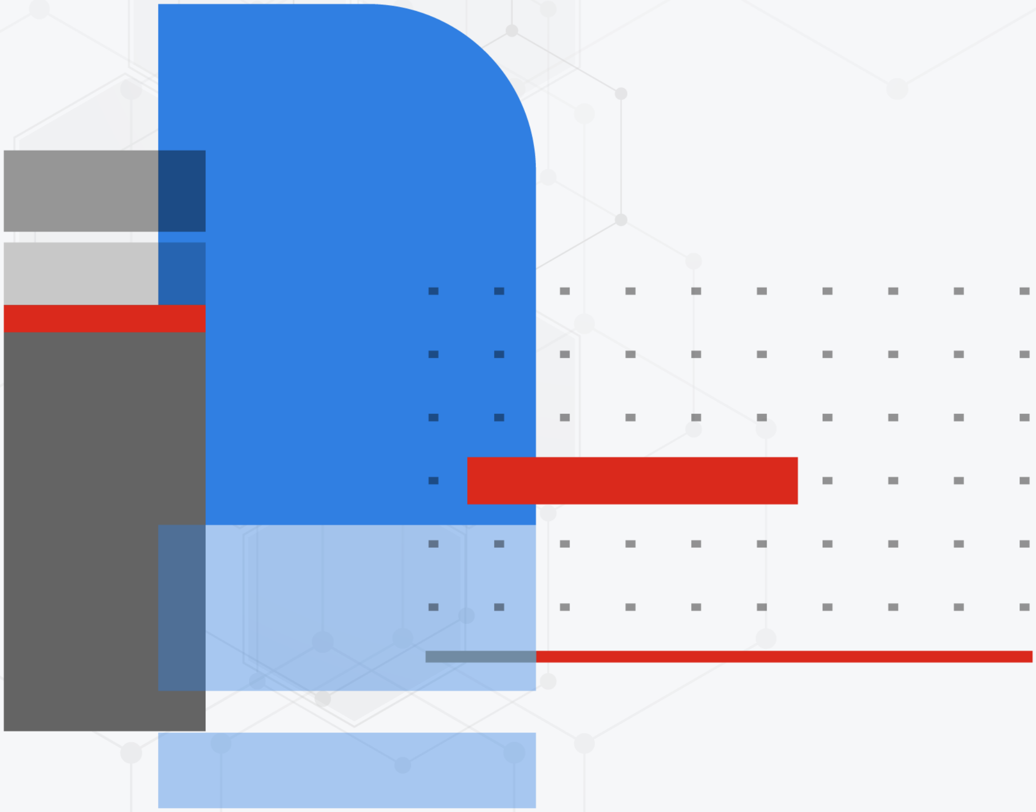
Release Notes

FortiOS 7.4.0



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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

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

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

April 17, 2024
FortiOS 7.4.0 Release Notes
01-740-879079-20240417

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-05-11	Initial release.
2023-05-12	Updated Fortinet Security Fabric upgrade on page 34.
2023-05-15	Updated Resolved issues on page 44 and Known issues on page 72.
2023-05-16	Updated Fortinet Security Fabric upgrade on page 34, Product integration and support on page 41, SSL VPN support on page 43, Resolved issues on page 44, and Known issues on page 72.
2023-05-17	Updated New features or enhancements on page 14.
2023-05-23	Updated Resolved issues on page 44 and Known issues on page 72.
2023-05-29	Updated New features or enhancements on page 14, Resolved issues on page 44, and Known issues on page 72.
2023-06-05	Updated Changes in table size on page 13, New features or enhancements on page 14, Resolved issues on page 44, and Known issues on page 72.
2023-06-12	Updated Resolved issues on page 44. Added IP pools and VIPs are not considered local addresses for certain FortiOS versions on page 10 and Remove support for SHA-1 certificate used for web management interface (GUI) on page 10.
2023-06-19	Updated Resolved issues on page 44 and Known issues on page 72.
2023-06-26	Updated Resolved issues on page 44 and Known issues on page 72.
2023-07-24	Updated New features or enhancements on page 14 and Known issues on page 72.
2023-07-31	Updated New features or enhancements on page 14 and Known issues on page 72.
2023-08-08	Updated New features or enhancements on page 14, Resolved issues on page 44, Known issues on page 72, and Built-in IPS Engine on page 82.
2023-08-17	Updated Known issues on page 72.
2023-08-21	Updated Changes in default behavior on page 12, New features or enhancements on page 14, Resolved issues on page 44, and Known issues on page 72.
2023-09-05	Updated Changes in table size on page 13, New features or enhancements on page 14, Resolved issues on page 44, and Known issues on page 72.
2023-09-06	Updated Built-in AV Engine on page 81 and Built-in IPS Engine on page 82.
2023-09-11	Updated Resolved issues on page 44. Added Number of configurable DDNS entries on page 10.
2023-09-18	Updated Known issues on page 72.

Date	Change Description
2023-10-04	Updated Changes in default behavior on page 12, Changes in table size on page 13, Resolved issues on page 44, and Known issues on page 72.
2023-10-16	Updated IP pools and VIPs are not considered local addresses for certain FortiOS versions on page 10, New features or enhancements on page 14, Resolved issues on page 44, and Known issues on page 72.
2023-10-30	Updated Resolved issues on page 44 and Known issues on page 72.
2023-11-14	Updated Resolved issues on page 44 and Known issues on page 72.
2023-11-27	Updated New features or enhancements on page 14 and Known issues on page 72.
2023-12-12	Updated New features or enhancements on page 14, Resolved issues on page 44, and Known issues on page 72.
2023-12-19	Updated Resolved issues on page 44.
2023-12-27	Updated Known issues on page 72.
2024-01-23	Updated Known issues on page 72.
2024-02-05	Updated Known issues on page 72.
2024-02-13	Updated IP pools and VIPs are not considered local addresses for certain FortiOS versions on page 10.
2024-02-20	Updated Resolved issues on page 44 and Known issues on page 72.
2024-02-23	Added BIOS-level signature and file integrity checking during downgrade on page 39.
2024-03-05	Updated New features or enhancements on page 14, Resolved issues on page 44, and Known issues on page 72.
2024-03-20	Updated Resolved issues on page 44 and Known issues on page 72.
2024-04-01	Added GUI firmware upgrade does not respect upgrade path on page 40.
2024-04-17	Updated Resolved issues on page 44 and Known issues on page 72.

Introduction and supported models

This guide provides release information for FortiOS 7.4.0 build 2360.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.4.0 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-70F, FG-71F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100F, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-400F, FG-401F, FG-500E, FG-501E, FG-600E, FG-601E, FG-600F, FG-601F, FG-800D, FG-900D, FG-1000D, 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-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-5001E, FG-5001E1, FG-6000F, FG-7000E, FG-7000F
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-60F, FGR-60F-3G4G, FGR-70F, FGR-70F-3G4G
FortiFirewall	FFW-3980E, 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 7.4.0 supports the following FG-6000F, FG-7000E, and FG-7000F models:

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

Special notices

Hyperscale incompatibilities and limitations

See Hyperscale firewall incompatibilities and limitations in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 7.4.0 features.

FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 7.4.0 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 not considered local addresses for certain FortiOS versions

For FortiOS 6.4.9 and later, 7.0.1 to 7.0.12, 7.2.0 to 7.2.5, and 7.4.0, all IP addresses used as IP pools and VIPs are not 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 not considered a destination for those IP addresses and cannot receive reply traffic at the application layer without special handling.

- This behavior affects FortiOS features in the application layer that use an IP pool as its source IP pool, including SSL VPN web mode, explicit web proxy, and the phase 1 local gateway in an interface mode IPsec VPN.
- The FortiGate will not receive reply traffic at the application layer, and the corresponding FortiOS feature will not work as desired.
- Configuring an IP pool as the source NAT IP address in a regular firewall policy works as before.

For details on the history of the behavior changes for IP pools and VIPs, and for issues and their workarounds for the affected FortiOS versions, see Technical Tip: IP pool and virtual IP behavior changes in FortiOS 6.4, 7.0, 7.2, and 7.4.

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

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

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

Number of configurable DDNS entries

Starting in FortiOS 7.4.0, the number of DDNS entries that can be configured is restricted by table size. The limits are 16, 32, and 64 entries for entry-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.

Changes in GUI behavior

Bug ID	Description
742365	Prior to this enhancement, a ZTNA configuration required configuring: • An EMS connection and EMS tags • A ZTNA server configuration • A ZTNA rules (proxy policy) • An authentication scheme and rules (optional) In this enhancement, there are now two ways to configure the ZTNA rule in the GUI. **1.** Full ZTNA policy: under *System* > *Feature Visibility*, enable *Explicit Proxy*. Under *Policy & Objects* > *Proxy Policy*, create a policy with the *ZTNA* type. **2.** Simple ZTNA policy: a regular *Firewall Policy* is used for policy management. When creating a new *Firewall Policy*, configure a ZTNA policy with *ZTNA* mode. As a result, the *Policy & Objects* > *ZTNA* > *ZTNA rules* tab has been removed. Existing ZTNA rules now appear in *Policy & Objects* > *Proxy Policy* after upgrade.
804656	Simplify automation triggers and actions for better management: • Hide simple triggers and actions that should be reused from the creation page. • Add shortcut to create automation rule from the *Log & Report* > *System Events* page.
811852	Combine the *Device Inventory* widget and *Asset Identity Center* to create a more streamlined appearance and conserve resources. The *Asset Identity Center* offers a unified view of asset information, consolidates data from various sources, and can handle significantly larger sets of data.
860252	The *Network* > *Diagnostics* page now supports launching multiple packet captures at a time. The packet capture dialog is dockable, can be minimized, and run in the background. The minimized dialog aligns with other CLI terminals that are minimized. A new command palette feature is available for quickly changing between pages and actions using keyboard shortcuts. Activate the command palette menu by pressing `ctrl+p` (or `cmd+p` for Mac) and enter the destination page to jump to. Press `Enter` to jump to the page. Similarly, activate the command palette menu for specific actions by pressing `ctrl+shift+p` (or `cmd+shift+p` for Mac) and enter the action to take. Press `Enter` to run the action.
863212	Redesign all dashboard widgets and FortiView pages with a modern look, new graphs, and faster performance. Administrators can: • Search for dashboard widgets and FortiView pages using the global search function. They can also preview and add them to existing dashboards. • View physical and logical topologies as a dashboard menu. The performance of the managed FortiAP and WiFi client widgets has been improved.

Changes in default behavior

<table>
<tr><th>Bug ID</th><th>Description</th></tr>
<tr><td>798427</td><td>

The following enhancements have been added to the *FortiSandbox Files* FortiView monitor:

- Add a pie chart with different file statuses for disk data sources.
- Add the *Reports* view, which lists PDF reports after they are downloaded successfully.
- PDF reports are downloaded on-demand. By default, only 10 are kept in memory.
- PDFs are deleted from memory after 24 hours.

</td></tr>
<tr><td>841712</td><td>

On FortiGates licensed for hyperscale firewall features, the `config system setting` options `nat46-force-ipv4-packet-forwarding` and `nat64-force-ipv6-packet-forwarding` now also apply to NP7-offloaded traffic. The `config system npu` option `nat46-force-ipv4-packet-forwarding` has been removed.

</td></tr>
<tr><td>844004</td><td>

Change the `default ip-managed-by-fortiipam` setting to `inherit-global`.

```
config system interface
    edit <name>
        set ip-managed-by-fortiipam {enable | disable | inherit-global}
    next
end
```

The default setting inherits from the global configuration (`inherit-global`) through the relevant `manage-` option under `config system ipam`.

</td></tr>
<tr><td>864035</td><td>

When the `auto-firmware-upgrade` setting is enabled, the FortiGate checks for updates every day between the firmware upgrade time interval. When a newer firmware is found, the installation is scheduled after the upgrade delay in days (0-14, default = 3) between the firmware upgrade time interval. After a successful update, an email is sent to the account owner.

```
config system fortiguard
    set auto-firmware-upgrade {enable | disable}
    set auto-firmware-upgrade-delay <integer>
end
```

Affected platforms: FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-70F, FG-71F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FGR-60F, FGR-60F-3G4G, FGR-70F, FGR-70F-3G4G, FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ.

</td></tr>
<tr><td>883727</td><td>

For FortiGates with NP7 processors, the `policy-offload-level` option of the `config system npu` command has been removed. The policy offload level is only set using the `policy-offload-level` option of the `config system settings` command, allowing you to configure the policy offload level separately for each VDOM. By default, `policy-offload-level` is set to `disable`. You can change the `policy-offload-level` to `dos-offload`. If your FortiGate is configured for hyperscale firewall features, you can set the `policy-offload-level` to `full-offload` in a hyperscale firewall VDOM.

</td></tr>
</table>

Changes in table size

Bug ID	Description
858877	Increase the number of supported dynamic FSSO IP addresses from 100 to 3000 per dynamic FSSO group. The dynamic FSSO type addresses can be pointed to FortiManager's Universal Connector, which imports the addresses from Cisco ACI or Guardicore Centra.
861745	The number of DDNS entries that can be configured is restricted by table size, with limits of 16, 32, and 64 entries for entry-level, mid-range, and high-end FortiGate models respectively.
870538	Increase `firewall.address`, `firewall.service.group`, and `firewall.policy` table size for FG-600F and FG-601F. The new sizes are 4000, 4000, and 30000 respectively.
883103	Increase `firewall.address` from 40,000 to 50,000 for FG-1000D, FG-1100E, and FG-1101E. Increase `firewall.address` from 65,000 to 100,000 for FG-1200D, FG-1500D, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, and FG-2500E. Increase `firewall.address` from 65,000 to 150,000 for FG-2600F and FG-2601F.
891426	Increase the Geneve table size to 1024 entries, and the virtual wire pair table size to 512 entries. This enhancement provides greater flexibility and scalability for network configurations.

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
855561	Use API endpoint domain name from instance metadata to support FortiOS VM OCI DRCC region.
860965	Support the AWS T4g instance family with the FG-ARM64-AWS firmware image. Support the AWS C6a and C6in instance families with the FG-VM64-AWS firmware image.
868592	Support Saudi Cloud Computing Company (SCCC) and alibabacloud.sa domain (a standalone cloud backed by AliCloud).
881186	Support deploying VMware FortiGate VMs directly as a Zero Trust Application Gateway using the OVF template (.vapp). ZTNA related parameters such as EMS server, external and internal interface IPs, and application server mapping can be configured during OVF deployment. ZTNA policies, authentication schemes, rules, and user groups are also bootstrapped.
881898	Support the new AWS C7gn instance family with the FG-ARM64-AWS firmware image.
888303	Upgrade the AWS ENA network interface driver to 2.8.3.
894654	Support UEFI Preferred boot mode on AWS FortiGate VM models with instance types that support `--boot-mode uefi-preferred`.
926152	Support AWS Snowball Edge (SBE) devices, which are compute and storage resources at the Edge with limited connection or air-gapped entirely.

GUI

See GUI in the New Features Guide for more information.

Feature ID	Description
761507	In the *Top FortiSandbox Files* FortiView monitor, it is possible to drill down on a submitted file, and view its static and dynamic file analysis. It is possible to download the full FortiSandbox report in PDF format. This feature works with FortiGate Cloud Sandbox, FortiSandbox Cloud, and FortiSandbox appliance. FortiSandbox must be running version 3.2.1 or later.

