FORTINET

Release Notes

FortiOS 8.0.2





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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

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

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com



October 22, 2026
FortiOS 8.0.2 Release Notes

TABLE OF CONTENTS

Change Log **5**
Introduction and supported models **6**
Supported models 6
FortiGate 6000 and 7000 support 7
Special notices **8**
FortiManager support for updated FortiOS private data encryption key 8
Hyperscale incompatibilities and limitations 9
FortiGate 6000 and 7000 incompatibilities and limitations 10
Agentless VPN (formerly SSL VPN web mode) not supported on some FortiGate series models 10
2 GB RAM FortiGate models no longer support most FortiOS proxy-related features 11
2 GB RAM FortiGate models no longer support Security Rating and Security Fabric topology 11
Policy check required for hairpin traffic 11
FortiGate WiFi controller support with FortiOS 8.0.0 12
FortiLink split interface with LLDP neighbor detection mode 12
Upgrade information **13**
Fortinet Security Fabric upgrade 13
Downgrading to previous firmware versions 15
Firmware image checksums 15
FortiGate 6000 and 7000 upgrade information 15
Password policy enforcement 17
FortiGate VM upgrade requirement 17
Traffic loss during graceful upgrade on SLBC HA with override enable due to premature failover 17
Product integration and support **18**
Virtualization environments 19
Language support 19
Agentless VPN support 20
Resolved issues **21**
Intrusion Prevention 21
Known issues **22**
New known issues 22
Existing known issues 22
AntiVirus 22
FortiGate 6000/7000 Platform 22
GUI 23
HA 24
HyperScale 24
IPsec VPN 24
REST API 24
Routing 24

Upgrade 25
User and Authentication 25
Built-in AV Engine **26**
Built-in IPS Engine **27**
Limitations **28**
Citrix XenServer limitations 28
Open source XenServer limitations 28

Change Log

Date	Change Description
2026-10-22	Initial release of 8.0.2.

Introduction and supported models

This guide provides release information for FortiOS 8.0.2 build 0251.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 8.0.2 supports the following models.

FortiGate	FG-30G, FG-31G, FG-40F, FG-40F-3G4G, FG-50G, FG-51G, FG-50G-5G, FG-51G-5G, FG-50G-SFP, FG-50G-DSL, FG-50G-SFP-POE, FG-51G-SFP-POE, FG-60F, FG-61F, FG-70F, FG-71F, FG-70G, FG-71G, FG-70G-POE, FG-71G-POE, FG-80F, FG-80F-BP, FG-80F-DSL, FG-80F-POE, FG-81F, FG-81F-POE, FG-90G, FG-91G, FG-100F, FG-101F, FG-120G, FG-121G, FG-200E, FG-200F, FG-200G, FG-201E, FG-201F, FG-201G, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-400F, FG-401F, FG-400G, FG-401G, FG-500E, FG-501E, FG-600E, FG-601E, FG-600F, FG-601F, FG-700G, FG-701G, FG-800D, FG-900D, FG-900G, FG-901G, FG-1000D, FG-1000F, FG-1001F, FG-1100E, FG-1101E, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000F, FG-3001F, FG-3000G, FG-3001G, FG-3200F, FG-3201F, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3500G, FG-3501G, FG-3600E, FG-3601E, FG-3700F, FG-3701F, FG-3800G, FG-3801G, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-4800F, FG-4801F, FG-6000F, FG-7000E, FG-7000F
FortiWiFi	FWF-30G, FWF-31G, FWF-40F, FWF-40F-3G4G, FWF-50G, FWF-50G-5G, FWF-50G-SFP, FWF-50G-DSL, FWF-51G, FWF-60F, FWF-61F, FWF-70G, FWF-71G, FWF-70G-POE, FWF-80F-2R, FWF-80F-2R-3G4G-DSL, FWF-81F-2R, FWF-81F-2R-3G4G-DSL, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-50G-5G, FGR-60F, FGR-60F-3G4G, FGR-60G, FGR-60G-M12, FGR-60G-5G, FGR-70F, FGR-70F-3G4G, FGR-70G, FGR-70G-5G, FGR-70G-5G-Dual
FortiFirewall	FFW-1801F, FFW-2600F, FFW-3001F, FFW-3501F, FFW-3980E, FFW-4200F, FFW-4400F, FFW-4401F, FFW-4801F, FFW-VM64, FFW-VM64-KVM
FortiGate VM	FG-ARM64-AWS, FG-ARM64-AZURE, FG-ARM64-GCP, FG-ARM64-KVM, FG-ARM64-OCI, FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-XEN

Starting with FortiOS 7.6.1, New deployments on Azure Marketplace use Generation 2 (Gen2) VM images and no longer support Azure F-series, Fs-series, Standard Dv2, and Standard Dsv2 instance types, or similar instance families, which require Gen1 images. Existing FortiGate VMs deployed on F-series or Fs-series instance types can continue to operate and be upgraded to FortiOS 7.6.1 or later. Upgrade to newer instance families for better and more stable performance. See Instance type support for details.

FortiGate 6000 and 7000 support

FortiOS 8.0.2 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

- FortiManager support for updated FortiOS private data encryption key on page 8
- Hyperscale incompatibilities and limitations on page 9
- FortiGate 6000 and 7000 incompatibilities and limitations on page 10
- Agentless VPN (formerly SSL VPN web mode) not supported on some FortiGate series models on page 10
- 2 GB RAM FortiGate models no longer support most FortiOS proxy-related features on page 11
- 2 GB RAM FortiGate models no longer support Security Rating and Security Fabric topology on page 11
- Policy check required for hairpin traffic on page 11
- FortiGate WiFi controller support with FortiOS 8.0.0 on page 12
- FortiLink split interface with LLDP neighbor detection mode on page 12

FortiManager support for updated FortiOS private data encryption key

With the introduction of FortiOS 7.6.1, Fortinet has updated the private-data-encryption key feature. Administrators are no longer required to manually input a 32-digit hexadecimal `private-data-encryption` key. Instead administrators simply enable the command, and a random `private-data-encryption` key is generated.

