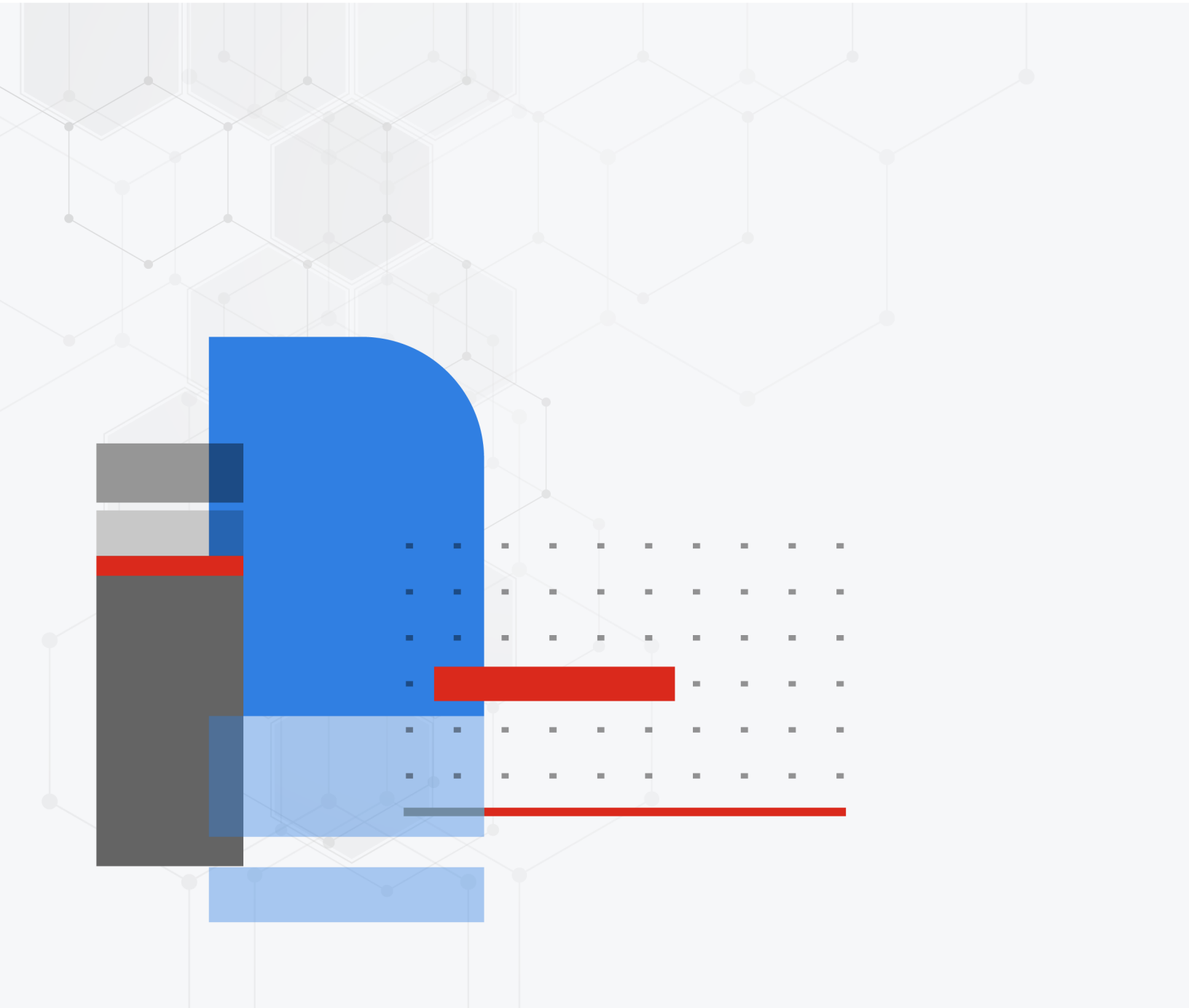




Release Notes

FortiOS 7.4.7



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



June 9, 2025

FortiOS 7.4.7 Release Notes

01-747-1114568-20250609

TABLE OF CONTENTS

Change Log	5
Introduction and supported models	6
Supported models	6
Special branch supported models	6
FortiGate 6000 and 7000 support	7
Special notices	8
Hyperscale incompatibilities and limitations	8
FortiGate 6000 and 7000 incompatibilities and limitations	8
SMB drive mapping with ZTNA access proxy	8
Local out traffic using ECMP routes could use different port or route to server	9
Hyperscale NP7 hardware limitation	9
Changes in default behavior	10
Changes in table size	11
Upgrade information	12
Fortinet Security Fabric upgrade	12
Downgrading to previous firmware versions	14
Firmware image checksums	14
FortiGate 6000 and 7000 upgrade information	14
IPS-based and voipd-based VoIP profiles	15
GUI firmware upgrade does not respect upgrade path in previous versions	17
2 GB RAM FortiGate models no longer support FortiOS proxy-related features	17
FortiGate VM memory and upgrade	17
Managed FortiSwitch do not permit empty passwords for administrator accounts	17
Policies that use an interface show missing or empty values after an upgrade	18
Product integration and support	19
Virtualization environments	20
Language support	20
SSL VPN support	21
SSL VPN web mode	21
FortiExtender modem firmware compatibility	21
Resolved issues	24
Anti Virus	24
FortiGate 6000 and 7000 platforms	24
GUI	24
HA	24
Intrusion Prevention	25
Log & Report	25
SSL VPN	25
Known issues	26
New known issues	26

Firewall	26
GUI	26
HA	26
IPsec VPN	27
REST API	27
Routing	27
Security Fabric	27
Switch Controller	27
System	28
Upgrade	28
User & Authentication	28
VM	28
Existing known issues	29
Explicit Proxy	29
Firewall	29
FortiGate 6000 and 7000 platforms	30
GUI	31
HA	31
Hyperscale	32
Intrusion Prevention	32
IPsec VPN	32
Log & Report	33
Proxy	33
Routing	33
Security Fabric	34
SSL VPN	34
Switch Controller	34
System	35
Upgrade	36
User & Authentication	36
VM	37
WiFi Controller	37
ZTNA	38
Built-in AV Engine	39
Built-in IPS Engine	40
Limitations	41
Citrix XenServer limitations	41
Open source XenServer limitations	41
Limitations on HA cluster formation between different FortiGate Rugged 60F and 60F 3G4G models	41

Change Log

Date	Change Description
2025-01-21	Initial release.
2025-01-28	Updated Managed FortiSwitch do not permit empty passwords for administrator accounts on page 17 .
