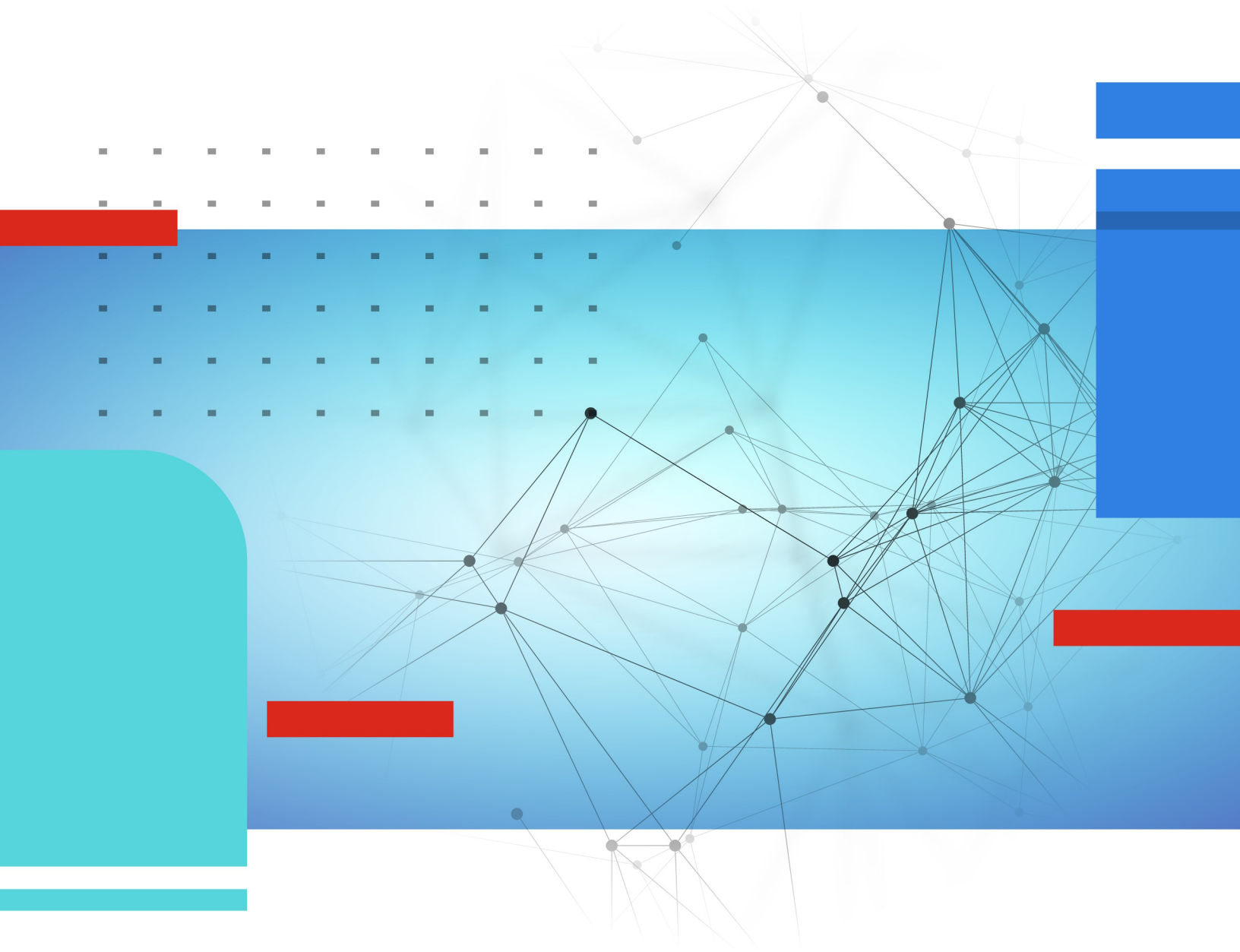
Release Notes

FortiOS 7.6.8



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



October 22, 2026
FortiOS 7.6.8 Release Notes

TABLE OF CONTENTS

Change Log **6**
Introduction and supported models **7**
Supported models 7
FortiGate 6000 and 7000 support 8
Special notices **9**
FortiGate cannot restore configuration file after private-data-encryption is re-enabled 9
FortiManager support for updated FortiOS private data encryption key 10
Hyperscale incompatibilities and limitations 11
Hyperscale NP7 hardware limitation 11
FortiGate 6000 and 7000 incompatibilities and limitations 12
FortiGate VM memory and upgrade 12
Changes to NP7 traffic shaping 12
SSL VPN tunnel mode replaced with IPsec VPN 13
Agentless VPN (formerly SSL VPN web mode) not supported on some FortiGate series models 13
2 GB RAM FortiGate models no longer support most FortiOS proxy-related features 14
2 GB RAM FortiGate models no longer support Security Rating and Security Fabric topology 14
GUI access conflict with IPSec TCP tunnel on the same interface 14
SAML certificate verification 15
Policy check required for hairpin traffic 15
Changing vlan-lookup-cache requires system restart 16
CSF downstream GUI login fails with Security Fabric SAML SSO **17**
Changes in CLI **18**
Changes in default behavior **19**
New features or enhancements **20**
Hyperscale 20
LAN Edge 20
Log & Report 21
Policy & Objects 21
Security Profiles 21
System 22
Upgrade information **23**
Fortinet Security Fabric upgrade 23
Downgrading to previous firmware versions 25
Firmware image checksums 25
FortiGate 6000 and 7000 upgrade information 25
Default setting of cp-accel-mode is changed to none on 2GB memory models 27
Policies that use an interface show missing or empty values after an upgrade 27
Managed FortiSwitch do not permit empty passwords for administrator accounts 28
Removed speed setting affects SFP+ interfaces after upgrade 28

Hyperscale with FGCP HA clusters and interface monitoring ... 28
Password policy enforcement ... 29
Product integration and support ... 30
Virtualization environments ... 31
Language support ... 31
Agentless VPN support ... 32
FortiExtender modem firmware compatibility ... 32
Resolved issues ... 35
AntiVirus ... 35
Application Control ... 35
Data Leak Prevention ... 35
DNS Filter ... 36
Endpoint Control ... 36
Explicit Proxy ... 36
Firewall ... 37
FortiGate 6000/7000 Platform ... 38
FortiView ... 39
GUI ... 39
HA ... 40
HyperScale ... 41
Intrusion Prevention ... 42
IPsec VPN ... 42
Log and Report ... 43
Proxy ... 44
REST API ... 44
Routing ... 45
SD-WAN ... 45
Security Fabric ... 45
SSL-VPN ... 46
Switch Controller ... 46
System ... 47
Upgrade ... 48
User and Authentication ... 49
VM ... 50
VoIP ... 50
Web Filter ... 51
WiFi Controller ... 51
ZTNA ... 51
Known issues ... 53
New known issues ... 53
FortiGate 6000/7000 Platform ... 53
Existing known issues ... 53
Endpoint Control ... 53
Firewall ... 53

FortiGate 6000/7000 Platform 54
FortiView 54
GUI 55
HA 55
HyperScale 55
Intrusion Prevention 55
IPsec VPN 56
Proxy 56
REST API 56
Security Fabric 56
Switch Controller 56
System 57
User and Authentication 57
VM 57
Web Filter 57
Built-in AV Engine 58
Resolved engine issues 58
Built-in IPS Engine 59
Limitations 60
Citrix XenServer limitations 60
Open source XenServer limitations 60

Change Log

Date	Change Description
2026-10-22	Initial release.
2026-10-22	Updated Special notices on page 9, Upgrade information on page 23, Resolved issues on page 35, and Known issues on page 53.