Feature ID	Description
766712	Improve the FortiOS user experience by adding more integration of support resources for troubleshooting. Online guides, FortiOS documentation, and additional support can be accessed straight from the help menu. The FortiAnswers community can be accessed within the FortiOS interface by clicking on the link at the bottom of the global search results.

Hyperscale

Feature ID	Description

836653	On FortiGates licensed for hyperscale firewall features, the following diagnose commands display summary information for IPv4 or IPv6 hardware sessions.
	`# diagnose sys npu-session list-brief`
	`# diagnose sys npu-session list-brief6`

LAN Edge

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

Feature ID	Description
541626	Support retrieving and displaying DHCP option 82 data from managed FortiSwitches. `diagnose switch-controller switch-info option82-mapping snooping {ascii | hex} <managed_switch_serial_number> <vlan> [port]` The serial number and VLAN are required, the port is optional. Managed FortiSwitches must be running FortiSwitch 7.2.2 or later, and the managed FortiSwitches must be configured with DHCP option 82 settings.

541631	Support DHCP option 82 configuration options in the switch controller settings including circuit ID, remote ID, and other general settings used for DHCP snooping on managed FortiSwitches.
	`config switch-controller global`
	`    set dhcp-option82-format {ascii | legacy}`
	`    set dhcp-option82-circuit-id {intfname vlan hostname mode description}`
	`    set dhcp-option82-remote-id {hostname ip mac}`
	`    set dhcp-snoop-client-req {forward-untrusted | drop-untrusted}`
	`    set dhcp-snoop-client-db-exp <integer>`
	`    set dhcp-snoop-db-per-port-learn-limit <integer>`
	`end`
	Managed FortiSwitches must be running FortiSwitch 7.2.2 or later.

769722	Allow a managed FortiSwitch ID to be edited and store the device serial number as a new read-only field.

<table>
<tr><th>Feature ID</th><th>Description</th></tr>
<tr><td></td><td>

```
config switch-controller managed-switch
    edit <id>
        set sn <serial_number>
    next
end
```

The device ID can be configured to a maximum of 16 alphanumeric characters, including dashes (-) and underscores (_).
Some related `config`, `execute`, and `diagnose` commands have been modified to configure and display user-definable FortiSwitch IDs accordingly. The system data and daemons have been modified to use the new switch serial number field to ensure the existing switch controller and dependent features still work.

</td></tr>
<tr><td>805867</td><td>Increase the number of supported NAC devices to 48 times the maximum number of FortiSwitch units supported on that FortiGate model.</td></tr>
<tr><td>844011</td><td>

In managed FortiSwitch switch controller CLI commands, allow a user-configurable access control list (ACL) per port on a managed FortiSwitch to control user/system access to particular resources:

```
config switch-controller acl ingress
    edit <id>
        config action
            set drop {enable | disable}
        end
        config classifier
            set dst-ip-prefix <ip_netmask>
            set src-mac <MAC_address>
        end
    next
end
```

```
config switch-controller acl group
    edit <name>
        set ingress <id>
    next
end
```

```
config switch-controller managed-switch
    edit <switch_id>
        config ports
            edit <name>
                set acl-group <name>
            next
        end
    next
end
```

</td></tr>
</table>

Feature ID	Description
	The user-configurable ACL will be assigned to ACL group 3 in FortiSwitch. Since the range of group identifiers varies among FortiSwitch platforms, platforms that do not support group 3 may not be supported. The user-configurable ACL may conflict with an ACL implemented by other managed FortiSwitch features.

852280	Add the ability to perform multi-processing for the wireless daemon that handles all WPA authentication requests (wpad_ac) by allowing users to specify the `wpad-process-count`. The count varies by model based on the number of FortiAPs it is allowed to manage.
	`config wireless-controller global`
	`    set wpad-process-count <integer>`
	`end`

852998	Wi-Fi 5G Hz UNII-3 channels (149, 153, 157, 161, and 165) are allowed in European countries and region code E countries (with a few exceptions).

860247	Add option in `dtls-policy` for `ipsec-vpn-sn` under `config wireless-controller wtp-profile`, which automatically establishes an IPsec VPN tunnel between the FortiGate and FortiAP that carries CAPWAP data packets and includes the FortiAP serial number within this tunnel.
	`config wireless-controller wtp-profile`
	`    edit <name>`
	`        set dtls-policy {clear-text | dtls-enabled | ipsec-vpn | `**`ipsec-vpn-sn`**`}`
	`    next`
	`end`

866172	The local radio of FortiWiFi-8xF, 6xF, and 40F models when operating in client mode is now capable of connecting with a third-party SSID using WPA3-SAE or OWE security mode. This provides a more secure and robust wireless connection, ensuring data integrity and privacy.
	`config system interface`
	`    edit <name>`
	`        config wifi-networks`
	`            edit <id>`
	`                set wifi-ssid <string>`
	`                set wifi-security {wpa3-sae | owe}`
	`                set wifi-passphrase <password>`
	`            next`
	`        end`
	`    next`
	`end`

866173	FortiAP 431G and 433G models operating in single 5G mode can make use of the UNII-4 frequency band, 5.85 GHz - 5.925 GHz. Additional channels 169, 173, and 177 are provided to the user in the 5 GHz radio.
866174	The `wtp-profile` of FAP-432F, FAP-433F, FAP-U432F, and FAP-U433F models can set external antenna parameters when the corresponding external antenna is installed. `config wireless-controller wtp-profile`

Feature ID	Description

	`    edit <name>`
	`        config radio-1`
	`            set optional-antenna {none | FANT-04ABGN-0606-O-R | FANT-04ABGN-0606-P-R}`
	`        end`
	`    next`
	`end`

867444	Add support for enforcing a maximum number of FortiExtender devices in LAN extension mode per FortiGate platform. Support for enforcing a maximum number of FortiExtender devices in WAN extension mode per FortiGate platform was added in a previous version of FortiOS.

869610	Add CLI support for WPA3-SAE security mode for FortiAP wireless mesh backhaul SSIDs:
	`config wireless-controller vap`
	`    edit <name>`
	`        set mesh-backhaul enable`
	`        set ssid <string>`
	`        set security wpa3-sae`
	`        set pmf enable`
	`        set sae-h2e-only enable`
	`        set schedule <string>`
	`        set sae-password <password>`
	`    next`
	`end`
	Add support for Wi-Fi 6E FortiAP devices to configure mesh connections on 6 GHz bands using WPA3-SAE with H2E only enabled.

877392	When a FortiExtender is configured as a FortiGate LAN extension and has two uplinks to the FortiGate access controller (AC), add the ability to perform a fast fail over of the CAPWAP LAN extension control channel. Two CAPWAP sessions are established between the FortiGate and the FortiExtender: one is active,the other is in standby and when the active uplink goes down, CAPWAP changes to use the other uplink quickly. When the previously active uplink comes back up, CAPWAP continues to use the previously standby uplink used for the failover event as the control channel. To display the active and standby sessions for the CAPWAP LAN extension control channel: • On the FortiGate, use `get extender session-info` where the active session is marked as `lan-extension` and the standby session is marked as `secondary`. • On the FortiExtender, use `get extender status` where the active and standby sessions and the uplink ports are displayed when both uplinks are up, and where the active session and the uplink port is displayed when a single uplink is up.
884375	Add support for FAP-234G management.
901451	Add Miracast service option in `wireless-controller bonjour-profile` configuration.

Log & Report

Feature ID	Description
780571	Add *Logs Sent Daily* chart for remote logging sources (FortiAnalyzer, FortiGate Cloud, and FortiAnalyzer Cloud) to the *Logging & Analytics Fabric Connector* card within the *Security Fabric > Fabric Connectors* page and to the *Dashboard* as a widget for a selected remote logging source.

Network

See Network in the New Features Guide for more information.

Feature ID	Description
764122	Enable VLAN switch for FG-81F-POE.
784626	Add Multiprotocol Border Gateway Protocol Ethernet Virtual Private Network (MP-BGP EVPN) support for VXLAN, which allows for learning MAC addresses in a way that is more suitable for large deployments than flood-and-learn. MP-BGP EVPN is a standards-based control plane that supports the distribution of attached host MAC and IP addresses using MP-BGP, namely, using the EVPN address family and MAC addresses treated as routing entries in BGP. As a control plane that is separate from the data plane, MP-BGP EVPN avoids flood-and-learn in the network, and the wide use of BGP as an external gateway protocol on the internet proves its ability to scale well with large deployments. MP-BGP EVPN supports the following features: • Route type 2 (MAC/IP advertisement route) and route type 3 (inclusive multicast Ethernet tag route) • Intra-subnet communication • Single-homing use cases • VLAN-based service, namely, there is only one broadcast domain per EVPN instance (EVI). This is due to the current VXLAN design that supports a single VNI for a VXLAN interface. • EVPN running on IPv4 unicast VXLAN • Egress replication for broadcast, unknown unicast, and multicast (BUM) traffic • VXLAN MAC learning from traffic • IP address local learning • ARP suppression
812329	Support DVLAN mode 802.1ad and 802.1Q on NP7 platforms over a virtual wire pair, which provides better performance and packet processing.
829476	Support secure explicit web proxy with HTTPS connections between web clients and the FortiGate. `config web-proxy explicit` ` set secure-web-proxy {disable	enable	secure}` ` set secure-web-proxy-cert <certificate1> <certificate2> ...` ` set ssl-dh-bits {768	1024	1536	2048}`

<table>
<tr><th>Feature ID</th><th>Description</th></tr>
<tr><td></td><td>

```
end
```

</td></tr>
<tr><td>838346</td><td>Add the subscriber RSSO user and authentication server information associated with PBA sessions logs to the corresponding PBA creation event logs since these details are helpful for identifying users in CGNAT applications.</td></tr>
<tr><td>844004</td><td>

Interfaces with a LAN role, wireless network interfaces (`vap-switch` type), and FortiExtender LAN extension interfaces (`lan-extension` type) can now receive an IP address from an IPAM server without any additional configuration at the interface level in the CLI. IPAM also detects and resolves any IP conflicts that may occur on the interfaces that it manages.

```
config system ipam
    set status {enable | disable}
    set automatic-conflict-resolution {enable | disable}
    set manage-lan-addresses {enable | disable}
    set manage-lan-extension-addresses {enable | disable}
    set manage-ssid-addresses {enable | disable}
end
```

When a `manage-` option is enabled, any interface that meets the specified criteria will automatically receive an IP address from IPAM. However, if this option is disabled, interfaces that meet the criteria will not be configured by IPAM. All `manage-` options are disabled by default. The central FortiIPAM configuration can be overridden at the interface level.

```
config system interface
    edit <name>
        set ip-managed-by-fortiipam {enable | disable | inherit-global}
    next
end
```

</td></tr>
<tr><td>846399</td><td>Add 100G speed option for FG-180xF for ports 37, 38, 39, and 40. Upon firmware upgrade, existing port speed configurations are preserved.</td></tr>
<tr><td>858436</td><td>

BGP conditional advertisement allows the router to advertise a route only when certain conditions are met. Add capability on the FortiGate to cross-check prefixes and make conditional advertisements between IP address families, namely, to conditionally advertise an IPv6 prefix when an IPv4 prefix is present, or vice-versa. A global option is added in the BGP configuration settings.

```
config router bgp
    set cross-family-conditional-adv {enable | disable}
end
```

The `condition-routemap` setting can be configured with IPv4 and IPv6 route maps concurrently as conditions. IPv4 and IPv6 BGP conditional advertisement is already supported in previous versions of FortiOS.

</td></tr>
</table>

Feature ID	Description
860256	Support configuring DHCP relays on interfaces with secondary IP addresses. The FortiGate will track the number of unanswered DHCP requests for a client on the interface's primary IP. After three unanswered DHCP requests, the FortiGate will forward DHCP requests to DHCP relays configured under the secondary IP using the secondary IP address as the source. After three unanswered DHCP requests, the FortiGate will return to using the primary IP and restart the process. This feature is configured by setting `dhcp-smart-relay` within a specific port under `config system interface`, and setting `secip-relay-ip` within the `config secondaryip` settings of that port. DHCP relay targets under both the primary and secondary IP may be the same or unique. If smart relay is not configured, all requests are forwarded using the primary IP address on the interface.
861745	Add GUI support for multiple DDNS interfaces. The visibility of DDNS entries in the GUI is no longer tied to the requirement of using the FortiGuard DNS server.

868091	The DHCP shared subnet feature allows the FortiGate to act as a DHCP server that assigns IP ranges in different subnets to requests coming from the same DHCP relay agent. For example, clients on the same interface or VLAN requesting IP addresses from the DHCP relay will have their requests relayed to the FortiGate. The FortiGate may have more than one server and pool associated with the relay agent, and it assigns IP addresses from the second server when the first one is exhausted.
	`config system dhcp server`
	`    edit <id>`
	`        set shared-subnet {enable | disable}`
	`        set relay-agent <IP_address>`
	`    next`
	`end`

875169	Add capability for the FortiGate to manage the broadcast flag for its DHCP client. This feature is enabled by default.
	`config system interface`
	`    edit <name>`
	`        set mode dhcp`
	`        set dhcp-broadcast-flag {enable | disable}`
	`    next`
	`end`

875468	Enhance logging for explicit proxy traffic to improve troubleshooting the HTTP proxy status for each HTTP transaction:
	• Support monitoring HTTP header requests and responses in the UTM web filter log. This requires an SSL deep inspection profile to be configured in the corresponding firewall policy.
	• Support logging the explicit web proxy forward server name using `set log-forward-server`, which is disabled by default.
	`config web-proxy global`
	`    set log-forward-server {enable | disable}`
	`end`

Feature ID	Description
	• Support logging TCP connection failures in the traffic log when a client initiates a TCP connection to a remote host through the FortiGate and the remote host is unreachable.
876182	FortiGates have the ability to signal the LAG interface status to the peer devices when available links fall below the number of `min-links` configured on the FortiGate.

888378	On FortiGates with a cellular modem and dual SIM support, support real-time switching to passive SIM when any of the following issues arise with the active SIM:
	• Ping link monitor fails
	• Active SIM card cannot be detected
	• Modem disconnection is detected after a specified interval has elapsed
	`config system lte-modem`
	`    config sim-switch`
	`        set by-sim-state {enable | disable}`
	`        set by-connection-state {enable | disable}`
	`        set by-link-monitor {enable | disable}`
	`        set link-monitor <string>`
	`        set sim-switch-log-alert-interval <integer>`
	`        set sim-switch-log-alert-threshold <integer>`
	`        set modem-disconnection-time <integer>`
	`    end`
	`end`

Operational Technology

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

Feature ID	Description

851994	Add option to set/unset the `default-purdue-level` setting within the `system interface` configuration, and apply this default Purdue Level value to discovered assets based on the interface with which they were detected. This feature requires a FortiGuard Industrial Security Service (ISS) license on the FortiGate so the Industrial Database can be used. Device identification must be enabled on interfaces connected to OT devices.
	`config system interface`
	`    edit <name>`
	`        set default-purdue-level {1 | 1.5 | 2 | 2.5 | 3 | 3.5 | 4 | 5 | 5.5}`
	`    next`
	`end`
	By default, the `default-purdue-level` is `3`. If the asset's Purdue Level is manually overridden, then it takes precedence over this default value set in the interface.

