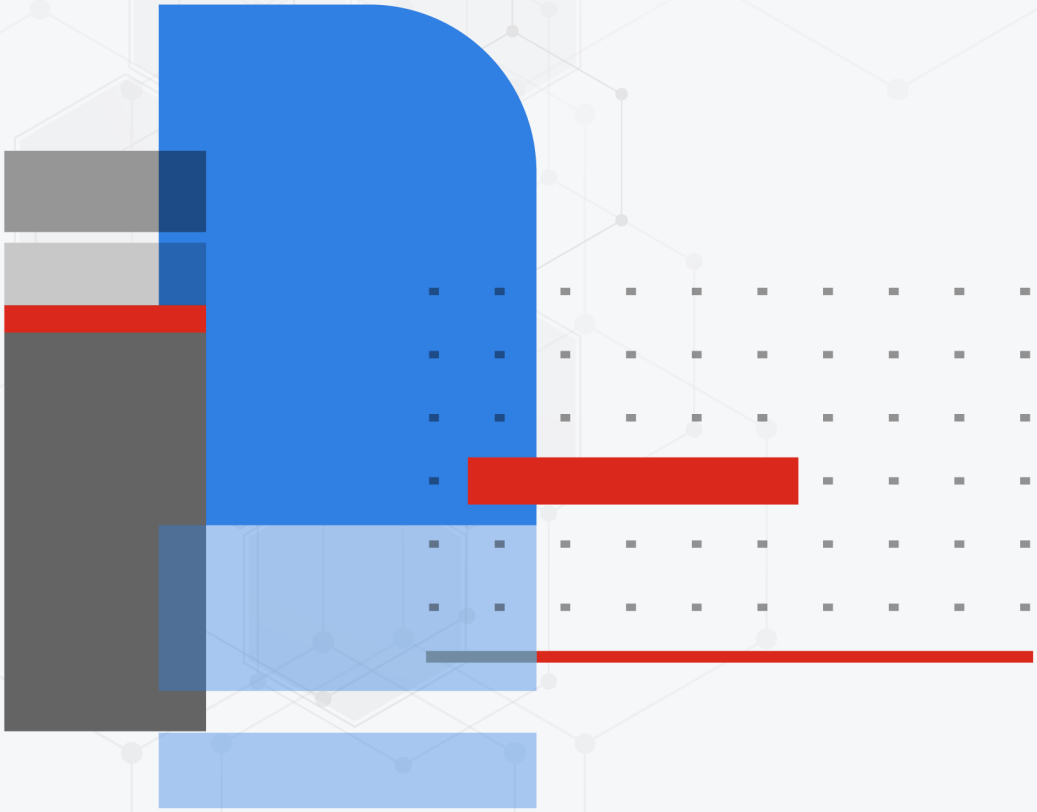
Release Notes

FortiOS 7.4.5



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

September 20, 2024
FortiOS 7.4.5 Release Notes
01-745-1060986-20240920

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-09-17	Initial release.
2024-09-18	Updated New features or enhancements on page 20, Resolved issues on page 42, Known issues on page 62, and Built-in IPS Engine on page 70.
2024-09-19	Updated Resolved issues on page 42 and Known issues on page 62.
2024-09-20	UpdatedRADIUS vulnerability on page 12 and Known issues on page 62.

Introduction and supported models

This guide provides release information for FortiOS 7.4.5 build 2702.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.4.5 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-90G, FG-91G, FG-100F, FG-101F, FG-120G, FG-121G, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-400F, FG-401F, FG-500E, FG-501E, FG-600E, FG-601E, FG-600F, FG-601F, FG-800D, FG-900D, FG-900G, FG-901G, FG-1000D, FG-1000F, FG-1001F, FG-1100E, FG-1101E, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3000F, FG-3001F, FG-3100D, FG-3200D, FG-3200F, FG-3201F, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3700F, FG-3701F, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-4800F, FG-4801F, FG-5001E, FG-5001E1, FG-6000F, FG-7000E, FG-7000F
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-80F-2R-3G4G-DSL, FWF-81F-2R, FWF-81F-2R-3G4G-DSL, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-60F, FGR-60F-3G4G, FGR-70F, FGR-70F-3G4G
FortiFirewall	FFW-1801F, FFW-2600F, FFW-3001F, FFW-3501F, FFW-3980E, FFW-4200F, FFW-4400F, FFW-4401F, FFW-4801F, FFW-VM64, FFW-VM64-KVM
FortiGate VM	FG-ARM64-AWS, FG-ARM64-AZURE, FG-ARM64-GCP, FG-ARM64-KVM, FG-ARM64-OCI, FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VM64-XEN

FortiGate 6000 and 7000 support

FortiOS 7.4.5 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 7.4.5 features.

FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 7.4.5 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.

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 FortiOS7.4.5, 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.

Local out traffic using ECMP routes could use different port or route to server

Starting from version 7.4.1, when there is ECMP routes, local out traffic may use different route/port to connect out to server. For critical traffic which is sensitive to source IP addresses, it is suggested to specify the interface or SD-WAN for the traffic since FortiOS has implemented `interface-select-method` command for nearly all local-out traffic.

```
config system fortiguard
    set interface-select-method specify
    set interface "wan1"
end
```

Hyperscale NP7 hardware limitation

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

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

RADIUS vulnerability

Fortinet has resolved a RADIUS vulnerability as described in CVE-2024-3596. As a result, firewall authentication, FortiGate administrative web UI authentication, and WiFi authentication may be affected depending on the functionality of the RADIUS server software used in your environment. RFC 3579 contains information on the affected RADIUS attribute, message-authenticator.

In order to protect against the RADIUS vulnerability described in CVE-2024-3596, as a RADIUS client, FortiGate will:

1. Force the validation of message-authenticator.
2. Reject RADIUS responses with unrecognized proxy-state attribute.

Message-authenticator checking is made mandatory under UDP/TCP. It is not mandatory when using TLS. Users are highly encouraged to use RADSEC with the RADIUS server configuration. For more information, see Configuring a RADSEC client.

If FortiGate is using UDP/TCP mode without RADSEC, the RADIUS server should be patched to ensure the message-authenticator attribute is used in its RADIUS messages.

Affected Product Integration

- FortiAuthenticator version 6.6.1 and older.

Solution

- Upgrade FortiAuthenticator to version 6.6.2 and follow the Upgrade instructions.

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.
1041367	FortiGate VMs, regardless of the number of vCPUs, now receive the IPS full extended database. The previous restriction of a minimum of eight cores is no longer applicable.

Bug ID	Description
1043962	Automatic firmware upgrade control In FOS 7.4.5 and later, the option to control automatic firmware upgrades has been updated. Previously, this option was enabled only on entry-level models and disabled by default on all other models, allowing users to manually control firmware upgrades. In 7.4.5 and later, this option is enabled by default on all FortiGate models, including FortiGate VMs. This means that the system will automatically upgrade to the latest firmware unless manually configured otherwise. Action Required: If you need to manage firmware upgrades manually, review and adjust the auto-upgrade settings according to your requirements. For more information, see Enabling automatic firmware upgrades.

