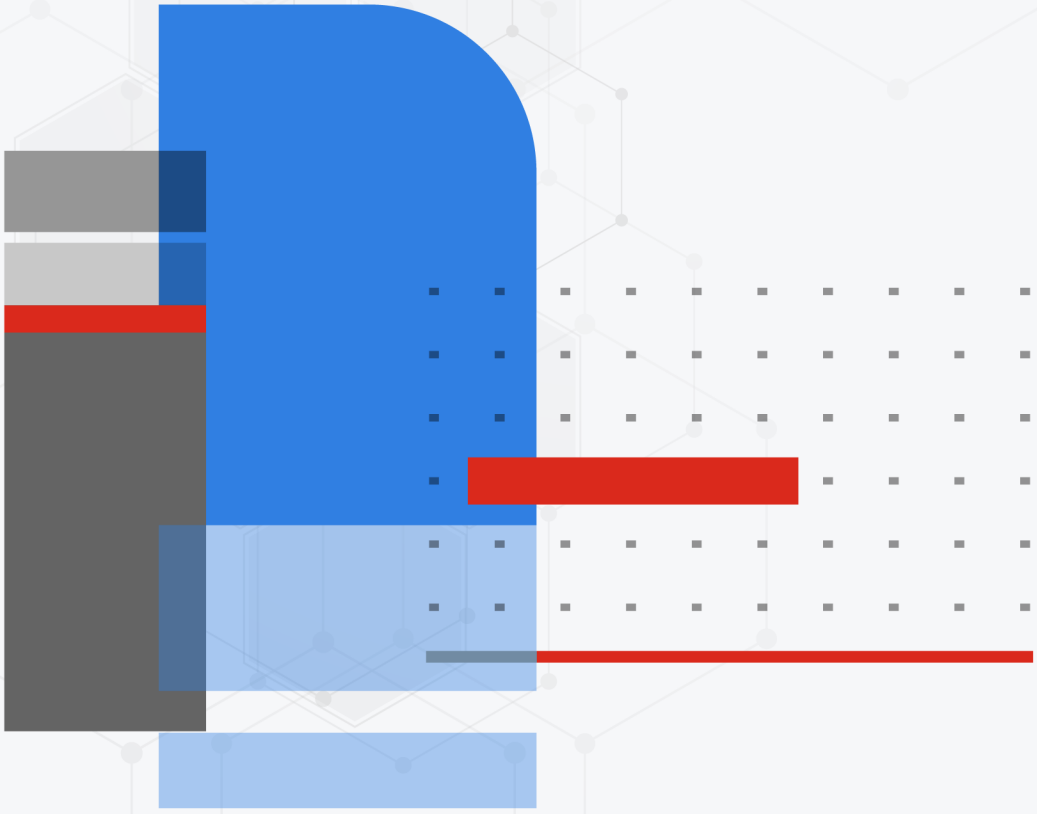
Release Notes

FortiOS 7.4.8



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

March 30, 2026
FortiOS 7.4.8 Release Notes
01-748-1118472-20260330

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-05-27	Initial release.
2025-05-30	Updated Introduction and supported models on page 8.
2025-06-02	Updated New features or enhancements on page 18 and Resolved issues on page 32.
2025-06-03	Updated Resolved issues on page 32 and Known issues on page 70.
2025-06-04	Updated Changes in default behavior on page 16 and Known issues on page 70.
2025-06-05	Updated Resolved issues on page 32 and Known issues on page 70.
2025-06-09	Updated Resolved issues on page 32 and Known issues on page 70.
2025-06-11	Updated Introduction and supported models on page 8, Resolved issues on page 32, and Known issues on page 70.
2025-06-12	Added SSL VPN not supported on FortiGate G-series Entry-Level models on page 12. Updated Known issues on page 70.
2025-06-13	Updated SSL VPN not supported on FortiGate G-series Entry-Level models on page 12.
2025-06-16	Updated Introduction and supported models on page 8, SSL VPN not supported on FortiGate G-series Entry-Level models on page 12, New features or enhancements on page 18, Resolved issues on page 32, and Known issues on page 70.
2025-06-20	Added Loopback-based VIPs cannot pass traffic after upgrade on page 25. Updated Resolved issues on page 32 and Known issues on page 70.
2025-06-24	Updated New features or enhancements on page 18, Resolved issues on page 32, and Known issues on page 70.
2025-07-02	Added FIPS-CC mode no longer supports TACACS+ on page 26. Updated Introduction and supported models on page 8, Resolved issues on page 32, and Known issues on page 70.
2025-07-03	Updated Known issues on page 70.
2025-07-07	Updated Resolved issues on page 32 and Known issues on page 70.
2025-07-14	Updated Known issues on page 70.
2025-07-23	Updated Resolved issues on page 32 and Known issues on page 70.
2025-07-28	Added FortiSwitch port page design change on page 12. Updated Resolved issues on page 32.
2025-07-29	Updated Special notices on page 10.
2025-08-05	Updated Resolved issues on page 32 and Known issues on page 70.

Date	Change Description
2025-08-12	Updated Resolved issues on page 32 and Known issues on page 70.
2025-08-19	Updated Known issues on page 70.
2025-08-20	Updated Special notices on page 10 and Changes in default behavior on page 16.
2025-08-26	Updated Known issues on page 70.
2025-09-02	Added Memory increase on low-end models with 4 GB RAM and ASLR on page 13. Updated Upgrade information on page 19, Resolved issues on page 32, and Known issues on page 70.
2025-09-15	Updated Resolved issues on page 32 and Known issues on page 70.
2025-09-22	Updated Known issues on page 70.
2025-09-29	Updated Resolved issues on page 32, Known issues on page 70, and Built-in IPS Engine on page 84.
2025-10-14	Updated Known issues on page 70.
2025-10-27	Updated Resolved issues on page 32.
2025-11-05	Updated Loopback-based VIPs cannot pass traffic after upgrade on page 25 and Known issues on page 70.
2025-11-17	Added Changes in GUI behavior on page 15.
2025-11-26	Updated Known issues on page 70.
2025-11-27	Updated Introduction and supported models on page 8.
2025-12-02	Updated Resolved issues on page 32 and Known issues on page 70.
2025-12-23	Updated New features or enhancements on page 18, Resolved issues on page 32 and Known issues on page 70.
2026-01-19	Updated Known issues on page 70.
2026-02-02	Updated Changes in table size on page 17 and Known issues on page 70.
2026-02-17	Updated Resolved issues on page 32.
2026-03-02	Updated Resolved issues on page 32.
2026-03-03	Updated Special branch supported models on page 9.
2026-03-16	Updated Known issues on page 70.
2026-03-30	Updated Resolved issues on page 32 and Known issues on page 70.

Introduction and supported models

This guide provides release information for FortiOS 7.4.8 build 2795.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.4.8 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-50G, FG-50G-5G, FG-50G-DSL, FG-50G-SFP, FG-50G-SFP-POE, FG-51G, FG-51G-5G, FG-51G-SFP-POE, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-70F, FG-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-200G, FG- 201G, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-400F, FG-401F, FG-500E, FG-501E, FG-600E, FG-601E, FG-600F, FG-601F, FG-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-50G, FWF-50G-5G, FWF-50G-DSL, FWF-50G-SFP, FWF-51G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-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 7.4.8. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 2795.

FG-30G	is released on build 5164.
FG-31G	is released on build 5164.
FGR-50G-5G	is released on build 6345.
FG-70G-POE	is released on build 6345.
FGR-70G	is released on build 6345.
FGR-70G-5G	is released on build 6402.
FGR-70G-5G-DUAL	is released on build 6345.
FG-71G	is released on build 6345.
FG-71G-POE	is released on build 6345.
FWF-30G	is released on build 5164.
FWF-31G	is released on build 5164.
FWF-70G	is released on build 6345.
FWF-70G-POE	is released on build 6345.
FWF-71G	is released on build 6345.

FortiGate 6000 and 7000 support

FortiOS 7.4.8 supports the following FG-6000F, FG-7000E, and FG-7000F models:

FG-6000F	FG-6001F, FG-6300F, FG-6301F, FG-6500F, FG-6501F
FG-7000E	FG-7030E, FG-7040E, FG-7060E
FG-7000F	FG-7081F, FG-7121F

Special notices

Hyperscale incompatibilities and limitations

See Hyperscale firewall incompatibilities and limitations in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 7.4.8 features.

FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 7.4.8 features.

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

SMB drive mapping with ZTNA access proxy

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

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

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

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

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

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

Hyperscale NP7 hardware limitation

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

The following known issues for the Queuing based Traffic Management (QTM) module on NP7 are fixed:

- Incorrect checksum for fragments after QTM.
- Packets longer than 6000 bytes cause QTM to hang.
- Refreshing causes QTM to hang.
- MTU is not honored after QTM, so the packet is not fragmented.

As a result of these changes, you can no longer use the following command to change QoS type used for traffic shaping for sessions offloaded to NP7 processors:

```
config system npu
    set default-qos-type {policing | shaping}
end
```

Instead, `default-qos-type` can only be set to `policing`.

For NP7 sessions, policy traffic shaping, per-IP shaping, and regular port shaping (outbandwidth enabled on an interface without a shaping profile) always use the NP7 accounting and traffic shaping module (called the TPE module). This is the same as changing the `default-qos-type` to `policing`.

For NP7 sessions, shaping profiles on interfaces now only use QTM for traffic shaping (equivalent to setting `default-qos-type` to `shaping`). Shaping profiles on interfaces are also called Multiclass shaping (MCS). The interface can be a physical interface, LAG interface, and VLAN interface (over physical or LAG). The FortiGate supports shaping profiles on a maximum of 100 interfaces.

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

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

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

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

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

FortiSwitch port page design change

Due to a FortiSwitch port page design change, the right-click popup menu is no longer available to configure some features, such as STP, BDPU, and edge port. A drop-down list is available instead. Beside the feature status of the desired port, click the *edit* icon to access the drop-down list and configure the feature.

Memory increase on low-end models with 4 GB RAM and ASLR

Total memory increase by an average of 7% low-end models with 4 GB RAM after enabling ASLR.

Changes in CLI

Bug ID	Description

1009740	Rename the server-type setting's iot-query option to vpatch-query.
	
	`config system central-management`
	`  config server-list`
	`  edit <id>`
	`  set server-type {update|rating|vpatch-query|iot-collect}`
	`  set server-address <x.x.x.x>`
	`  next`
	`  end`
	`end`

1035072	The options empty-cert-action, user-agent-detect and client-cert have been removed from system.access-proxy. Instead, they are added to the following config:
	
	`config firewall access-proxy-virtual-host`
	`  set empty-cert-action <action>`
	`  user-agent-detect {enable|disable}`
	`  client-cert {enable|disable}`
	`end`
	
	`config firewall vip`
	`  set type access-proxy`
	`  set empty-cert-action <action>`
	`  user-agent-detect {enable|disable}`
	`  client-cert {enable|disable}`
	`end`

Changes in GUI behavior

Bug ID	Description
1112727	On a new installation, users logging into the GUI are directed to the FortiCare registration dialog. This dialog ensures users remember to register their device with FortiCare. This feature is initially supported on the FortiGate 900G series and FortiGate 200G series.

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 7.4.8, 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.
1106205	The default IPS database setting for FGT-20xE models has been updated from extended to regular to optimize the size of IPS signatures. **Note**: The default FOS CLI setting in `config ips global` remains extended. This ensures that the IPS database configuration will change only during a factory reset and not during an upgrade, which prevents any disruption to existing customer setups. Additionally, if a user unsets the database after a factory reset, the database CLI configuration under `config ips global` will revert to the default extended setting.
1172149	In previous firmware, when the media type is not configured to match the actual media type, the interface will come up. However, starting in FortiOS 7.4.8, if the media type is not configured correctly, the interface may not come up, or it may be unstable and degraded. See Media type for interfaces that support transceiver modules for more information.

Changes in table size

Bug ID	Description
1032057	On Entry-Level FortiGate models, increase the number of VIP and VIP6 from 512 to 4096.
1042266	On high-end FortiGate models, the number of policy routes and policy routes6 is increased from 2048 to 5000.
1104085	Increase per-VDOM limit for dlp.dictionary from 256 to 2048.

New features or enhancements

More detailed information is available in the New Features Guide.