Introduction and supported models

This guide provides release information for FortiOS 7.6.8 build 3744.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.6.8 supports the following models.

FortiGate	FG-30G, FG-31G, 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-3800G, FG-3801G, 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-30G, FWF-31G, 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-60G, FGR-70F, FGR-70G, FGR-70G-5G, 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



Starting with FortiOS 7.6.1, New deployments on Azure Marketplace use Generation 2 (Gen2) VM images and no longer support Azure F-series, Fs-series, Standard Dv2, and Standard Dsv2 instance types, or similar instance families, which require Gen1 images. Existing FortiGate VMs deployed on F-series or Fs-series instance types can continue to operate and be upgraded to FortiOS 7.6.1 or later. Upgrade to newer instance families for better and more stable performance. See Instance type support for details.

FortiGate 6000 and 7000 support

FortiOS 7.6.8 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 on page 9
- FortiManager support for updated FortiOS private data encryption key on page 10
- Hyperscale incompatibilities and limitations on page 11
- Hyperscale NP7 hardware limitation on page 11
- FortiGate 6000 and 7000 incompatibilities and limitations on page 12
- FortiGate VM memory and upgrade on page 12
- Changes to NP7 traffic shaping on page 12
- SSL VPN tunnel mode replaced with IPsec VPN on page 13
- Agentless VPN (formerly SSL VPN web mode) not supported on some FortiGate series models on page 13
- 2 GB RAM FortiGate models no longer support most FortiOS proxy-related features on page 14
- 2 GB RAM FortiGate models no longer support Security Rating and Security Fabric topology on page 14
- GUI access conflict with IPSec TCP tunnel on the same interface on page 14
- SAML certificate verification on page 15
- Policy check required for hairpin traffic on page 15
- Changing vlan-lookup-cache requires system restart on page 16
- CSF downstream GUI login fails with Security Fabric SAML SSO on page 17

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 7.6.8 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 7.6.8 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.

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

For security purposes, in previous versions, FortiGate required 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 has now been loosened with the following configuration:

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

Option	Description
`enable`	Both response and assertion must be signed and valid.
`disable`	At least one of response or assertion must be signed and valid (default).

By default, the setting is disabled, which only requires one of the response or assertion to be signed and valid.

For more information, see Identity Providers.

Policy check required for hairpin traffic

In FortiOS 7.6.5, the default setting for `allow-traffic-redirect` and `ipv6-allow-traffic-redirect` 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.

Changing vlan-lookup-cache requires system restart

Enabling or disabling `vlan-lookup-cache` or any configuration change that causes a system restart can disrupt the operation of an FGCP cluster. If possible, you should make this configuration change to the individual FortiGates before setting up the cluster. If the cluster is already operating, you should temporarily remove the secondary FortiGate(s) from the cluster, change the configuration of the individual FortiGates and then re-form the cluster. You can remove FortiGate(s) from a cluster using the *Remove Device from HA cluster* button on the *System > HA GUI* page. For more information, see Disconnecting a FortiGate.

CSF downstream GUI login fails with Security Fabric SAML SSO

After upgrading to FortiOS 7.6.8, administrator GUI login using SAML single sign-on (SSO) fails. The browser is redirected to `/error/saml` and the login page reports *Single Sign-On Failed*. This affects any FortiGate whose admin GUI acts as a SAML service provider (SP), including Security Fabric SAML SSO login to a downstream FortiGate, admin SAML SSO login to a standalone FortiGate using an external IdP, and FortiCloud SSO admin login.

Changes in CLI

Bug ID	Description
1220299	In Agentless VPN settings, when multiple domains in dns-suffix is configured, parse each entries separated by ";".

Changes in default behavior

Bug ID	Description
1073893	When a large TCP packet enters an IPsec tunnel, the FortiGate no longer adjusts the TCP MSS value automatically. Instead, it sends an ICMP message (ICMP_FRAG_NEEDED) to notify the sender of the correct MTU size. The sender can then adjust the TCP MSS and subsequent packet sizes accordingly.

New features or enhancements

More detailed information is available in the New Features Guide.

Hyperscale

Feature ID	Description

1236578	SCTP traffic processing behavior can now be configured on SoC4 and SoC5 platforms. New NPU settings control SCTP offloading and whether SCTP control packets are forwarded to the host for processing.
	CLI changes
	`config system npu`
	`  set sctp-offload {enable | disable}`
	`  set sctp-ctrlpkt-to-host {enable | disable}`
	`end`

1280968	Added the `ipv4-option` setting under `config system npu` > `config fp-anomaly` to control how IPv4 packets containing IP options are processed.
	CLI changes
	`config system npu`
	`  config fp-anomaly`
	`  set ipv4-option {allow | trap-to-host}`
	`  end`
	`end`

LAN Edge

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

Feature ID	Description
1164734	Enhances RSPAN and ERSPAN configuration by allowing settings to be applied at the individual FortiSwitch stack level instead of all switches under a FortiLink interface. This provides more granular traffic monitoring control and greater deployment flexibility.

Feature ID	Description
1295481	Multicast packets are now forwarded to the incoming interface when switch-controller-access-vlan (intra-VLAN blocking) is enabled on that interface and a matching multicast policy exists. This allows multicast applications to keep working for clients on the same access VLAN without disabling intra-VLAN blocking

Log & Report

See Logging in the New Features Guide for more information.

Feature ID	Description
1301863	FortiGate generates new system event logs that record device-level and account-level contract and license changes. These logs provide visibility into contract state changes that determine a FortiGate's eligibility for automatic upgrades.

Policy & Objects

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

Feature ID	Description
1298417	Adds support for the match-vip option in deny firewall policies within hyperscale VDOM. This enhancement ensures VIP traffic is correctly matched and blocked after DNAT, improving policy enforcement consistency.

