`end`

Changes in table size

Bug ID	Description
913153	Increase the number of software switch members from 256 to 1024 per switch interface.
988201	On FortiGate 400F, 401F, 600F and 601F models, increase the number of firewall addresses and firewall address6 objects from 20000 to 40000.
989627	On FortiGate 260F models, the number of system admins is increased from 300 to 500.

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
979375	FIPS-CC cipher mode is silently enabled when configured using cloud-init for AWS.
995867	FortiGate-VM is officially certified on AliCloud Apsara Stack.
997374	High availability (HA) failover is now supported for IPv6 networks on GCP. The *NextHopInstance route* table attribute is used during an HA failover event.

LAN Edge

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

Feature ID	Description
919714	Users can now use FortiSwitch event log IDs as triggers for automation stitches. This allows for automated actions like console alerts, script execution, and email notifications in response to events, such as switch group modifications or location changes. This boosts automation and system management efficiency.
952124	Users connected to a WiFi Access Point in a FortiExtender can now access the internet, even when the FortiGate is in LAN-extension mode. This ensures seamless internet connectivity for WiFi clients using the FortiGate LAN-extension interface.
975075	The FortiAP K series now supports IEEE 802.11be, also known as Wi-Fi 7, for these models: FAP-441K, FAP-443K, FAP-241K and FAP-243K. This expands device compatibility, boosts network performance, and enhances user experience.
975545	Support for Dynamic Access Control List (DACL) on the 802.1x ports of managed switches. This allows customers to use RADIUS attributes to configure DACLs, enabling traffic control on a per-user session or per-port basis for switch ports directly connected to user clients.
976646	FortiOS extends captive portal support to newer wireless authentication methods, such as OWE and WPA3-SAE varieties. This ensures that users can benefit from the most advanced and secure authentication methods available.

Feature ID	Description
983561	Enhanced memory optimization in FortiGate-managed FAPs by introducing controls to limit data from rogue APs, station capabilities, rogue stations, and Bluetooth devices. This prevents rapid memory increase and enhances CAPWAP stability.

990058	FortiOS supports managing the USB port status on compatible FortiAP models.
	`conf wireless-controller wtp-profile`
	`edit <name>`
	`set usb-port {enable | disable}`
	`next`
	`end`

997048	FortiOS supports beacon protection, improving Wi-Fi security by protecting beacon frames. This helps devices connect to legitimate networks, reducing attack risks.
	`config wireless-controller vap`
	`edit <name>`
	`set beacon-protection {enable | disable}`
	`next`
	`end`

999971	Supports receiving the NAS-Filter-Rule attribute after successful WiFi 802.1X authentication. These rules can be forwarded to FortiAP to create dynamic Access Control Lists (dACLs) for the WiFi station, enhancing network access control and security.
1006398	Enhanced device matching logic based on DPP policy priority. Users can utilize the CLI to dictate the retention duration of matched devices for dynamic port or NAC policies, providing greater control over device management.

Log & Report

See Logging in the New Features Guide for more information.

Feature ID	Description
969386	FortiOS now adds an event timestamp and timezone information in the Log package header.

Network

See Network in the New Features Guide for more information.

Feature ID	Description
652281	Disable all proxy features on FortiGate models with 2 GB of RAM or less by default. Mandatory and basic mandatory category processes start on 2 GB memory platforms. Proxy dependency and multiple workers category processes start based on a configuration change on 2 GB memory platforms.
733258	Support DNS over QUIC (DoQ) and DNS over HTTP3 (DoH3) for transparent and local-in DNS modes. Connections can be established faster than with DNS over TLS (DoT) or DNS over HTTPS (DoH). Additionally, the FortiGate is now capable of handling the QUIC/TLS handshake and performing deep inspection for HTTP3 and QUIC traffic.

888417	Internal Switch Fabric (ISF) Hash Configuration Support for NP7 Platforms. This provides a new level of flexibility and control to NP7 platform users, allowing them to fine-tune network settings for optimal performance and security. These NP7 FortiGate models support this feature: FG-1800F, FG-2600F, FG-3500F, FG-4200F, and FG-4400F.
	Use the following command to configure NPU port mapping:
	`config system npu-post`
	`  config port-npu-map`
	`  edit <interface-name>`
	`  set npu-group <group-name>`
	`  next`
	`end`
	Use the following command to configure the load balancing algorithm used by the ISF to distribute traffic received by an interface to the interfaces of the NP7 processors in your FortiGate:
	`config system interface`
	`  edit <interface>`
	`  set sw-algorithm {l2 | l3 | eh | default}`
	`  next`
	`end`

962341	Support Radius Vendor-Specific Attributes (VSA) for Captive Portal redirects. This provides a smoother user experience during Captive Portal redirects, especially in environments where vendor-specific attributes are heavily used such as corporate networks or public WiFi hotspots.
963570	You can monitor ARP packets for a specific VLAN on a DHCP-snooping trusted port of a managed FortiSwitch unit and save the VLAN ID, MAC addresses, and IP addresses in the DHCP-snooping database.
964518	Selective Subnet Assignment is now supported in IPAM. This ensures that the configured IPAM pool will not utilize any subnets listed in the exclude table, providing more control and flexibility over the configuration of IPAM pools.

967653	FortiOS allows backup interval customization for DHCP leases during power cycles. This provides enhanced control and flexibility, ensuring lease preservation during events like outages or reboots.
	`config system global`
	`  set dhcp-lease-backup-interval < integer >`
	`end`

Feature ID	Description

971109	The new dhcp-relay-allow-no-end-option supports DHCP packets without an end option, enhancing our systems adaptability to diverse network conditions. In the realm of DHCP packets, the end option signifies the end of valid information in the options field. However, there may be scenarios where this end option is absent. This enhancement is designed to manage such situations effectively.
	`config system interface`
	`edit <interface>`
	`set dhcp-relay-allow-no-end-option {disable |enable}`
	`next`
	`end`

973573	You can now specify a tagged VLAN for users to be assigned to when the authentication server is unavailable. Previously, you could only specify an untagged VLAN. This feature is available with 802.1x MAC-based authentication. It is compatible with both Extensible Authentication Protocol (EAP) and MAC authentication bypass (MAB).
976152	FortiOS includes support for source IP anchoring in dial-up IPsec Tunnels. This allows the gateway to match connections based on the IPv4/IPv6 gateway address parameters, such as the subnet, address range, or country.

977097	A new CLI option allows users to choose to discard or permit IPv4 SCTP packets with zero checksums on the NP7 platform.
	`config system npu`
	`config fp-anomaly`
	`set sctp-csum-err {allow | drop | trap-to-host}`
	`end`
	`end`

978974	Users can upgrade their LTE modem firmware directly from the FortiGuard. This eliminates the need for manual downloading and uploading and provides users flexibility to schedule the upgrade.
990096	FortiOS allows multiple remote Autonomous Systems (AS) to be assigned to a single BGP neighbor group using AS path lists. This enhancement offers increased flexibility and efficiency in managing BGP configurations, especially in intricate network environments.

Operational Technology

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

Feature ID	Description
952000	Support for Modbus Serial to Modbus TCP has been added. All FortiGate rugged models equipped with a Serial RS-232 (DB9/ RJ45) interface can perform real-time monitoring, control, and coordination across your network. Industrial automation users can now transfer Modbus data more efficiently, reducing the need for extra devices and streamlining operations.