Policy & Objects

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

<table>
<thead>
<tr><th>Feature ID</th><th>Description</th></tr>
</thead>
<tbody>
<tr><td>740416</td><td>Improve the backend of the FortiOS GUI to speed up loading of a large number of policies. This is achieved by only loading the necessary data when needed, rather than loading all the data at once. This can significantly improve performance and reduce the time it takes to load a large number of policies. A new layout has also been added for the policy list with the option to choose between the new layout and the old layout.</td></tr>
<tr><td>795814</td><td>The FortiGate has the ability to process Ethernet frames with both the Cisco Security Group Tag and VLAN tag.</td></tr>
<tr><td>795908</td><td>Add scanunit support for learning mode. The scanunit provides a more powerful file detection mechanism through full-scanning in learning mode. This improves the accuracy of the IPS engine in detecting malicious files.</td></tr>
<tr><td>823710</td><td>Supports the Port Control Protocol (PCP) by allowing the FortiGate to act as a PCP server and dynamically manage network addresses and port translations for PCP clients. The PCP server must be enabled with a pool (<code>config system pcp-server</code>). In the firewall policy, enable either <code>pcp-outbound</code> or <code>pcp-inbound</code> mode and assign the pool.</td></tr>
<tr><td>838344</td><td>A route tag (<code>route-tag</code>) firewall address object can include IPv4 or IPv6 addresses associated with a BGP route tag number, and is updated dynamically with BGP routing updates. The route tag firewall address object allows for a more dynamic and flexible configuration that does not require manual intervention to dynamic routing updates. This address object can be used wherever a firewall address can be used, such as in a firewall policy, a router policy, or an SD-WAN service rule.</td></tr>
<tr><td>838363</td><td>Internet Service Database (ISDB) on-demand mode replaces the full-sized ISDB file with a much smaller file that is downloaded onto the flash drive. This file contains only the essential entries for Internet Services. When a service is used in a firewall policy, the FortiGate queries FortiGuard to download the IP addresses and stores them on the flash drive. The FortiGate also queries the local MAC Database (MADB) for corresponding MAC information.
<pre>
config system global
    set internet-service-database on-demand
end
</pre></td></tr>
<tr><td>838535</td><td>Support matching by destination port when matching a central NAT rule if the protocols are TCP, UDP, or SCTP.</td></tr>
<tr><td>869833</td><td>Support address exclusion in firewall address groups for IPv6.
<pre>
config firewall addrgrp6
    edit <name>
        set member <name1>, <name2>, ...
        set exclude {enable | disable}
        set exclude-member <name1>, <name2> ,...
    next
end
</pre></td></tr>
</tbody>
</table>

<table>
<tr><th>Feature ID</th><th>Description</th></tr>
<tr><td>875307</td><td>

Traffic shaping now supports the following:

- Local-in and local-out traffic matching: the FortiGate can apply shaping policies to local traffic entering or leaving the firewall interface based on source and destination IP addresses, ports, protocols, and applications.
- VLAN COS matching on shaping policy: the FortiGate can use the class of service (COS) value of VLAN packets as a matching criterion for shaping policies. This enables the FortiGate to prioritize traffic based on the COS value assigned by the switch or router.
- Multi-stage VLAN COS marking: the FortiGate can configure the traffic shaper to dynamically change the COS value of outgoing VLAN packets based on the shaper profile. This allows the FortiGate to mark traffic with different COS values at different stages of the shaping process.

</td></tr>
<tr><td>875309</td><td>

A port block allocation (PBA) IP pool for NAT64 traffic can be configured in the CLI.

```
config firewall ippool
    edit <name>
        set type port-block-allocation
        set nat64 enable
    next
end
```

PBA support for NAT64 is supported for FortiGates with a hyperscale firewall license. This feature has been added to mainstream FortiOS to make it available to non-hyperscale customers, including customers running a VM version of FortiOS. Hyperscale firewall logging is designed for optimal performance and does not have the same detailed logging features as are available for non-hyperscale traffic.

</td></tr>
</table>

SD-WAN

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

<table>
<tr><th>Feature ID</th><th>Description</th></tr>
<tr><td>838343</td><td>

In an SD-WAN hub and spoke configuration where ADVPN is used, when a primary shortcut goes out of SLA, traffic switches to the backup shortcut. During idle timeout, sessions will prefer using the primary parent tunnel and try to establish a new primary shortcut. However, because it is out of SLA, traffic switches back to the backup shortcut, which causes unnecessary traffic interruption.

Add the `shortcut-stickiness` option to keep existing sessions on the established ADVPN shortcuts while they remain in SLA instead of switching to a new link every idle timeout. New sessions will be routed by the primary shortcut if it is in SLA.

```
config system sdwan
    config service
        edit <id>
            set shortcut-stickiness {enable | disable}
        next
    end
end
```

</td></tr>
</table>

<table>
<tr><th>Feature ID</th><th>Description</th></tr>
<tr><td>841590</td><td>When using FortiMonitor to detect advanced SD-WAN application performance metrics, the FortiGate can log these statistics. These logs can be sent to FortiAnalyzer and FortiManager for review and reporting. The log sending frequency is measured in seconds (0 - 3600, default = 0).
<pre>
config system sdwan
    set app-perf-log-period <integer>
end
</pre></td></tr>
<tr><td>864074</td><td>Allow better control over the source IP for local-out traffic used by each egress interface by allowing a preferred source IP to be defined in the following scenarios.
<ul>
<li>Static route configuration:
<pre>
config router static
    edit <id>
        set preferred-source <IP_address>
    next
end
</pre></li>
<li>SD-WAN member configuration:
<pre>
config system sdwan
    config members
        edit <id>
            set preferred-source <IP_address>
        next
    end
end
</pre></li>
<li>Route map configuration (so that a BGP route can support a preferred source):
<pre>
config router route-map
    edit <name>
        config rule
            edit <id>
                set set-ip-prefsrc <IP_address>
            next
        end
    next
end
</pre></li>
</ul></td></tr>
<tr><td>864130</td><td>Add support for traffic classification on SLA probes to ensure they are prioritized in times of congestion. The <code>class-id</code> is a data source (2 - 15) that is defined in the shaping policy profile.
<pre>
config system sdwan
    config health-check
        edit <name>
            set class-id <integer>
        next
    end
end
</pre></td></tr>
</table>

<table>
<tr><th>Feature ID</th><th>Description</th></tr>
<tr><td>869198</td><td>Make the health check sensitive enough to detect small amounts of packet loss by decreasing the link monitor check interval and probe timeout minimum limit down to 20 ms, which will significantly impact VOD/voice.</td></tr>
<tr><td>872934</td><td>

When ADVPN is configured on a FortiGate spoke along with maximize bandwidth (SLA) or `load-balance` mode in the CLI, then spoke-to-spoke traffic is load balanced between multiple ADVPN shortcuts only when a shortcut is within the configured SLA conditions. The SD-WAN rule must be configured with `set mode load-balance` and `set tie-break fib-best-match`.

```
config system sdwan
    config service
        edit <id>
            set mode load-balance
            set dst <name>
            config sla
                edit <name>
                    set id <integer>
                next
            end
            set priority-members <seq_num1>, <seq_num2>, ...
            set tie-break fib-best-match
        next
    end
end
```

</td></tr>
<tr><td>879047</td><td>

Steer multicast traffic by SD-WAN rules. When an SD-WAN member is out of SLA, multicast traffic can fail over to another member, and switch back when SLA recovers.

To use this feature in SD-WAN:

```
config router multicast
    config pim-sm-global
        set pim-use-sdwan {enable | disable}
    end
end
```

This feature does not support ADVPN. The following setting is added to disable the use of shortcuts.

```
config system sdwan
    config service
        edit <id>
            set shortcut {enable | disable}
        next
    end
end
```

</td></tr>
</table>

Feature ID	Description
884773	In the SD-WAN with ADVPN use case, two spokes can communicate with each other on the control plane by an ADVPN shortcut. In order to separate the control traffic from data traffic, the IKE creates a dynamic selector for health check packets sent between the spokes. BGP traffic is also matched by this dynamic IKE selector. Therefore, when spokes establish BGP peering with other spokes, the BGP traffic does not count towards the data traffic and will not impact IPsec idle timeout and shortcut tunnel tear down.

886108	VRFs and sources can be configured in SD-WAN IPv6 health checks.
	`config system sdwan`
	`   config health-check`
	`      edit <name>`
	`         set addr-mode ipv6`
	`         set vrf <vrf_id>`
	`         set source6 <IPv6_address>`
	`      next`
	`   end`
	`end`

Security Fabric

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

Feature ID	Description
785104	Add the ability to set multiple regions and compartments for a single OCI SDN connector. This reduces the number of SDN connectors needed for any given OCI environment that uses multiple regions and multiple compartments.

799982	Support adding FortiClient EMS and FortiClient EMS Cloud on a per-VDOM basis. Enabling override is necessary to add an EMS server for each VDOM.
	`config endpoint-control settings`
	`    set override {enable | disable}`
	`end`

839877	FortiPolicy can be added to the Security Fabric. When FortiPolicy joins the Security Fabric and is authorized in the *Security Fabric* widget, it appears in the Fabric topology pages. A FortiGate can grant permission to FortiPolicy to perform firewall address and policy changes. Two security rating tests for FortiPolicy have been added to the *Security Posture* scorecard.
856405	Add *MAC Address* external connector threat feed. A MAC address threat feed is a dynamic list that contains MAC addresses, MAC ranges, and MAC OUIs. The list is periodically updated from an external server and stored in text file format on an external server. After the FortiGate imports this list, it can be used as a source in firewall policies, proxy policies, and ZTNA rules. For policies in transparent mode or virtual wire pair policies, the MAC address threat feed can be used as a source or destination address.

Security Profiles

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

Feature ID	Description

766158	Introduce a multi-tiered approach to determining the action taken on a video. The channel filter is checked first, and if the video's channel matches a configuration entry, the corresponding action is taken. If not, the FortiGuard category filter is checked and the corresponding action is taken if the video's category matches a configuration entry. If neither of these conditions are met, the default action specified in the video filter profile is used. Logging is also enabled by default.
	`config videofilter profile`
	`    edit <name>`
	`        set default-action {allow | monitor | block}`
	`        set log {enable | disable}`
	`    next`
	`end`

780875	Support OT/IoT virtual patching on NAC policies by enabling the category as a *Vulnerability* and setting the match criteria based on severity. Devices that match the criteria can be assigned and isolated to a NAC VLAN.
829478	Improve replacement message displayed for YouTube videos blocked by video filtering. When a user visits a video directly by URL, a full-page replacement message is displayed. When a user loads a video from YouTube, the page will load but the replacement message will display in the video frame.
854704	FortiGate VMs with eight or more vCPUs can be configured to have a minimum of eight cores to be eligible to run the full extended database (DB). Any FortiGate VM with less than eight cores will receive a slim version of the extended DB. This slim-extended DB is a smaller version of the full extended DB, and it is designed for customers who prefer performance.

System

See System in the New Features Guide for more information.

Feature ID	Description
739200	When using `execute restore image tftp <filename-string> <tftp-server-ip>`, prevent a FortiGate with an expired support contract from performing a firmware upgrade to a higher major version such as from FortiOS 6.0 to 7.0, or a firmware upgrade to a higher minor version such as from FortiOS 7.0 to 7.2. For security updates, allow a FortiGate with an expired support contract to perform a firmware upgrade to a higher patch build such as from FortiOS 7.4.0 to 7.4.1.

Feature ID	Description
749989	FortiGates, FortiSwitches, FortiAPs, and FortiExtenders can download an EOS (end of support) package automatically from FortiGuard during the bootup process or by using manual commands. Based on the downloaded EOS package files, when a device passes the EOS date, a warning message is displayed in the device's tooltip, and the device is highlighted in the GUI. The End-of-Support security rating check rule audits the EOS of FortiGates and Fabric devices. This allows administrators to have clear visibility of their Security Fabric, and help prevent any security gaps or vulnerabilities that may arise due to any devices that are past their hardware EOS date.
754765	Add FortiConverter option in the FortiOS GUI. This provides an integrated solution for migrating configurations to a new or older FortiGate appliance directly from the FortiGate itself, without the need to access the FortiConverter portal.
836287	Support adding YAML to the file name when backing up the config as YAML, and detecting file format when restoring the configuration. The `execute restore yaml-config` command has been removed and `execute restore config` should be used. In the GUI, the *File format* field has been removed from the *Restore system Configuration* page.

852279	Add FortiGuard DLP service that offers a database with categorized predefined DLP data type patterns such as:
	• Drivers licenses for various countries, various states in the USA, and various provinces in Canada
	• Tax numbers for various countries
	• Credit card numbers
	• Bank statements
	When enabled, the DLP database (DLDB) is downloaded to the FortiGate and its predefined patterns can configured in DLP profiles.
	`config system fortiguard`
	`    set update-dldb {enable | disable}`
	`end`

852284	Add `fqdn-max-refresh` setting to control the global upper limit of the FQDN refresh timer. FQDN entries with a TTL longer than the maximum refresh value will have their refresh timer reduced to this upper limit. The timer is measured in seconds (3600 - 86400, default = 3600).
	`config system dns`
	`    set set fqdn-max-refresh <integer>`
	`end`

854405	Add amperage and wattage sensors for PSU power consumption. The new sensors can be shown from the REST API, GUI, SNMP, and CLI.
855520	Harden REST API and GUI access.
868163	Implement real-time file system integrity checking in order to: • Prevent unauthorized modification of important binaries. • Detect unauthorized binaries and prevent them from running.

Feature ID	Description
868164	Implement BIOS-level signature and file integrity checking by enforcing each FortiOS GA firmware image, AV engine files, and IPS engine files to be dually-signed by the Fortinet CA and a third-party CA. The BIOS verifies that each file matches their secure hash as indicated by their certificates. Users are warned when there is a failed integrity check, and the system may be prevented from booting depending on the severity and the BIOS security level.
875306	Add new command to compute the SHA256 file hashes for each file in a directory. `# diagnose sys filesystem hash`
882815	Local system administrator usernames are required to follow these naming conventions: • Can include lower and upper case letters (a-z, A-Z), numbers (0-9), underscores (_), and dashes (-) • Cannot start with a dash (-) • Can end with dollar symbol ($) The new rules are enforced for new administrator users and when renaming existing administrator users.
894191	Improve GUI memory consumption for FortiGates with 2 GB of RAM or less.

User & Authentication

See Authentication in the New Features Guide for more information.

Feature ID	Description

843996	Add support for RADSEC clients in order to secure the communication channel over TLS for all RADIUS traffic, including RADIUS authentication and RADIUS accounting over port 2083. This enhancement also adds support for TCP connections, which use port 1812 for authentication and port 1813 for accounting.
	`config user radius`
	`    edit <name>`
	`        set transport-protocol {udp | tcp | tls}`
	`        set ca-cert <string>`
	`        set client-cert <string>`
	`        set tls-min-proto-version {default | SSLv3 | TLSv1 | TLSv1-1 | TLSv1-2}`
	`        set server-identity-check {enable | disable}`
	`    next`
	`end`

857597	Simplify the activation of FortiToken Cloud trials by allowing administrators to activate free trials directly in the FortiGate GUI. This can be performed while enabling two-factor authentication within a user or administrator configuration, or from the *System > FortiGuard* page.

