Release Notes

FortiOS 7.6.3

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, 2025
FortiOS 7.6.3 Release Notes
01-763-1125831-20250417

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-04-16	Initial release.
2025-04-16	Updated Resolved issues on page 34 and Known issues on page 55.
2025-04-17	Updated Resolved issues on page 34 and Known issues on page 55.

Introduction and supported models

This guide provides release information for FortiOS 7.6.3 build 3150.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.6.3 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60F, FG-61F, FG-70F, FG-71F, FG-80F, FG-80F-BP, FG-80F-DSL, FG-80F-POE, FG-81F, FG-81F-POE, FG-90G, FG-91G, FG-100F, FG-101F, FG-120G, FG-121G, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-400F, FG-401F, FG-500E, FG-501E, FG-600E, FG-601E, FG-600F, FG-601F, FG-800D, FG-900D, FG-900G, FG-901G, FG-1000D, FG-1000F, FG-1001F, FG-1100E, FG-1101E, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3000F, FG-3001F, FG-3100D, FG-3200D, FG-3200F, FG-3201F, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3700F, FG-3701F, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-4800F, FG-4801F, FG-5001E, FG-5001E1, FG-6000F, FG-7000E, FG-7000F
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60F, FWF-61F, FWF-80F-2R, FWF-80F-2R-3G4G-DSL, FWF-81F-2R, FWF-81F-2R-3G4G-DSL, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-60F, FGR-60F-3G4G, FGR-70F, FGR-70F-3G4G
FortiFirewall	FFW-1801F, FFW-2600F, FFW-3001F, FFW-3501F, FFW-3980E, FFW-4200F, FFW-4400F, FFW-4401F, FFW-4801F, FFW-VM64, FFW-VM64-KVM
FortiGate VM	FG-ARM64-AWS, FG-ARM64-AZURE, FG-ARM64-GCP, FG-ARM64-KVM, FG-ARM64-OCI, FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VM64-XEN

FortiGate 6000 and 7000 support

FortiOS 7.6.3 supports the following FG-6000F, FG-7000E, and FG-7000F models:

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

Special notices

FortiGate cannot restore configuration file after private-data-encryption is re-enabled

In a new enhancement, enabling `private-data-encryption` will utilize a randomly generated private key. Therefore, FortiGate cannot restore the configuration file in the following sequence:

1. `private-data-encryption` enabled with random key, and configuration is backed up.
2. `private-data-encryption` disabled.
3. `private-data-encryption` enabled again, with new random key.
4. Restore configuration file in step 1.

When disabling `private-data-encryption`, a warning in the CLI will be displayed:

```
This operation will restore system default data encryption key!

Previous config files encrypted with the private key cannot be restored after this
operation!

Do you want to continue? (y/n)y
```

FortiManager support for updated FortiOS private data encryption key

With the introduction of FortiOS 7.6.1, Fortinet has updated the private-data-encryption key feature. Administrators are no longer required to manually input a 32-digit hexadecimal `private-data-encryption` key. Instead administrators simply enable the command, and a random `private-data-encryption` key is generated.

Previous FortiOS CLI behavior

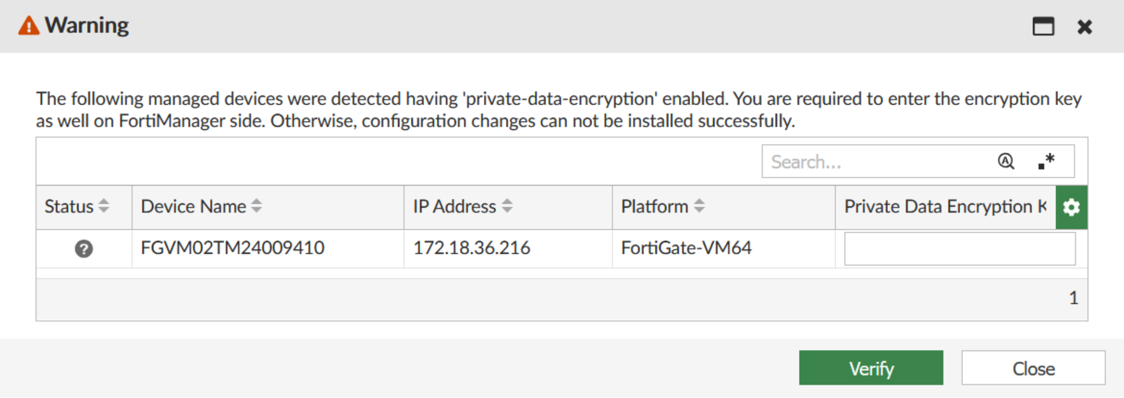
```
config system global
    set private-data-encryption enable
end
Please type your private data encryption key (32 hexadecimal numbers):
12345678901234567890123456789abc
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
12345678901234567890123456789abc
Your private data encryption key is accepted.
```

New FortiOS CLI behavior

```
config system global
    set private-data-encryption enable
end
This operation will generate a random private data encryption key!
Previous config files encrypted with the system default key cannot be restored after this
operation!
Do you want to continue? (y/n)y
Private data encryption key generation succeeded!
```

FortiManager behavior

Support for the FortiGate `private-data-encryption` key by the Device Manager in FortiManager 7.6.2 and earlier is unchanged. It automatically detects the remote FortiGate `private-data-encryption` key status and prompts the administrator to manually type the private key (see picture below). FortiManager 7.6.2 and earlier does not support the updated, random `private-data-encryption` key as the administrator will have no knowledge of the key generated in the FortiOS CLI command above. It will be supported in a later version of FortiManager.



The following managed devices were detected having 'private-data-encryption' enabled. You are required to enter the encryption key as well on FortiManager side. Otherwise, configuration changes can not be installed successfully.

Status	Device Name	IP Address	Platform	Private Data Encryption K
?	FGVM02TM24009410	172.18.36.216	FortiGate-VM64	

1

FortiOS upgrade behavior

If in FortiOS 7.4.5 or 7.6.0 the 32-digit hexadecimal private key is enabled, and then the FortiGate device is upgraded to 7.6.1, the 32-digit hexadecimal `private-data-encryption` key is preserved. As a result, FortiManager 7.6.2 and earlier is aware of the 32-digit hexadecimal `private-data-encryption` key and can continue to manage the FortiGate device. However, if the `private-data-encryption` key is enabled after an upgrade of FortiOS to 7.6.1, FortiManager 7.6.2 and earlier no longer can manage FortiGate devices running FortiOS 7.6.1.

Hyperscale incompatibilities and limitations

See Hyperscale firewall incompatibilities and limitations in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 7.6.3 features.

Hyperscale NP7 hardware limitation

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

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

FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 7.6.3 features.

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

FortiGate VM memory and upgrade

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

RADIUS vulnerability

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

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

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

Message-authenticator checking is made mandatory under UDP/TCP. It is not mandatory when using TLS. Therefore, if FortiGate is using UDP/TCP mode without RADSEC, the RADIUS server should be patched to ensure the message-authenticator attribute is used in its RADIUS messages.

Affected Product Integration

- FortiAuthenticator version 6.6.1 and older
- Third party RADIUS server that does not support sending the message-authenticator attribute

Solution

- Upgrade FortiAuthenticator to version 6.6.2, 6.5.6 or 6.4.10 and follow the upgrade instructions: https://docs.fortinet.com/document/fortiauthenticator/6.6.2/release-notes/859240/upgrade-instructions
- Upgrade the RADIUS server and/or enable it to send the correct message-authenticator attribute

Changes to NP7 traffic shaping

The following known issues for the Queuing based Traffic Management (QTM) module on NP7 are fixed:

- Incorrect checksum for fragments after QTM.
- Packets longer than 6000 bytes cause QTM to hang.
- Refreshing causes QTM to hang.
- MTU is not honored after QTM, so the packet is not fragmented.

As a result of these changes, you can no longer use the following command to change QoS type used for traffic shaping for sessions offloaded to NP7 processors:

```
config system npu
    set default-qos-type {policing | shaping}
end
```

Instead, `default-qos-type` can only be set to `policing`.

For NP7 sessions, policy traffic shaping, per-IP shaping, and regular port shaping (outbandwidth enabled on an interface without a shaping profile) always use the NP7 accounting and traffic shaping module (called the TPE module). This is the same as changing the `default-qos-type` to `policing`.

For NP7 sessions, shaping profiles on interfaces now only use QTM for traffic shaping (equivalent to setting `default-qos-type` to `shaping`). Shaping profiles on interfaces are also called Multiclass shaping (MCS). The interface can be a physical interface, LAG interface, and VLAN interface (over physical or LAG). The FortiGate supports shaping profiles on a maximum of 100 interfaces.

VNE interfaces and /32 netmask

The IPv4 address field for VNE interfaces enforces a /32 netmask. This change requires manually adding a route to the interface on the peer side of the VNE tunnel to reach it.

SSL VPN tunnel mode no longer supported

Starting in FortiOS 7.6.3, the SSL VPN tunnel mode feature is no longer available in the GUI and CLI. Settings will not be upgraded from previous versions. This applies to all FortiGate models.

To ensure uninterrupted remote access, customers must migrate their SSL VPN tunnel mode configuration to IPsec VPN before upgrading to FortiOS 7.6.3.

See Migration from SSL VPN tunnel mode to IPsec VPN in the FortiOS *7.6 New Feature* guide for detailed steps on migrating to IPsec VPN before upgrade.

A complete migration guide can be found in the following links:

- For FortiOS 7.6, see SSL VPN to IPsec VPN Migration.
- For FortiOS 7.4, see SSL VPN to IPsec VPN Migration.

Agentless VPN (formerly SSL VPN web mode) not supported on FortiGate 40F, 60F, and 90G series models

On the following FortiGate models, the Agentless VPN (formerly SSL VPN web mode) feature is no longer available from the GUI or CLI. Settings will not be upgraded from previous versions.

The affected models include:

- FGT-40F/FWF-40F and variants
- FGT-60F/FWF-60F
- FGT-61F/FWF-61F
- FGR-60F and variants (2GB versions only)
- FGT-90G and FGT-91G

To confirm if your FortiGate model has 2 GB RAM, enter `diagnose hardware sysinfo conserve` in the CLI, and check that the total RAM value is below 2000 MB (1000 MB = 1 GB).