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.
965490	Increase the maximum connection numbers in these FEX lan-extension controllers: • Models 60F to 100: change from 6 to 18 (2 wanext, 16 lanext) • Models 100 to 400: change from 10 to 18 (2 wanext, 16 lanext) • Models 400 to 1000: change from 10 to 34 (2 wanext, 32 lanext) • Models 1000 to 3000: change from 18 to 258 (2 wanext, 256 lanext) • Models 3000 to 7000: change from 34 to 1026 (2 wanext, 1024 lanext) • Models VM2 and VM2V: change from 6 to 18 (2 wanext, 16 lanext) • Models VM4 and VM4V: change from 10 to 34 (2 wanext, 32 lanext) • Models VM8 and VM8V: change from 18 to 258 (2 wanext, 256 lanext) • Models VM16V to VMUL: change from 34 to 1026 (2 wanext, 1024 lanext)
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.
1012680	On Entry-Level FortiGate models except 40F, increase the number of static routes and static routes6 from 100 to 250.

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.
1029721	FortiOS Azure SDN connector moves private IP on the trusted NIC during A/P HA failover.
1031828	Introduce GraphQL bulk query to FortiGate on Azure to reduce the number of API queries going out to Azure and as a result, reducing the time taken to resolve SDN connector Dynamic objects in a large environment. Configure the `FGT_VM64_AZURE` SDN connector and firewall address objects. The following IP address filters are supported: `Spoke_1 (AZ) # show` `config firewall address` `edit "AZ"` `set uuid 6b18eb16-7069-51ef-c174-58f82ee3d1b2` `set type dynamic` `set sdn "6899_AutoScale_1"` `next` `end` `Spoke_1 (AZ) # set filter` `<key1=value1> [& <key2=value2>] [| <key3=value3>]` Available filter keys are: `<Vm><Tag.><Size><Location><SecurityGroup>` `<Vnet><Subnet><ResourceGroup><ApplicationSecurityGroup><Vmss><Subscription>` `<LoadBalancer><ApplicationGateway>` `<ServiceTag><Region>` `<K8S_Cluster><K8S_Namespace><K8S_ServiceName><K8S_NodeName>` `<K8S_PodName><K8S_Region><K8S_Zone><K8S_Label.>`

LAN Edge

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

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

Feature ID	Description
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.
1006607	FortiOS WiFi controllers MPSK feature now includes both WPA2-Personal and WPA3-SAE security modes. This provides customers with more versatile security options, leveraging the MPSK feature with the latest WPA3-SAE security mode.
1012115	Support fast failover for FortiExtender. This enhancement ensures that FortiGate can swiftly recover data sessions in the event of a failover, reducing downtime and enhancing reliability.
1030088	The FortiAP sniffer includes improved packet detection, capturing all frame types across specified channel bandwidths ranging from 320 MHz to 20 MHz. This is vital for in-depth network analysis and troubleshooting, ensuring comprehensive wireless traffic examination for better network management and security.
1043784	In FortiOS, the WiFi controller supported the MPSK feature on a WPA2-Personal SSID by applying an MPSK profile or enabling RADIUS MAC authentication. However, for a WPA3-SAE SSID, the MPSK feature was only supported through the application of an MPSK profile. This enhancement allows WPA3-SAE SSIDs to utilize RADIUS MAC authentication to implement the MPSK feature.

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.

Feature ID	Description
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`
961038	Added 2.5G and 5G speed options for the 10/1 GigE RJ45 interface on the FGT2600F platform. Also added an automatic option (the new default) that automatically adjusts the port speed. Existing port speed configurations will be maintained during the firmware upgrade.
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.
985285	Enhancement to Packet Capture Functionality. This feature adds the capability to store packet capture criteria, allowing for the re-initiation of packet captures multiple times using the same parameters such as interface, filters, and more, thereby streamlining packet capture management. Additionally, this feature incorporates diagnostic commands to list, initiate, terminate, and remove GUI packet captures, enhancing the level of control users have over their packet capture operations.
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.
1049910	FortiGate now supports inspecting 802.1ah packets within a virtual wire pair configuration. This enhancement enables deep packet inspection and UTM scanning. By leveraging this capability, FortiGate can effectively analyze and inspect the 802.1ah header, perform the necessary inspection, and then re-add the header, ensuring robust protection against a wide range of cyber threats.

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.
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 NP7 and SOC5 models. This enhances system performance and efficiency, especially when there is a high volume of incoming traffic. NPU offloading for shaping ingress traffic is not supported by NP6 and SOC4 FortiGate models.
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`

Feature ID	Description
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.
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>` `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.
1007937	Support the Zstandard (zstd) compression algorithm for web content. This enhancement enables FortiOS to decode, scan, and forward zstd-encoded web content in a proxy-based policy. The content can then be passed or blocked based on the UTM profile settings. This ensures a seamless and secure browsing experience.
1012620	A FortiGate full fabric upgrade now performs upgrades by groups in the following order: 1. PoE PD (Powered Devices) 2. PSE (Power Source Equipment) and non-POE devices 3. FortiGate itself
1039849	OCI SDN connectors support IPv6 for dynamic firewall addresses and high availability failover.

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.

Feature ID	Description
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.
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`
955835	Previously, when auto-upgrade was disabled, users would receive a warning advising them to execute exec federated-upgrade cancel in order to remove any scheduled upgrades. However, with the new update, the system is now capable of autonomously canceling any pending upgrades, eliminating the need for manual user action.
957562	New feature to control the rate at which NP7 processors generate ICMPv4 and ICMPv6 error packets to prevent excessive CPU usage. This feature is enabled by default, and you can use the following options to change the configuration if required for your network conditions: `config system npu` `  config icmp-error-rate-ctrl`

Feature ID	Description
	`` set icmpv4-error-rate-limit {disable | enable} set icmpv4-error-rate <packets-per-second> set icmpv4-error-bucket-size <token-bucket-size> set icmpv6-error-rate-limit {disable | enable} set icmpv6-error-rate <packets-per-second> set icmpv6-error-bucket-size <token-bucket-size> next end ```
971546	GUI support added to control the use of CLI commands in administrator profiles.
1000368	FortiOS allows the delay-tcp-npu-session enable option to be applied globally, eliminating the need to set the command for each firewall policy, conserving resources. ``` config system global set delay-tcp-npu-session {enable | disable} end ```
1013511	This enhancement requires the kernel to verify the signed hashes of important file-system and object files during bootup. This prevents unauthorized changes to file-systems to be mounted, and other unauthorized objects to be loaded into user space on boot-up. If the signed hash verification fails, the system will halt.
1061119	This enhancement reduces ipshelper CPU usage during the database update process, optimizing system performance and ensuring smoother operations.

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.
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.
1006448	Enhanced SSL VPN security by restricting and validating HTTP messages that are used only by web mode and tunnel mode.

WiFi Controller

See Wireless in the New Features Guide for more information.

Bug ID	Description
1029522	The FortiOS WiFi controller was initially limited to integrating with the Polestar BLE-based Real-Time Location Service (RTLS), making the configuration highly specific to that single system. This enhancement supports an additional BLE-RTLS system: Evresys, providing greater flexibility and adaptability.
1044322	The FortiGate WiFi Controller now supports uploading the portal servers certificate to the FortiAP. This allows the FortiAP to use the same server certificate to secure the HTTPS POST actions. With the corresponding CA imported on users devices, authentication is smoother and free of security warnings, enhancing the user experience.

