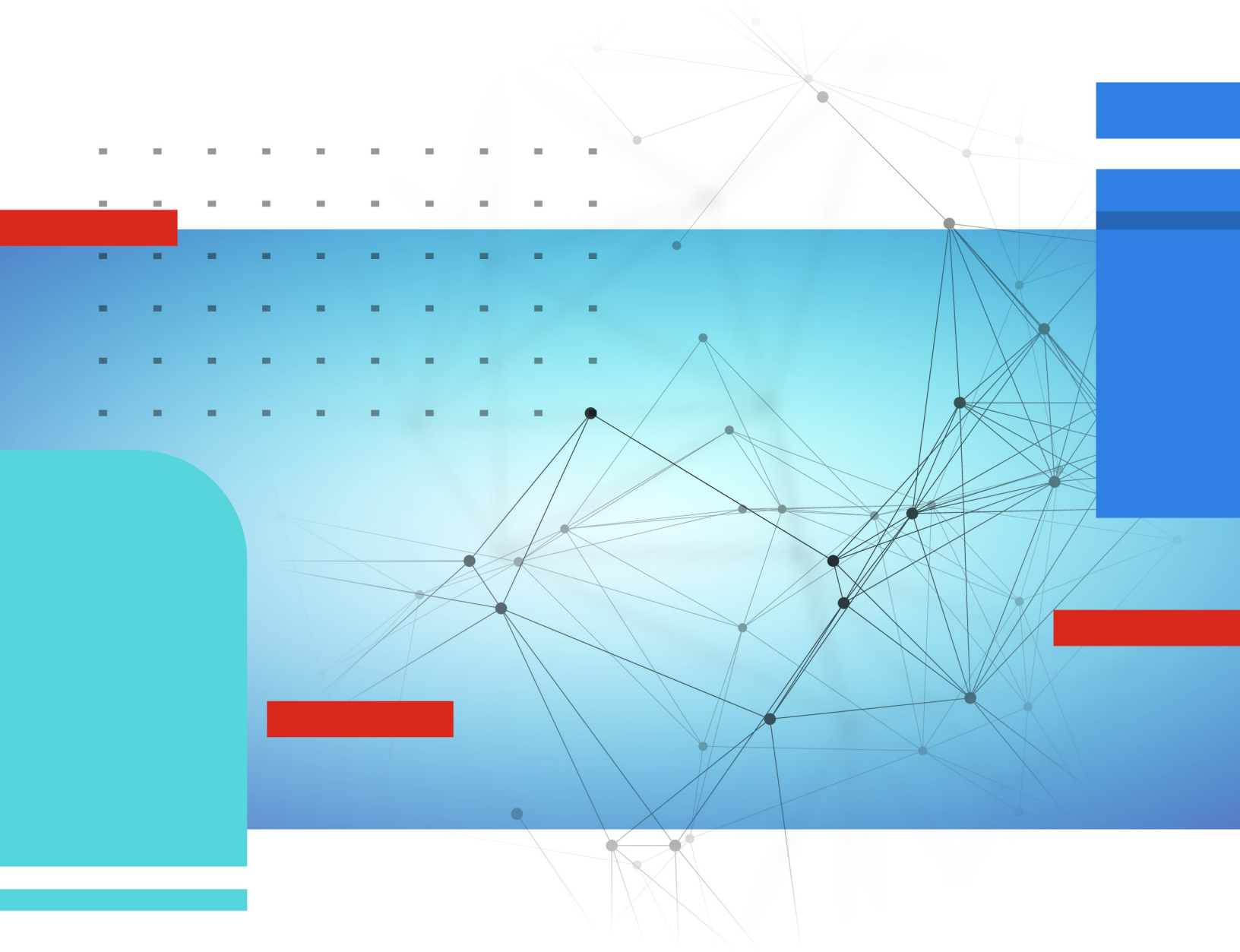
Release Notes

FortiOS 7.6.5



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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

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

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

December 29, 2025
FortiOS 7.6.5 Release Notes
01-765-1205860-20251229

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-12-11	Initial release.
2025-12-16	Updated Changes in default behavior on page 19, Changes in default values on page 20, New features or enhancements on page 22, Resolved issues on page 42, and Known issues on page 63.
2025-12-22	Updated Changes in CLI on page 17, New features or enhancements on page 22, Resolved issues on page 42 and Built-in IPS Engine on page 71.
2025-12-29	Updated Changes in default behavior on page 19, Resolved issues on page 42, and Built-in IPS Engine on page 71.

Introduction and supported models

This guide provides release information for FortiOS 7.6.5 build 3651.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.6.5 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-50G, FG-50G-5G, FG-50G-SFP, FG-50G-DSL, FG-50G-SFP-POE, FG-51G, FG-51G-5G, FG-51G-SFP-POE, FG-60F, FG-61F, FG-70F, FG-70G, FG-70G-POE, FG-71F, FG-71G, FG-71G-POE, 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-200G, FG-201E, FG-201F, FG-201G, 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-700G, FG-701G, 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-50G, FWF-50G-5G, FWF-50G-SFP, FWF-50G-DSL, FWF-51G, FWF-60F, FWF-61F, FWF-70G, FWF-70G-POE, FWF-71G, 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-50G-5G, FGR-60F, FGR-60F-3G4G, FGR-70F, FGR-70G, FGR-70G-5G-Dual, 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 7.6.5 supports the following FG-6000F, FG-7000E, and FG-7000F models:

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

Special notices

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.

How FortiManager 7.6.3 and later works with FortiOS private data encryption keys has changed. This topic covers the changes. See FortiManager behavior on page 10.

Previous FortiOS CLI behavior

```
config system global
    set private-data-encryption enable
end
Please type your private data encryption key (32 hexadecimal numbers):
1234567890123456789012345678 9abc
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
1234567890123456789012345678 9abc
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

FortiManager 7.6.3 can centrally manage FortiGates with the private-data-encryption setting enabled, with the following limitations:

- FortiManager cannot import objects that include the password type attribute.
- FortiManager cannot be used to create NAT and transparent VDOMs.

This applies to FortiGates with private keys that are manually configured in FortiOS 7.6.0 and earlier and private keys that are randomly generated in FortiOS 7.6.1 and later.

FortiManager does not require you to verify the private key of the FortiGate when adding it to FortiManager.

FortiGates that require the protection of private data encryption and need to be managed by FortiManager should follow these procedures on a fresh install.

1. On the FortiGate, enable private-data-encryption.
2. On the FortiManager, add the FortiGate to the Device Manager. FortiManager will not be required to provide the key for PDE, as it will not be importing any password-related settings.
3. Make all configuration changes directly on the FortiManager.
4. Push and install the changes to the FortiGate.

If you require the use of NAT or Transparent VDOMs, you should perform this additional step before the steps above.

1. Enable multi-vdom mode on the FortiGate.
2. Add the VDOMs that you will use on the FortiGate.
3. Follow the above steps to enable private-data-encryption and manage the FortiGate from the FortiManager.

For more information, see the FortiManager Administration Guide.

FortiOS upgrade behavior with FortiManager 7.6.2 and earlier

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 7.6.5 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 7.6.5 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 set up 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.

SSL VPN tunnel mode replaced with IPsec VPN

Starting in FortiOS 7.6.3, the SSL VPN tunnel mode feature is replaced with IPsec VPN, which can be configured to use TCP port 443. SSL VPN tunnel mode 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 and later.

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 some FortiGate 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-50G/FWF-50G and variants
- FGT-60F/FWF-60F
- FGT-61F/FWF-61F
- FGR-60F and variants (2GB versions only)
- FGT-70G/FWF-70G and variants
- 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 most 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 most proxy-related features.

However FortiOS 7.6.5 brings back proxy-based inspection for email protocols on FortiGate models with 2 GB RAM. This covers the following services:

- SMTP(s)
- POP3(s)
- IMAP(s)

- NNTP

Firewall policies can once again support proxy-based inspection mode when users select one or more of the above services in the firewall policy.

This change impacts the FortiGate 40F, 60F, and 50G 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.

GUI access conflict with IPSec TCP tunnel on the same interface

In FortiOS version 7.6.1, the default IKE TCP port has been changed to port 443 on new deployments. In the FortiOS 7.6.1 Release Notes, see Bug ID 1051144 in Changes in default values.

This may affect GUI access for interfaces bound to an IPsec tunnel in the scenario that the GUI admin port is also using port 443.

In case GUI connectivity is lost, connect to the FortiGate by:

1. Connecting from an interface that is not bound to an IPsec tunnel.
2. Connecting to the interface using SSH, if SSH is enabled.
3. Connecting to the FortiGate from console.

To ensure continued functionality, users are recommended to either:

- Choose an alternative interface for GUI access by configuring:

```
config system global
    set admin-sport <port>
end
```

- Customize the `ike-tcp-port` to a value other than 443:

```
config system settings
    set ike-tcp-port <port>
end
```

SAML certificate verification

SAML certification verification has added a new setting in FortiOS 7.6.5. For security purposes, FortiGate by default requires a signature verification for both the SAML response message and the SAML assertion carried inside the SAML response. This means that the SAML response must have a valid signature, and the SAML assertion must also have a valid signature. If the Identity Provider (IdP) provides an invalid signature, or fails to sign one of these, the FortiGate will reject the SAML response.

This check can be loosened up with the following configuration:

```
config user saml
    edit <name>
        set require-signed-resp-and-asrt <enable | disable>
    next
end
```

- `enable`: Both response and assertion must be signed and valid. (Default)
- `disable`: At least one of response or assertion must be signed and valid.

For more information, see Identify Providers.

Policy check required for hairpin traffic

The default setting for `allow-traffic-redirect` and `ipv6-allow-traffic-redirect` has been changed from `enable` to `disable`:

```
config system global
  set allow-traffic-redirect disable
  set ipv6-allow-traffic-redirect disable
end
```

Upon upgrade, both of these settings will be changed to `disable`, even if they were enabled before.

Disabling this setting ensures that hairpin traffic arriving at an interface and redirected out on the same interface requires a firewall policy to explicitly allow the traffic. If you want to redirect traffic without the need for a policy based only on routing decision, then manually enable these settings.

Changes in CLI

Bug ID	Description

1083204	You can enable the following option to add all multicast traffic denied by a firewall policy to the session table:
	
	`config system settings`
	`  set ses-denied-multicast-traffic enable`
	`end`
	
	Enabling this option can affect CPU usage since the software needs to maintain more sessions in the session table. However, on FortiGates with NP6 or NP7 processors, you can use the following command to offload denied multicast sessions to NP processors and reduce CPU usage:
	
	`config system npu`
	`  set mcast-denied-ses-offload enable`
	`end`

1153276	If your FortiGate with NP7 processors is terminating VXLAN-over-IPsec connections, you may notice traffic drops during broadcast storms. One cause of the traffic drops could be VXLAN MAC flapping. VXLAN MAC flapping can occur when the FortiGate receives large numbers of packets that flip MAC addresses in the forwarding database (FDB) between local and remote paths. This activity can use excessive CPU resources and can lead to FDB instability.
	You can use the following command to stop VXLAN MAC flapping:
	
	`config system npu`
	`  set vxlan-mac-flapping-guard enable`
	`end`
	
	When `vxlan-mac-flapping-guard` is enabled, each VXLAN FDB entry records the encapsulation direction when it is first learned, and if a later packet tries to flip the same MAC to the opposite direction, the update is rejected. This behavior prevents VXLAN MAC flapping during loops or broadcast storms.
	You can restore normal VXLAN FDB behavior by disabling this option.

Changes in GUI behavior

Bug ID	Description
1112727	On a new installation, users logging into the GUI are directed to the FortiCare registration dialog. This dialog ensures users remember to register their device with FortiCare. This feature is supported on the FortiGate 50G, 70G, 90G, 120G, 200G, 700G, 900G, and variants. See also Enforce FortiCare registration after new GUI login.
1124242	Devices must be registered with FortiCare to access the GUI and full CLI. Until a device is registered with FortiCare, the FortiOS CLI is read-only, except for the following commands, which can be edited: • config firewall • config ftp-proxy • config router • config system • config web-proxy Note that only a subset of settings related to network configurations are supported. See also Enforce FortiCare registration with read-only CLI.
1190308	On IPsec VPN configurations, the GUI will only provide options to set *Auto* or *UDP* for *Transport mode*. UDP is the default setting for static and dialup tunnels, except when the FortiClient is selected. To configure TCP transport, use the CLI.

Changes in default behavior

Bug ID	Description
1107163	The default DH groups for Phase1 and Phase2 IPsec VPN tunnels will be updated from 14 and 5 to 20 and 21 when configured from the CLI. VPNs that had the default DH group 14 and 5 before upgrade will be updated to DH groups 14, 20, and 21 after upgrade.

1138921	On FortiGates with NP7 processors, the default setting for vlan-lookup-cache has been changed to disable, and the htab-msg-queue mode is now set to dedicated.
	`config system npu`
	`  set vlan-lookup-cache disable`
	`  set htab-msg-queue dedicated`
	`end`

1166396	With `asymroute-icmp` and `asymroute6-icmp` enabled, ICMP replies are no longer strictly routed back through the same interface they arrived on. If a return route via the incoming interface is unavailable, the system will now choose the best available route instead. This behavior improves reliability and reduces packet drops in asymmetric routing scenarios.
	`config system settings`
	`  set asymroute-icmp {enable | disable}`
	`  set asymroute6-icmp {enable | disable}`
	`end`

1176942	When `auth-ike-saml-port` is used, iprope will match the local-in traffic only when the destination port is `auth-ike-saml-port`, and the destination interface has `ike-saml-server` enabled.
1189391	FortiGate models with two (2) WAN ports will have the following added to their default configuration: • Both WAN ports are set to DHCP mode. • An SD-WAN zone is created, and both WAN ports are added as members. • Default firewall policy utilizes the SD-WAN zone. • An SLA is created, utilizing IP addresses 1.1.1.1 and 9.9.9.9 for internet connectivity evaluation. Affected models (where x can be 0 or 1): 6xE, 6xF, 7xF, 7xG, 8xE, 8xF, 9xE, 9xG, 10xE, 100EF, 10xF, 12xG, 140E, 20xE, 20xF. See also Create default configuration of SD-WAN on FortiGate models with two WAN ports.
1204277	The default auto-update schedule for FortiGuard packages has been changed from automatic to daily.

Changes in default values

Bug ID	Description

1118690	On a hyperscale FortiGate, the default values for IPv4 and IPv6 high and low session quotas have been updated. For both session types the high threshold is now 64000, and the low threshold is now 51200.
	These session quotas are set using the following options:
	`config system npu`
	`set ipv6-prefix-session-quota {disable | enable}`
	`set ipv6-prefix-session-quota-high <high-threshold>`
	`set ipv6-prefix-session-quota-low <low-threshold>`
	`set ipv4-session-quota {disable | enable}`
	`set ipv4-session-quota-high <high-threshold>`
	`set ipv4-session-quota-low <low-threshold>`
	`end`

1200360	The quarantine option is now disabled by default when creating tunnel-mode SSIDs, preventing automatic creation of unused quarantine VLANs and simplifying configuration and management.

Changes in table size

Bug ID	Description
1204202	Increase per-vdom limit for router.route-map from 256 to 512.

New features or enhancements

More detailed information is available in the New Features Guide.

GUI

See GUI in the New Features Guide for more information.

Feature ID	Description
1183975	The FortiGate setup wizard includes options to configure a gateway to establish internet connectivity, which is required for successful registration with FortiCare. Additionally, for air-gapped environments, the wizard allows users to upload an offline license file directly, enabling successful registration even when the device cannot reach FortiCare. This enhancement resolves setup-blocking issues and improves deployment flexibility.
1186780	Security Rating tooltips now include a footer button to view all insights for a configuration object, plus individual controls to hide specific insights directly from the tooltip. Hidden insights are still indicated, improving visibility and user control.

LAN Edge

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

Feature ID	Description
1078408	FortiAP now supports management over IPv6. This enhancement enables seamless integration into modern, IPv6-based network environments. It improves scalability, simplifies configuration in large deployments, and ensures compliance with evolving regulatory and infrastructure standards
1095618	DARRP channel selection can be handled by FortiAIOps when available, which collects radio data from FortiGate via REST APIs and recommends optimal channels to reduce interference. This shift enables smarter, centralized Wi-Fi tuning in high-density environments like campuses.
1139482	Added support for WPA2/WPA3-Enterprise and WPA3-SAE authentication in client mode on FWF G-series models, enabling secure and flexible network authentication.

Feature ID	Description
1150610	FortiAPs can now automatically request certificates from EST or SCEP servers configured in the wtp-profile, eliminating the need for manual CA uploads via TFTP. This streamlines 802.1X WAN deployments and simplifies certificate renewal.
1185065	FortiAP-K models now support Multi-Link Operation (MLO) as part of Wi-Fi 7, enabling simultaneous data transmission across multiple bands (2.4, 5, and 6 GHz) for improved performance and efficiency.
1185772	Default soft-switch interfaces and open SSIDs have been removed across FortiWiFi platforms to enhance security and simplify network design. For 4xF/6xF/G-series models, the default WiFi VAP remains in tunnel mode with preconfigured IP, DHCP, and firewall policies for easy setup. On 8xF-2R models, WiFi VAPs now operate in bridge mode, integrating with the hardware switch so clients receive DHCP from the internal interface and benefit from firewall policy control.
1187026	Mesh leaf FAP settings can now be configured directly through the GUI, enabling faster, more intuitive setup of mesh connections.
1187056	When customers run an older FortiOS version that does not support a newly released FortiAP model, the AP will now be classified as FAP MVP, a generic Wi-Fi 7 2x2 dual-band profile. This provides limited management and visibility until the user upgrades to a FortiOS release that fully supports the AP mode.
1217645	Previously, virtual switches in a software switch could not enable 802.1X authentication. Now, this restriction is removed802.1X can be enabled when the software switchs intra-switch-policy is set to explicit, allowing secure dynamic VLAN control and traffic regulation.

Log & Report

See Logging in the New Features Guide for more information.

Feature ID	Description
1170883	In *Log Settings > Global settings* under *Preferences*, when *Resolved hostnames* is enabled, provide the following options: • *On log creation* (resolve-ip enabled) will add the resolved hostname when the logs are generated and add it as dstname. In the GUI, display the dstname field. • *When viewed* (resolve-hosts enabled) will resolve the destination IP addresses during fetching of logs. If both are enabled from CLI, then On log creation takes precedence.