On these FortiGate models, consider migrating to using IPsec Dialup VPN for remote access.

See SSL VPN to IPsec VPN Migration for more information.

FortiGate models not listed above will continue to support Agentless VPN (formerly SSL VPN web mode). However, SSL VPN tunnel mode is not longer supported on any models.

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

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

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

2 GB RAM FortiGate models no longer support Security Rating and Security Fabric topology

To enhance the stability of physical FortiGate devices devices with 2 GB RAM, the Security Rating feature and Security Fabric topology visibility have been removed. These changes prioritizes device stability and mitigate potential performance issues. For more information, see Optimizations for physical FortiGate devices with 2 GB RAM.

Changes in CLI

Bug ID	Description

1080094	Add `sta-offline-ip2mac-cleanup` and `sta-offline-cleanup` in wireless timers:
	`config wireless-controller timers`
	`    set sta-offline-ip2mac-cleanup 300`
	`    set sta-offline-cleanup 300`
	`end`
	Add `max-sta-offline-ip2mac` and `max-sta-offline` in wireless global:
	`config wireless-controller global`
	`    set max-sta-offline-ip2mac 1024`
	`    set max-sta-offline 1024`
	`end`

1098022	Increase the maximum IPS signature hold time from 7 days to 21 days.
1142013	Policing improvement for QTM by limiting buffer size or switching to TPE (`shaping-profile mode of config`).

Changes in default behavior

<table>
<tr><th>Bug ID</th><th>Description</th></tr>
<tr><td>1020808</td><td>Certificate Rekeying During Re-enrollment
Previously, the FortiOS EST protocol implementation reused the same private key for certificate renewal. Starting with version 7.4.6 and 7.6.3, FortiOS allows certificates generated through the EST protocol to undergo a rekey process during re-enrollment, enhancing security and flexibility.
A new option has been added to specify whether to use an existing key or generate a new one, with the default now set to create a new one.<pre>
config vpn certificate local
    edit <name>
        set est-regeneration-method {create-new-key | use-existing-key}
    next
end
</pre></td></tr>
<tr><td>1055443</td><td>Add <code>ipv4/v6-session-quota</code> back for software sessions in hyperscale VDOM.</td></tr>
<tr><td>1106205</td><td>The default IPS database setting for FGT-20xE models has been updated from extended to regular to optimize the size of IPS signatures.
<b>Note</b>: The default FOS CLI setting in <code>config ips global</code> remains extended. This ensures that the IPS database configuration will change only during a factory reset and not during an upgrade, which prevents any disruption to existing customer setups. Additionally, if a user unsets the database after a factory reset, the database CLI configuration under <code>config ips global</code> will revert to the default extended setting.</td></tr>
</table>

Changes in table size

Bug ID	Description
1024218	On FortiGate 90xG models, the number of firewall policies is increased from 10000 to 50000.
1129770	On mid-range FortiGate models, increase the number of IP addresses from 300,000 to 1,000,000. On high-end FortiGate models, increase the number of IP addresses from 300,000 to 5,000,000.

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
1118577	FortiGate-VM supports the AliCloud ecs.g8i instance family.

GUI

See GUI in the New Features Guide for more information.

Feature ID	Description
1076795	A setting for enabling/disabling private data encryption can be found in the GUI under *System > Settings* in the *Security* section.
1117904	Enhanced global search in the top header menu provides quicker Command Palette access. This menu allows fast navigation to GUI pages, running actions like opening the CLI console, executing diagnostic commands, and searching configurations.

LAN Edge

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

Feature ID	Description
984616	Introducing Split Tunnel Mode for FortiExtender in LAN extension mode. With this feature, specific traffic patterns defined by the split service are sent directly to the FEXT local gateway. This reduces the load on the central FGT by routing less traffic through the LAN extension tunnel, thereby enhancing efficiency and network performance.
1058404	FortiGate can now register authorized FEXT (FortiExtender) devices. Previously, it could only register FAP (FortiAP) and FSW (FortiSwitch) devices. This new feature ensures comprehensive network management by including all connected devices.

Network

See Network in the New Features Guide for more information.

Feature ID	Description
1025233	Previously, support for inspecting TLS connections that utilize ECH was added in proxy mode. In this enhancement, flow mode can now support the following: • Inspect DNS over TLS (DoT) and DNS over HTTPS (DoH) traffic • Strip the ECH response returned from the DNS server over DoT or DoH • Block TLS ClientHello that uses ECH, allowing TLS to fall back to using a plaintext ClientHello
1082763	Enhanced PIM support for VRFs is now available with the GUI

Policy & Objects

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

Feature ID	Description
1003586	To support configuration of isolator servers for explicit web proxy and transparent web proxy types, added GUI enhancements in *Network > Explicit Proxy* and *Policy & Objects > Proxy Policy* pages.
1082240	The NAC Policy GUI now allows users to select device categories from a drop-down list (such as FortiCam, FortiFone, FortiAP), enhancing user experience by simplifying the selection process. Previously, users had to manually type in text such as 'MacOS' or 'IP Camera' to match device discovery.
1094162	The `diag sys npu-session list-brief` command now includes additional values for timeout, duration, and policy-id and an improved filter that includes EIF sessions to enhance its functionality and filtering capabilities.
1107413	Support for configuring users and groups in policy routes has been added, allowing administrators to use users and user groups as source filters. This enhancement provides granular control over network traffic, enabling organizations to prioritize resources for specific users or groups.
1108832	Adds support for displaying real-time traffic statistics in QTM, offering users a more intuitive and comprehensive view of traffic shaping performance across various interfaces on NP7/NP7Lite platform devices.

SD-WAN

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

Feature ID	Description
907576	Added support for the Fabric Overlay Orchestrator Topology dashboard widget in the GUI to provide an interactive view of hub and spoke devices previously configured using the Fabric Overlay Orchestrator feature. This dashboard widget is only available on the hub or root FortiGate device.
1094535	Introducing passive monitoring of TCP metrics per application, expanding the range of metrics measured and logged. Previously, monitoring was limited to per session with a limited set of metrics.

Security Fabric

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

Feature ID	Description

831492	This enhancement added support to allow individual FortiGate's in CSF to have their own automation setting.
	The `fabric-sync` option has been added in the `config automation setting` command.
	`config automation setting`
	`    set fabric-sync { enable | disable }`
	`end`

1058641	A `trigger-action-stitch` feature was added to FortiOS to detect and log NPU-stuck events with specific event IDs for info, warning, and error levels. This addresses previous issues where the NP7 experienced NPU-stuck problems under high load, causing CPU spikes and potential system instability. It provides real-time monitoring and logging of NPU health, helping to maintain system stability by allowing timely awareness.

Security Profiles

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

Feature ID	Description
1055921	The inline CASB security profile has been enhanced to support control factors, such as tenant information in JSON data exchanged between a web browser and a custom SaaS application. For example, for some custom SaaS applications, the URL does not change to reflect the type or identity of the user or organization when logged in, as such tenant information is exchanged using JSON data instead of through changes in the URL. With this enhancement, JSON data can be extracted using JQ filters.

<table>
<tr><th>Feature ID</th><th>Description</th></tr>
<tr><td>1074271</td><td>Enhanced the IPS engine to detect industrial Ethernet protocols, such as LLDP, GOOSE, EtherCAT, and PROFINET RT. Device detection starts to detect and log the Ethernet devices through the L2 protocol. IPS sensor detects the Ethernet protocol and logs the traffic. Custom signature rules have been enhanced with three new rule options for ethertype, mac_src, and mac_dst.</td></tr>
<tr><td>1078890</td><td>Fortinet now leverages AMQP (Advanced Message Queuing Protocol) to deliver real-time update notifications to FortiGate devices. When enabled, this feature allows FortiGate to receive notifications directly from FortiGuard, eliminating the need for polling or persistent HTTP connections. By leveraging Fortinet's cloud infrastructure, AMQP enables event-driven updates, reducing resource consumption and minimizing overhead. Notifications are pushed instantly to devices, ensuring proactive management and swift response to critical updates.
CLI configuration:
<pre>
config system fortiguard
    set subscribe-update-notification {enable | disable}
end
</pre></td></tr>
<tr><td>1091818</td><td>As cyber threats become increasingly sophisticated, traditional signature-based detection is struggling to keep up. To improve it, we are using AI/ML-based models trained on features extracted during protocol decoding (for example, HTTP traffic). These models act as classifiers, distinguishing exploits from clean traffic through supervised learning.
Instead of applying ML models blindly across all traffic, we will first use signatures for preliminary filtering, allowing AI-based detection to be more targeted and efficient. This hybrid approach will reduce false positives while maintaining high performance.
The AI/Machine Learning IPS Definitions package is downloaded by FortiOS from FortiGuard through FortiGuard updates. Devices with an active IPS subscription can download this package.
The setting is enabled by default at IPS global setting level:
<pre>
config ips global
    set machine-learning-detection {enable | disable}
end
</pre></td></tr>
<tr><td>1102608</td><td>Zero-day malware stream scanning feature enables real-time delivery of malware IOCs to FortiGate devices using fortimq daemon , eliminating the need for frequent cloud polling and reducing server load. This approach ensures that new threats are blocked within seconds, improving detection speed and response time.
FortiGate automatically maintains an up-to-date malware hash database, removing outdated entries and optimizing performance without manual intervention. By integrating seamlessly with AV profiles, this feature enhances scalability, efficiency, and overall network security against evolving malware threats.
<pre>
config antivirus profile
    edit <profile_name>
        config <protocol>
            set malware-stream {disable | block | monitor}
        end
    next
end
</pre></td></tr>
</table>

<table>
<tr><th>Feature ID</th><th>Description</th></tr>
<tr><td>1104259</td><td>A new command has been added under the GTP profile to control whether the FortiGate will block GTP Echo Requests if there is no active tunnel over the associated GTP path.
<pre><code>config firewall gtp
    edit <name>
        set echo-requires-path-in-use {enable | disable}
    next
end</code></pre></td></tr>
</table>

System

See System in the New Features Guide for more information.