2025-01-30	Updated Policies that use an interface show missing or empty values after an upgrade on page 18 and Managed FortiSwitch do not permit empty passwords for administrator accounts on page 17 .
2025-02-05	Updated Known issues on page 26 .
2025-02-12	Updated Known issues on page 26 .
2025-02-18	Updated Known issues on page 26 .
2025-03-03	Updated Known issues on page 26 .
2025-03-06	Updated Known issues on page 26 .
2025-03-10	Updated Known issues on page 26 .
2025-03-13	Updated Introduction and supported models on page 6 .
2025-03-17	Updated Known issues on page 26 .
2025-04-08	Updated Known issues on page 26 .
2025-04-14	Updated Known issues on page 26 .
2025-04-21	Added Special branch supported models on page 6 .
2025-04-29	Updated Known issues on page 26 .
2025-05-12	Updated Resolved issues on page 24 and Known issues on page 26 .
2025-05-20	Updated Introduction and supported models on page 6 .
2025-05-26	Updated Resolved issues on page 24 and Known issues on page 26 .
2025-06-04	Updated Changes in default behavior on page 10 .
2025-06-05	Updated Known issues on page 26 .
2025-06-09	Updated Known issues on page 26 .

Introduction and supported models

This guide provides release information for FortiOS 7.4.7 build 2731.

For FortiOS documentation, see the [Fortinet Document Library](#).

Supported models

FortiOS 7.4.7 supports the following models.

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

Special branch supported models

The following models are released on a special branch of FortiOS 7.4.7. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 2731.

FGR-50G	is released on build 5098.
----------------	----------------------------

FortiGate 6000 and 7000 support

FortiOS 7.4.7 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

- [Hyperscale incompatibilities and limitations on page 8](#)
- [FortiGate 6000 and 7000 incompatibilities and limitations on page 8](#)
- [SMB drive mapping with ZTNA access proxy on page 8](#)
- [Local out traffic using ECMP routes could use different port or route to server on page 9](#)
- [Hyperscale NP7 hardware limitation on page 9](#)

Hyperscale incompatibilities and limitations

See [Hyperscale firewall incompatibilities and limitations](#) in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 7.4.7 features.

FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 7.4.7 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.

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 `cg-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 (`cg-block-size`).