Policy & Objects

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

Feature ID	Description
1132012	Filtering support has been added to mutable policy lists, allowing users to refine policies based on key metrics, such as Bytes, Packets, Hit Count, and Last User. This enhancement provides more precise control for identifying high-impact or frequently used policies, improving efficiency in policy management and troubleshooting.

System

See System in the New Features Guide for more information.

Feature ID	Description

752946	To enhance the security of system administrator passwords, FortiGate now uses PBKDF2 as the hashing scheme with randomized salts to hash and store the password.
	To maintain downgrade support, a new command is introduced:
	`config system password-policy`
	`  set login-lockout-upon-downgrade {enable | disable}`
	`end`

1141036	To enhance security and reduce vulnerabilities, FortiGate appliances that are no longer under a valid Firmware & General Updates (FMWR) license or have reached End of Engineering Support (EOES) will now automatically upgrade to the latest patch within their current minor version. This proactive measure ensures that all devices remain protected with the most up-to-date security features.

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 19 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 7.4.8 greatly increases the interoperability between other Fortinet products. This includes:

FortiAnalyzer	• 7.4.7
FortiManager	• 7.4.7
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 7.4.8. When Security Fabric is enabled in FortiOS 7.4.8, all FortiGate devices must be running FortiOS 7.4.8.

Downgrading to previous firmware versions

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

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

Firmware image checksums

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

FortiGate 6000 and 7000 upgrade information

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 7.4.8:

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 7.4.8 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 or later. This change will cause the admin to lose access.

To regain access, configure a password override on the FortiGate device using the following commands:

```
config switch-controller switch-profile
    edit default
        set login-passwd-override enable
        set login-passwd <passwd>
    next
end
```

FortiSwitch units with an existing admin password will not be affected by this change.

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

If local-in policy used an interface in version 7.4.5 GA, or any previous GA version that was part of the SD-WAN zone, these policies will be deleted or show empty values after upgrading to version 7.4.6 or later.

This issue is resolved in FortiOS 7.4.8 with mantis 1104649.

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

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

Statistics for traffic shaping using QTM

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

Loopback-based VIPs cannot pass traffic after upgrade

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

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

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

FIPS-CC mode no longer supports TACACS+

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

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

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

Product integration and support

The following table lists FortiOS 7.4.8 product integration and support information:

FortiManager and FortiAnalyzer	See the FortiOS Compatibility Tool for information about FortiOS compatibility with FortiManager and FortiAnalyzer.
Web browsers	• Microsoft Edge 135 • Mozilla Firefox version 138 • Google Chrome version 136 Other browser versions have not been tested, but may fully function. Other web browsers may function correctly, but are not supported by Fortinet.
Explicit web proxy browser	• Microsoft Edge 135 • Mozilla Firefox version 138 • Google Chrome version 136 Other browser versions have not been tested, but may fully function. Other web browsers may function correctly, but are not supported by Fortinet.
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C

Fortinet Single Sign-On (FSSO)	• 5.0 build 0321 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	• 7.00041
IPS Engine	• 7.00570

See also:

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)	✓

Language	GUI
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
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

FortiExtender model	Modem firmware image name	Modem firmware file on Support site	Geographical region
FEV-211F_AM	FEM_12_EM7511-22-1-2-AMERICA	FEM_12_EM7511-22.1.2-build0001-AMERICA.out	America
FEV-211F	FEM_12-22-1-0-AMEU	FEM_12-22.1.0-build0001-AMEU.out	World
FEX-211F-AM	FEM_12_EM7511-22-1-2-AMERICA	FEM_12_EM7511-22.1.2-build0001-AMERICA.out	America
FEX-212F	FEM_12-19-2-0-WRLD	FEM_12-19.2.0-build0002-WRLD.out	World
	FEM_12-22-1-1-WRLD	FEM_12-22.1.1-build0001-WRLD.out	World
FEX-311F	FEM_EM160-22-02-03	FEM_EM160-22.2.3-build0001.out	World
	FEM_EM160-22-1-2	FEM_EM160-22.1.2-build0001.out	World
FEX-511F	FEM_RM502Q-21-2-2	FEM_RM502Q-21.2.2-build0003.out	World
	FEM_RM502Q-22-03-03	FEM_RM502Q-22.3.3-build0004.out	World
	FEM_RM502Q-22-04-04-AU	FEM_RM502Q-22.4.4-build0005_AU.out	Australia
	FEM_RM502Q-22-1-1	FEM_RM502Q-22.1.1-build0001.out	World
	FEM_RM502Q-22-2-2	FEM_RM502Q-22.2.2-build0002.out	World

The modem firmware can also be uploaded manually by downloading the file from the Fortinet Customer Service & Support site. The firmware file names are listed in the third column of the table.

To download the modem firmware:

1. Go to https://support.fortinet.com/Download/FirmwareImages.aspx.
2. From the *Select Product* dropdown, select *FortiExtender*.
3. Select the *Download* tab.
4. Click *MODEM-Firmware*.
5. Select the FortiExtender model and image name, then download the firmware file.

Resolved issues

The following issues have been fixed in version 7.4.8. 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
1055609	Files are dropped by Quard when sending to FortiSandbox under heavy load, as new connections are established despite existing ones being active.
1068321	Previous unsigned MMDB and AVAI databases are kept after upgrading FortiOS.
1073326	Entry-level FortiGates with 2GB of memory may encounter a memory usage issue during FGD-based firmware upgrades causing the AV engine to restart.
1080003	FGT memory gradually increases when FGT Flow AV Profile is inspecting TCP 6200 traffic with outbreak prevention enabled.
1100819	SMB traffic fails when the file server uses AES-256-GCM/CCM encryption with FortiOS.
1104189	In TP VDOM, the WAD creates the expectation session for FTP data connection if the firewall is in the proxy mode. This session does not have the outdev info.

Application Control

Bug ID	Description
1064413	Traffic fails to follow SD-WAN rules when SNAT is enabled and "snat-route-change" is activated due to session drops caused by SNAT check failures after route changes.
1066078, 1066567	Application classification fails when SSL inspection is bypassed, causing Inline IPS to miss blocking certain apps like Tencent Meeting and Facebook due to incomplete traffic processing.
1102636	After the first DB update, only signatures in the built-in DB are loaded, preventing new categories and updated signatures from appearing correctly.
1118703	Web traffic designated as blocked is allowed due to the config entry priority in the application control profile.
1144469	No security events logged for custom Application Control profiles in Monitor mode when applied to policies configured to log all sessions.

DNS Filter

Bug ID	Description
1086355	DNS query logs are not logged on FortiGate when traffic uses a VIP mapped to a loopback interface hosting a DNS server.
1096380	FortiGate in proxy mode sends the cached DNS response when it receives a DNS registration request.
1100282	When using FortiGate DNS servers, some clients cannot handle large UDP DNS responses exceeding 512B received from the FortiGate.
1134108	The IPS engine memory usage increases rapidly when a flow-based policy uses an external Threat Feed with over 1M domain entries, causing device unresponsiveness.

Endpoint Control

Bug ID	Description
1055192	Downstream FortiGates incorrectly send a REST API request to declare themselves as root to EMS, causing potential management issues in Fabric trees.

Bug ID	Description
1066250	Verification of EMS and upgrade of FGT with verified EMS should promote CA to fabric-ca.
1093786	Expired 'FCEM' contracts are loaded in FGVM when multiple account-level licenses exist under the same tag due to selection based on entry order rather than expiration date.
1133386, 1141380	Connection failures occur when FGT201G devices attempt to connect to external servers due to improper handling of private keys by certain daemons.

Explicit Proxy

Bug ID	Description
893935	HTTP requests are forwarded to the server through a web proxy even when `forward-server group-down` is set to block.
1004634	Health check issues occur when forward server is configured in proxy mode firewall policy.
1014477	Files do not get uploaded on webmail applications with antivirus, app control, or IPS enabled on an explicit proxy policy.
1021710	The `server-down-option-block` command does not work as expected when creating a connection to a forward proxy server.
1025974	When FortiGate is configured as a downstream proxy with an FQDN type, browsing traffic may encounter a gateway timeout error.
1048194	FortiGate blocks traffic if a `onetime` schedule is configured in an explicit proxy policy and the schedule has not expired.
1067291	Applications do not connect over explicit proxy when a deep-inspection profile is applied.
1084871	Explicit proxy fails to open all HTTP sessions to remote servers when using FQDN URL.
1107762	Overflow occurs in WAD daemon when oversize-limit exceeds 4096 MiB during byte conversion.
1114438	Policy Test feature fails to function correctly when testing HTTP(S) server configurations due to missing source port initialization.

File Filter

Bug ID	Description
1011320	Adding File Filter to a flow-based firewall policy may impact performance.
1095866	Clients incorrectly believe write operations succeed when WAD blocks SMB file uploads due to forwarded success responses.

Firewall

Bug ID	Description
723186	Policy & Objects > Multicast Policy: Mac type addresses are not listed in the Src/dst omniselect on the GUI.
946762	Policy & Objects > Firewall Policy: The column filter for "Secondary security posture Tag" does not filter matching results when multiple tags are present on a policy.
993138	Misleading logs with subtype="ztna" appear when only virtual-server in a firewall policy.
994986	Firewall policy list "By Sequence" view 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" does not have this issue.
996622	On FortiGate, the IPv6 real server shown as DOWN by the health check but it is considered UP in the kernel.
1025078, 1086315	When using a virtual server, some customers observed issues of memory usage increases and client sessions not disconnecting.
1028356	Incorrect DNAT hit counts are displayed when VIP order is changed in Central NAT.
1038650	Policy list refreshes entirely when right-clicking on hitcount or bytes columns to update statistics or clear counters.
1050864	No route is found when FTP server attempts to connect back to client in active mode due to incorrect dst inheritance from master session.
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.
1055898	Does not support HTTP/2 post with out content-length in half-ssl virtual server.
1057080	On the Firewall Policy page, search results do not display in an expanded format.
1064748	FortiGate incorrectly uses outgoing interface IP instead of configured IPPool for SNAT when HTTP multiplexing is enabled on a load balancer VIP.
1066136	Denied sessions were bidirectional causing all traffic to be blocked.

Bug ID	Description
1078662	If an interface on an NP7 platform has the `set inbandwidth XXX`, `set outbandwidth XXX`, and `set egress-shaping-profile XX` settings, the following issues may occur: • Fragment packet checksum is incorrect. • MTU is not honored when sending packets out. • QTM hangs and blocks traffic when packet size is larger than 6000 bytes.
1079590	Reply traffic isn't sent out of FortiGate when heavy traffic fills up the txqueue on EMAC VLAN interfaces.
1081542	Packet drops occur when high traffic causes nTurbo buffers to be reused without proper initialization under CPU-intensive conditions with ASIC offloading enabled.
1082334	*Policy & Objects > Firewall Policy*: When Korean characters are used in a firewall policy name, an error is not displayed when the length is longer than the limit.
1088507	ICMP Echo replies sent via local-in-policy with virtual-patch enabled are routed through incorrect interfaces during traffic handling.
1097628	On the policy list, the *Not* filter on *Source* and *Destination* columns does not work well for "all" and "ems" addresses.
1098208	After FortiGate exits conserve mode, some policies failed to install into the kernel at the same time.
1101865	Trailing stray characters appear in Netflow App Info reports, causing warnings in analysis programs.
1103748	Combine with 111268 Threat feeds used as source or destination addresses in security policies may not match correctly.
1104208	NAT is not correctly applied to traffic when a single SYN packet is sent to a VIP without an acknowledgment or reset.
1106112	Shared memory files on entry-level platforms can't be removed upon restart due to being stored in a persistent directory instead of a temporary one.
1107254	Sequence number position changes when scrolling within interface pair view.
1108236	Incorrect logs are displayed when viewing matching logs for an implicit deny policy due to an invalid filter operator.
1108540	Taking more than one minute time to fetch for addresses when trying to add an address member from address Group page.
1110135	Policy & Objects > Firewall Policy: Policy lookup for UDP protocol with FQDN does not work.
1112628	Threat feeds used as source or destination addresses in security policies may not match correctly.
1117165	Leaving the `apn` field empty in a GTP APN traffic shaping policy means that the policy will not match any traffic. Consequently, APN traffic shaping can only be applied to specific APNs. To configure GTP APN traffic shaping:

Bug ID	Description
	config gtp apn-shaper edit <policy-id> set apn [<apn-name> <apngrp-name> ...] set rate-limit <limit> set action {drop | reject} set back-off-time <time> next end
1120749	If session is in SYN_SENT or SYN_RECV state, and FortiGate receive a second SYN with different ISN, it will drop the 2nd SYN.
1121944	For a firewall policy allowing traffic from client -> server, but no policy from server -> client. In the case that traffic is not matched from server -> client, a block session is formed that will block both direction of traffic.
1127977	Traffic fails to pass FortiGate when firewall policies are applied in TP VDOM due to flag checks treating packets as local instead of forwarding them.
1130932	An error condition occurs when disabling the outbound shaping-profile on the interface edit page.
1131860	A two to three minute delay occurs when enforcing policy changes to existing or new traffic due to linear duplicate address checks during iprope updates.
1136058	Policies are deleted and replaced with "implicit" when exporting CSV from the Interface Pair View in Firewall Policy GUI.
1139282	Incorrect SNI is sent during HTTP2/HTTP3 requests using "http-host" load balancing because WAD uses the proxy's SNI instead of the request's hostname.
1142813	Filtering by comments fails when quick-editing firewall policies in the Firewall Policy page.
1150376	FortiGate fails to match policies with predefined ISDB objects when a custom Internet Service Database entry is created, as an invalid dummy entry (id=0) persists in the kernel, preventing proper policy lookup.