Feature ID	Description
972541	Support for IEC 60870-5-101 Serial to IEC 60870-5-104 TCP/IP transport has been added. All FortiGate rugged models equipped with a Serial RS-232 (DB9/ RJ45) interface can now perform telecontrol, teleprotection, and associated telecommunications for electric power systems over network access.

Policy & Objects

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

Feature ID	Description
807549	FortiOS supports NPU offloading for shaping ingress traffic on the NP7 platform. This improves system performance and efficiency, especially with a high volume of incoming traffic.
865786	This feature combines the policy name and ID into a unified Policy column, ensuring the ID and name are consistently visible. It also introduces the ability to move policies using their ID, simplifying management when handling large policy tables that may include hundreds of policies.

961309	The src-vip-filter in VIP now allows src-filter to be used as the destination filter for reverse SNAT rules, in addition to its traditional role in forward DNAT rules. This dual functionality simplifies bidirectional NAT, enhancing IP address mapping and translation efficiency.
	`config firewall vip`
	`edit <name>`
	`set src-filter <IP>`
	`set extip <IP>`
	`set mappedip <IP>`
	`set extintf <string>`
	`set nat-source-vip enable`
	`set src-vip-filter enable`
	`next`
	`end`

966992	FortiOS now supports a configurable interim log for PBA NAT logging. This enables continuous access to PBA event logs during an ongoing session, providing comprehensive logging throughout the session's lifespan.
	`config firewall ippool`
	`edit <name>`
	`set type port-block-allocation`
	`set pba-interim-log <integer>`
	`next`
	`end`

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

Feature ID	Description
977005	FortiOS supports DSCP Marking for Self-generated traffic, enabling the FortiGate to operate as a fully functional CPE device capable of directly connecting to the provider's network without needing a CPE router. This enhancement reduces user costs and complexity.

SD-WAN

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

Feature ID	Description
987765	Enhancements have been added to improve overall ADVPN 2.0 operation for SD-WAN, including: • The local spoke directly sends a shortcut-query to a remote spoke to trigger a shortcut after ADVPN 2.0 path management makes a path decision. • ADVPN 2.0 path management can trigger multiple shortcuts for load-balancing SD-WAN rules.Traffic can be load-balanced over these multiple shortcuts to use as much of the available WAN bandwidth as possible without wasting idle links if they are healthy. The algorithm to calculate multiple shortcuts for the load-balancing service considers transport group and in-SLA status for both local and remote parent overlays. • Spokes can automatically deactivate all shortcuts connecting to the same spoke when user traffic is not observed for a specified time interval. This is enabled by configuring a shared idle timeout setting in the IPsec VPN Phase 1 interface settings for the associated overlays.
1016452	To ensure FortiGate spoke traffic remains uninterrupted when configuration is orchestrated from the SD-WAN Overlay-as-a-Service (OaaS), there is added support for an OaaS agent on the FortiGate. The OaaS agent communicates with the OaaS controller in FortiCloud, validates and compares FortiOS configuration, and applies FortiOS configuration to the FortiGate as a transaction when it has been orchestrated from the OaaS portal. If any configuration change fails to be applied, the OaaS agent rolls back all configuration changes that were orchestrated. Secure communication between the OaaS agent and the OaaS controller is achieved using the FGFM management tunnel. The new CLI command `get oaas status` displays the detailed OaaS status.

Security Fabric

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

Feature ID	Description

789237	FortiOS supports customizing the source IP address and the outgoing interface for communication with the upstream FortiGate in the Security Fabric.
	`config system csf`
	`set source-ip <class_ip>`

Feature ID	Description
	`set upstream-interface-select-method {auto | sdwan | specify}` `end`

943352	Users can apply a FortiVoice tag dynamic address to a NAC policy.
	`config user nac-policy`
	`edit <name>`
	`set category fortivoice-tag`
	`set fortivoice-tag <string>`
	`next`
	`end`

972642	The external resource entry limit is now global. Additionally, file size restrictions now adjust according to the device model. This allows for a more flexible and optimized use of resources, tailored to the specific capabilities and requirements of different device models.

Security Profiles

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

Feature ID	Description
886575	FortiOS extends Search Engine support to Flow-based Web Filter Profiles. This introduces several features, including: Safe Search, Restrict YouTube Access, and Restrict Vimeo Access.
937178	FortiOS antivirus supports XLSB, OpenOffice, and RTF files through its CDR feature. This allows FortiGate to sanitize these files by removing active content, such as hyperlinks and embedded media, while preserving the text. It also provides an additional tool for network administrators to protect users from malicious documents.
939342	GUI support for Exact Data Match (EDM) for Data Loss Prevention. This improves the user experience during configuration and optimizes data management.
968303	Add support to control TLS connections that utilize Encrypted Client Hello (ECH), with options to block, allow, or force the client to switch to a non-ECH TLS connection by modifying DoH responses. This increases control and flexibility for managing TLS connections.

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.

Feature ID	Description

883606	FortiOS allows customers to enable or disable the INDEX extension, which appends a VDOM or an interface index in RFC tables.
	`config system snmp sysinfo`
	`  set append-index {enable | disable}`
	`end`

925233	Supports the separation of the SSHD host key and administration server certificate. This improvement introduces support for ECDSA 384 and ECDSA 256, allowing the SSHD to accommodate the most commonly used host key algorithms.
	`config system global`
	`  set ssh-hostkey-override {enable | disable}`
	`  set ssh-hostkey-password <password>`
	`  set ssh-hostkey <encrypted_private_key>`
	`end`

971546	GUI support added to control the use of CLI commands in administrator profiles.

User & Authentication

See Authentication in the New Features Guide for more information.

Feature ID	Description
951626	Support for client certificate validation and EMS tag matching has been added to the explicit proxy policy, improving user experience and security.
973805	Added support to cache the client certificate as an authentication cookie, eliminating the need for repeated authentication.

VPN

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

Feature ID	Description
951763	FortiOS supports a cross-validation mechanism for IPsec VPN, bolstering security and user authentication. This mechanism cross-checks whether the username provided by the client matches the identity field specified in the peer certificate. The identity field, which could be an Othername, RFC822Name, or CN, serves as a unique identifier for the client.
972643	FortiOS supports the TCP Encapsulation of IKE and IPsec packets across multiple vendors. This cross-vendor interoperability ensures that users can maintain a secure and efficient network, while also having the flexibility to choose the hardware that aligns best with user requirements.

Feature ID	Description
979375	FIPS-CC cipher mode is silently enabled when configured using cloud-init for AWS.
996136	FortiOS supports session resumptions for IPSec tunnel version 2. This enhances user experience by maintaining the tunnel in an idle state, allowing for uninterrupted usage even after a client resumes from sleep or when connectivity is restored after a disruption. It also removes the necessity for re-authentication when reconnecting, improving efficiency.

