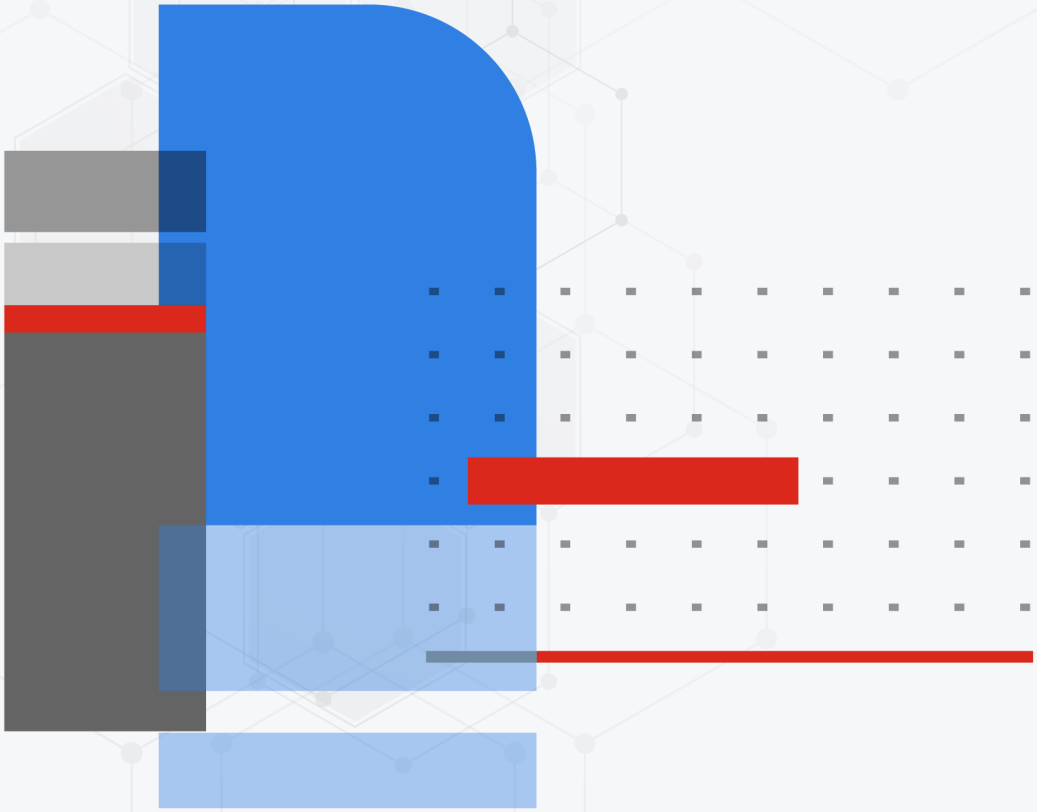
Release Notes

FortiOS 7.4.13



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 7.4.13 Release Notes

TABLE OF CONTENTS

Change Log **6**
Introduction and supported models **7**
Supported models 7
Special branch supported models 8
FortiGate 6000 and 7000 support 8
Special notices **9**
Hyperscale incompatibilities and limitations 9
FortiGate 6000 and 7000 incompatibilities and limitations 9
SMB drive mapping with ZTNA access proxy 9
Local out traffic using ECMP routes could use different port or route to server 10
Hyperscale NP7 hardware limitation 10
SAML certificate verification 10
Changes to NP7 traffic shaping 11
GUI cannot be accessed when using a server certificate with an RSA 1024 bit key 12
SSL VPN not supported on FortiGate G-series Entry-Level models 12
Policy check required for hairpin traffic 12
Changes in default behavior **13**
New features or enhancements **14**
Upgrade information **15**
Fortinet Security Fabric upgrade 15
Downgrading to previous firmware versions 17
Firmware image checksums 17
FortiGate 6000 and 7000 upgrade information 17
FortiGate 5001E primary blade failed to install image 19
IPS-based and voipd-based VoIP profiles 19
GUI firmware upgrade does not respect upgrade path in previous versions 20
2 GB RAM FortiGate models no longer support FortiOS proxy-related features 20
FortiGate VM memory and upgrade 21
Managed FortiSwitch do not permit empty passwords for administrator accounts 21
Policies that use an interface show missing or empty values after an upgrade 21
Statistics for traffic shaping using QTM 22
Loopback-based VIPs cannot pass traffic after upgrade 22
FIPS-CC mode no longer supports TACACS+ 22
Traffic loss during graceful upgrade on SLBC HA with override enable due to premature failover 23
Product integration and support **24**
Virtualization environments 25
Language support 25
SSL VPN support 26
SSL VPN web mode 26
FortiExtender modem firmware compatibility 26

Resolved issues **29**
Data Leak Prevention 29
DNS Filter 29
Explicit Proxy 29
Firewall 30
FortiGate 6000/7000 Platform 30
GUI 31
HA 31
HyperScale 32
Intrusion Prevention 32
IPsec VPN 32
Log and Report 33
Proxy 33
Routing 34
SD-WAN 34
Security Fabric 34
SSL-VPN 34
Switch Controller 35
System 35
Upgrade 36
User and Authentication 37
VM 37
Web Filter 37
WiFi Controller 38
Common Vulnerabilities and Exposures 38
Known issues **39**
New known issues 39
Existing known issues 39
Explicit Proxy 39
Firewall 40
FortiGate 6000/7000 Platform 40
FortiView 41
GUI 41
HA 42
HyperScale 42
IPsec VPN 44
Proxy 44
REST API 44
Routing 45
Security Fabric 45
Switch Controller 45
System 45
Upgrade 46
User and Authentication 46
VM 47
WiFi Controller 47

ZTNA 48
Built-in AV Engine **49**
Resolved engine issues 49
Built-in IPS Engine **50**
Limitations **51**
Citrix XenServer limitations 51
Open source XenServer limitations 51
Limitations on HA cluster formation between different FortiGate Rugged 60F and 60F 3G4G models 51

Change Log

Date	Change Description
2026-10-22	Initial release.