Network

See Network in the New Features Guide for more information.

Feature ID	Description

1124535	FortiGate now provides control over whether domains from delegated IPv6 prefixes are included in DNS Search List (DNSSL) options sent via Router Advertisements. This feature improves flexibility in managing domain propagation for downstream clients.
	
	`config ip6-delegated-prefix-list`
	`  edit <id>`
	`  set dnssl-service {enable | disable}`
	`  next`
	`end`

Policy & Objects

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

Feature ID	Description
1078303	FQDN address groups within the ISDB, previously supported in firewall policies, can now also be applied to NGFW policies.

1169071	Manually override and disable passive learning of FQDN addresses by disabling the following command on the firewall address object:
	
	`config firewall address`
	`  edit <address>`
	`  set passive-fqdn-learning {disable | enable}`
	`  next`
	`end`
	
	By default, the setting is enabled.

SD-WAN

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

Feature ID	Description

1135850	Added IPv6 support for HTTP and TWAMP protocols in SD-WAN health-checks. Added `probe-response` in ipv6-allowaccess of interface settings.
	FGT_A:
	`config system sdwan`
	`config health-check`
	`edit "ipv6_test"`
	`set addr-mode ipv6`
	`set server 2000:172:16:200::1`
	`set protocol twamp`
	`next`
	`end`
	`end`
	FGT_B:
	`config system interface`
	`edit "port3"`
	`...`
	`config ipv6`
	`set ip6-address 2000:172:16:200::1/64`
	`set ip6-allowaccess ping https ssh probe-response`
	`end`
	`next`
	`end`
	`config system probe-response`
	`set mode twamp`
	`end`

1156116	Enhancements to SD-WAN interface speed test to allow for dynamic QoS application and more resiliency for cloud speed test connections. • Automatically apply scheduled speed-test results (Out/In Bandwidth) to interface for QoS purpose. Respect any configured min+max in/out bandwidth values. • Select FTNT_Auto as default cloud server group to perform speed-test if a specific server group isn't specified. • Initiate retry mechanism once speed-test against cloud server fails.

1187047	• Allow to choose three-hour window in firewall schedule setting. If the time-based firewall schedule is applied to speed-test, it will randomize the start of the speed test during the three-hour window.
	`config firewall schedule recurring`
	`edit <name>`
	`set label-day <none | over-night | early-morning | morning | midday | afternoon | evening | night | late-night>`
	`next`
	`end`

Feature ID	Description

	• Two new attributes `retries` and `retry-pause` are added into speed-test-schedule to improve retry mechanism. When `retries X` and `retry-pause Y` are set, FortiGate attempts test X times then pauses Y seconds. Three attempts total are made in the same pattern. If all attempts fail, the next server is selected, and the pattern is repeated.
	
	`config system speed-test-schedule`
	`edit "port1"`
	`set retries <value>`
	`set retry-pause <value>`
	`next`
	`end`
	
	• The `server-name` attribute is allowed in speed-test-schedule to define what cloud server-group will do the speed-test first.
	
	`config system speed-test-schedule`
	`edit "port1"`
	`set server-name <server group name>`
	`next`
	`end`

1187158	This feature enables hubs to detect when a spoke is dead (no SLA probes over a configurable duration) and suppress routes to that spoke. A BGP route-map-out is used to match this suppression status, and adjusts the MED to inform BGP peers of the hub to direct traffic to the spoke through another hub.
	
	`config system sdwan`
	`config health-check`
	`edit`
	`set update-bgp-route [enable/disable]`
	`next`
	`end`
	`end`
	
	`config router route-map`
	`edit "suppress_dead_spoke"`
	`config rule`
	`edit 1`
	`set match-suppress enable`
	`set set-metric 999`
	`next`
	`edit 2`
	`set set-metric 10`
	`next`
	`end`
	`next`

Feature ID	Description

	end
	
	config router bgp
	  config neighbor
	  edit "172.31.0.129"
	  set attribute-unchanged med
	  set route-map-out "suppress_dead_spoke"
	  next
	  end
	end

Security Profiles

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

Feature ID	Description
1166828	In this enhancement, proxy-based inspection is brought back for email protocols on FortiGate models with 2 GB RAM. This covers the following services: • SMTP(s) • POP3(s) • IMAP(s) • NNTP Firewall policies can once again support proxy-based inspection mode when users select one or more of the above services in the firewall policy.

1178045	Add CLI setting to configure the FortiSandbox inline mode block (ILB) timeout:
	
	config antivirus profile
	  edit <name>
	  set fortisandbox-scan-timeout <30-180>
	  next
	end

System

See System in the New Features Guide for more information.

Feature ID	Description
1000357	Improved Hyperscale FortiOS support for SNMP MIB OIDs to monitor IP and PBA usage in CGNAT IP pools. The newly supported fields include: • fgFwIppStatsFreePBAs, number of free PBAs in ippool list. • fgFwIppStatsInusePBAs, number of in-use PBAs in ippool list. • fgFwIppStatsTotalPBAs, number of PBAs in ippool list. • fgFwIppStatsInuseIPs, number of in-use IPs in ippool. • fgFwIppStatsFreeIPs number of free IPs in ippool. The fgFwIppStatsExpiringPBAs SNMP field is not supported by FortiOS 7.6.5.
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.

1123102	Added support for FortiSASE Sovereign licensing bundles for FortiGate 91G and 901G. With this licensing applied, the GUI and CLI is restricted to read-only after the following CLI settings are configured:
	`config system sov-sase`
	`  set status enable`
	`end`
	After the CLI settings above are configured, all FortiGate configuration changes are managed from FortiSASE-Sovereign Portal.

1133400	Optimize memory usage on FortiGate models with 2GB or 4GB of RAM by: • Starting the router daemon only when routing configurations are detected • Reducing the memory reserved for Network Processors (NPs) • Setting nTurbo max frame size to 1500. Interfaces with higher MTU will not offload to nTurbo Affected 2GB model families: 40F, 60F and 50G Affected 4GB model families: 70F, 80F and 70G
1202253	FortiGate expands HTTPS management interface capabilities by supporting quantum-resistant TLS algorithms, including hybrid key exchange and PQC certificates. This ensures secure administrative access while maintaining compatibility with non-PQC-capable clients.

User & Authentication

See Authentication in the New Features Guide for more information.

Feature ID	Description
1216102	When using SAML authentication in a web proxy, the timeout value of the sign-on URL in the auth query can be configured with the following setting:

Feature ID	Description
	config web-proxy global set auth-sign-timeout <30-3600> end This allows the client a longer time to access the sign-on URL to the IdP.

VPN

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

Feature ID	Description
1152420	FortiOS now supports Post-Quantum Cryptography (PQC) for Agentless VPN. This enhancement introduces new CLI options for Agentless VPN, allowing you to select pure and hybrid PQC algorithms to prepare for future quantum computing threats.
1195216	FortiGate now supports TLS 1.3 hybrid Post-Quantum Cryptography (PQC) key exchanges in SSL deep inspection (flow mode), enabling secure traffic inspection. This enhancement ensures compatibility with modern browsers and PQC-enabled servers that utilize algorithms such as X25519MLKEM768.
1205594	IPsec VPN over UDP may now use port 443 for the IKE negotiation port. config system settings set ike-port 443 end

WiFi Controller

See Wireless in the New Features Guide for more information.

Feature ID	Description
1211127	WiFi controllers now process the RADIUS Filter-ID attribute during 802.1X authentication to automatically map clients to existing user groups. This enhancement triggers the creation of WSSO firewall authentication entries, ensuring the correct firewall policies are applied immediately without requiring additional user login steps.
1189709	FWF models now secure the out-of-the-box experience by broadcasting a temporary, unique MAC-based SSID for only five minutes upon first power-up, replacing the static default. The initial login workflow now requires an admin password change and launches a WiFi Setup Wizard, which prompts administrators to either securely customize the WiFi Network or disable the WiFi Network entirely.

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 30 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 7.6.5 is verified to work with these Fortinet products. This includes:

FortiAnalyzer	• 7.6.5
FortiManager	• 7.6.5
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 7.6.5. When Security Fabric is enabled in FortiOS 7.6.5, all FortiGate devices must be running FortiOS 7.6.5.

Downgrading to previous firmware versions

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

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

Firmware image checksums

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

FortiGate 6000 and 7000 upgrade information

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

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

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

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

To perform a graceful upgrade of your FortiGate 6000 or 7000 to FortiOS 7.6.5:

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

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

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

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

2. Download the FortiOS 7.6.5 FG-6000F, FG-7000E, or FG-7000F firmware from https://support.fortinet.com.
3. Perform a normal upgrade of your HA cluster using the downloaded firmware image file.
4. When the upgrade is complete, verify that you have installed the correct firmware version.
   For example, check the FortiGate dashboard or use the `get system status` command.
5. 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.

This issue is resolved in FortiOS 7.6.3 with mantis 1104649.

After following the upgrade path to FortiOS 7.6.3, you must manually recreate these policies and assign them to the appropriate SD-WAN zone.

Although not recommended, you can skip the upgrade path and upgrade directly to FortiOS 7.6.3, and the policies remain untouched. Skipping upgrade steps might cause devices to miss other important FortiOS checks and changes and is not recommended.

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.

Removed speed setting affects SFP+ interfaces after upgrade

Starting in FortiOS 7.6.1, the `1000auto` speed setting is removed. If a FortiGate SFP+ port speed is set to `1000auto` before upgrade, the upgrade process automatically changes the setting to `10000full`. This change can cause the interface to go down when the connecting device has a different speed setting.

Workaround: After upgrade, align the port settings. Edit the port and set the speed to `1000full` to restore the connection.