Security Profiles

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

Feature ID	Description
1270148	The signature hold timer, previously available for IPS signatures only, now extends to Application Control signatures. When a new application signature arrives in an APDB package update, FortiGate places it on hold for the configured period instead of applying it immediately. This gives administrators a window to review newly added application signatures before they can affect production traffic.

System

See System in the New Features Guide for more information.

Feature ID	Description
1299497	Automation email notifications now use enhanced email templates by default for improved readability. The updated notifications replace plain-text formatting, remove raw log content from messages, and include additional event information where applicable.
1321435	The FortiGate now exposes per-tunnel, per-traffic-class egress shaping statistics for IPsec VPN tunnels through SNMP. Administrators can poll the new `fgVpn2TunShapingTable` MIB table to monitor the guaranteed, maximum, and current bandwidth, transmitted bytes, dropped packets and dropped bytes for each traffic class on each IPsec tunnel.

Upgrade information

Supported upgrade path information is available through the Upgrade Path Tool on the Fortinet Document Library.

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 23 and Upgrading all devices in the FortiOS Administration Guide.

To view supported upgrade path information:

1. Go to the Fortinet Document Library at https://docs.fortinet.com/product/fortigate.
2. From the right side-bar, go to *Tools & Resources* and select *Upgrade Path Tool*.
3. Check that *Choose a product* is *FortiGate / FortiOS*.
4. In the *Product Model* list, select your model.
5. In the *Current Version* list, select the FortiOS version you are currently running.
6. In the *Target Upgrade Version* list, select the target FortiOS version for the upgrade.
7. Click *Go* to view the upgrade path.

Fortinet Security Fabric upgrade

FortiOS 7.6.8 is verified to work with these Fortinet products. This includes:

FortiAnalyzer	• 7.6.8
FortiManager	• 7.6.8
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 7.6.8. When Security Fabric is enabled in FortiOS 7.6.8, all FortiGate devices must be running FortiOS 7.6.8.

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

To make sure a FortiGate 6000 or 7000 firmware upgrade is successful, before starting the upgrade, Fortinet recommends you use health checking to make sure the FIMs and FPMs are all synchronized and operating as expected.

If you are following a multi-step upgrade path, you should re-do health checking after each upgrade step to make sure all components are synchronized before the next step.

You should also perform a final round of health checking after the firmware upgrade process is complete.

For recommended health checking commands, see the Fortinet community article: Technical Tip: FortiGate-6000/7000 Chassis health check commands.

Both management boards and all of the FPCs in a FortiGate 6000 FGCP HA cluster run the same firmware image. You upgrade the firmware from the primary FortiGate 6000 management board. The firmware image is copied to the FPCs and all components upgrade at the same time.

All of the FIMs and FPMs in a FortiGate 7000 FGCP HA cluster also run the same firmware image. You upgrade the firmware from the primary FIM in the primary FortiGate 7000. The firmware image is copied to the secondary FIM and the FPMs and all components upgrade at the same time.

A graceful firmware upgrade of a FortiGate 6000 or 7000 FGCP cluster only causes minimal traffic interruption. Use the following command to enable graceful upgrade.

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

The `uninterruptible` option is enabled by default. To improve session synchronization during a graceful upgrade, you can also enable `session-pickup`:

```
config system ha
   set session-pickup enable
end
```



For the FortiGate 7000F platform, enabling session pickup requires using the `session-sync-dev` option to select one or more interfaces to use for session synchronization. The recommended session synchronization configuration is to add two 100Gbps FIM management interfaces to a LAG and configure the HA `session-sync-dev` option to use this LAG for session synchronization. The recommended interfaces to use for this LAG are the M1 interface of the FIM in slot 1 and the M1 interface of the FIM in slot 2. You should use a switch to connect the LAGs in the two chassis. To support graceful upgrade with session synchronization:

```
config system ha
   set upgrade-mode uninterruptible
   set session-syn-dev <lag>
   set session-pickup enable
end
```

During a graceful firmware upgrade the secondary FortiGate 6000 or 7000 upgrades its firmware first, traffic then fails over to the secondary FortiGate 6000 or 7000 and then the primary FortiGate 6000 or 7000 firmware is upgraded. 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 `upgrade-mode` to `simultaneous`, 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.

Normally, you would want to set `upgrade-mode` to `uninterruptible` to minimize traffic interruptions. If a traffic interruption is not going to cause any problems, you can set `upgrade-mode` to `simultaneous` so that the firmware upgrade process takes less time.

As well, some firmware upgrades may not support setting `upgrade-mode` to `uninterruptible`. Make sure to review the release notes before running a firmware upgrade to verify whether or not setting `upgrade-mode` to `uninterruptible` is supported to upgrade to that version.

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

Due to `1000auto` speed setting removal on FortiGate 1000F/1001F in FortiOS 7.6.1, upgrade from previous version may result in interface down because speed setting changed to `10000full` on SFP+ interface, which previously used speed `1000auto`. Administrators may need to manually change speed setting to `1000full` to restore the connection.

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 7.6.8 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 0335 and later (needed for FSSO agent support OU in group filters)
	  • Windows Server 2025 Standard
	  • Windows Server 2025 Datacenter
	  • Windows Server 2025 Core
	  • 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	• 7.00062
IPS Engine	• 7.01200

See also:

- Virtualization environments on page 31
- Language support on page 31
- Agentless VPN support on page 32
- FortiExtender modem firmware compatibility on page 32

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, 8.0, and 9.0.

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
FEV-211F_AM	FEM_12_EM7511-22-1-2-AMERICA	FEM_12_EM7511-22.1.2-build0001-AMERICA.out	America

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

AntiVirus

Bug ID	Description
1256662	Internal 500 error occurs when AV profile is enabled in the firewall policy after AV engine update
1277694	Scanunit workers generate 500 Internal Error when they run out of file descriptors.
1307986	Server response is sent to FSA for scanning when FortiGate has FSA inline scanning enabled and client performs an HTTP POST to upload a file.
1319493	Resubmission of unclaimed scan requests drops HTTPS traffic.

Application Control

Bug ID	Description
1285724	Inconsistency in Risk Score Display occurs when using CLI and GUI on FortiGate

Data Leak Prevention

Bug ID	Description
1276142	Failure to fetch MPIP labels from Microsoft Pureview occurs when FortiGate is configured with sdn-connector
1301589	DLP fails to filter documents when the MIP label is located in an ole xml stream or an unencrypted msofficex file.