CONFIDENTIAL

Introduction and supported models

This guide provides release information for FortiOS 7.4.13 build 2933.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.4.13 supports the following models.

FortiGate	FG-30G, FG-31G, FG-40F, FG-40F-3G4G, FG-50G, FG-50G-5G, FG-50G-DSL, FG-50G-SFP, FG-50G-SFP-POE, FG-51G, FG-51G-5G, FG-51G-SFP-POE, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-70F, FG-70G, FG-70G-POE, FG-71F, FG-71G, FG-71G-POE, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-DSL, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-90G, FG-91G, FG-100F, FG-101F, FG-120G, FG-121G, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-200G, 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-30G, FWF-31G, FWF-40F, FWF-40F-3G4G, FWF-50G, FWF-50G-5G, FWF-50G-DSL, FWF-50G-SFP, FWF-51G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-70G, FWF-71G, FWF-70G-POE, 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-70F-3G4G, FGR-70G, FGR-70G-5G-Dual
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

CONFIDENTIAL

Special branch supported models

The following models are released on a special branch of FortiOS 7.4.13. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 2933.

FGR-60G	is released on build 6929.
FGR-60G-5G	is released on build 6929.
FGR-60G-M12	is released on build 6929.
FGR-70G-5G	is released on build 6927.
FG-3800G	is released on build 6932.
FG-3801G	is released on build 6932.

FortiGate 6000 and 7000 support

FortiOS 7.4.13 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

CONFIDENTIAL

Special notices

- Hyperscale incompatibilities and limitations on page 9
- FortiGate 6000 and 7000 incompatibilities and limitations on page 9
- SMB drive mapping with ZTNA access proxy on page 9
- Local out traffic using ECMP routes could use different port or route to server on page 10
- Hyperscale NP7 hardware limitation on page 10
- SAML certificate verification on page 10
- Changes to NP7 traffic shaping on page 11
- GUI cannot be accessed when using a server certificate with an RSA 1024 bit key on page 12
- SSL VPN not supported on FortiGate G-series Entry-Level models on page 12
- Policy check required for hairpin traffic on page 12

Hyperscale incompatibilities and limitations

See Hyperscale firewall incompatibilities and limitations in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 7.4.13 features.

FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 7.4.13 features.

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

SMB drive mapping with ZTNA access proxy

In FortiOS 7.4.1 and later, SMB drive mapping on a Windows PC made through a ZTNA access proxy becomes inaccessible after the PC reboots when access proxy with TCP forwarding is configured as FQDN. When configured with an IP for SMB traffic, same issue is not observed.

CONFIDENTIAL

One way to solve the issue is to enter the credentials into Windows Credential Manager in the form of `domain\username`.

Another way to solve the issue is to leverage the KDC proxy to issue a TGT (Kerberos) ticket for the remote user. See ZTNA access proxy with KDC to access shared drives for more information. This way, there is no reply in Credential Manager anymore, and the user is authenticated against the DC.

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

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

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

Hyperscale NP7 hardware limitation

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

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

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:

CONFIDENTIAL

```
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 Identify Providers.

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.

CONFIDENTIAL

GUI cannot be accessed when using a server certificate with an RSA 1024 bit key

The GUI cannot be accessed when using an admin server certificate with an RSA 1024 bit key after upgrading to FortiOS 7.6.1, 7.4.8, or 7.2.11. An RSA key of at least 2048 bits is required. Certificates that are using an RSA key of less than 2048 bits are no longer supported.

SSL VPN not supported on FortiGate G-series Entry-Level models

The SSL VPN web and tunnel mode feature will not be available from the GUI or the CLI on the FortiGate G-Series Entry-Level models, including 50G, 70G, 90G and variants. Settings will not be upgraded from previous versions.

Consider migrating to using IPsec Dialup VPN for remote access. See FortiOS 7.4 SSL VPN to IPsec VPN migration.

Policy check required for hairpin traffic

In FortiOS 7.4.10, 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.

CONFIDENTIAL

Changes in default behavior

Bug ID	Description
1240706	In NGFW policy-based mode, traffic may be bypassed when the IPS engine is not running such as when FortiGate first boots up, the IPS engine is upgrading or when it is manually stopped with debug commands. Instead, NGFW policy mode VDOMs will now drop traffic when IPS sockets are not available.
1245249	Additional commands are allowed before device registration to accommodate users that require configuring the device for central management, ZTP and LTP. Commands added:

Command	Description
`config firewall policy`	Configure IPv4/IPv6 policies.
`config router setting`	Configure router settings.
`config router static`	Configure IPv4 static routing tables.
`config router static6`	Configure IPv6 static routing tables.
`config system admin`	Configure admin users.
`config system central-management`	Configure central management.
`config system dns`	Configure DNS.
`config system interface`	Configure interfaces.
`config system pppoe-interface`	Configure the PPPoE interfaces.
`config system settings`	Configure VDOM settings.

CONFIDENTIAL

New features or enhancements

More detailed information is available in the New Features Guide.

CONFIDENTIAL

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 15 and Upgrading Fabric or managed 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 7.4.13 greatly increases the interoperability between other Fortinet products. This includes:

FortiAnalyzer	• 7.4.10
FortiManager	• 7.4.10
FortiExtender	• 7.4.0 and later

CONFIDENTIAL

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

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

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



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

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

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

CONFIDENTIAL

17. FortiMonitor



If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.4.13. When Security Fabric is enabled in FortiOS 7.4.13, all FortiGate devices must be running FortiOS 7.4.13.

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.

CONFIDENTIAL

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
```

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.

