Release Notes

FortiOS 7.4.3

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

March 11, 2024
FortiOS 7.4.3 Release Notes
01-743-986078-20240311

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-02-07	Initial release.
2024-02-12	Updated Resolved issues on page 24 and Known issues on page 25.
2024-02-13	Updated Known issues on page 25 and Remote access with write rights through FortiGate Cloud on page 10.
2024-02-20	Updated Known issues on page 25.
2024-02-23	Added BIOS-level signature and file integrity checking during downgrade on page 17.
2024-02-26	Updated Known issues on page 25.
2024-02-28	Added FortiAP-W2 models may experience bootup failure during automatic firmware and federated upgrade process if they are powered by a managed FortiSwitch's PoE port on page 11.
2024-03-04	Updated Known issues on page 25.
2024-03-11	Updated Known issues on page 25.

Introduction and supported models

This guide provides release information for FortiOS 7.4.3 build 2573.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.4.3 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-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100F, FG-101F, 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-81F-2R, 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-3980E, FFW-4200F, FFW-4400F, FFW-4401F, FFW-VM64, FFW-VM64-KVM
FortiGate VM	FG-ARM64-AWS, FG-ARM64-AZURE, FG-ARM64-GCP, FG-ARM64-KVM, FG-ARM64-OCI, FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VM64-XEN

FortiGate 6000 and 7000 support

FortiOS 7.4.3 supports the following FG-6000F, FG-7000E, and FG-7000F models:

FG-6000F	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

See Hyperscale firewall incompatibilities and limitations in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 7.4.3 features.

FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 7.4.3 features.

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

Remove OCVPN support

The IPsec-based OCVPN service has been discontinued and licenses for it can no longer be purchased as of FortiOS 7.4.0. GUI, CLI, and license verification support for OCVPN has been removed from FortiOS. Upon upgrade, all IPsec phase 1 and phase 2 configurations, firewall policies, and routing configuration previously generated by the OCVPN service will remain. Alternative solutions for OCVPN are the Fabric Overlay Orchestrator in FortiOS 7.2.4 and later, and the SD-WAN overlay templates in FortiManager 7.2.0 and later.

Remove WTP profiles for older FortiAP models

Support for WTP profiles has been removed for FortiAP B, C, and D series models, and FortiAP-S models in FortiOS 7.4.0 and later. These models can no longer be managed or configured by the FortiGate wireless controller. When one of these models tries to discover the FortiGate, the FortiGate's event log includes a message that the FortiGate's wireless controller `can not be managed because it is not supported`.

IP pools and VIPs are now considered local addresses

In FortiOS 7.4.1 and later, all IP addresses used as IP pools and VIPs are now considered local IP addresses if responding to ARP requests on these external IP addresses is enabled (`set arp-reply enable`, by default). For these cases, the FortiGate is considered a destination for those IP addresses and can receive reply traffic at the application layer.

Previously in FortiOS 7.4.0, this was not the case. For details on the history of the behavior changes for IP pools and VIPs, and for issues and their workarounds for the affected FortiOS versions, see Technical Tip: IP pool and virtual IP behavior changes in FortiOS 6.4, 7.0, 7.2, and 7.4.

Remove support for SHA-1 certificate used for web management interface (GUI)

In FortiOS 7.4.0 and later, users should use the built-in Fortinet_GUI_Server certificate or SHA-256 and higher certificates for the web management interface. For example:

```
config system global
    set admin-server-cert Fortinet_GUI_Server
end
```

Number of configurable DDNS entries

Starting in FortiOS 7.4.0, the number of DDNS entries that can be configured is restricted by table size. The limits are 16, 32, and 64 entries for lentry-level, mid-range, and high-end FortiGate models respectively.

After upgrading to FortiOS 7.4.0 or later, any already configured DDNS entries that exceed the limit for the FortiGate model in use will be deleted. For example, if a user has 20 DDNS entries before upgrading to 7.4.0 and is using a entry-level FortiGate model, the last four DDNS entries will be deleted after upgrading.

In such instances where the number of DDNS entries exceeds the supported limit for the FortiGate model in use, users have the option to upgrade their FortiGate model to one that supports a higher number of DDNS entries.

