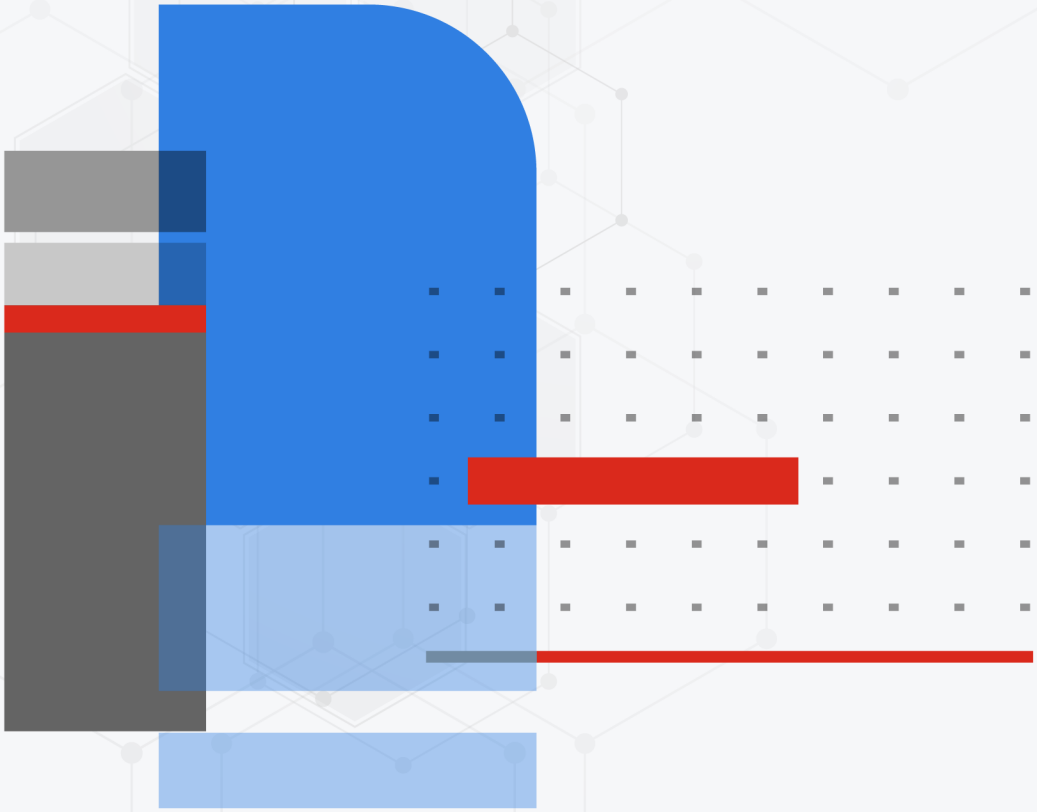
Release Notes

FortiOS 7.4.6



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 11, 2025
FortiOS 7.4.6 Release Notes
01-746-1084734-20250611

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-12-12	Initial release.
2024-12-16	Updated Resolved issues on page 28 and Known issues on page 36.
2024-12-18	Updated Special notices on page 9.
2024-12-19	Updated Introduction and supported models on page 7 and Fortinet Security Fabric upgrade on page 16.
2024-12-20	Updated Resolved issues on page 28 and Known issues on page 36.
2025-01-02	Updated Resolved issues on page 28 and Known issues on page 36.
2025-01-03	Updated Policies that use an interface show missing or empty values after an upgrade on page 22.
2025-01-20	Updated Resolved issues on page 28 and Known issues on page 36.
2025-01-27	Updated Managed FortiSwitch do not permit empty passwords for administrator accounts on page 21.
2025-02-05	Updated Resolved issues on page 28 and Known issues on page 36.
2025-02-18	Updated New features or enhancements on page 13, Resolved issues on page 28, and Known issues on page 36.
2025-03-03	Updated Known issues on page 36.
2025-03-05	Updated Known issues on page 36.
2025-03-10	Updated Resolved issues on page 28 and Known issues on page 36.
2025-03-17	Updated Resolved issues on page 28 and Known issues on page 36.
2025-03-31	Updated Known issues on page 36.
2025-04-14	Updated Resolved issues on page 28 and Known issues on page 36.
2025-04-29	Updated Resolved issues on page 28 and Known issues on page 36.
2025-05-12	Updated Resolved issues on page 28 and Known issues on page 36.
2025-05-27	Updated Resolved issues on page 28 and Known issues on page 36.
2025-06-04	Updated Changes in default behavior on page 11 and Known issues on page 36.
2025-06-05	Updated Known issues on page 36.
2025-06-09	Updated Resolved issues on page 28 and Known issues on page 36.
2025-06-11	Updated Changes in default behavior on page 11 and Resolved issues on page 28.