DNS Filter

Bug ID	Description
1243152	Incorrect client and server cookies are returned for cached DNS entries when conditional forwarding with EDNS cookies is configured
1254420	High CPU usage occurs in dnsproxy when handling DNS requests for IPv6-only domains.
1265529	Wildcard FQDNs starting with '*.' do not match base domains when learning resolved IPs from DNS queries.
1295373	SRV records are redirected to the mgmt interface instead of the VWP interface when a DNS filter profile is applied in the policy
1313580	Error condition in dnsproxy occurs when allocating DNS relay connections

Endpoint Control

Bug ID	Description
1226271	Memory usage issues caused by EMS endpoint requesting many client avatar entries.
1299308	ZTNA destinations are blocked with Implicit Deny when the FortiGate loses connection with the EMS server due to SSL verification failure.

Explicit Proxy

Bug ID	Description
1135770	Group query fails to match for some users after upgrade when using LDAP server authentication with recursive group search enabled in explicit proxy.
1253730	Intermittent HTTPS request timeouts occur when proxy-based UTM inspection is enabled on a Virtual Server VIP.
1291974	Error condition occurs when FortiGate is configured with explicit web proxy and forwarding server using FQDN that resolves to both IPv4 and IPv6 addresses without an IPv6 interface
1292536	PAC file data is cleared when deleting a VDOM named 'root'
1298780	SSL websites fail to load in Firefox when FortiGate restarts

Bug ID	Description
1305730	Explicit proxy policy matches IPv4 destination when configured with IPv6 FQDN object and DNS server resolves only to an A record
1308272	Applying an IPS or AppCtrl Profile to a Proxy-Policy drops WebSocket tunnels.
1311271	Explicit or web proxy policies stop WAD from responding when a request attached to a 1way origin server is answered locally.

Firewall

Bug ID	Description
1134818	Intermittent issues occur with SCTP COOKIE packets on FortiGate 1800F when virtual wire pair is configured under fiber interfaces.
1212625	Fragmented packets are dropped when egress shaping-profile is configured on a VLAN interface
1222166	Traffic shaping fails when SD-WAN load balancing is enabled after reboot.
1225460	Traffic offload failure occurs when using back-to-back EMAC VLAN interfaces for inter-VDOM traffic
1232145	Traffic is blocked when auto-asic-offload is enabled on firewall policy with back-to-back EMAC VLAN and Inter-VDOM Link topology.
1234453	VXLAN traffic fails when offloading is enabled
1236578	SCTP COOKIE-ECHO packets are dropped when ASIC offloading is disabled on FortiGate.
1238766	SCTP traffic forwarding issue occurs when using the hardware switch on FortiGate-80F
1258998	Packets do not match firewall policies when dynamic address contains non-standard dotted IP address after upgrade
1270066	Shaping statistics unavailable when UTM is enabled in policy on SOC5 platform
1270575	Traffic fragmentation issues occur when passing through multiple VDOMs on FortiGate
1275753	Traffic is allowed by incorrect firewall policy when NAT64 rules are evaluated incorrectly with multiple policies configured.
1279396	TLS_AES_256_GCM_SHA384 cipher suite is not advertised when using an EC384 certificate on a VIP
1280020	COS marking is removed when traffic is accelerated over a hardware switch
1280836	Installation failure occurs when setting a large number of address objects in firewall policy
1283427	Traffic disruption occurs when offloading is enabled in the firewall policy
1286869	Session offloading fails when sflow configuration is removed

Bug ID	Description
1292043	Session count increase occurs when asymmetric ECMP return traffic is combined with auxiliary-session handling after upgrading the connected router.
1295481	Multicast packets are forwarded to the incoming interface when switch-controller-access-vlan is enabled on that interface.
1299325	A reboot resets diffservcode values to 00000 when diffservcode-rev 000011 and diffservcode-forward are set in a firewall policy.
1307143	Traffic is incorrectly shaped when memory optimization settings are applied.
1308113	An error condition occurs in the SSL configuration when setting ssl-server-algorithm custom twice with ssl-server-min-version set to client
1308123	PRP/MMS/SNMP packets are blocked when PRP NPU attributes are enabled for a transparent vdom on FortiGate Rugged 70F
1314398	DFR reassembly drops GTP session packets when an out-of-order small fragment arrives first on NP7 models.
1314405	Fragmentation drops COS marking on outgoing packets.
1316379	Configuring 221 or more srcaddr objects in a local-in policy causes FortiGate to reboot unexpectedly.

FortiGate 6000/7000 Platform

Bug ID	Description
1241479	IVS related DCE counters do not work as expected on SoC5 platforms.
1275854	Merge occurs when FortiGate-400G and 401G models are integrated into FortiOS 7.x
1280968	IGMP join issues occur on interfaces configured in virtual switch on FortiGate.
1283535	fragmented IKE packet drop
1307574	License sync issue occurs when VDOM license is added to the FIM through the GUI
1310503	An FPM with Fabric and Base links DOWN to the secondary FIM on SLBC platforms fails to trigger HA failover.
1314590	FGCP HA is not supported for HA between an AC powered and a DC powered FortiGate 6000F or FortiGate 7000F chassis. This issue has been resolved for FortiOS 7.4.13, 7.6.8, and 8.0.1 for the FortiGate 7000F only.
1339747	Multihop BFD remains DOWN on SLBC platforms

FortiView

Bug ID	Description
1158855	An error condition in FortiGate occurs when generating a query after using the Fortinet Support Tool for GUI capture.

GUI

Bug ID	Description
1145907	The bandwidth widget reports traffic incorrectly on a backup VLAN interface on FortiGate NP6 platform models when fast-path processing is disabled.
1212624	Memory usage issues caused by the V8 JavaScript engine
1223774	Firewall policy GUI page shows 'no-inspection' for SSL when profile group is applied.
1225806	Memory usage issues caused by V8 ExternalPointerTable leak
1229180	Unknown status occurs when loading config with 9k+ tunnels across VDOMs
1249651	No interface bandwidth is displayed when traffic passes through virtual-switch interfaces
1255792	Failed to add logs sent occurs when adding Logs sent widget to dashboard
1260292	Print button is not visible when using prof_admin profile after FortiOS upgrade
1261462	Error saving request object to CLI occurs when editing copied ISDB policies with FQDN address in destination
1262347	Multiple clicks are required to configure wildcard URL filters from the GUI
1264166	GUI CLI console generates "Connection lost. Press Enter to start a new session." under FIPS-CC mode.
1274994	Duplicate policy entry occurs when numerous policies are configured with implicit policy enabled
1276291	Firewall Users Method and User Group graph disappears when using FortiGate v7.4.11
1277951	Packet capture file download fails when session ID exceeds the maximum value.
1278004	Having 5500 security policies causes the Security Policy page to stop responding.
1278206	HTTPS GUI access fails when using a Low Encryption license after upgrading to FortiOS 7.4.11
1280043	FortiGate GUI hides srcaddr6 and dstaddr6 fields when nat46 is enabled.
1292309	Slow scrolling occurs on the policy page with a large number of policies
1300025	Admin session termination occurs when using Chrome or Edge browsers for login.