FortiGate 6000 and 7000 platforms

Bug ID	Description
653335	SSL VPN user status does not display on the FortiManager GUI.
790464	After a failover, ARP entries are removed from all slots when an ARP query of single slot does not respond.
790464	After a failover, ARP entries are removed from all slots when an ARP query of single slot does not respond.

Bug ID	Description
892774	On FortiGate 7000 models, the hit counter on the FortiManager GUI does not display the correct values.
976521	High CPU usage by the node process occurs when loading 7000 policies due to fetching all statistics in one request.
998615	When doing a GUI-packet capture on FortiGate, the through-traffic packets are not captured.
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).
1050727	MAC info packets carrying session sync data are dropped under asymmetric routing conditions with L2 connections available.
1057080	On the *Firewall Policy* page, search results do not display in an expanded format.
1060619	CSF is not working as expected.
1060864	Ports fail to establish or exhibit CRC/input errors when 100G QSFP28 LR transceivers are used with FIM-7920E and Cisco ASR in specific setups.
1062080	SNMP query returns an error when there is a large number of BGP routes.
1078334	Combine with 1103739 High cmdbsvr CPU usage and FTP hang issues occur during scheduled automation backup executions due to automated backups appending device serial numbers to file names.
1081015	ISDB updates fail during FortiGate database synchronization attempts due to missing FFDB package handling and failed temporary file transfers.
1083246	Intermittent traffic disruption occurs when using Fortinet_Factory on FortiGate-200G.
1086889	FIMs can be in split-brain state when one FIM reboots, leading to incorrect master election and network instability.
1086953	On FortiGate 7000 secondary units, slot 3 (FPM) has no ISDB database and does not update due a filesync connection issue.
1088402	On FortiGate 6K/7K FGSP clusters, the configuration does not synchronize properly with `standalone-config-sync` enabled.
1095936	Fewer sensor entries appear when executing 'chassis-sensor list' after system bootup due to delayed sensor initialization on SMM.
1096156	GUI unreachable due to certificates and private keys mismatch in a HA setup.
1097428	The Security Profile menu does not appear in the GUI for Global VDOM on 6K/7K devices despite being accessible via CLI.
1102413	Session count for VDOMs incorrect in 6K/7K devices.
1102481	Local-in remote access issues due to incorrect destination address.
1103739	High cmdbsvr CPU usage and FTP hang issues occur during scheduled automation backup executions due to automated backups appending device serial numbers to file names.

Bug ID	Description
1103810	100G SFPs are experiencing compatibility issues with the 7060E.
1105009	The command 'execute load-balance slot manage X' fails on 6K/7K platforms when admin-telnet is disabled and then re-enabled.
1106519	ISDB/FFDB was out-of-sync from MBD to FPCs after running `exec update-now` on 6K/7K platform.
1108181	Unexpected behavior observed in the confsyncd daemon due to an erroneous memory allocation.
1109415	New SNMP MIB table for chassis sensor.
1109601	Graceful upgrades fail when hatalk daemon restarts, disrupting slbha state synchronization during FortiOS version transitions.
1112581	On the FortiGate 7000F platform, after upgrading from FortiOS 7.4.7 to 7.6.2, cmdbsvr CPU usage can be at 99% on one or more FPMs for several minutes. During high CPU usage, FortiGuard packets cannot be synchronized to the affected FPM(s).
1113805	Firewall policy statistics reset after reboot on FGT-6k devices caused by improper persistence of aggregated data.
1115656	FGT-6K session filter by source interface doesn't set correct interface index.
1116862	Graceful upgrade of a FortiGate 7000E chassis to FortiOS 7.6.2 may fail for some configurations.
1118004	On a FortiGate 7000E FGCP cluster, after using the `execute ha disconnect` command to disconnect a chassis from the cluster, you can't use the special management ports to connect to the FIM in slot 2 or to any of the FPMs of either chassis. You can still connect to the FIM in slot 1.
1121918	Confsyncd crashes occur when syncing ha-mgmt-intf to a newly joined HA slave due to invalid pointer attributes.
1124603	Traffic drop occurs on 7KF-FGT devices when traffic shaping is enabled during or after migration, causing intermittent internet connectivity loss.
1129283	Bandwidth Widget shows cumulative Tx and Rx rather than current throughput.
1130218	Policies fail when Security Posture Tags are configured on SLBC platforms due to dynamic address sync issues outside HA mode.
1135891	The PSU status incorrectly shows as "Critically High" on the GUI dashboard widget.
1139867	In a FG-7121F chassis HA system with 7000F image, the secondary chassis GTP-C tunnels were not synchronized with the primary chassis GTP-C tunnels.
1149405	The image upgrade fails when performing a non-graceful update due to an ISIZE mismatch during verification.

FortiSASE

Bug ID	Description
1140953	Unable to download large files using HTTPS traffic over internet through FortiSASE.

FortiView

Bug ID	Description
1125124	When running more than 1M concurrent HTTP sessions across the firewall and trying to access session list on the GUI on FortiView, we see packet loss and loss of a session.
1133164	Subnet filtering fails for firewall users due to partial API support.
1139219	The Quarantine widget experiences delays when loading the complete IP list.

GUI

Bug ID	Description
919473	Network > Interfaces: When an IPsec tunnel is bound to an interface, "Interface Integrate" for that interface fails.
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.
1054026	Offline license file upload fails via GUI in air-gapped environments when using FortiCare-offlined licenses with certificates incompatible with the system's BIOS version.
1055197	On FortiGate G series with dual WAN links, Interface bandwidth widget may show incorrect incoming and outgoing bandwidth count where the actual traffic does not match the display numbers.
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.
1055865	NodeJS errors when event log socket is closed.
1057628	*Catch WebSocket* errors from *PerMessageDeflate* occur when the client abruptly closes the connection.

Bug ID	Description
1058608	The FortiGate Cloud status incorrectly shows as Activated after logging out using the GUI dashboard.
1062753	Incorrect percentage is displayed in the dashboard widget for "Files Uploaded Today" to FortiSandbox.
1069557	Add API filter support for firewall user monitor API and search bar.
1081912	When inserting a policy using the new layout, the destination information is not displayed.
1087857	On the *Policy & Objects* > *Firewall Policy* page in the GUI on the secondary FortiGate in an HA cluster, create a new address, and the page keeps loading.
1092475	On the *Policy & Objects* > *Firewall Policy* page, in the *Edit Policy* dialog, the GTP-profile do not display in the GUI when Central SNAT is enabled.
1092489	The `config system fortiguard > fortiguard-anycast` setting was changed to automatically disable when the FortiGuard page is shown on GUI.
1099309	The FortiOS GUI fails to load topology-related pages when temporary files generated during Security Rating operations are mistakenly read by the REST API.
1101932	IPsec monitor widget: IPsec phase2 tunnel details are not displayed on the tooltip when hovered over the phase2 selector.
1102404	VDOM search function do not work properly if VDOM has uppercase letters.
1110382	Admin can log in to GUI (HTTPS) with password, even when `admin-https-pki-required` is enabled.
1112716	No log output when running debug flow on GUI.
1112727	FortiCare/FortiCloud registration is not enforced correctly when accessing FOS GUI, resulting in potential security risks. Registration level is not properly indicated, and admin access is not restricted as expected. This feature is initially supported on the FortiGate 900G series and FortiGate 200G series.
1114549	Authorization of FEXT devices fails when using the FortiGate GUI.
1114658	Duplicated logs occur during Node.js health-check operations when internal communication between daemons is exposed through HTTP requests, as the traffic is captured in logs and packet captures.
1118810	Asset Identity Center - View tooltip on IoT/OT Vulnerabilities. OT license is reported as inactive, even with full license.
1148930	Exported FSW ports to tenant VDOM are not displayed on the GUI when the tenant VDOM has a FortiLink, causing virtual switches to be filtered out due to the lack of a fsw-wan1-peer attribute.
1148959	An error condition in httpsd occurs when fetching data from cmdbsvr fails.

HA

Bug ID	Description
794395	The secondary unit in an HA cluster would display messages indicating that external resources were not in sync, despite the resources being correctly synchronized.
965217	In an HA configuration, FortiGate may experience intermittent heartbeat loss causing unexpected failover to the secondary unit.
982081	After changing the status to down on the ha1 and ha2 ports, setting the status back to up does not bring up the ports.
985967	Session synced with FGSP does not allow immediate failover when UTM is enabled in flow mode.
992758	When uploading certificates, HA becomes unsynchronized.
1000808	When FortiGate in HA boots up, an unnecessary primary unit selection occurs and reports *only member* as the reason, even though the cluster consists of two or more members. It may also occur when a new member joins the cluster.
1007516	Rx_dropped counters increase on ha1 and ha2 interfaces, causing them to flap and resulting in FGSP member loss during high session and CPU usage spikes.
1025585	Network traffic may be disrupted due to a linking issue with upstream routers.
1052532	Newly created VDOM is out of sync for a while after secondary reboots.
1054041	DHCP client can't get IPv4 address from server with vcluster.
1055336	*User & Authentication > RADIUS servers*: The *Test User Credentials* button from RADIUS server does not honor custom NAS-ID type from the GUI. **Workaround**: Test user credentials from the command line. `diagnose test authserver radius <server_name> <chap | pap | mschap | mschap2> <username> <password>`
1060006	Rebooting a member in an FGSP cluster with standalone-config-sync enabled may cause desynchronization due to port_ha communication failure.
1060023	High CPU load occurs due to recursive session syncs between primary and secondary HA nodes during URL category ID updates.
1063192	*Network > Interfaces*: In a multi-VDOM environment, if an interface is reserved as a HA management interface, disable/enable actions on the interface fail with error 'Failed to save changes'. **Workaround**: Perform the operation using the command line.
1064728	UDP single-packet sessions cause a race condition during expiration, leading to inconsistent synchronization between primary and secondary FGCP clusters, resulting in an imbalance of session counts across units.

Bug ID	Description
1067274	Reply packets fail to reach the session owner instance in FortiOS asymmetric L3 FGSP deployments, causing network loops and preventing TCP connections from forming.
1080655	HA synchronization fails after configuration changes on FortiGate devices due to improper handling of a hasync flag in the fgfmd daemon.
1084662	Inconsistent FFDB signed statuses occur on secondary blades when a signature file fails to synchronize during HA database sync events.
1085314, 1095879	Firewall policy page takes a long time to load on the HA Primary unit due to a loop condition between BGP and NSM when other protocols' same route is redistributed to BGP.
1091189	Switches observe MAC address flapping in HA A-A setups when both FortiGates use identical virtual MACs on their primary VLANs.
1095786	Traffic interruption occurs when performing a manual HA failback after an initial failover in VWP setups.
1099346	Connection issues occur when FortiGate slave uses master's certificate to connect to FMG instead of its own.
1100177	In an FGSP setup, on asymmetric TCP flow during SYN/ACK packet on the other member, the TCP MSS value is not adjusted according to the firewall policy.
1101456	In a HA setup, the aggregate interface status remains up after configuring 'status down' in FortiOS due to a race condition.
1104892	Duplicate IP detected messages are seen from the Secondary FortiGate in a cluster.
1105422	"Detected Tx Unit Hang" error occurred on the HA secondary, causing it to become out-of-sync.
1107137	The secondary FortiGate with an HA Reserved Management Interface cannot be accessed using HTTPS after upgrading from version 7.4.3.
1109919	Cluster enters split-brain when EMAC interfaces are disabled within a zone.
1115190	The SNMP value of fgVWLHealthCheckLinkState on the secondary unit should should always be set to dead(1).
1117725	HA synchronization fails due to checksum mismatches on CA certificates across all VDOMs when adding or modifying certificates sourced from a bundle.
1121117	When two HA clusters are on the same subnet, the L2 session-sync packets could be received by each other even if they are two different HA clusters.
1136097	HA state may become out of sync due to a race condition caused by missing local-in ipropes.
1137565	vSN support added in 7.2.9, 7.4.6, and 7.6.1. FG-100F/101F do not yet support vSN and logical-sn.
1138763	IKE hasync loop and high memory consumption when peer address/port changes.
1143791	The heartbeat interface default route is lost and HA fails to synchronize when changing the interface mtu-override option.