Changes in default behavior

Bug ID	Description
949997	LDAPS authentication behavior changed. FortiOS 7.4.4 and later enhances the security standards for LDAPS by requiring FortiOS to trust the server certificate during the TLS handshake. If the LDAP server's CA certificate was not present and is not added after upgrading to FortiOS 7.4.7, LDAPS authentication will fail. To ensure smooth operation, import the LDAP server's CA certificate to FortiGate prior to upgrading. For more details, see Configuring client certificate authentication on the LDAP server .

Changes in table size

Bug ID	Description
1042266	On high-end FortiGate models, the number of policy routes and policy routes6 is increased from 2048 to 5000.

Upgrade information

Supported upgrade path information is available on the [Fortinet Customer Service & Support site](#).

FortiGate	Upgrade option	Details
Individual FortiGate devices	Manual update	Use the procedure in this topic. See also Upgrading individual devices in the FortiOS Administration Guide.
	Automatic update based on FortiGuard upgrade path	See Enabling automatic firmware updates in the FortiOS Administration Guide for details
Multiple FortiGate devices in a Fortinet Security Fabric	Manual, immediate or scheduled update based on FortiGuard upgrade path	See Fortinet Security Fabric upgrade on page 12 and Upgrading Fabric or managed devices in the FortiOS Administration Guide.

To view supported upgrade path information:

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

Fortinet Security Fabric upgrade

FortiOS 7.4.7 greatly increases the interoperability between other Fortinet products. This includes:

FortiAnalyzer	• 7.4.6
FortiManager	• 7.4.6
FortiExtender	• 7.4.0 and later

FortiSwitch OS (FortiLink support)	<ul style="list-style-type: none"> • 6.4.6 build 0470 and later
FortiAP	<ul style="list-style-type: none"> • 7.2.2 and later
FortiAP-U	<ul style="list-style-type: none"> • 6.2.5 and later
FortiAP-W2	<ul style="list-style-type: none"> • 7.2.2 and later
FortiClient* EMS	<ul style="list-style-type: none"> • 7.0.3 build 0229 and later
FortiClient* Microsoft Windows	<ul style="list-style-type: none"> • 7.0.3 build 0193 and later
FortiClient* Mac OS X	<ul style="list-style-type: none"> • 7.0.3 build 0131 and later
FortiClient* Linux	<ul style="list-style-type: none"> • 7.0.3 build 0137 and later
FortiClient* iOS	<ul style="list-style-type: none"> • 7.0.2 build 0036 and later
FortiClient* Android	<ul style="list-style-type: none"> • 7.0.2 build 0031 and later
FortiSandbox	<ul style="list-style-type: none"> • 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
- 17. FortiMonitor



If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.4.7. When Security Fabric is enabled in FortiOS 7.4.7, all FortiGate devices must be running FortiOS 7.4.7.

Downgrading to previous firmware versions

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

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

Firmware image checksums

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

FortiGate 6000 and 7000 upgrade information

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

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

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



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

To perform a graceful upgrade of your FortiGate 6000 or 7000 to FortiOS 7.4.7:

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

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



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

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

2. Download the FortiOS 7.4.7 FG-6000F, FG-7000E, or FG-7000F firmware from <https://support.fortinet.com>.
3. Perform a normal upgrade of your HA cluster using the downloaded firmware image file.
4. When the upgrade is complete, verify that you have installed the correct firmware version.
For example, check the FortiGate dashboard or use the `get system status` command.
5. Confirm that all components are synchronized and operating normally.
For example, open the Cluster Status dashboard widget to view the status of all components, or use `diagnose sys confsync status` to confirm that all components are synchronized.

IPS-based and voipd-based VoIP profiles

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.

Before upgrade	After upgrade
<pre>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</pre>	<pre>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</pre>

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, 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.

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.

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

Product integration and support

The following table lists FortiOS 7.4.7 product integration and support information:

Web browsers	<ul style="list-style-type: none">• Microsoft Edge 135• Mozilla Firefox version 138• Google Chrome version 136 <p>Other browser versions have not been tested, but may fully function. Other web browsers may function correctly, but are not supported by Fortinet.</p>
Explicit web proxy browser	<ul style="list-style-type: none">• Microsoft Edge 135• Mozilla Firefox version 138• Google Chrome version 136 <p>Other browser versions have not been tested, but may fully function. Other web browsers may function correctly, but are not supported by Fortinet.</p>
FortiController	<ul style="list-style-type: none">• 5.2.5 and later <p>Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C</p>
Fortinet Single Sign-On (FSSO)	<ul style="list-style-type: none">• 5.0 build 0319 and later (needed for FSSO agent support OU in group filters)<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 7.00035
IPS Engine	<ul style="list-style-type: none">• 7.00559

See also:

- [Virtualization environments on page 20](#)
- [Language support on page 20](#)
- [SSL VPN support on page 21](#)
- [FortiExtender modem firmware compatibility on page 21](#)

Virtualization environments

The following table lists hypervisors and recommended versions.