Upgrade information

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

FortiGate	Upgrade option	Details
Individual FortiGate devices	Manual update	Use the procedure in this topic. See also Upgrading individual devices in the FortiOS Administration Guide.
	Automatic update based on FortiGuard upgrade path	See Enabling automatic firmware updates in the FortiOS Administration Guide for details
Multiple FortiGate devices in a Fortinet Security Fabric	Manual, immediate or scheduled update based on FortiGuard upgrade path	See Fortinet Security Fabric upgrade on page 29 and Upgrading Fabric or managed devices in the FortiOS Administration Guide.

To view supported upgrade path information:

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

Fortinet Security Fabric upgrade

FortiOS 7.4.4 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 7.4.4. When Security Fabric is enabled in FortiOS 7.4.4, all FortiGate devices must be running FortiOS 7.4.4.

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 7.4.4:

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 7.4.4 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, open the Cluster Status dashboard widget 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`

GUI firmware upgrade does not respect upgrade path

When performing a firmware upgrade that requires multiple version jumps, the Follow upgrade path option in the GUI does not respect the recommended upgrade path, and instead upgrades the firmware directly to the final version. This can result in unexpected configuration loss. To upgrade a device in the GUI, upgrade to each interim version in the upgrade path individually.

For example, when upgrading from 7.0.7 to 7.0.12 the recommended upgrade path is 7.0.7 -> 7.0.9 -> 7.0.11 -> 7.0.12. To ensure that there is no configuration loss, first upgrade to 7.0.9, then 7.0.11, and then 7.0.12.

FortiOS restricts automatic firmware upgrades to FortiGate only

FortiOS 7.4.4 restricts the automatic firmware upgrades to the FortiGate only.

Automatic firmware upgrades would update the FortiGate and any connected FSW/FAP/FEX. This had caused issues with FortiAPs going into a boot loop due to reboot timing.

FortiOS 7.4.4 includes a temporary fix, restricting the automatic firmware upgrades to the FortiGate only.

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

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

This change impacts the FortiGate/FortiWiFi 40F, 60E, 60F, 80E, and 90E series devices, along with their variants, and the FortiGate-Rugged 60F (2 GB versions only). See Proxy-related features no longer supported on FortiGate 2 GB RAM models for more information.

Product integration and support

The following table lists FortiOS 7.4.4 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 0315 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	• 7.00026
IPS Engine	• 7.00536

See also:

- Virtualization environments on page 36
- Language support on page 36
- SSL VPN support on page 37
- FortiExtender modem firmware compatibility on page 37

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

Anti Virus

Bug ID	Description
948197	Large file downloads may intermittently stall when flow-based UTM and SSL deep inspection are enabled.
977634	FortiOS *High Security Alert* block page reference URL is incorrect.
977905	An issue in the WAD prevents access to SMB when an AV proxy based profile is included in a policy.
993785	When logged in as an administrator with Security Fabric access permissions set to none, trying to create a new antivirus profile on the *Security Profiles* > *Antivirus* page shows an error.

Application Control

Bug ID	Description
934197	Selected applications will disappear after searching or filtering for other applications in override.
982147	Users cannot create application control profiles using the GUI or CLI.
988029	On FortiGate, when in policy-based mode, the *Service* of a security policy cannot be changed from *Specify* to *App Default*.

Data Loss Prevention

Bug ID	Description
977334	Users cannot download files more than 5MB in size using FPX when SSL deep inspection and DLP profiles are enabled.
1007202	An upgrade issue may prevent the upload or download of large files using HTTP2.

DNS Filter

Bug ID	Description
804790	SDNS server latency increases by 15 seconds when a request times out. This increase may give a perception that this server is unreachable or has a latency value that doesn't reflect real-world conditions.
875072	The DNS filter prevents web connectivity with NPU acceleration.
1010464	When the DNS filter is enabled with `external-ip-blocklist`, the IPS Engine remains in D status for an extended period of time and causes the DNS session to end.

Endpoint Control

Bug ID	Description
937462	The *Assets - FortiClient* monitor widget still shows *online/register vpn* entry even the VPN tunnel is down.
979811	The ZTNA channel is not cleaned when overwriting old lls entries.
987456	FortiOS experiences a CPU usage issue in the daemon when connecting to an EMS that has a large amount of EMS tags.
990643	FortiGate blocks pages when browsing websites though a transparent proxy-redirect policy on SDWAN.
1007809	On FortiGate, anonpages and active(anon) pages frequently use a high amount of memory, causing FortiGate to enter into conserve mode.
1011209	The proxy policy does not work as expected when the session-ttl value is greater than the global session-ttl value.

Explicit Proxy

Bug ID	Description
830418	Website content does not load properly when using an explicit proxy.
978473	Explicit proxy policy function issues when matching external-threat feed categories.
980752	Applications on the BOX cannot be started through proxy.
983358	A memory usage issue with the SAML causes FortiGate to enter into conserve mode.
983897	Traffic that should not be matching a policy is incorrectly matching an allow policy or a deny policy.

Bug ID	Description
1001700	If explicit webproxy uses SAML authentication and the PAC file is enabled at the same time, the browser will report a too many redirects error when trying to visit any websites.
1006362	Debug daemon may be blocked while handling client connection and increases the GUI load time.
1020976	Traffic is stuck going through a web proxy policy with NTLM authentication.
1021050	RSSO authentication connection fails in explicit proxy policy.

File Filter

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

Firewall

Bug ID	Description
921658	SD-WAN IPsec egress traffic shaping is not working when traffic offloading is enabled on an NP7 unit.
951422	Unable to download files larger than 30MB using FortiGate AWS with AV and IPS enabled in proxy mode.
958311	Firewall address list may show incorrect error for an unresolved FQDN address. This is purely a GUI display issue; the FQDN address can be resolved by the FortiGate and traffic can be matched.
966466	On an FG-3001F NP7 device, packet loss occurs even on local-in traffic.
969255	On the *Policy & Objects* > *Services* page, administrators with firewall read-write permission cannot delete service entries.
970179	Unrelated route changes will cause the existing session to be marked dirty.
972473	WAD crashes when using load balancing with SSL offloading.
973388	TCP state of a session was not updated properly.
976651	On the *Policy & Objects* > *Firewall Policy* page, adding a global threat feed to a policy displays an error message - *Invalid entries* - and is not available to select in the *Source* field.
976713	A *Hello Retry Request* message is not sent from the FortiGate during an SSL offload by `config firewall ssl-server`.
977641	In transparent mode, multicast packets are not forwarded through the bridge and are dropped.
979802	On the *Policy & Objects* > *Firewall Policy* page, changing a policy action hides the *NAT* toggle, *IP pool configuration* field, and *Security Profiles* field in the GUI.

Bug ID	Description
980766	FortiGate drops traffic on unrelated firewall policies when `tcp-without-syn` is enabled.
981283	NAT64/46 HTTP virtual server does not work as expected in the policy.
981907	Global Search does not return results for a full or partial IP address search.
985057	The `set holddown-interval` command description in the CLI is incorrect.
985419	On the *Policy & Objects* > *Firewall Policy* page, the *Log violation traffic* checkbox displays as being unchecked when the policy is configured and reopened for editing. This purely a GUI display issue and does impact system operation.
987397	When creating or editing an entry on the *Policy & Objects* > *Virtual IPs* page in the GUI, if a subnet source filter is added after an IP range source filter in the *Optional Filters* section, an error message - *Invalid source filter IP address/subnet/range* - is shown and the settings cannot be saved.
991961	Address objects are not sorted in alphabetical order for address group or firewall policies.
996876	Adding IPv6 address group memberships to a policy using FortiGate REST API does not work as expected.
1008863	SNAT `type port-block-allocation` does not work as expected in NAT64.
1011438	On the *Policy & Objects* > *Firewall Policy List* page, the *Interface Pair View* does not display policies alphanumerically and by interface alias.
1012239	When creating a new policy using the GUI in TP mode, NAT is automatically enabled.
1014584	On the *Policy & Objects* > *Firewall Policy* page, firewall policies with FQDN show as *unresolved* in the table.