Hyperscale

Bug ID	Description
1013892	Unexpected behavior observed in NPD when the threat feed object attempted to update manually in the HA pair.
1024274	When Hyperscale logging is enabled with multicast log, the log is not sent to servers that are configured to receive multicast logs.
1047362	Decoding errors occur when Netflow data packets contain certain values for each NPU but lack corresponding templates for proper interpretation.
1074547	SNAT session drops occur when kernel sessions become dirty in hyperscale VDOM environments due to inconsistent NAT resource allocation between software and hardware sessions.
1075915	NP gets stuck during extended traffic with specific DoS anomalies due to MSE hash table issues from depfail.
1089281	With FG-480xF/FFW-480xF using npu-group other than "0", with log2host with around ~1M CPS, can result in NP chip getting stuck.
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.
1121524	Client could not get DHCP IP address with policy-offload-level set to full-offload.

ICAP

Bug ID	Description
1072282	HTTP 400 errors occur due to missing space after status code in converted HTTP responses.

Intrusion Prevention

Bug ID	Description
891295	FortiGate experiences a performance issue with geography-type addresses matching in NGFW policy mode.

Bug ID	Description
995997	ISDB is shown in 'dia test app ipsmonitor 1' output when IPS/AppCtrl feature are not enabled.
1013666	IPS engine attempts to use FortiGuard for vulnerability lookup even though FMG is configured as override server in a closed network, causing vulnerability lookup to fail.
1074732	Traffic is dropped silently when IPv6 traffic is sent with UTM and nTurbo enabled on FortiGate-121G.
1086789	High CPU usage due to an uninitialized return value in the load balance comparison function when SD-WAN load balancing is enabled.
1090134	IPS engine re-initialization after receiving a threat feed update from an external resource.
1093788	Sniffer logs are not generated when using VLANs.
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'` Even after upgrade, you may still need to power off the FortiGate. Wait 30 seconds, and then power on the FortiGate to fully resolve the issue. **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.
1121953	IPSengine processes consume memory, can lead to the conserve mode.
1122188	Internal diagnostic commands fail or delay when ipsmonitor processes each request sequentially due to sequential forwarding to IPS daemon processes.
1149760	Inline-IPS fails to match sensor locations for the "Web.Server.Password.File.Access" signature because it incorrectly reverses traffic direction definitions.

IPsec VPN

Bug ID	Description
979591	Changes to IPsec phase1 fragmentation settings do not take effect immediately when made on dynamic configurations.
995912	VPN tunnels exhibit instability following an upgrade, with processes stuck during NP7 debugging due to improper prioritization of certain packets.

Bug ID	Description
1002325	If Spoke re-auth is enabled, shortcut tunnel rekey will fail and go down when SA expired. Shortcut tunnel will flap while it re-establishes again.
1012615	IPsec VPN traffic is dropped after upgrading to version 7.4.3.
1020690	The *IPsec Aggregate* interface displays as DOWN on the *Network > Interfaces* and the *Policy & Objects > Firewall Policy* pages when the member including the Dialup VPN is actually UP. This is purely a GUI display issue and does affect system operation. The correct status is shown on the *VPN > IPsec Tunnels* page.
1042465	Packet drops occur when FortiOS CPUs are overwhelmed by high traffic bursts while IPsec acceleration is enabled, leading to CP queue overflows despite prior optimizations.
1054440	Incrementing TX and RX errors on VPN interface occur when NPU offload is disabled, busy CPU cores, or high burst traffic cause packet drops due to full queues on SoC3/Soc4 platforms.
1057558	When configuring dialup and loopback-asymroute disable, and has multiple paths for IKE/IPsec traffic. When the incoming ESP traffic changes path due to routing change, reply traffic still egresses on the old interface and traffic is dropped.
1059778	IPsec does not work as expected when the traffic path is from spoke dial-up to hub1, and then from hub1 to another site via a site-to-site tunnel.
1061176	CPU usage issues observed during IPsec tunnel establishment with large number of tunnels.
1068626	SOC4 platform IPsec traffic may stop in specific corner cases due to the IPsec outbound process becoming unresponsive.
1071769	L2TP/IPsec connections fail due to interface changes from break-before-make rekeys and Windows rejecting selectors during FGT-initiated QM rekeys.
1073670	Unexpected behavior observed in the IKED during HA split-brain events when IPsec tunnels are configured to use DHCP.
1076636	Unexpected behavior in IKED occurs when a peer attempts to negotiate with two different gateway profiles simultaneously.
1077122	The Phase2 SA is present in the kernel but there is no IKE Phase1 SA after an HA upgrade.
1080164	Tcp-MSS settings are not applied to IPv6 traffic when configured on egress interfaces.
1080420	Tunnel fails when DPD is enabled because FortiGate does not increment its receive message ID after processing an unexpected payload, causing out-of-sync message IDs and ignoring subsequent DPD requests.
1082624	EAP authentication fails for local users specified directly in firewall policies, while RADIUS users authenticate successfully.
1087651	Authentication fails when using FortiClient with IPsec IKEv2 after waiting more than 60 seconds to enter the 2FA token, caused by a fixed 60-second RADIUS timeout.
1094028	Unexpected behavior observed in the IKED after configuration changes when the phase1 monitor feature is used.

Bug ID	Description
1102528	NP7 tunnel offloading failure-recovery issue may cause use-after-free memory corruption when there are many concurrent IPsec tunnels, which leads to high CPU usage and kernel panic.
1102584	Kernel crash caused by memory corruption due to a use-after-free issue, resulting in a system hang. This issue occurs with a large number of IPsec tunnels.
1110093	IPsec SA offloading stops on some FortiGate models when handling more than 50,000 concurrent secure associations.
1112665	Static routes are marked inactive when an old IPSec tunnel is deleted during an INITIAL-CONTACT message in IKEv1, mistakenly deactivating the new tunnel's status in the kernel.
1113354	Group list got truncated because of fixed size buffers.
1116825	FortiGate presents certificate information when accessed using IPsec VPN listening interface.
1117758	FGT fails to negotiate encryption algorithm CHACHA20_POLY1305 against third party client.
1120517	IPsec tunnel failure occurs when using aggressive mode with PSK authentication.
1126436	The IKE TCP port is exposed on all IP addresses and interfaces when no local-in firewall policy regulates the traffic.
1132864	After changing system.settings.ike-tcp-port from default value to customized value, virtual IKE fails to be re-initialized.
1134882	The ipv4-split-include setting is missing from the GUI.
1136536	VPN authentication fails on FortiSASE when a large number of RADIUS groups are configured.
1144548	Authentication failure occurs when using IPsec VPN IKEv2 with MsCHAPv2 and radius server.
1145219	IPsec tunnels drop unexpectedly during rekeying when using certificate authentication with multiple dialup gateways and peer-initiated SA_INIT requests.
1145411	Changing the ip-fragmentation setting on dynamic IPsec phase1 does not take effect immediately after modification due to an issue with the change handler function in certain FortiOS builds.

Log & Report

Bug ID	Description
1001583	On the *Log & Report > Forward Traffic* page, the GUI experiences a performance issue and reverts to the last input when multiple ports are added to a filter for destination ports.

Bug ID	Description
1002502	Add log when duplicate IP detected.
1004103	Log & Report > Reports: When reports are renamed, the scheduled reports page does not load and displays error notification 'unable to fetch reports'.
1024990	Local-out traffic logs appear when FortiGate initiates internal processes like certificate probes or FGD queries, causing policyid=0 and srcintf="root" entries in kernel-level logs.
1045253	Log items cannot be created and sent to FortiGate Cloud log server when confirm queue becomes full.
1074460	Erroneous memory allocation results in intermittent HTTPSD disruption caused by a corrupted traffic log file.
1083537	Serial numbers are lost in FortiAnalyzer when high availability information packets lack serial number data, causing cached entries to expire and be removed.
1084934	Firewall logs show *Object Object* in GUI and `dstintf="unknown-0"` in raw logs.
1091064	Missing poluuid and policyname fields occur in Forward Traffic logs when HA failover happens in FGCP clusters.
1100883	Forward Traffic log fetched from FortiGate Cloud taking a long time to load on GUI.
1118089	Temporary log files persist in /var/log after successful FTP uploads, leading to increased disk usage.
1119147	Secondary device fails to generate reports at the set time.
1121505	Log & report > Forward Traffic: 'Security' tab for security event logs does not load.
1129448	The body of the emails sent through alertmail is partially missing.
1141733	Traffic interruptions occur when revisiting the forward traffic log page during searches with applied filters.

Proxy

Bug ID	Description
877333	WAD crash with a signal 11 error due to a memory corruption issue when handling VIP cases.
979502	On FortiGate, when the `waps` file is broken, the WAD process does not start.
983997	Certificate validation fails on FortiGate/FortiProxy when using root CAs with identical subjects but distinct public keys and serial numbers.
987655	RPM files could not be blocked in HTTP downloading on Box Cloud website in proxy mode.
988473	On FortiGate 61E and 81E models, a daemon WAD issue causes high memory usage.

Bug ID	Description
1014014	Proxyd always selects the first certificate in the list when multiple server certificates are configured, regardless of SNI.
1043423	Unexpected behavior is observed in the WAD user info history daemon due to erroneous memory allocation.
1051875	Strict SNI certificate checks skip IP destination validation under strict mode.
1054052	The WAD process does not load a self-sign certificate when `set admin-server-cert self-sign` is configured in an explicit proxy.
1054835	HTTP/2 large file transfers are slow when IPS, APP, or SSL inspect-all is enabled due to excessive buffering during traffic forwarding.
1060812	Botnet detection fails in transparent proxy setups caused by implementation error.
1061303	Duplicate DN used in LDAP servers causes wad signal 11 crash at wad_user_stats_dn_cache_find.
1066113	Accessing certain websites via HTTPS fails when using inspect-all deep-inspection in proxy mode firewall policy.
1068747	WAD process fails to boot up and crashes if waps file is broken.
1083663	A signal 11 segmentation fault crash is reported in wad user info daemon during the restoration of IoT info.
1087635	Wad process crashes due to segmentation fault with AV scanning enabled on webproxy policy and HTTP response code 304.
1096728	An error case observed in the WAD, affecting some VIP traffic, caused by erroneous memory allocation.
1107205	FortiGate encounters a WAD memory usage issue when using a secure explicit web proxy with WAD user authentication to visit some websites.
1111846	Inline CASB profile in ZTNA proxy policy does not block Gmail traffic, including uploading local files and sending emails with attachments.
1120964	An error condition in WAD occurs during shutdown after factory-reset on 32-bit ARM platforms.
1121171	Large file downloads through proxy HTTP2 is slow when IPS/APP/SSL inspect-all enabled.
1126253	When VDOM configuration file is restored, it changes the no-inspection profile under ssl-ssh-profile to deep-inspection.
1126385	WAD fails to handle deep-inspection traffic under FIPS mode.
1128581	Firewall policy enabled with AV and Webfilter is unable to upload large file (over 10 MB) attachments into Gmail.
1135475	WAD crashes with signal 11 by accessing a null pointer if the client session is closed before server connection is done in vs server pool mode.
1146601	With proxy inline-ips, WAD daemon gets memory leak, leading to conserve mode.