```
config system interface
    edit <port>
        set speed 1000full
    next
end
```

Hyperscale with FGCP HA clusters and interface monitoring

For previous versions of hyperscale FortiOS, FGCP HA clustering with hardware session synchronization with `config vcluster-status disabled` allowed you to monitor `hw-session-sync-dev` interfaces. FortiOS 7.6.3 changed this behavior, and you can no longer monitor `hw-session-sync-dev` interfaces.

If your HA configuration includes monitoring `hw-session-sync-dev` interfaces, the upgrade to FortiOS 7.6.4 removes the monitor interface configuration.

You can work around this problem by removing monitoring from `hw-session-sync-dev` interfaces or by selecting different interfaces to be `hw-session-sync-dev` interfaces before performing the upgrade.

Password policy enforcement

After upgrade to FortiOS 7.6.5 or later, the password policy is enforced, and your password must meet the requirements before you can log in to FortiOS. Passwords must contain:

- 1 uppercase letter
- 1 lowercase letter
- 1 special character
- 1 number (0-9)
- A minimum length of 12 characters

If your password meets the requirements, you can log in to FortiOS after upgrade.

If your password does not meet the requirements, you must change your password before you can log in to the GUI or CLI.

Product integration and support

The following table lists FortiOS 7.6.5 product integration and support information:

FortiManager and FortiAnalyzer	See the FortiOS Compatibility Tool for information about FortiOS compatibility with FortiManager and FortiAnalyzer.
Web browsers	• Microsoft Edge 135 • Mozilla Firefox version 138 • Google Chrome version 136 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 135 • Mozilla Firefox version 138 • Google Chrome version 136 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 0328 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	• 7.00048
IPS Engine	• 7.01168

See also:

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	✓

Language	GUI
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 replaced with IPsec VPN on page 13.

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 138 Google Chrome version 136
Microsoft Windows 10 (64-bit)	Microsoft Edge 135 Mozilla Firefox version 138 Google Chrome version 136
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 138 Google Chrome version 136
macOS Ventura 13.1	Apple Safari version 18 Mozilla Firefox version 137 Google Chrome version 136
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
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

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

Agentless VPN (formerly SSL VPN web mode)

See also SSL VPN tunnel mode replaced with IPsec VPN on page 13.

Bug ID	Description
893190	When using two-factor authentication for SSL VPN users, the FortiGate does not respect the two-factor token timeout configured in config system global. This causes the token to expire prematurely for different two-factor authentication types including email, SMS, FortiToken.
983513	The two-factor-fac-expiry command is not working as expected for remote RADIUS users with a remote token set in FortiAuthenticator.
1164876	Abnormal SSL VPN web portal GUI is displayed when unsupported element is applied in template.
1180110	An error condition occurs during SSL VPN web mode password renewal.

Anti Virus

Bug ID	Description
1078174	An error condition in scanunit occurs during stress testing.
1153880	File upload disconnection occurs when FortiGate AntiVirus is enabled in proxy mode with deep inspection.
1181573	SSL inspection does not correctly add the Authority Key Identifier (AKID) when operating in Flow mode with DPI enabled.

DNS Filter

Bug ID	Description
1151824	DNS query failure occurs when using proxy-based inspection mode with DNS filter in firewall policy.
1179030	An error condition in dnsproxy occurs when handling DNS requests for TYPE65 records.

Explicit Proxy

Bug ID	Description
979401	IPv6 address pools cannot be set in explicit proxy policies.
1094870	FTPS data connections fail to establish when using flow-mode firewall policies configured for FTP service.
1116834	Authentication pop-up does not appear when accessing HTTPS websites via FortiGate with explicit proxy when authentication rules, webproxy-forward-server, and certificate-inspection are configured in proxy-policy.
1118847	Explicit proxy policies filtering by HTTP method incorrectly match all traffic, causing unintended deep inspection.
1157551	Memory usage issue caused by improper internal state handling when using WebProxy.
1202441	Captive portal is unavailable when accessing the Internet after firmware upgrade.
1203767	File upload issues occur when using FortiGate as a proxy with content-range header.
1209746	Intermittent connectivity issues occur when using FTP Proxy through NPU VDOM link.
1219524	HTTP requests are blocked when `request-obs-fold` is set to `keep` and `obs-fold` is present in Content-Type.

Firewall

Bug ID	Description
1084957	Offloading issues occur when session-denied-offload is enabled for denied multicast sessions.

Bug ID	Description
1086315, 1025078	Some customers observed memory usage increase and client session not disconnecting issues using virtual server.
1093616	Bytes counter issue occurs when existing sessions are re-validated on a new firewall policy.
1120499	Packet loss occurs when default-qos-type policing is configured on FortiGate-3700F.
1134809	Security policy hit counter resets when learning mode is enabled in NGFW policy mode.
1152839	Packet loss occurs when asymmetric routing is used with IPv6 traffic.
1154805	Firewall deny policy mismatch occurs when local user traffic is specified.
1157120	Traffic failure occurs when GRE pass-through has a tunnel key set to zero during offload.
1157283	High priority traffic drops when bursty traffic is present on low priority queues.
1160065	Configuration settings in firewall.service.custom altered after upgrading from 7.4.x to versions 7.6.0 through 7.6.4 on FortiGate models with 2 GB of RAM.
1164742	SNAT failure occurs when GRE traffic is offloaded on NP7
1169071	Incorrect FQDN translation occurs when passive learning of FQDNs is enabled.
1176942	Auth-ike-saml-port responds on VIP/IPpool IP address when configured on a FortiGate with mismatched interface IP addresses.
1178995	Slow upload speed when per-ip shaper is configured with auto-asic offload enabled.
1187335	Video playback issues occur when SNAT is applied and RTSP session helper does not rewrite the destination field.
1187861	The diagnose debug flow trace incorrectly displays the operation as DNAT instead of SNAT when a central SNAT policy is matched.
1188448	Traffic drop occurs when configuring virtual wire pair to inspect 802.1Q double tagged VLAN traffic.
1188867	An error condition occurs in firewall policies when referencing FSSO usernames with special characters in NGFW policy mode.
1189618	Packets are dropped when auto-asic-offload and IPS are enabled.
1191592	Traffic is mis-routed to the FortiGate login page when a VIP with an unresolved FQDN mapped address is configured.
1194430	WAD logs may display an incorrect destination interface and firewall policy, even though traffic is sent to the correct real server, when a Virtual Server uses multiple real servers in different subnets with separate firewall policies per interface.
1195869	QTM stats issue occurs when traffic is VLAN/IPsec through hardware switch.
1200717	Traffic is allowed by local-in policy 4294967295 when VIP is configured with port-forwarding.
1202418	Incorrect policy matching occurs when multiple DCE-RPC packets arrive simultaneously.

Bug ID	Description
1204648	Secondary SCTP session failure occurs when an existing SCTP session has a different source port number than the EXP session.
1211358	Service negate enable option is reset to default state when restoring a full-config backup with service-negate enabled in firewall policies.
1212720	Traffic from LAN to WWAN is blocked when dstintf is set to wan instead of wwan in firewall policy on FortiWiFi-40F-3G4G.

FortiGate 6000/7000 Platform

Bug ID	Description
1092619	Session synchronization fails when encryption is enabled on FortiGate models in some cluster setups.
1159322	GTP-C tunnel sync issue occurs when using FGSP with load balancing.
1166353	VXLAN traffic is removed when offloaded to NP7Lite with VLAN ID.
1173455	Cluster out-of-sync when adding or deleting VDOMs with long names in HA mode.
1178328	Unexpected behavior occurs in the system when IPv6 traffic goes through GRE TP VDOM on SOC5 platform.
1181032	On 6K/7K platforms, confsync out of sync occurs when configuring an ACME certificate.
1182822	FortiGate 320xF and 370xF models may experience traffic drops when NPU is enabled in a firewall policy due to a missing channel.