Upgrade information

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

FortiGate	Upgrade option	Details
Individual FortiGate devices	Manual update	Use the procedure in this topic. See also Upgrading individual devices in the FortiOS Administration Guide.
	Automatic update based on FortiGuard upgrade path	See Enabling automatic firmware updates in the FortiOS Administration Guide for details
Multiple FortiGate devices in a Fortinet Security Fabric	Manual, immediate or scheduled update based on FortiGuard upgrade path	See Fortinet Security Fabric upgrade on page 31 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 7.4.5 greatly increases the interoperability between other Fortinet products. This includes:

FortiAnalyzer	• 7.4.4
FortiManager	• 7.4.4
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. FortiGate devices
4. Managed FortiExtender devices
5. Managed FortiSwitch devices
6. Managed FortiAP devices
7. FortiClient EMS
8. FortiClient
9. FortiSandbox
10. FortiMail
11. FortiWeb
12. FortiNAC
13. FortiVoice
14. FortiDeceptor
15. FortiNDR
16. FortiTester
17. FortiMonitor

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.4.5. When Security Fabric is enabled in FortiOS 7.4.5, all FortiGate devices must be running FortiOS 7.4.5.

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 7.4.5:

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 7.4.5 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.

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.

FortiGate VM memory and upgrade

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

Product integration and support

The following table lists FortiOS 7.4.5 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 0318 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	• 7.00031
IPS Engine	• 7.00548

See also:

- Virtualization environments on page 38
- Language support on page 38
- SSL VPN support on page 39
- FortiExtender modem firmware compatibility on page 39

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

Anti Virus

Bug ID	Description
977905	An issue in the WAD prevents access to SMB when an AV proxy based profile is included in a policy.
1028114	FortiGate cannot connect to FortiSandboxCloud when `inline content block scan mode` is set to default in an antivirus profile.
1031084	When FortiGate is in HA AA mode, the secondary unit does not connect to all FSA types for inline scanning.
1042358	A memory usage issue in the WAD process prevents the AV Engine from loading properly.
1044961	On FortiGate, the Scanunit does not work as expected due to zlib data check issue..

Application Control

Bug ID	Description
951150	The Zoom meeting remote control feature is not blocked during meetings.

Data Loss Prevention

Bug ID	Description
1012922	When a DLP policy is set to block the upload or download of test PDF documents, the policy does not function as expected.
1036260	The DLP blocks all traffic with deep packet inspection and displays an error page.
1049719	The DLP dictionary with a regex configuration does not deny an accent mark on FortiGate.

DNS Filter

Bug ID	Description
1026058	When IP is not resolved or does not exist, the DNS alters the response for the domain and results in a performance issue on the client device.

Explicit Proxy

Bug ID	Description
890776	The GUI-explicit-proxy setting on the *System* > *Feature Visibility* page is not retained after a FortiGate reboot or upgrade.
1042125	FortiGate generates a replacement error message when the `message-upon-server-error` option is disabled.

File Filter

Bug ID	Description
900911	When `srcure-web-proxy` is enabled, if the client disconnects without sending any data as soon as the TCP connection with FortiGate is established, a WAD process signal 11 error occurs.
1004198	.exe files in ZIP archives are not blocked by file-filter profiles during CIFS file transfers.

Firewall

Bug ID	Description
807191	On FortiGate, the `diagnose netlink interface list` command shows no traffic running through the policy, even with NP offload enabled or disabled.
837866	On the NP7 platform, traffic is blocked when `egress-shaping-profile` and `outbandwidth` are enabled on a vlan parent interface.
876034	Traffic is allowed to pass through ports that are configured with a block policy.
966466	On an FG-3001F NP7 device, packet loss occurs even on local-in traffic.
992610	The source interface displays the name of the VDOM and local out traffic displays as forward traffic.

Bug ID	Description
998699	On the *Policy & Objects* > *Firewall Policy* page, the *Firewall/Network* options are missing in the GUI when enabling a security profile group in a policy.
1002269	When a schedule is added to a firewall policy, the schedule is not activated at the time configured in the policy.
1004267	On the *Policy & Objects* > *Firewall Policy* page, when searching for an address object with a comment keyword, no results are displayed.
1008680	On FortiOS, the *Dashboard* > *FortiView Destination Interfaces*, *Dashboard* > *FortiView Source Interfaces* pages, and *Policy & Objects* > *Firewall Policy* > *Edit Policy* page display incorrect bandwidth units.
1010037	When editing object address in the *Policy & Objects* > *Addresses* page on the GUI, the GUI does not function as expected if the address being edited contains a slash character.
1010824	FortiGate creates dummy destination IP logs when pinging a FortiGate VIP.
1013488	On the *Policy & Objects* > *Firewall Policy* page, searching for service port numbers in the *Firewall Policy* list does not return any results.
1022116	After editing a policy on the *Interface Pair View* window on the *Policy & Objects* > *Firewall Policy* page, the display order changes.
1034378	SMTP traffic does not egress from the same interface when a UTM profile is used in a proxy-based policy.
1036676	When a loopback interface has an IP that matches a VIP's `extip` with an `extintf "any"`, FortiGate will match the VIP but the oif loopback causes an unintended policy 0 match and drops.
1047208	The FortiGate virtual server does not setup an http2 connection with a WebSocket server due to a WAD process issue.
1058494	When `snat-hairpin-traffic` is enabled, SNAT is not automatically applied to hairpin traffic, causing a SNAT mismatch in `strict-dirty-session-check`.
1062333	FortiGate does not reply to an ARP request when VIP is disabled due to an iplist reference issue.

FortiGate 6000 and 7000 platforms

Bug ID	Description
694958	On FortiGate 7000 models, the *Power Supply* status displays as *Normal* in the GUI when there is a logged power failure.
885205	IPv6 ECMP is not supported for the FortiGate 6000F and 7000E platforms. IPv6 ECMP is supported for the FortiGate 7000F platform.
986845	On FortiOS, the *Security Fabric* widget does not display information on blade status.

Bug ID	Description
997161	On FortiGate 6000 FPCs and FortiGate 7000 FPMs the node process may consume large amounts of CPU resources, possibly affecting FPC or FPM performance. (You can run the `diagnose sys top` command from an FPC or FPM CLI to view CPU usage.) This problem may be caused by security rating result submission.
1018594	On FortiGate 7000, if `gtp-mode` is enabled and then disabled, after disabling *gtp-enhanced mode* and rebooting the device, traffic is disrupted on the FIM and cannot be recovered.
1022499	IPv6 routes are not fully synchronized between HA primary and secondary units.
1029415	On FortiGate 6000 models in an HA cluster, the secondary unit does not send out logs when an interface is configured.
1030917	FortiGate displays an erroneous error for high/low warning alarms. SFP data transfer functions as expected.
1032573	In an HA configuration, FortiGate does not respond to SNMP queries causing the device to display as being DOWN.
1033050	On FortiGate 6000 models in an HA cluster, the secondary unit does not send out automated stitch emails for certain events.
1035601	An SNMP query for policy statistics returns 0 on MBD.
1037965	When applying a script to a configuration, the updated configuration is applied to the FIM but is not fully synchronized on the FPCs.
1047553	HA remote access does not work as expected when `ha-port-dtag-mode` is double-tagging.
1057499	FIM interfaces are DOWN after restoring the root VDOM configuration due to a speed issue.

GUI

Bug ID	Description
946521	On the *System* > *Interfaces* page, the *set monitor-bandwidth* setting is not automatically disabled set when the interface bandwidth monitor for a port is deleted.
989512	When the number of users in the *Firewall User* monitor exceeds 2000, the search bar, column filters, and graphs are no longer displayed due to results being lazily loaded.
991573	In the *Assets* widget preview window of the *Asset & Identities* widget, clicking the *Refresh* button does not update the data.
992346, 993890	The `Node.JS` restarts and causes a `kill ESRCH` error on FortiGate after an upgrade.
1006079	When changing administrator account settings, the `trusthost10` setting is duplicated.
1009143	On FortiOS, the time displayed in the CLI and in the GUI do not match.