VPN

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

<table>
<tr><th>Feature ID</th><th>Description</th></tr>
<tr><td>827018</td><td>

Update the SSL VPN web portal page layout with Neutrino styling:

- Update the top navigation bar. Users can now download and launch FortiClient.
- Allow the history and theme to be accessed from the user menu.
- Display the *Quick Connection* section at the top. Users can save the connection as a bookmark after launch.
- Separate bookmarks into *Predefined* and *Personal* tabs. Users can search through their bookmarks.
- Make a CLI console available for SSH and Telnet sessions.

</td></tr>
<tr><td>827464</td><td>

The FortiGate device ID is carried by the IKEv2 message NOTIFY payload when it is configured.

```
config vpn ipsec phase1-interface
    edit <name>
        set dev-id-notification enable
        set dev-id <string>
    next
end
```

</td></tr>
<tr><td>857394</td><td>

Enhance the FortiGate with a Key Management Interoperability Protocol (KMIP) client that sends KMIP requests to locate the KMS server, creates keys if they do not exist on the KMS server, and retrieves keys from the Key Management Services (KMS) server for use as IPsec security association (SA) keys for IKEv2 only.

The FortiGate acting as the responder will try to locate keys on the KMS server first. If they do not exist, the FortiGate requests to create new keys on KMS server. The responder sends the keys names to the FortiGate acting as the initiator using IKE messages, and the initiator locates and retrieve keys from KMS server using the keys names. The `keylifeseconds` parameter in phase 2 defines how often the FortiGate will try to synchronize local keys to those on the KMS server.

```
config vpn kmip-server
    edit <name>
        config server-list
            edit <id>
                set server <server_IP>
                set cert <string>
            next
        end
        set username <username_defined_on_KMS_server>
        set password <password>
    next
end
```

```
config vpn ipsec phase1-interface
    edit <name>
        set kms <server_ID>
```

</td></tr>
</table>

Feature ID	Description

	`    next`
	`end`
	The following diagnostic commands have been added:
	`# get vpn ike kms-keys`
	`# diagnose debug application kmipd -1`
	`# execute kmip <parameter>`

862145	Allow SSL VPN web mode users to log in to the web portal and be redirected to a custom landing page. The new landing page accepts SSO credentials and SSO from form data. This allows administrators to streamline web application access for their users. The custom redirected portal can also listen for a logout URL so that when users log out from the web application, they are also logged out from the SSL VPN web connection. Settings can be configured on the *VPN > SSL-VPN Portals* page when creating or editing a portal entry. In the *Web Mode* section, set *Landing page* to *Custom*.
865022	Update the SSL VPN web login page and portal with Fortinet corporate styling. Fortinet branding elements are incorporated into each theme. Some changes include: • The header displays the title of the portal with a new static subheader. • Add quick access to RDP and VNC directly from the *Quick Connection* launch that prompts users for a username and password without requiring pre-configuration. • Display at the most three entries per row in the bookmarks tabs. • Rename some elements. • Add new *Security Fabric* (default) and *Jet Stream* themes.
866412	Add user group information to the *Dashboard > SSL-VPN Monitor* page.

868222	Support IPv6 source IP address for communications to the OCSP server.
	`config vpn certificate ocsp-server`
	`    edit <name>`
	`        set source-ip <IPv4/IPv6_address>`
	`    next`
	`end`

881903	Adjust the DTLS heartbeat parameters for SSL VPN. This improves the success rate of establishing a DTLS tunnel in networks with congestion or jitter.
	`config vpn ssl settings`
	`    set dtls-heartbeat-idle-timeout <integer>`
	`    set dtls-heartbeat-interval <integer>`
	`    set dtls-heartbeat-fail-count <integer>`
	`end`
	The default value for these attributes is 3 seconds, which is also the minimum allowable value. The maximum allowable value for these attributes is 10 seconds.

Feature ID	Description
884772	Securely exchange serial numbers between FortiGates connected with IPsec VPN. This feature is supported in IKEv2, IKEv1 main mode, and IKEv1 aggressive mode. The exchange is only performed with participating FortiGates that have enabled the `exchange-fgt-device-id` setting under `config vpn ipsec phase1-interface`.
886564	This enhancement changes to the Internet Key Exchange (IKE) protocol to bolster the security measures and improve the performance of IPsec VPN. The three key changes include EMS SN Verification, IPsec SAML-based authentication, and IPsec Split DNS.

ZTNA

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

Feature ID	Description

829475	All entry-level FortiGates (lower than 100 series) have ZTNA, proxy, explicit proxy, WANOpt, and web cache disabled by default. The following setting controls the proxy features.
	`config system global`
	`    set proxy-and-explicit-proxy enable | disable}`
	`end`

841165	When configuring a firewall policy for IP- or MAC-based access control that uses different EMS tag types (such as ZTNA tags and classification tags), a logical AND can be used for matching. By separating each tag type into primary and secondary groups, the disparate tag types will be matched with a logical AND operator.
864995	In order to allow FortiClient EMS to share FortiClient information based on IP subnet mask, the FortiGate must send its interface IP and netmask to EMS. This enhancement allows the FortiGate to include its IP and netmask information in the gateway MAC request.

Upgrade information

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

To view supported upgrade path information:

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

Fortinet Security Fabric upgrade

FortiOS 7.4.0 greatly increases the interoperability between other Fortinet products. This includes:

FortiAnalyzer	• 7.4.0
FortiManager	• 7.4.0
FortiExtender	• 7.4.0 and later
FortiSwitch OS (FortiLink support)	• 6.4.6 build 0470 and later
FortiAP	• 7.2.2 and later
FortiAP-U	• 6.2.5 and later
FortiAP-W2	• 7.2.2 and later
FortiClient* EMS	• 7.0.3 build 0229 and later
FortiClient* Microsoft Windows	• 7.0.3 build 0193 and later
FortiClient* Mac OS X	• 7.0.3 build 0131 and later
FortiClient* Linux	• 7.0.3 build 0137 and later
FortiClient* iOS	• 7.0.2 build 0036 and later
FortiClient* Android	• 7.0.2 build 0031 and later
FortiSandbox	• 2.3.3 and later for post-transfer scanning • 4.2.0 and later for post-transfer and inline scanning

[*] If you are using FortiClient only for IPsec VPN or SSL VPN, FortiClient version 6.0 and later are supported.

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

When using FortiClient with FortiAnalyzer, you should upgrade both to their latest versions. The versions between the two products should match. For example, if using FortiAnalyzer 7.4.0, use FortiClient 7.4.0.

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

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

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.4.0. When Security Fabric is enabled in FortiOS 7.4.0, all FortiGate devices must be running FortiOS 7.4.0.

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- admin user account

- session helpers
- system access profiles

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in, go to *Support* > *Firmware Image Checksums* (in the *Downloads* section), enter the image file name including the extension, and click *Get Checksum Code*.

FortiGate 6000 and 7000 upgrade information

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

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

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

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

To perform a graceful upgrade of your FortiGate 6000 or 7000 to FortiOS 7.4.0:

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

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

2. Download the FortiOS 7.4.0 FG-6000F, FG-7000E, or FG-7000F firmware from https://support.fortinet.com.
3. Perform a normal upgrade of your HA cluster using the downloaded firmware image file.
4. When the upgrade is complete, verify that you have installed the correct firmware version.
   For example, check the FortiGate dashboard or use the `get system status` command.

5. Confirm that all components are synchronized and operating normally.

   For example, go to *Monitor > Configuration Sync Monitor* to view the status of all components, or use `diagnose sys confsync status` to confirm that all components are synchronized.

IPS-based and voipd-based VoIP profiles

Staring in FortiOS 7.4.0, 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`.

<table>
<tr><th>Before upgrade</th><th>After upgrade</th></tr>
<tr><td><pre>
config voip profile
    edit "ips_voip_filter"
        set feature-set flow
    next
    edit "sip_alg_profile"
        set feature-set proxy
    next
end
</pre></td><td><pre>
config voip profile
    edit "ips_voip_filter"
        set feature-set ips
    next
    edit "sip_alg_profile"
        set feature-set voipd
    next
end
</pre></td></tr>
</table>

Before upgrade	After upgrade

config firewall policy
    edit 1
        set voip-profile "ips_voip_filter"
    next
    edit 2
        set voip-profile "sip_alg_profile"
    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

BIOS-level signature and file integrity checking during downgrade

When downgrading to a version of FortiOS prior to 6.4.13, 7.0.12, and 7.2.5 that does not support BIOS-level signature and file integrity check during bootup, the following steps should be taken if the BIOS version of the FortiGate matches the following versions:

- 6000100 or greater
- 5000100 or greater

To downgrade or upgrade to or from a version that does not support BIOS-level signature and file integrity check during bootup:

1. If the current security level is 2, change the security level to 0. This issue does not affect security level 1 or below.
2. Downgrade to the desired FortiOS firmware version.
3. If upgrading back to 6.4.13, 7.0.12, 7.2.5, 7.4.0, or later, ensure that the security level is set to 0.
4. Upgrade to the desired FortiOS firmware version.
5. Change the security level back to 2.

To verify the BIOS version:

The BIOS version is displayed during bootup:

```
Please stand by while rebooting the system.
Restarting system
FortiGate-1001F (13:13-05.16.2023)
Ver:06000100
```

To verify the security level:

```
# get system status
Version: FortiGate-VM64 v7.4.2,build2571,231219 (GA.F)
First GA patch build date: 230509
Security Level: 1
```

To change the security level:

1. Connect to the console port of the FortiGate.
2. Reboot the FortiGate (`execute reboot`) and enter the BIOS menu.
3. Press [`I`] to enter the *System Information* menu
4. Press [`U`] to enter the *Set security level* menu
5. Enter the required security level.
6. Continue to boot the device.

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.

Product integration and support

The following table lists FortiOS 7.4.0 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 0311 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 • Windows Server 2008 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 Core (requires Microsoft SHA2 support package) • Novell eDirectory 8.8
AV Engine	• 7.00015
IPS Engine	• 7.00493

Virtualization environments

The following table lists hypervisors and recommended versions.

Hypervisor	Recommended versions
Citrix Hypervisor	• 8.1 Express Edition, Dec 17, 2019
Linux KVM	• Ubuntu 18.0.4 LTS • Red Hat Enterprise Linux release 8.4 • SUSE Linux Enterprise Server 12 SP3 release 12.3
Microsoft Windows Server	• 2012R2 with Hyper-V role
Windows 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.

Resolved issues

The following issues have been fixed in version 7.4.0. To inquire about a particular bug, please contact Customer Service & Support.

Anti Spam

Bug ID	Description
848593	After spam mail is detected by the email filter, the X-ASE-REPORT does not insert into the mail header of the spam mail.
857911	The *Anti-Spam Block/Allow List Entry* dialog page is not showing the proper *Type* values in the dropdown.
877613	*Mark as Reject* can be still chosen as an *Action* in an *Anti-Spam Block/Allow List* in the GUI.

Anti Virus

Bug ID	Description
818092	CDR archived files are deleted at random times and not retained.
845960	Flow mode opens port 8008 over the AV profile that does not have HTTP scan enabled.
849020	FortiGate enters conserve mode and the console prints a `fork()` failed message.
851706	Nothing is displayed in the *Advanced Threat Protection Statistics* dashboard widget.
863461	Scanunit displays unclear warnings when AV package validation fails.
869398	FortiGate sends too many unnecessary requests to FortiSandbox and causes high resource usage.
879946	An incorrect warning is shown for antivirus flow: *Setting a proxy profile in a flow policy. Proxy features will not work*.

Application Control

Bug ID	Description
857632	Unable to access to some websites when application control with deep inspection is enabled.

Bug ID	Description
901166	Unable to connect to any site when application control is enabled with proxy-based or certificate inspection.

Data Loss Prevention

Bug ID	Description
893697	DLP is not blocking VME video files.

DNS Filter

Bug ID	Description
871854	DNS UTM log still presents unknown FortiGuard category even when the DNS proxy received a rating value.
878674	Forward traffic log is generated for allowed DNS traffic if the DNS filter is enabled but the policy is set to log security events only.

Endpoint Control

Bug ID	Description
861316	A system object tagging entry is hindering the FortiGate's ability to process ZTNA tags.

Explicit Proxy

Bug ID	Description
849794	Random websites are not accessible after upgrading when using a proxy policy.
865135	Multipart boundary parsing failed with CRLF before the end of boundary 1.
865828	The `internet-service6-custom` and `internet-service6-custom-group` options do not work with custom IPv6 addresses.

Bug ID	Description
875736	The `proxy-re-authentication-mode` option has been removed in 7.2.4 and is replaced with `proxy-keep-alive-mode re-authentication`. The new `proxy-re-authentication-time` timer is associated with this re-authentication mode. There are two unresolved issues: • After upgrading, the previously configured `proxy-auth-timeout` value for the absolute re-authentication mode is not preserved in the new `proxy-re-authentication-time`. • The new `proxy-re-authentication-time` is currently configured in seconds, but it should be configured in minutes to be consistent with other related authentication timers (such as `proxy-auth-timeout`).
878713	The hit count and bytes of the implicit deny rule does not increase on the proxy policy.
880361	Transparent web proxy policy has no match if the source or destination interface is the same and member of SD-WAN.
882867	Proxy policy match resolves IP to multiple internet service application IDs.
888078	Enabling `http-ip-header` on virtual server changes the log produced for transparent web proxy.
901239	Unexpected behavior in WAD caused by deploying virtual servers in non-server pool mode.
901614	Firewall schedule does not work as expected with a proxy policy.
901627	Explicit proxy and SD-WAN fail to match a policy if the destination has multiple zones set.

Firewall

Bug ID	Description
719311	On the *Policy & Objects* > *Firewall Policy* page in 6.4.0 onwards, the IPv4 and IPv6 policy tables are combined but the custom section name (global label) is not automatically checked for duplicates. If there is a duplicate custom section name, the policy list may show empty for that section. This is a display issue only and does not impact policy traffic.
770541	Within the *Policy & Objects* menu, the firewall, DoS, and traffic shaping policy pages take around five seconds to load when the FortiGate cannot reach the FortiGuard DNS servers.
804603	An httpsd singal 6 crash occurs due to `/api/v2/monitor/license/forticare-resllers`.
816493	The `set sub-type ems-tag` option is blocked in HA diff installation.
835413	Inaccurate sFlow interface data reported to PRTG after upgrading to 7.0.
838535	Support matching by destination port when matching a central NAT rule if the protocols are TCP, UDP, or SCTP.
848058	NPD failed to parse zone in the source interface of a DoS/ACL policy and failed to offload.
850175	When the UTM is enabled, NP7 NTurbo is not set properly, which causes the shaper to not guarantee the SIP traffic based on the class ID.

Bug ID	Description
851212	After traffic flow changes to FGSP peer from owner, iprope information for synchronized sessions does not update on the peer side.
854107	NGFW VDOM incorrectly includes all interfaces belonging to the root VDOM on interface and policy related GUI pages.
856187	Explicit FTPS stops working with IP pool after upgrading.
860480	FG-3000D cluster kernel panic occurs when upgrading from 7.0.5 to 7.0.6 and later.
861990	Increased CPU usage in softirq after upgrading from 7.0.5 to 7.0.6.
864612	When the service protocol is an IP with no specific port, it is skipped to be cached and causes a `protocol/port` service name in the log.
865661	Standard and full ISDB sizes are not configurable on FG-101F.
872744	Packets are not matching the existing session in transparent mode.
875309	Support port block allocation (PBA) IP pools for NAT64 traffic.
875565	The policy or other cache lists are sometimes not freed in time. This may cause unexpected policies to be stored in the cache list.
879225	Egress interface cannot be intermittently matched for wake-on-LAN (broadcast) packets.
879705	Traffic issues occur with virtual servers after upgrading.
881572	Columns for NPU sessions are missing on the *FortiView Sessions* monitor page.
884578	Unexpected behavior in WAD caused by enabling HTTP/2 while usingvirtual servers.
884908	Implicit deny policy is allowing `"icmp/0/0"` traffic.
888957	The one-time schedule pre-expiration event log button is always set to disable.
895962	Intermittent behavior in WAD during SSL renegotiation while using virtual servers.
927009	When running tests with SNAT PBA source and destination IP addresses, octets are shown in reverse order.