Introduction and supported models

This guide provides release information for FortiOS 7.4.6 build 2726.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.4.6 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
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 7.4.6. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 2726.

FG-6000F	is released on build 8336.
FG-7000E	is released on build 8336.
FG-7000F	is released on build 8336.

Special notices

Hyperscale incompatibilities and limitations

See Hyperscale firewall incompatibilities and limitations in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 7.4.6 features.

FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 7.4.6 features.

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

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`).

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 7.4.6, 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.

1020808	Certificate Rekeying During Re-enrollment
	Previously, the FortiOS EST protocol implementation reused the same private key for certificate renewal. Starting with version 7.4.6, FortiOS allows certificates generated through the EST protocol to undergo a rekey process during re-enrollment, enhancing security and flexibility.
	A new option has been added to specify whether to use an existing key or generate a new one, with the default now set to create a new one.
	`config vpn certificate local`
	`edit <name>`
	`set est-regeneration-method {create-new-key | use-existing-key}`
	`next`
	`end`

1063233	The BIOS security level is updated from levels 0/1/2 to levels Low and High. Level High will correspond to previous behaviors in level 2, and level Low will correspond to behaviors in level 1. BIOS that still uses levels 0 will now behave like level 1/Low.
1093412	The `sess-sync` feature does not work after enabling encryption. Previously the `sess-sync` feature was not affected when encryption was enabled, but the `sess-sync` traffic was not encrypted.

Changes in table size

Bug ID	Description
1070828	On FortiGate, increase maximum number of configurable IPv6 tunnels from 4 to 32.

New features or enhancements

More detailed information is available in the New Features Guide.

LAN Edge

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

Feature ID	Description
952927	The FOS WiFi controller has been enhanced to support both TCP and TLS protocols for Radius communication during the 802.1X authentication of WiFi stations. This solves the problem for customers who require stable and secure authentication processes, particularly in complex network infrastructures where UDP might not be sufficient.
1078491	The FortiOS WiFi controller now supports pushing RADIUS server settings using TCP or TLS protocols to FortiAP's for Local-Bridge mode Captive Portal SSIDs, enhancing security and reliability compared to the previous UDP-only support.

Operational Technology

See Operational Technology in the New Features Guide for more information.

Feature ID	Description
1000362	FortiGate Rugged 70F and FortiGate Rugged 70F-3G4G include a general purpose input output (GPIO) module, also known as, a digital I/O (DIO) module. Added support for SNMP traps or notifications and automation stitch notifications when DIO module alarm functionality is activated, that is, when a change in any digital input is detected and the digital output is activated. Notification support depends on previously configured `config system digital-io` and `execute digital-io set-output` settings prior to event notification. SNMP and automation stitch notifications can be configured using these CLI commands on FortiGate Rugged 70F and FortiGate Rugged 70F-3G4G devices only: • For automation stitch support, in `config system automation-condition` added new options `set condition-type input` and `set input-state open | close` • For SNMP support, in `config system snmp community` added new option `set events dio`

Feature ID	Description
1075708	FortiGate Rugged 70F and FortiGate Rugged 70F-3G4G include a general purpose input output (GPIO) module, also known as, a digital I/O (DIO) module. This module is used for activating a digital output when triggered by a change in any digital input. For example, when a switch change from open to closed or a voltage change from low to high is detected, then a digital output is activated. In this example, the digital input is connected to a cabinet door and the output is connected to a buzzer. Added CLI support for configuring the above DIO alarm functionality on FortiGate Rugged 70F and FortiGate Rugged 70F-3G4G devices only: • `config system digital-io`: command to configure input mode • `execute digital-io set-output`: command to configure output mode • `diag sys digital-io state`: command to check current input/output status

SD-WAN

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

Feature ID	Description
1071495	Users can now specify an SD-WAN zone as an interface in the following policies: • Local-in policy • DoS policy • Interface policy • Multicast policy • TTL policy • Central SNAT map This update simplifies policy management and boosts operational efficiency.