<table>
<tr><th>Feature ID</th><th>Description</th></tr>
<tr><td>947069</td><td>Introducing a new desktop application developed for Windows and macOS called Fortinet Support Tool. This application is an evolution of the Fortinet Support Tool Chrome extension, formerly the FortiGate Support Tool. While the extension remains available, this new software expands its capabilities, empowering administrators to capture real-time debugging information through a REST API key generated directly on the FortiGate device.</td></tr>
<tr><td>1077192</td><td>Add FortiOS support for ACME External Account Binding (EAB) as defined in RFC 8555 section 7.3.4.
EAB is a way to associate an ACME account with an existing non-ACME account, such as a CA customer database, by adding additional information in <code>newAccount</code> requests. This additional information is used by the CA operating the ACME server to verify domain ownership by the requester without the need for human users to follow interactive natural-language instructions from the CA.
<pre><code>config vpn certificate local
    edit <name>
        set eab-key-id <key>
        set eab-key-hmac <HMAC>
    next
end</code></pre></td></tr>
<tr><td>1077562</td><td>Add statistics for traffic shaping using QTM, and add <code>egress-shaping-profile offload</code> for SoC5.</td></tr>
<tr><td>1106111</td><td>FortiTelemetry provides information about the user experience based on application and network performance, which is collected by FortiTelemetry agents that send raw metrics to FortiTelemetry Cloud for analysis. FortiTelemetry Cloud then returns "application experience score" and "application failure rate" metrics to the FortiGate acting as a FortiTelemetry Controller, and these metrics are displayed on FortiTelemetry monitor pages.</td></tr>
<tr><td>1115892</td><td>Connectivity Fault Management (CFM) has been extended to the following models: FG80F-POE and FG20xF. This enhancement allows administrators to diagnose and resolve issues in Ethernet networks efficiently.</td></tr>
</table>

VPN

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

Feature ID	Description
976976	In IPsec dial-up VPN config using IKEv2, users can now configure Remote Gateway Match and Security posture tags within the VPN tunnel configuration in the GUI.

1051144	Display GUI warnings for IKE-TCP port conflicts
	FortiOS version 7.6.1 and later by default uses TCP port 443 for encapsulating IKE and ESP traffic using TCP as transport, as shown below:
	`config system settings`
	`    set ike-tcp-port 443`
	`end`
	If administrators assign port 443 for HTTPS administrative access on an interface that is also bound to an IPsec tunnel, FortiOS will display a warning indicating that HTTPS access on that port will no longer be available. This is because port 443 is also used for IKE over TCP, and in such cases, IKE takes precedence over HTTPS, resulting in the loss of GUI access on that interface.
	In addition, FortiOS will flag a Security Posture failure under *Security Fabric > Security Rating*, specifically for the HTTPS Port Conflict with IKE Port check, indicating a configuration issue.

1058426	Added a new FortiClient Secure Internet Access (SIA) template for VPN Wizard, enabling the configuration of a Remote access IPsec VPN to ensure all FortiClient traffic is routed through FortiGate IPsec VPN tunnel for security inspection. The template allows administrators to select the desired security profile, including certificate or deep inspection, and configure policies to block access to botnet and C&C servers. Additionally, it provides an option to allow remote VPN users access to specified local subnets and local interfaces.
1070448	Add support for configuring Quantum Key Distribution (QKD) and Digital Signature Algorithm/Post-Quantum Cryptography (PQC). This feature allows you to mix keys from QKD, PQC, and traditional Diffie-Hellman (DH) key exchange, ensuring robust security. By combining different types of keys, users can achieve maximum resilience against potential threats.

ZTNA

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

Feature ID	Description
1049209	In this enhancement, Windows users signed in to their workstations using Microsoft Entra ID domain are automatically allowed access to ZTNA-protected TCP resources by using the same IdP login information. FortiGate queries Entra ID using the client’s login token to look up and validate the user. This allows single sign-on (SSO) and eliminates the extra step for each user to authenticate when they access a TCP application.

<table>
<tr><th>Feature ID</th><th>Description</th></tr>
<tr><td>1132509</td><td>
<p>Entry-level platforms with 2GB memory now support ZTNA tags in IP/MAC-based access control. Once registered with the EMS server, the platforms can synchronize posture tags and IP/MAC addresses for use in firewall policies.</p>
<p>The following settings can now be configured from CLI:</p>
<pre>
config firewall policy
    edit <id>
        set ztna-status {enable | disable}
        set ztna-ems-tag <tag>
        set ztna-ems-tag-secondary <tag>
        set ztna-geo-tag <tag>
        set ztna-ems-tag-negate {enable | disable}
    next
end
</pre>
</td></tr>
</table>

Upgrade information

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

FortiGate	Upgrade option	Details
Individual FortiGate devices	Manual update	Use the procedure in this topic. See also Upgrading individual devices in the FortiOS Administration Guide.
	Automatic update based on FortiGuard upgrade path	See Enabling automatic firmware updates in the FortiOS Administration Guide for details
Multiple FortiGate devices in a Fortinet Security Fabric	Manual, immediate or scheduled update based on FortiGuard upgrade path	See Fortinet Security Fabric upgrade on page 24 and Upgrading all devices in the FortiOS Administration Guide.

To view supported upgrade path information:

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

Fortinet Security Fabric upgrade

FortiOS 7.6.3 is verified to work with these Fortinet products. This includes:

FortiAnalyzer	• 7.6.3
FortiManager	• 7.6.3
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, FortiClient version 6.0 and later are supported.

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

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

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

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

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.6.3. When Security Fabric is enabled in FortiOS 7.6.3, all FortiGate devices must be running FortiOS 7.6.3.

Downgrading to previous firmware versions

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

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- admin user account
- session helpers
- system access profiles

Firmware image checksums

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

FortiGate 6000 and 7000 upgrade information

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

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

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

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

To perform a graceful upgrade of your FortiGate 6000 or 7000 to FortiOS 7.6.3:

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

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

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

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

2. Download the FortiOS 7.6.3 FG-6000F, FG-7000E, or FG-7000F firmware from https://support.fortinet.com.
3. Perform a normal upgrade of your HA cluster using the downloaded firmware image file.
4. When the upgrade is complete, verify that you have installed the correct firmware version.

   For example, check the FortiGate dashboard or use the `get system status` command.
5. Check the *Cluster Status* dashboard widget or use the `diagnose sys confsync status` command to confirm that all components are synchronized and operating normally.

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

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

Previous FortiOS CLI behavior:

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

New FortiOS CLI behavior after upgrade:

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

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

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

Policies that use an interface show missing or empty values after an upgrade

If local-in policy, DoS policy, interface policy, multicast policy, TTL policy, or central SNAT map used an interface in version 7.4.5, 7.6.0 GA or any previous GA version that was part of the SD-WAN zone, these policies will be deleted or show empty values after upgrading to version 7.4.6 or 7.6.1 or later.

After upgrading to version 7.4.6 or 7.6.1 GA or later, users must manually recreate these policies and assign them to the appropriate SD-WAN zone.

Managed FortiSwitch do not permit empty passwords for administrator accounts

Starting from FortiOS version 7.6.1, a managed FortiSwitch no longer permits empty passwords for the admin account. If a FortiSwitch unit was previously authorized without an admin password, the FortiGate will automatically generate a random admin password for the FortiSwitch upon upgrading to 7.6.1 or later. This change will cause the admin to lose access.

To regain access, configure a password override on the FortiGate device using the following commands:

```
config switch-controller switch-profile
    edit default
        set login-passwd-override enable
        set login-passwd <passwd>
    next
end
```

FortiSwitch units with an existing admin password will not be affected by this change.

SLBC FG-5001E primary blade fails to install image

For FG-5001E in a session-aware load balanced cluster (SLBC), all secondary blades install the image successfully. However, the primary blade fails, showing a `sync timeout` error, even with `graceful-upgrade` disabled.

Product integration and support

The following table lists FortiOS 7.6.3 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 0319 and later (needed for FSSO agent support OU in group filters) ◦ Windows Server 2022 Standard ◦ Windows Server 2022 Datacenter ◦ Windows Server 2019 Standard ◦ Windows Server 2019 Datacenter ◦ Windows Server 2019 Core ◦ Windows Server 2016 Datacenter ◦ Windows Server 2016 Standard ◦ Windows Server 2016 Core ◦ Windows Server 2012 Standard ◦ Windows Server 2012 R2 Standard ◦ Windows Server 2012 Core ◦ Novell eDirectory 8.8
AV Engine	• 7.00040
IPS Engine	• 7.01040

See also:

- Virtualization environments on page 30
- Language support on page 30
- Agentless VPN support on page 31
- FortiExtender modem firmware compatibility on page 31

Virtualization environments

The following table lists hypervisors and recommended versions.

Hypervisor	Recommended versions
Citrix Hypervisor	• 8.2 Express Edition, CU1
Linux KVM	• Ubuntu 22.04.3 LTS • Red Hat Enterprise Linux release 9.4 • SUSE Linux Enterprise Server 12 SP3 release 12.3
Microsoft Windows Server	• Windows Server 2022
Windows Hyper-V Server	• Microsoft Hyper-V Server 2022
Open source XenServer	• Version 3.4.3 • Version 4.1 and later
VMware ESXi	• Versions 6.5, 6.7, 7.0, and 8.0.

Language support

The following table lists language support information.

Language support

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

Agentless VPN support

The following table lists the operating systems and web browsers supported by Agentless VPN (formerly SSL VPN web mode). See also SSL VPN tunnel mode no longer supported on page 12.