1183709	FortiGate models fail to install proto=18 routes during initial SD-WAN health check configuration, causing secondaries to miss updated routes unless manually triggered.
1185528	Subscription license on the secondary chassis is missing after the graceful upgrade from 7.2.10 to 7.2.12.
1185779	CPU usage issues observed during GTP session sync on FGSP nodes.
1188338	The MLD state transitions to "Stopped" on the primary FIM when FortiOS incorrectly uses the FPM as the primary instead of the FIM, disrupting multicast6 traffic.
1198697	Link/Activity LEDs remain on when executing shutdown on FortiGate 120G/121G.
1203314	FDB sync issue occurs when using NAT VDOM virtual-wire-pair.
1204630	Traffic disruption when VRF routes are not synchronized to secondary blades.
1211372	An error condition in confsyncd occurs when file sizes change between scans.
1214688	Fragmented UDP-ESP packets are not forwarded when received on FortiGate.

Bug ID	Description
1219115	In 6K/7K platforms, SSL VPN load balancing does not work correctly when split-port is set to 1-M1 and 1-M2.
1222830	Management access loss when FIM02 on standby chassis is primary Worker.

FortiView

Bug ID	Description
1146317	Incorrect offload status when NPU Accelerated sessions have an offload value of 9.
1192657	No data is displayed when Cloud is chosen as best available device.

GUI

Bug ID	Description
1040164	Interface X1/X2 does not display on the GUI-Network-Interface page faceplate for FortiGate-90G Gen2.
1055740	CPU usage issues observed during GUI login with a USB drive containing many files.
1063643	GUI interface panel mismatch when FortiGate 121G Gen2 faceplate is changed.
1098643	Unexpected behavior observed in the WebSocket caused by stale connections, resulting in persistent memory allocation errors or Node.js restarts.
1107513, 1138545	An error condition in Node.js occurs when handling stale websocket connections.
1149411	Increased Node.js memory usage occurs caused by erroneous memory allocation.
1160891	Incorrect inbound traffic values appear on the bandwidth widget for EMAC VLAN interfaces when configured over physical interfaces.
1166328	An error condition in httpsd occurs when ACME is enabled.
1174970	Configuration changes to FortiGate Cloud SSO Admin settings are lost after reboot.
1175204	Incorrect IP address displayed in GUI when fortiguard-anycast-source is set to AWS.
1177282	Failed to save changes when reordering NAC policies via GUI on FortiGate models after upgrade.
1180629	GUI displays username sensitivity warning when username-sensitivity is disabled.

Bug ID	Description
1181363	Failure to load FGD categories when creating or editing webfilter rating override entries.
1182557	VCI options are lost when saving changes on the GUI.
1183360	VPN status display issue when upgrading from 7.6.2 to 7.6.3.
1183906	Incomplete IP list appears when viewing threat feed object entries in GUI.
1190608	Permission denied error occurs when Remote+Wildcard administrator attempts to create Web Profile Override in GUI.
1191076	Interface bandwidth data is not displayed when LAG is upgraded from 2x40G to 2x100G ports.
1191960	Incorrect certificate HASH algorithm name is displayed in FortiGate GUI when viewing certificate information.
1192959	An empty page is displayed when clicking FortiTokens in the navigation menu.
1193206	Faceplate fails to load after editing an interface.
1193884	VLAN interface bandwidth displays incorrectly in GUI dashboard widget when LAG members are removed and re-added.
1194972	Devices are not visible on Asset & Identities > OT view when API response from /api/v2/monitor/user/device/query retrieves devices without sufficient information.
1195382	In Edit FortiAP dialog, Transmit power mode cannot be overridden when 8 SSIDs selected on wtp-profile.
1196746	An error condition occurs in IPsec when 'Interface Subnet' type is selected for IPv4 split tunnel address.
1197356	Search function issues occur in Asset Identity Center when searching by device name or OS.
1198106	Inaccurate SD-WAN spillover algorithm description when priority values are the same.
1198609	Memory usage issues caused by Node.js forking when using the JIT optimizer in V8.
1199029	DHCP Server conflicts occur when changing from DHCP Server to Relay mode on an interface.
1203007	Configuration view issue when logging in with FortiGate Cloud SSO super_admin account.
1203716	Memory usage issues caused by Node.js compressing or decompressing in a thread are resolved by forking a new process.
1205624	Warning message displays when creating Phase 2 in IPsec without matching encryption authentication pairs to Phase 1 proposal.
1208267	GUI displays a blank page after logging in as a vdom-admin with 2FA.
1212726	Authentication issues occur when using FortiCloud SSO via FortiGate Cloud login.

Bug ID	Description
1214424	Authentication failure occurs when logging in to the GUI after upgrading from version 7.6.3 to 7.6.4.
1217386	Incorrect label appended when copying policy in GUI.
1220854	Read-write mode is displayed after login with read-only vdom-admin when FortiGate is managed by FortiManager.

HA

Bug ID	Description
1096472	Traffic disruption occurs when moving VDOMs between VClusters.
1121141	IP address is not released by DHCP client when MAC changes during HA enablement.
1142218	Source IP cannot be selected when HA-direct is enabled and multiple ha-mgmt-interfaces are configured.
1148862	HA synchronization issues occur when user local password expiration and UUIDs are mismatched.
1163147	Token license activation fails when using a virtual serial number (vSN) on a new HA FortiGate.
1170958	HA status shows as 'Unknown' when changing HA group ID.
1187401	Unexpected behavior in the system occurs when an HA unit is restarted.
1191128	Intermittent traffic disruption occurs when the secondary FortiGate is rebooting in HA mode.
1191136	HA ports cannot be added to an aggregate interface when running FortiOS 7.2.11 build 1740.
1203672	Config overwrite issue occurs when restoring config from TFTP server on master via CLI in HA setup.
1206861	CPU usage issues observed during hasync usage of the SSL VPN reserved UDP port 8903.
1208912	Session loss when AS path prepend redirection is used after rebooting an FGSP peer.
1212718	FGFM tunnel remains down after HA failover event when undestroyed FGFM session prevents new FGFM sessions from being created.
1221816	Network instability when FIM is rebooted on primary after failover using 'diag sys ha reset-uptime'.

HyperScale

Bug ID	Description
1138921	Suggest to change the default NPU setting to reduce the high-frequent of spv/tpv table messages.
1184045	IPv6 TCP/UDP traffic fails to pass through when a threat feed object is integrated into an IPv6 High Security policy due to an internal state handling issue, which erroneously disables IPv6 functionality.
1199557	Unsupported network interfaces are permitted as members of a Link Aggregation Group (LAG) when the LAG is configured for hardware session synchronization, leading to potential configuration errors.
1200885	Renaming an ippool in a FortiGate setup with VDOMs results in unintended behavior affecting network traffic.
1204615	Improvements to session management to resolve memory usage issues when creating hardware sessions.

ICAP

Bug ID	Description
1028368	ICAP connection queue-full errors occur when the max connection count is split and allocated to each worker.

Intrusion Prevention

Bug ID	Description
899659	Inaccurate session anomaly frequency values appear when threshold is exceeded under full-offload conditions.
1091118	Oversized packets exceeding the MTU cause delayed ACKs, leading to unintended behavior.
1144684	High CPU usage occurs when processing multiple RTSP streams due to inefficient resource management by the RTSP decoder.
1157469	Traffic outage when disabling nTurbo acceleration.

Bug ID	Description
1162794	Unintended behavior occurs in the IPS Engine caused by the SCADA dissector.
1190395	Intermittent traffic disruption occurs due to an error condition in the IPS Engine caused by a DAC handler issue.
1199243	Definition file update issues occur when device-identification is enabled for a zone interface in the firewall policy.
1211362	Decrypted traffic mirror MAC address changes do not take effect until IPS Engine is restarted when used in a firewall policy.
1216974	Intermittent traffic disruption caused by an error condition in the IPS Engine during hybrid key generation.
1218520	BFD flaps occur due to an error condition in the IPS engine.

IPsec VPN

Bug ID	Description
1068626	SOC4 platform IPSec traffic may stop in specific corner cases due to the IPSec outbound process becoming unresponsive.
1106454	IKE debug prints large number of "compute DH shared secret request pending" when rekeying or DH group setting not matched on both sides.
1137576	IPsec tunnel failure occurs when IKE Diffie-Hellman processing fails.