CONFIDENTIAL

FortiGate 5001E primary blade failed to install image

SLBC FortiGate 5001E primary blade failed to install image, even though graceful-upgrade was disabled.

IPS-based and voipd-based VoIP profiles

In FortiOS 7.4.0 and later, the new IPS-based VoIP profile allows flow-based SIP to complement SIP ALG while working together. There are now two types of VoIP profiles that can be configured:

```
config voip profile
    edit <name>
        set feature-set {ips | voipd}
    next
end
```

A voipd-based VoIP profile is handled by the voipd daemon using SIP ALG inspection. This is renamed from proxy in previous FortiOS versions.

An ips-based VoIP profile is handled by the IPS daemon using flow-based SIP inspection. This is renamed from flow in previous FortiOS versions.

Both VoIP profile types can be configured at the same time on a firewall policy. For example:

```
config firewall policy
    edit 1
        set voip-profile "voip_sip_alg"
        set ips-voip-filter "voip_sip_ips"
    next
end
```

Where:

- `voip-profile` can select a `voip-profile` with `feature-set voipd`.
- `ips-voip-filter` can select a `voip-profile` with `feature-set ips`.

The VoIP profile selection within a firewall policy is restored to pre-7.0 behavior. The VoIP profile can be selected regardless of the inspection mode used in the firewall policy. The new `ips-voip-filter` setting allows users to select an IPS-based VoIP profile to apply flow-based SIP inspection, which can work concurrently with SIP ALG.

Upon upgrade, the `feature-set` setting of the `voip profile` determines whether the profile applied in the firewall policy is `voip-profile` or `ips-voip-filter`.

CONFIDENTIAL

Before upgrade	After upgrade
config voip profile edit "ips_voip_filter" set feature-set flow next edit "sip_alg_profile" set feature-set proxy next end config firewall policy edit 1 set voip-profile "ips_voip_filter" next edit 2 set voip-profile "sip_alg_profile" next end	config voip profile edit "ips_voip_filter" set feature-set ips next edit "sip_alg_profile" set feature-set voipd next end config firewall policy edit 1 set ips-voip-filter "ips_voip_filter" next edit 2 set voip-profile "sip_alg_profile" next end

GUI firmware upgrade does not respect upgrade path in previous versions

When performing a firmware upgrade from 7.4.0 - 7.4.3 that requires multiple version jumps, the *Follow upgrade path* option in the GUI does not respect the recommended upgrade path, and instead upgrades the firmware directly to the final version. This can result in unexpected configuration loss. To upgrade a device in the GUI, upgrade to each interim version in the upgrade path individually.

For example, when upgrading from 7.0.7 to 7.0.12 the recommended upgrade path is 7.0.7 -> 7.0.9 -> 7.0.11 -> 7.0.12. To ensure that there is no configuration loss, first upgrade to 7.0.9, then 7.0.11, and then 7.0.12.

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

As part of improvements to enhance performance and optimize memory usage on FortiGate models with 2 GB RAM or less, starting from version 7.4.4, FortiOS no longer supports proxy-related features.

This change impacts the FortiGate/FortiWiFi 40F, 50G, 60E, 60F, 80E, and 90E series devices, along with their variants, and the FortiGate-Rugged 60F (2 GB versions only). See Proxy-related features no longer supported on FortiGate 2 GB RAM models for more information.

CONFIDENTIAL

FortiGate VM memory and upgrade

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

Managed FortiSwitch do not permit empty passwords for administrator accounts

Starting from FortiOS version 7.4.6, 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 7.4.6 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.

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

If local-in policy used an interface in version 7.4.5 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 later.

This issue is resolved in FortiOS 7.4.8 with mantis 1104649.

After following the upgrade path to FortiOS 7.4.8, you must manually recreate these policies and assign them to the appropriate SD-WAN zone.

CONFIDENTIAL

Although not recommended, you can skip the upgrade path and upgrade directly to FortiOS 7.4.8, and the policies remain untouched. Skipping upgrade steps might cause devices to miss other important FortiOS checks and changes and is not recommended.

Statistics for traffic shaping using QTM

Statistics for traffic shaping using QTM, and the `egress-shaping-profile offload` command for SoC5, have been added.

Loopback-based VIPs cannot pass traffic after upgrade

For users upgrading from versions 7.4.5, 7.4.6, and 7.4.7 to version 7.4.8 or later and employing loopback-based VIPs (external IP = loopback IP + `extintf "any"`), the following policy adjustments are recommended to maintain uninterrupted traffic flow if not already configured:

1. Create an entry firewall policy:
   - From external interfaces (for example, `wan1`) to the loopback interface
2. Add an exit firewall policy:
   - From the loopback interface to real-server interfaces (for example, `port4`, `port5`)

See also Technical Tip: How to configure VIP with loopback on FortiOS 7.4.8.