Hypervisor	Recommended versions
Citrix Hypervisor	<ul style="list-style-type: none">8.2 Express Edition, CU1
Linux KVM	<ul style="list-style-type: none">Ubuntu 22.04.3 LTSRed Hat Enterprise Linux release 9.4SUSE Linux Enterprise Server 12 SP3 release 12.3
Microsoft Windows Server	<ul style="list-style-type: none">Windows Server 2019
Windows Hyper-V Server	<ul style="list-style-type: none">Microsoft Hyper-V Server 2019
Open source XenServer	<ul style="list-style-type: none">Version 3.4.3Version 4.1 and later
VMware ESXi	<ul style="list-style-type: none">Versions 6.5, 6.7, 7.0, and 8.0.

Language support

The following table lists language support information.

Language support

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

SSL VPN support

SSL VPN web mode

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

Supported operating systems and web browsers

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

FortiExtender model	Modem firmware image name	Modem firmware file on Support site	Geographical region
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
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

FortiExtender model	Modem firmware image name	Modem firmware file on Support site	Geographical region
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 7.4.7. To inquire about a particular bug, please contact [Customer Service & Support](#).

Anti Virus

Bug ID	Description
1068321	Previous unsigned MMDB and AVAI databases are kept after upgrading FortiOS.

FortiGate 6000 and 7000 platforms

Bug ID	Description
1149405	The image upgrade fails when performing a non-graceful update due to an ISIZE mismatch during verification.

GUI

Bug ID	Description
1110382	Admin can login to GUI (HTTPS) with password, even when <code>admin-https-pki-required</code> is enabled.

HA

Bug ID	Description
1054041	DHCP client can't get IPv4 address from server with vcluster.

Intrusion Prevention

Bug ID	Description
1107445	Remove IPS diagnose command <code>diagnose ips cfgscript run</code> .

Log & Report

Bug ID	Description
1045253	Log items cannot be created and sent to FortiGate Cloud log server when confirm queue becomes full.

SSL VPN

Bug ID	Description
1000674	When generating function backtrace in crash logs for ARM32, SSL VPN frequently crashes due to segmentation faults.
1101837	Insufficient session expiration in SSL VPN using SAML authentication.

Known issues

Known issues are organized into the following categories:

- [New known issues on page 26](#)
- [Existing known issues on page 29](#)

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 7.4.7.

Firewall

Bug ID	Description
1148166	Source port translation was not permitted with traffic to UDP port 7001.

GUI

Bug ID	Description
1148324	VLAN interface is not displayed on GUI after upgrade
1152464	DHCP reservation from DHCP monitor page checks DHCP IP range instead of subnet/netmask.
1153294	HTML definition for "Pre-login Disclaimer Message" is not working.

HA

Bug ID	Description
1151668	Interface bandwidth widget doest display HB and Managed port.

IPsec VPN

Bug ID	Description
1152486	Unable to select policy-based IPsec tunnel in the firewall policy for SD-WAN member while configuring in GUI.

REST API

Bug ID	Description
1154124	FortiNAC dynamic address REST API request via FortiGate Security Fabric denied with HTTP 400 Bad Request.

Routing

Bug ID	Description
1142290	GUI error when adding ssl.root interface in route-map.

Security Fabric

Bug ID	Description
1154494	Automation stitch for non-root FGT in security fabric is not triggered.
1156006	SFTP backup fails to execute as expected when triggered through the automation stitch

Switch Controller

Bug ID	Description
1153175	Intermittent issues configuring allowed-VLANs on the MCLAG interface via FortiGate GUI and CLI.
1153905	FortiSwitch client page keeps loading.