FortiGate 6000 and 7000 platforms

Bug ID	Description
638799	The DHCPv6 client does not work with vcluster2.
639064	On FortiGate 6000F models, there is no information on FPCs available for traffic matching the firewall policy with `srcaddr-negate` enabled.
787604	Transceiver information in unavailable for FPM/FIM2 ports in the GUI.
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.
938475	On FortiGate 7000E models, a memory usage issue occurs when multiple threads try to access VLAN group.
940541	A permanent MAC address is used instead of an HA virtual MAC address during automation.

Bug ID	Description
946399	Address entries cannot be edited using the *Edit* button from the *tooltip* pop-up window.
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.
983236	Under normal conditions, a FortiGate 6000 or 7000 may generate event log messages due to a known issue with a feature added to FortiOS 7.2 and 7.4. The feature is designed to create event log messages for certain DP channel traffic issues but also generates event log messages when the DP processor detects traffic anomalies that are part of normal traffic processing. This causes the event log messages to detect false positives that don't affect normal operation. For example, *DP channel 15 RX drop detected!* messages can be created when a routine problem is detected with a packet that would normally cause the DP processor to drop the packet. Similar discard message may also appear if the DP buffer is full.
994241	On FortiGate 7000F using FGSP and FGCP, when TCP traffic takes an asymmetric path, the TCP ACK and data packets might be dropped in NP7.
1003879	Incorrect SLBC traffic-related statistics may be displayed on the FortiGate 6000 or FortiGate 7000 GUI (for example, in a dashboard widgets). This can occur if an FPC or FPM is not correctly registered for statistic collection during startup. This is purely a GUI display issue and does not impact system operation.
1013046	On FortiGate 6000 and 7000 models, interested traffic cannot trigger the IPsec tunnel.
1025926	After a firmware upgrade, the configuration does not synchronize because the sdn connector password is unmatched.

FortiView

Bug ID	Description
941521	On the *FortiView Web Sites* page, the *Category* filter does not work in the Japanese GUI.
945448	On the *Asset Vulnerability Monitor* page, filtering by FortiClient user does not show any results.
1009287	CPU usage issue caused by ending multiple sessions using the *FortiView Sessions* page.

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.
896008	The GUI-based CLI widget has display issues on wide resolution screens.
908670	A *No language entry found for* error message occurs when loading the GUI. This is purely a GUI display issue and does not impact system function.
931486	Unexpected behavior in httpsd when the user has a lot of FQDN addresses.
957441	On the *Firmware & Registration* page, the GUI displays a *Cannot determine mkey for cmdb source entry.* error message. This is purely a GUI display issue and does not impact system function.
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.
961797	In a new page layout, changes made (saves or edits) in the Virtual IP page may produce a warning pop-up message on the screen.
964386	GUI dashboards show all the IPv6 sessions on every VDOM.
970528	The `hsts-max-age` is not enforced as set under `config system global`.
972887	The interface firewall object created automatically is not found by a firewall policy search with IP address.
974988	FortiGate GUI should not show a license expired notification due to an expired device-level FortiManager Cloud license if it still has a valid account-level FortiManager Cloud license (function is not affected).
975403	On the *System* > *Replacement Messages* page, the `?` is removed from custom replacement messages.
979508	The *Operation Technology* category cannot be turned on or off from the GUI. The option to enable and disable the *Operational Technology* category on application control profiles when hovering the mouse over the category name is missing.
981244	On the FortiGate GUI, IPsec or GRE configurations are missing when using `set type tunnel`.
983422	A GTP profile cannot be applied to policy using the GUI.
994915	The CLI GUI console is disconnected after creating a new VDOM.
996845	When saving a packet capture, the file name saves as a generic file name with no identifiable information.
1006079	When changing administrator account settings, the `trusthost10` setting is duplicated.
1006868	On the *FortiGuard* page, when setting a schedule using the *Scheduled updates* option on the GUI, the CLI displays the wrong value.
1013455	On the FortiGate GUI, inter-VDOM links are not available for packet capture.

Bug ID	Description
1013866	On FortiOS, the category action change is not saved if the category number is the same as the existing entry ID.

HA

Bug ID	Description
956577	For SSL VPN users, some endpoint logs are generated on the secondary HA vcluster VDOM.
962491	Some long lasting TCP established sessions expire on the HA secondary unit earlier than on the primary unit.
962525	In HA mode, FortiGate uses `ha-mgmt-interface` as the portal for the DNS resolver, even if this port may not able to reach the DNS server.
962681	In a three member A-P cluster, the dhcp lease list (`execute dhcp lease-list`) might be empty on secondary units.
964412	The firewall does not detect that the secondary HA unit has been upgraded and returned to the cluster.
964427	There is a session count discrepancy when the firewall is configured without NAT.
964828	Enabling HA direct prevents users from changing the interface as the `set-interface` command is hidden in the CLI.
970334	The vcluster2 on a Secondary HA unit does not use `session-sync-dev` to synchronize sessions to FGSP peer unit.
971075	The last interface belonging to the non-root management VDOM is not visible when accessing the GUI using the HA management interface.
972163	Under heavy traffic, some sessions are not fully synchronized to the FGCP secondary unit.
972896	No configuration error when restoring a configuration with incorrect `config firewall wildcard-fqdn custom` entries, resulting in an `HA-unsync` status.
974749	TCP/SCTP sessions count mismatch in an HA pair in A-P mode.
976024	VXLAN traffic does not pass through after HA cluster failover.
976160	In a FortiGate HA, the unit periodically produces a warning message for a missing sync file.
985237	Output is missing from the `diagnose sys ha vlan-hb-monitor` command.
985601	When configuring VDOMs in an HA cluster, the VDOM assigned to the VDOM link in vcluster2 active on the secondary unit is incorrect.
993849	After restoring a VDOM configuration, the HA is not synchronized.
1000001	A secondary HA unit may go into conserve mode when joining an HA cluster if the FortiGate configuration is large.

Bug ID	Description
1004215	Local out traffic from the primary HA unit uses the wrong interface when SNMP points to the secondary HA unit.

Hyperscale

Bug ID	Description
961684	When DoS policies are used and the system is under stress conditions, BGP might go down.
967017	TCP or UDP timer profiles configured using `config-system npu` may not work as intended.
975264	Hyperscale should not support threat feed addresses with the negate option.
976972	New primary can get stuck on failover with HTTP CC sessions.
981918	Hyperscale policy loses the `cgn-log-server-grp` setting with log mode per-mapping when the system reboots.
986501	When switching from a hyperscale to regular interface, the FortiGate encounters a kernel interruption during configuration.
994019	Harpin traffic may not work due to a rare situation caused by a race condition.
1016478	When modifying existing policies with a BOA loaded configuration, NPD is not working as expected.
1024313	The template for the netflow v9 log packets is not included in the configuration.