FIPS-CC mode no longer supports TACACS+

Starting in FortiOS 7.4.8, TACACS+ is no longer supported in FIPS-CC mode.

Because the TACACS+ protocol is now 30 years old, it uses MD5 for encryption and is insecure. MD5 is not an approved FIPS cipher.

After upgrading to FortiOS 7.4.8 or later, use RADIUS or another authentication method instead of TACAS+. Please note that FortiOS 7.6.0 and later only supports RADIUS over TLS.

CONFIDENTIAL

Traffic loss during graceful upgrade on SLBC HA with override enable due to premature failover

During a graceful firmware upgrade on a FortiGate 6000/7000 Active-Passive HA cluster with HA override enable, traffic loss and session failures may occur when the original primary unit upgrades and reclaims the primary role before its internal modules (FPCs/FPMs) fully come online and synchronize.

CONFIDENTIAL

Product integration and support

The following table lists FortiOS 7.4.13 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 Standard
	  • Windows Server 2016 Datacenter
	  • 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	• 7.00607

CONFIDENTIAL

See also:

- Virtualization environments on page 25
- Language support on page 25
- SSL VPN support on page 26
- FortiExtender modem firmware compatibility on page 26

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 2019
Windows Hyper-V Server	• Microsoft Hyper-V Server 2019
Open source XenServer	• Version 3.4.3 • Version 4.1 and later
VMware ESXi	• Versions 6.5, 6.7, 7.0, and 8.0.

Language support

The following table lists language support information.

Language support

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

CONFIDENTIAL

Language	GUI
Portuguese (Brazil)	✓
Spanish	✓

SSL VPN support

SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 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.

CONFIDENTIAL

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

CONFIDENTIAL

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.

CONFIDENTIAL

Resolved issues

The following issues have been fixed in version 7.4.13. To inquire about a particular bug, please contact Customer Service & Support.

Data Leak Prevention

Bug ID	Description
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
1295373	SRV records are redirected to the mgmt interface instead of the VWP interface when a DNS filter profile is applied in the policy
1298350	DNS over TLS server appears unreachable

Explicit Proxy

Bug ID	Description
1253730	Intermittent HTTPS request timeouts occur when proxy-based UTM inspection is enabled on a Virtual Server VIP.
1292536	PAC file data is cleared when deleting a VDOM named 'root'

CONFIDENTIAL

Firewall

Bug ID	Description
1157283	High priority traffic drops when bursty traffic is present on low priority queues.
1212625	Fragmented packets are dropped when egress shaping-profile is configured on a VLAN interface
1217396	Default-qos-type changes to policing-enhanced after reboot
1222166	Traffic shaping fails when SD-WAN load balancing is enabled after reboot.
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
1270575	Traffic fragmentation issues occur when passing through multiple VDOMs on FortiGate
1271340	L2TPv3 packets are discarded when protocol 115 is not included as a known protocol on FortiGate
1277509	Unexpected behavior related to the QTM module when egress-shaping-profile is configured on the parent interface of a VLAN interface.
1279396	TLS_AES_256_GCM_SHA384 cipher suite is not advertised when using an EC384 certificate on a VIP
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
1307143	Traffic is incorrectly shaped when memory optimization settings are applied.

FortiGate 6000/7000 Platform

Bug ID	Description
1283535	fragmented IKE packet drop
1314590	FGCP HA is not supported for HA between an AC powered and a DC powered FortiGate 6000F, FortiGate 7000E or FortiGate 7000F chassis.

CONFIDENTIAL

GUI

Bug ID	Description
1167631	Internet traffic disruption occurs when an error condition in httpsd happens after firmware upgrade to 7.4.8
1212624	Memory usage issues caused by the V8 JavaScript engine
1225806	Memory usage issues caused by V8 ExternalPointerTable leak
1247676	SSH deep scan toggle does not save when enabled on low-end models.
1260292	Print button is not visible when using prof_admin profile after FortiOS upgrade
1282417	License information page load delay occurs when FortiToken Cloud is unreachable

HA

Bug ID	Description
1009939	When bandwidth is low, tftp backup command on slave fails when it should be able to reach the server.
1233776	FSSO user list disappearance occurs when HA failover happens twice.
1258325	FortiToken Mobile push fails when private-data-encryption is enabled after a full HA cluster shutdown
1260236	Unexpected power off events occur in FortiGate 70G when configured in HA Active/Passive mode with wireless traffic.
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
1269523	Rebooting the secondary FortiGate in HA active-passive mode causes traffic loss due to split-brain and unintended ARP broadcasts from the secondary FortiGate.
1270605	HA cluster sync fails when adding a new VDOM in HA primary
1285215	TCP/135 traffic fails when DCE-RPC session helper is enabled with asymmetric traffic in FGSP-transparent mode
1286934	Authentication issues occur in FortiCloud SSO during HA failover due to serial mismatch
1296784	Session synchronization issues occur when FGSP is configured over FGCP cluster environment.
1323497	An IKE NAT port change blocks traffic after HA failover.

CONFIDENTIAL

HyperScale

Bug ID	Description
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

Intrusion Prevention

Bug ID	Description
1182611	An error condition in IPS Engine occurs when stress testing with traffic load on FortiGate-200E
1224669	An error condition in IPS engine occurs when Thread Protection is enabled
1231590	An error condition in IPS engine occurs when FortiSandbox is enabled
1244350	MCDB update issues occur when FortiGate is configured with NGFW policy mode
1267456	A ClientHello packet larger than the MSS generates an SSL error when retransmitted to the server.
1328306	Local-in Virtual Patch fails to inspect traffic when using the HA-MGMT interface.