FortiGate models with 2 GB RAM can be a Security Fabric root

A Security Fabric topology is a tree topology consisting of a FortiGate root device and downstream devices within the mid-tier part of the tree or downstream (leaf) devices at the lowest point of the tree.

As part of improvements to reducing memory usage on FortiGate models with 2 GB RAM, FortiOS 7.4.2 and later can authorize up to five devices when serving as a Fabric root.

The affected models are the FortiGate 40F, 60E, 60F, 80E, and 90E series devices and their variants.

To confirm if your FortiGate model has 2 GB RAM, enter `diagnose hardware sysinfo conserve` in the CLI and check that the total RAM value is below 2000 MB (1000 MB = 1 GB).

Admin and super_admin administrators cannot log in after a prof_admin VDOM administrator restores the VDOM configuration and reboots the FortiGate

When a VDOM administrator using the prof_admin profile is used to restore a VDOM configuration and then reboot the FortiGate, an administrator using the super_admin profile (including the default admin administrator) cannot log in to the FortiGate.

Therefore, in FortiOS 7.4.1, a prof_admin VDOM administrator should not be used to restore a VDOM configuration (FortiOS 7.4.2 and later are not affected).

Workarounds:

1. If a prof_admin VDOM administrator has already been used to restore a VDOM configuration, then **do not reboot**. Instead, log in using a super_admin administrator (such as default admin), back up the full configuration, and restore the full configuration. After the full configuration restore and reboot, super_admin administrators will continue to have the ability to log into the FortiGate.

   ⚠ After this workaround is done, the FortiGate is **still susceptible to the issue** if the backup and restore is performed again by the prof_admin VDOM administrator. A FortiOS firmware upgrade with this issue resolved will be required to fully resolve this issue.

2. To recover super_admin access after having restored a VDOM configuration and performing a FortiGate reboot, power off the device and boot up the FortiGate from the backup partition using console access.

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.

Remote access with write rights through FortiGate Cloud

Remote access with read and write rights through FortiGate Cloud now requires a paid FortiGate Cloud subscription. The FortiGate can still be accessed in a read-only state with the free tier of FortiGate Cloud. Alternatively, you can access your FortiGate through its web interface.

Please contact your Fortinet Sales/Partner for details on purchasing a FortiGate Cloud Service subscription license for your FortiGate device.

For more information see the FortiGate Cloud feature comparison and FortiGate Cloud Administration guide FAQ.

FortiGuard Web Filtering Category v10 update

Fortinet has updated its web filtering categories to v10, which includes two new URL categories for AI chat and cryptocurrency websites. To use the new categories, customers must upgrade their Fortinet products to one of the versions below:

- FortiManager - Fixed in 6.0.12, 6.2.9, 6.4.7, 7.0.2, 7.2.0, 7.4.0.
- FortiOS - Fixed in 7.2.7 and 7.4.1.
- FortiClient - Fixed in Windows 7.2.3, macOS 7.2.3, Linux 7.2.3.
- FortiClient EMS - Fixed in 7.2.1.
- FortiMail - Fixed in 7.0.7, 7.2.5, 7.4.1.
- FortiProxy - Fixed in 7.4.1.

Please read the following CSB for more information to caveats on the usage in FortiManager and FortiOS: https://support.fortinet.com/Information/Bulletin.aspx

FortiAP-W2 models may experience bootup failure during automatic firmware and federated upgrade process if they are powered by a managed FortiSwitch's PoE port

Disable automatic firmware upgrades and the federated upgrade feature if you have FortiAP-W2 devices that are exclusively powered by a PoE port from a FortiGate or FortiSwitch.

The federated upgrade feature starts the upgrades of managed FortiSwitch and FortiAP devices start at approximately the same time. Some FortiAP-W2 devices take a longer time to upgrade than the FortiSwitch devices. When the FortiSwitch finishes upgrading, it reboots, and can disrupt the PoE power to the FortiAP devices. If a FortiAP device is still upgrading when the power is disrupted, it can cause the FortiAP device to experience a bootup failure.

Both automatic firmware upgrade and manually triggering federated upgrade can cause this issue.