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

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

FortiExtender modem firmware compatibility

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

FortiExtender model	Modem firmware image name	Modem firmware file on Support site	Geographical region
FEX-101F-AM	FEM_EM06A-22-1-1	FEM_EM06A-22.1.1-build0001.out	America
FEX-101F-EA	FEM_EM06E-22-01-01	FEM_EM06E-22.1.1-build0001.out	EU
	FEM_EM06E-22.2.2	FEM_EM06E-22.2.2-build0002.out	EU

FortiExtender model	Modem firmware image name	Modem firmware file on Support site	Geographical region
FEX-201E	FEM_06-19-0-0-AMEU	FEM_06-19.0.0-build0000-AMEU.out	America and EU
	FEM_06-19-1-0-AMEU	FEM_06-19.1.0-build0001-AMEU.out	America and EU
	FEM_06-22-1-1-AMEU	FEM_06-22.1.1-build0001-AMEU.out	America and EU
	FEM_06-22-1-2-AMEU	FEM_06-22.1.2-build0001-AMEU.out	America and EU
FEX-201F-AM	FEM_07A-22-1-0-AMERICA	FEM_07A-22.1.0-build0001-AMERICA.out	America
	FEM_07A-22-2-0-AMERICA	FEM_07A-22.2.0-build0002-AMERICA.out	America
FEX-201F-EA	FEM_07E-22-0-0-WRLD	FEM_07E-22.0.0-build0001-WRLD.out	World
	FEM_07E-22-1-1-WRLD	FEM_07E-22.1.1-build0001-WRLD.out	World
FEX-202F-AM	FEM_07A-22-1-0-AMERICA	FEM_07A-22.1.0-build0001-AMERICA.out	America
	FEM_07A-22-2-0-AMERICA	FEM_07A-22.2.0-build0002-AMERICA.out	America
FEX-202F-EA	FEM_07E-22-1-1-WRLD	FEM_07E-22.1.1-build0001-WRLD.out	World
FEX-211E	FEM_12-19-1-0-WRLD	FEM_12-19.1.0-build0001-WRLD.out	World
	FEM_12-19-2-0-WRLD	FEM_12-19.2.0-build0002-WRLD.out	World
	FEM_12-22-1-0-AMEU	FEM_12-22.0.0-build0001-AMEU.out	America and EU
	FEM_12-22-1-1-WRLD	FEM_12-22.1.1-build0001-WRLD.out	World
FEV-211F_AM	FEM_12_EM7511-22-1-2-AMERICA	FEM_12_EM7511-22.1.2-build0001-AMERICA.out	America
FEV-211F	FEM_12-22-1-0-AMEU	FEM_12-22.1.0-build0001-AMEU.out	World
FEX-211F-AM	FEM_12_EM7511-22-1-2-AMERICA	FEM_12_EM7511-22.1.2-build0001-AMERICA.out	America
FEX-212F	FEM_12-19-2-0-WRLD	FEM_12-19.2.0-build0002-WRLD.out	World
	FEM_12-22-1-1-WRLD	FEM_12-22.1.1-build0001-WRLD.out	World
FEX-311F	FEM_EM160-22-02-03	FEM_EM160-22.2.3-build0001.out	World
	FEM_EM160-22-1-2	FEM_EM160-22.1.2-build0001.out	World

FortiExtender model	Modem firmware image name	Modem firmware file on Support site	Geographical region
FEX-511F	FEM_RM502Q-21-2-2	FEM_RM502Q-21.2.2-build0003.out	World
	FEM_RM502Q-22-03-03	FEM_RM502Q-22.3.3-build0004.out	World
	FEM_RM502Q-22-04-04-AU	FEM_RM502Q-22.4.4-build0005_AU.out	Australia
	FEM_RM502Q-22-1-1	FEM_RM502Q-22.1.1-build0001.out	World
	FEM_RM502Q-22-2-2	FEM_RM502Q-22.2.2-build0002.out	World

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

To download the modem firmware:

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

Resolved issues

The following issues have been fixed in version 7.6.3. To inquire about a particular bug, please contact Customer Service & Support.

Agentless VPN (formerly SSL VPN web mode)

See also SSL VPN tunnel mode no longer supported on page 12.

Bug ID	Description
1017304	SSL VPN web mode missing several security headers in the HTTP response.
1058211	Traffic could not go though SSL VPN tunnel when DTLS is enabled with a loopback interface as source address.
1077157	FortiGate sends out expired server certificate for a given SSL VPN realm, even when the certificate configured in `virtual-host-server-cert` has been updated.
1083262	FNBAMD session hangs after a massive authorization request.
1036557, 1091173	Performance degradation occurs in SSL-VPN due to connection/session timeout management issues.
1093580	SSL VPN authentication is triggered even with EMS SN check enabled.
1101837	Insufficient session expiration in SSL VPN using SAML authentication.
1102362	SSL VPN web mode missing HTTP response headers.
1107663	FortiClient 7.2.6 GA Azure auto login cannot connect after upgrade.
1111135	Log additional debug information to aid troubleshooting.
1115510	SAML metadata couldn't be generated causing SAML authentication to fail.
1126825	SSL VPN stops functioning when ssl.root interface is added to a zone used by at least one policy.

Anti Virus

Bug ID	Description
1054835	Large file downloads take longer than expected due to a WAD process issue.
1100819	SMB traffic fails when the file server uses AES-256-GCM/CCM encryption with FortiOS.
1111973	Unable to create an AV profile on devices that have 2 GB RAM.

Application Control

Bug ID	Description
1064413	When using SD-WAN load balancing, some sites are slow or inaccessible when the Application Control action is set to *Allow*.

DNS Filter

Bug ID	Description
1025233	Support Encrypted Client Hello (ECH) in flow mode.
1096380	FortiGate in proxy mode sends the cached DNS response when it receives a DNS registration request.
1100282	Chrome flex OS cannot access SharePoint when using FortiGate DNS servers.

Endpoint Control

Bug ID	Description
1066250	Verification of EMS and upgrade of FGT with verified EMS should promote CA to fabric-ca.
1090981	EMS is unable to properly synchronize the FortiGate configuration for non-web ZTNA applications when FortiGate has multiple EMS units.
1093786	Expired FCEM contract generated by FortiFlex is loaded to FortiGate VM.
1098350	Sometimes the *GUI >Asset FortiClient* cannot display `ems-tag` for VPN user which make "Matched Endpoints" page missed those user.

Explicit Proxy

Bug ID	Description
1114438	Policy test feature not working on FortiProxy 7.4.5 and 7.4.6 when no wad debugs are running in the background.
1115137	Expand the `proxy-auth-timeout` maximum value.
1116555	Deep scanning occurs when accessing subcategories of websites with category-based proxy policies despite disabling subcategory checks.

Bug ID	Description
1134310	SSL exemption not working on proxy policy when partial match occurs.

Firewall

Bug ID	Description
723186	GUI should not filter out mac address type from multicast policy page.
946762	On policy list, the *ZTNA Tag* and *Secondary ZTNA Tag* options does not work when multiple tags are used in the policy.
993138	Misleading logs with subtype="ztna" appear when only virtual-server in a firewall policy.
994986	The *By Sequence* view in the Firewall policy list may incorrectly show a duplicate implicit deny policy in the middle of the list. This is purely a GUI display issue and does not impact policy operation. The *Interface Pair View* and *Sequence Grouping View* do not have this issue.
1025078, 1086315	When using a virtual server, some customers observed issues of memory usage increases and client sessions not disconnecting.
1025969	Policy enforcement fails for wildcard FQDN hosts as destination targets because the address records are not added to the wildcard entry when processing a server response for an FQDN's domain name.
1038650	On policy list, using the *Clear counter* and *Update statistic* options for a single policy should not refresh the whole policy list.
1050906	Under heavy network traffic, the Netflow session cache for sampled traffic quickly reaches the hardcoded RAM limit, causing the sFlow daemon to shut down.
1055898	HTTP/2 post without content-length is not supported in half-ssl virtual server.
1066136	Denied sessions were bidirectional and caused all traffic to be blocked.
1078662	If an interface on an NP7 platform has the `set inbandwidth XXX`, `set outbandwidth XXX`, and `set egress-shaping-profile XX` settings, the following issues may occur: • Fragment packet checksum is incorrect. • MTU is not honored when sending packets out. • QTM hangs and blocks traffic when packet size is larger than 6000 bytes.
1081542	On FortiGate, packets are dropped when UTM and ASIC offloading are enabled.
1088507	ICMP Echo replies sent through local-in-policy with virtual-patch enabled are routed through incorrect interfaces during traffic handling.
1097628	Firewall policy filter does not work well on source and destination columns for "all" and "ems" addresses.
1098208	After FortiGate exits conserve mode, some policies failed to install into the kernel at the same time.

Bug ID	Description
1101865	Unexpected trailing characters in Netflow template 257.
1103748, 111268	Threat feeds used as source or destination addresses in security policies may not match correctly.
1104208	NAT is incorrectly applied to traffic when a single SYN packet is sent to a VIP without an acknowledgment or reset.
1106112	Small platforms cannot remove FFDB shared memory files.
1107003	The local-in/central-snat/multiple policy dialog page should filter out member interfaces of SD-WAN from omniselect list.
1108540	Search in the Address group dialog box using a partial word match takes more than a minute.
1110135	Policy lookup for UDP protocol with FQDN not working.
1111263	`tcpsock` command missing PID/process name for sessions in established state.

1117165	Leaving the `apn` field empty in a GTP APN traffic shaping policy means that the policy will not match any traffic. Consequently, APN traffic shaping can only be applied to specific APNs.
	To configure GTP APN traffic shaping:
	`config gtp apn-shaper`
	`    edit <policy-id>`
	`        set apn [<apn-name> <apngrp-name> ...]`
	`        set rate-limit <limit>`
	`        set action {drop | reject}`
	`        set back-off-time <time>`
	`    next`
	`end`

1120749	If session is in SYN_SENT or SYN_RECV state, and FortiGate receives a second SYN with different ISN, it will drop the second SYN.
1121944	A firewall policy allows traffic from client to server, but no policy exists for server to client. When traffic is not matched from server to client, a block session forms that blocks traffic in both directions.
1136163	The local-in-policy session TTL does not follow the service session-ttl.
1139282	VIP with `set ldb-method http-host` sends incorrect FQDN in ClientHello to second realserver when using HTTP2.