IPsec VPN

Bug ID	Description
1091195	Traffic drop occurs when npu-offload is enabled at IPsec-phase1-interface
1113625	Traffic disruption occurs when FortiExtender or LAN Extension sessions are offloaded on the FortiGate side.
1137576	IPSEC tunnel failure occurs when IKE Diffie-Hellman processing fails
1217216	DHCP requests fail when FortiGate sends the full DN instead of the CN in Option 61 during IKEv2
1245740	MTU reduction occurs when using IPsec with GCM on 9xG and 12xG devices
1246587	Traffic forwarding issues occur when NPU offload is enabled for IPSEC VPN
1252546	Negotiation timeout occurs when entering OTP within 120 seconds validity period

CONFIDENTIAL

Bug ID	Description
1254266	IPsec dial-up VPN connection fails when username case sensitivity does not match for RADIUS users.
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.
1278940	Unexpected behavior occurs in the system when receiving IPsec VPN traffic with large ICMP packets and NPU offload enabled
1293470	Data transmission issues occur in IPsec VPN tunnels when npu-offload is enabled on FortiGate.
1318272	Enabling system.settings.ike-policy-route after IPsec tunnel configuration blocks ESP traffic from reaching the egress interface.

Log and Report

Bug ID	Description
1198455	When running ITS test occasionally the wrong link status reading is logged
1237774	Log field information loss occurs when the URL or Referrer header exceeds a certain character limit
1241256	Failure to send OT information to FortiAnalyzer occurs when a large number of IoT/OT vulnerabilities are generated.
1269067	Synchronization fails when generating a large number of IoT/OT vulnerabilities
1269332	FortiGate loses FortiAnalyzer serial number during failover from primary to secondary FAZ

Proxy

Bug ID	Description
1224454	SSL deep inspection blocks or bypasses traffic when the first ClientHello TCP segment payload is 1024B or less.
1224915	Intermittent page could not be reached issue occurs when authentication is required by QUIC
1233324	High memory usage occurs when inline IPS is enabled with long-lived connections and IPS DB updates.
1244955	An error condition occurs in WAD during peer port validation.

CONFIDENTIAL

Bug ID	Description
1323515	An FSSO identity lookup that returns no user and matches no proxy-policy stops WAD from responding.

Routing

Bug ID	Description
1272281	VRRP failure occurs when using hardware-switch on FortiGate
1277718	Routing tables are incorrectly assigned to VRF 0 when restoring VDOM configuration

SD-WAN

Bug ID	Description
1118705	Speed test failure occurs when using BGP over loopback design
1273960	Packet loss occurs when upgrading from 7.0.14 to 7.2.10

Security Fabric

Bug ID	Description
1269373	High CPU usage occurs when SFTP backup automation is configured on the FortiGate
1296597	An error condition in Autod occurs when deleting deprecated triggers during upgrade to 7.4.12

SSL-VPN

Bug ID	Description
1309910	Security vulnerability occurs when connecting to a malicious SSH server with crafted packets.

CONFIDENTIAL

Switch Controller

Bug ID	Description
1195908	Virtual VLAN switch forwarding issues occur when STP is enabled in HA setups with multiple members on FortiGate-600F.
1269995	An error condition in fltund occurs during upgrade to 7.6.6

System

Bug ID	Description
1046171	System hang occurs when attempting to delete a VDOM with IPV6 traffic is still present.
1116876	VDSL connection failure occurs when configured on FortiGate 50G-DSL
1144387	FortiGate 50G DSL fails to acquire an IP address from a DSL modem
1161211	Memory usage issues caused by polling FGT memory usage
1166455	TCP packet drop occurs when sending traffic over VLAN+redundant port
1193085	Proxy-arp configuration failure occurs when the proxy-arp address group exceeds 256 entries
1208271	Downloading the full Malicious Certificate Database (MCDB) on every update consumes significant network bandwidth.
1222654	FortiGate-40F fails to display LAN A SPEED and WAN SPEED amber LEDs during the diag hardware test led nic-led.
1227167	Memory usage issues caused by the node process
1231510	IP address assignment issues occur on DSL interfaces configured with static IP after reboot or at irregular intervals
1245329	Configuration loss occurs when FortiGate enters extreme low memory mode
1248631	Intermittent reboot issues occur in FortiWiFi-50G when WiFi clients connect via RADIUS or ax bands
1259458	Intermittent reboot of FortiGate-71G caused by an error condition in the IPS engine.
1262639	Bandwidth distribution issue occurs when using LACP after upgrade to 7.4
1264805	Unexpected behavior in the system occurs when upgrading to 7.4.9
1265816	SPEED LED blinking occurs when upgrading to FortiOS 7.4.10 on FortiGate FG-40F