Bug ID	Description
1017181	The `Node.JS` restarts and causes an `Error: The socket was closed while data was being compressed` error.
1018682	When creating a firewall policy, applications groups with custom application signatures cannot be saved using the GUI.
1044745	On the *Dashboard* > *User & Devices* page on a VDOM, the *Address* column shows multiple devices with the FortiGate VLAN gateway instead of the Client IP.
1050865	When updating an administrator password in the GUI, the password expiration date does not update when the new password is created.
1058473	Expired licenses are still displayed in the GUI after 30 days.

HA

Bug ID	Description
825380	When workspace configuration save mode is set to *manual* in the *System* > *Settings*, configuration changes made on the primary unit and then saved do not synchronize with the secondary unit when one of the cluster units are rebooted or shutdown after the change.
998004	When the HA management interface is set a LAG, it is not synchronized to newly joining secondary HA devices.
1002682	The VMware SDN connector does not respect the `ha-direct` setting and uses the management interface, causing traffic to be dropped.
1005596	Using RADIUS login on the secondary unit does not work as expected when trying to login to the primary and secondary units at the same time.
1015950	When upgrading a FortiGate VM Analyzer, a CPU usage issue causes the auto scale cluster to go out of synchronization.
1017177	A WAD processing issue causes the SNMP to not respond in an HA cluster.
1018937	In a FortiGate HA configuration, the tunnel connection to FortiManager is disrupted due to a mismatched serial number and local certificate issue.
1024535	In an FGSP cluster configuration running in TP mode, reply traffic in asymmetric flow is not offloaded to NP.
1027149	When creating a new VDOM in an HA configuration, FortiGate may not operate as expected due to an `hasync` issue.
1029441	In an HA cluster on the SOC4 platform, the secondary unit enters a continuous rebooting cycle due to an interruption in the kernel after a firmware upgrade.
1032415	On the *System* > *HA* page, all HA vcluster device roles display as *Primary* in the *Role* column.

Bug ID	Description
1034326	In a HA cluster using FGSP mode, the primary and secondary units cannot synchronize the lease agreements due to a synchronization issue with the DHCP server.
1047094	The HA Secondary unit cannot communicate with FortiGate Cloud when it uses *standalone-mgmt-vdom* using the HA Primary unit.
1055336	Using the *Test User Credentials* button from the Radius Server in the GUI does not honor the custom `nas-id-type`.

Hyperscale

Bug ID	Description
1024902	After FTP traffic passes, the `npu-session stat` does not display the accurate amount of actual sessions on FortiGate.
1034100	The NPD process is interrupted in a Hyperscale VDOM configuration after an upgrade and sessions are not setup on hardware.

ICAP

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

Intrusion Prevention

Bug ID	Description
910267	In an FGSP setup running emix traffic, nTurbo values run in the negative.
979586	When applying an IPS profile with offloading enabled, WLAN authentication does not function as expected caused by EAP transaction timeouts.
1001860	On the *Security Profiles* > *Intrusion Prevention* page, when a new IPS filter is created with no filter selected, the *Details* column of the IPS Signatures and Filters table is blank instead of *All Attributes*.
1008107	Throughput capacity drops during failover to the secondary unit in an A/P cluster.
1011702	FortiGate experiences a CPU usage issue which may lead to an interruption in the kernel when dos-policy is enabled.

Bug ID	Description
1026354	On FortiGate, the softirq experiences a CPU usage issue with the IPSengine when traffic hits a firewall policy without an IPS profile.
1040783	FortiGate encounters CPU usage issue due to IPSEngine utilization when using an `app-ctrl utm` profile.

IPsec VPN

Bug ID	Description
942618	Traffic does not pass through an `vpn-id-ipip` IPsec tunnel when wanopt is enabled on a firewall policy.
986756	VPN traffic does not pass between VDOMs through intervdom links.
1002345	IKE daemon randomly does not operate as expected during phase1 rekeying depending on soft rekey margin, timing, and packet ordering.
1004272	On NP7 platforms that are used a hub in a hub and spoke configuration, traffic packets are dropped on IPsec tunnel spokes due to an anti-replay error.
1019269	On the *VPN* > *IPsec Tunnels* page, when language setting on FortiOS is set to anything other than English, the *Status* column displays active (green up arrow) when the tunnel is inactive.
1020250	A second IPsec tunnel cannot be added on different IP versions that use the same *peerid*.
1023871	IPSec IKEv2 with SAML cannot match the Entra ID group during EAP due to a buffer size issue.
1024558	IPsec interfaces created on `802.1ad + 802.3ad` interfaces with NP offloading enable do not work as expected after a firmware upgrade.
1025202	After a peer-side interface shutdown and reboot, the `dpd status` does not return to `OK`, even when the peer-interface is up and SA renegotiated.
1027537	On the SOC4 platform, L2TP & ETHERIP traffic does not traverse through an IPSec tunnel with NP offload enabled.
1029262	IPsec VPN traffic does not pass over the tunnel when the HA heartbeat cable is reconnected.
1031963	The firewall `hit` and `bytes` counts display values of *0* in a policy-based VPN.
1031985	IPSec VPN tunnel does not go down when the VPN peer route is removed from the routing table.
1033154	FortiGate does not unregister the `net_device` causing the unit to encounter a performance issue.
1039988	When performing a SAML authentication, authd gets stuck in a loop due to a CPU usage issue.
1042324	The Phase1 monitor BGP remains active when the tunnel is DOWN.
1050646	FortiGate does not always send the full Server Certificate Chain causing disconnections with IKEv2 VPN using the native Windows client.
1057165	The IPsec tunnel with QKD experiences flapping each time a DHCP configuration/interface update occurs.

Log & Report

Bug ID	Description
925649	An interruption may occur in the daemon locallogd when the system is in memory conserve mode.
1010244	When uploading the log file to the FTP server, some parts of the log files are not included in the upload.
1010428	On the *Log & Report* > *System Events* page, the log displays an FortiGate has experienced an unexpected power off error message when an interruption occurs in the kernel.
1011172	The miglogd does not forward log packages to FortiAnalyzer due to a memory usage issue.
1012862	User equipment IP addresses are not visible in traffic logs.
1018392	A memory usage issue in the fgtlogd daemon causes FortiGate to enter into conserve mode.
1021195	The IPS engine sends a high frequency of IoT device queries even when the device identification is set to disabled.
1025797	The `appcat` field location is inconsistently placed in the system log.
1028167	A system log message is not generated when `syslogd setting` is enabled or disabled in the GUI or CLI.
1028309	On FortiGate, a CPU usage issue occurs in the locallogd.
1034824	On the *Log & Report* > *Forward Traffic* page, application icons may not display in the *Application Name* column.
1040678	The first character User-Agent information is not included in the web filter log.
1044092	When filtering forward traffic logs using FortiAnalyzer as a source, data takes longer than expected to load and generates a memory error message.
1050071	The `unset pac-file-data` from pac-policy does not generate a system event log and the pac-file-data is deleted.
1060204	When the threat feed download times out, a system event log is not generated.

Proxy

Bug ID	Description
723764	Replacement page is not provided to client when blocking traffic from an application control profile.
871273	When the kernel API tries to access the command buffer, the device enters D state due to a kernel interruption.
933502	When a forward server with proxy authorization is configured with certain traffic, a memory usage issue in the WAD process interrupts the operation of FortiGate.