FortiGate 6000 and 7000 platforms

Bug ID	Description
790464	After a failover, ARP entries are removed from all slots when an ARP query of single slot does not respond.
976521	High CPU usage by the node process occurs when loading 7000 policies due to fetching all statistics in one request.
998615	When doing a GUI-packet capture on FortiGate, the through-traffic packets are not captured.
1062080	SNMP query returns an error when there is a large number of BGP routes.
1078334, 1103739	High cmdbsvr CPU usage and FTP hang issues occur during scheduled automation backup executions due to automated backups appending device serial numbers to file names.
1095936	Different sensors appear in the list of FIM1 and FIM2.
1096156	GUI unreachable due to certificates and private keys mismatches in a HA setup.
1097428	The *Security Profile* menu does not appear in the GUI for Global VDOM on FortiGate 6K/7K devices despite being accessible through CLI.
1102413	Session count for VDOMs incorrect in FortiGate 6K/7K devices.
1102481	Local-in remote access issues due to incorrect destination address.
1105009	The command `execute load-balance slot manage X` fails on FortiGate 6K/7K devices when `admin-telnet` is disabled and then re-enabled.
1108181	Unexpected behavior observed in the confsyncd daemon due to an erroneous memory allocation.
1109415	New SNMP MIB table for chassis sensor.
1109601	Sometimes graceful upgrade failed from 7.4.6/7.4.7 to a later GA release.
1109963	SFF-8472 diagnostic support was not recognized on SFP transceivers in FG-7941F systems.
1112581	On the FortiGate 7000F platform, after upgrading from FortiOS 7.4.7 to 7.6.2, cmdbsvr CPU usage can be at 99% on one or more FPMs for several minutes. During high CPU usage, FortiGuard packets cannot be synchronized to the affected FPM(s).
1115656	FG-6K session filter by source interface doesn't set correct interface index.
1116862	Graceful upgrade of a FortiGate 7000E chassis to FortiOS 7.6.2 may fail for some configurations.
1118004	On a FortiGate 7000E FGCP cluster, after using the *execute ha disconnect* command to disconnect a chassis from the cluster, you can't use the special management ports to connect to the FIM in slot 2 or to any of the FPMs of either chassis. You can still connect to the FIM in slot 1.
1121918	If `ha-mgmt-intf` is enabled, then a newly joined HA slave chassis failed to sync.
1124603	Traffic shaping causes traffic drop on FG-7000F.
1130218	Policies fail when Security Posture Tags are configured on SLBC platforms due to dynamic address sync issues outside HA mode.

FortiView

Bug ID	Description
1125124	When running more than 1 million concurrent HTTP sessions across the firewall, and trying to access session list on FortiView in the GUI, packet loss and loss of a session are observed.

GUI

Bug ID	Description
919473	Unable to move/migrate interface using "Interface Integrate" feature if there is an IPsec tunnel bound to it.
1047963	High Node.js memory usage when building FortiManager in Report Runner fails. Occurs when FortiManager has a slow connection, is unreachable from the FortiGate (because FMG is behind NAT), or the IP is incorrect.
1054026	Offline license file cannot be uploaded to FGT by GUI.
1055865	NodeJS errors when event log socket is closed.
1092489	The `config system fortiguard > fortiguard-anycast` setting was changed to automatically disable when the FortiGuard page is shown on GUI.
1097405	Patch schedule minutes are ignored when set through the GUI for automatic upgrades.
1099309	The FortiOS GUI fails to load topology-related pages when temporary files generated during Security Rating operations are mistakenly read by the REST API.
1101932	Phase-2 details not seen in the *IPsec Monitor* dashboard on FortiGate GUI.
1102404	VDOM search function does not work properly if VDOM has uppercase letters.
1110382	Admin can log in to GUI (HTTPS) with password, even when *admin-https-pki-required* is enabled.
1110827	GUI shows LAN interfaces that have an IP address in the network ranges 172.31.0.0/16 or 192.168.0.0/16 to be managed by IPAM, even though the feature is globally disabled.
1111113	When launching the GUI console using Jet Stream theme, the character spacing appears wider than usual.
1112716	No log output when running debug flow on GUI.
1114658	Improve Node.js health check from forticron to use IPC server in Node.js rather than HTTP server.
1115684	FortiOS GUI ignores the FortiCare Elite contract.
1118810	In the Asset Identity Center, the tooltip for IoT/OT Vulnerabilities says OT license is inactive even with full license.

HA

Bug ID	Description
982081	After changing the status to down on the ha1 and ha2 ports, setting the status back to up does not bring up the ports.
1068674	PBA logs missing during HA failover.
1073514	In HA cluster, when a FortiToken is aggregated or revoked from a local.user, cluster is out of SYNC.
1085314, 1095879	Firewall policy page takes a long time to load on the HA Primary unit due to a loop condition between BGP and NSM when other protocols' same route is redistributed to BGP.
1087924	HA secondary unit experiences high CPU usage when frequent changes are made to CMDB on the HA primary unit.
1088956, 1101490	Duplicated logs occur in FAZ during sniffer mode operation in HA active-passive setups because both active and passive FortiGates forward L2 packets to the IPS engine, causing duplicate entries.
1091189	The passive member in an A-A HA sends traffic with the virtual mac.
1091657	SDN connector limits the API traffic flow through root VDOM or HA management VDOM.
1095786	Traffic interruption occurs when performing a manual HA failback after an initial failover in VWP setups.
1098192	Joining a FortiGate with RAID enabled in an existing cluster causes the primary to shut down due to differing RAID statuses.
1100177	In an FGSP setup, on asymmetric TCP flow during SYN/ACK packet on the other member, the TCP MSS value is not adjusted according to the firewall policy.
1101456	In a HA setup, the aggregate interface status remains up after configuring 'status down' in FortiOS due to a race condition.
1101879	Multiple SCTP expectation sessions are created during resynchronization due to a flag allowing duplication.
1105422	"Detected Tx Unit Hang" error occurs on the HA secondary, causing it to become out-of-sync.
1107137	The secondary FortiGate with an HA Reserved Management Interface cannot be accessed using HTTPS after upgrading from version 7.4.3.
1108895	In an FGSP cluster, enabling and disabling `standalone-config-sync` results in the local `dev_base` being deleted and synchronized with the peer, which leads to the absence of the `dev_base`.
1108895	In an FGSP cluster, enabling and disabling `standalone-config-sync` results in the local `dev_base` being deleted and synchronized with the peer, which leads to the absence of the `dev_base`.
1109919	Cluster experiences split-brain when EMAC interfaces are disabled within a zone.
1110498	Add IPv6 destination support under HA management interface configuration.
1113842	New LACP interface is not shown under `diagnose sys ha standalone-peers` on both FGSP members.

Bug ID	Description
1115190	The SNMP value of fgVWLHealthCheckLinkState on the secondary unit should always be set to dead(1).
1117725	HA is out of sync with checksum mismatch on CA certificate on all VDOMs.
1121117	When two HA clusters are on the same subnet, the L2 session-sync packets could be received by each other, even if they are from two different HA clusters.
1129088	The sessionsync daemon experiences high CPU usage when syncing expectation sessions under heavy SCTP traffic and FGSP enablement due to inefficiencies in the dump API.
1135866	HA second unit cannot sync firewall ZTNA dynamic address with HA primary unit after primary disables EMS server.
1137565	vSN support was added in 7.2.9, 7.4.6, and 7.6.1. However FG100F/ 101F support was missed by mistake. FG100F/ 101F does not support logical-sn.
1138763	IKE hasync loop and high memory consumption when peer address/port changes.

Hyperscale

Bug ID	Description
1013892	Unexpected behavior observed in NPD when the threat feed object attempted to update manually in the HA pair.
1055443	Add `ipv4/v6-session-quota` back for software sessions in hyperscale VDOM.
1074547	SNAT session drops occur when kernel sessions become dirty in hyperscale VDOM environments due to inconsistent NAT resource allocation between software and hardware sessions.
1093287	Using fixed-allocation IP Pools may cause NP7 NSS/PRP modules to become stuck, potentially disrupting traffic. Other PBA IP pools do not have this issue.
1094162	The `diag sys npu-session list-brief` command now includes additional values for timeout, duration, and policy-id and an improved filter that includes EIF sessions to enhance its functionality and filtering capabilities.
1108263	HA configurations are lost if `hw-sess-sync-dev` is configured with more interfaces than expected. (The expectation is two times the number of NP7 chips.)
1114113	The `get sys ha status` command does not offer detailed interface statistics for hardware session sync devices.
1115761	When handling very high traffic loads (150M 250M concurrent sessions), the system sometimes fails to free up memory, even after all sessions have been cleared and traffic has stopped.
1121524	Client could not get DHCP IP address with policy-offload-level set to full-offload.

Intrusion Prevention

Bug ID	Description
1040783	FortiGate encounters CPU usage issue due to IPSEngine utilization when using an `app-ctrl utm` profile.
1101633	Child process that loads IPS database does not have CMDB permission to write to IPS table.
1107445	Remove IPS diagnose command `diagnose ips cfgscript run`.
1113473	When IPS generates traffic log for tunnel traffic, traffic log should include outer packet details.
1121953	IPSengine processes consume memory and can lead to the conserve mode.

IPsec VPN

Bug ID	Description
1002325	When spoke re-authauthorization is enabled, shortcut tunnel rekey fails and goes down when SA expires. Shortcut tunnel flaps while it re-establishes again.
1042465	VPN interface error counter increases, traffic intermittent when NPU acceleration is enabled globally.
1049015	IPsec performance issue on Intel-based platforms occurs due to FortiOS not enabling all available IPsec drivers.
1054440	Incrementing TX and RX errors on VPN interface occur when NPU offload is disabled, busy CPU cores, or high burst traffic cause packet drops due to full queues on SoC3/Soc4 platforms.
1057558	Dialup and `loopback-asymroute disable` with multiple paths for IKE/IPsec traffic are configured. When the incoming ESP traffic changes path because of a routing change, reply traffic still egresses on the old interface, and traffic is dropped.
1059778	IPsec does not work as expected when the traffic path is from spoke dial-up to hub1, and then from hub1 to another site through a site-to-site tunnel.
1060048	Throughput is limited in Site to Site VPN connections between the FW1kF and the FWVM Google Cloud platform.
1064078	Egress shaper fails to enforce bandwidth limits on VPN ID with IPIP encapsulation IPsec interfaces due to incorrect handling of traffic forwarding across multiple network processing units.
1071769	L2TP/IPsec connection FortiGate-Windows Native VPN client breaks after the Windows client initiates the ISAKMP SA renegotiation.
1073670	Intermittent disruption observed in the IKED on secondary HA during HA split-brain when IPsec tunnels were configured with 'set assign-ip-from dhcp'.
1087651	FortiGate does not correctly utilize timeout timers for 2FA with Remote Access over FortiClient VPN IPsec (IKEv2).