System

See System in the New Features Guide for more information.

Feature ID	Description
954888	FortiGate A-P HA cluster now supports sharing a single FortiGuard service license for both cluster units for the following models and their variants: 40F, 60F, 70F, 80F, and 100F.

Feature ID	Description

983862	Dynamic Source Port for GTP-U Packets is now supported on NP7 Platforms. This feature establishes two sessions for bidirectional traffic, regardless of the source ports. By reducing the number of sessions, it significantly decreases memory usage. This is particularly beneficial for customers handling high volumes of GTP-U traffic, offering a memory-efficient and streamlined solution.
	`config system global`
	`    set gtpu-dynamic-source-port {enable | disable}`
	`end`

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 16 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 7.4.6 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)	• 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
17. FortiMonitor

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.4.6. When Security Fabric is enabled in FortiOS 7.4.6, all FortiGate devices must be running FortiOS 7.4.6.

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 7.4.6:

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 7.4.6 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

`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, 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. 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.

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

Product integration and support

The following table lists FortiOS 7.4.6 product integration and support information:

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 0319 and later (needed for FSSO agent support OU in group filters)
	  • Windows Server 2022 Standard
	  • Windows Server 2022 Datacenter
	  • Windows Server 2019 Standard
	  • Windows Server 2019 Datacenter
	  • Windows Server 2019 Core
	  • Windows Server 2016 Datacenter
	  • Windows Server 2016 Standard
	  • Windows Server 2016 Core
	  • Windows Server 2012 Standard
	  • Windows Server 2012 R2 Standard
	  • Windows Server 2012 Core
	  • Novell eDirectory 8.8

AV Engine	• 7.00035
IPS Engine	• 7.00559

See also:

- Virtualization environments on page 24
- Language support on page 24
- SSL VPN support on page 25
- FortiExtender modem firmware compatibility on page 25

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	✓
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 7.4.6. To inquire about a particular bug, please contact Customer Service & Support.

Anti Spam

Bug ID	Description
1050805	Client termination occurs during email processing when inserting antispam tags in emails lacking body sections or delimiters, particularly with multipart base64 encoded data.

Anti Virus

Bug ID	Description
1058701	On FortiGate, the `av-mem-limit` does not work as expected when `set av-failopen pass` configured due to a memory usage issue.
1078882	The scanunit tries to scan with no payload, resulting in an error message from FortiNDR and generating an error on FortiGate.

Data Loss Prevention

Bug ID	Description
984784	When a DLP profile is set to MAPI, there is a slow connection between Outlook and the Exchange server.

Explicit Proxy

Bug ID	Description
1015722	WAD auto-tuning is not working ideally for various cases, resulting in throughput for single file downloads not reaching the ideal speed when `tcp-window-type` is set to `auto-tuning`.
1076642	Unable to load pages with cloudflare protected websites with `auth` enabled, if Auth scheme is set to Form-Based in explicit proxy.

Firewall

Bug ID	Description
1007029	On FortiGate, connections are disrupted between client email exchange servers and a virtual server when HTTP2 support is enabled.
1007566	When the FortiGate has thousands of addresses and hundreds address groups, the GUI can take a few minutes to search for a specific address inside the address group dialog.
1050906	Under heavy network traffic, the Netflow session cache for sampled traffic quickly reaches the hardcoded RAM limit, causing the sFlow daemon to shut down.
1059989	Modifying the shaping profile, whether it is assigned to an interface or not, results in IPsec tunnels going down.
1060452	FortiGate in policy-based mode showing the incorrect policy ID in forward traffic logs.
1068393	Incorrect matching of zones and SD-WAN zones occurs where interfaces do not exist.