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.
968464	nTurbo passes the wrong ID to the IPS engine when the `set vrf` value is above 32.
1000223	HTTPS connections to a Virtual IP (VIP) on TCP port 8015 are incorrectly blocked by the firewall, displaying an IPS block page even when no packet from the outside to TCP port 8015 should reach the internal VIP address.
1008064	The IPS DB is not preserved when upgrading to 7.2.5 or later.

IPsec VPN

Bug ID	Description
564920	IPsec VPN fails to connect if `ftm-push` is configured.
787673	IPsec VPN types are not saved to the configuration when edited using the GUI.
914418	File transfer stops after a while when offloading is enabled.
950012	IPsec traffic may stop for the SOC4 platform due to a rare error condition.
950445	After a third-party router failover, traffic traversing the IPsec tunnel is lost.
965915	After an HA failover, static gateway IPsec routing fails.
966085	IKEv2 authorization with an invalid certificate can cause tunnel status mismatch.
968055	After an upgrade, L2TP/IPsec connections using the RIP protocol do not function as expected.
968080	Shortcut negotiation cannot trigger when traffic flows over an existing shortcut unless `auto-discovery-forwarder` is set on the spoke.
968218	When the IPsec tunnel destination MAC address is changed, tunnel traffic may stop.
968376	Changes to the IPsec tunnel type from a static to dialup user on the GUI does not change the actual configuration.
974648	Editing existing IPsec aggregate members does not update in the bundle list.
977486	On FortiGate, a Tunnel Mode IPsec VPN policy cannot be created using the GUI.
978243	Unable to send all prefixes through FortiClient using dial-up IPsec VPN split tunnel to macOS devices.
982599	When a NAT port is changed between two static IPsec endpoints, the new port cannot be applied on the tunnel.
989570	On FortiGate, firewall address groups created using the VPN wizard cannot be edited.
994115	When ASIC offload is enabled and packet size is larger than 1422, FortiGate does not generate an *ICMP Type 3, Code 4* error message.
996625	Unable to create a FortiClient dial-up VPN with certificate authentication because a peer CA certificate cannot be selected.
998229	Traffic loss is experienced on inter-region ADVPN tunnels after phase 2 rekey.
999619	The IPsec peer name check process is not working as expected when configuring static and dynamic tunnels in a certain order.
1001602	Using IPSec over back to back EMAC VLAN interfaces does not work as expected with NPU offload enabled.
1007043	Iked may experience an interruption in operation resulting in all VPN tunnels going down.
1009732	If there are more than 2000 dialup IPsec tunnel interfaces used in multiple FGT firewall polices, and IKE policy update may not able to complete before IKE watchdog timeout.

Log & Report

Bug ID	Description
872493	Disk logging files are cached in the kernel, causing high memory usage.
954565	Although there is enough disk space for logging, IPS archive full message is shown.
957130	When running version 7.2.3 of FortiGate, log retrieval speed from FortiAnalyzer is slow.
960661	FortiAnalyzer report is not available to view for the secondary unit in the HA cluster on the *Log & Report* > *Reports* page.
967692	The received traffic counter is not increasing when the traffic is HTTPS with webfilter.
972087	Logs entries are still visible in *General System Events* after being excluded from the disk logging filter.
973673	The `monitor-failure-retry-period` is not working as expected when the log daemon restarts the next oftp connection after a connection timeout.
978526	The configuration attribute `cfgattr="password[*]"` does not appear in the log when `password-policy` is enabled.
985508	SYN.ACK traffic is blocked when `set allow-traffic-redirect` is enabled.
987261	In the webfilter content block UTM log in proxy inspection mode, `sentbyte` and `rcvdbyte` are zero.
993476	FortiGate encounters a CPU usage issue after rebooting with multiple VDOMs configured.
996551	The UTM Log for blocking `unknown-content-encoding` is shown under the `utm-webfilter` when a web filter profile is not applied.
1005171	After upgrading to version 7.0.14, the system event log generates false positives for individual ports that are not used in any configuration.
1006611	FortiOS may not function as expected when the miglogd application attempts to process logs.
1008626	ReportD does not function as expected when event logs have message fields over 2000 bytes.

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.
915404	Proxyd did not account for all RFC-compliant SMTP pipelining cases.
922093	CPU usage issue in WAD caused by source port exhaustion when using WAN optimization.
926315	A web cache issue on FPX results in an unexpected disruption on FortiOS.

Bug ID	Description
947814	Too many redirects on TWPP after the second KRB keytab is configured.
955990	Captive portal reappears repeatedly in the browser after importing user credentials.
965966	An error condition occurred in WAD due to heavy HTTP video traffic when using a video filter profile with deep inspection enabled.
979361	After an upgrade, FortiOS encounters an error condition in the application daemon wad caused by an SSL cache error.
986528	The WAD process is interrupted when trying to build a local rating.
988473	On FortiGate 61E and 81E models, a daemon WAD issue causes high memory usage.
994101	SSL Logs show *certificate-probe-failed* error when web profile is enabled.
1000653	The proxy policy does not validate IP addresses in the XFF when an HTTP address is sent by AGW.
1003481	FortiGate may not work as expected due to an error condition in the daemon WAD.
1010718	The proxy policy is deleted from the configuration without notification after an upgrade.
1012965	Deep inspection and web filter for an explicit proxy policy do not work if `profile-protocol-options` has additional ports for HTTP.
1016970	High memory usage in WAD causes FortiGate to enter into conserve mode.
1020828	An HTTP2 stream issue causes an error condition in the WAD.

REST API

Bug ID	Description
964424	REST API GET `/ips/sensor/{name}` adds extra space to `locations`, `severity`, `protocol`, `os`, and `application` field values.
984499	REST API query `/api/v2/monitor/system/ha-peer` does not return the primary attribute of an HA cluster member.

Routing

Bug ID	Description
792512	The dashboard Session widget cannot display the correct IPv6 session count per VDOM.
924693	On the *Network* > *SD-WAN* > *SD-WAN Rules* page, member interfaces that are down are incorrectly shown as up. The tooltip on the interface shows the correct status.