For more information about federated upgrade and automatic firmware upgrades, see Upgrading all device firmware by following the upgrade path (federated update) and Enabling automatic firmware updates.

To disable automatic upgrade:

```
config system fortiguard
    set auto-firmware-upgrade disable
end
```

CLI system permissions

Starting in FortiOS 7.4.2, the usage of CLI diagnostic commands (`cli-diagnose`), previously named `system-diagnostics`, is disabled by default, with the exception of super_admin profile users. Users can now exercise more granular control over the CLI commands. See CLI system permissions for more information.

When the user upgrades to FortiOS 7.4.2 or later, the following settings for CLI options will be applied, irrespective of whether `system-diagnostics` was enabled or disabled in FortiOS 7.4.1 or earlier.

CLI option	Status
`cli-diagnose`	Disabled
`cli-get`	Enabled
`cli-show`	Enabled
`cli-exec`	Enabled
`cli-config`	Enabled

To enable permission to run CLI diagnostic commands after upgrading:

```
config system accprofile
    edit <name>
        set cli-diagnose enable
    next
end
```

Many diagnostic commands have privileged access. As a result, using them could unintentionally grant unexpected access or cause serious problems, so understanding the risks involved is crucial.

Upgrade information

Supported upgrade path information is available on the Fortinet Customer Service & Support site.

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

FortiAnalyzer	• 7.4.2
FortiManager	• 7.4.2
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. Managed FortiExtender devices
4. FortiGate 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
18. FortiPolicy

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.4.3. When Security Fabric is enabled in FortiOS 7.4.3, all FortiGate devices must be running FortiOS 7.4.3.

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 7.4.3:

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 7.4.3 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, go to *Monitor > Configuration Sync Monitor* 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

BIOS-level signature and file integrity checking during downgrade

When downgrading to a version of FortiOS prior to 6.4.13, 7.0.12, and 7.2.5 that does not support BIOS-level signature and file integrity check during bootup, the following steps should be taken if the BIOS version of the FortiGate matches the following versions:

- 6000100 or greater
- 5000100 or greater

To downgrade or upgrade to or from a version that does not support BIOS-level signature and file integrity check during bootup:

1. If the current security level is 2, change the security level to 0. This issue does not affect security level 1 or below.
2. Downgrade to the desired FortiOS firmware version.
3. If upgrading back to 6.4.13, 7.0.12, 7.2.5, 7.4.0, or later, ensure that the security level is set to 0.
4. Upgrade to the desired FortiOS firmware version.
5. Change the security level back to 2.

To verify the BIOS version:

The BIOS version is displayed during bootup:

```
Please stand by while rebooting the system.
Restarting system
FortiGate-1001F (13:13-05.16.2023)
Ver:06000100
```

To verify the security level:

```
# get system status
Version: FortiGate-VM64 v7.4.2,build2571,231219 (GA.F)
First GA patch build date: 230509
Security Level: 1
```

To change the security level:

1. Connect to the console port of the FortiGate.
2. Reboot the FortiGate (`execute reboot`) and enter the BIOS menu.
3. Press [`I`] to enter the *System Information* menu
4. Press [`U`] to enter the *Set security level* menu
5. Enter the required security level.
6. Continue to boot the device.

Product integration and support

The following table lists FortiOS 7.4.3 product integration and support information:

Web browsers	• Microsoft Edge 112 • Mozilla Firefox version 113 • Google Chrome version 113 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 112 • Mozilla Firefox version 113 • Google Chrome version 113 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 0314 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	• 7.00021
IPS Engine	• 7.00524

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	• 8.2 Express Edition, CU1
Linux KVM	• Ubuntu 22.04.3 LTS • Red Hat Enterprise Linux release 8.4 • 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 113 Google Chrome version 112
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 113 Google Chrome version 112
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 113 Google Chrome version 112
macOS Ventura 13.1	Apple Safari version 16 Mozilla Firefox version 103 Google Chrome version 111
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

FortiExtender modem firmware compatibility

The following table lists the modem firmware file name and version for each FortiExtender model and its compatible geographical region.