1144548	Authentication failure occurs when using IPsec VPN IKEv2 with MsCHAPv2 and RADIUS server.
1146975	IPsec tunnel issues occur when NPU offload is enabled on SOC4 platforms.
1174914	IPsec tunnel sourcing from secondary IP address instead of primary IP occurs when local-gw is set and then unset on the phase1-interface.
1179794	VPN IPsec client to site connection fails when EAP proxy times out.
1180324	Auth-ike-saml-port setting is lost when set to 10443 during FortiGate update or reboot.
1180987	VPN tunnels may not come up after HA failover events, causing routes via these VPN tunnels to not be added to the routing table.
1182043	IPsec VPN connectivity issues occur when 'local-gw' is set to 0.0.0.0 under the dial-up IPsec VPN interface.
1184605	Firewall policy issues occur when a new policy is created for a connected VPN user without explicit mention in the policy.
1186237	CPU utilization increases when a remote access VPN user connects or disconnects

Bug ID	Description
1190688	High CPU usage occurs when changing firewall policies in a FortiGate device with a large number of policies.
1192598	IPsec phase1-interface option 'loopback-asymroute' is not available for IKEv1.
1195129	Intermittent traffic disruption caused by error condition in IKE daemon when connecting to Dialup IPsec IKEv2 on Azure VM64.
1195400	Reauthentication failure occurs when using IPsec IKEv1 after upgrade.
1195785	High CPU utilization occurs when IKE handles async DH errors during IKEv1 phase1 or phase2 rekey.
1197607	An error condition in IKEd occurs when using FortiClient to dialup IPsec with SAML authentication on Azure FGT-VM.
1199265	Intermittent traffic disruption occurs when IPsec tunnels are stuck and the engine hangs on the SOC4 platform.
1199815	Intermittent IPsec traffic disruption occurs when IKE tunnel status is out of sync with kernel.
1200669	VPN setting is deleted after device reboot when password policy is enabled and pre-shared key length meets minimum requirements.
1200709	Intermittent BGP disruption caused by DPDK enablement.
1203271	DPD probes are sent excessively when dpd-retrycount is set to 0.
1204679	RADIUS authentication issues occur when packet fragmentation happens over IPsec tunnels.
1206506	Traffic disruption occurs when IPsec tunnel manager write sequence issue happens.
1210730	Drv-drift counter increase occurs when sending TCP traffic through IPsec with vpn-id-ipip encapsulation.
1218538	Traffic drop occurs when tunnel ID changes from random 10.0.0.x to remote gateway public IP.
1223316	Incorrect local ID is sent during IPsec phase 1 when localid-type is set to address.

Intrusion Prevention

Bug ID	Description
1140846	Unexpected behavior observed in the IPS Engine when handling HTTPS traffic using HTTP/2 in certain configurations.
1157185	High CPU usage occurs in IPS Engine when traffic looping happens due to incorrect VRF validation in local-out path.

Bug ID	Description
1158024	Packet drops and lower CPU utilization on FPC blades when using IPv6 traffic with np-accel-mode enabled and auto-asic-offload.

Log and Report

Bug ID	Description
1116246	An error condition in locallogd occurs when the system enters memory conserve mode.
1119074	An error condition in syslog occurs when processing misaligned incoming CMDB messages.
1129247	Certificate verification fails when using OFTP custom certificate with non-Fortinet organization name.
1143662	Username is truncated in application logs when it exceeds 31 characters.
1154982	CPU usage issues observed during high syslogd activity.
1171020	Authentication logs are missing when 2FA timeout occurs during SSL VPN authentication.
1175276	Syslog-override setting status reverts to disabled when restoring VDOM configuration with syslog-override enabled.
1177974	Audit logs are not received by FortiAnalyzer when FortiAnalyzer is enabled or disabled in FortiGate.
1180182	Alert email fails when device is rebooted under HA mode.
1189755	When user performs a log search and also triggers a drill-down for more logs simultaneously, the page may be stuck in loading.
1190659	Log search issues occur when searching for a specific mac address in the GUI.
1193296	IPS log display issue occurs when double quote is in agent field.
1197727	Incorrect CEF format occurs when forwarding logs with FTNTFGTaction field.
1200810	CPU usage issues observed during quarantine logging.
1210810	System log issues occur when exiting memory conservation mode.

Proxy

Bug ID	Description
764143	SSL version restrictions not enforced in flow mode when using 'min-allowed-ssl-version'.
776013	CPU usage issues observed during HTTP2 usage.
1159485	Traffic duplication may occur on FortiGate due to retransmission of out-of-sync TCP streams when insecure ciphers are used.
1178184	SSL errors occur when accessing a specific website due to an unexpected record type when Web Filtering and DPI are enabled in Flow mode.
1180097	An error condition in WAD occurs when using HTTP2 or HTTP3 with concurrent authentication requests.
1183893	Handshake failure occurs when using explicit web proxy with deep inspection to access HTTPS websites through HTTP requests.
1191144	An error condition in WAD occurs when sec-default-action is set to accept under web-proxy explicit.
1197212	WAD incorrectly prioritizes the default FortiGuard CA bundle over user-installed CAs when building certificate chains for cross-signed server certificates.
1213957	TCP download rate drops when FortiGate uses SSL inspection with an antivirus profile in flow mode.
1220714	On 200G series FortiGate, some private keys are not loaded resulting in HTTPS traffic description caused by the missing private keys.

REST API

Bug ID	Description
1154124	Adding dynamic fabric addresses via the FortiNAC REST API fails due to an issue with HTTP header validation.
1174023	Invalid values in 'name' and 'group' fields occur when using GET /api/v2/monitor/webfilter/fortiguard-categories.
1175330	Incorrect FGT configuration returned when long-vdom-name is enabled.
1186413	Incorrect POE max value is returned when querying REST API for FortiGate 400 series switches.

Routing

Bug ID	Description
1157835	Private AS removal issue occurs when remove-private-as is enabled in a neighbor-group and local-as is private.
1169479	The SLAAC IPv6 address does not get flushed after link goes down.
1188061	Incorrect BGP4-MIB bgpLocalAS OID value occurs when 4-byte BGP AS is configured higher than 2147483647.
1193788	BGP TCP Auth Options key-chain is not applied to the BGP neighbor, causing the neighborship to not establish.
1196770	BGP default route installation issue occurs when capability-default-originate is enabled.
1197960	BGP peer flaps when stressful traffic is present on the interface with Quality of Service enabled and top priority.
1202262	PIM failure occurs when using virtual-switch interface.

SD-WAN

Bug ID	Description
1157493	SDWAN rule with multiple mac address entries only uses the first mac address when address type is mac.
1192488	Link Monitor failure occurs when HTTP response header has an invalid format.

Security Fabric

Bug ID	Description
995772	Missing devices observed when loading into OT view with insufficient device information.
1006397	In case of failure during a federated upgrade process, the system does not report granular failure details for individual devices.
1156006	SFTP backup fails when triggered through automation stitch on a FortiGate in an HA cluster using Windows-style paths.

Bug ID	Description
1191533	FortiAP upgrades/downgrades fail to complete properly after an HA failover using "diag sys ha reset-uptime" in a FortiGate CSF topology.
1191902	Automation stitch sync issue occurs when HA secondary unit is used in Security Fabric.
1224923	IP collection fails when Azure returns a SubscriptionNotFound 404 error.

Switch Controller

Bug ID	Description
1138263	FortiSwitch port configurations fail to update and GUI display issues occur when user-info process overloads system resources with excessive connections.
1141909	The 10G port on FortiGate-120G is not coming up when connected to a FortiSwitch S148F port using a 10G DAC cable
1149256	Renamed FortiSwitch failed to sync to secondary FortiGate.
1165703	Random devices not matching to NAC policy occurs when multiple MACs are present on the same user-device-store entry.
1170323	Interfaces cannot be enabled as FortiLink interfaces on FortiGate with hardware revision 2.
1183725	Outage occurs when modifying LLDP profile on multiple ports including FortiLink trunk ports.
1198110	FortiSwitch disconnection observed when adding managed-switch.
1199648	Traffic interruption occurs when shutting down an interface in a dual inter-crossed connection with Hardware Switch.
1208846	Authentication issues occur when upgrading FortiGate due to RADIUS auth type mismatch.
1216633	Unable to change switch name when space is in the name.

System

Bug ID	Description