Bug ID	Description
935886	SD-WAN packet duplication feature in force mode suddenly stops duplicating and starts to duplicate again once the FortiGate is rebooted.
943333	When SD-WAN health-check is configured, the IPv6 interface IP address of shortcut fails to be pinged.
966681	FortiGate cannot ping an IPv6 loopback address.
969671	GRE tunnel, established over a VLAN that has been created on specific interface types, may reference non-existent device indexes due to the reloading of VLANs.
974921	When creating or editing a rule on the *Network* > *Routing Objects* page, if the weight is set to *0* the changes are not saved.
977215	SD-WAN health check with state = dead moves between 100% and 0% packet loss while the state stays the same.
977327	DTLS with SSL VPN not working as expected on multiple ports that are within the same SD-WAN zone.
977751	BGP advertisement and Route-Reflector advertisement do not advertise additional routes after first table is announced and encoded.
978204	BFD/BGP dropping when `outbandwidth` is applied.
978683	The `link-down-failover` command does not bring the BGP peering down when the IPsec tunnel is brought down on the peer FortiGate.
983172	After traffic switching, ingress and egress ports do not follow the correct session.
984478	The SD-WAN Rules GUI page keeps loading.
984612	After upgrading from 7.2.5 and 7.2.6, management access and ZTNA Access Proxy do not work when accessed from external networks
985539	SD-WAN health check logs are not generated for ADVPN shortcuts.
986147	SD-WAN traffic is distributed unexpectedly on different shortcuts when in priority mode.
987360	SDWAN health checks are not deleted after all related references are removed when applied over ADVPN.
988498	Multicast traffic flow is not functioning as expected when static-join is used.
989012	The `ICMP_TIME_EXCEEDED` packet does not follow the original ICMP path displays the incorrect traceroute from the user.
989840	Issue with PIM neighborship over an IPSec tunnel with NP offload.
990211	On the *Network* > *BGP* > *Neighbor Groups* page, an error message is shown under *IPv4 Filtering* for routes that are already have in and out routes configured in the GUI.
991995	FortiGate does not remove the BGP community list when using regex.
995264	When using the BGP ORF debugging command, `received-prefix-filter` does not display an output.

Bug ID	Description
995972	When accessing the ZebOS in chroot, the ospfd does not work as expected.
1000433	The IPv6 route with dynamic gateway enabled cannot be configured after an upgrade and reboot.
1001556	VXLAN does not match SD-WAN rule when a service is specified.
1006703	OSPF logs for neighbor status are not generated when using multiple VRFs.
1009907	The OSPF daemon does not function as expected causing routing to stop working after an HA cluster failover.
1012895	The `set-regexp` command does not function as expected in the `extcommunity-list`.

Security Fabric

Bug ID	Description
789237	Support the use of loopback IP as the source for Security Fabric connections.
941728	Email notifications not working as expected for automation Reboot stitch.
956423	In HA, the primary unit may sometimes show a blank GUI screen.
958429	The webhook request header does not contain `Content-type: application/json` when using the JSON format. This causes Microsoft Teams to reject the request.
966740	On the *Security Fabric* > *Security Rating* page, the format of the *Unused Policies* test *Last Used* date is incorrect.
967842	Error message *Fail to retrieve FortiView data* displays when switching from the CSF root summary page to CSF child summary page.
968585	The automation stitch triggered by the FortiAnalyzer event handler does not work as expected.
968621	Erroneous memory allocation resulting in unexpected behavior in csfd after upgrading.
972921	The comments are not working as expected in the threat feed list for the domain threat feed.
984127	FortiGate shows the wrong notification to setup an upstream device that is not a FortiGate to the Security Fabric.
985198	The IP address threat feed connection status indicates an *Other Error*.
988526	Address object changes from the CLI of the root FortiGate in Security Fabric are not synchronized with downstream devices.
990703	In certain scenarios, dynamic addresses managed by the Azure SDN connector may be removed leading to potential network interruptions.
991462	Scheduled automation stitches for the SFTP backup is continuously triggered when `execute-security-fabric` is enabled and set to `once` or `weekly`.

Bug ID	Description
993279	Scheduled automation stitches for the SFTP backup does not generate unique backup files when `execute-security-fabric` is enabled.
994167	An issue with the csfd results in FortiGate being disconnected from the Security Fabric.
1003503	Optimizing federated auto-firmware upgrade with FortiGate, FortiSwitch, and FortiAP.

SSL VPN

Bug ID	Description
821240	Erroneous memory allocation observed in SSLVPNVD caused by a rare error condition.
905050	Intermittent behavior in samld due to an absent crucial parameter in the SP login response may lead to SSL VPN users experiencing disconnections.
906756	Update SSL VPN host check logic for unsupported OS.
951827	SSL VPN client certificate verification failed after importing the VDOM user peer CA certificate into the global VDOM.
979000	FortiGate does not execute the radius disconnect request from FortiAuthenticator.
979590	On FortiOS, the OS checklist for SSL VPN does not include macOS Monterrey 12.7.x for host check.
981121	When authenticating SSL VPN users on RADIUS with 2-factor authentication, the Framed-IP is not always assigned as expected.
981310	SSL VPN Web mode experiences intermittent traffic disruption due to the non-standard response of the users web server.
982705	When editing a security policy, the custom signature is removed from the policy.
987501	On FortiGate, the GRE tunnel stops sending traffic after an upgrade.
993822	After a SMAL user is connected to SSL VPN, an incorrect Framed-IP-Address is set in the radius accounting packet.
999378	When the GUI tries to write a QR code for the SSL VPN configuration to the file system to send in an email, it tries to write it in a read-only folder.
1022439	SAMLD encounters a memory usage issue, preventing successful login attempts on SSL VPN.

Switch Controller

Bug ID	Description
899414	On the *WiFi & Switch Controller* > *WiFi maps* page *Diagnostics and Tools* panel, and on the *WiFi & Switch Controller* > *FortiSwitch Clients* page, the status of the LACP interface is incorrectly shown as down when it is up. This is a GUI issue that does not affect the operations of the LACP interface. To view the correct status of the LACP interface, go to the *WiFi & Switch Controller* > *FortiSwitch* Ports page, or use the CLI.
911232	Security rating shows an incorrect warning for unregistered FortiSwitches on the *WiFi & Switch Controller* > *Managed FortiSwitches*.
984404	After upgrading the version 7.4.2, the FortiSwitch shows as *not registered* in the GUI.
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.
989015	The SWC switch port does not have all of the speed options compared to FortiSwitch.
991855	The `access-mode` and `storm control policy` commands are not visible in FortiGate clusters causing them to go out of synchronization and does not send updated configurations to the FortiSwitch.
995518	On the *WiFi & Switch Controller* > *Managed FortiSwitches* > *Upgrade* page, the *FortiGuard* option is not available to upgrade when new firmware is available.
1000663	The switch-controller managed-switch ports' configurations are getting removed after each reboot.

System

Bug ID	Description
733096	FG-100F HA secondary's unused ports flaps from down to up, then to down.
782710	Traffic going through a VLAN over VXLAN is not offloaded to NP7.
811367	Ports 33-35 constantly show suspect messaging in the transceiver output. Affected platforms: FG-2600F and FG-2601F.
820268	VIP traffic access to the EMAC VLAN interface uses incorrect MAC address on NP7 platform.
880271	Aggregate interface (LAG) dropping traffic.
880610	On FortiGate, the device enters into conserve mode unexpectedly due to a memory usage issue.
882131	PPPoE interface with SFP does not recover after a connectivity failure.
882187	FortiGate enters conserve mode in a few hours after enabling UTM on the policies.