CONFIDENTIAL

Bug ID	Description
1268808	Packet drops occur when querying SNMP OID 1.3.6.1.4.1.12356.101.4.4.2.1.8 for Processor 13
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
1282021	Error condition in GUI occurs when deleting a VDOM
1283008	[B2867] bmr-hostname is not updated while vne tunnel is established.
1283972	Reboot occurs when FortiSentry triggers a reboot for suspicious cases.
1289434	LED activity lights do not blink when FortiGate is upgraded to version 7.4.x
1290942	FortiGate-70G, FortiGate-71G, FortiWall-70G, and FortiWall-71G WAN interface SPEED LED remains lit after reboot when configured as admin-down with no Ethernet cable connected.
1299330	Third-party CAPWAP fragments are dropped when they pass through NP7 or NP7Lite FortiGate.
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.
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
1269764	Private data encryption wipes IPsec PSKs on platforms with TPM during upgrade from FortiOS 7.2.13 to 7.4.11.
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).
1282918	Using "execute restore secondary-image" prevents FortiGate from booting when the system reboots into the secondary partition.
1283569	FGT force-upg is not automatically cancelled after manually upgrading to a new major.minior
1316497	Upgrading to FortiOS 7.4 generates incorrect obsolete Internet Service logs during initialization.

CONFIDENTIAL

User and Authentication

Bug ID	Description
1211983	Certificate chain issues occur when firewall encounters a certificate renewal issue while using EST simplereenroll process
1233862	Certificate renewal through EST protocol fails when DNS lookup fails
1236839	An error condition in fnbamd occurs when referencing two peer users during certificate authentication
1250279	ACME protocol violation occurs when order validation exceeds 30 seconds
1263865	Connection failure occurs when maximum session limit is reached with EAP enabled in IKE config and TFA for users.
1271821	Token verification fails when username case sensitivity does not match for LDAP users with 2FA enabled.
1325322	Changing authentication configuration during a SAML authentication loop stops WAD from responding.

VM

Bug ID	Description
1294311	SDN connector fails to manage Azure vWAN when deployed in GermanyWestCentral location
1311756	Instance token refresh fails when certificate file size exceeds the fixed buffer size in FortiGate VM.
1324904	Live Migration on Azure VMs wipes RPS settings in config system affinity-packet-redistribution.

Web Filter

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

CONFIDENTIAL

WiFi Controller

Bug ID	Description
1242199	SSID interface is missing in routing table after FMG pushed the configuration to FGT
1243404	Wi-Fi client's FT Roaming failed due to invalid PMKID when 802.11r is enabled on WPA2-Enterprise SSID.
1243456	Wi-Fi client's FT reassociation is rejected when 802.11r is enabled on WPA2-Enterprise SSID.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
1179021	FortiOS 7.4.13 is no longer vulnerable to the following CVE Reference: • CVE-2025-54821

CONFIDENTIAL

Known issues

Known issues are organized into the following categories:

- New known issues on page 39
- Existing known issues on page 39

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

New known issues

The following issues have been identified in version 7.4.13.

Existing known issues

The following issues have been identified in a previous version of FortiOS and remain in FortiOS 7.4.13.

Explicit Proxy

Bug ID	Description
1026362	Web pages do not load when persistent-cookie is disabled for session-cookie-based authentication with captive-portal.
1256323	Packets are forwarded to an offline server when using active-passive load balance method in a forwarding server group
1353958	After upgrading FortiOS to the latest Frontier AI vul fix v7.2.14, 7.4.13, 7.6.8 and 8.0.2, the client browser shows net::ERR_EMPTY_RESPONSE only for the websites on non-standard HTTPS ports(eg., 8443 or 8011) with deep inspection enabled. Other standard HTTPS websites are working as expected.

CONFIDENTIAL

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.
1114635	In the GUI, cannot filter Address objects correctly when using CIDR notation.

FortiGate 6000/7000 Platform

Bug ID	Description
911244	FortiGate 7000E IPv6 routes may not be synchronized correctly among FIMs and FPMs.
1006759	After an HA failover, there is no IPsec route in the kernel. **Workaround**: Bring down and bring up the tunnel
1026665	On the FortiGate 7000F platform with virtual clustering enabled and syslog logging configured. When running the diagnose log test command from a primary vcluster VDOM, some FPMs may not send log messages to the configured syslog servers.
1048808	If the secondary reboots, after it rejoins the cluster SIP sessions are not resynchronized.

1070365	FGCP HA session synchronization may stop working as expected on a FortiGate 7000F cluster managed by FortiManager. This happens if the HA configuration uses management interfaces as session synchronization interfaces by configuring the `session-sync-dev` option, for example:
	`config system ha`
	`  set session-sync-dev 1-M1 1-M2`
	`end`
	The problem occurs when FortiManager updates the configuration of the FortiGate 7000Fs in the cluster. When this happens, FortiManager may incorrectly change the VDOM of the management interfaces added to the `session-sync-dev` command from vsys_ha to mgmt-vdom and the interfaces stop working as session sync interfaces.
	You can work around the problem by re-configuring the session-sync-dev option on the FortiGate 7000F cluster (this resets the VDOM of the session sync interfaces to vsys_ha) and then retrieving the FortiGate configuration from FortiManager. This synchronizes the correct configuration to FortiManager.

1092728	FGT7000F/2718: IPv6 Fragment traffic fail randomly
1153360	Counter values fail to match totals and may overflow during continuous clearing in certain FortiGate models.
1170524	SSH login attempts via special ports fail for VDOM admin users with access to 'mgmt-vdom' on SLBC FortiController models.