828849	No "Diagnostics" information is available for Avago AFBR-79EBPZ Bidi transceivers on FortiGate when using the get system interface transceiver command.

Bug ID	Description
906269	An error condition occurs in EXT4-fs when booting without a backup image installed.
918574	Unintended traffic sent to public servers occurs when cloud-communication and include-default-servers settings are disabled on FortiGate models.
945871	D-NAT functionality fails when using a Software Switch in explicit mode due to incorrect session matching during packet forwarding.
986926, 1015698, 1024737, 1039956, 1042577, 1058256	Unexpected interface downtime occurs on some FortiGate models when using DAC cables after upgrade, due to improper Signal-OK loss detection.
991285, 1112999	Broadcasts are unexpectedly forwarded between VXLAN peers when certain FortiGate models are configured as hubs in a Hub-Spoke topology.
1035407	An error condition occurs in FortiGate when ARM Cortex-A9 errata 845369 is encountered.
1044794	After installing a .deb image during bootup device shows "File - 1 seems to be corrupted" error and cannot boot up.
1046484	After shutting down FortiGate using the "execute shutdown" command, the system automatically boots up again.
1058256	Some FortiGate models experience unexpected interface down time when using DAC cables after upgrade, due to improper Signal-OK loss detection.
1061796	Inaccurate traffic counters display for EMAC-VLAN interfaces when VLAN ID is set to 0 and traffic is offloaded to the NPU.
1102417	Huawei LTE modem E3372 not recognized on FGT-90G.
1121078	TX Power levels are missing when using FTL4E1QE1CFTN QSFP+ER transceivers on FortiGate devices.
1122446	GPS location updates fail to occur when the GPS signal reception is poor on FortiGate devices.
1124535	DNS search list options are appended to router advertisements when using IPv6 prefix delegation with SLAAC.
1124535	DNS Search list options are appended to Router Advertisements when using IPv6 prefix delegation with SLAAC.
1135974	FortiGate-50G-5G fails to get an IPv6 address when set pdp-type ipv4v6.
1145397	When editing user exemption configurations via the GUI on FortiGate devices, unexpected behavior occurs due to a mismatch between GUI and CLI data structures.
1149202	ICOND application startup issue occurs when using raw type over IPsec tunnel on FortiGate Rugged 70F.

Bug ID	Description
1154920	Intermittent 10G SFP+ link establishment issues occur when FortiGate-200F reboots and connects to a Ciena 3924 switch.
1155432	An error condition occurs in cid-scan when the invariant about reference count for a cid_host and the cid_host zombie list is broken.
1158452	Traffic disruption occurs when creating EMAC-VLAN interfaces with traffic running in the background.
1160683	Windows Wi-Fi clients unable to obtain DHCP IP due to dropped fragmented CAPWAP packets on virtual switch interface.
1164836	NTP server unable to be set with 64 digit key in FIPS-CC mode.
1168062	Config overwrite issue occurs when importing FortiGate YAML config using the current Python library.
1169448	iPad device name appears as MAC address in logs and DHCP Monitor when connected via WiFi to FortiGate.
1173177	High CPU usage occurs when making a configuration change on FortiGate-6301F devices, causing CPU Core0 to spike on all FPC and MBD.
1175134	Message server status goes down when configured with loopback as source.
1175221	The 100full speed option is missing for the shared SFP ports of the FortiGateRugged-60F.
1178202	VLAN tag is stripped when forwarding VXLAN packets between spokes.
1180084	ZTP deployments fail on FortiGate 9xG Gen2 devices because DHCP client mode is not configured by default on interfaces a and b.
1180734	After FortiGate is upgraded from 7.4.7 to 7.4.8, an unexpected behavior occurred.
1181444	USB-Tethering fails to work on FortiGate 91G when configuring it as a WWAN connection.
1184180	Unexpected behavior occurs when restoring an invalid configuration with a system.interface defined as type aggregate and a system.virtual-switch with the same name.
1184749	PPPoE connection failure occurs when Multilink MRRU is enabled on a VLAN interface.
1188339	STP forwarding fails after rebooting when stpforward is enabled on a hard-switch interface.
1191813	Connectivity issues occur when auto negotiation is enabled on the Cisco switch end.
1192440	SNMP sensors report down when snmpd rebuilds interface cache.
1192920	Packet capture issues occur when capturing a high volume of matched packets.
1193889	Certificate error occurs when connecting to FortiAnalyzer via SSH.
1194982	Interface bandwidth becomes zero when fast path is enabled.

Bug ID	Description
1197255	Error condition in sflowd occurs when removing entries from netflow cache under high load.
1197885	Memory usage issues caused by ASLR when upgrading from 7.4.7GA to 7.4.8GA.
1198181	An error condition in SNMP daemon occurs when querying fgVpnSslStatsEntry after upgrading to 7.6.4.
1198758	Intermittent traffic disruption occurs when using KPN SIM card with default APN settings.
1199132	An error condition occurs in the lan-extension-controller when changing the controller address.
1199169	IPv6 address acquisition issues occur during upgrade to v7.6.4.
1199322	VDSL2 sync issue occurs when ITU G.993.5 is enabled on 50G-DSL.
1200320	VPN goes down when dhcpc tries to renew IP lease and receives a DHCPNAK response.
1200604	Config backup to FGT Cloud fails when retrieving full config.
1203193	FGR-70G and FGR-70G-5G-Dual do not support CLI for automation-stitch notifications when DIO module alarm functionality is activated, namely, 'set condition-type input' is not available under 'config system automation-condition'.
1204023	SNMP response contains wrong values when querying certain OIDs under FgSoftware.
1205316	Recurrent disconnections occur when IMS APN attachment attempts are made.
1206778	Unable to update FortiGuard licenses when file permissions are inccorect.
1211645	Authentication error when using HEX based keys with SHA1 or SHA256 in NTPv4.
1211647	Authentication error when using SHA256 as key-type in NTPv4.
1211704	Time synchronization issues occur when NTP server authentication is enabled.
1211873	Device connection state is not updated when connected to FortiGate integrated hardware switch on platforms with no logdisk.
1228304	Unexpected behavior occurs when FortiGate receives Forward Relocation Request without PDN IE message.
999816, 1064241	FortiGate 100E/101E units may enter an unresponsive state (no GUI, SSH, or console access) due to a rare timing issue, requiring a system reboot to regain access.

Upgrade

Bug ID	Description
1214360	An error condition in the browser occurs when uploading a firmware image file during upgrade from 7.6.2 to 7.6.4 .

User and Authentication

Bug ID	Description
1139688	Username truncated when RADIUS Accounting-Request username exceeds 66 characters.
1142387	SCEP enrollment fails when using IP address to connect to the server.
1158484	When user logs into the FortiGate via FortiManager's CLI console, users are not forced to change password even if password has expired.
1165116	Event log is not generated for expired authentication attempts, for example, when it fails due to 2FA timetout.
1170894	IKEv2 local user authentication issues occur when using two-factor email authentication with extended timeout values.
1177318	Factory default certificates not displaying certificate information in the CLI for FortiGate-201G models.
1177593	User addition fails with FortiToken Cloud when using 2 HA FortiGates with virtual serial number enabled.
1178467	Administrator accounts are unintentionally unlocked when the admin-lockout-threshold is increased.
1182725	EAP-proxy fails to match group when the group length exceeds 128 characters.
1185705	Seed import failure occurs when uploading token seed file via GUI.
1189693	LDAP authentication fails on OpenLDAP due to the type of ldap_result used.
1196434	SAML authentication issues occur when LASSO_PROFILE_SIGNATURE_VERIFY_HINT_FORCE is set and the SAML response is not signed.
1205671	Authentication failure occurs when all-usergroup is enabled under radius.
1207282	Authentication failure occurs when using multiple wildcard entries for admin access with TACACS server.
1213932	SAML authentication issues occur when authd encounters an error condition during IPsec SAML SSO authentication.
1223051	Authentication failure occurs when using remote RADIUS server with TFA enabled.

VM

Bug ID	Description
1159433	DPDK error when traffic reaches more than 4GBps.
1194713	ARM_KVM/GCP/OCI unable to format shared data partition on ARM VMs.
1195615	Failover issue occurs when reserved IP address exists in an OCI subnet and is not associated with a VNIC.
1198515	Memory usage issues caused by IPsec tunnel rekey when DPDK is enabled.
1204790	IP address collection issues occur when a VM reports a provisioning error in a VMSS.