System

Bug ID	Description
1012577	Traffic on WAN interface is dropped when policy-offload-level (under config system setting) is set to dos-offload.
1054955	USB GPIO and host function were not set up properly on 9xG and 12xG.
1067448	VLAN switch is not working on 120G/121G.
1075911	Traffic randomly stops working through an aggregate interface.
1085407	FortiGate unresponsive when <code>default-qos-type</code> is set to <code>shaping</code> .
1091551	Hardware limitation on the NP7 platform causes the following QTM related issues: <ul style="list-style-type: none"> Incorrect checksum for fragments after QTM. The workaround is to not parse Layer4 after QTM. Packets longer than 6000 bytes cause QTM unresponsiveness. Refresh issue causes QTM unresponsiveness. The workaround is to use one refresh list. MTU is not honored after QTM, so packets are not fragmented.
1104410	The FortiGate-120G SFP ports fail to establish connectivity when configured with 'set speed 1000full' due to improper auto-negotiation handling.
1105321	FG-4201F with NP7 network processors shows EIF0_IGR and EIF1_IGR usage stuck at 100% and host softirq stuck at 99% after running the iptunnel traffic.
1146354	Network interface settings page will not load if user has 'prof_admin_elevated_profile' on 401F.

Upgrade

Bug ID	Description
1097503	Fabric upgrade from 7.2.9 to 7.4.5 failed.

User & Authentication

Bug ID	Description
1148767	FSSO users show in small letters, user filtering is not working, and PIE charts are not visible.

VM

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

Existing known issues

The following issues have been identified in a previous version of FortiOS and remain in FortiOS 7.4.7.

Explicit Proxy

Bug ID	Description
1026362	Web pages do not load when <code>persistent-cookie</code> is disabled for session-cookie-based authentication with <i>captive-portal</i> .

Firewall

Bug ID	Description
959065	On the <i>Policy & Objects > Traffic Shaping</i> page, when deleting or creating a shaper, the counters for the other shapers are cleared.
994986	The <i>By Sequence</i> view in the Firewall policy list may incorrectly show a duplicate implicit deny policy in the middle of the list. This is purely a GUI display issue and does not impact policy operation. The <i>Interface Pair View</i> and <i>Sequence Grouping View</i> do not have this issue.
1004263	Session counters are not updated when ASIC offload is enabled on firewall policy. FortiGate GUI displays incorrect information in the "Bytes" and "Last Used" columns.
1057080	On the <i>Firewall Policy</i> page, search results do not display in an expanded format.
1078662	If an interface on an NP7 platform has the <code>set inbandwidth XXX, set outbandwidth XXX,</code> and <code>set egress-shaping-profile XX</code> settings, the following issues may occur: <ul style="list-style-type: none"> Fragment packet checksum is incorrect. MTU is not honored when sending packets out. QTM hangs and blocks traffic when packet size is larger than 6000 bytes. Workaround: <pre>config system interface edit xxx unset egress-shaping-profile next end</pre>
1114635	Unable to filter address object by CIDR notation.
1117165	Leaving the <code>apn</code> field empty in a GTP APN traffic shaping policy means that the policy will not match any traffic. Consequently, APN traffic shaping can only be applied to specific APNs. To configure GTP APN traffic shaping:

Bug ID	Description
	<pre> config gtp apn-shaper edit <policy-id> set apn [<apn-name> <apngrp-name> ...] set rate-limit <limit> set action {drop reject} set back-off-time <time> next end </pre>

FortiGate 6000 and 7000 platforms

Bug ID	Description
790464	After a failover, ARP entries are removed from all slots when an ARP query of single slot does not respond.
911244	FortiGate 7000E IPv6 routes may not be synchronized correctly among FIMs and FPMs.
976521	High CPU usage by the node process occurs when loading 7000 policies due to fetching all statistics in one request.
1006759	<p>After an HA failover, there is no IPsec route in the kernel.</p> <p>Workaround: Bring down and bring up the tunnel.</p>
1026665	On the FortiGate 7000F platform with virtual clustering enabled and syslog logging configured, when running the <code>diagnose log test</code> 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.
1060619	CSF is not working as expected.
1070365	<p>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 <code>session-sync-dev</code> option, for example:</p> <pre> config system ha set session-sync-dev 1-M1 1-M2 end </pre> <p>The problem occurs when FortiManager updates the configuration of the FortiGate 7000F devices in the cluster it incorrectly changes to the VDOM of the management interfaces added to the <code>session-sync-dev</code> command from <code>mgmt-vdom</code> to <code>vsys_ha</code> and the interfaces stop working as session sync interfaces.</p> <p>You can work around the problem by re-configuring the <code>session-sync-dev</code> option on the FortiGate 7000F cluster (this resets the VDOM of the session sync interfaces to <code>vsys_ha</code>) and then retrieving the FortiGate configuration from FortiManager. This synchronizes the correct configuration to FortiManager.</p>

Bug ID	Description
1078532	When upgrading the FG6001F platform, in some instances the slave chassis does not synchronize the FPC subscription license from master chassis. Workaround: use the <code>execute update-now</code> command.
1092728	On FortiGate 6000 and 7000 platforms, fragmented IPv6 traffic is randomly dropped.
1109601	Graceful upgrades fail when hataalk daemon restarts, disrupting slbha state synchronization during FortiOS version transitions.