REST API

Bug ID	Description
943756	When creating a VPN remote certificate with the API, the "remote" key fails to be set, resulting in incomplete configuration.
989677	Update JavaScripts to the latest Long Term Support version.
1019750	The available interfaces list is slow in configurations with many IPsec tunnel connections.
1051870	After a firmware upgrade, some VLAN interfaces attached to LAG interface are not displayed in the GUI.
1071799	Failed to rename switch-controller managed-switch entries through the CMDB REST API.
1074529	Renaming an address object using the cmdb API in workspace mode transactions creates a new object instead of updating the existing one.
1084335	Existing API key may not work as expected with a 403 error *wrong vdom* displaying after upgrading to FortiOS version 7.4.5.
1107698	Adding ipv6-trusthost under api-user will override ipv4-trusthost setting and allow all IPv4 soure IP addresses.

Routing

Bug ID	Description
897308	The system fib version does not match VDOM fib version in 1801F when queried due to a misalignment in how genid is reported by the Linux kernel to user space.
981876	VRRP master stops sending advertisement messages for three seconds randomly during HA cluster operations in multi-VLAN environments.
1008434	The speed test result files are not deleted after tests run. The new test ID may collide with a previous result. In this case, the GUI may read a previously failed result and report errors.
1041812	In a hub and spoke HA configuration, SD-WAN pages take longer than expected to load in the GUI when there are a large number of spokes (~350) configured.
1042909	When creating a new static route on the *Network* > *Static Routes* page, the *Priority* field still displays when the *Destination* is switched from *Subnet* to *Internet Service*.
1044403	HTTPS/SSH traffic fails on the interface when policy routing is enabled due to incorrect ARP requests from cached routes.
1048338	Unexpected SD-WAN event logs are generated on HA passive devices indicating no role match or selected.

Bug ID	Description
1057504	PIM-SM fails to update the failback neighbor when a higher-priority DR becomes available in VRRP environments, causing incorrect routing decisions.
1058616	The SD-WAN Rules GUI page does not load on HA secondary FortiGates due to restricted access to the virtual-wan/health-check monitor API.
1058700	The load-balance mode in SD-WAN rules only considers up to 8 paths as active when more than 8 are configured.
1065805	A malformed payload error occurs when an ADVPN-2.0 shortcut-reply message has a msg id of 0 and is fragmented, bypassing proper reassembly in FortiOS.
1071662	Shortcut creation fails when using ADVPN 2.0 with BGP on Loopback interfaces for segregated transports due to depublication errors caused by incorrect VRF handling in specific FortiOS versions.
1072311, 1075911	BGP flaps occur when high L2P TPE drops are detected under heavy IPsec traffic conditions.
1084907	Inactive IPv6 routes occur when dual stack BFD is configured without assigning the correct interface for IPv6, causing it to default to an IPv4 interface instead.
1085897	VPNv4 routes are lost on restarting side when PE VRF exits graceful-restart prematurely before CE VRFs finish.
1086944	The BGP router-id fails to reset after editing the neighbor group settings because the dialog doesn't properly handle the reset functionality.
1091628	Interface IP addresses are incorrectly added and removed from the kernel before their interfaces are properly generated, causing secondary IPs to be deleted from other VDOMs during new VDOM creation.
1095307	Network > SD-WAN > SD-WAN Rules: Filtering on members with alias names does not display matching results.
1095879	Firewall policy page takes a long time to load on HA Primary unit due to loop condition between BGP and NSM when other protocol's same route is redistributed to BGP.
1096400	The SD-WAN Rules and Performance SLAs GUI pages fail to load correctly in large environments due to costly API requests loading all stats by default.
1100529	BGP Stale route not working as expected.
1106035	CPU usage issues observed during auto BMRK operations
1108192	Restoring image from FTP server failed using SD-WAN.
1109286	Incorrect priorities are applied during remote health-checks when iked restarts because lnkmtd retains stale tunnel cache entries.
1114687	The snmpd cache update takes longer when querying SD-WAN health-check data due to delays in retrieving bandwidth statistics.
1116924	In SD-WAN, when detect mode *Prefer Passive* is used, routing table is not updated in time

Bug ID	Description
1118891	ADVPN shortcut is established even between different transport-groups.
1119119	Inadvertent behavior observed in BGPD due to erroneous memory freeing when applying route-maps.
1122021	FortiGate disregard currently SLA valid SDWAN members for path selection.
1129698	When FortiAnalyzer setting `interface-select-method` is `sdwan`, FortiAnalyzer connection is closed and restarted, even though SD-WAN interface doesn't change.
1134763	Session marked dirty by mistake when unrelated route changes in different VRF.
1138483	The link-monitor daemon truncates hostnames exceeding 63 characters when used in SDWAN health-check configurations, causing DNS resolution failures and impacting service availability.
1142955	High CPU usage occurs when link monitor daemon fetches session counts on every interface during REST API calls.
1147497	Slow performance and network issues when surfing to Internet from GRE tunnels.

Security Fabric

Bug ID	Description
903922	GUI performance limitation - Security Fabric physical and logical topology is slow to load when there are a lot of downstream devices including FortiGates, FortiSwitches, FortiAPs and endpoint device traffic. This is a GUI only display issue and does not impact operations of downstream devices.
907452	On FortiOS, GUI access can be prevented when requesting a security rating over CSF from FortiAnalyzer.
987531	Threat Feed connectors in different VDOMs cannot use the source IP when using internal interfaces.
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 cannot load properly and displays a *Failed to load Topology Results* error.
1026700	Internal REST API requests are routed through the httpsd CSF proxy, leading to issues with chunked encoding for large responses and blocking behavior.
1040700	The external connector only allows users to specify the interface in the root vdom and not the vdom it is configured in.
1055616	External resources are not loaded immediately on devices without a disk after a reboot due to delayed forticron checks, causing a 30-minute delay before WAD reloads them.

Bug ID	Description
1068310	CSF root cannot accept downstream device with authorization-request-type serial/certificate with non-default management port.
1085248	FortiGate encounters CPU and memory usage issue when loading 20 large external threat feeds (100K entries each).
1098787	Azure SDN Connector failure occurs when service tags API returns empty results with Resource Group scope permissions.
1099235	Scheduled triggers do not include eventtime in log entries, causing automation scripts using %%log.eventtime%% to fail and generate filenames with missing or incorrect timestamps.
1110643	Security Fabric issues occur when running FortiOS 7.4 or 7.6 with 200G.
1111619	The `replacemsg-group` in `automation-action` gets unset when system reboots.
1113463	FortiGate Azure connector fails to retrieve AKS information on AKS 1.29.5.
1117104	Scheduled automation incorrectly triggers reschedule after reboot when using specific time zones and NTP configurations.
1118086	An error condition occurs when enabling CSF root on 50G series devices.
1119616	Externally maintained threat feed containing both resource FQDNs and IP address ranges/subnets. Entry like <addr>/0x1 then matches half of all possible IPv4 address and causing network disruption.
1120652	Fabric topology - 2 devices on different vdoms but behind same router show wrong vdom data on tooltip.
1134970	Inconsistent DNS TTL behavior in Kubernetes API through SDN-Connector.

SSL VPN

Bug ID	Description
858478	DTLS tunnels become unavailable after changing SSL VPN listen ports due to improper UDP socket setup during recreation.
947536	SSLVPN crashes on corporate FortiGate due to watchdog timeout when a single connection enters an infinite loop of read iterations and the worker process becomes unresponsive to new connections
995331	DTLS ports are disabled after changing SSL VPN settings' algorithm from high to medium or low.
1000674	When generating function backtrace in crash logs for ARM32, SSL VPN frequently crashes due to segmentation faults.
1026775	Remove SSL VPN from FG9xG.

Bug ID	Description
1047705	SAML login from a Windows FortiClient is blocked when `sslvpn-webmode` is disabled in the `config system global` command.
1058211	Traffic could not go through sslvpn tunnel when DTLS enabled with loopback interface as source address.
1063777	Login fails for local remote TAC+ users with FortiToken when waiting for token response.
1066564	SMB bookmarks become inaccessible through SSL-VPN web portal mode due to incorrect DNS server path definitions.
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.
1078149	Blocked internal resource access occurs when FCT reestablishes a TLS tunnel using the same DHCP IP after a brief link downtime, due to improper handling of the previous tunnel's AP session and tun dev index.
1082427, 1012486	The SSL VPN OS checklist in FortiOS does not include minor versions of macOS 13 and 14, nor macOS Sequoia 15.0.
1082696	When FCT reestablishes a TLS tunnel quickly after a network disruption, SSL VPN attempts an IP association with the same IP, causing a duplication and no value assigned to the tun dev index.
1083262	FNBAMD session hangs with massive auth request after a period time.
1094825	SSL VPN crashes when multiple routes are configured with the same address.
1101837	Insufficient session expiration in SSL VPN using SAML authentication.
1111135	Log additional debug information to aid troubleshooting.
1115510	SAML metadata fails to generate when haproxy binds to the reserved SSL VPN source port 8900, preventing SAML authentication.
1115577	Add customization support for the SSL-VPN header replacement message.
1122349	SSL VPN crashes and disconnects client connections due to a DHCP state machine issue, causing high CPU usage and watchdog timeouts.

Switch Controller

Bug ID	Description
1015992	WiFi & Switch Controller > Fortilink Interface: When a Fortilink interface is down and the 'Lockdown ISL' toggle is set to 'disable' on the GUI, the setting is not retained.
1016034	In HA environments with FortiSwitches connected, the lockdown ISL setting on Fortilink gets enabled during HA failover.

Bug ID	Description
1034470	FortiGate GUI shows multiple entries for the same FortiSwitch when exporting it for use by several VDOMs.
1044150	Firmware installation fails when upgrading FortiSwitch devices through FGT GUI.
1055052	The NAC policy is not visible in the GUI due to switch-fortilink not set in the NAC policy.
1069164	The managed switch incorrectly reverts to the default time zone after reboot due to improper handling of zero-minute GMT values in the configuration.
1071594	Users cannot de-select all values from Allowed VLANs and related policies due to a GUI malfunction.
1074981	The FortiSwitch port configuration GUI under FortiOS 7.6.0 no longer allows users to de-select all values for Allowed VLANs, Security Policy, or QOS Policy.
1077496	High CPU utilization occurs when flpold/flcfgd processes mishandle socket messages during WAD operations due to incomplete or corrupted data.
1096481	Access-mode changes cannot be made for FortiSwitch ports when using the FortiOS GUI.
1108965	Sync errors occur when incomplete transaction flags related to dhcp-snooping-static-client replay past configuration changes during sync attempts.
1113465	VLAN configurations intermittently fail to assign on FSW ports when devices matching DPP policy come online, caused by a race condition during FSW initialization.
1124356	DPP mac classification issue occurs when DPP policy with vlan-policy and 802.1x is configured together.
1130242	Only the last SNMP community configuration is pushed from FGT to FSW during bulk processing.
1138333	Increase Fortilink configuration daemon memory usage efficiency.

System

Bug ID	Description
860534	VDOM settings are removed after rebooting FortiGate in TP mode with multiple VDOMs enabled.
901621	On the NP7 platform, setting the interface configuration using set inbandwidth <x> or set outbandwidth <x> commands stops traffic flow.
932077	Connection issue between SOC4 platform and third-party switches, for example Hirschmann GRS 105 or Cisco switch, because SOC4 doesn't support certain carrier extension signals.
934342	LED of MGMT and HA port do not go off after issuing "execute shutdown" on some models.
953547	SCTP traffic does not get forwarded by a connected hardware switch on FortiGate.