FortiGate 6000 and 7000 platforms

Bug ID	Description
1016439	Enabling or disabling a vcluster causes some backup routes (proto = 20) to be lost when a routing table has a significant amount of routes (over 10000 routes).
1056894	On the FortiGate 6000 platform, IPv6 VRF routing tables appear under the new and old FPC primary units when the primary FPC slot is changed.
1081015, 1086953	ISDB updates fail during FortiGate database synchronization attempts due to missing FFDB package handling and failed temporary file transfers.

GUI

Bug ID	Description
1033626	During a firewall failover, multicast traffic is not forwarded within an appropriate time frame.
1035356	The WAN interface is accessible in the GUI under certain interface configurations even though it is not allowed in the configuration file.
1092489	The `config system fortiguard > fortiguard-anycast` setting was changed to automatically disable when the FortiGuard page is shown on GUI.

HA

Bug ID	Description
1050162	The `auth-pwd` and `private-key` error after upgrading from B2662 when `private-data-encryption` enabled.
1084662	Inconsistent FFDB signed statuses occur on secondary blades when a signature file fails to synchronize during HA database sync events.

Hyperscale

Bug ID	Description
1047362	Decoding errors occur when Netflow data packets contain certain values for each NPU but lack corresponding templates for proper interpretation.
1090234	The system crashes due to a null pointer dereference when the hairpin session query function accesses uninitialized pointers after ICMP rate control functions were incorrectly added.

Intrusion Prevention

Bug ID	Description
1016531	FortiGate encounters a memory usage issue in the IPS engine when `av-failopen` is set to `pass`.
1090134	IPS engine re-initialization after receiving a threat feed update from an external resource.

IPsec VPN

Bug ID	Description
1018749	IPsec inserted SA's are not deleted successfully after flushing all tunnels.
1061925	IPsec tunnels are flushed when unrelated changes are made in the system.
1073995	Authentication for native iOS IPsec VPN user with FortiToken 2FA does not work as expected.
1081951	FortiGate encounters a steadily increasing IKED memory usage issue after upgrading to version 7.4.5.

Log & Report

Bug ID	Description
1083537, 1088358	Serial numbers are lost in FortiAnalyzer when high availability information packets lack serial number data, causing cached entries to expire and be removed.

Proxy

Bug ID	Description
916178	FortiGate encounters an issue with the WAD daemon when deep inspection and SSL exemption are enabled while visiting a server with an expired certificate.
1018780	FortiGate encounters a memory usage issue caused by the WAD process after an upgrade.
1020828	An HTTP2 stream issue causes an error condition in the WAD.
1023127	WAD crashes on the FortiGates with signal 11.
1039006	Some websites cannot open subpages when the HTTP2 header value exceeds 16MB.
1047441	On FortiGate, the WAD process may not work as expected with H2 traffic when creating UTM logs.
1048296	FortiGate experiences an HTTP2 framing error when accessing websites using proxy mode with deep inspection configured due to a frame sizing issue in the WAD process.
1054835	HTTP/2 large file transfers are slow when IPS, APP, or SSL inspect-all is enabled due to excessive buffering during traffic forwarding.
1064758	The *Protocol* option tcp window size in a proxy policy does not work as expected.

Bug ID	Description
1067942	An error occurs in the WAD process when DoH traffic is sent to a transparent proxy after enabling HTTP policy redirect, and without having a transparent proxy configured.
1078385	FortiGate experiences a memory usage issue in the WAD process when sending AVDBs updates from the config daemon to workers.
1088385	FortiGate intermittently loses the FortiAnalyzer serial number and is required to verify again the FortiAnalyzer serial number and certificate.

REST API

Bug ID	Description
989677	Update JavaScripts to the latest Long Term Support version.
1084335	Existing API key may not work as expected with a 403 error *wrong vdom* displaying after upgrading to FortiOS version 7.4.5. **Workaround**: After upgrading to version 7.4.5, create a new API user and use the new API key.