Bug ID	Description
882862	LAG interface members are not shutting down when the remote end interface (one member in the LAG) is down.
883606	FortiOS allows customers to enable or disable the INDEX extension that appends the VDOM or interface index in RFC tables.
901721	In a certain edge case, traffic directed towards a VLAN interface could trigger an error condition in the kernel.
910364	CPU usage issue in miglogd caused by constant updates to the ZTNA tags.
912092	FortiGate does not send ARP probe for UDP NP-offloaded sessions.
920349	Connectivity was lost after creating new VDOM and NPU_VLINK.
921604	On the FortiGate 601F, the ports (x7) have no cables attached but the link LEDs are green.
924143	Logs for failed login attempt `lock-duration` is not consistent with the configuration.
925554	On the *Network* > *Interfaces* page, hardware and software switches show VLAN interfaces as down instead of up. The actual status of the VLAN interface can be verified using the command line.
929896	Unable to configure a 9600 baud-rate on DNP3-Proxy.
930803	Unable to monitor DSL parameters and the `get sys dsl status` command shows errors.
932002	On FortiGate 3000 models, the unit can become unresponsive until the unit goes through a power cycle caused by a CPU usage issue.
938449	In the 4.19 kernel, when a neighbor's MAC is changed, the session and IPsec tunnel cannot be flushed from the NPU.
947398	When an EMAC VLAN interface is set up on top of a redundant interface, the kernel may encounter an error when rebooting.
952284	A FortiGate with 2G of memory enters conserve mode when a node uses 20% of the memory.
953140	FG-1801F silently drops forward traffic at the NP7 modules.
954529	The `diagnose npu sniffer stop` command can lead to a traffic outage.
957135	EMAC VLAN interface uses two MAC addresses when it should only use an internally generated MAC address.
960643	IP addresses with an expired quarantine period might not be removed from quarantine.
960707	Egress shaping does not work on NP when applied on the WAN interface.
962153	A port that uses a copper-transceiver does not update the link status in real-time.
964465	Administrator with read-write permission for WiFi and read permission for network configuration cannot create SSIDs.
964820	Traffic forwarding on Dialup VPN IPSec does not work as expected when `npu-offload` is enabled.
966187	Unable to set a static ARP entry on the EMAC VLAN interface.

Bug ID	Description
968134	FortiGate 200F experiences a performance issue due to Marvell switch HOL mode.
968421	IPsec experiences traffic loss when `inbound-dscp-copy` and `npu-offload` are enabled on FFW-4401F.
971109	FortiGate does not forward requests for some devices causing VoIP devices to not get IP addresses on the network.
971404	Session expiration does not get updated for offloaded traffic between a specific host range.
971460	After an upgrade, the daemon ipldbd causes a CPU usage issue on one core.
974740	FortiGate 2600F does not set 10G ports to 100G.
974746	Changing interface settings causes the cluster to reboot and leads to a kernel interruption.
975496	FortiGate 200F slow download and upload speeds when traversing from a 1G to a 10G interface.
975895	FortiGate locks when *Configuration save mode* is set to *Manual* and triggers a reboot.
977231	An error condition occurred in fgfm caused by an out-of-band management configuration.
977688	On FortiGate, the application cmdbsvr operation is interrupted when performing a configuration backup from the GUI.
977740	Transparent-mode VDOM system switch-interface and Firewall policies deleted after a power cycle.
979957	When a FortiGate is added to FortiManager in backup mode, the ability to enable or disable *auto-firmware-update* on FortiGuard does not function as expected. This generates an error indicating the FortiGate is managed by FortiManager, despite backup mode suggesting otherwise.
981685	On the FortiGate 4400F, high CPU usage by random CPU cores in the system space.
982200	FortiGate enters into conserve mode due to excessive memory usage by Slabs.
982651	Security mode 802.1X authentication happens every hour on a hardware switch with 7.2 code.
983102	FortiGate uses one core causing CPU usage to go to 99%.
984148	The SNMP OID session count for NP6 and NP7 is not displayed.
984696	Network usage is not accurately reported by the `get system performance status` command.
985928	On FortiGate, the HA Firewall sends STP frames in a software switch when the parameters are blocked.
985978	On FortiGate, SNMP polling for NPU and related OIDs do not return any values.
986698	The NP7 should use the updated MAC address from the ARP table to forward traffic to the destination server.
986713	When restoring a FortiGate from a backup configuration, the device enters into system maintenance mode and is not accessible.
988528	With NGFW mixed traffic, the CPU usage goes to 99%.
989473	On FortiGate, the device may not work as expected due to a memory usage issue with the cmdbsvr.
989574	The `intrazone allow` setting does not function as expected if the zone has only one member.

Bug ID	Description
990409	After an upgrade on FortiOS, the kernel operation is interrupted and reboots due to a switch command issue.
990757	During an upgrade on FortiGate, the device does not continue updating past the *Disk usage changed, please wait for reboot* message during reboot.
991925	The EMAC VLAN, with a vlanid over a physical interface and a VIP configuration, has the incorrect mac address once traffic is offloaded.
995269	On FortiGate, the multicast session walker is rescheduled on the same CPU instead of the next CPU.
995395	Typo in the `set ipv6-allow-local-in-slient-drop` command.
996893	On FortiWiFi 81F-2R-3G4G-POE models, GPS service cannot be activated.
1001498	On FortiGate, TCP and UDP traffic cannot pass through with `dos-offload` enabled.
1001601	A kernel interruption on FortiGate prevents it from rebooting after an upgrade with a specific configuration.
1002766	FortiGate prevents select interface `a` as an option for traceroute, ssl, and telnet services.
1003349	CPU usage issue in WAD after upgrading from 7.4.1 to 7.4.3 when using address group member.
1004804	FortiGate running firmware 7.2.7, the device encounters an error condition in the application daemon.
1006979	FortiGate may encounter a memory usage issue on the flpold process, causing the primary and secondary units to go out of synchronization.
1007934	FortiGate may experience a memory usage issue with the node daemon once a connection is closed.
1008049	The I2C bus become stuck during an upgrade due to an error in the `switch-config-init` command.
1009853	Outgoing traffic from EMAC-VLAN uses default cos tag when traffic is not offloaded.
1011229	On FortiGate, a slab memory usage issue causes the device to enter into conserve mode.
1012518	Some FortiGate models on NP6/NP6Lite/NP6xLite platforms experience unexpected behavior due to certain traffic conditions after upgrading to 7.2.8. Traffic may be interrupted momentarily.
1015955	On FG-140E models, an interruption occurs in the kernel after an upgrade, preventing the device to properly boot up.
1018787	On FortiGate, a TCAM issue prevents ports from being mapped properly.

Upgrade

Bug ID	Description
925567	When upgrading multiple firmware versions in the GUI, the *Follow upgrade path* option does not respect the recommended upgrade path.
952828	The automatic patch upgrade feature overlooks patch release with the Feature label. Consequently, a FortiGate running 7.4.2 GA does not automatically upgrade to 7.4.3 GA.
955810	Upgrading FortiOS is unsuccessful due to *unmount shared data partition failed* error.
977281	After the FortiGate in an HA environment is upgraded using the Fabric upgrade feature, the GUI might incorrectly show the status *Downgrade to 7.2.X shortly*, even though the upgrade has completed. This is only a display issue; the Fabric upgrade will not recur unless it is manually scheduled.
981863	FortiGate encounters an error *ftar:215 Unrecognized archive format* during a firmware upgrade.
999324	FortiGate Pay-As-You-Go or On-demand VM versions cannot upload firmware using the *System* > *Firmware & Registration* > *File Upload* page.
1017519	Auto firmware-upgrade may run when a FortiGate is added to a FortiManager that is added behind a NAT.