Bug ID	Description
973034	LACPDU packet drops occur when FortiGate fails to reliably send required packets due to incorrect npu_tc assignment for hi-priority traffic.
976722	Invalid YAML files are generated when exporting configurations containing multi-value attributes or long strings with newline characters.
979645	TCP traffic is classified as ip-frag and dropped when HPE entries are incorrectly configured in FortiOS versions prior to the fix.
984696	Network usage is not accurately reported by the `get system performance status` command.
986926	On the FortiGate 90xG models, the ULL interfaces for x5 - x8 are down after being set to 25G speed.
992323, 1056133, 1075607, 1082413, 1084898	Traffic interrupted when traffic shaping is enabled on 9xG and 12xG.
996863	Automatic firmware updates trigger email alert after every reboot of FortiGate.
1010899	Config loss occurs when restoring SNMP mib-views configuration.
1012577	Traffic on WAN interface is dropped when `policy-offload-level` (under `config system setting`) is set to `dos-offload`.
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.
1017941	On the FortiGate 220xE and 330xE, the GUI interface bandwidth show terabyte spike for gigabyte interface.
1024737	On FortiGate, when `set ull-port-mode` is set to 25G, ports x5-x8 show a status of DOWN.
1027335	Interface cannot ping out with dos-offloading enabled but no DoS policy.
1034821	On FortiGate, NP7 offloaded traffic does not use the updated MAC address from the ARP table to forward traffic using a GRE tunnel.
1039956	FortiGate 601F port x6 keeps flapping after upgrade.
1039980	Unexpected behavior in system occurs when out of memory during emergency restart.
1040137	NPD skips config parsing when policy-offload-level set to disable.
1042577	FortiGate does not detect transceivers and interface X8 not coming up after upgrade.
1044178	No ICMP error messages are sent when oversized packets are received by IPv6 tunnels with fragmentation disabled.
1044472	Traffic drop occurs when VXLAN is a member of software switch in implicit mode.

Bug ID	Description
1045301	Config revision files are incomplete during restores after firmware updates due to background save timeouts.
1045701	FGT-80F-BP fails to boot up after burning image, showing error message "cli 161 die in an exception in line 300: end".
1046484	After shutting down FortiGate using the "execute shutdown" command, the system automatically boots up again.
1047996	FortiGate 4800F model split ports do not work as expected causing issues with LACP and MRU on split ports.
1048496	On FortiGate, the SNMP daemon does not work as expected resulting in the SNMP queries timing out.
1048684	The FortiGate Internet Service Database (ISDB) update mechanism fails on a 100E FortiGate model due to insufficient memory allocation.
1050162	The `auth-pwd` and `private-key` error after upgrading from B2662 when `private-data-encryption` enabled.
1054955	USB GPIO and host function were not set up properly on 9xG and 12xG.
1056166	Error messages appear during bootup when FortiOS devices that support CGNAT lack a valid hyperscale license.
1056580	Lack of speed options occurs when configuring network interfaces on FGT91G/121G devices, limiting available settings.
1057098	The "dsl" test appears in hardware tests for non-DSL models where it should not be enabled.
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.
1058740, 1073326	Unexpected behavior observed in entry-level FortiGate models, including FortiGate VMs with less than 2 GB of RAM, during system updates due to memory allocation issue.
1060729	IPsec tunnels become unreachable on FortiGates with np7lite hardware when "vpn-id-ipip" is configured due to missing support for VPN ID IP/IP offloading in NPU processing.
1061796	Inaccurate traffic counters display for EMAC-VLAN interfaces when VLAN ID is set to 0 and traffic is offloaded to the NPU.
1063017	Factory reset does not complete with reboot after receiving "execute factoryreset" command from FortiManager.
1065553	An incorrect /8 connected route is advertised by FortiGate 80F-DSL when configured with a LANTIQ-based DSL modem.
1066296	snmpwalk receives "No Session Data" response of fgFwPolLastUsed OID while the background traffic keeps running.
1066622	Source IP is not getting replaced as per the config 'set fmg-source-ip ' after adding the device directly.

Bug ID	Description
1067448	VLAN switch is not working on 120G/121G.
1068756	After updating to the latest unsigned version of an object, update daemon will not download a new signed version of that object, if the versions are the same.
1069208	If the DHCP offer contains padding when DHCP relay is used, the DHCP relay deletes the padding before relaying the packet.
1069686	Mediatype options don't match the serdes capabilities of 100G ports on FGT3980E devices, causing failed mediatype settings.
1071229	Ping reply packets are dropped after two successful requests when using VXLAN over IPsec on FortiGate.
1071749	Write permission violation log observed in FortiGate in a rare case caused by the host check plugin used in FortiClient/browser side.
1072320	Link/Activity LEDs of MGMT and HA ports remain lit after executing 'exec shutdown' in FortiOS v7.4.2 and later.
1072787	IPv6 connections fail when iPhones access test sites via IPoE due to improper handling of NA messages using link-local addresses.
1074099	Factory reset fails when command is received from FMG.
1075032	NP7 offloaded traffic continues to use old gateway's MAC address when receiving packets with TTL=1 after a gateway change.
1075116	Admin user gets logged out when entering an 'unset sdns-server-ip' command in FortiOS CLI during configuration through a tool with specific command timing and sequence.
1075279	Member interfaces of VWP appear in packet capture creation dialog despite being ineligible.
1076883	When the top application bandwidth feature is disabled, the GUI process still performs the initial check for application bandwidth, which may cause FortiCron to experience high CPU usage.
1077562	Hardware egress shaping doesn't work on SOC5 when NPU offload is enabled.
1078119	Traffic is intermittently interrupted on virtual-vlan-switch on Soc5 based platforms when a multicast or broadcast packet is received.
1078568	When FortiManager adds FortiGate via serial number and is behind NAT, FortiGate cannot initiate requests to FortiManager, causing the GUI to fail in retrieving the certificate CN/SAN and resulting in an error.
1079850	HA1/HA2 ports down until reboot after set status up.
1082005	PCI test failure occurs when running HQIP test.
1082415	4G USB modem Huawei K5161Z not working in FG-90G.
1085990	CRC errors occur on NP6 platform SFP port when connected to Cisco ISR 4431 with fiber transceiver.
1086268	VXLAN interface cannot be created if its underlying interface is DHCP.

Bug ID	Description
1111818	Traffic drop by NP when vxlan as a member of software switch in implicit mode.
1087270	Unexpected traffic increase over the FortiGate 6000 base backplane.
1089143	The time change in FOS is restored after reboot. The RTC node is not created correctly so the time change can't be kept in RTC.
1089397	Frequent kernel panics occur due to dynamic update of EMS IP/MAC addresses in multiple VDOMs, causing the device to freeze and require a reboot.
1090372	Access profile entries exceed global limit when built-in profiles consume table size slots.
1091175	VLAN statistics on LAGs are not displayed correctly when asic-offload is enabled due to incorrect OID usage.
1091551	Hardware limitation on the NP7 platform causes the following QTM related issues: • Incorrect checksum for fragments after QTM. • Packets longer than 6000 bytes cause QTM unresponsiveness. • Refresh issue causes QTM unresponsiveness. • MTU is not honored after QTM, so packets are not fragmented.
1093042	High memory consumption occurs when multiple SNMP child processes are created due to frequent queries, as they fail to terminate properly and accumulate in memory.
1094404	State of peer ports of FGT ports(negotiated speed, 1G) is down after upgrade on specific FGT.
1095834	When FortiGate is managed by FortiManager, which has a slow connection or is unreachable, memory consumption of node process keeps increasing.
1096409	EXPIRE dates cannot be displayed properly when displaying the output of `get sys fortiguard-service status`.
1102416	Cannot push `config sfp-dsl enable` and vectoring under interface.
1102919	GTP tunnels are deleted, even when associated requests exist. The problem occurred when multiple Create Session Request from different source IPs create the same GTP tunnel, and the first Create Session Response with an authentication-failed cause leads to the deletion of the half-open tunnel and all associated requests.
1103146	Duplicated RADIUS packets are captured by the sniffer when performing firewall authentication with a RADIUS server.
1104173	Kernel panic occurs when pushing 'Device Setting' from FortiManager to NP7 platforms with Broadcom switch, causing the device to become unresponsive and requiring a reboot.
1104410	The FortiGate 120G SFP ports fail to establish connectivity when configured with 'set speed 1000full' due to improper auto-negotiation handling.
1105989	System global configuration lost due to port collision.
1105995	The switch MTU doesn't set correctly on 100m speed.
1107270	Communication over VXLAN is lost after upgrade on NP7 platform.

Bug ID	Description
1109633	When visiting the GUI login page, FortiGate prompts user for certificate when no PKI admin is set.
1110461	CLI permission settings under `prof_admin` return to their default value after reboot.
1113720	Packets not forwarded due to improper handling of specific flags in the bridging code, which incorrectly treats them as local instead of resolving their destination MAC address and forwarding.
1113795, 1133386	FGT 200G cu_acd process didn't restart after "diag sys kill 9 <cu_acd pid#>".
1114594	On the FG-200G, SDNS is unable to connect to FortiGuard servers. This issue only affects FG-200G.
1115486	Virtual switch interface drops LLDP packets.
1116220	FortiGate 3601E 25Gauto link not coming up using DAC cables.
1117005	CPU spikes and management access issues occur on certain FortiGate models post-upgrade when IPsec Phase 1 NPU-offload is enabled during maintenance.
1117819	6-Byte fragments are dropped by NP7 when handling short CAPWAP packets when performing a check.
1119595	URLfilter fails to track DNS TTLs and update the IPs of FQDN addresses after they have been changed.
1120467	No SNMP trap at power failure for DC PSU.
1121522	Memory leak in slab causes the system to enter memory conserve mode. The issue occurs due to out-of-order log packets and incomplete session scrubbing, resulting in residual entries in the log2host table.
1121548	Enabling `device-identification` also gets endpoint information, even though intermediate router exists on FGT and endpoints.
1122032, 1130921	Traffic fails to transmit through the NP7Lite interface on FG-50G-5G and other SoC5 platforms.
1122741	Two duplicate FGFM sessions could be triggered when connecting to FortiGate Cloud, and the first FGFM session that enters in GET_IP state kills the other FGFM session, which schedules an FGFM session restart two minutes later.
1123727	Incorrect traffic class (TC) settings and shaper class ID handling cause improper Quality of Service (QoS) application and session offloading failures for VLANs configured over Link Aggregation Groups (LAG) and hardware switches on FortiOS devices using SOC5 hardware.
1124024	When `set append-index disable` in `system.snmp.sysinfo`, querying per-VDOM BGPPeerTable might get incorrect results because of no updates.
1125301	FortiGate encounters parsing errors and potential system halts when configuration strings contain un-escaped single quotation marks, especially in password fields.
1125947	FortiGate encounters a memory usage issue due to usage by HTTSD.

Bug ID	Description
1126100	Expired user passwords are stored as plaintext in configuration files when password history is enabled.
1126327	The SNMP query for fgSwPortSwitchSerialNum is giving switch name as the output instead of SN.
1127534	Update built-in CRDB bundle to version 1.56.
1127700	Packets are dropped during VLAN over VXLAN traffic due to incorrect handling of VLAN tags and session keys.
1128087	In new version of RDP client, FGT drops some RDP sessions due to IPv6 extended headers.
1128311	np7lite models kernel panic and reboot during stress test with configuration changes and background traffic.
1130265	Add "Host:" field in HTTP 1.1 header in proxy CONNECT for FortiGuard.
1132414	When connecting port5-14 on 3201F with third-party switches using optical transceivers, the 1 GB link is down.
1133159	Inbandwidth settings are not enforced for traffic with multiple class IDs in a FortiOS shaping profile, resulting in reduced available bandwidth beyond 12 classes.
1133575	The 100M speed option is not available for wan1 and wan2 interfaces during configuration in certain FortiGate models.
1136151	GRE traffic does not work and device access is lost over the tunnel.
1136646	Enabling private-data-encryption corrupts certificate after restoring backup file.
1137220	diagnose traffictest run -c a.b.c.d returns error.
1142591	Unexpected behavior occurs when high load IP fragment traffic is sent through an IPsec tunnel with vpn-id-ipip encapsulation and offloading enabled.
1142782	GRE tunnel traffic is limited when sessions share same local/remote IPs, causing them to be assigned to single CPU core.
1152059	Device information is not detected when device-detection is enabled.
1153285	FGT loses SSH/HTTPS/HTTP access after config revert, displaying repeated warnings about BIOS creating subtree suites.

Upgrade

Bug ID	Description
1087263	Upgrading an FGCP HA cluster of FortiGates with NP7 processors from 7.2.8, 7.2.9, or 7.2.10 to FortiOS 7.4.5, 7.4.6, or 7.4.7 may cause the cluster to experience an infinite reboot loop. This issue has been resolved by FortiOS 7.4.8.