Bug ID	Description
1301041	An error condition in httpsd occurs when serving error responses through Apache ErrorDocument sub-requests
1304918	Automation Stitch edit page displays the wrong HA cluster destination in a CSF fabric with multiple FortiGate HA clusters.
1307573	Multiple categories appear for the same user group in Sequence Grouping View after upgrading to FortiOS 7.6.7
1309154	Configuring HA-Direct while a source-ip is set for FortiAnalyzer causes the FortiGate GUI to display the FortiAnalyzer status as down.
1312045	FortiSwitch Ports search generates ERR_HTTP2_SERVER_REFUSED_STREAM and disconnects the GUI user.
1317062	Hit count is not visible in the GUI for SNAT policies when Central SNAT is configured
1320690	The GUI hides the dedicated management interface when configured in dedicated-mgmt.
1321675	The GUI hides FortiLink VLANs from non-root VDOMs when searching for VLANs while configuring FortiSwitch ports.

HA

Bug ID	Description
1235434	Asymmetric traffic occurs when UDP session syncing fails between FGSP peers.
1249067	The ip_session_tree_walker() function unnecessarily traverses a session's siblings and parent's siblings when the session lacks a child session.
1258325	FortiToken Mobile push fails when private-data-encryption is enabled after a full HA cluster shutdown
1265113	Return traffic occurs when virtual cluster failover happens
1267616	FGSP session synchronization issues occur when FGSP links experience high latency.
1268268	DHCP server offers use physical MAC instead of VMAC when HA is formed after reboot or upgrade
1270605	HA cluster sync fails when adding a new VDOM in HA primary
1271356	Link down condition occurs on FortiGate 4801F when media type is set to SR and forward error correction is set to CL74-FC-FEC at 25G speed
1271911	Virtual MAC address is not set correctly when override-wait-time is enabled and secondary device is configured before timeout.
1275263	An error condition occurs in FGSP cluster when adding new nodes.

Bug ID	Description
1285215	TCP/135 traffic fails when DCE-RPC session helper is enabled with asymmetric traffic in FGSP-transparent mode
1290957	HA synchronization fails when FIPS-CC mode is enabled
1292621	A SCIM database exceeding 16MB leaves HA out of sync across secondary nodes.
1293476	BFD flaps occur when there is a FGCP or FGSP failover
1294432	HA synchronization issue occurs when running auto-script to modify SDWAN member order in SDWAN rule
1296191	HA failover occurs twice within the same second when a secondary unit leaves the cluster with override disabled.
1296784	Session synchronization issues occur when FGSP is configured over FGCP cluster environment.
1298467	High CPU consumption occurs when policy package is pushed from FortiManager
1306225	FortiGate sends only one cluster member detail during authentication to FIC when configured in an HA cluster.
1309304	Adding, removing, or renaming a FortiSwitch leaves the HA cluster out of sync.
1311587	HA cluster synchronization issues occur when private-data-encryption is enabled
1317118	Adding a switch leaves the HA configuration out of sync because the event triggers a CMDB update only on the primary unit.
1323497	An IKE NAT port change blocks traffic after HA failover.

HyperScale

Bug ID	Description
1285581	A performance drop may occur on specific FortiGate model when processing TCP PBA NAT-overload and HTTP CPS traffic
1288505	Traffic disruption occurs when session sync between FGCP peers uses layer2 RLT packet
1290329	Packet loopback occurs when flapping a member of a LAG as hardware session sync device
1295024	FGT 4201F B3688 has increase in performance by ~100% for CPS PBA eimoff eifoff log2host

Intrusion Prevention

Bug ID	Description
1049160	IPSA self test failure occurs when upgrading to FortiOS 7.6.0 build 3388 with debug image.
1123425	OT signatures are not displayed after FortiGate reboot
1267456	A ClientHello packet larger than the MSS generates an SSL error when retransmitted to the server.
1301803	High memory usage occurs when running IPS engine version 8.0.34
1304696	HTTP2 traffic consumes excessive memory and leaves FortiGate in conserve mode.
1328188	Certificate inspection blocks TLS 1.0 connections when IPS engine is updated to 7.01196.
1328306	Local-in Virtual Patch fails to inspect traffic when using the HA-MGMT interface.

IPsec VPN

Bug ID	Description
1073893	When a large TCP packet enters an IPsec tunnel, the FortiGate no longer adjusts the TCP MSS value automatically. Instead, it sends an ICMP message (ICMP_FRAG_NEEDED) to notify the sender of the correct MTU size. The sender can then adjust the TCP MSS and subsequent packet sizes accordingly.
1113625	Traffic disruption occurs when FortiExtender or LAN Extension sessions are offloaded on the FortiGate side.
1129023	FCT IKE2 dialup VPN bypasses 2FA authentication when the user group includes a RADIUS server member.
1201323	The copy-dscp feature drops traffic with an original IPv4 checksum of 0xffff on NP7 models.
1212605	Error condition in IKE daemon occurs when changing dh-mode from hardware to software
1215507	IPsec tunnel disruption occurs when changing IP pool on the router
1222252	VLAN CoS marking fails when traffic goes through an IPSec tunnel
1236634	Renewing expired certificates in ipsec.phase1-interface causes iked to restart unexpectedly.
1243205	High CPU softirq usage occurs when using EMAC-VLAN interface with IPsec VPN on SoC5 platforms.
1246587	Traffic forwarding issues occur when NPU offload is enabled for IPSEC VPN
1254266	IPsec dial-up VPN connection fails when username case sensitivity does not match for RADIUS users.

Bug ID	Description
1272584	IPv4 multicast traffic over IPsec fails on FortiGate-6501F when configured on v8.0.0 and v7.6.7.
1273353	VPN tunnels experience intermittent disruption when IPSec VPN server certificates are renewed via SCEP
1273969	High memory usage occurs when VWL triggers shortcut-offer for existing shortcut tunnels in SD-WAN ADVPN deployment on FortiGate-40F and FortiGate-60F.
1283050	An error condition in IKE daemon occurs when using DDNS with specific network conditions.
1293470	Data transmission issues occur in IPsec VPN tunnels when npu-offload is enabled on FortiGate.
1295501	An error condition in the application occurs when High Availability is enabled on FortiGate devices configured with FIPS-CC mode
1304588	Intermediate CA is not sent in certificate payload for IKEv2 signature-based authentication when send-cert-chain is enabled on phase 1 settings.
1311512	An error condition occurs in IKEv1 when setting negotiate-timeout to 15 or lower.
1318272	Enabling system.settings.ike-policy-route after IPsec tunnel configuration blocks ESP traffic from reaching the egress interface.
1321797	PPTP connection failure occurs when Compression Control Protocol negotiation happens on FortiGate 120G
1328024	Tunnel gateway switching leaves the negotiation timeout outdated, which expires the tunnel negotiation before 2FA completes.