FortiExtender model	Modem firmware image name	Modem firmware file on Support site	Geographical region
FEX-101F-AM	FEM_EM06A-22-1-1	FEM_EM06A-22.1.1-build0001.out	America
FEX-101F-EA	FEM_EM06E-22-01-01	FEM_EM06E-22.1.1-build0001.out	EU
	FEM_EM06E-22.2.2	FEM_EM06E-22.2.2-build0002.out	EU

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

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

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
989429	FortiOS 7.4.3 is no longer vulnerable to the following CVE Reference: • CVE-2024-21762
993323	FortiOS 7.4.3 is no longer vulnerable to the following CVE Reference: • CVE-2024-23113

Known issues

The following issues have been identified in version 7.4.3. To inquire about a particular bug or report a bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
977634	FortiOS *High Security Alert* block page reference URL is incorrect.

Application Control

Bug ID	Description
934197	Selected applications will disappear after searching or filtering for other applications in override.

Firewall

Bug ID	Description
760292	The date in the graph of *Last 7 Days* traffic statistics for the policy is incorrect.
959065	Once a traffic shaper is applied to a traffic shaping firewall policy, the counters should not clear when deleting or creating a traffic shaper.
966466	On an FG-3001F NP7 device, packet loss occurs even on local-in traffic.
981283	NAT64/46 HTTP virtual server does not work as expected in the policy.

FortiGate 6000 and 7000 platforms

Bug ID	Description
781163	*FortiView Sources* page is unable to display historical data from FortiAnalyzer due to *Fail to retrieve FortiView data* error.

Bug ID	Description
787604	Transceiver information in unavailable for FPM/FIM2 ports in the GUI.
790464	Existing ARP entries are removed from all slots when an ARP query of a single slot does not respond.
885205	IPv6 ECMP is not supported for the FortiGate 6000F and 7000E platforms. IPv6 ECMP is supported for the FortiGate 7000F platform.
887946	UTM traffic is blocked by an FGSP configuration with asymmetric routing.
910883	The FortiGate 6000s or 7000s in an FGSP cluster may load balance FTP data sessions to different FPCs or FPMs. This can cause delays while the affected FortiGate 6000 or 7000 re-installs the sessions on the correct FPC or FPM.
911244	FortiGate 7000E IPv6 routes may not be synchronized correctly among FIMs and FPMs.
973407	FIM installed NPU session causes the SSE to get stuck.
978241	FortiGate does not honor worker port partition when SNATing connections using a fixed port range IP pool.

GUI

Bug ID	Description
848660	Read-only administrator may encounter a *Maximum number of monitored interfaces reached* error when viewing an interface bandwidth widget for an interface that does not have the monitor bandwidth feature enabled. **Workaround**: super_admin users can enable the monitor bandwidth feature on the interface first, then the widget can work for read-only administrators.
853352	When viewing entries in slide-out pan of the *Policy & Objects > Internet Service Database* page, users cannot scroll down to the end if there are over 100K entries.
885427	Suggest showing the SFP status information on the faceplate of FGR-60F/60F-3G4G devices.
925388	After updating, the CMDB may not start up properly. This issue causes problems with both the GUI and CLI.
931486	Unexpected behavior in httpsd when the user has a lot of FQDN addresses.
961796	When administrator GUI access (HTTPS) is enabled on SD-WAN member interfaces, the GUI may not be accessible on the SD-WAN interface due to incorrect routing of the response packet. **Workaround**: access the GUI using another internal interface that is not part of an SD-WAN link.
964386	GUI dashboards show all the IPv6 sessions on every VDOM.
966702	List of security profiles it is not displayed correctly in the GUI.
972887	The interface firewall object created automatically is not found by a firewall policy search with IP address.

Bug ID	Description
974988	FortiGate GUI should not show a license expired notification due to an expired device-level FortiManager Cloud license if it still has a valid account-level FortiManager Cloud license (function is not affected).
975403	FortiGate removes the `?` from custom replacement messages.
979508	The *Operation Technology* category cannot be turned on or off from the GUI. The option to enable/disable the *Operational Technology* category on application control profiles when hovering the mouse over the category name is missing. **Workaround**: use the CLI to configure it.
983422	A GTP profile cannot be applied to policy using the GUI. **Workaround**: use the CLI to apply the GTP profile.
989512	When the number of users in the *Firewall User* monitor exceeds 2000, the search bar is no longer be displayed.