Routing

Bug ID	Description
1057474	FortiGate does not generate a PIM register after stopping and starting a multicast stream.
1069060	Routes are not displayed correctly when the BGP configuration is in a specific order.
1085271	An IGMP membership report with a `0.0.0.0` source does not work as expected in kernel 4.19.13.

Security Fabric

Bug ID	Description
1082980	The AZURE type dynamic firewall address takes longer than normal to resolve itself, even with the correct filter value in the robot test bed.

SSL VPN

Bug ID	Description
998219	Internet services cannot be used (IPv4 and IPv6) as destination in SSL VPN policies with dual stack enabled.
1046374	An unauthenticated user mismatch occurs with the user.
1077157	FortiGate sends out expired server certificate for a given SSL VPN realm, even when the certificate configured in `virtual-host-server-cert` has been updated.

Switch Controller

Bug ID	Description
1063144	FortiGate 101F default FortiLink interface has no members.
1064814	Random CPU spikes and for cu_acd process.
1077496	High CPU utilization occurs when flpold/flcfgd processes mishandle socket messages during WAD operations due to incomplete or corrupted data.

System

Bug ID	Description
960707	Egress shaping does not work on NP when applied on the WAN interface.
983467	FortiGate 60F and 61F models may experience a memory usage issue during a FortiGuard update due to the ips-helper process. This can cause the FortiGate to go into conserve mode if there is not enough free memory.
986926	On the FortiGate 90xG models, the ULL interfaces for x5 - x8 are down after being set to 25G speed.
1013010	On some FortiGates, 25 GB transceivers are displayed as 10 GB transceivers in the `get system interface transceiver` command.
1015698	On FortiGate 601F models, the X5 - X8 interfaces with 25G SFP28 DAC are down after upgrading to version 7.4.4 or later.

Bug ID	Description
1020921	When configuring an SNMP trusted host that matches the management *Admin* trusted host subnet, the GUI may give an incorrect warning that the current SNMP trusted host does not match. This is purely a GUI display issue and does not impact the actual SNMP traffic.
1024737	On FortiGate, when `set ull-port-mode` is set to 25G, ports x5-x8 show a status of DOWN.
1025114	Insufficient free memory on entry-level FortiGate devices with 2 GB RAM may cause unexpected behavior in the IPS engine.
1032018	The SFP+ port LED does not illuminate and displays a speed 10Mbps even though the link status up and speed is set to 1000Mbps.
1032602	FortiGate encounters a memory usage issue on DNS proxy, resulting in FortiGate going into conserve mode.
1039956	FortiGate 601F port x6 keeps flapping after upgrade.
1042577	FortiGate does not detect transceivers and interface X8 not coming up after upgrade.
1050883	Backing up a configuration using SFTP with the domain username does not work when characters @ and \ are in the username.
1056174	FortiOS processes packets on a non-active port of a redundant link.
1058256	On FortiGate, interfaces with DAC cables remain down after upgrading to version 7.4.4.
1062698	DNSproxy CPU is running high.
1068150	The DHCP relay uses the wrong interface to send DHCP offer packets to the client.
1075032	NP7 offloaded traffic continues to use old gateway's MAC address when receiving packets with TTL=1 after a gateway change.
1075585	Shared copper WAN1 and WAN2 ports remain down when the interface speed is set to `100full`.
920320, 1029447	FortiGate encounters increasing `Rx_CRC_Errors` on SFP ports on the NP6 platform when an Ethernet frame contains carrier extension symbols to Cisco devices.

Upgrade

Bug ID	Description
1106072	The image file transfer between FortiManager and FortiGate may not work as expected when transferred by the FGFM tunnel.

User & Authentication

Bug ID	Description
1020808	Use new keys for certificate renewal via EST server.
1072870	FortiGate initiates LDAPS sessions that do not respect the `ssl-min-proto-version` option set under the `config system global` command.

VM

Bug ID	Description
972520	The FortiGate-AWS HA secondary `awsd debug` result prints raw HTML content.
1072695	The VLAN interface is not reachable on a FortiGate VM running KVM with Intel 10G NIC (10GB Ethernet card).