Bug ID	Description
949464	On FortiGate, a memory usage issue in the WAD process may cause the unit to enter into conserve mode.
956481	On FortiGate 6000 models, when an explicit proxy is configured, the TCP 3-way handshake does complete as expected.
982553	After upgrading from version 6.4.13 to version 7.0.12 or 7.0.13, FortiGate experiences a memory usage issue.
987483	On FortiGate, the WAD daemon does not work as expected due to a NULL pointer issue.
999118	TCP connections are not distributed properly when `src-affinity-exempt` is enabled.
1014778	When downgrading to a previous firmware version, the restoration of IoT device information results in an out of bound access interruption due to newly added `iot` attributes.
1021346	Starting from version 7.4.4, FortiOS no longer supports proxy-related features for FortiGate models with 2 GB RAM or less. When upgrading from FOS 7.4.3 or earlier to later versions, the UTM profile feature set was not properly changed from proxy to flow.
1021699	When some regex objects do not match the policy, it can result in all other objects in the same policy to not match.
1033729	An IMAP connection to an external application email server is not established in a proxy mode policy with DPI enabled.
1036201	A memory usage issue occurs in the WAD daemon process for `wad-config-notify`.
1042055	On FortiGate, an interruption occurs in the WAD process when in proxy-mode causing the unit to go into memory conserve mode.
1062516	The WAD process does not work as expected when FortiGate is configured as a HTTP load balancer with an HTTP session and changes are made to the virtual server live.
1067014	All wad-workers encounter a gradual memory usage issue, `/proc/pid/maps` shows increasing symbolic links to `/tmp/casb_shm`.

REST API

Bug ID	Description
859680	In an HA setup with vCluster, a CMDB API request to the primary cluster does not synchronize the configuration to the secondary cluster.
1014694	The `count` and `start` API request attributes that required for some API endpoints are skipped, causing the REST API to not function as expected.
1026195	When importing a certificate using API, it is not visible on FortiOS despite displaying that the import was successful.
1057999	REST API returns an HTTP 500 error when `ssl-static-key-ciphers` is enabled under `global system settings`.

Routing

Bug ID	Description
779825	In SD-WAN with `interface-select-method` enabled, if link performance is affected, local out traffic continues on the same link.
923994	On the *Network* > *Static Routes* page, VRF information does not display in the VRF column.
993843	On FortiGate 1800F models, the VXLAN tunnel on a Loopback interface does not match SD-WAN rules.
1002132	A BGP neighbor over GRE tunnel does not get established after upgrading due to anti-spoofing not functioning as expected.
1002851	BGP Stale routes do not function as expected in an HA configuration.
1003756	When creating a rule on the *Network* > *Routing Objects* page, the *Prefix-list* is set to 0.0.0.0 0.0.0.0 when an incorrect format is entered in the *Prefix* field.
1004249	FortiGate routes traffic to an interface with a physical status of DOWN.
1006753	When renewing the LTE WWAN IP, some packets are sent using the old IP address causing traffic to drop.
1008818	The default configuration of the Fabric Overlay Orchestrator causes concurrent disconnects with the BGP.
1011263	FortiGate does not advertise default route to its EBGP neighbor when `capability-default-originate` is enabled.
1013773	FortiGate does not automatically add the set LTE dynamic route to the routing table.
1020474	In a hub and spoke configuration, the IPsec SA MTU calculation does not match with the `vpn-id-ipip` encapsulation resulting in a fragmentation issue.
1021666	When adding a route using SD-WAN zone, there is no overlap check on existing gateway IP addresses which prevents routes from being added.
1022665	When the SNAT does not match the outgoing interface during failover from the secondary to the primary, SD-WAN traffic does not failover back to the primary WAN.
1023878	SD-WAN SLA shows intermittent disruptions of packet loss on all links simultaneously, even though there is no actual packet loss.
1025201	FortiGate encounters a duplication issue in a hub and spoke configuration with `set packet-duplication force` enabled on a spoke and `set packet-de-duplication` enabled on the hub.
1029460	Creating a BGP IPv4 network prefix or neighbor in the GUI unintentionally creates an empty IPv6 network prefix.
1031394	On the *Network* > *Routing Objects* page, the *Set AS path* on the *Edit Rule* pane does not allow the use of the full range AS numbers.
1042848	BGP multipath routing does not work as expected in a BGP confederation setup.
1046169	On FortiGate, outgoing traffic goes through the wrong interface for local-in traffic coming on an SDWAN interface.

Bug ID	Description
1049721	When BGP enables local-as-replace-as and there is a network loop condition, the NLRI's as-path is increased indefinitely.
1050992	IKE-SAML reply traffic does not egress from the same interface as ingress traffic when the route is present in the routing table.
1057135	The gateway/offload value of offloaded one-way UDP sessions is reset when unrelated routing changes are made.
1060456	When hovering over a vlan interface on the *SD-WAN Rules* tab on the *Network* > *SD-WAN* page, the interface shows as disabled in the SD-WAN rule even though it is active.

Security Fabric

Bug ID	Description
972921	On the *Security Fabric* > *External Connectors* page, the comments are not working as expected in the threat feed list for the domain threat feed.
987531	Threat Feed connectors in different VDOMs cannot use the source IP when using internal interfaces.
1003503	During a full fabric upgrade where a PoE powered device (PD) connected to a Power Sourcing Equipment (PSE) are upgraded, the upgrade of the PD may be interrupted if the PSE finishes upgrading first, causing a boot loop on the PD. This behavior is now avoided by performing upgrades on PDs first before upgrading PSEs and the FortiGate itself.
1007607	When creating a new IPv6 address, SDN connectors cannot be added for dynamic addresses.
1008901	STIX threat feeds cannot download properly due to a JSON parsing issue.
1014961	The SDN Connector for nutanix does not return all the entries.
1019244	The *System* > *Fabric Management* page may not load properly after an unsuccessful federated upgrade.
1019284	When optimizing a security rating, resolving an alert for one rating causes another alert to appear for another rating and the alerts cycle between both ratings continuously.
1036018	When the Security Fabric is enabled and the FortiGate is set as *root*, the *System* > *Firmware & Registration* page does not load.
1042972	Cannot test an automation stitch that uses the *Schedule* trigger from the GUI.
1056262	With a FortiGate configured with a `root-vdom` and a `mgmt-vdom`, when an automation stitch is configured for a compromised host with IP-Ban action, the IP is banned from the `mgmt-vdom`.
1057862	FortiGate models with 2GB of memory that manage many extension devices (FortiSwitches and FortiAPs) may enter conserve mode due to the GUI process experiencing a memory usage issue over time.

Bug ID	Description
1058589	Webhook requests use the same `Content-Type: application/json` in HTTP headers for all requests, even if it has a custom header.