Log and Report

Bug ID	Description
1249376	Unknown app and appcat fields occur when updating APDB from built-in version to 35.00157
1249778	VPN XAuth user information is missing from the FortiGate Daily Security Report after upgrading from v7.4.9 to v7.6.5
1269332	FortiGate loses FortiAnalyzer serial number during failover from primary to secondary FAZ
1281906	Traffic logs are generated when logging is disabled on proxy policies after upgrading to FortiOS 7.6.6
1294193	Memory usage issues caused by logging connection disruptions to FortiAnalyzer
1316969	Disk log cleanup deletes IPS PCAP archives when other UTM log categories are missing log files for the same roll number.
1321626	Concurrent DNS queries for the same FQDN generate "fgfm connection to device is down" logs without corresponding connection up logs.

Proxy

Bug ID	Description
1224454	SSL deep inspection blocks or bypasses traffic when the first ClientHello TCP segment payload is 1024B or less.
1228854	HTTP status code 302 is not forwarded to the client when ssl-http-location-conversion is enabled
1244955	An error condition occurs in WAD during peer port validation.
1252579	High CPU usage occurs when proxy-based inspection mode is enabled and udp-not-quic traffic is allowed
1257499	Protocol switching web traffic based on HTTP and HTTPS may get blocked when the profile-protocol-options websocket status is disabled.
1269317	An error condition in WAD occurs when upgrading FortiGate VM to FortiOS 7.6.6
1276917	Phantom UDP/443 traffic occurs when UDP/443 traffic is redirected to WAD for QUIC handling and the packet is not QUIC on FortiGate 120G.
1280944	Traffic is blocked when the unsupported-ssl-version allow setting is enabled and the min-allowed-ssl-version is set to TLS 1.1
1285189	Incomplete certificate chain is sent when FortiGate performs SSL inspection in proxy mode
1297169	Memory usage issues caused by proxy-inline-ips being enabled
1303431	An error condition in WAD occurs when validating certificates after upgrade from v7.6.6 to v7.6.7
1305726	TLS handshake failure occurs when TLS-AES-256-GCM-SHA384 is the only configured SSL cipher suite
1307625	Proxy-based mode in VWP policy slows website loading when NPU is enabled.
1323515	An FSSO identity lookup that returns no user and matches no proxy-policy stops WAD from responding.

REST API

Bug ID	Description
1265839	Group Filter functionality is impacted when a large number of users are authenticated.
1314746	REST API JSON filtering of policy and address-group lists drops entries or displays incorrect results.

Routing

Bug ID	Description
1217353	BFD session failure occurs when using a loopback interface as a BGP neighbor
1260891	BFD packet transmission issues occur when a port member of the aggregate interface is shut down and then brought back up on the switch side.
1267696	BGP network advertisement fails when AS is changed
1277718	Routing tables are incorrectly assigned to VRF 0 when restoring VDOM configuration
1278445	Intermittent BGP disruption occurs when IPsec SA negotiation fails during AUTH exchanges between two spokes.

SD-WAN

Bug ID	Description
1185318	Speed-test results are not synchronized to secondary HA devices when acting as a speed-test server
1264814	Longer outage duration occurs when SD-WAN changes a VPN tunnel's priority
1273960	Packet loss occurs when upgrading from 7.0.14 to 7.2.10
1281211	Traffic disruption occurs when SD-WAN has 'embed-measured health' enabled on the spoke
1291673	Shortcut flapping occurs when traffic degradation happens on SD-WAN with ADVPN

Security Fabric

Bug ID	Description
1050209	Duplicate security rating entries occur when adding a VDOM
1210303	APIC device overload occurs when FortiGate logs in multiple times without proper logout.
1269373	High CPU usage occurs when SFTP backup automation is configured on the FortiGate
1277653	An error condition in csfd occurs when shared memory allocation fails.
1296597	An error condition in Autod occurs when deleting deprecated triggers during upgrade to 7.4.12
1301642	An error condition in Autod occurs when using email automation-action

Bug ID	Description
1309335	Duplicate empty VNet objects occur when Azure API returns VNet ID in all lower-case characters

SSL-VPN

Bug ID	Description
1272872	WAD blocks file uploads to an SSL VPN web app when SSL VPN traffic is processed by WAD.
1309910	Security vulnerability occurs when connecting to a malicious SSH server with crafted packets.
1317069	Agentless VPN SAML login fails when using a global-range SP certificate.

Switch Controller

Bug ID	Description
1215775	Communication to management IP fails when a VLAN interface is assigned to a hardware switch in transparent mode
1250878	Traffic mirroring issues occur when SPAN is enabled with hardware switch on FortiGate-60F
1275148	Allowed VLANs are deleted when adding new allowed VLANs on a trunk port.
1290927	Enabling stpforward on a hardware switch causes a network loop on SoC5 platforms.
1293984	FortiSwitch topology hides MCLAG ICL link.
1296864	Sync loss with FortiSwitch occurs when the default admin account is removed
1308243	Security group name changes to 'SSo_Guest_Users' when renaming the user group on FortiGate
1312267	Custom 802.1X security policy cannot be added to pre-provisioned FortiSwitch when authserver-timeout-vlan is enabled
1312703	FortiGate removes RADIUS configuration from a FortiSwitch when the switch is associated with another VDOM as a virtual switch during a reboot.