WiFi Controller

Bug ID	Description
1049471	On FortiGate 90G and 120G models, traffic is dropped due to the MAC address of the VAP interface being updated with the old MAC address when HA is enabled.
1062730	On FortiGate, the `set max-clients` feature does not work as expected and allows more clients to connect than the maximum value configured.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
1054998	FortiOS 7.4.6 is no longer vulnerable to the following CVE Reference: • CVE-2024-3596
1066080	FortiOS7.4.6 is no longer vulnerable to the following CVE Reference: • CVE-2025-22251

Known issues

Known issues are organized into the following categories:

- New known issues on page 36
- Existing known issues on page 38

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 7.4.6.

Firewall

Bug ID	Description
1114635	Not able to filter address object by CIDR notation.

FortiGate 6000 and 7000 platforms

Bug ID	Description
1092728	On FortiGate 6000 and 7000 platforms, fragmented IPv6 traffic is randomly dropped.
1109601	Graceful upgrades fail when hatalk daemon restarts, disrupting slbha state synchronization during FortiOS version transitions.

GUI

Bug ID	Description
1114549	Authorization of FEXT devices fails when using the FortiGate GUI.

Security Fabric

Bug ID	Description
1150382	Security profile names containing two forward slashes (//) cause the webpage to become unresponsive when attempting to edit.

Switch Controller

Bug ID	Description
1114032	GUI Switch port interface keeps loading with https 500 error on monitor/switch-controller/managed-switch/tx-rx.

System

Bug ID	Description
1069208	If the DHCP offer contains padding when DHCP relay is used, the DHCP relay deletes the padding before relaying the packet.
1114298	FortiGate Cloud remote login triggers 2 admin login events (1 successful and 1 unsuccessful for PKI admin).
1148214	Interface page in the GUI is not displayed.

Upgrade

Bug ID	Description
1104649	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. **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.
1114550	FortiExtender shows as offline after upgrading FGT from 7.4.5 to 7.4.6. **Workaround**: Reboot FortiExtender manually.

User & Authentication

Bug ID	Description

1112718	When RADIUS server has the `require-message-authenticator` setting disabled, the GUI RADIUS server dialogs *Test connectivity* and *Test user credentials* still check for the `message-authenticator` value and incorrectly fail the test with *missing authenticator* error message.
	`config user radius`
	`edit <radius server>`
	`set require-message-authenticator disable`
	`next`
	`end`
	This is only a GUI display issue and the end-to-end integration with RADIUS server should still work.
	Workaround: user can confirm if the connection to RADIUS server via CLI command `diagnose test authserver radius <server> <method> <user> <password>`.

WiFi Controller

Bug ID	Description
1083395	In an HA environment with FortiAPs managed by primary FortiGate, the secondary FortiGate GUI *Managed FortiAP* page may show the FortiAP status as offline if the FortiAP traffic is not routed through the secondary FortiGate. This is only a GUI issue and does not impact FortiAP operation.

Existing known issues

The following issues have been identified in a previous version of FortiOS and remain in FortiOS 7.4.6.

Explicit Proxy

Bug ID	Description
1026362	Web pages do not load when `persistent-cookie` is disabled for `session-cookie-based authentication` with *captive-portal*.

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.
994986	The *By Sequence* view in the Firewall policy list may incorrectly show a duplicate implicit deny policy in the middle of the list. This is purely a GUI display issue and does not impact policy operation. The *Interface Pair View* and *Sequence Grouping View* do not have this issue.
1004263	Session counters are not being updated when ASIC offload is enabled on firewall policy. FortiGate GUI is displaying incorrect information in the "Bytes" and "Last Used" columns.
1057080	On the *Firewall Policy* page, search results do not display in an expanded format.

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	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.
1060619	CSF is not working as expected.

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 7000F devices in the cluster it incorrectly changes to the VDOM of the management interfaces added to the `session-sync-dev` command from `mgmt-vdom` to `vsys_ha` and the interfaces stop working as session sync interfaces.