FortiGate 6000 and 7000 platforms

Bug ID	Description
838036	Merge FortiGate 6000 and 7000 series platforms.
898191	Support SLBC integrated memory and disk logging in the new local logd framework.

FortiView

Bug ID	Description
798427	The FortiSandbox PDF report query should be changed to on-demand.
838652	The *FortiView Sessions* monitor displays VDOM sessions from other VDOMs.
892798	Memory and CPU usage issues caused by malformed method header while using virtual servers.

GUI

Bug ID	Description
440197	On the *System* > *FortiGuard* page, the override FortiGuard server for *AntiVirus & IPS Updates* shows an *Unknown* status, even if the server is working correctly. This is a display issue only; the override feature is working properly.
535794	Policy page should show new name/content for firewall objects after editing them from the tooltip.
677806	On the *Network* > *Interfaces* page when VDOM mode is enabled, the *Global* view incorrectly shows the status of IPsec tunnel interfaces from non-management VDOMs as up. The VDOM view shows the correct status.
685431	On the *Policy & Objects* > *Firewall Policy* page, the policy list can take around 30 seconds or more to load when there is a large number (over 20 thousand) of policies.
699508	When an administrator ends a session by closing the browser, the administrator timeout event is not logged until the next time the administrator logs in.
722358	When a FortiGate local administrator is assigned to more than two VDOMs and tries logging in to the GUI console, they get a command parse error when entering VDOM configuration mode.
753328	Incorrect shortcut name shown on the *Network* > *SD-WAN* > *Performance SLAs* page.
791367	Users should be able to perform a sniffer on a VWP member in the GUI.
821030	Security Fabric root FortiGate is unable to resolve firewall object conflicts in the GUI.
821734	*Log & Report* > *Forward Traffic* logs do not show the *Policy ID* if there is no *Policy Name*.
822991	On the *Log & Report* > *Forward Traffic* page, using the filter *Result : Deny(all)* does not work as expected.
827893	Security rating test for *FortiCare Support* fails when connected to FortiManager Cloud or FortiAnalyzer Cloud.
829736	Incorrect information is being displayed for the HA role on the *System* > *HA* page.
829773	Unable to load the *Network* > *SD-WAN* > *SD-WAN Rules* table sometimes due to a JavaScript error.
837048	Unable to delete the LAN interface's addresses without switching it back to a none-LAN role.

Bug ID	Description
842079	On the *System* > *HA* page, a *Failed to retrieve info* caution message appears when hovering over the secondary unit's *Hostname*. The same issue is observed on the *Dashboard* > *Status* > *Security Fabric* widget.
848083	On the *System* > *FortiGuard* page, the license table shows expiry notifications for FortiGuard entitlements, which are hidden by the GUI 's *Feature Visibility*.
853414	Policy and dashboard widgets do not load when the FortiGate manages a FortiSwitch with tenant ports (exported from root to other VDOM).
854529	The local standalone mode in a VAP configuration is disabled when viewing or updating its settings in the GUI.
857464	The *CPU* and *Sessions* widgets report the current numbers at the wrong places for most time periods.
861466	The *Active Administrator Sessions* widget shows the incorrect interface when accessing the firewall through the GUI.
862474	IPsec tunnel interface *Bandwidth* widget inbound is zero and outbound value is lower than the binding interface.
865956	On the *Network* > *Policy Routes* page, entries cannot be copied and pasted above or below.
866790	*System* > *Firmware & Registration* menu is not visible for administrator accounts without read-write permissions for the `sysgrp-permission` category.
867588	FortiCare *Reseller* dropdown name option needs correcting.
867802	GUI always displays *Access denied* error after logging in.
869138	Unable to select addresses in *FortiView* monitors.
869828	An httpsd crash occurs when the GUI fails to get the disk log settings from the FortiGate.
870675	CLI console in GUI reports *Connection lost.* when the administrator has more than 100 VDOMs assigned.
872063	The VLAN ID cannot be changed in the GUI.
874502	An access privilege prompt is not displayed when logging in to the GUI of a FortiGate managed by a FortiManager with `post-login-banner` enabled. The user is logged in with read-only permissions.
880292	Global administrator backup configuration for specific VDOM contains configurations associated with only the root VDOM.
881678	On the *Network* > *Routing Objects* page, editing a prefix list with a large number of rule entries fails with an error notification that *The integer value is not within valid range*.
889647	CLI console disconnects and has `'/tmp/daemon_debug/node_...'` crash.
890531	Node.JS boots earlier than autod, which leads to a Node.JS crash.
890683	GUI being exposed to port 80 on the interfaces defined in the ACME settings, even if administrative access is disabled on the interface.

Bug ID	Description
891895	When remotely accessing the FortiGate from FortiGate Cloud, the web GUI console displays `Connection lost. Press Enter to start a new session.`
893286	On the *Dashboard > Status* page, the *CPU*, *Memory*, and *Sessions* widgets always show zero data.

HA

Bug ID	Description
662978	Long lasting sessions are expired on HA secondary device with a 10G interface.
816904	DCE/RPC traffic is dropped when no session matches with the FGSP cluster and asynchronous traffic.
825680	TACACS authentication to secondary FortiGate fails when HA group ID is changed on a FortiGate cluster.
826790	DHCP over IPsec is not working in an FGSP cluster.
830538	FGCP FortiGates go out-of sync when the certificates used for IPsec are updated using SCEP.
830879	Running `execute ha manage 0 <remote_admin>` fails and displays a `Permission denied, please try again.` error if the 169.254.0.0/16 local subnet is not in the trusted host list.
843837	HA A-P virtual cluster information is not correctly presented in the GUI and CLI.
852308	New factory reset box failed to synchronize with primary, which was upgraded from 7.0.
856004	Telnet connection running ping fails during FGSP failover for virtual wire pair with VLAN traffic.
856643	FG-500E interface stops sending IPv6 RAs after upgrading from 7.0.5 to 7.0.7.
859242	Unable to synchronize IPsec SA between FGCP members after upgrading.
860497	Output of `diagnose sys ntp status` is misleading when run on a secondary cluster member.
861827	FortiGate uses dedicated management interface to connect to 154.52.29.102 (productapi.fortinet.com) even though `ha-direct` is disabled.
864226	FG-2600F kernel panic occurs after a failover on both members of the cluster.
866296	The HBDEV status is displayed as `DOWN` when upgrading one node of the HA cluster to 6.4.9.
868622	The session is not synchronized after HA failover by detecting monitored interface as down.
869557	Upgrading or re-uploading an image to the HA secondary node causes the OS to be `un-certified`.
870312	On a FortiGate HA cluster, both primary and secondary units are displayed as the *Primary* on the GUI top banner, and as `Current HA mode` in the CLI.

Bug ID	Description
870367	FGCP A-P devices get out of HA synchronization periodically due to FortiTokens being added and deleted.
871636	HA configuration synchronization packets (Ethertype 0x8893) are dropped when going through VXLAN.
872431	Primary FortiGate synchronizes the changing HA command to the secondary.
873028	In HA A-A mode, authenticated users experience intermittent drops and disconnections.
873561	Several session counts of primary unit do not match.
874397	When re-enabling `sync-config` on the primary FGCP cluster member, it is automatically disabled on the secondary.
874823	FGSP `session-sync-dev` ports do not use L2 Ethernet frames but always use UDP, which reduces the performance.
875984	FortiGate is going to out-of-sync after changing parameters of VDOM link interfaces.
876178	hasync crashing with signal 6 after upgrading to 7.2.3 from 7.0.7.
878173	When downloading the speed test server list, the HA cluster gets and stays out-of-sync.
880786	Running `diagnose sys ha vlan-hb-monitor` incorrectly shows inter-VDOM VLANs inactive.
881337	Adding a VLAN interface on any VDOM causes BGP flapping and VIP connectivity issues on VDOMs in vcluster2.
881847	HA interfaces flapping on FG-3401E.
882354	When WAN extension redundant mode is configured in HA, after a redundant switch it will makes the HA be out-of-sync.
883546	In HA, sending lot of CLI configurations causes the creation of a VDOM on the secondary unit.
885245	Unexpected failover occurs due to uptime, even if the uptime difference is less than the `ha-uptime-diff-margin`.
885844	HA shows as being out-of-sync after upgrading due to a checksum mismatch for `endpoint-control fctems`.
888110	Unable to set the interface configured as an SD-WAN member to `pingserver-monitor-interface` in the CLI.
896608	HA cluster became out-of-sync after enabling a password policy and logging on to FortiGate.
897865	When NP7 platforms enable the GTP enhanced mode it does not use uninterruptible upgrade.

Hyperscale

Bug ID	Description
771857	Firewall virtual IP (VIP) features that are not supported by hyperscale firewall policies are no longer visible from the CLI or GUI when configuring firewall VIPs in a hyperscale firewall VDOM.
837270	Allowing intra-zone traffic is now supported in hyperscale firewall VDOMs. Options to block or allow intra-zone traffic are available in the GUI and CLI.
841712	On FortiGates licensed for hyperscale firewall features, the `config system setting` options `nat46-force-ipv4-packet-forwarding` and `nat64-force-ipv6-packet-forwarding` now also apply to NP7-offloaded traffic. The `config system npu` option `nat46-force-ipv4-packet-forwarding` has been removed.
843305	Get `PARSE SKIP ERROR=17 NPD ERR PBR ADDRESS` console error log when performing a system bootup.
877696	Get KTRIE invalid node related error and kernel panic on standby after adding a second device into A-P mode HA cluster.

Intrusion Prevention

Bug ID	Description
696811	`IPSA self test failed, disable IPSA! IPSA disabled: self test failed` message appears in system event logs.
842073	Improvements to IPS engine to optimize CPU usage when a decrypted traffic mirror profile is applied to policies in flow mode.
842523	IPv6 with hardware offloading and IPS drops traffic (`msg="anti-replay check fails, drop)`.
845944	Firewall policy change causes high CPU spike with IPS engine.
872137	Unable to pass traffic when using GRE over IPsec (IPsec in transport mode).
873975	Source MAC changes and the packet drops due to both sides of the session using the same source MAC address.
881549	Memory leak was detected due to IPS engine restart.
883600	Under `config ips global`, configuring `set exclude-signatures none` does not save to backup configuration.
891497	IPS configuration script crashes sometimes when a VDOM is deleted.

IPsec VPN

Bug ID	Description
699973	IPsec aggregate shows down status on *Interfaces*, *Firewall Policy*, and *Static Routes* configuration pages.
726326	IPsec server with NP offloading drops packets with an invalid SPI during rekey.
788751	IPsec VPN Interface shows incorrect TX/RX counter.
797342	Users cannot define an MTU value for the aggregate VPN.
798045	FortiGate is unable to install SA (`failed to add SA, error 22`) when there is an overlap in configured selectors.
803010	The `vpn-id-ipip` encapsulated IPsec tunnel with NPU offloading cannot be reached by IPv6.
812229	ASCII-encoded byte code of remote gateway IP is displayed in the GUI and CLI when a VPN tunnel is formed using IKEv1 or v2 if the `peer-id` is not configured.
828933	iked signal 11 crash occurs once when running a VPN test script.
842571	If `mode-cfg` is used, a race condition can result in an IP conflict and sporadic routing problems in an ADVPN/SD-WAN network. Connectivity can only be restored by manually flushing the IPsec tunnels on affected spokes.
848014	ESP tunnel traffic hopping from VRF.
852868	Issues with synchronization of the route information (using `add-route` option) on spokes during HA failover that connect to dialup VPN.
855705	NAT detection in shortcut tunnel sometimes goes wrong.
855772	FortiGate IPsec tunnel role could be incorrect after rebooting or upgrading, and causes negotiation to be stuck when it comes up.
858681	When upgrading from 6.4.9 to 7.0.6 or 7.0.8, the traffic is not working between the spokes on the ADVPN environment.
858697	Native IPsec iOS authentication failure using LDAP account with two-factor authentication.
858715	IPsec phase 2 fails when both HA cluster members reboot at the same time.
861195	In IPsec VPN, the fnbamd process crashes when the password and one-time password are entered in the same *Password* field of the VPN client.
869166	IPsec tunnel does not coming up after the upgrading firmware on the branch FortiGate (FG-61E).
873097	Phase 2 not initiating the rekey at soft limit timeout on new kernel platforms.
876795	RADIUS server will reject new authentication if a previous session is missing ACCT-STOP to terminate the session, which causes the VPN connection to fail.
882483	ADVPN spoke does not delete the BGP route entry to another spoke over IPsec when the IPsec VPN tunnel is down.
884921	Proxy DHCP is not following RFC 2132 for option 61.

Bug ID	Description
885333	Forwarded broadcast traffic on ADVPN shortcut tunnel interface is dropped.
885818	If a tunnel in an IPsec aggregate is down but its DPD link is on, the IPsec aggregate interface may still forward traffic to a down tunnel causing traffic to drop.
887800	In an L2TP configuration, `set enforce-ipsec enable` is not working as expected after upgrading.
889602	ADVPN hub is not advertising additional paths by specific tunnels.
891462	The *Peer ID* field in the *IPsec* widget should not show a warning message that *Two-factor authentication is not enabled*.
892699	In an HA cluster, static routes via the IPsec tunnel interface are not inactive in the routing table when the tunnel is down.
916260	The IPsec VPN tunnel list can take more than 10 seconds to load if the FortiGate has large number of tunnels, interfaces, policies, and addresses. This is a GUI display issue and does not impact tunnel operation.

Log & Report

Bug ID	Description
714470	The `exclude-list` log filter is not working as expected.
755632	Unable to view or download generated reports in the GUI if the report layout is custom.
816616	GUI logging issue for automation script that performs a backup to an external FTP server.
823183	FortiGates are showing *Logs Queued* in the GUI after a FortiAnalyzer reboot, even tough the queued logs were actually all uploaded to FortiAnalyzer and cleared when the connection restores.
825318	*Archived Data* tab is missing from intrusion prevention and application control log *Details* pane once `log-packet` is enabled.
828211	Policy ID filter is not working as expected.
829862	On the *Log & Report* > *ZTNA Traffic* page, the client's *Device* ID is shown as *[object Object]*. The Log Details pane show the correct ID information.
836846	Packet captured by firewall policy cannot be downloaded.
838357	A deny policy with log traffic disabled is generating logs.
839601	When log pages are scrolled down, no logs are displayed after 500 lines of logs.
854604	Logs are outputted, even if `FDS-license-expiring-warning` is disabled.
856670	Forward traffic log does not contain `result` and `security action` values for sessions denied by WAD.
857573	Log filter with negation of destination IP display all logs.