1207410	Port flapping occurs when using iavf driver.
1213875	License download failure occurs when using proxy setting for Azure and AWS PAYG.
1215317	Public IP disassociation occurs when SDN connector uses wrong Azure Management API endpoint.
1215396	Unexpected behavior occurs when configuring a VLAN sub-interface on a physical port with DPDK enabled.
1219012	Dynamic object updates fail when an SDN connector is not functioning.
1220070	Discrepancy in interface stats occurs when COS is set and DPDK offload is enabled.
1221924	Inconsistency in IPS-socket size occurs when using a subscription license
1224484	An error condition occurs in the diag daemon during image upgrade matrix operations.

VoIP

Bug ID	Description
1201825	Packet drop occurs when SIP ALG and Hyperscale are enabled.
1204573	Calls fail to establish when FortiGate receives a SIP 302 Redirect response from a Load Balancer.

Web Application Firewall

Bug ID	Description
1130819	Registration traffic is blocked when WAF profile is enabled.
1208919	Credit card information detection issues occur when WAF credit card signature requires PCRE_MULTILINE.

Web Filter

Bug ID	Description
1074960	Internet connectivity slowness may occur in proxy-mode inspection policies due to traffic cannot fully utilize queues from all NPUs.
1096297	Timeout occurs when web filter is enabled and fragments occur.
1096442	Web filter logs are not displayed when offload is enabled in the policy.
1156789	Web filter settings category name, block screen category name, and log category name are translated into different Japanese when using web filter profile on FortiGate.
1185240	IP address is added to custom header when http-ip-header is enabled on virtual server and custom header value starts with 'a' (v7.4.8) or 'h' (v7.6.4).
1208074	Translation issues occur when FortiGate GUI is set to Portuguese.
1211319	URL filter issues occur when using perl style regex flags after upgrade,
1214017	Memory usage issues occur when adding an external threat feed with a large number of similar patterns.

WiFi Controller

Bug ID	Description
1127637	wpad requests are sent exclusively to IPv6 addresses and do not attempt fallback to IPv4 in environments supporting dual-stack configurations.
1158774	Wireless and wired devices cannot communicate across a software switch on FortiGate-G models when capwap-offload is enabled. This issue affects deployments attempting to create a flat Layer 2 network between wired and wireless segments.

Bug ID	Description
1165690	The cw_acd process on the FortiGate may exhibit high CPU usage when Radio-3 is dedicated to monitor mode and perform rogue AP scanning.
1180552	Logs display incorrect channel ID after DFS detection.
1189187	The AP profile's auto-transmit power range adjusts unexpectedly when a single endpoint is modified.
1191723	Wireless clients encounter VLAN flapping between NAC and onboarding.
1192914	There is no WiFi SSID signal after power off / power on FWF40F.
1207256	Inconsistent client signal-to-noise ratio values occur on some FortiGate models.
1209209	FortiGate devices fail to process authentication responses during IKEv2 setup, resulting in connection failures.

ZTNA

Bug ID	Description
1121978	Adding new HTTPS/HTTP ZTNA server mappings via GUI fails with a duplicate entry error, while attempting to exit after cancellation alters existing entries' URLs.
1178076	When access proxy is configured, client cannot access multiple virtual hosts on the same connection.
1178742	ZTNA destination unreachable in rare cases where 'sni-server-cert-check' is enabled on a FortiGate and the SNI field is missing.
1183544	Portal displays wrong layout when accessing Agentless ZTNA web bookmarks with complex URLs.
1184250	ZTNA access failure occurs when using a wildcard FQDN on the first attempt.
1185076	EMS rejects the wrong FQDN format when configuring virtual-host in ZTNA server->tcp-forwarding entry.
1194525	Traffic blockage occurs when ZTNA UDP forwarding with deep-inspection is enabled.
1198173	An error condition occurs in WAD when using ZTNA portal RDP web bookmarks.
1199808	Incorrect policy type recorded on ZTNA traffic logs.
1208519	Traffic is denied when accessing HTTPS bookmarks with subdomains of the ZTNA Portal's root domain.

Known issues

Known issues are organized into the following categories:

- New known issues on page 63
- Existing known issues on page 63

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 7.6.5.

WiFi Controller

Bug ID	Description
1227978	Wi-Fi clients cannot maintain previous IP addresses after roaming from one FAP to another in the inter-controller layer-3 roaming topology.

Existing known issues

The following issues have been identified in a previous version of FortiOS and remain in FortiOS 7.6.5.

Agentless VPN (formerly SSL VPN web mode)

See also SSL VPN tunnel mode replaced with IPsec VPN on page 13.

Bug ID	Description
1173772	Unable to connect to SMB over SSL VPN web mode in FIPS-CC mode.

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.

Explicit Proxy

Bug ID	Description
1145590	certificate-inspection dropping client hello segment when traffic is tunneled in webproxy.

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.
835847	Password policy was not correctly updated when using automation stitch.
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.
1102072	On the FortiGate 7000 platform, cmdbsvr CPU usage can be higher than normal for extended periods on one or more FPM.

Bug ID	Description
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.
1130491	6KF WCCP doesn't seem to work as expected.
1131269	Dial up tunnel - syn and syn ack are on different blades even though ipsec-tunnel-slot set to master.
1132294	ip nat port-preserve feature is not working when client's source port doesn't fall under FPM's nat port-range.
1170210	FGT Wireless controller Wifi client cannot ping GW/FGT interface. Pass-through traffic works fine.
1185528	Subscription license on the secondary chassis is missing after the graceful upgrade from 7.2.10/11 to 7.2.12. **Workaround**: Run `execute update-now` again.
1185869	Multicast traffic not working.

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
793029	Unexpected behavior occurs on some FortiGate models when a FortiClient lacks a required MAC address attribute.
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.
1140785	GUI packet capture displays incorrect information.

HA

Bug ID	Description
1234340	Asymmetric session handling fails when FGSP peering is established between two FortiGate devices with incomplete base MAC information. **Workaround**: Re-enable Port12 to populate the peer MAC information on both devices.

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.
1042011	Observed `NPD-0 :DEL PRP FAIL! 0xffffffff; NPD-0 :PRP ADD FAIL! 0xffffffff nat_type=00000044 block_sz=128 port_base=11000`.
1130107	Session-helper DNS session is created by hw and can be seen in log2host table.
1151441	(4801F-HA) "ha2" port as hw-session-sync-dev shows out-of-sync even though it is connected to NP7.

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`.
1093769	Unexpected IPS UTM log has been generated for established TCP sessions that lack application data in NFGW policy mode.

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.

Log & Report

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

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.
1103046	Shaping profile with queuing - no interface stats.

Security Fabric

Bug ID	Description
1040058	The Security Rating topology and results does not display non-FortiGate devices.

Switch Controller

Bug ID	Description
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.
1041726	Traffic flow speed is reduced or interrupted when the traffic shaper is enabled.
1103617	Integrating an interface does not work when adding a new member into an existing interface or creating a new interface.
1142465	ARP entries age out quickly after a system reboot, despite a long reachable-time setting.

Upgrade

Bug ID	Description
1091213	Upgrade causes X5 & X7 SFP Interfaces to go down.

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.
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.
1141380	FortiGate cannot send token activation code to email.

VM

Bug ID	Description
1125805	Unable to access the FortiGate VM web interface deployed on AWS when ACME is enabled.

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 7.00048 is released as the built-in AV Engine.

Built-in IPS Engine

IPS Engine 7.01168 is released as the built-in IPS Engine. Refer to the IPS Engine Release Notes for information.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

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

Open source XenServer limitations

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

www.fortinet.com