Bug ID	Description
1097503	Fabric upgrade from 7.2.9 to 7.4.5 failed.
1102990	SLBC FortiGate 5001E primary blade failed to install image, even though graceful-upgrade was disabled.
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. See Policies that use an interface show missing or empty values after an upgrade on page 25 for more information.
1106072	The image file transfer between FortiManager and FortiGate may not work as expected when transferred by the FGFM tunnel.
1110809	Egress-shaping-profile setting lost on interface after upgrade.
1114232	When upgrading FortiGate from earlier than 7.4.1 to 7.4.1 or later, system.replacemsg.webproxy configuration is lost.
1123954	FortiGuard updates are automatically enabled during upgrades from versions where they were previously disabled, bypassing user acknowledgment.
1130861	FG-4401F enters a reboot loop after upgrading from 7.2.9 GA to 7.4.6 GA with a large config file (more than 10K policies).

User & Authentication

Bug ID	Description
940989	Page fails to reload after successful FTM push authentication for remote LDAP users in firewall policies.
957637	*System* > *Certificates*: When a valid signed CA certificate is uploaded on the FortiGate, "Unable to create certificate" is displayed. This is a cosmetic issue. The certificate is uploaded and can be verified through the command line or the GUI after upload.
1008709	EST HTTP passwords are not encrypted in the config file during certificate enrollment with EST.
1020808	Use new keys for cert renewal via EST server.
1025260	Wildcard admin remote auth passwd change in system GUI does not work.
1042326	Admin access to GUI remains valid despite exceeding the two-factor-email-expiry timeout.

Bug ID	Description
1043189	Low-end FortiGate model with 2GB memory can experience conserve mode when processing large user store data with over 5000 user records and each record has large number of IoT vulnerability data. For example, the Users and Devices page or FortiNAC request can trigger the following API call that causes httpsd process to spike in CPU and memory. GET request /api/v2/monitor/user/device/query
1043222	CMPv2 IR does not work as expected due to server certification validation error conditions.
1044084	On the Dashboard > Firewall User Monitor page, the Search field does not display in the GUI when there are a large number (+1000) FSSO user logos.
1070743	FortiToken activation-code emails fail to send when using the shortcut method due to missing recipient email addresses in the logs after an upgrade.
1075207	Errors may occur in the FNBAMD due to the presence of two wildcard-enabled remote administrators in separate VDOMs.
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.
1080510	SCEP certificate auto-renewal fails to trigger when forticron experiences excessive pending DNS requests due to server unavailability.
1093538	In SAML config, after enabling AD FS claim and rebooting, "Attribute used to identify users" and "Attribute used to identify groups" fields will be blank.

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.

1137727	Delays in SSH login verification occur on some FortiGate models when hashing passwords, and immediate failure messages are returned for invalid usernames.

VM

Bug ID	Description
999842	Azure fails to honor seamless live migration. In most cases, the public IP to private IP NAT fails to forward traffic from/to SD-WAN.
1012000	When unicast HA setup has a large number of interfaces, FGT Hyper-V takes a long time to boot up.
1019467	When the underlying interface is removed, the IPsec tunnel interface will still hold a dst reference.
1030534	On FortiGate, an HA failover does not work as expected when using an OCI environment.
1061669	FGT_KVM console cannot be accessed using serial tools under a trial license when configured with multiple virtio interfaces and queues.
1067046	Dynamic firewall address list entries are deleted when AWS STS tokens expire prematurely.
1070910	FortiFlex license fails to install consistently during Day0 configuration when using Port2 for Internet access, as injection occurs before connectivity is established.
1082197	VLAN traffic fails to pass through E810-XXV NIC with SFP28 transceiver and 25G speed after enabling DPDK.
1083073	Security rules with port range can be pushed to the Azure VWAN SLB successfully, but the SLB doesn't allow the specified port range.
1085482	Instability occurs in Azure FGT-VM with MLX4 DPDK configurations due to unsupported data paths.
1088457	DPDK process failed to initialize with certain combination of hugepage and mbuf settings in dpdk global setting.
1092977	PPPoE interfaces on VM not getting IP address after firmware upgrade.
1093458	The FGVM console becomes unresponsive after a hard reboot in OpenStack environments running on Redhat Enterprise Linux 9.2 when using USB keyboards.
1094274	FortiOS becomes unresponsive when sending IPv6 traffic over MLX5 network adapters due to incorrect WQE handling.
1094600	The virtual-wire pair fails to create during FortiOS initialization on cloud platforms when the underlying interface uses DHCP and hasn't acquired an IP address yet, preventing VXLAN configuration from completing successfully.
1101264	HA failover actions are triggered even when the Azure SDN connector is in a "disabled" state, causing increased downtime during failover.
1107933	The FortiGate device uses a single CPU core for GRE decapsulation tasks when running on AWS with ena NIC drivers because L4 hash functionality is not enabled, preventing RPS from distributing traffic efficiently.

Bug ID	Description
1107962	Dynamic addresses are removed/added every few seconds when the OCI SDN connector fetches only the first page of API results.
1109724	Azd daemon on Azure NVA keeps consuming memory until FortiGate enters conserve mode.
1121521	Azure SDN connector does not properly catch AKS cluster state.
1121974	Due to continuous disk logging, slab memory for dentry continuously increases in FortiGate VM.
1135522	One of the FGSP standalone cluster with config-sync enabled keeps showing kernel warning logs. HA constantly became out-of-sync.
1146370	AWS bootstrap is unable to parse IAM role profile properly due to the length.
1146634	ifLinkUpDown SNMP trap is not triggered on FGT_VM64_KVM using the virtio driver when an interface is brought up or down.

WAN Optimization

Bug ID	Description
642875	Memory usage issues caused by an error condition in WanOpt.

Web Filter

Bug ID	Description
537134	When a webfilter time-based quota is configured, once quota is reached, long session are not terminated.
874516	SMB traffic fails when the file server uses AES-256-GCM/CCM encryption with FortiOS.
906603	Security Profiles > Webfilter: When a new webfilter is created and the action on the FortiGuard category based filter is set to 'allow' and saved, the action is saved as 'monitor' on commit.
1093624	URLs fail to match intended regex patterns when special characters are escaped with backslashes.
1099818	Output of `diagnose webfilter fortiguard cache dump` command shows the message "Cache is not enabled".
1107456	FG120G webfilter.profile tablesize is incorrect.

Bug ID	Description
1118132, 1122036, 1127984	Webfilter local category override not working after reboot in flow mode.
1131440	Webfilter user category override not working after reboot in flow mode.
1138711	Webfilter user category (local and external) override databases are not recreated after FortiGate reboot after reboot or IPS engine restart.

WiFi Controller

Bug ID	Description
823387	Email addresses collected through captive portal fail to display under WiFi clients when using guest SSID configurations.
921080	The Fortigate Hostapd does not support IPv6 address of RADIUS server.
949682	Intermittent traffic disruption observed in cw_acd caused by a rare error condition.
987030	Unexpected behavior observed in the CAPWAP daemon when managing multiple APs and clients through dynamic VAP changes.
1018895	Clients on local-bridging SSIDs appear offline despite having active traffic when acd-process-count is 2, caused by the AP failing to report client IPs to the controller.
1030197	Client traffic is blocked after a failure when connecting through SSID using radius-mac-auth and radius-mac-auth-usergroup because the secondary FortiGate in HA does not receive necessary client details during failover.
1033483	Secondary AC wpad_ac memory usage increases during stress tests with simulators in HA setups.
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.
1062560	GUI Local WiFi Radio Channel Utilization shows "N/A" while it is actually available and readable.
1063976	Empty SN values occur in AP DTLS session timeout messages.
1071329	Change the region/SKU assignment of the following nine countries: BB, BZ, CO, DO, GD, GY, HN, FM, and PA to A (from K model) or N (G & Older model).
1073390	Duplicated WiFi event logs occur when acd-process-count is set for multi-core processing in FortiGate.
1075138	An unknown source IP appears in client-authentication logs when laptops connect to wireless networks at specific sites.

Bug ID	Description
1076738	Group name fails to display in station list after local authentication with 2FA for Enterprise+User-group SSID connections.
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.
1086128	An error condition in CAPWAP occurred due to a rare case.
1089563	The VLAN ID is lost during roaming with WPA-PSK and Fast BSS Transition enabled, causing connectivity issues as the client loses its network segmentation.
1089999	FAPs remain offline post-upgrade when using image stored on FortiGate.
1091796	DFS channels are allowed to configure on the wtp-profile of FAP-241K/243K in regions "A", "E", "I", "Y", "S", "V", "H", "D" and "N" (without Brazil).
1094415	VLAN pooling assigns incorrect VLAN IDs when FortiOS is upgraded, causing clients on AP groups to receive IPs from the optional VLAN instead of the pool.
1096961	The "AP image receive success" log (id 43618) does not generate when upgrading FAP from FMG.
1098727	Enable 5GHz channels 52-64, 108, 116-128 for FAP-231G-P, 431G-P Uzbekistan. (Uzbekistan has no DFS certification process.)
1098819	FortiAPs show as "Not Registered" after FortiGate web page reloads following a firmware upgrade.
1100220	COA disconnect is not functional for MPSK profiles when using external FortiGuest.
1101583	FortiAP goes offline when the cw_acd process becomes stuck at 99% CPU usage. This issue is caused by the FortiAP sending corrupt data in certain scenarios, leading to the process hanging.
1102808	When the configuration contains a large number of vlan-pool entries, deleting or adding a few entries can cause the cw_acd crash.
1108726	FortiAPs periodically lose connectivity with FortiGate (acting as WLC) due to an error case.
1114144	WSSO firewall authentication sessions fail to establish when FortiGate processes multiple group attributes with the initial group missing.
1114311	Packets are incorrectly routed when FAP management interface uses clear-text dtls-policy in a software switch with explicit intra-switch-policy.
1123829	Support legal firewall policy when SD-WAN/zone member interface manages FAP with `dtls-policy` set to `ipsec-vpn`.
1128272	Management connection fails for FAP-231F when using PPPoE interface on FGT-120G.
1130750	WiFi & Switch controller > Managed FortiAPs: When a channel override on a 5GHz channel is enabled is edited on a managed AP, the channel selection is unset.

Bug ID	Description
1131094	The iPhone 16 fails to connect to a WPA3-SAE SSID on FWF-61F due to incorrect ordering of RSN and RSNXE parameters during the authentication handshake.
1132497	Compilation issue occurs when building FWF models in v7.4.8 B2767
1133829	The FAP remains offline after the FortiGate reboots or wireless-controller restart-acd due to the controller sending an empty country string to the access point.
1151713	FortiAPs may go offline when memory pool of WiFi daemon cw_acd is fully occupied and not released properly. cw_acd debug constantly shows `ERR: NO MEM for USER_LOCAL_MSG`.
1154739	FAP registration statuses are not properly retrieved from the REST API when converting JSON arrays to delimited strings due to improper pointer offsetting during string copying.

ZTNA

Bug ID	Description
1020084	Health check on the ZTNA realserver does not work as expected if a blackhole route is added to the realserver address.
1035072	FortiClient access to TCP-FWD with SAML authentication does not redirect the loop if `set ztna vip` and `saml SP` use the same IP address.
1056179	PPPoE encounters a performance issue after an upgrade.
1101022	FortiClient gets a blank page when doing SAML authentication due to the use of a stale user node.
1114976	ZTNA policy matching failed due to an accidental deletion of firewall.policy with ztna tags when the firewall.policy is updated.
1115153	Authentication loops occur during ZTNA connections requiring SAML when FortiClient uses multiple sessions with inconsistent cookies.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
1005155	FortiOS 7.4.8 no longer vulnerable to the following CVE: • CVE-2024-55599
1051974	FortiOS 7.4.8 no longer vulnerable to the following CVE:

Bug ID	CVE references
	• CVE-2025-25250
1070560	FortiOS 7.4.8 no longer vulnerable to the following CVE: • CVE-2025-22252
1077059	FortiOS 7.4.8 no longer vulnerable to the following CVE: • CVE-2024-52963
1081022	FortiOS7.4.8 no longer vulnerable to the following CVE: • CVE-2025-22862
1085628	FortiOS 7.4.8 no longer vulnerable to the following CVE: • CVE-2025-24471
1103790	FortiOS 7.4.8 no longer vulnerable to the following CVE: • CVE-2025-25248
1108301	FortiOS 7.4.8 no longer vulnerable to the following CVE: • CVE-2025-22254
1137151	FortiOS 7.4.8 no longer vulnerable to the following CVE: • CVE-2025-53744

Known issues

Known issues are organized into the following categories:

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 7.4.8.