Bug ID	Description
858304	When FortiGate Cloud logging is enabled, the option to display *7 days* of logs is not visible on the *Dashboard > FortiView* pages.
858589	Unable to download more than 500 logs from the FortiGate GUI.
860141	Syslog did not update the time after daylight saving time (DST) adjustment.
860264	The miglogd process may send empty logs to other logging devices.
860459	Unable to back up logs (FG-201E).
860487	Incorrect time and time zone appear in the forward traffic log when `timezone` is set to `18` (GMT-3 Brasilia).
861567	In A-P mode, when the link monitor fails, the event log displays a description of `ha state is changed from 0 to 1`.
861893	In *Forward Traffic* logs, the *Policy ID* column is blank.
863548	When searching old logs on the *Log & Report > Forward Traffic* page and then navigating to another page, the `log_se` process on the FortiGate is still busy as the cancel request is not sent after navigating to the other page.
864111	An internal error occurs on the FortiCloud Report page when a Japanese report name is too long.
864219	A miglogd crash occurs when creating a dynamic interface cache on an ADVPN environment.
869073	A syslogd signal 11 crash occurs once while running VPN scripts.
871142	SAML SSO administrator login with post-login banner enabled does not have a login event.
872181	On the *Log & Report > Log Settings > Local Logs* page, the *Local reports* and *Historical FortiView* settings cannot be enabled.
872326	FortiGate cannot retrieve logs from FortiAnalyzer Cloud. Results are shown rarely.
873987	High memory usage from miglogd processes even without traffic.
874026	Caching a large number of service port entries causes high log daemon memory usage.
879228	FortiAnalyzer override settings are not taking effect when `ha-direct` is enabled.
893199	The FortiGate does not generate deallocate/allocate logs of the first IP pool when the first IP pool has been exhausted.
901545	FG-40F and FWF-61F halt after upgrading.
918571	The log_se process resource utilization is causing a network outage.

Proxy

Bug ID	Description
707827	The video filter does not display the proper replacement message when the user redirects to a blocked video from the YouTube homepage or video recommendation list.
727629, 901296	An error case occurs in WAD while handling the HTTP requests for an explicit proxy policy.
746587	Error condition in WAD occurs during traffic scans in proxy mode.
766158	Video filter FortiGuard category takes precedence over allowed channel ID exception in the same category.
781613	Intermittent traffic disruption caused by race condition in WAD.
818371	An error condition occurs in WAD while parsing certain URIs.
823078	Improvements to WAD to optimize CPU usage when using user groups.
825977	An error condition occurs in WAD during an AV scan submission.
828917	Unexpected behavior in WAD when there are multiple LDAP servers configured on the FortiGate.
834387	In a firewall proxy policy, the SD-WAN zone assigned to interface is not checked.
835745	An error condition occurs in WAD when the `srcintf` of a `firewall proxy-policy` is set to an SD-WAN zone.
837095	WAD daemon runs high with many child processes and is not coming down after configuring 250 CGN VDOMs.
850426	POP3 proxy is unable to extract the username if `AUTH PLAIN` or `AUTH LOGIN` commands were used for authentication.
853864	FortiGate out-of-band certificate check issue occurs in a proxy mode policy with SSL inspection.
854511	Unable to make API calls using Postman Runtime script after upgrading to 7.2.0.
855853	Improvements to WAD to optimize CPU usage when using user groups.
855882	Improvements to WAD to resolve a memory usage issue when user-info updates the FortiAP information.
856235	The WAD process memory usage gradually increases over a few days, causing the FortiGate to enter into conserve mode.
857368	WAD crashed while parsing a Huffman-encoded HTTP header.
858148	Memory usage issue caused by the WAD `user-info` history daemon.
870151	Memory usage issue occurs on the WAD worker in a specific scenario.
870554	An error condition occurs in WAD when the `dstaddr6` of a `firewall proxy-policy` is set to an IPv6 address.
874563	User information attributes can cause disruption when they are not properly merged.

Bug ID	Description
880712	An error condition occurs in WAD due to an improper NULL check.
882182	Unexpected behavior in WAD due to the activation of firewall protocol options, with both client and server comfort features enabled.
885674	Unable to send logs from FortiClient to FortiAnalyzer when deep inspection is enabled on firewall policy.
886284	An error condition occurs in WAD when a task is queued in the dev-vuln daemon and the user-info daemon restarts.
898016	Kerberos authentication stops working after the upgrading to 7.2.3.

REST API

Bug ID	Description
849273	`/api/v2/monitor/system/certificate/download` can still download already deleted CSR files.
864393	High CPU usage of httpsd on FG-3600E HA system.
868265	The active sessions count for a specific policy displayed in the *Fortiview Sessions* monitor (*Active Sessions* column), on the *Firewall Policy* page, and in the results of `diagnose sys session list` (`total session` value) are different. The total session count indicated in the CLI is the accurate value.
891135	In the FortiOS API, policies with a large number of service objects drop objects without an error.
892237	Updating the HA monitor interface using the REST API PUT request fails and returns a -37 error.

Routing

Bug ID	Description
708904	`No IGMP-IF for ifindex` log points to multicast enabled interface.
724468	Router policy destination address not take effect when `internet-service-id` is configured.
821149	Early packet drop occurs when running UTM traffic on virtual switch interface.
827565	Using `set load-balance-mode weight-based` in SD-WAN implicit rule does not take effect occasionally.
839784	DHCP relay packets are not being sent out of WWAN interface.
848310	IPsec traffic sourced from a loopback interface does not follow the policy route or SD-WAN rules.

Bug ID	Description
850778	Spoke-to-spoke communication randomly breaks. The BGP route to reach the spoke subnet points to the main ADVPN tunnel instead of the shortcut tunnel.
850862	When creating a new rule on the *Network > Routing Objects* page, the user cannot create a route map with a rule that has multiple similar or different AS paths in the GUI.
852498	BGP packets are marked with DSCP CS0 instead of CS6.
852525	When enabled, FEC is not effectively reducing packet loss when behind NAT.
858248	OSPF summary address for route redistribution from static route via IPsec VPN always persists.
858299	Redistributed BGP routes to the OSPF change its forward address to the tunnel ID.
859135	Disabling the VDSL interface caused packet drops afterwards on another interface.
860075	Traffic session is processed by a different SD-WAN rule and randomly times out.
862165	FortiGate does not add the route in the routing table when it changes for SD-WAN members.
862418	Application VWL crash occurs after FortiManager configuration push causes an SD-WAN related outage.
862573	SD-WAN GUI does not load, and the lnkmtd process crashes frequently.
863318	Application forticron signal 11 (Segmentation fault) received.
863833	BGP stuck in active state due to collisions when BGP neighborship is done over VDOM link.
865914	When BSM carries multiple CRPs, PIM might use the incorrect prefix to update the mroute's RP information.
867196	SD-WAN and IP pool setting are not working as expected when one SD-WAN member link is down.
870983	Unable to set `local-as` in BGP confederation configuration.
870990	Routing advertised by directly connected EBGP peer is not installed (`denied due to non-connected next-hop`).
874677	Sometimes an IPv6 single-hop BFD neighbor fails to come up after a system reboot.
875177	TCP/HTTP health check does not work as expected for virtual servers in active-standby mode.
875668	SD-WAN SLA log information has incorrect inbound and outbound bandwidth values.
880390	When `execute speed-test-server download` fails with a `token parse error`, it still reports `Download completed`.
881306	SD-WAN member shows as selected, even if the interface is down or underlying transport is down.
883918	Delay in joining `(S,G)` in PIM-SM.
884298	Sandbox traffic does not follow SD-WAN rules.
884372	All BGP routes in dual ADVPN redundant configuration are not getting updated to the correct WAN interface post-rollback to WAN failover.
890379	After upgrading, SD-WAN is unable to fail over the traffic when one interface is down.

Bug ID	Description
893603	GUI does not show gateway IP on the routing table page if VDOM mode is transparent.
896065	ISIS cannot establish the neighborship to peers, and all peers are in INIT states.
897940	Link monitor's probe timeout value range is not appropriate when the user decreases the minimum interval.
898549	IPv6 route to SLA IPv6 target is lost after disabling and enabling the physical interface.

Security Fabric

Bug ID	Description
809106	*Security Fabric* widget and *Fabric Connectors* page do not identify FortiGates properly in HA.
819192	After adding a Fabric device widget, the device widget does not appear in the dashboard.
825291	Security rating test for *FortiAnalyzer* fails when connected to FortiAnalyzer Cloud.
831311	When using automation email action to reference the result of a previously executed automation CLI script action, there is a 16 KB size limit for the script output.
832015	Root FortiGate cannot finish the security rating with a large Fabric topology (more than 25 to 30 devices) because the REST API is not limited to the local network.
844412	When a custom LLDP profile has `auto-isl` disabled, the security rating test, *Lockdown LLDP Profile*, fails.
848822	The *FortiAP Firmware Versions* and *FortiSwitch Firmware Versions* security rating tests fail because the firmware version on the FortiAPs and FortiSwitches is not recognized correctly.
851656	Sessions with `csf_syncd_log` flag in a Security Fabric are not logged.
852340	Various places in the GUI do not show the secondary HA device.
862532	Unable to load topology pages for a specific Security Fabric topology on the root and downstream FortiGates.
867313	*Error triggering automation stitch* message appears when the license expiry notification type is *FortiGuard Web Filter*.
868701	In a simple cluster, the primary unit failed to upgrade to 7.2.3.
870527	FortiGate cannot display more than 500 VMs in a GCP dynamic address.
875100	Unable to remove external resource in a certain VDOM when the external resource has no reference in that VDOM.
880011	When the Security Fabric is enabled and `admin-https-redirection` is enabled on a downstream FortiGate, the following GUI features do not work for the downstream FortiGate when the administrator manages the downstream FortiGate using the root FortiGate's GUI: • Web console access • Diagnostic packet capture

Bug ID	Description
	• GUI notification when a new device joins or leaves the Security Fabric • GUI notification if a configuration on the current page changes These features still work for the root FortiGate's GUI.
885810	The gcpd daemon constantly crashes (signal 11 segmentation fault).
887967	Fabric crashes when synchronizing objects with names longer than 64 characters.

SSL VPN

Bug ID	Description
631809	Configuring thousands of `mac-addr-check-rule` in portal makes the CPU spike significantly if several hundreds of users are connecting to the FortiGate, thus causing SSL VPN packet drops.
710657	The `dstaddr`/`dstaddr6` of an SSL VPN policy can be set to `all` when split tunnel mode is enabled and only the default portal is set.
746440	When sending the SSL VPN settings email (*VPN > SSL-VPN Settings > Send SSL-VPN Configuration*), the *Email* template only includes a hyperlink to the configuration, which is not supported by Gmail and Fortinet email.
767086	Customer's internal website does not load properly in SSL VPN web mode.
787768	The `web-mode` setting should not be enabled when the portal is mapped in an SSL VPN policy where a VIP is applied.
808107	FortiGate is not sending Accounting-Request packet that contains the Interim-Update AVP when two-factor authentication is assigned to a user (defined on the FortiGate) while connecting using SSL VPN.
810239	Unable to view PDF files in SSL VPN web mode.
819754	Multiple DNS suffixes cannot be set for the SSL VPN portal.
822657	Internal resource pages and menus are not showing correctly in SSL VPN web mode.
828194	SSL VPN stops passing traffic after some time.
839261	On the *VPN > SSL-VPN Settings* page, when the `source-address-negate` option is enabled for an address in the CLI, the GUI does not display an exclamation mark against that address entry in the *Hosts* field. This is cosmetic and does not affect on the FortiGate functionality or operation. The `source-address-negate` option being enabled can be confirmed in the CLI.
850898	OS checklist for the SSL VPN in FortiOS does not include macOS Ventura (13).
852652	MacOS clients bypass the host check policy.
854615	Internal web interface is not working using web mode. The page is not loading properly.

Bug ID	Description
854642	Internal website with JavaScript is proxying some functions in SSL VPN web mode, which breaks them.
856194	Problem loading some graphs trough SSL VPN web mode after upgrading.
856554	SSL VPN web mode top-right dropdown button (user profile menu) does not work.
858478	SSL VPN DTLS tunnel is unavailable after changing the SSL VPN listening port.
859088	FortiGate adds extra parenthesis and causes clicking all links to fail in SSL VPN web mode.
859115	SSL VPN bookmark not accessible.
863860	RDP over SSL VPN web mode to a Windows Server changes the time zone to GMT.
864096	EcoStruxure Building Operations 2022 does not render using SSL VPN bookmark.
864417	In the second authentication of RADIUS two-factor authentication, the `acct-update-interval` returned is `0`. SSL VPN uses the second return and not send RADIUS `acct-interim-update` packet.
867182	RDP/VNC host name is not encrypted when URL obscuration is enabled.
868491	SSL VPN web mode connection to VMware vCenter 7 is not working.
870061	Kernel does not delete original route after address assigned to the client changes.
871039	Internal website is not displaying user-uploaded PDF files when visited through SSL VPN web mode.
871048	RDP over VPN SSL web mode stops working after upgrading.
871229	SSL VPN web mode does not load when connecting to customer's internal site.
872577	SSL VPN crashes are generating random disconnections (FG-5001E).
872745	SSL VPN web mode to RDP broker leads to connection being closed.
873313	SSL VPN policy is ignored if no user or user group is set and the FSSO group is set.
873516	FortiGate misses the closing parenthesis when running the function to rewrite the URL.
873995	Problem with the internal website using SSL VPN web mode.
875167	Webpage opened in SSL VPN web portal is not displayed correctly.
877124	RDP freezes in web mode with high CPU usage of SSL VPN process.
880791	Internal website access issue with SSL VPN web portal.
881220	Found bad login for SSL VPN web-based access when enabling URL obscuration.
884051	Unable to access to Grafana tool using SSL VPN web mode (bookmark).
884860	SSL VPN tunnel mode gets disconnected when SSL VPN web mode is disconnected by `limit-user-logins`.

Bug ID	Description
886989	SSL VPN process reaches 99% CPU usage when HTTP back-end server resets the connection in the middle of a post request.
888149	When `srcaddr6` contains `addrgrp6`, sslvpnd crashes after dual-stack tunnel is established.
889392	SSL VPN is adding extra JS code blocking access to a website.
890876	One of the speed-connect website JavaScript files has trouble with host process.
891830	Internal website with JavaScript lacks some menus when using SSL VPN web mode.
894704	FortiOS check would block iOS and Android mobile devices from connecting to the SSL VPN tunnel.
896007	Specific SAP feature is not working with SSL VPN web mode.
896343	SSL VPN web mode is not working as expected for customer's web server.
898889	The internal website does not load completely with SSL VPN web mode.

Switch Controller

Bug ID	Description
730472	FortiSwitch enabled VLANs with VLAN and proxy ARP access have large latencies on initial ARP resolutions.
762615, 765283	FortiSwitches managed by FortiGate go offline intermittently and require a FortiGate reboot to recover.
769722	Support FortiLink to recognize a FortiSwitch based on its name and not just by serial number.
857778	Switch controller managed switch port configuration changes do not take effect on the FortiSwitch.
858113	On the *WiFi & Switch Controller > Managed FortiSwitches* page, when an administrator with restricted access permissions is logged in, the *Diagnostics and Tools* page for a FortiSwitch cannot be accessed.
858749	Redirected traffic should not hit the firewall policy when `allow-traffic-redirect` is enabled.
870083	FortiLink interface should not permit changes of the `system interface allowaccess` settings.
876021	FortiLink virtually managed switch port status is not getting pushed after the FortiGate reboots.
886887	When a MAC VLAN appears on the same MCLAG trunk, continuous event logs are received on FortiGate and FortiAnalyzer.
894735	Unable to configure more than one NAC policy using the same EMS tag for different FortiSwitch groups.