GUI

Bug ID	Description
853352	When viewing entries in slide-out window of the <i>Policy & Objects > Internet Service Database</i> page, users cannot scroll down to the end if there are over 100000 entries.
885427	Suggest showing the SFP status information on the faceplate of FGR-60F/60F-3G4G devices.
1047963	High Node.js memory usage when building FortiManager in Report Runner fails. Occurs when FortiManager has a slow connection, is unreachable from the FortiGate (because FMG is behind NAT), or the IP is incorrect.
1055197	On FortiGate G series models with dual WAN links, the <i>Interface Bandwidth</i> widget may show an incorrect incoming and outgoing bandwidth count where the actual traffic does not match the display numbers.
1071907	There is no setting for the type option on the GUI for npu_vlink interface.
1114549	Authorization of FEXT devices fails when using the FortiGate GUI.
1145907	Bandwidth widget does not report the traffic correctly for backup VLAN interfaces.

HA

Bug ID	Description
781171	When performing HA upgrade in the GUI, if the secondary unit takes several minutes to boot up, the GUI may show a misleading error message <i>Image upgrade failed</i> due to premature timeout. This is just a GUI display issue and the HA upgrade can still complete without issue.
1000808	FortiGate in an HA setup has an unnecessary primary unit selection when a new member joins or reboots one member in the VC cluster when the VC has more than 2 units.
1107137	The secondary FortiGate with an HA Reserved Management Interface cannot be accessed using HTTPS after upgrading from version 7.4.3.
1137565	vSN support was added in 7.2.9, 7.4.6, and 7.6.1. FG-100F/101F do not yet support vSN and logical-sn. No workaround until the devices support vSN.

Hyperscale

Bug ID	Description
817562	Ipmd fails to correctly handle different VRFs, treating all as vrf 0, causing improper route management and affecting network traffic isolation.
896203	NPD parse errors occur after system reboot when running with multiple VDOMs and large address groups.
961328	Port selection remains in direct mode despite setting pba-port-select-mode to random, causing non-random port allocation for NAT sessions.
977376	FG-4201F has a 10% performance drop during a CPS test case with DoS policy.
1024274	When Hyperscale logging is enabled with multicast log, the log is not sent to servers that are configured to receive multicast logs.
1025908	Session count on peer device is 50% less during FGSP testing in new setups using VRRP-based configuration.

Intrusion Prevention

Bug ID	Description
1117043	<p>After upgrade, event log shows <code>logdesc="IPSA driver update failed" msg="Fail to update IPSA driver status!"</code>.</p> <p>This issue only affects physical FortiGate models with the following IPS engine versions:</p> <ul style="list-style-type: none"> IPS Engine version: 7.550 - 7.567 IPS Engine version: 7.1019 - 7.1039 <p>To determine the IPS Engine versions, use the command:</p> <pre>get sys fortiguard-service status grep 'IPS/FlowAV Engine'</pre> <p>Workaround: Power off the FortiGate. Wait 30 seconds, and then power on the FortiGate.</p> <p>Note: Reboot using the CLI is not an effective workaround and requires additional steps. After executing <code>exec shutdown</code>, unplug the power to the FortiGate. Wait one minute, and the power on the FortiGate.</p>
1141238	"Detect Botnet Connections" info shown on GUI.

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.

Bug ID	Description
897871	GRE over IPsec does not work in transport mode.
944600	CPU usage issues occurred when IPsec VPN traffic was received on the VLAN interface of an NP7 vlink.
970703	FortiGate 6K and 7K models do not support IPsec VPN over vdom-link/npu-vlink.
1012615	IPsec VPN traffic is dropped after upgrading to version 7.4.3.
1140823	IPsec tunnels stuck on spoke np6xlite drop the ESP packet.

Log & Report

Bug ID	Description
1113588	FortiGate prompts error <i>Fetching data from Disk is taking longer than expected. Suggest trying a different log source or check the availability of Disk.</i> when viewing logs for the last 7 days from disk or FortiAnalyzer.
1148101	Logs are not uploaded to FortiAnalyzer.