SSL VPN

Bug ID	Description
943971	On the *VPN* > *SSL-VPN Settings* page, when renaming a selected *Restrict Access Host* object, the object is deselected.
983513	The `two-factor-fac-expiry` command is not working as expected for remote RADIUS users with a remote token set in FortiAuthenicator.
999661	When changing SSLVPN access in the *Restrict Access* field to *Allow access from any host* and enabling the *Negate Source* option on the *VPN* > *SSLVPN* page, the changes made in the GUI are not reflected in the CLI.
1003672	When RDP is accessed through SSL VPN web mode, keyboard strokes on-screen lag behind what is being typed by users.
1004633	FortiGate does not respond to ARP packets related to SSL VPN client IP addresses.
1018928	A CPU usage issue occurs in the tvc daemon when the vpn server cannot be reached.
1024584	The SSL VPN IP pool may get exhausted when `tunnel-connect-without-reauth` is enabled.
1024837	OneLogin SAML does not work as expected with SSL VPN after upgrading to 7.0.15 or 7.4.3.
1027863	NAS-IP per SSL-VPN realm does not work as expected under the `config vpn ssl web realm` after upgrading firmware.
1041202	SSL VPN does not work as expected if an LDAP user UPN exceeds 35 characters.
1042457	Duplicate log entries are created for SSL VPN when the tunnel is up or down.
1048915	The SSL VPN web mode flag is determined incorrectly causing the authenticated `POST` request to be dropped.
1061165	SSL VPN encounters a signal 11 interruption and does not work as expected due to a word-length heap memory issue.

Switch Controller

Bug ID	Description
688724	A non-default LLDP profile with a configured `med-network-policy` cannot be applied on a switch port.

Bug ID	Description
960240	On the *WiFi & Switch Controller* > *Managed FortiSwitches* page, ISL links do not display as solid connections.
1023888	On the *WiFi & Switch Controller* > *FortiSwitch Ports* page, changes made to the *Allowed VLANs* and *Native VLAN* columns are not saved when edited on the GUI.
1032105	FortiGate in an HA configuration goes out of synchronization due to a split-port interface on FortiSwitch.
1033874	FortiGate does not work as expected due an issue with a null variable in the `cu_acd`.
1042390	On the *WiFi & Switch Controller* > *SSID* page, NAC policies using a Wildcard MAC Address cannot be saved using the GUI. **Workaround**: use the CLI to perform the operation.
1052908	When the name of the FortiSwitch does not match its serial number, it shows up as *not registered* on the *System* > *Firmware & Registration* and *Security Fabric* > *Fabric Connectors* pages.
1058289	FortiGate 90G and 91G models only supports up to 8 FortiSwitches and not 24 due to table size issue.

System

Bug ID	Description
907752	On FortiGate 1000D models, the SFP 1G port randomly experiences flapping during operation.
916172	GRE traffic is still allowed to flow through when the GRE interface is disabled.
917886	On FortiGate, fragmented packets with specific flow types are not forwarded to the correct ports on a LAG interface.
948875	The passthrough GRE keepalive packets are not offloaded on NP7 platforms.
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.
966237	On NP7 platforms, egress shaping on a physical interface is not enforced on traffic according to the shaping profile definition.
966384	On FortiGate 401F and 601F models, the CR mediatype option on x5-x8 ports is not available.
967436	DAC cable between FortiGate and FortiSwitch stops working after upgrading from 7.2.6 to 7.2.7.
972170	On FortiGate 80F models, the 100FULL speed option is not available for the SPF port.
975778	VLAN traffic is stopped when created on LACP with `split-port-mode` configured.
976314	After upgrading FortiGate and not changing any configuration details, the output of `s_duplex in get hardware nic port` command displays `Half` instead of `Full`. This is purely a display issue and does not affect system operation.

Bug ID	Description
978122	FortiGate experiences packet drop when `egress-shaping-profile` is applied to a LAG interface.
981433	The ipmcsensord does not work as expected when executing sensor-related commands before the high-end device sensor finishes booting up.
986926	On the FortiGate 90xG models, the ULL interfaces for x5 - x8 are down after being set to 25G speed.
989629	FortiGate does not show additional speed options outside of *auto* on a WAN interface.
991264	The locallogd process may cause a CPU usage issue on FortiGate.
995442	FortiGate may generate a *Power Redundancy Alarm* error when there is no power loss. The error also does not show up in the system log.
995967	When FortiGate firmware is upgraded, the interface speed changes from *auto* to *1000* full.
997563	SNMP *ifSpeed* OID show values as zero on VLAN interfaces in hardware switches.
999816	FortiGate 100 models may become unresponsive and prevent access to the GUI, requiring a reboot to regain access due to an issue with the SOC3.
1000194	FortiGate does not show QoS statistics in the `diagnose netlink interface list` command when offloading is disabled in a firewall policy and IPsec phase 1 tunnel on NP7 platforms.
1001133	After an upgrade, FortiGate receives a `PSU RPS LOST` traps error despite not having any RPS connected.
1001722	VLAN/EMAC VLAN traffic is unexpectedly blocked under certain conditions.
1001938	Support Kazakhstan time zone change to a single time zone, UTC+5.
1002323	After restoring a configuration on FortiGate with the interface changed from aggregate to physical, the interface switches back to aggregate and cannot be changed back to physical.
1004883	VLAN traffic is stopped when created on LACP with `split-port-mode` configured.
1005573	FortiGate incorrectly sends `set csr` instead of `set certificate` to FortiManager after auto enrolling a certificate using SCEP.
1006024	Administrator accounts using an admin profile with only *FortiGuard Updates* read-write permissions cannot open the *FortiGuard* page.
1006685	FortiGate enters a loop cycle and generates a large number of LCAP packets when FortiGate does not receive LCAP packets from a peer device.
1008022	After a restarting FortiGate from the GUI, the `auto-nego` SFP port settings are not reflected in FortiGate.
1009278	Traffic does not hit a new policy created in the GUI or CLI due to an `auto-script` command issue.
1011968	Jumbo frame packets do not pass through all split ports and may cause packets to drop.
1015736	On FortiWiFi 60/61F models, the STATUS LED light does not turn on after rebooting the device.

Bug ID	Description
1017446	Some TTL exceeded packets are not forwarded on their destination and an error message is not always generated.
1018022	On FortiGate, VXLAN traffic is not offloaded properly resulting in some packets being dropped.
1018843	When FortiGate experiences a memory usage issue and enters into conserve mode, the system file integrity check may not work as expected and cause the device to shutdown.
1019749	On a VDOM, running `sudo global show` does not return any system interfaces information.
1020602	After configuring a virtual wire pair (VWP) setting, it is not present in FortiGate after a reboot.
1020921	When configuring an SNMP trusted host that matches the management *Admin* trusted host subnet, the GUI may give an incorrect warning that the current SNMP trusted host does not match. This is purely a GUI display issue and does not impact the actual SNMP traffic.
1021355	FortiGate encounters a CPU usage issue when there are a high volume of traffic and scripts running on the device which could lead to an issue with performance.
1021542	FortiGate reboots twice after a factory reset when `gtp-enchanced-mode` is enabled.
1021632	FortiGate may experience intermittent traffic loss on an LACP interface in a virtual wire pair with `l2forward` enabled.
1022935	FortiGate experiences a CPU usage issue when `dedicated-management-cpu` is enabled.
1024737	On FortiGate, when `set ull-port-mode` is set to 25G, ports x5-x8 show a status of DOWN.
1025503	On the *Network* > *Diagnostics* page, FortiGate shows that the packet capture capacity has been reached when there is no captured packet on the device.
1025576	Passthrough GRE traffic using Transparent Ethernet Bridging packets as the protocol type are not offloaded on NP7 platforms.
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.
1029353	The SNMP trap is not sent out when a virus is detected on the antivirus scanner.
1032018	The SFP+ port LED does not illuminate and displays a speed 10Mbps even though the link status up and speed is set to 1000Mbps.
1034286	FortiGate does not auto negotiate to `Full duplex` when connecting to FortiSwitch due to a duplication error.
1034322	FortiGates using a SOC4 platform with a virtual switch configured may continuously reboot when upgrading due to an interruption in the kernel.
1037075	On FortiGate, an interruption occurs in the kernel when running WAD process monitoring scripts.
1037393	FortiGate reboots due to the maximum buffer length difference between nTurbo and NPU HW. NPU will fragment packets which are more than 10000, but carries wrong extend info to nTurbo in the 2nd fragment.