System

Bug ID	Description
550701	Inadvertent traffic disruption caused by WAD due to deadlock.
631046	`diagnose sys logdisk smart` does not work for NVMe disk models.
649729	HA synchronization packets are hashed to a single queue when `sync-packet-balance` is enabled.
666664	Interface belonging to other VDOMs should be removed from interface list when configuring a GENEVE interface.
700621	The forticron daemon is constantly being restarted.
709679	Get `can not set mac address(16)` error message when setting a MAC address on an interface in HA that is already set.
729912	DNS proxy does not transfer the DNS query for IPv6 neighbor discovery (ND) when client devices are using random MAC addresses, so one device can configure many IPv6 addresses.
748496	Wrong IP displayed in GUI widget if FortiGuard anycast AWS is used.
754970	HPE does not enforce a limit on fragmented packets sent to the CPU when ip-reassembly is enabled.
763739	On FG-200F, the *Outbound* bandwidth in the *Bandwidth* widget does not match outbandwidth setting.
776646	On the *Network* > *Interfaces* page, configuring a delegated interface to obtain the IPv6 prefix from an upstream DHCPv6 server fails with an error notification (*CLI internal error*).
790595	Improve dnsproxy process memory management.
799570	High memory usage occurs on FG-200F.
805122	In FIPS-CC mode, if `cfg-save` is set to `revert`, the system will halt a configuration change or certificate purge.
810879	DoS policy ID cannot be moved in GUI and CLI when multiple DoS policies are enabled.
813607	LACP interfaces are flapping after upgrading to 6.4.9.
815937	FCLF8522P2BTLFTN transceiver is not working after upgrade.
820268	VIP traffic access to the EMAC VLAN interface uses incorrect MAC address on NP7 platform.
822333	The tab title does not show the server address when accessing RDP/VNC using SSL VPN web mode.
826490	NP7 platforms may reboot unexpectedly when unable to handle kernel null pointer de-reference.
831466	A cmdbsvr crash is observed on the FortiGate.
838933	DoS anomaly has incorrect threshold after loading a modified configuration file.

Bug ID	Description
840960	When kernel debug level is set to `>=KERN_INFO` on NP6xLite platforms, some tuples missing debug messages may get flooded and cause the system to get stuck.
845736	After rebooting the FortiGate, the MTU value on the VXLAN interface was changed.
846399	Add 100G speed option for FG-180xF for ports 37, 38, 39, and 40. Upon firmware upgrade, existing port speed configurations are preserved.
847314	NP7 platforms may encounter random kernel crash after reboot or factory reset.
850683	Console keeps displaying `bcm_nl.nr_request_drop ...` after the FortiGate reboots because of the `cfg-save revert` setting under `config system global`. Affected platforms: FG-10xF and FG-20xF.
850688	FG-20xF system halts if setting `cfg-save` to `revert` under `config system global` and after the `cfg-revert-timeout` occurs.
853144	Network device kernel null pointer is causing a kernel crash.
853794	Issue with the `server_host_key_algorithm` compatibility when using SSH on SolarWinds.
853811	Fortinet 10 GB transceiver LACP flapping when shut/no shut was performed on the interface from the switch side.
855573	False alarm of the PSU2 occurs with only one installed.
855775	Time zone for Kyiv, Ukraine is missing.
859717	The FortiGate is only offering the `ssh-ed25519` algorithm for an SSH connection.
859795	High CPU utilization occurs when relay is enabled on VLAN, and this prevents users from getting an IP from DHCP.
861144	`execute ping-option interface` cannot specific an interface name of `a`.
861661	SNMP OID 1.3.6.1.2.1.4.32 ipAddressPrefixTable is not available.
862941	GUI displays a blank page if `vdom-admin` user has partial permissions.
865770	RX and TX counters are incorrect on inter-VDOM link configured with VLANs.
865966	DHCP lease list CLI format gets misaligned when the data is over 15 characters long.
867428	Add check to skip invalid names when creating a VDOM.
867435	FG-400E-BP has crash at `initXXXXXXXXXXX[1]: segfault at 3845d5a` after package validation fails.
867978	Subnet overlap error occurs when configuring the same IPv4 link-local addresses on two different interfaces.
868225	After a cold reboot (such as a power outage), traffic interfaces may not come up with a possible loss of VLAN configurations.
868821	`execute ssh-regen-keys` should be global-level command.

Bug ID	Description
869044	If the original packet was forwarded with NAT, generated ICMP error is routed back to SNAT'ed address.
869113	If a device is rebooted that has an `ipsec-STS-timeout` configured or the user configures the `ipsec-STS-timeout` before any NPU tunnel is created, NPU will send random STS messages that have an invalid tunnel index and trigger NP6XLite error messages.
869305	SNMP multicast counters are not increasing.
869599	Forticron memory is leaking.
870381	Memory corruption or incorrect memory access when processing a bad WQE.
872739	The fgfmsd process crashes since updating to 6.4.11.
874292	`ssh-rsa` should be disabled under the SSH `server_host_key_algorithm`.
874603	Dashboard loads slowly and csfd process has high CPU usage.
875868	HQIP test fails on FG-2201E.
876403	ACME auto-renewal is not performed after HA failover.
876853	No output of `execute sensor list` is displayed after rebooting.
877039	On the *Network* > *BGP* page, creating or editing a table entry increases memory consumption of the FortiGate to 99%.
877154	FortiGate with new kernel crashes when starting debug flow.
877240	Get `zip conf file failed -1` error message when running a script configuring the FortiGate.
878400	When traffic is offloaded to an NP7 source MAC, the packets sent from the EMAC VLAN interface are not correct.
879131	Unsetting the port 8888 setting in `system fortiguard` will set port 443, even if the protocol is UDP.
880290	NP7 is not configured properly when the ULL ports are added to LAG interface, which causes accounting on the LAG to not work.
881094	FG-3501F NP7 is dropping all traffic after it is offloaded.
882089	Unable to use ping and SSH when vne.root is not configured in local-in-policy.
883071	Kernel panic occurs due to null pointer dereference.
884970	Unbalanced throughput on LAG members with LAG enhancement feature enabled.
885189	Control the server host key algorithm in the CLI.
887268	Unable to configure `dscp-based-priority` when `traffic-priority dscp` is configured under `system global`.
887772	CPU usage issue in WAD caused by checking authentication group member information.
888941	Some sessions are still reported as offloaded when `auto-asic-offload` is disabled.
889634	Unable to configure IPv6 setting on system interface (FWF-81F-2R-POE).

Bug ID	Description
891165	Auto-script causes FortiGate to repeat commands.
891841	Unable to handle kernel NULL pointer dereference at 0000000000000000 for NP7 device; the device keeps rebooting.
892195	LAG interface has NOARP flag after interface settings change.
892274	Daylight saving time is not applied for Cairo time zone.
892478	Interface release from cmdb and iprope keep updating when DHCP client renewal fails.
894884	FSTR session ticket zero causes a memory leak.
895972	FortiGate as L2TP client is not working after upgrading to 7.2.4.
897521	grep command including -f does not provide the full output.
899884	FG-3000F reboots unexpectedly with NULL pointer dereference.
901721	In a certain edge case, traffic directed towards a VLAN interface could trigger a kernal panic.
958437	An error message is shown when attempting to create a FortiExtender WAN extension interface.

Upgrade

Bug ID	Description
850691	The endpoint-control fctems entry 0 is added after upgrading from 6.4 to 7.0.8 when the FortiGate does not have EMS server, which means the endpoint-control fctems feature was not enabled previously. This leads to a FortiManager installation failure.
883305	SSH public keys are lost after upgrading from Beta 1 to latest interim build, and they can no longer be configured.
892647	Static route configurations were lost upgrading from 7.0.7 to 7.2.3.
900761	FG-601E crashes randomly after upgrading to 7.0.8 and 7.0.11.
903113	Upgrading FortiOS firmware with a local file from 6.2.13, 6.4.12, 7.0.11, or 7.2.4 and earlier may fail for certain models because the image file size exceeds the upload limit. Affected models: FortiGate 6000 and 7000 series, FWF-80F-2R, and FWF-81F-2R-POE.

User & Authentication

Bug ID	Description
705731	Chrome throttles timers, which causes the keepalive page not update correctly and results in a user timeout.

Bug ID	Description
751763	When MAC-based authentication is enabled, multiple RADIUS authentication requests may be sent at the same time. This results in duplicate sessions for the same device.
768669	If an administrator login fails due to an LDAP server connection timeout, `invalid password` appears as the reason in the system log, which is confusing. The `server connection timeout` reason is added to the system event logs for a failed administrator login.
794477	When a user's membership in AD or port range is changed, all of the user sessions are cleared.
843528	RADIUS MAC authentication using ClearPass is intermittently using old credentials.
846545	LDAPS connectivity test fails with old WinAD after OpenSSL was upgraded to 3.0.2.
850473	SSL VPN and firewall authentication SAML does not work when the application requires SHA-256.
853793	FG-81F 802.1X MAC authentication bypass (MAB) failed to authenticate Cisco AP.
854114	Some embedded SSL certificates entered the `Error` state after enabling FIPS-CC.
855898	All devices are detected as *Other identified device* in the *Device Inventory* widget.
856370	The EAP proxy worker application crashes frequently.
857438	SSL VPN group matching does not work as expected for Azure auto login.
858877	Dynamic address only has 100 IP addresses while FSSO group lists all 56K ACI endpoints.
858961	Client's firewall authentication session timeout is set to 900 when it passes MAC authentication bypass by ping.
859845	In some cases, the proper hostnames are not showing up when looking at APs on the FortiSwitch ports screen.
864703	ACME client fails to work with some CA servers.
865166	A cid scan crash occurs when device detections happen in a certain order.
865487	Fortinet_GUI_Server certificate auto-regenerates every day.
867225	ARP does not trigger FortiGuard device identification query.
868481	When the *Guest User Print Template* is customized in a VDOM, printing the guest user credentials from *User & Authentication > Guest Management* still uses the default *Guest User Print Template*.
873981	CMP should be supported for EC certificates.
883006	Adding a new group membership to an FSSO user terminates all the user's open sessions.
901743	An error condition occurs during the processing of the UDP packets when device identification is activated on an interface.

VM

Bug ID	Description
740796	IPv6 traffic triggers `<interface>: hw csum failure` message on CLI console.
856645	Session is not crated over NSX imported object when traffic starts to flow.
859165	Unable to enable FIPS cipher mode on FG-VM-ARM64-AWS.
859589	VPNs over Oracle Cloud stop processing traffic.
860096	CPU spike observed on all the cores in a GCP firewall VM.
865772	Interface does not get turned back up after changing the MTU in the aggregate interface.
868698	During a same zone AWS HA failover, moving the secondary IP will cause the EIP to be in a disassociated state.
869359	Azure auto-scale HA shows certificate error for secondary VM.
874559	FortiGate VM HA primary loses connection when setting up secondary unit.
878074	FG-ARM64-GCP and FG-ARM64-AZURE have HA synchronization issue with internal IP after failover.
881728	Kernel hangs on FG-VM64-AZURE.
881768	AWS MAC is not shown when the interface is attached immediately.
883203	FG-AWS SDN is unable to retrieve EKS cluster information, even thought its role is trusted by the EKS role.
883896	Backup virtual server not working as expected (`ERR_EMPTY_RESPONSE`).
885829	Azure SDN connector stopped processing when Azure returned `NotFound` error for VMSS interface from an AD DS-managed subscription.
890278	FG-VM Rackspace On-Demand upgrade from 7.2.3 to 7.2.4 breaks the pay-as-you-go license, and reverts it to an evaluation license.
899984	If FGTVM was deployed in UEFI boot mode, do not downgrade to any GA version earlier than 7.2.4.

VoIP

Bug ID	Description
757477	PRACK will cause voipd crashes when the following conditions are met: `block-unknown` is disabled in the SIP profile, the PRACK message contains SDP, and PRACK fails to find any related previous transactions (this is not a usual case).
887384	SIP session is dropped by ALG with `media type doesn't match` message.

Web Filter

Bug ID	Description
766126	Block replacement page is not pushed automatically to replace the video content when using a video filter.
856793	In flow mode, URL filter configuration changes cause a spike in CPU usage of the IPS engine process.
863728	The urlfilter process causes a memory leak, even when the firewall policy not using the web filter feature.
878442	FortiGuard block page image (logo) is missing when the `Fortinet-Other` ISDB is used.

WiFi Controller

Bug ID	Description
807605	FortiOS exhibits segmentation fault on hostapd on the secondary controller configured in HA.
824441	Suggest replacing the *IP Address* column with *MAC Address* in the *Collected Email* widget.
825182	The 6 GHz channel lists should be updated according to the latest WiFi country region channels map.
828901	Connectivity loss occurs due to switch and FortiAPs (hostapd crash).
831736	Application hostapd crash found on FG-101F.
834644	A hostapd process crash is shown in device crash logs.
835783	CAPWAP traffic is not offloaded when re-enabling `capwap-offload`.
837130	Wireless client shows portal related webpage while doing MAC authentication with MAB mode.
846730	*Dynamic VLAN assignment* is disabled in the GUI when editing an SSID with `radius mac-auth` and `dynamic-vlan` enabled.
856038	The `voice-enterprise` value changed after upgrading.
856830	HA FortiGate encounters multiple hostapd crashes.
857084	Hostapd segmentation fault signal 6 occurs upon HA failover.
857140	Hostapd segmentation fault signal 11 occurs upon RF chamber setup.
857975	The cw_acd process appears to be stuck, and is sending several access requests for MAC authentication.
858653	Invalid wireless MAC OUI detected for a valid client on the network.
861552	Wireless client gets disconnect from WiFi if it is connected to a WPA2 SSID more than 12 hours.

Bug ID	Description
865260	Incorrect source IP in the self-originating traffic to RADIUS server.
868022	Wi-Fi clients on a RADIUS MAC MPSK SSID get prematurely de-authenticated by the secondary FortiGate in the HA cluster.
874997	Fetching the registration status does not always work.
882551	FortiWiFi fails to act as the root mesh AP, and leaf AP does not come online.
887829	Add support for G-series FortiAP models in syntax XML export files.
891625	Quarantined STA connected to a long interface name VAP is not moved to quarantined VLAN 4093.
892575	MPSK SSID with `mpsk-schedules` stopped working after the system time was changed due to daylight saving time.
900605	NAS-ID is not updated immediately after modifying it in the applied RADIUS server when the `wpad-process-count` is set to a non-zero value.