Bug ID	Description
1094028	Unexpected behavior observed in the IKED after configuration changes when the phase1 monitor feature is used.
1103594	ADVPN IPsec traffic over shortcuts drops during IPsec tunnel rekey.
1103754	Failed HTTP sessions occur when passing through nTurbo due to improper handling of fragmented packets.
1107198	Transparent mode, policy-based IPsec VPN, local-out traffic automatically enters VPN.
1109028	With `set peertype one`, the FortiGate will not accept ID_IPV4_Address as peer ID for dynamic IPsec IKEv2.
1109627	IPsec VPN match-security-posture-tag feature won't work when FortiClient is behind NAT.
1112665	Static Route is marked inactive, but the VPN IPsec is up.
1113354	Group list is truncated because of fixed-size buffers.
1116825	Juniper device unable to establish IKEv1 tunnel with FGT.
1117758	FGT fails to negotiate encryption algorithm CHACHA20_POLY1305 against third- party client.
1117910	iked spikes to 99.9% if client sends FIN after ike tcp session is established.
1120003	FortiGate presents certificate information when accessed using IPsec VPN listening interface.
1127444	For ADVPN 2.0 shortcut negotiation, UDP hole punching for spoke behind NAT uses source port 500 instead of 4500.
1136536	SIA IPsec VPN authentication fails on FortiSASE when number of groups is greater than 150 user groups.

Log & Report

Bug ID	Description
1004103	An *Unable to fetch reports* error is displayed when trying to view renamed FAZ reports.
1009584	FGT-VM64 has no crash log record and event logs for license status change from *Valid* to *Warning*.
1074460	Erroneous memory allocation results in intermittent HTTPSD disruption caused by a corrupted traffic log file.
1084934	Firewall logs show *Object Object* in GUI and `dstintf="unknown-0"` in raw logs.
1087534	When trying to load a large number of logs in Log Viewer, the page keeps loading and displays a warning message.
1091064	Forward traffic does not contain `poluuid` and `policyname` fields.
1100883	Forward Traffic log fetched from FortiGate Cloud takes a long time to load on GUI.
1107571	Some WiFi Log descriptions are inaccurate.

Bug ID	Description
1116428	Observed *Device vulnerability lookup on FortiGuard* in high frequency under the system event log.
1118089	tmp files for log upload are not deleted even though FTP upload is complete.
1119147	Secondary device fails to generate reports at the set time.
1121505	On FG-200F, the *Security Tab* keeps loading on *Log* > *Details* > *Security* in Forward traffic Logs.
1122938	Syslog traffic uses the correct exit interface after a change in source interface but fails to update the source IP.
1129448	The body is partially missing from emails sent by alert mail.
1130821	IPS sensor log-attack-context output is both truncated and monitored with payload loss.

Proxy

Bug ID	Description
958200	Packets captured by IPS indicates HTTP/1.1 in case of HTTP/2 request.
988473	On FortiGate 61E and 81E models, a daemon WAD issue causes high memory usage.
1014014	FortiGate to IMAPs server connection is not working with TLS 1.2 because of client hello includes TLS1.3 parameter.
1023054	After an upgrade on a 2GB FortiGate device, the firewall policy does not switch from *Proxy-based* to *Flow-based* in the *Inspection mode* field.
1051875	The IP SNI check for `strict sni-server-cert-check` is skipped due to a WAD process issue.
1066113	Accessing certain websites through HTTPS fails when using inspect-all deep-inspection in proxy mode firewall policy.
1096728	An error case observed in the WAD, which affects some VIP traffic, is caused by erroneous memory allocation.
1107205	FortiGate encounters a WAD memory usage issue when using a secure explicit web proxy with WAD user authentication to visit certain websites.
1116771	Add a limit on the memory used by user-device-store as a percentage of the total system memory.
1121171	Large file downloads through proxy HTTP2 are slow when IPS/APP/SSL inspect-all enabled.
1126253	When VDOM configuration file is restored, it changes the no-inspection profile under ssl-ssh-profile to deep-inspection.
1126385	WAD fails to handle deep-inspection traffic under FIPS mode.

REST API

Bug ID	Description
943756	The API key `remote` could not be handled correctly for POST request `/api/v2/cmdb/vpn.certificate/remote`.
1019750	The available interfaces list is slow in configurations with many IPsec tunnel connections.
1026547	Sensor information through REST API on a FG-81F returns 404 error.
1071799	Failed to rename switch-controller managed-switch entries through the CMDB REST API.
1107698	Adding ipv6-trusthost under api-user will override ipv4-trusthost setting and allow all IPv4 soure IP addresses.

Routing

Bug ID	Description
897308	The system fib version does not match VDOM fib version in FG-1801F.
1008434	The speed-test result files are not deleted after test runs. The new test ID may collide with a previous result. In this case, the GUI may read a previously failed result and report errors.
1058283	Routing Widget is unresponsive due to high number of routes when using search to filter the routes and do route-lookup.
1058700	SD-WAN rule in load-balance mode limited to 8 active SD-WAN members.
1072311	BGP flaps occur when high L2P TPE drops are detected under heavy IPsec traffic conditions.
1080449	IPv6 prefix delegation does not add IPv6 route automatically.
1082842	The loopback interface does not appear as an outgoing option for BGP peer connections when configuring through the GUI.
1084851	When adding new static route and prefix-list using CLI, `0.0.0.0/0` takes effect, in spite of invalid format of `dst` and `prefix`.
1084907	IPv6 routes are inactive when dual stack BFD is configured.
1086944	The BGP router-id fails to reset after editing the neighbor group settings because the dialog doesn't properly handle the reset functionality.
1093215	Users can create a BGP neighbor without configuring remote-as using CLI, and after completing BGP neighbor configuration, neighbor will remain in admin down state.
1095307	When filtering an SD-WAN rule with a member, it fails to show results for physical interfaces with Alias names.
1099554	FortiGate uses link-local IPv6 address as nexthop in VLAN network, instead of global address.

Bug ID	Description
1105064	IPv6 traffic can't match the correct firewall policy in certain SD-WAN cases.
1108192	Restore image from FTP server failed using SD-WAN.
1108874	SD-WAN Default_DNS performance SLA shows all participants of Default_DNS are down.
1111233	`auto-asic-offload` disabled under `vne-interface` after upgrading from 7.4.6 to 7.6.1.
1111967	SD-WAN zone not selectable as interface in GUI for DoS policy, multicast policy, and central snat map.
1114687	SNMP response times out when querying SD-WAN health check.
1116924	In SD-WAN, when detect mode *Prefer Passive* is used, routing table is not updated in time
1118891	ADVPN shortcut is established between different transport-groups.
1119119	Inadvertent behavior observed in BGPD due to erroneous memory freeing when applying route-maps.
1122021	FortiGate disregards SD-WAN members for path selection even when they are in SLA.
1128032	Traffic fails with Fabric Overlay Orchestrator using automatic policy creation with system zones.
1129698	When FortiAnalyzer setting `interface-select-method` is `sdwan`, FortiAnalyzer connection is closed and restarted, even though SD-WAN interface doesn't change.
1133796	IPv6 routes are stuck on kernel routing table.
1138483	link-monitor daemon drops the trailing characters when a long hostname is used for SD-WAN health-check.

Security Fabric

Bug ID	Description
903922	Physical and logical topology is slow to load when there are a lot of managed FortiAP devices (over 50). This issue does not impact FortiAP management and operation.
1006397	Granular failure details for each device in a federated upgrade are now reported, allowing users to identify individual devices with specific failure reasons during the upgrade process.
1011833	FortiGate experiences a CPU usage issue in the `Node.js` daemon when there multiple administrator sessions running simultaneously.
1021684	In some cases, the *Security Fabric* topology cannot load properly and displays a *Failed to load Topology Results* error.
1090401	Error messages from netxd API calls are not displayed when running as a daemon because they are printed to stderr instead of the CLI.
1099235	Scheduled triggers do not include eventtime in log entries, causing automation scripts using %%log.eventtime%% to fail and generate filenames with missing or incorrect timestamps.

Bug ID	Description
1101806	Failed to trigger Security Rating Summary event automation stitch due to issue with log field ID.
1111619	The `replacemsg-group` in `automation-action` gets unset when system reboots.
1113463	FortiGate Azure connector fails to retrieve AKS information on AKS 1.29.5.
1119616	Externally maintained threat feed contains both resource FQDNs and IP address ranges/subnets. Entry such as <addr>/0x1 then matches half of all possible IPv4 address and causes network disruption.
1120652	Fabric topology with two devices on different VDOMs but behind the same router shows wrong VDOM data on tooltip.
1134970	Inconsistent DNS TTL behavior in Kubernetes API through SDN-Connector.

Switch Controller

Bug ID	Description
1015992	Cannot disable Lockdown ISL setting on FortiLink.
1016034	Lockdown ISL setting on FortiLink is enabled automatically after HA failover.
1108965	Config sync error due to dhcp-snooping-static-client.
1113465	VLAN configurations intermittently fail to assign on FSW ports when devices matching DPP policy come online, which is caused by a race condition during FSW initialization.
1130242	Partial SNMP community configuration gets pushed from the FGT to the FSW.
1138333	Increase efficiency of FortiLink configuration daemon memory usage.