Bug ID	Description
1041165	The MAC Authentication Bypass (MAB) does not initiate on a virtual switch due a kernel configuration issue.
1041457	The kernel 4.19 cannot concurrently reassemble IPv4 fragments for a source IP with more than 64 destination IP addresses
1041669	FortiGate does not upgrade if `private-data-encryption` is enabled and the device is not rebooted.
1043979	An interruption occurs in the kernel resulting in intermittent power disruptions and rebooting of FortiGate.
1046966	When upgrading FortiGate from version 7.4.3 to 7.4.4, if a `set vlan 3` setting is present, the device repeatedly reboots and does not boot up.
1048299	User names for some cloud-based services cannot be configured under `config system email-server` that exceed 64 characters.
1049119	FortiGate encounters an interruption in the kernel due to a NULL pointer issue.
1050908	In some scenarios, when FortiGate as a DHCP client sends out `DHCP-REQUEST` packets, the SRC IP address is set in the IP header.
1051961	On FortiGate, IP addresses cannot be assigned within a configured IP range due to a DHCP server issue.
1052004	FortiGate encounters a memory usage issue when there is no traffic running and the configuration is not fully loaded.
1053536	On FortiGate, the console displays error messages when adding Pre and Post-login banners due to a rare error condition.
1058397	On FortiGate 900 models, when the baudrate is configured, the changes are not applied and is set to 9600.
1061334	FortiGate returns a string with a *%* sign for the OID *1.3.6.1.4.1.12356.101.4.8.2.1.8* (*fgLinkMonitorPacketLoss*).
1061413	`EXPIRE` dates are not displayed properly when executing the `get sys fortiguard-service status` command due to a formatting issue.
1065969	FortiGate does not boot after restoring a configuration file containing an invalid string format.

Upgrade

Bug ID	Description
955835	When `auto-upgrade` is disabled, scheduled upgrades on FortiGate are not automatically canceled.

Bug ID	Description
1013821	On FortiGate, an interrupted occurs in the kernel in both HA FortiGates when an HA cluster's firmware is upgraded.
1025687	After a firmware upgrade, the `config system npu-post` command does not work as expected.
1027462	When restoring an FortiGate, the 7.4.1 config file with deprecated Inline CASB entries displays errors messages and causes the `confsyncd` to not function as expected.
1031574	During a graceful upgrade, the confsync daemon and updated daemon encounter a memory usage issue, causing a race condition.
1055486	On the *Firmware and Registration* page, when performing a Fabric Upgrade using the GUI for the whole Fabric topology that includes managed FortiAPs and FortiSwitches, the root FortiGate may use an incorrect recommended image for FortiAP and FortiSwitch due to a parsing issue.

User & Authentication

Bug ID	Description
974298	When using the local-in firewall authentication with SAML method, SAML users cannot get access using the authentication portal.
989760	On the *System* > *Certificates* page, error Unable to create certificate displays when uploading certificates using the PKCS12 (.pfx) format. The certificates are still uploaded.
1001026	Users are unable to use passwords that contain the *ñ* character for authentication.
1004258	The Strict-SNI SSL Profile might block connections even if SNI and Certificate CN match.
1009213	After upgrading firmware on FortiGate, an interruption occurs in the fnbamd resulting in auto-connect not working as expected.
1009884	FortiGate encounters a CPU usage issue in the `authd` process after a firmware upgrade.
1016112	SSL VPN access is prevented when the LDAP server includes a two-factor authentication filter.
1018846	When SCEP is used with SSL connections, some TLS connections are missing the SNI extension on FortiGate.
1021157	Users are unable to use passwords that contain Polish characters *ńżźćłśąó* for RADIUS authentication.
1023605	Multiple errors observed in the IOTD debug log caused by connection timeouts.
1034898	After a firmware upgrade, FortiToken does not work as expected when using the GUI.
1036265	The `reply-to` option under `config system alertmail` is removed even for `custom mail-servers` with 2-factor authentication after an upgrade.
1039004	The `username-case-sensitive disable` setting is not respected for RSSO when a username has a capital letter.

Bug ID	Description
1039490	FortiGate does not use a policy with deep inspection enabled on SSL profiles for SWG user access.
1039663	The TACACS+ connection times out, irrespective of the `remoteauthtimeout` setting, due to an issue with the `ldapconntimeout` setting, after upgrading to version 7.4.4.
1039771	FortiOS may reply to an FTM push message using a different egress interface instead of the original interface.
1050942	The Active Firewall-Authentication for 2FA FAC RADIUS users using PAP method does not work as expected after upgrading to version 7.4.4.
1060009	On FortiGate, RADSEC sent incorrect accounting packets due to a hashing issue.

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.
999599	On FortiGate AWS, the IPsec configuration goes missing after an upgrade due to an inconsistent table-size.
1006570	VPN tunnels go down due to IKE authentication loss after a firmware upgrade on the VM.
1012927	When FortiGate returns an *ICMP TTL-EXCEEDED* message, the `geneve` option field header is missing.
1016327	After rebooting, DPDK mode is disabled on a VLAN interface and traffic stops.
1030534	On FortiGate, an HA failover does not work as expected when using an OCI environment.
1036917	When a intended policy is configured for interesting traffic subnets, traffic flow hits the implicit deny rule instead of the configured policy.
1040088	In an HA configuration, the secondary unit heartbeat port is accessible even though access to the interface is not allowed on that unit.

Bug ID	Description
1046696	A FortiGate VM HA in Azure Cloud may intermittently go out of synchronization due to an issue in the daemon process.
1054244	FortiToken does not work as expected after moving a FortiGate-VM license to a new VM with the same serial number.
1058355	FortiGate VM Azure does not work as expected and enters into conserve mode in vWAN setup.
1073016	The OCI SDN connector cannot call the API to the Oracle service when an IAM role is enabled.

Web Application Firewall

Bug ID	Description
1071022	A matched pattern in the HTTP body cannot be blocked with a `waf` profile for some content types.

Web Filter

Bug ID	Description
975115	FortiGate prevents adding a regex string to a static URL filter table.
1026023	The webfilter and traffic logs show the incorrect realserver IP address due to a WAD process issue.
1045884	When enabling the *log all search keywords* in the web filter profile and VDOM mode is disabled, the *Key Word* column is not populated with data.

WiFi Controller

Bug ID	Description
908282	On FortiGate, an interruption occurs with the `cw_acd` during failover to the secondary FortiGate.
949682	Intermittent traffic disruption observed in `cw_acd` caused by a rare error condition.
989929	A kernel interruption occurs on FortiWiFi 40F/60F models when WiFi stations connect to SSID on the local radio.
1001672	FortiWiFi reboots or becomes unresponsive when connecting to SSID after upgrading to 7.0.14.
1012433	Guest WiFi clients cannot be removed using RADIUS CoA after FortiGate reboots.

Bug ID	Description
1017238	On the *WiFi & Switch Controller* > *SSIDs* page, when creating new SSIDs, settings cannot be saved with captive portal enabled and a *Portal Type* of *Disclaimer Only* or *Email Collect*.
1019680	FortiWiFi cannot access internal FAP consoles due to a login prompt issue in `diagnose sys modem com`.
1028181	Wi-Fi devices would encounter service delay when roaming over captive-portal SSID with MAC-address authentication.
1048928	Cannot retrieve DHCP IP's from the assigned VLAN when connecting Bridge SSID with RADIUS-based MAC authentication.