CONFIDENTIAL

Bug ID	Description
1183170	6kf/v7.4.9/sdwan: Sdwan is not working in mgmt vdom
1185528	Issue description: subscription license on the secondary chassis is missing after the graceful upgrade from 7.2.10 to 7.2.12 **Workaround**: run "execute update-now" again
1225359	During a graceful firmware upgrade on a FortiGate 6000/7000 Active-Passive HA cluster with HA override enable, traffic loss and session failures may occur when the original primary unit upgrades and reclaims the primary role before its internal modules (FPCs/FPMs) fully come online and synchronize.
1349258	7KF/B2933: Uninterruptible-upgrade upgrade fails from 7.2.13 to 7.4.13

FortiView

Bug ID	Description
1123502	FortiView Threats: drill down to malicious website entry return Failed to retrieve FortiView data from disk

GUI

Bug ID	Description
853352	When viewing entries in slide-out window of the Policy & Objects > Internet Service Database page, users cannot scroll down to the end if there are over 100K entries.
885427	On the Network > Interfaces page, the SFP port is grayed out on the faceplate diagram even though the port is working. This is purely a GUI display issue and does not affect system operation. **Workaround**: View the SFP port information and status using the interface list in the CLI.
1071907	There is no setting for the type option on the GUI for npu_vlink interface.
1145907	The bandwidth widget reports traffic incorrectly on a backup VLAN interface on FortiGate NP6 platform models when fast-path processing is disabled.
1153294	Custom HTML content does not render correctly on login pages when configured through the FortiGate web interface or CLI.
1237136	Dynamic VLANs are not visible on the GUI when a port-security-policy is applied

CONFIDENTIAL

HA

Bug ID	Description
781171	When performing HA upgrade via the GUI, if the secondary unit takes several minutes to bootup, the GUI may show a misleading error message "Image upgrade failed" due to premature timeout. This is just a GUI display issue and the HA upgrade can still complete without issue.
977155	HA synchronization fails when devices have different private keys
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.
1210147	HA out-of-sync occurs due to certificate
1226122	System > HA: There is no "upgrade" button on secondary GUI page when HA in "local-only" or "secondary-only" MVC upgrade mode **Workaround**: is to upgrade the secondary via the command line
1231480	LACPDU transmission issues occur when HA failover is triggered by a monitoring port disconnect

HyperScale

Bug ID	Description
1025908	Session count on peer device is 50% less during fgsp testing in new setups using VRRP-based configuration.
1027251	4401f: Logs are not sent out from FGT with log2host setting when log-server becomes reachable and it has correct dmac
1034685	4401f:Log cache is not cleared and holding the wrong dmac for unreachable gateway
1042151	/FortiOS/v7.00/images/build3380/: syslog over TCP not working
1058477	sentb and rcvdb show -ve value for end session syslog message.
1069044	Unable to clear/purge npu-session when src filter is set
1069531	diag sys session stat' command shows incorrect session_count
1072076	/build2693/: New HA master send syslog session-end log packet using wrong mac address after failover
1072247	/build2693/: New HA master not send syslog session-end log packet after failover
1078916	/build2699/: Log rate on GUI is double of real log rate
1091244	3440: hypersale hw-session-sync-dev should print properly error message when set members over 8

CONFIDENTIAL

Bug ID	Description
1091815	hw session doesn't sync when one of multiple interface hw-session-sync-dev is down
1095593	Count for dropping arpmiss exception packets is too high
1101562	hyperscale hw-session-sync-dev LAG members can exceed 2*number of NP
1119021	Sessionsync daemon makes hw-session-sync dev up even it's physically down, no such issue with sw session sync dev
1119031	4201:HW sessions are not synced to slave when one of the hw-session-sync-dev members is down
1128155	FGT1801F log-transport TCP should be hidden for log servers under L2host and Netflow on CLI
1135433	IPv6 entries appear in the output of pba list, after reaching max PBA limit for ippool
1138823	FGT1801F non-hyperscale vdom shows incorrect output of "diag firewall ippool get-pub/priv" commands
1140493	config should be blocked when user tries to set same interface as hw-session-sync-dev and monitor.
1141632	The system fails to send new syslog packets when a highavailability failover occurs on FortiGate models.
1143144	Both HW log(ps) rate and log(pm) rate showing in dia sys npu-session stat when set log-mode per-nat-mapping
1144290	2771/Log rate show 0 when using TCP for syslog
1150863	Unintended session deletion may occur after FGSP failover due to a dirty Rsession.
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.
1197891	when unsupported ports are configured for hw-session-sync-dev it results in hardware session sync not functioning correctly. **Workaround**: change interface and reboot as simply fixing the config does not restore the proper configuration
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.
1201968	4401f:Memory leak/ leak to log2host tbl can be seen when there are ~60M cc with log2host setting after couple of failovers
1202268	4401f:Not all the HW sessions are synced to new slave after a failover

CONFIDENTIAL

IPsec VPN

Bug ID	Description
866413	traffic over GRE tunnel over IPSec tunnel or traffic over IPsec tunnel with GRE encapsulation is not offloaded on NP7 based units.
897871	GRE over IPsec doesn't work in transport-mode (b8591)
970703	6K7K do not support ipsec-vpn over vdom-link / npu-vlink
1036262	Tunnel traffic is encrypted as FortiGate-ESP packets when transport is UDP and FortiGate-ESP is enabled. **Workaround**: Disable fortinet-esp when transport is set to udp.
1164175	DH group mismatches with INVALID_KE when peer proposes a DH group in its IKE_SA_INIT which is not in the expected order

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.