System

Bug ID	Description
814119	`drop-overlapped-fragment {enable | disable}` does not work on NP7 platforms.
932077	Connection issue between SOC4 platform and Hirschmann GRS 105 switches since SOC4 doesn't support certain carrier extension signals.
976722	Invalid YAML files are generated when exporting configurations containing multi-value attributes or long strings with newline characters.

Bug ID	Description
992323, 1056133, 1075607, 1082413, 1084898	Traffic interrupted when traffic shaping is enabled on 9xG and 12xG.
1017941	GUI interface bandwidth shows Tetrabyte spike for Gigabyte interface. **Affected platforms**: FGT-220xE and FGT-330xE
1040137	NPD skips config parsing when policy-offload-level set to disable.
1040489	Traffic using VXLAN VTEP with a loopback over an IPsec VPN is dropped when VXLAN and IPsec are configured in different VDOMs due to incorrect tunnel creation success indicators.
1046484	After shutting down FortiGate using the "execute shutdown" command, the system automatically boots up again.
1069208	If the DHCP offer contains padding when DHCP relay is used, the DHCP relay deletes the padding before relaying the packet.
1075279	Member interfaces of VWP appear in packet capture creation dialog despite being ineligible.
1076883	When the top application bandwidth feature is disabled, the GUI process still performs the initial check for application bandwidth, which may cause FortiCron to experience high CPU usage.
1077562	Hardware egress shaping doesn't work on SOC5 when NPU offload is enabled.
1078119	Traffic is intermittently interrupted on virtual-vlan-switch on Soc5 based platforms when a multicast or broadcast packet is received.
1078568	When FortiManager adds FortiGate through serial number and is behind NAT, FortiGate cannot initiate requests to FortiManager, causing the GUI to fail in retrieving the certificate CN/SAN and resulting in an error.
1079850	HA1/HA2 ports remain down after setting status to up. Rebooting fixes the issue.
1085407	FortiGate unresponsive when `default-qos-type` is set to `shaping`.
1086268	VXLAN interface cannot be created if its underlying interface is DHCP.
1087160	NP drops traffic when VXLAN is a member of software switch in implicit mode.
1087270	Unexpected traffic increase over the FortiGate 6000 base backplane.
1089143	The time change in FOS is restored after reboot. The RTC node is not created correctly so the time change can't be kept in RTC.
1089272	The inability to view or click the "+" sign occurs when a user is assigned an admin profile with only read access, restricting actions that require write privileges.
1090372	Cannot create more than seven access profile entries on a FortiGate 40F.
1091175	Incorrect values shows on the Interface Bandwidth monitor and SNMP.
1091551	Hardware limitation on the NP7 platform causes the following QTM related issues: • Incorrect checksum for fragments after QTM.

Bug ID	Description
	• Packets longer than 6000 bytes cause QTM unresponsiveness. • Refresh issue causes QTM unresponsiveness. • MTU is not honored after QTM, so packets are not fragmented.
1095834	Memory usage of node process continuously increases when FortiManager is configured but unreachable.
1096409	EXPIRE dates cannot be displayed properly when displaying the output of `get sys fortiguard-service status`.
1096878	DNS cache flushing occurs too frequently due to unnecessary interface-reload events triggered by DHCP6 packets and SLAAC updates.
1099770	NP7 drops encrypted GRE packets that have checksum bit set (1) due to invalid checksum.
1101392	Administrators can execute the command `diagnose sys ha reset-uptime` when the permissions of Admin Profile is set to Read.
1102416	Cannot push `config sfp-dsl enable` and vectoring under interface.
1103146	Duplicated RADIUS packets are captured by the sniffer when performing firewall authentication with a RADIUS server.
1104410	The FortiGate-120G SFP ports fail to establish connectivity when configured with `set speed 1000full` due to improper auto-negotiation handling.
1105989	System global configuration lost due to port collision.
1105995	The switch MTU doesn't set correctly on 100m speed.
1109633	The FGT prompts the user to choose a certificate during login, even no PKI admin is set.
1110527	FortiGate did not update password-expire time on the start or end of daylight savings time.
1112376	Unexpected behavior observed in the newcli daemon due to inconsistencies in node registration between cmdbsvr and other daemons.
1115486	Virtual switch interface drops LLDP packets.
1116922	FortiGate encounters a memory usage issue if too many ports have LLDP reception enabled.
1117435	Add SNMP new OIDs `fgAdminLoggedInTable` for `get sys admin list`.
1117527	VXLAN interface should be brought down when underlay interface is down.
1120467	No SNMP trap at power failure for DC PSU.
1120907	High traffic load on a particular interface causes packet loss on other interfaces of the FortiGate.
1122306	Typo in log-controller-update request.
1123727	Offload failed when egress shaping applied on VLAN interface on SOC5 platform.
1124024	When `set append-index disable` in system.snmp.sysinfo, querying per-VDOM BGPPeerTable might get incorrect results because of no updates.
1125301	FortiGate stuck after reloading configuration that contains expired user passwords.

Bug ID	Description
1126100	Expired user passwords are stored as plaintext in configuration files when password history is enabled.
1126327	The SNMP query for `fgSwPortSwitchSerialNum` gives switch name as the output instead of SN.
1128087	In new version of RDP client, FortiGate drops some RDP sessions due to IPv6 extended headers.
1133159	Inbandwidth setting not respected with large number of class IDs in shaping profile.
1133842	Packet dropped with 'DCE_IVS_IGR_DIR_DROP' over hardware switch.
1142013	Policing improvement for QTM by limiting buffer size or switching to TPE (`shaping-profile mode of config`).

Upgrade

Bug ID	Description
1043815	Upgrading the firmware for a large number (100+) of FortiSwitch or FortiAP devices at the same time may cause performance issues with the GUI and some devices may not upgrade.
1102990	SLBC FortiGate 5001E primary blade failed to install image, even though graceful-upgrade was disabled.
1104649	In 7.6.1 and 7.6.2, if a local-in policy, local-in-policy6, DoS policy, interface policy, multicast policy, TTL policy, or central SNAT map is used in an interface in version 7.4.5, 7.6.0, or any previous GA version that was part of the SD-WAN zone, these policies will be deleted or show empty values after upgrading to version 7.6.1 or 7.6.2.
1105771	Upgrade from 7.4.6 GA to 7.6.1 GA results in an incomplete WAD device memory list table and triggers WAD error.
1106072	The image file transfer between FortiManager and FortiGate may not work as expected when transferred by the FGFM tunnel.
1110809	Egress-shaping-profile setting lost on interface after upgrade.
1114232	When upgrading FortiGate from earlier than 7.4.1 to 7.4.1 or later, system.replacemsg.webproxy configuration is lost.
1123954	Upgrading FortiOS from 7.2.10 to 7.4.5 will automatically enable FortiGuard updates without a warning.
1130861	FG-4401F enters a reboot loop after upgrading from 7.2.9 GA to 7.4.6 GA with a large config file (more than 10K policies).

User & Authentication

Bug ID	Description
1017348	Memory usage by fsso_ldap daemon increases continuously when the LDAP server responds with "LDAP_UNWILLING_TO_PERFORM" due to an unhandled memory allocation issue.
1020808	Use new keys for certificate renewal through EST server.
1025260	Wildcard admin remote authorization password change in system GUI does not work.
1043189	Low-end FortiGate models with 2GB memory can enter conserve mode when processing large amounts (over 5000 user records) of stored user store data, when each record has a large amount of IoT vulnerability data. For example, the Users and Devices page or FortiNAC request can trigger the following API call that causes httpsd process to spike in CPU and memory: `GET request /api/v2/monitor/user/device/query`
1054818	Password encryption changed for `config vpn certificate local` without actual certificate changes.
1075207	Errors may occur in the FNBAMD due to the presence of two wildcard-enabled remote administrators in separate VDOMs.
1077636	No SNMP trap available to detect FSSO external connected status change.
1091483	When importing local certificate, GUI displays an error, even when certificate is correctly imported.
1093538	In SAML config, after enabling "AD FS claim" (Active Directory Federated Services and rebooting, the "Attribute used to identify users" and "Attribute used to identify groups" fields are blank.
1093542	FortiGate admin user authentication with token+RADIUS fails when wildcard user is configured.
1093654	FGT uses global DNS when attempting to provision a certificate through SCEP or EST.
1105305	Guest user not removed past expiry time.
1119143	Unable to view local certificate in GUI or CLI after certificate import.
1121987	Overlapping text when viewing FSSO user login groups membership.
1136244	RSSO not working on 7.6.x with Cisco Meraki MX.

VM

Bug ID	Description
999842	Azure fails to honor seamless live migration. In most cases, the public IP to private IP NAT fails to forward traffic from/to SD-WAN.
1012000	When unicast HA setup has a large number of interfaces, FGT Hyper-V takes a long time to boot up.
1094600	The system.virtual-wire-pair and system.vxlan do not work on cloud images (Azure, AWS, GCP).

Bug ID	Description
1101264	On Azure-FGT A-P HA cluster with SDN connector v7.4.5, the failover time increased from 2-4 request timed out to 10-12.
1102434	Configuring VRF on hbdev causes FGT VM HA not to sync.
1107007	samld stops working when certificate set to Fortinet_Factory in user SAML.
1107962	Dynamic addresses are removed/added every few seconds when the OCI SDN connector fetches only the first page of API results.
1109724	Azd daemon on Azure NVA keeps consuming memory until FortiGate enters conserve mode.
1113362	FGT-VM64-AZURE cannot establish connection with other FGTs in the Security Fabric tree.
1121521	Azure SDN connector does not properly catch AKS cluster state.
1121974	Due to continuous disk logging, slab memory for dentry continuously increases in FortiGate VM.
1128351	Configuration fails to fully apply during bootstrap when the reboot function does not trigger an immediate reboot, causing cloudinit to re-run with insufficient tablespace.

Web Filter

Bug ID	Description
874516, 1100819	SMB traffic fails when the file server uses AES-256-GCM/CCM encryption with FortiOS.
906603	For newly created webfilter profile, GUI commits local and remote categories' *Allow* action to *Monitor*.
1099818	Output of `diagnose webfilter fortiguard cache dump` command shows the message "Cache is not enabled".
1107456	FG-120G webfilter.profile tablesize is incorrect.
1110668	Add an option to control webfilter.urlfilter simple-type entries match subdomains.
1110850	The value for x-forwarded-for is not properly displayed in the log on AWS environment.
1118132, 1122036, 1127984	Webfilter local category override does not working after rebooting in flow mode.