ZTNA

Bug ID	Description
832508	The EMS tag name (defined in the EMS server's *Zero Trust Tagging Rules*) format changed in 7.2.1 from `FCTEMS<serial_number>_<tag_name>` to `EMS<id>_ZTNA_<tag_name>`. After upgrading from 7.2.0 to 7.2.1, the EMS tag format was converted properly in the CLI configuration, but the WAD daemon is unable to recognize this new format, so the ZTNA traffic will not match any ZTNA policies with EMS tag name checking enabled.
859421	ZTNA server (access proxy VIP) is causing all interfaces that receive ARP request to reply with their MAC address.
863057	ZTNA real server address group gets unset once the FortiGate restarts.
865316	Adding an EMS tag on the *Policy & Objects > Firewall Policy* edit page for a normal firewall policy forces NAT to be enabled.
875589	An error case occurs in WAD when a client EMS tag changes.
888814	Unable to match first group attribute from SAML assertion for ZTNA rule.
945016	When NAT is enabled in a firewall policy ZTNA mode, saving it in GUI will cause NAT to be disabled.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
858921	FortiOS 7.4.0 is no longer vulnerable to the following CVE Reference: • CVE-2023-26207

Known issues

The following issues have been identified in version 7.4.0. To inquire about a particular bug or report a bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
908706	On the *Security Profiles > AntiVirus* page, a VDOM administrator with a custom administrator profile cannot create or modify an antivirus profile belonging to the VDOM. **Workaround**: set the VDOM administrator profile to *super_admin*.

Data Loss Prevention

Bug ID	Description
911291	The FortiGate does not parse the entries of the sensor from DLP signature package properly, and therefore cannot block files matching a sensor as expected. **Workaround**: reboot the FortiGate after loading the DLP signature package.

Explicit Proxy

Bug ID	Description
817582	When there are many users authenticated by an explicit proxy policy, the *Firewall Users* widget can take a long time to load. This issue does not impact explicit proxy functionality.

Firewall

Bug ID	Description
843554	If the first firewall service object in the service list (based on the order in the command line table) has a protocol type of *IP*, the GUI may incorrectly modify its protocol number whenever a new firewall service of the same protocol type *IP* is created in the GUI.

Bug ID	Description

	This silent misconfiguration can result in unexpected behavior of firewall policies that use the impacted service. For example, some 6K and 7K platforms have firewall service *ALL* (protocol type *IP*) as the first service, and this can cause the *ALL* service to be modified unexpectedly.
	Workaround: create a new service in the CLI, or move a non-IP type services to the top of the firewall service list. For example, if `ALL` is the first firewall service in the list:
	`config firewall service custom`
	`    edit "unused"`
	`        set tcp-portrange 1`
	`    next`
	`    move "unused" before "ALL"`
	`end`

895946	Access to some websites fails after upgrading to FortiOS 7.2.3 when the firewall policy is in flow-based inspection mode. **Workaround**: access is possible with one of the following settings. • Change the firewall policy inspection mode to proxy-based. • Remove the IPS security profile from the firewall policy. • Set `tcp-mss-sender` and `tcp-mss-receiver` in the firewall policy to `1300`. • Set `tcp-mss` to `1300` on the VPN tunnel interface. • Bypass the inter-VDOM link (may work in applicable scenarios, such as if the VDOM default route points to physical interface instead of an inter-VDOM).
910068	On the *Policy & Objects* > *Firewall Policy* page, if any of the interface names contain a space, the page does not load when *Interface Pair View* is selected. **Workaround**: remove all space characters in interface names referenced in policies.
912740	On a FortiGate managed by FortiManager, after upgrading to 7.4.0, the *Firewall Policy* list may show separate sequence grouping for each policy because the `global-label` is updated to be unique for each policy. **Workaround**: drag and drop the policy to the correct sequence group in the GUI, or remove the `global-label` for each member policy in the group except for the leading policy. • Policy 1 (`global-label "group1"`) • Policy 2 • Policy 3 (`global-label "group2"`) • Policy 4
919418	On the *Policy & Objects* > *Firewall Policy* page, when the interface name used in a virtual wire pair is a substring of interfaces used in a firewall policy, such policies are not displayed. For example, if a virtual wire pair consists of interfaces port1 and port2, firewall policies with port10, port11, port21, port22 are not displayed.
948393	Policy lookup should not get result with `policy_action: deny` for non-TCP protocols and non-80/443 TCP ports.
951984	The best output route may not be found for local out DNAT traffic.
967205	Changing the destination in the policy replaces applied services with service, ALL.

FortiGate 6000 and 7000 platforms

Bug ID	Description
790464	Existing ARP entries are removed from all slots when an ARP query of a single slot does not respond.
885205	IPv6 ECMP is not supported for the FortiGate 6000F and 7000E platforms. IPv6 ECMP is supported for the FortiGate 7000F platform.
887946	UTM traffic is blocked by an FGSP configuration with asymmetric routing.
888310	The FortiGate 6000 or 7000 front panel does not appear on the *Network* > *Interfaces* and *System* > *HA* GUI pages.
888447	In some cases, the FortiGate 7000F platform cannot correctly reassemble fragmented packets.
888873, 909160	The FortiGate 7000E and 7000F platforms do not support GTP and PFCP load balancing.
891430	The FortiGate 6000 and 7000 *System Information* dashboard widget incorrectly displays the management board or primary FIM serial number instead of the chassis serial number. Use `get system status` to view the chassis serial number.
891642	FortiGate 6000 and 7000 platforms do not support managing FortiSwitch devices over FortiLink.
896758	Virtual clustering is not supported by FortiGate 6000 and 7000 platforms.
897629	The FortiGate 6000 and 7000 platforms do not support EMAC VLANs.
899905	Adding a FortiAnalyzer to a FortiGate 6000 or 7000 Security Fabric configuration from the FortiOS GUI is not supported. **Workaround**: add the FortiGate 6000 or 7000 to the FortiAnalyzer from the FortiAnalyzer GUI.
901695	On FortiGate 7000F platforms, NP7-offloaded UDP sessions are not affected by the `udp-idle-timer` option of the `config system global` command.
902545	Unable to select a management interface LAG to be the direct SLBC logging interface.
905450	SNMP walk failed to get the BGP routing information.
905692	On a FortiGate 6000 or 7000, the active worker count returned by the output of `diagnose sys ha dump-by group` can be incorrect after an FPC or FPM goes down.
905788	Unable to select a management interface LAG to be the FGSP session synchronization interface.
907140	Authenticated users are not synchronized to the secondary FortiGate 6000 or 7000 chassis when the secondary chassis joins a primary chassis to form an FGCP cluster.
907695	The FortiGate 6000 and 7000 platforms do not support IPsec VPN over a loopback interface or an NPU inter-VDOM link interface.
908576	On a FortiGate 7000F, after a new FPM becomes the primary FPM, IPsec VPN dynamic routes are not synchronized to the new primary FPM. **Workaround**: reset IPsec VPN tunnels that use dynamic routing.
908674	Sessions for IPsec dialup tunnels that are configured to be handled by a specific FPC or FPM may

Bug ID	Description
	be incorrectly sent to a different FPC or FPM, resulting in traffic being blocked.
910095	FGCP session synchronization may not synchronize all sessions on FortiGate 6000 and 7000 models.
910824	On the FortiGate 7000F platform, fragmented IPv6 ICMP traffic is not load balanced correctly when the `dp-icmp-distribution-method` option under `config load-balance` is set to `dst-ip`. This problem may also occur for other `dp-icmp-distribution-method` configurations.
910883	The FortiGate 6000s or 7000s in an FGSP cluster may load balance FTP data sessions to different FPCs or FPMs. This can cause delays while the affected FortiGate 6000 or 7000 re-installs the sessions on the correct FPC or FPM.
911244	FortiGate 7000E IPv6 routes may not be synchronized correctly among FIMs and FPMs.
937879	FortiGate-7000F chassis with FIM-7941Fs cannot load balance fragmented IPv6 TCP and UDP traffic. Instead, fragmented IPv6 TCP and UDP traffic received by the FIM-7941F interfaces is sent directly to the primary FPM, bypassing the NP7 load balancers. IPv6 ICMP fragmented traffic load balancing works as expected. Load balancing fragmented IPv6 TCP and UDP traffic works as expected in FortiGate-7000F chassis with FIM-7921Fs.
973407	FIM installed NPU session causes the SSE to get stuck.

GUI

Bug ID	Description
825598	The FortiGate may display a false alarm message `TypeError [ERR_INVALID_URL]: Invalid URL` in the crashlog for the node process. This error does not affect the operation of the GUI.
898902	In the *System > Administrators* dialog, when there are a lot of VDOMs (over 200), the dialog can take more than one minute to load the *Two-factor Authentication* toggle. This issue does not affect configuring other settings in the dialog. **Workaround**: use the CLI to configure `two-factor-authentication` under `config system admin`.
905200	When logged in to the GUI of a non-management VDOM and trying to complete the *Migrate Config with FortiConverter* step in the startup menu, the page does not update and the loading spinner is stuck. **Workaround**: in the browser's URL bar, remove everything after the `/prompt`, log in to the FortiGate GUI with the management VDOM, and enable the *Don't show again* toggle on the *Migrate Config with FortiConverter* page in the startup menu.
905795	Random FortiSwitch is shown as offline on the GUI when it is actually online.

HA

Bug ID	Description

916903,
919982,
922867
	When an HA management interface is configured, the GUI may not show the last interface entry in `config system interface` on several pages, such as the interface list, policy list, address list, and DNS servers page. This is a GUI-only display issue and does not impact the underlying operation of the affected interface.
	Workaround: create a dummy interface to be the last entry in the `config system interface` table.
	`config system interface`
	`    edit <name>`
	`        set vdom "root"`
	`        set status down`
	`        set type loopback`
	`        set snmp-index <integer>`
	`    next`
	`end`

Hyperscale

Bug ID	Description
802182	After successfully changing the VLAN ID of an interface from the CLI, an error message similar to `cmdb_txn_cache_data(query=log.npu-server,leve=1) failed` may appear.
817562	NPD/LPMD cannot differentiate the different VRFs, and considers all VRFs as 0.
915796	With an enabled hyperscale license, in some cases with exception traffic (like ICMP error traverse), the FortiGate may experience unexpected disruptions when handling the exception traffic.

Intrusion Prevention

Bug ID	Description
926639	Constant reloading of the shared memory external domain table is causing high CPU usage due to lock contention when reloading the table.

IPsec VPN

Bug ID	Description
852051	Unexpected condition in IPsec engine on SoC4 platforms leads to intermittent IPsec VPN operation.

Log & Report

Bug ID	Description
860822	When viewing logs on the *Log & Report* > *System Events* page, filtering by *domain\username* does not display matching entries. **Workaround**: use a double backslash (*domain\\username*) while filtering or searching by username only without the domain.

Proxy

Bug ID	Description
783549	An error condition occurs in WAD caused by multiple outstanding requests sent from the client to server with UTM enabled.
845361	A rare error condition occured in WAD caused by compounded SMB2 requests.
899358	Proxy-based deep inspection connection issue occurs.

Security Fabric

Bug ID	Description
862424	On a FortiGate that has large tables (over 1000 firewall policies, address, or other tables), security rating reports may cause the FortiGate to go into conserve mode.
935846	Adding a real device to autolink to a serial number model device results in an error.

SSL VPN

<table>
<tr><th>Bug ID</th><th>Description</th></tr>
<tr><td>887674</td><td>FortiGate will intermittently stop accepting new SSL VPN connections across all VDOMs.</td></tr>
<tr><td>922446</td><td>SSL VPN service over PPPoE interface does not work as expected if the PPPoE interface is configured with <code>config system pppoe-interface</code>.
<pre>
config system pppoe-interface
    edit <name>
        set device <string>
        set username <string>
        set password <password>
    next
end

config vpn ssl settings
    set source-interface <PPPoE_interface_name>
end
</pre>
This issue is also observed on VNE tunnel configurations.
<b>Workaround</b>: configure the PPPoE interface with <code>config system interface</code> to allow the SSL VPN service to continue to work over the PPPoE interface.
<ol>
<li>Delete the existing PPPoE interface and related configuration:
<pre>
config system pppoe-interface
    delete <PPPoE_interface_name>
end
</pre></li>
<li>Configure the PPPoE interface under <code>config system interface</code>:
<pre>
config system interface
    edit <PPPoE_interface_name>
        set mode pppoe
        set username <string>
        set password <password>
    next
end
</pre></li>
<li>Apply this interface in the SSL VPN settings:
<pre>
config vpn ssl settings
    set source-interface <PPPoE_interface_name>
end
</pre></li>
</ol></td></tr>
</table>

Switch Controller

Bug ID	Description

904640	When a FortiSwitch port is reconfigured, the FortiGate may incorrectly retain old detected device data from the port that results in an unexpected number of detected device MACs for the port. Using `diagnose switch-controller mac-cache show` to check the device data can result in the *Device Information* column being blank on the *WiFi & Switch Controller > FortiSwitch Ports* page or in the *Assets* widget.
	Workaround: disable the device retention cache to remove old device data.
	`config switch-controller global`
	`    set mac-retention-period 0`
	`end`

911232	Security rating shows an incorrect warning for unregistered FortiSwitches on the *WiFi & Switch Controller > Managed FortiSwitches*. **Workaround**: select a FortiSwitch and use the *Diagnostics & Tools* tooltip to view the correct registration status.

System

Bug ID	Description
842159	FortiGate 200F interfaces stop passing traffic after some time.
861962	When configuring an 802.3ad aggregate interface with a 1 Gbps speed, the port's LED is off and traffic cannot pass through. Affected platforms: 110xE, 220xE, 330xE, 340xE, and 360xE.
873391	If the FortiGate is added to FortiManager using the IPv6 address and tunnel is down for some reason, the FortiGate will not reconnect to FortiManager since `fmg` under `system central-management` is not set properly. **Workaround**: set `fmg` manually or connect from the FortiManager side.
884023	When a user is logged in as a VDOM administrator with restricted access and tries to upload a certificate (*System > Certificates*), the *Create* button on the *Create Certificate* pane is greyed out.
904486	The FortiGate may display a false alarm message and subsequently initiate a reboot.
912383	FGR-70F and FGR-70F-3G4G failed to perform regular reboot process (using `execute reboot` command) with an SD card inserted.
921134	GUI is inaccessible when using a SHA1 certificate as `admin-server-cert`.
923364	System goes into halt state with `Error: Package validation failed...` message in cases where there are no engine files in the FortiGate when the BIOS security level is set to 2. **Workaround**: set the BIOS security level to 0 or 1.

User & Authentication

Bug ID	Description
823884	When a search is performed on a user *(User & Authentication* > *User Definition* page), the search results highlight all the groups the user belongs to.
923164	EAP proxy daemon may keep reloading after updating the certificate bundle. **Workaround**: reboot the system.

VM

Bug ID	Description
924689	FortiGate VMs in an HA cluster deployed on the Hyper-V platform may get into an unresponsive state where multiple services are impacted: GUI management, CLI commands, SSL VPN sessions, DHCP assignment, traffic throughput, and reboot function. **Workaround**: reboot the FortiGate VM through the hypervisor management interface.

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.
873273	The *Automatically connect to nearest saved network* option does not work as expected when FWF-60E client-mode local radio loses connection.
903922	Physical and logical topology is slow to load when there are a lot of managed FortiAP (over 50). This issue does not impact FortiAP management and operation.
904349	Unable to create FortiAP profile in the GUI for dual-5G mode FortiAP U231F/U431F models. **Workaround**: use the CLI to update the profile to dual-5G mode.
944465	On the *WiFi & Switch Controller* > *Managed FortiAPs* page of a non-management VDOM, the *Register* button is unavailable in the *Device Registration* pane.

Built-in AV Engine

AV Engine 7.00015 is released as the built-in AV Engine. Refer to the AV Engine Release Notes for information.

Built-in IPS Engine

IPS Engine 7.00493 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