1063349	Title: HTTP/2 traffic carrying multiple Cookie headers is blocked when strict web checking (strict-web-check) is enabled in the web proxy global settings.
	Description: On FortiGate running an affected release, enabling strict-web-check under config web-proxy global caused the proxy mode policy to block HTTP/2 requests that carry more than one Cookie header field. HTTP/2 (per RFC 7540 8.1.2.5) permits the Cookie header to be split into multiple separate header fields, but strict mode rejected such requests as malformed, returning a connection error to the client.
	Workaround: Disable the option:
	`config web-proxy global`
	`  set strict-web-check disable`
	`end`

REST API

Bug ID	Description
1154124	Adding dynamic fabric addresses via the FortiNAC REST API fails due to an issue with HTTP header validation.

CONFIDENTIAL

Routing

Bug ID	Description
903444	Command 'diagnose ip rtcache list' is no longer supported in FortiOS 4.19 kernel

1040655	From 7.4.1, when there is ECMP routes, local out traffic may use different route/port to connect out to server, for critical traffic which is sensitive to source IP address, suggest customer set specify interface or SD-WAN for the traffic since FortiOS has implemented "interface-select-method" command for nearly all local-out traffic.
	e.g.
	`config system fortiguard`
	`set interface-select-method specify`
	`set interface "wan1"`
	`end`

1133796	ipv6 routes are stuck on kernel routing table
1150878	The IPoE tunnel interface cannot be selected in the Interface Bandwidth widget.

Security Fabric

Bug ID	Description
1156006	SFTP backup fails when triggered through automation stitch on a FortiGate in an HA cluster using Windows-style paths.

Switch Controller

Bug ID	Description
1150215	Offline FSWs are offline in the GUI topology view, but shown as online in the list view.

System

Bug ID	Description
1021903	The le-switch member list does not update when the role of an interface is changed in a lan-extension environment.
1078541	FortiFirewall 2600F models may become stuck after a fresh image burn. Upgrading from a previous version stills works. **Workaround**: power cycle the unit.

CONFIDENTIAL

Bug ID	Description
1085407	FortiGate unresponsive when default-qos-type is set to shaping.
1105321	4201F NP7 EIF0_IGR and EIF1_IGR usage are stuck at 100%, and host softirq is stuck at 99% after running the iptunnel traffic
1114298	FortiGate Cloud remote login triggers 2 admin login events (1 successful and 1 unsuccessful for PKI admin)
1136616	2731: no graphs on some vlan interfaces in dashboard interface widget
1164332	NP7 stops forwarding traffic after reassembling large packet in DFR
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
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'.
1213236	On v7.2.x, FGT700G/701G interface wan1/2 and lan1-6 default speed is 5000auto, but it actually working at auto mode and will negotiate to 1G if peer side speed is 1G. But on V7.4.9, the default speed setting changed to auto and 5000auto can only work at 5000M speed. So in upgrade scenario, customer may notice interface down due to speed setting not match. **Workaround**: Manually change port speed to auto.
1283702	MTU configuration for VLAN interface is lost after reboot when VLAN is configured over a physical port or LAG.

Upgrade

Bug ID	Description
1114550	FortiExtender shows as offline after upgrading FGT from V7.4.5GA to V7.4.6GA. **Workaround**: Reboot FortiExtender manually.

User and Authentication

Bug ID	Description
884462	NTLM auth does not work with Chrome
972391	RADIUS group usage not displayed correctly in GUI when used for firewall admin authentication.

CONFIDENTIAL

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.
1148767	FSSO users are showing in small letters, filtering of users are not working and PIE charts are also not visible
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
978021	In FTP passive mode with GWLB setup, Geneve header VNI lengths are zero in syn-ack packets, leading to retransmission issues.
1125437	The "set distance" option under interface configured as dhcp client doesn't work o vm

WiFi Controller

Bug ID	Description
814541	GUI issue - When there are extra large number of managed FortiAP devices (500+) and large number of WiFi clients (5000+), the "Managed FortiAP" page and "FortiAP Status" widget can take a long time to load. This issue does not impact FortiAP operation.
964757	The FortiGate fails to generate debug/sniffer logs for a user when connecting to a specific SSID despite showing station logs with radius requests and challenges, while other SSIDs function correctly.
1080094	High memory usage may occur due to offline station entries not being automatically cleaned up over time.
1144969	Inconsistent IP addresses may display between the GUI page and the device column hover popup when WiFi client switch between different SSIDs.

CONFIDENTIAL

ZTNA

Bug ID	Description
819987	Mapped drives become inaccessible after laptop reboots when using FortiGate ZTNA access proxy with FQDN destinations.

CONFIDENTIAL

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.

CONFIDENTIAL

Built-in IPS Engine

IPS Engine 7.00607 is released as the built-in IPS Engine. Refer to the IPS Engine Release Notes for information.

CONFIDENTIAL

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.

Limitations on HA cluster formation between different FortiGate Rugged 60F and 60F 3G4G models

FortiGate Rugged 60F and 60F 3G4G models have various generations defined as follows:

- Gen1
- Gen2 = Gen1 + TPM
- Gen3 = Gen2 + Dual DC-input
- Gen4 = Gen3 + GPS antenna
- Gen5 = Gen4 + memory

The following HA clusters can be formed:

- Gen1 and Gen2 can form an HA cluster.
- Gen4 and Gen5 can form an HA cluster.

CONFIDENTIAL

- Gen1 and Gen2 cannot form an HA cluster with Gen3, Gen4, or Gen5 due to differences in the `config system vin-alarm` command.

CONFIDENTIAL



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.