System

Bug ID	Description
953547	SCTP traffic does not get forwarded by a connected hardware switch on FortiGate.
1114381	FortiGate 40x/60xF: Packet loss occurs when congestion happens on FortiGate interfaces
1153804	Inconsistent interface IP addresses occur when configuring IP and secondary IP on an interface
1161211	Memory usage issues caused by polling FGT memory usage
1168786	100G ports turn up after reboot when administratively down on platforms with Marvell switch like FortiGate 480xF.
1193085	Proxy-arp configuration failure occurs when the proxy-arp address group exceeds 256 entries
1222654	FortiGate-40F fails to display LAN A SPEED and WAN SPEED amber LEDs during the diag hardware test led nic-led.
1229444	TX counters are not displayed for EMAC VLAN interfaces when non-offloaded traffic is present
1238946	DHCPv6 address allocation issues occur when Router Advertisement messages contain multiple unicast addresses.
1241782	An error condition in icond occurs when enabled on FortiGate Rugged-70G
1245329	Configuration loss occurs when FortiGate enters extreme low memory mode
1261417	An error condition in cmdbsvr occurs when OpenSSL cleans up resources.
1262639	Bandwidth distribution issue occurs when using LACP after upgrade to 7.4
1265816	SPEED LED blinking occurs when upgrading to FortiOS 7.4.10 on FortiGate FG-40F
1268808	Packet drops occur when querying SNMP OID 1.3.6.1.4.1.12356.101.4.4.2.1.8 for Processor 13
1271259	Transceiver issue occurs when using FR-1 QSFP 100G with FortiGate
1273362	Port LEDs remain solid green when transmitting or receiving data on FortiGate 80F after upgrade to 7.4.11
1275047	Port LEDs fail to illuminate when connected at 100Mbps with auto speed setting
1275741	Memory usage issues caused by np6 ring buffer filling up
1277460	Speed setting changes to 10000auto when FortiGate-1000F is rebooted after configuring speed auto on port3
1281707	Unexpected behavior in reportd and cmdbsvr causes device reboot.
1289434	LED activity lights do not blink when FortiGate is upgraded to version 7.4.x
1290014	Moving a VM from the root ADOM to customer ADOM fails when changing the vdom-type to admin
1290942	FortiGate-70G, FortiGate-71G, FortiWiFi-70G, and FortiWiFi-71G WAN interface SPEED LED remains lit after reboot when configured as admin-down with no Ethernet cable connected.

Bug ID	Description
1293990	Incorrect IPv6 SNMP interface counters occur when sessions are processed by the CPU.
1294887	LLDP transmission issue occurs when LLDP-MED inventory software revision value exceeds 32 characters
1295619	MTU size changes on WWAN interfaces are not applied when MTU override is enabled on FortiGate 5G models
1301576	High CPU utilization occurs when forticldd process experiences unlimited retries with no delay after a tcps read fails.
1304395	Traffic drop occurs when one member of an aggregate interface goes down in active mode
1304523	Traffic drop occurs when one LACP member link goes down
1304527	FortiASIC EEI Test generates "ASIC number not correct: expected 2, got 1" on FortiGate-900G, FortiGate-901G, and FortiGate-3700F/3701F.
1304601	Traffic drop occurs when one member of an aggregate interface goes down
1307500	TX packet and byte counters increase when unused ports are in a link down state
1308703	Third-party CAPWAP fragments are dropped when they pass through NP7 or NP7Lite FortiGate.
1309281	Third-party CAPWAP fragments are dropped when they pass through NP7 or NP7Lite FortiGate.
1312694	A factoryreset script generates "[FORTISM Violation" messages in the crashlog.
1314361	Wake-on-LAN packets are dropped by SOC5 families due to an incorrect checksum.
1314404	UWDB delta updates fail when delta update files contain only the header with no body.
1316514	IPGO delta update generates "Failed to bspatch /tmp/delta/upd.0.delta, code=65280" during a delta update.
1324928	Off-network .lic files generated on Windows generate "FortiGate Manual License is invalid" during manual license upload via TFTP.

Upgrade

Bug ID	Description
1259436	FortiGate-30G fails to restore image upgrade when IMAGE_SIGNATURE_CMS is missing on 3xG platforms.
1269764	Private data encryption wipes IPsec PSKs on platforms with TPM during upgrade from FortiOS 7.2.13 to 7.4.11.
1270824	Firmware upgrade issues occur when upgrading 648FF via FortiGate GUI

Bug ID	Description
1271250	A forced automatic firmware upgrade occurs when a valid FMWR license is in place and the device is not at EOES in an HA setup.
1277454	Upgrading from 7.6.6 to 7.6.7 may result in the loss of specific `config system global` settings (e.g., hostname, timezone, admin-scp, vdom-mode).
1283493	Firmware image transfer delays occur when high latency is present across regions.
1283569	FGT force-upg is not automatically cancelled after manually upgrading to a new major.minior
1297497	FortiGate-30G, FortiGate-31G, FWF-30G, and FWF-31G fail to restore firmware images via the execute restore image url command due to a signature verification error.

User and Authentication

Bug ID	Description
1144487	CPU usage issues observed during high load on fnbamd
1186128	Certificate enrollment fails when SCEP server requires HTTP POST
1210840	Client certificate request occurs when client-identity-check is disabled
1249801	Certificate renewal fails when ike-tcp-service is enabled on the same interface as ACME
1258884	Password expiry override does not work when configured with unset password-expire
1263909	Certificate enrollment and renewal fails when FortiGate uses HTTP GET instead of HTTP POST for SCEP requests
1271821	Token verification fails when username case sensitivity does not match for LDAP users with 2FA enabled.
1279114	Certificate renewal issues occur with EST when source-ip is enabled
1283430	Firewall auth list is flushed when DHCP client renews its lease
1286569	Authentication failure occurs when primary Radius server connection fails
1286748	A corrupted or missing SCIM database generates "totalResults": -1 in the ListResponse.
1287880	Entra ID generates a timeout error during SCIM provisioning when adding a user to an existing group.
1301025	SSO failure occurs when FortiGate acts as the IdP
1302924	Executing "execute vpn certificate local generate" as a FortiManager script with HA enabled generates an invalid certificate.
1304425	An expired or revoked certificate in the certificate chain consumes CPU on FortiGate.
1310424	EAP authentication fails when a SCIM-type group is configured in a firewall policy

Bug ID	Description
1322127	A SAML response larger than 16KiB blocks SAML SSO login on FortiGate.
1325322	Changing authentication configuration during a SAML authentication loop stops WAD from responding.

VM

Bug ID	Description
1188422	FFW_VM License validation fails when FortiManager is configured as a license server
1282482	Hardware checksum failure occurs when Confidential VM and gvnic features are enabled on GCP VMs
1294311	SDN connector fails to manage Azure vWAN when deployed in GermanyWestCentral location
1303540	Secondary private IP fails to move during HA failover when using OCI SDN Connector with HA support enabled on FortiOS 7.6.7
1306348	LAG creation fails when setting the MAC address on FortiGate-VM with SRIOV interfaces
1311756	Instance token refresh fails when certificate file size exceeds the fixed buffer size in FortiGate VM.
1318073	Azure SDN connector fails to initiate API calls to management.azure.com during HA failover when the connector has not finished initialization.
1323635	Secondary FortiGate fails to validate VM License with FGD when validation with FortiManager fails on VM platforms.
1324904	Live Migration on Azure VMs wipes RPS settings in config system affinity-packet-redistribution.

VoIP

Bug ID	Description
1258856	SIP ALG fails to sync SIP sessions between FGSP peers when UDP asymmetric traffic passes through without session-sync-dev configured.
1276335	Memory usage issues caused by voipd daemon with TCP socket connections

Web Filter

Bug ID	Description
1300576	FortiGate 121G displays an incorrect webfilter.profile tablesize of 32 instead of 512.