User & Authentication

Bug ID	Description
825561	2FA push for FAC token and FTC will not start the push notification process without user input on the browser.
893475	When using the TACACS test server button in a FortiGate environment with HA-direct interface enabled, the traffic originates from the cluster interface instead of the designated ha-direct interface.
934096	If AD password policy is not met, the password change is not set without a clear message to the user.
934263	After authentication in authorization portal, page loading stalls and the user is not redirected to `set redirect-url`.
960230	After the authentication timeout setting value is reached, the *Time Left* value on the *Firewall User Monitor* > *Firewall Users* > *Time Left* page increases to thousands of days.
988958	When rsso user groups are updated, the session table is not cleared of old sessions and traffic still hits the old policy.

VM

Bug ID	Description
938382	OpenStack Queens FortiGate VM HA heartbeat on broadcast is not working as expected.
954962	The Client Hello packet is delayed connecting to FortiGate proxy-based mode and certificate inspection in an AWS GWLB environment using a GENEVE interface.
967134	An interrupt distribution issue may cause the CPU load to not be balanced on the FG-VM cores.
980683	After upgrading FortiGate, the VM license status is removed even though the VM license is still valid.
996389	AWS SDN Connector stops processing caused by the IAM external account role missing the `sts:AssumeRole`value.
998208	The FortiGate-VM system stops after sending an image to the HA secondary during an firmware upgrade due to different Flex-VM CPU license.
1006570	VPN tunnels go down due to IKE authentication loss after a firmware upgrade on the VM.

VoIP

Bug ID	Description
986431	An error condition occurs with VoIP profile deep inspections, preventing SIP TLS calls from going through.
1004894	VOIPD experiences high memory usage and enters into conserve mode.

WAN Optimization

Bug ID	Description
1017543	HTTPS over wanopt traffic cannot pass when using ssl half mode in an ssl server.

Web Filter

Bug ID	Description
983759	User internal IP address is visible on the internet through certificate.

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

WiFi Controller

Bug ID	Description
883021	Is the FortiGate 100F RFC 2865 compliant and, if yes, why does the FortiGate not always re-authenticated after the Session-Timeout value?
883938	Flooded wireless STA traffic seen in L2 tunneled VLAN (FG-1800F).
915715	On a secondary FortiGate in an HA cluster, `user` and `vlan-id` values do not show up when using the `diagnose wireless-controller wlac -d sta online` command in the CLI.
950379	The diagnostics of online FortiAPs shows *Link Down* in the trunk port *Connected Via* field when the FortiAP has an LACP connection to a FortiSwitch.
965695	Join/leave is repeated between FortiAP 421E and FortiGate 100E at multiple sites.
982626	Application httpsd does not work as expected when selecting a MPSK setting in any MPSK enabled VAP using the GUI.
983019	HA synchronization issue with FortiAP causes connectivity flapping when managed by a secondary VM.
994752	Memory usage causes secondary HA note to enter conserve mode.
998578	On FortiGate devices running 7.4.2 or 7.4.3, managed FortiAP-W2 devices might randomly go offline.
1001104	Some FortiAP 231F units show join/leave behavior after the FortiGate is upgraded to 7.2.7.
1003070	On FortiGate, the sta count is not accurate when some wireless clients connect to APs managed by FortiGate.
1018107	Unable to manage FortiAP from FortiGate.

ZTNA

Bug ID	Description
973214	An error condition in the WAD due to filter issue generates an error message.

Bug ID	Description
975342	ZTNA TFAP access using a FQDN private server does not work if a ZTNA tag is not set on the policy.
1020565	Users visiting ZTNA SaaS applications on a web browser cannot reach the page and are given an error message.

Known issues

The following issues have been identified in version 7.4.4. To inquire about a particular bug or report a bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
1028114	FortiGate cannot connect to FortiSandboxCloud when `inline content block scan mode` is set to default in an antivirus profile.
1031084	When FortiGate is in HA AA mode, the secondary unit does not connect to all FSA types for inline scanning.

Explicit Proxy

Bug ID	Description
1020976	Traffic is stuck going through a web proxy policy with NTLM authentication.
1026362	Web pages do not load when `persistent-cookie` is disabled for `session-cookie-based authentication` with *captive-portal*.

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.

FortiGate 6000 and 7000 platforms

Bug ID	Description
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.
911244	FortiGate 7000E IPv6 routes may not be synchronized correctly among FIMs and FPMs.
1006759	After an HA failover, there is no IPsec route in the kernel.
1018594	On FortiGate 7000, if `gtp-mode` is enabled and then disabled, after disabling *gtp-enhanced mode* and rebooting the device, traffic is disrupted on the FIM and cannot be recovered. **Workaround**: downgrade to version 7.2.x or 7.4.3.
1026665	On the FortiGate 7000F platform with virtual clustering enabled and syslog logging configured, when running the `diagnose log test` command from a primary vcluster VDOM, some FPMs may not send log messages to the configured syslog servers.

GUI

Bug ID	Description
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.
989512	When the number of users in the *Firewall User* monitor exceeds 2000, the search bar is no longer being displayed.

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.
961328	FortiGate does not choose a random port when set to random mode.
977376	FG-4201F has a 10% performance drop during a CPS test case with DoS policy.

Bug ID	Description
1024274	When Hyperscale logging is enabled with multicast log, the log is not sent to servers that are configured to receive multicast logs.
1024902	After FTP traffic passes, the `npu-session stat` does not display the accurate amount of actual sessions on FortiGate.
1025908	When running FGSP setup, the session count is approximately 50% less on the peer device.

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.
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.

1003830	IPsec VPN tunnel phase 2 instability after upgrading to 7.4.2 on the NP6xlite platform.
	Workaround: disable replay detection on the phase 2 interface on both sides of the IPsec VPN:
	`config vpn ipsec phase2-interface`
	`edit <name>`
	`set replay disable`
	`next`
	`end`

Proxy

Bug ID	Description
910678	CPU usage issue in WAD caused by a high number of devices being detected by the device detection feature.
933002	Memory usage issue in WAD caused by a rare error condition.

Routing

Bug ID	Description
903444	The `diagnose ip rtcache list` command is no longer supported in the FortiOS 4.19 kernel.

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.

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.

System

Bug ID	Description
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`.
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.
968618	After the upgrade to 7.4, the NP7 L2P is dropping packets at the L2TI module.
971466	FGR 60F faces packet loss with a Cisco switch directly connected to it.
1021542	FortiGate reboots twice after a factory reset when `gtp-enchanced-mode` is enabled.

Bug ID	Description
1021903	After an interface role change, the updated role does not show in the le-switch member list.
1025870	On FortiGate Rugged FGR70F-3G4G models, `wan1` and `wan2` port mode changes to `static` after a factory reset.
1029351	The OPC VM does not boot up when in native mode.

Upgrade

Bug ID	Description
1027462	When restoring an FortiGate, the 7.4.1 config file with deprecated Inline CASB entries displays errors messages and causes the confsyncd to not function as expected.
1031574	During a graceful upgrade, the confsync daemon and updated daemon encounter a memory usage issue, causing a race condition.

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.
972391	RADIUS group is not properly displayed as used.

VM

Bug ID	Description
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.
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.
1018303	ZTNA does not allow tcp-forwarding SSH traffic to pass through.
1020084	ZTNA does not failover to the standby realserver if the existing realserver cannot be reached.

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