Proxy

Bug ID	Description
910678	CPU usage issue in WAD caused by a high number of devices being detected by the device detection feature.
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.
1060812	Botnet detection fails in transparent proxy setups caused by implementation error.

Routing

Bug ID	Description
903444	The <code>diagnose ip rtcache list</code> command is no longer supported in the FortiOS 4.19 kernel.
1040655	From version 7.4.1, when there is ECMP routes, local out traffic may use a different route/port to connect out to the server. Workaround: for critical traffic which is sensitive to source IP address, specify the interface or SD-WAN for the traffic using the <code>interface-select-method</code> command for nearly all local-out traffic. For example:

Bug ID	Description
	<pre>config system fortiguard set interface-select-method specify set interface "wan1" end</pre>

Security Fabric

Bug ID	Description
903922	Physical and logical topology is slow to load when there are a lot of managed FortiAP devices (over 50). This issue does not impact FortiAP management and operation.
1011833	FortiGate experiences a CPU usage issue in the node process when there multiple administrator sessions running simultaneously on the GUI in a Security Fabric with multiple downstream devices. This may result in slow loading times for multiple GUI pages.
1021684	In some cases, the <i>Security Fabric</i> topology does not load properly and displays a <i>Failed to load Topology Results</i> error.
1150382	Security profile names containing two forward slashes (//) cause the webpage to become unresponsive when attempting to edit.
1076439	Security Fabric Asset Identity Center shows "Failed to load user device store data".
1149817	FortiLink Tier2 switch is directly connected to FortiGate on <i>Security Fabric > Physical Topology</i> page.

SSL VPN

Bug ID	Description
1058211	Traffic could not go though SSL VPN tunnel when DTLS is enabled with a loopback interface as source address.

Switch Controller

Bug ID	Description
1114032	GUI Switch port interface keeps loading with https 500 error on monitor/switch-controller/managed-switch/tx-rx.
1138263	FortiGate 200F GUI does not display FortiSwitch ports, and changes are not updated on switch.
1150215	Offline FSWs show as offline in the GUI topology view but show as online in the list view.

System

Bug ID	Description
901621	<p>On the NP7 platform, setting the interface configuration using <code>set inbandwidth <x></code> or <code>set outbandwidth <x></code> commands stops traffic flow.</p> <p>Workaround: Change the NP7 <code>default-qos-type</code> setting from <code>shaping</code> to <code>policing</code>. This requires a restart of the device for the configuration to take effect:</p> <pre>config system npu set default-qos-type policing end</pre>
912383	FGR-70F and FGR-70F-3G4G failed to perform regular reboot process (using <code>execute reboot</code> command) with an SD card inserted.
992323, 1056133, 1075607, 1082413, 1084898	Traffic interrupted when traffic shaping is enabled on 9xG and 12xG.
1021903	The le-switch member list does not update when the role of an interface is changed in a lan-extension environment.
1046484	After shutting down FortiGate, the system automatically boots up again.
1048496	On FortiGate, the <code>snmp</code> daemon does not work as expected resulting in the SNMP queries timing out.
1057131	A FortiGuard update can cause the system to not operate as expected if the FortiGate is already in conserve mode. Users may need to reboot the FortiGate.
1069208	If the DHCP offer contains padding when DHCP relay is used, the DHCP relay deletes the padding before relaying the packet.
1078541	<p>The FortiFirewall 2600F model may become stuck after a fresh image burn. Upgrading from a previous version stills works.</p> <p>Workaround: power cycle the unit.</p>
1089143	The time change in FOS is restored after reboot. The RTC node is not created correctly so the time change cannot be kept in RTC.
1102416	Cannot push <code>config sfp-dsl enable</code> and <code>vectoring</code> under interface.
1113436	Connectivity issue while using offloading NP7 QinQ 802.1AD 802.1Q over LACP.
1114298	FortiGate Cloud remote login triggers 2 admin login events (1 successful and 1 unsuccessful for PKI admin).
1117005	<p>FortiGate encounters a CPU usage issue.</p> <p>Workaround: Disable IPsec phase1 <code>npu-offload</code>.</p>
1140755	Unable to delete software switch interface.
1148214	Interface page in the GUI is not displayed.