WiFi Controller

Bug ID	Description
1086302	Random users may experience unexpected authentication loss caused by IP address reassignment clearing active sessions for other stations.
1093829	WiFi Channels may appear empty in the FAP K-series profile for Taiwan on the 6GHz radio (Radio2) when the channel bandwidth is set to 320MHz(Wi-Fi 7 channel).
1221706	Captive-portal VAP configuration not syncing to Secondary Firewall
1242199	SSID interface is missing in routing table after FMG pushed the configuration to FGT
1254592	An error condition in hostapd occurs when using FQDN radius server with a large setup
1267078	Wifi client moves to another FAP and needs authentication again after authenticated via Cisco ISE
1287896	Status synchronization may fail between FortiGate and FortiAP when multicore processing is enabled.
1301027	FAP unable to Register to FGT on VPNv4/VRF segment
1303265	Communication failures occur between the firewall and access points during a failover event triggered by a hostapd process failure.
1306168	Enabling invalid-mac-oui in the WIDS profile consumes excessive cw_acd memory.
1320951	hard-timeout is not respected in the firewall auth session for radius wsso users flag(110)
1332657	CW_ACD Signal 11 crash on cwAcIotScanChk at capwap/ac/cwAcMisc.c when manage large number of FAP

ZTNA

Bug ID	Description
1225065	An error condition in WAD occurs when ZTNA policy rematch is triggered for existing sessions

Bug ID	Description
1300390	UUID becomes all-zero when FortiManager installs policy package with ZTNA EMS tag dynamic address objects on FortiGate
1302743	Load balancing info and preconnection-blob are not added to RDP packets when configuring ZTNA Web Portal with RDP Bookmarks.
1321696	ZTNA portal hides the Download FortiClient button when configuring ZTNA agentless web-based application access.

Known issues

Known issues are organized into the following categories:

- New known issues on page 53
- Existing known issues on page 53

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

New known issues

FortiGate 6000/7000 Platform

Bug ID	Description
1336373	7121F-2 (FIM-7941)/b0245: 100G FR transceiver link fails when RS-FEC is enabled on 1-P4, but works with FEC disabled

Existing known issues

The following issues have been identified in a previous version of FortiOS and remain in FortiOS 7.6.8.

Endpoint Control

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

Firewall

Bug ID	Description
959065	On the Policy & Objects > Traffic Shaping page, when deleting or creating a shaper, the counters for the other shapers are cleared.

Bug ID	Description
990528	When searching for an IP address on the Firewall Policy page, the search/filter functionality does not return the expected results.

FortiGate 6000/7000 Platform

Bug ID	Description
653335	SSLVPN 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.
1112582	Under some conditions, such as during conserve mode, you may not be able to log into the FortiGate 6000 management board GUI or CLI or when you log into the management board console a message similar to fork failed() continuously repeats.
1130491	Traffic disruption occurs when WCCP is enabled on FortiGate **Workaround**: Direct all related traffic to master FPC
1131269	UESP packet drop occurs when VPN peer uses different source ports for IKE-NATT and UESP **Workaround**: Add a flow rule to work around the issue
1132294	7KF/v7.6.3/b3490: ip nat port-preserve feature is not working when client's source port doesn't fall under FPM's nat port-range
1162187	7KF/b3617, FortiAP retains the same image after the upgrade
1171183	7KF-1/B3563: The Global Traffic widget do not loading after factory reset due to legacy auth disabled by default.

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
1237136	Dynamic VLANs are not visible on the GUI when a port-security-policy is applied

HA

Bug ID	Description
1135376	When HA members are not registered under the same FortiCare account, the HA cluster cannot obtain contract info of all members from FortiGuard servers.
1226122	System > HA: There is no "upgrade" button on secondary GUI page when HA in "local-only" or "secondary-only" MVC upgrade mode. **Workaround:** Upgrade the secondary via the command line.

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	4401f:Session-helper dns session is created by hw and can be seen in log2host table
1151441	4801F-HA) "ha1/ha2" port as hw-session-sync-dev shows out-of-sync even though it is connected to NP7
1245870	NPD-0 :was crashed when pol state PARSE with full-offload level when set SD-WAN interface
1262881	Hw session sync dev goes out of sync due to the discrepancy in lag driver between primary and secondary

Intrusion Prevention

Bug ID	Description
1076213	Fortigate with 4G memory might enter conserve mode during FortiGuard update when IPS or APP control is enabled. **Workaround**: Disable option 'proxy-inline-ips' under 'config ips settings'.
1093769	Unexpected IPS UTM logs may be generated in NGFW policy mode for unknown applications.

IPsec VPN

Bug ID	Description
1227338	IPsec VPN fails to use PPK when IKEV2 EAP is enabled

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
993345	The router API does not include all ECMP routes for SD-WAN included in the get router info routing-table command.

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 are offline after FGT upgraded from v7.4.6 or v7.6.0 to v7.6.1 or later when LLDP configuration set to vdom/disable under FortiLink interface. **Workaround**: Add LLDP configuration lldp-reception, lldp-transmission to enable under FortiLink interface, or rebuild FortiLink interface.
1172745	Timeout error occurs when running execute switch-controller diagnose-connection command

System

Bug ID	Description
1041726	Traffic flow speed is reduced or interrupted when the traffic shaper is enabled.
1142465	ARP entries age out quickly after a system reboot, despite a long reachable-time setting
1179259	TCP traffic is impacted over VXLAN when auto-asic-offload and UTM both enabled under the policy. **Workaround**: Disable auto-asic-offload on the impacted policy
1311807	Reachable value does not update after NTP recovery when NTP communication is restored

User and Authentication

Bug ID	Description
1082800	When performing LDAP user search from the GUI against a LDAP server with large number of users (more than 100K), the FortiGate may experience slowness and freeze due to HTTPSD process consumes too much memory. User may need to kill the HTTPSD process or perform a reboot to recover. **Workaround**: User can perform LDAP user search via the CLI.
1157003	Agentless FSSO connector issues occur when using Windows 2025 due to MS introduced additional restrictions to remote Event log reading.

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	The device encounters an issue where options in the ftgd-wf section cannot be unset when configuring a web filter via an Ansible playbook

Built-in AV Engine

AV Engine 7.00062 is released as the built-in AV Engine.

Resolved engine issues

Bug ID	Description
1003433	In a rare situation, the file filter may mistakenly classify PDF files as BAT files, leading to an undesired blockage of these files.

Built-in IPS Engine

IPS Engine 7.01200 is released as the built-in IPS Engine.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

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

Open source XenServer limitations

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



www.fortinet.com

Copyright© 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.