WiFi Controller

Bug ID	Description
823387	Email addresses collected from the captive portal do not show up under the user column under WiFi clients.
921080	The Fortigate Hostapd does not support IPv6 address of RADIUS server.
987030	Unexpected behavior observed in the CAPWAP daemon when managing multiple APs and clients through dynamic VAP changes.
1013892	On FortiGate's in an HA pair, the npd process do not work as expected when trying to manually update the threat feed.
1030197	For an SSID with radius-mac-auth and radius-mac-auth-usergroups in HA environment, the secondary unit is missing some information, and traffic is blocked after failover.
1039985	Erroneous memory allocation observed in the CAPWAP function on NP6 and NP6XLite platforms due to a rare error case.
1080094	Offline station data consumes excessive memory when the sta-offline-cleanup or max-sta-offline settings are not configured.
1083395	In an HA environment with FortiAPs managed by primary FortiGate, the secondary FortiGate GUI *Managed FortiAP* page may show the FortiAP status as offline if the FortiAP traffic is not routed through the secondary FortiGate. This is only a GUI issue and does not impact FortiAP operation.
1086128	An error condition in CAPWAP occurred due to a rare case.
1089999	FAPs remain offline post-upgrade when using image stored on FortiGate.
1094415	VLAN pooling does not work as expected on the SSID after FGT upgrades from 7.4.1 to 7.4.5.
1096961	When using FMG to upgrade FAP, FGT did not generate `AP image receive success` log (ID 43618).
1098727	Enable 5GHz channels 52-64, 108, 116-128 for FAP-231G-P, 431G-P Uzbekistan. (Uzbekistan has no DFS certification process.)
1100220	External/FortiGuest MPSK COA disconnect is not functional.
1101583	Intermittent traffic disruption observed in cw_acd caused by a rare error condition.
1102808	APs disconnect from the firewall when new configurations are applied.
1108726	FortiAPs periodically lose connectivity with FortiGate (acting as WLC) due to an error case.
1114144	WSSO firewall authorization session cannot be created when FGT receives multiple group attributes, and the first group does not exist.
1114311	Packets are incorrectly routed when FAP management interface uses clear-text dtls-policy in a software switch with explicit intra-switch-policy.

Bug ID	Description
1123829	Support legal firewall policy when SD-WAN/zone member interface manages FAP with `dtls-policy` set to `ipsec-vpn`.
1128272	FGT-120G PPPoE interface cannot manage teleworker FAP-231F.
1130750	Managed AP 5Ghz radio channel override value missing after changes on AP-profile.
1133829	FAP stays offline after the FGT is rebooted.
1139749	FortiGate does not honor source IP for MPSK RADIUS requests.

ZTNA

Bug ID	Description
1101022	FortiClient gets blank page when doing SAML authentication.
1107986	Should be unable to select geography object in ZTNA proxy-policy.
1111112	Unable to configure more than eight mapped ports for access proxy realservers when the limit is 16.
1114976	ZTNA policy matching failed due to an accidental deletion of firewall.policy with ZTNA tags when the firewall.policy is updated.

Known issues

Known issues are organized into the following categories:

- New known issues on page 55
- Existing known issues on page 56

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

New known issues

The following issues have been identified in version 7.6.3.

FortiGate 6000 and 7000 platforms

Bug ID	Description
1117663	Unexpected behavior in the bcm.user process after a factory reset can sometimes prevent the FPMs from booting up.
1131541	The `sslvpn-load-balance` setting under `load-balance` setting needs to be removed.
1140005	Policy statistics not aggregated.
1142465	ARP entries age out quickly after a system reboot, despite a long reachable-time setting.

Hyperscale

Bug ID	Description
1030907	With a FGSP and FGCP setup, sessions do not show on the HA secondary when the FGSP peer is in HA.

Log & Report

Bug ID	Description
1124896	FAZ and FGT-cloud *Logs Sent Daily* chart looses data after upgrade.

Existing known issues

The following issues have been identified in a previous version of FortiOS and remain in FortiOS 7.6.3.

Endpoint Control

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

Firewall

Bug ID	Description
959065	On the *Policy & Objects > Traffic Shaping* page, when deleting or creating a shaper, the counters for the other shapers are cleared.
990528	When searching for an IP address on the *Firewall Policy* page, the search/filter functionality does not return the expected results.

FortiGate 6000 and 7000 platforms

Bug ID	Description
653335	SSL VPN user status does not display on the FortiManager GUI.
936320	When there is a heavy traffic load, there are no results displayed on any *FortiView* pages in the GUI.
950983	*Feature Visibility* options are visible in the GUI on a `mgmt-vdom`.
994241	On FortiGate 7000F using FGSP and FGCP, when TCP traffic takes an asymmetric path, the TCP ACK and data packets might be dropped in NP7.
1006759	After an HA failover, there is no IPsec route in the kernel. **Workaround**: Bring down and bring up the tunnel.
1014826	SLBC does not function as expected with IPsec over TCP enabled.
1102072	On the FortiGate 7000 platform, cmdbsvr CPU usage can be higher than normal for extended periods on one or more FPM.
1112582	Under some conditions, such as during conserve mode, you may be unable to log in to the FortiGate 6000 management board GUI or CLI, or when you log in to the management board console, a message similar to fork failed() continuously repeats.

FortiView

Bug ID	Description
1034148	The *Application Bandwidth* widget on the *Dashboard* > *Status* page does not display some external applications bandwidth data.

GUI

Bug ID	Description
853352	When viewing entries in slide-out window of the *Policy & Objects* > *Internet Service Database* page, users cannot scroll down to the end if there are over 100000 entries.
1047146	After a firmware upgrade, a VLAN interface used in IPsec, SSL VPN, or SD-WAN is not displayed on the interface list or the SD-WAN page and cannot be configured in the GUI.

HA

Bug ID	Description
851743	When running the `diag sys ha checksum cluster` command, a previous line result is added further down in the output instead of new line result when a FortiGate is configured with several VDOMs .

Hyperscale

Bug ID	Description
1042011	On FortiGate, an login error message displays in the event log after completing an automation.
1089281	For FG-480xF/FFW-480xF, using `npu-group` other than `0` with log2host around ~1M CPS could result in NP chip getting stuck.

Intrusion Prevention

Bug ID	Description
1076213	FortiGate's with 4GB memory might enter conserve mode during the FortiGuard update when IPS or APP control is enabled. **Workaround**: Disable the `proxy-inline-ips` option under `config ips settings`.

IPsec VPN

Bug ID	Description
735398	On FortiGate, the IKE anti-replay does not log duplicate ESP packets when SA is offloaded in the event log.
944600	CPU usage issues occurred when IPsec VPN traffic was received on the VLAN interface of an NP7 vlink.
995912	After a firmware upgrade, some VPN tunnels experience intermittent signal disruptions causing traffic to be re-routed.
1042371	RADIUS authentication with EAP-TLS does not work as expected through IPsec tunnels.

Log & Report

Bug ID	Description
611460	On FortiOS, the *Log & Report > Forward Traffic* page does not completely load the entire log when the log exceeds 200MB.

Proxy

Bug ID	Description
1035490	The firewall policy works with proxy-based inspection mode on FortiGate models with 2GB RAM after an upgrade. **Workaround**: After an upgrade, reboot the FortiGate.

REST API

Bug ID	Description
938349	Unsuccessful API user login attempts do not get reset within the time specified in `admin-lockout-threshold`.
993345	The router API does not include all ECMP routes for SD-WAN included in the `get router info routing-table` command.
1051870	After a firmware upgrade, some vlan interfaces attached to LAG interface are not displayed in the GUI.

Security Fabric

Bug ID	Description
1019844	In an HA configuration, when the primary FortiGate unit fails over to a downstream unit, the previous primary unit displays as being permanently disconnected.
1040058	The Security Rating topology and results does not display non-FortiGate devices.

Switch Controller

Bug ID	Description
961142	An interface in FortiLink is flapping with an MCLAG FortiSwitch using DAC on an OPSFPP-T-05-PAB transceiver.
1113304	FortiSwitch units are offline after FortiGate is upgraded from 7.4.6 or 7.6.0 to 7.6.1 or later when LLDP configuration is set to vdom/disable under the FortiLink interface. **Workaround**: In LLDP configuration, enable `lldp-reception` and `lldp-transmission` under the FortiLink interface, or rebuild the FortiLink interface.

System

Bug ID	Description
947982	On NP7 platforms, DSW packets are missing resulting in VOIP experiencing performance issues during peak times.
971466	FortiGateRugged 60 models may experience packet loss when directly connected to Cisco switch.
1041726	Traffic flow speed is reduced or interrupted when the traffic shaper is enabled.
1047085	The FortiOS GUI is unresponsive due to a CPU usage issue with the `csfd` and `node` processes.
1058256	On FortiGate, interfaces with DAC cables remain down after upgrading to version 7.4.4.
1103617	Integrating an interface does not work when adding a new member into an existing interface or creating a new interface.

User & Authentication

Bug ID	Description
1021719	On the *System* > *Certificates* page, the *Create Certificate* pane does not function as expected after creating a new certificate.

Bug ID	Description
1082800	When performing LDAP user searches from the GUI against LDAP servers with a large number of users (more than 100000), FortiGate may experience a performance issue and not operate as expected due to the HTTPSD process consuming too much memory. User may need to stop the HTTPSD process or perform a reboot to recover. **Workaround**: Perform an LDAP user search using the CLI.

VM

Bug ID	Description
1146370	AWS bootstrap is unable to properly parse IAM role profile due to the length.

Web Filter

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

Built-in AV Engine

AV Engine 7.00040 is released as the built-in AV Engine.

Built-in IPS Engine

IPS Engine 7.01040 is released as the built-in IPS Engine.

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.

FORTINET®

www.fortinet.com

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.