Upgrade

Bug ID	Description
1104649	<p>In 7.4.6 and 7.4.7, if a local-in policy or local-in-policy6 is used in an interface in version 7.4.5, or any previous GA version that was part of the SD-WAN zone, the policies are deleted or show empty values after upgrading to version 7.4.6 or 7.4.7.</p> <p>Workaround: After upgrading to 7.4.6 or 7.4.7, users must manually recreate these policies and assign them to the appropriate SD-WAN zone.</p>
1114550	<p>FortiExtender shows as offline after upgrading FGT from 7.4.5 to 7.4.6.</p> <p>Workaround: Reboot FortiExtender manually.</p>

User & Authentication

Bug ID	Description
884462	NTLM authentication does not work with Chrome.
972391	RADIUS group usage not displayed correctly in GUI when used for firewall admin authentication.
1080234	<p>For FortiGate (versions 7.2.10 and 7.4.5 and later) and FortiNAC (versions 9.2.8 and 9.4.6 and prior) integration, when testing connectivity/user credentials against FortiNAC that acts as a RADIUS server, the FortiGate GUI and CLI returns an <i>invalid secret for the server</i> error.</p> <p>This error is expected when the FortiGate acts as the direct RADIUS client to the FortiNAC RADIUS server due to a change in how FortiGate handles RADIUS protocol in these versions. However, the end-to-end integration for the clients behind the FortiGate and FortiNAC is not impacted.</p> <p>Workaround: confirm the connectivity between the end clients and FortiNAC by checking if the clients can still be authorized against the FortiNAC as normal.</p>
1082800	<p>When performing LDAP user searches from the GUI against LDAP servers with a large number of users (more than 100000), FortiGate may experience a performance issue and not operate as expected due to the HTTPSD process consuming too much memory. User may need to stop the HTTPSD process or perform a reboot to recover.</p> <p>Workaround: Perform an LDAP user search using the CLI.</p>
1112718	<p>When RADIUS server has the <code>require-message-authenticator</code> setting disabled, the GUI RADIUS server dialogs <i>Test connectivity</i> and <i>Test user credentials</i> still check for the <code>message-authenticator</code> value and incorrectly fail the test with <i>missing authenticator</i> error message.</p> <pre>config user radius edit <radius server> set require-message-authenticator disable next end</pre> <p>This is only a GUI display issue and the end-to-end integration with RADIUS server should still work.</p> <p>Workaround: user can confirm if the connection to RADIUS server via CLI command</p> <pre>diagnose test authserver radius <server> <method> <user> <password>.</pre>

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.
1082197	VLAN traffic fails to pass through E810-XXV NIC with SFP28 transceiver and 25G speed after enabling DPDK.
1094274	FortiOS becomes unresponsive when sending IPv6 traffic over MLX5 network adapters due to incorrect WQE handling.

WiFi Controller

Bug ID	Description
814541	When there are extra large number of managed FortiAP devices (over 500) and large number of WiFi clients (over 5000), the <i>Managed FortiAPs</i> page and <i>FortiAP Status</i> widget can take a long time to load. This issue does not impact FortiAP operation.
869978	Traffic from VAP interface is not processed by FGT when CapWAP offloading is enabled.
949682	Intermittent traffic disruption observed in cw_acd caused by a rare error condition.
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.
972093	RADIUS accounting data usage is different between the bridge and tunnel VAP.
1050915	On the <i>WiFi & Switch Controller > Managed FortiAPs</i> page, when upgrading more than 30 managed FortiAPs at the same time using the <i>Managed FortiAP</i> page, the GUI may become slow and unresponsive when selecting the firmware. Workaround: Upgrade the FortiAPs in smaller batches of up to 20 devices to avoid performance impacts.
1080094	Offline station data consumes excessive memory when the sta-offline-cleanup or max-sta-offline settings are not configured.
1083395	In an HA environment with FortiAPs managed by primary FortiGate, the secondary FortiGate GUI <i>Managed FortiAP</i> page may show the FortiAP status as offline if the FortiAP traffic is not routed through the secondary FortiGate. This is only a GUI issue and does not impact FortiAP operation.

ZTNA

Bug ID	Description
819987	SMB drive mapping made through a ZTNA access proxy is inaccessible after rebooting.
1020084	Health check on the ZTNA realserver does not work as expected if a blackhole route is added to the realserver address.

Built-in AV Engine

AV Engine 7.00035 is released as the built-in AV Engine. Refer to the [AV Engine Release Notes](#) for information.

Built-in IPS Engine

IPS Engine 7.00559 is released as the built-in IPS Engine. Refer to the [IPS Engine Release Notes](#) for information.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

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

Open source XenServer limitations

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

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.

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



www.fortinet.com

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