ZTNA

Bug ID	Description
944772	FortiGate does not use data from FortiClient to send the VPN snapshot to EMS.
998172	When first connecting to the ZTNA server, the EMS websocket can become stuck and an error displays *ZTNA Access Denied - Policy restriction!*.
1008632	When visiting SaaS application web pages using ZTNA, web pages can stall or return an *ERR_CERT_COMMON_NAME_INVALID* error.
1012317	ZTNA intermittently does not match the firewall policy due to missing information in the policy.
1018303	ZTNA does not allow tcp-forwarding SSH traffic to pass through.
1026930	An interruption occurs in the WAD process causing TCP connections to stop for ZTNA proxy policies.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
1031370	FortiOS 7.4.5 is no longer vulnerable to the following CVE Reference: • CVE-2023-51385

Known issues

Known issues are organized into the following categories:

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

New known issues

The following issues have been identified in version 7.4.5.

FortiGate 6000 and 7000 platforms

Bug ID	Description
1016439	Enabling or disabling a vcluster causes some backup routes (proto = 20) to be lost when a routing table has a significant amount of routes (over 10000 routes).
1048808	If the secondary reboots, after it rejoins the cluster SIP sessions are not resynchronized.
1056894	On FortiGate, IPv6 VRF routing tables appear under the new and old FPC primary units when the primary FPC slot is changed.
1078532	When upgrading the FG6001F platform, in some instances the slave chassis does not synchronize the FPC subscription license from master chassis. **Workaround**: use the `execute update-now` command.

GUI

Bug ID	Description
1071907	There is no setting for the type option on the GUI for npu_vlink interface.

System

Bug ID	Description
1078541	The FortiFirewall 2600F model may become stuck after a fresh image burn. Upgrading from a previous version stills works. **Workaround**: power cycle the unit.

Existing known issues

The following issues have been identified in a previous version of FortiOS and remain in FortiOS 7.4.5.

Explicit Proxy

Bug ID	Description
1026362	Web pages do not load when `persistent-cookie` is disabled for `session-cookie-based authentication` with *captive-portal*.

Firewall

Bug ID	Description
959065	On the *Policy & Objects* > *Traffic Shaping* page, when deleting or creating a shaper, the counters for the other shapers are cleared.
1007566	When the FortiGate has thousands of addresses and hundreds address groups, the GUI can take a few minutes to search for a specific address inside the address group dialog. **Workaround**: User can create the address group in the CLI instead by using the exact address name. User can also perform a search in the CLI using a partial match. For example: `config firewall addrgrp` `edit address_group` `set member <pattern>?` `next` `end`

FortiGate 6000 and 7000 platforms

Bug ID	Description
790464	After a failover, ARP entries are removed from all slots when an ARP query of single slot does not respond.
911244	FortiGate 7000E IPv6 routes may not be synchronized correctly among FIMs and FPMs.
976521	On FortiGate 6000 models, a CPU usage issue occurs in the node process when navigating a policy list with a large number (+7000) of policies in a VDOM.
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.

Bug ID	Description
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.
1056894	On FortiGate, IPv6 VRF routing tables appear under the new and old FPC primary units when the primary FPC slot is changed.
1060619	CSF is not working as expected.
1070365	FGCP HA session synchronization may stop working as expected on a FortiGate 7000F cluster managed by FortiManager. This happens if the HA configuration uses management interfaces as session synchronization interfaces by configuring the `session-sync-dev` option, for example: `config system ha` `  set session-sync-dev 1-M1 1-M2` `end` The problem occurs when FortiManager updates the configuration of the FortiGate 7000F devices in the cluster it incorrectly changes to the VDOM of the management interfaces added to the `session-sync-dev` command from `mgmt-vdom` to `vsys_ha` and the interfaces stop working as session sync interfaces. You can work around the problem by re-configuring the `session-sync-dev` option on the FortiGate 7000F cluster (this resets the VDOM of the session sync interfaces to `vsys_ha`) and then retrieving the FortiGate configuration from FortiManager. This synchronizes the correct configuration to FortiManager.

GUI

Bug ID	Description
853352	When viewing entries in slide-out window of the *Policy & Objects* > *Internet Service Database* page, users cannot scroll down to the end if there are over 100K entries.
885427	Suggest showing the SFP status information on the faceplate of FGR-60F/60F-3G4G devices.

Hyperscale

Bug ID	Description
817562	NPD/LPMD cannot differentiate the different VRFs, and considers all VRFs as 0.
896203	The parse error, `NPD-0:NPD PARSE ADDR GRP gmail.com MEMBER ERR`, appears after rebooting the system.
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.
1024274	When Hyperscale logging is enabled with multicast log, the log is not sent to servers that are configured to receive multicast logs.

Bug ID	Description
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.

Log & Report

Bug ID	Description
1010244	When uploading the log file to the FTP server, some parts of the log files are not included in the upload.

Proxy

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

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.
1021684	On the *Security Fabric* > *Physical Topology* and *Security Fabric* > *Logical Topology* pages, the topology results do not load properly and displays an error.

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.
1015698	On FortiGate 601F models, the X5 - X8 interfaces with 25G SFP28 DAC are down after upgrading to version 7.4.4 or later.
1021903	After an interface role change, the updated role does not show in the le-switch member list.

Upgrade

Bug ID	Description
955835	When `auto-upgrade` is disabled, scheduled upgrades on FortiGate are not automatically canceled. To cancel any scheduled upgrades, `exec federated-upgrade cancel` must be done manually.
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	On the *User & Authentication* > *User Definition* page, 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.
1080234	For FortiGate (versions 7.2.10 and 7.4.5 and later) and FortiNAC (versions 9.2.8 and 9.4.6 and prior) integration, when testing connectivity/user credentials against FortiNAC that acts as a RADIUS server, the FortiGate GUI and CLI returns an *invalid secret for the server* error. This error is expected when the FortiGate acts as the direct RADIUS client to the FortiNAC RADIUS server due to a change in how FortiGate handles RADIUS protocol in these versions. However, the end-to-end integration for the clients behind the FortiGate and FortiNAC is not impacted. **Workaround**: confirm the connectivity between the end clients and FortiNAC by checking if the clients can still be authorized against the FortiNAC as normal.

VM

Bug ID	Description
978021	VNI length is zero in the GENEVE header when in FTP passive mode.

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 devices (over 50). This issue does not impact FortiAP management and operation.
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.
1050915	When upgrading more than 30 managed FortiAPs at the same time using the *Managed FortiAP* page, the GUI may become slow and unresponsive when selecting the firmware.

Bug ID	Description
	Workaround: Upgrade the FortiAPs in smaller batches of up to 20 devices to avoid performance impacts.

ZTNA

Bug ID	Description
819987	SMB drive mapping made through a ZTNA access proxy is inaccessible after rebooting.
1020084	Health check on the ZTNA realserver does not work as expected if a blackhole route is added to the realserver address.

Built-in AV Engine

AV Engine 7.00026 is released as the built-in AV Engine. Refer to the AV Engine Release Notes for information.

Built-in IPS Engine

IPS Engine 7.00548 is released as the built-in IPS Engine. Refer to the IPS Engine Release Notes for information.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

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

Open source XenServer limitations

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

www.fortinet.com