Bug ID	Description
	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.
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 `execute update-now` command.

GUI

Bug ID	Description
853352	When viewing entries in slide-out window of the *Policy & Objects* > *Internet Service Database* page, users cannot scroll down to the end if there are over 100000 entries.
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 *Interface Bandwidth* 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.
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 *Image upgrade failed* 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.
1054041	On FortiGate's in an HA environment, DHCP clients can not get an IPv4 address from the server with vcluster.
1107137	The secondary FortiGate with an HA Reserved Management Interface cannot be accessed using HTTPS after upgrading from version 7.4.3.

Bug ID	Description
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	lpmd 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	After upgrade, event log shows `logdesc="IPSA driver update failed" msg="Fail to update IPSA driver status!"`. This issue only affects physical FortiGate models with the following IPS engine versions: • IPS Engine version: 7.550 - 7.567 • IPS Engine version: 7.1019 - 7.1039 To determine the IPS Engine versions, use the command: `get sys fortiguard-service status | grep 'IPS/FlowAV Engine'` **Workaround**: Power off the FortiGate. Wait 30 seconds, and then power on the FortiGate. **Note**: Reboot using the CLI is not an effective workaround and requires additional steps. After executing `exec shutdown`, unplug the power to the FortiGate. Wait one minute, and the power on the FortiGate.
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.
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 drops the ESP packet.

Log & Report

Bug ID	Description
1113588	FortiGate prompts error *"Fetching data from Disk is taking longer than expected. Suggest trying a different log source or check the availability of Disk."* when viewing logs for the last 7 days from disk or FortiAnalyzer.
1148101	Logs are not uploaded to FortiAnalyzer.
1045253	Log items cannot be created and sent to FortiGate Cloud log server when confirm queue becomes full.

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 `diagnose ip rtcache list` 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 `interface-select-method` command for nearly all local-out traffic. For example:
	`config system fortiguard`
	`  set interface-select-method specify`
	`  set interface "wan1"`
	`end`

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 *Security Fabric* topology does not load properly and displays a *Failed to load Topology Results* error.
1076439	Security fabric Asset Identity Center shows "Failed to load user device store data".
1149817	FortiLink Tier2 switch is directly connected to FortiGate on Security Fabric - Physical Topology 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
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	On the NP7 platform, setting the interface configuration using set inbandwidth <x> or set outbandwidth <x> commands stops traffic flow.
	Workaround: Change the NP7 `default-qos-type` setting from `shaping` to `policing`. This requires a restart of the device for the configuration to take effect:
	`config system npu`
	`  set default-qos-type policing`
	`end`

912383	FGR-70F and FGR-70F-3G4G failed to perform regular reboot process (using `execute reboot` command) with an SD card inserted.
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 using the `execute shutdown` command, the system automatically boots up again.
1048496	On FortiGate, the `snmp` 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.
1078541	The FortiFirewall 2600F model may become stuck after a fresh image burn. Upgrading from a previous version stills works. **Workaround**: power cycle the unit.
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 `config sfp-dsl enable` and vectoring under interface.
1113436	Connectivity issue while using offloading NP7 QinQ 802.1AD 802.1Q over LACP.
1140755	Unable to delete software switch interface.
1117005	FortiGate encounters a CPU usage issue. **Workaround**: Disable IPsec phase1 npu-offload.

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	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 *invalid secret for the server* error. 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. **Workaround**: confirm the connectivity between the end clients and FortiNAC by checking if the clients can still be authorized against the FortiNAC as normal.
1082800	When performing LDAP user searches from the GUI against LDAP servers with a large number of users (more than 100000), FortiGate may experience a performance issue and not operate as expected due to the HTTPSD process consuming too much memory. User may need to stop the HTTPSD process or perform a reboot to recover. **Workaround**: Perform an LDAP user search using the CLI.

VM

Bug ID	Description
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 *Managed FortiAPs* page and *FortiAP Status* 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.

Bug ID	Description
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 *WiFi & Switch Controller* > *Managed FortiAPs* page, when upgrading more than 30 managed FortiAPs at the same time using the *Managed FortiAP* 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.

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