Explicit Proxy

Bug ID	Description
1103272	SSL certificates are misapplied when FortiGate processes requests with deny actions in proxy policies.
1056600	Unexpected behavior occurs during WAD module initialization on FortiGate devices due to improper dependency management leading to order issues or missing dependencies.

Firewall

Bug ID	Description
1088905	Virtual server HTTP health-check is always using IP address as a host, even when the full URL is configured in http-get.

FortiGate 6000 and 7000 platforms

Bug ID	Description
1104569	FortiGate FPM hangs after upgrade when confsynchbd fails to release a lock due to file permission issue.

Bug ID	Description
1147340	Duplicated interface entries occur in FortiGate HA configuration merges when the same interface is processed across multiple cycles without successful resolution, causing persistent sync failures and redundant log entries.
1153360	Counter values fail to match totals and may overflow during continuous clearing in certain FortiGate models.
1159714	Unexpected behavior observed on certain FortiGate models when configuration changes follow enabling "cfg-save revert" due to unresolved netdevice references in the np7 driver.
1171521	In some cases, after a FortiGate 7000F chassis restart, an FPM may hang while logging in, resulting in the FPM being out of synch with the chassis. This happens because confsynchbd becomes stuck after receiving a management heartbeat from the primary FIM. The issue can occur any time the chassis restarts, including after a firmware upgrade. **Workaround**: The active SMM and the primary FIM must both be in the same slot (for example, FIM1 and SMM1). Use the SMM `smm_switch` command to change the active SMM, which may help avoid the issue the next time the chassis restarts. Reboot all FPMs. This fix is not permanent. The issue can occur if the chassis restarts.
1173956	Too many addresses included in EMA Tag entry cannot be properly inserted as dynamic address objects causing traffic to fail because traffic cannot properly match the related firewall policy.

GUI

Bug ID	Description
1024000	FGT 4400F displays TB on 2 x 100 Gig VLAN interface bandwidth widget.
1145475	Multicast traffic dropped when adding or removing the Interface Bandwidth widget on dashboard.
1149411	Increased Node.js memory usage occurs caused by errorneous memory allocation.

HA

Bug ID	Description
1033083	HA sessions are not properly synchronized, causing a high number of sessions on the primary unit, and the standby unit enters conserve mode.
1068674	PBA logs missing during HA failover.

Bug ID	Description
1162432	Split brain occurs when renaming IPsec phase1-interface in an HA cluster with a lot of VDOMs.
1179351	FortiGate failed to load the private keys for factory certificates to fgfmd due to incorrect classification.
1210147	HA out-of-sync occurs due to certificate.

Hyperscale

Bug ID	Description
1155548	With host logging (log2host) enabled, session counts may begin to rise after a few days of operation. The rise in session count can reduce throughput and CPS performance. **Workaround**: Restart the FortiGate.
1219541	Traffic disruption occurs when changing an interface's VDOM. **Workaround**: Use two static routes 0.0.0.0/1 and 128.0.0.0/1 as the default route instead of 0.0.0.0/0.

IPsec VPN

Bug ID	Description
1101897	Abnormal spikes in VPN traffic sent bytes occur when counters roll back due to race conditions.
1125487	Gateway switching fails during IKE session resumption when moving from a FortiGate model without Azure AD auto-connect enabled to one with it due to missing mode communication.

Log & Report

Bug ID	Description
1130821	Incomplete log entries occur when attack context logging is enabled for attacks involving long user-agent strings.

Proxy

Bug ID	Description
1116771	Add a limit on the memory used by user-device-store as a percentage of the total system memory.

Routing

Bug ID	Description
969992	FortiGate devices may route SCTP traffic using outdated routes instead of the current optimal path when certain conditions are met.
1133796	IPv6 routes are stuck on kernel routing table.
1150878	The IPoE tunnel interface cannot be selected in the Interface Bandwidth widget.
1171689	Incorrect route selection occurs during BGP redistribution with route maps due to improper handling of parent protocol distances.

SD-WAN

Bug ID	Description
1199707	SIP traffic issue occurs when TCP syn-ack packets use a different egress interface than the syn packets. **Workaround**: Use UDP for SIP traffic.

SSL VPN

Bug ID	Description
1164811	SSL VPN web mode showing Access Denied error after upgrade on 2GB models.

System

Bug ID	Description
991285	Broadcasts are unexpectedly forwarded between VXLAN peers when certain FortiGate models are configured as hubs in a Hub-Spoke topology.

Bug ID	Description
1084819	FGT80F/81F LACP/shared ports wan1 and wan2 are down after an upgrade or reboot due to hardware shared-port medium changes.
1136616	No graphs on some VLAN interfaces in dashboard Interface widget.
1145397	When editing user exemption configurations via the GUI on FortiGate devices, unexpected behavior occurs due to a mismatch between GUI and CLI data structures.
1156262	An "Input value is invalid." error appears when configuring the maximum number of sessions in FortiGate's global resources.
1164332	NP7 stops forwarding traffic after reassembling large packet in DFR.
1197885	Memory usage issues caused by ASLR when upgrading from 7.4.7GA to 7.4.8GA. **Workaround**: Disable proxy-inline-ips.

Upgrade

Bug ID	Description
1135049	An error condition in ips_load_json_gzfile occurs during FortiOS same image upgrade.

User & Authentication

Bug ID	Description
1118212	Captive portal authentication fails after FortiToken push notification approval during radius authentication with FAC for remote groups.
1122979	Custom NAS-ID not sent to RADIUS server when testing connectivity via GUI.

VM

Bug ID	Description
1113362	FGT_VM_AZURE cannot establish connection with other FGTs in the Security Fabric tree.
1125437	The "set distance" option under interface configured as dhcp client doesn't work on VM.
1172881	IPS engine crash w DPDK enabled, stress traffic over ipsec tunnel and fragmentation, and "system affinity-packet-redistribution".

WiFi Controller

Bug ID	Description
1144969	Mismatch IP address details in *WiFi Client* GUI page.

ZTNA

Bug ID	Description
1121978	Adding new HTTPS/HTTP ZTNA server mappings via GUI fails with a duplicate entry error, while attempting to exit after cancellation alters existing entries' URLs.

Existing known issues

The following issues have been identified in a previous version of FortiOS and remain in FortiOS 7.4.8.

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.
1004263	Session counters not updated when ASIC offload is enabled on firewall policy. FortiGate GUI displays incorrect information in the *Bytes* and *Last Used* columns.
1114635	Unable to filter address object by CIDR notation.
1148166	Source port translation was not permitted with traffic to UDP port 7001.

FortiGate 6000 and 7000 platforms

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

1070365	FGCP HA session synchronization may stop working as expected on a FortiGate 7000F cluster managed by FortiManager. This happens if the HA configuration uses management interfaces as session synchronization interfaces by configuring the `session-sync-dev` option, for example:
	`config system ha`
	`set session-sync-dev 1-M1 1-M2`
	`end`
	The problem occurs when FortiManager updates the configuration of the FortiGate 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.
	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.
1092728	On FortiGate 6000 and 7000 platforms, fragmented IPv6 traffic is randomly dropped.
1149342	BGP flapping occurs when concurrent IP address management causes unexpected source IP usage on outbound connections during FortiGate VDOM migrations.

FortiView

Bug ID	Description
1123502	FortiView Threats: drill down to malicious website entry, and *Failed to retrieve FortiView data from disk* is returned.

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.
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.
1152464	The DHCP reservation widget incorrectly validates based on the subnet instead of individual IP addresses.
1153294	Custom HTML content does not render correctly on login pages when configured through the FortiGate web interface or CLI.

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.
1135376	When HA members are not registered under the same FortiCare account, the HA cluster cannot obtain contract info of all members from FortiGuard servers.
1151668	Interface bandwidth widget doesn't display HB and Managed port.
1226122	System > HA: There is no upgrade button on secondary GUI page when HA in local-only or secondary-only MVC upgrade mode. **Workaround**: upgrade the secondary via the command line.

Hyperscale

Bug ID	Description
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.

Bug ID	Description
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.
1025908	Session count on peer device is 50% less during fgsp testing in new setups using VRRP-based configuration.

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.
970703	FortiGate 6K and 7K models do not support IPsec VPN over vdom-link/npu-vlink.
1140823	IPsec tunnels become stuck on spoke np6xlite, causing ESP packet drops after extended operation due to improper vifid formation during multiple rekey operations.
1152486	Unable to select policy-based IPsec tunnel in the firewall policy for SD-WAN member when configuring in GUI.

Log & Report

Bug ID	Description
1113588	FortiGate displays 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 fail to appear in FortiAnalyzer, and FortiView sources are missing from the Dashboard.

Proxy

Bug ID	Description
1035490	The firewall policy works with proxy-based inspection mode on FortiGate models with 2GB RAM after an upgrade. *Workaround*: After an upgrade, reboot the FortiGate.

REST API

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

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`

1142290	An error message appears in FortiGate when attempting to add the ssl.root interface to a route-map via the GUI.

Security Fabric

Bug ID	Description
1076439	Security Fabric Asset Identity Center shows *"Failed to load user device store data"*.
1149817	*Security Fabric > Physical Topology*: FortiLink Tier2 switch shows directly connected to FortiGate on *Security Fabric - Physical Topology* page. The correct topology can be seen on the *WiFi & Switch Controller > Managed FortiSwitches > Topology* view.
1150382	Security profile names containing two forward slashes (//) cause the web page to become unresponsive when attempting to edit.
1156006	SFTP backup fails when triggered through automation stitch on a FortiGate in an HA cluster using Windows-style paths.

Switch Controller

Bug ID	Description
961142	An interface in FortiLink is flapping with an MCLAG FortiSwitch using DAC on an OPSFPP-T-05-PAB transceiver.
1114032	The GUI becomes slow or unresponsive when transceiver-related API requests fail.
1138263	FortiSwitch port configurations fail to update and GUI display issues occur when user-info process overloads system resources with excessive connections.
1146176	config sync error on managed FSW after upgrade when "Name" field and port exported are configured on the same FSW.
1150215	Offline FSWs show as offline in the GUI topology view but show as online in the list view.
1153175	Intermittent issues configuring allowed VLANs on the MCLAG interface using FortiGate GUI and CLI.
1153905	FortiSwitch client page keeps loading.

System

Bug ID	Description
912383	FGR-70F and FGR-70F-3G4G failed to perform regular reboot process (using `execute reboot` command) with an SD card inserted.
945871	D-NAT functionality fails when using a Software Switch in explicit mode due to incorrect session matching during packet forwarding.
1021903	The le-switch member list does not update when the role of an interface is changed in a lan-extension environment.
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.
1085407	FortiGate unresponsive when `default-qos-type` is set to `shaping`.
1105321	FG-4201F with NP7 network processors shows EIF0_IGR and EIF1_IGR usage stuck at 100% and host softirq stuck at 99% after running the iptunnel traffic.
1113436	Packets are dropped when using auto-asic-offload with 802.1AD over LACP on FortiGate due to missing MAC address assignment on QinQ lag interfaces.
1114298	FortiGate Cloud remote login triggers two admin login events (1 successful and 1 unsuccessful for PKI admin).
1140755	When attempting to delete a software switch interface, it becomes permanently hidden due to an unreverted temporary flag.

Bug ID	Description
1146354	The network interface settings page fails to load on certain FortiGate models when the admin profile does not have the System > Configuration > Read/Write permission.
1164174	Configuration loss occurs when FortiGate enters conserve mode.
1164174	Configuration loss occurs when FortiGate enters conserve mode.
1170282	FortiGate HA becomes out of sync after provisioning a certificate by using ACME protocol.

Upgrade

Bug ID	Description
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
884462	NTLM authentication does not work with Chrome.
972391	RADIUS group usage not displayed correctly in GUI when used for firewall admin authentication.
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.
1148767	FSSO users are showing in small letters, filtering of users is not working, and PIE charts are also not visible.
1157003	Agentless FSSO connector issues occur when using Windows 2025 due to MS introduced additional restrictions to remote Event log reading.

VM

Bug ID	Description
978021	In FTP passive mode with GWLB setup, Geneve header VNI lengths are zero in syn-ack packets, leading to retransmission issues.

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.
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.
1080094	High memory usage may occur due to offline station entries not being automatically cleaned up over time.

ZTNA

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

Built-in AV Engine

AV Engine 7.00041 is released as the built-in AV Engine.

Built-in IPS Engine

IPS Engine 7.00570 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