HA

Bug ID	Description
971075	The last interface belonging to the management VDOM (not root VDOM) is not displayed when accessing `ha-mgmt-interface`.
1000001	A secondary HA unit may go into conserve mode when joining an HA cluster if the FortiGate's configuration is large.

Hyperscale

Bug ID	Description
817562	NPD/LPMD cannot differentiate the different VRFs, and considers all VRFs as 0.
850252	Restoring a specific VDOM configuration from the GUI does not restore the complete configuration.
896203	The parse error, `NPD-0:NPD PARSE ADDR GRP gmail.com MEMBER ERR`, appears after rebooting the system.
976972	New primary can get stuck on failover with HTTP CC sessions.
977376	FG-4201F has a 10% performance drop during a CPS test case with DoS policy.
975264	Hyperscale should not support threat feed addresses with the negate option.
981918	Hyperscale policy loses the `cgn-log-server-grp` setting with log mode per-mapping when the system reboots.

Intrusion Prevention

Bug ID	Description
782966	IPS sensor GUI shows *All Attributes* in the filter table when IPS filters with default values are selected in the CLI.

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.

1003830	IPsec VPN tunnel phase 2 instability after upgrading to 7.4.2 on the NP6xlite platform.
	Workaround: disable replay detection on the phase 2 interface on both sides of the IPsec VPN:
	`config vpn ipsec phase2-interface`
	`    edit <name>`
	`        set replay disable`
	`    next`
	`end`

Log & Report

Bug ID	Description
960661	FortiAnalyzer report is not available to view for the secondary unit in the HA cluster. **Workaround**: view the report directly in FortiAnalyzer.

Proxy

Bug ID	Description
900546	DNS proxy may resolve with an IPv4 address, even when `pref-dns-result` is set to IPv6, if the IPv4 response comes first and there is no DNS cache.
910678	CPU usage issue in WAD caused by a high number of devices being detected by the device detection feature.
922093	High CPU due to WAD process and disrupted HTTPS connections.
933002	Memory usage issue in WAD caused by a rare error condition.
965966	An error condition occurred in WAD due to heavy HTTP video traffic when using a video filter profile with deep inspection enabled.

REST API

Bug ID	Description
964424	REST API GET `/ips/sensor/{name}` adds extra space to `locations`, `severity`, `protocol`, `os`, and `application` field values.

Routing

Bug ID	Description
903444	The `diagnose ip rtcache list` command is no longer supported in the FortiOS 4.19 kernel.
974921	Configuring the *Set weight* on the route map to *0* in the GUI does not save this setting in the CLI configuration.
984478	The SD-WAN Rules GUI page keeps loading.
989840	Issue with PIM neighborship over an IPSec tunnel with NP offload.

Security Fabric

Bug ID	Description
948322	After deauthorizing a downstream FortiGate from the *System* > *Firmware & Registration* page, the page may appear to be stuck to loading.

Bug ID	Description
	Workaround: perform a full page refresh to allow the page to load again.
966740	Security rating *Last Ran* displays incorrect values.
968585	The automation stitch triggered by the FortiAnalyzer event handler does not work as expected.
972921	The comments are not working as expected in the threat feed list for the domain threat feed.

SSL VPN

Bug ID	Description
951827	SSL VPN client certificate verification failed after importing the VDOM user peer CA certificate into the global VDOM.

Switch Controller

Bug ID	Description
955550	Unexpected behavior in cu_acd and fortilinkd is causing the CPU to handle the majority of the traffic instead of the NPU.
988335	If a user's network has more than 20 MAC addresses in a NAC environment, it is possible for the CAPWAP to come down.

System

Bug ID	Description
907622	GUI is missing DDNS *Domain* text field box when creating a new DDNS entry.
910364	CPU usage issue in miglogd caused by constant updates to the ZTNA tags.
912383	FGR-70F and FGR-70F-3G4G failed to perform regular reboot process (using `execute reboot` command) with an SD card inserted.
921134	GUI is inaccessible when using a SHA1 certificate as `admin-server-cert`.
953692	SNMP stops working when a second server is added. The FortiGate stops answering SNMP requests to both servers.
956697	On NP7 platforms, the FortiGate maybe reboot twice when upgrading to 7.4.2 or restoring a configuration after a factory reset or burn image. This issue does not impact FortiOS functionality.

Bug ID	Description
964465	Administrator with read-write permission for WiFi and read permission for network configuration cannot create SSIDs. **Workaround**: give the administrator read-write permission for network configuration.
968618	After the upgrade to 7.4, the NP7 L2P is dropping packets at the L2TI module.
971404	Session expiration does not get updated for offloaded traffic between a specific host range.
971466	FGR 60F faces packet loss with a Cisco switch directly connected to it.
977231	An error condition occurred in fgfm caused by an out-of-band management configuration.
921604	On the FortiGate 601F, the ports (x7) have no cables attached but the link LEDs are green.

Upgrade

Bug ID	Description
952828	The automatic patch upgrade feature overlooks patch release with the Feature label. Consequentaly, a FortiGate running 7.4.2 GA does not automatically upgrade to 7.4.3 GA. **Workaround**: Manually upgrade to a 7.4 Feature patch on the *System* > *Firmware & Registration* page.

977281	After the FortiGate in an HA environment is upgraded using the Fabric upgrade feature, the GUI might incorrectly show the status *Downgrade to 7.2.X shortly*, even though the upgrade has completed.
	This is only a display issue; the Fabric upgrade will not recur unless it is manually scheduled.
	Workaround: Confirm the Fabric upgrade status to make sure that it is not enabled:
	`config system federated-upgrade`
	`    set status disabled`
	`end`

999324	FortiGate Pay-As-You-Go or On-demand VM versions cannot upload firmware using the *System* > *Firmware & Registration* > *File Upload* page. **Workaround**: Use the *Latest Firmware* or *All Upgrade* page to upgrade the firmware.

User & Authentication

Bug ID	Description
667150	When a remote LDAP user with Two-factor Authentication enabled and Authentication type 'FortiToken' tries to access the internet through firewall authentication, the web page does not receive the FortiToken notification or proceed to authenticate the user.

Bug ID	Description
	Workaround: click the *Continue* button on the authentication page after approving the FortiToken on the mobile device.
884462	NTLM authentication does not work with Chrome.
967146	Upon expiration, the SSL certificate is removed from GUI but not from the CLI.
972391	RADIUS group is not properly displayed as used.
975689	Unable to print with custom guest user print template.
982573	*Dashboard > Assets & Identities* page shows devices and interfaces from all VDOMs.

VM

Bug ID	Description
938382	OpenStack Queens FortiGate VM HA heartbeat on broadcast is not working as expected.
967134	An interrupt distribution issue may cause the CPU load to not be balanced on the FG-VM cores.
977110	Interface disappears after enabling `unicast-status` on HA.
978021	VNI length is zero in the GENEVE header when in FTP passive mode.

Web Filter

Bug ID	Description
634781	Unable to customize replacement message for FortiGuard category in web filter profile.

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	CAPWAP tunnel traffic over tunnel SSID is dropped when offloading is enabled.
883938	Flooded wireless STA traffic seen in L2 tunneled VLAN (FG-1800F).

Bug ID	Description
903922	Physical and logical topology is slow to load when there are a lot of managed FortiAP (over 50). This issue does not impact FortiAP management and operation.
949682	Intermittent traffic disruption observed in cw_acd caused by a rare error condition.
964757	Clients randomly unable to connect to 802.1X SSID when FortiAP has a DTLS policy enabled.
972093	RADIUS accounting data usage is different between the bridge and tunnel VAP.
998578	On FortiGate devices running 7.4.2 or 7.4.3, managed FortiAP-W2 devices might randomly go offline. **Workaround**: Reboot the FortiAP-W2 device, or use version 7.4.1 or earlier on the FortiGate.

ZTNA

Bug ID	Description
819987	SMB drive mapping made through a ZTNA access proxy is inaccessible after rebooting.

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.

FORTINET®

www.fortinet.com