How FortiManager 8.0.0 works with FortiOS private data encryption keys has changed. This topic covers the changes. See FortiManager behavior on page 9.

Previous FortiOS CLI behavior

```
config system global
    set private-data-encryption enable
end
Please type your private data encryption key (32 hexadecimal numbers):
1234567890123456789012345678 9abc
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
1234567890123456789012345678 9abc
Your private data encryption key is accepted.
```

New FortiOS CLI behavior

```
config system global
    set private-data-encryption enable
end
This operation will generate a random private data encryption key!
Previous config files encrypted with the system default key cannot be restored after this
operation!
```

```
Do you want to continue? (y/n)y
Private data encryption key generation succeeded!
```

FortiManager behavior

FortiManager 8.0.0 can centrally manage FortiGates with the private-data-encryption setting enabled, with the following limitations:

- FortiManager can import objects that include the password type attribute.

  When FortiManager imports objects that include a password-type attribute, the administrator will be prompted to specify the password used by the object during the import process.
- FortiManager cannot be used to create NAT and transparent VDOMs.

This applies to FortiGates with private keys that are manually configured in FortiOS 7.6.0 and earlier and private keys that are randomly generated in FortiOS 7.6.1 and later.

FortiManager does not require you to verify the private key of the FortiGate when adding it to FortiManager.

FortiGates that require the protection of private data encryption and need to be managed by FortiManager should follow these procedures on a fresh install.

1. On the FortiGate, enable `private-data-encryption`.
2. On the FortiManager, add the FortiGate to the Device Manager. FortiManager will not be required to provide the key for PDE, as it will not be importing any password-related settings.
3. Make all configuration changes directly on the FortiManager.
4. Push and install the changes to the FortiGate.

If you require the use of NAT or Transparent VDOMs, you should perform this additional step before the steps above.

1. Enable `multi-vdom` mode on the FortiGate.
2. Add the VDOMs that you will use on the FortiGate.
3. Follow the above steps to enable `private-data-encryption` and manage the FortiGate from the FortiManager.

For more information, see the FortiManager Administration Guide.

Hyperscale incompatibilities and limitations

See Hyperscale firewall incompatibilities and limitations in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 8.0.2 features.

FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 8.0.2 features.

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

Agentless VPN (formerly SSL VPN web mode) not supported on some FortiGate series models

On the following FortiGate models, the Agentless VPN (formerly SSL VPN web mode) feature is no longer available from the GUI or CLI. Settings will not be upgraded from previous versions.

The affected models include:

- FGT-40F/FWF-40F and variants
- FGT-50G/FWF-50G and variants
- FGT-60F/FWF-60F
- FGT-61F/FWF-61F
- FGR-60F and variants (2GB versions only)
- FGT-70G/FWF-70G and variants
- FGT-90G and FGT-91G

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

On these FortiGate models, consider migrating to using IPsec Dialup VPN for remote access.

See SSL VPN to IPsec VPN Migration for more information.

FortiGate models not listed above will continue to support Agentless VPN (formerly SSL VPN web mode). However, SSL VPN tunnel mode is not longer supported on any models.

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

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

However FortiOS 7.6.5 brings back proxy-based inspection for email protocols on FortiGate models with 2 GB RAM. This covers the following services:

- SMTP(s)
- POP3(s)
- IMAP(s)
- NNTP

Firewall policies can once again support proxy-based inspection mode when users select one or more of the above services in the firewall policy.

This change impacts the FortiGate 40F, 60F, and 50G series devices, along with their variants.

See Proxy-related features no longer supported on FortiGate 2 GB RAM models for more information.

2 GB RAM FortiGate models no longer support Security Rating and Security Fabric topology

To enhance the stability of physical FortiGate devices devices with 2 GB RAM, the Security Rating feature and Security Fabric topology visibility have been removed. These changes prioritizes device stability and mitigate potential performance issues. For more information, see Optimizations for physical FortiGate devices with 2 GB RAM.

Policy check required for hairpin traffic

In FortiOS 7.6.5, the default setting for `allow-traffic-redirect` and `ipv6-allow-traffic-redirect` changed from `enable` to `disable`:

```
config system global
  set allow-traffic-redirect disable
  set ipv6-allow-traffic-redirect disable
end
```

Upon upgrade, both of these settings will be changed to `disable`, even if they were enabled before.

Disabling this setting ensures that hairpin traffic arriving at an interface and redirected out on the same interface requires a firewall policy to explicitly allow the traffic. If you want to redirect traffic without the need for a policy based only on routing decision, then manually enable these settings.

FortiGate WiFi controller support with FortiOS 8.0.0

FortiGate WiFi Controller running FortiOS 8.0.0 no longer supports FortiAP-C, FortiAP-U E-series, and FortiAP-W2 E-series models, except for FAP-221E, 223E, 421E and 423E.

FortiLink split interface with LLDP neighbor detection mode

When FortiLink neighbor detection mode is set to LLDP and the FortiLink split interface is enabled, one FortiLink member port remains in the up/active state, while the other remains in the down/standby state.

Upgrade information

Supported upgrade path information is available through the Upgrade Path Tool on the Fortinet Document Library.

FortiGate	Upgrade option	Details
Individual FortiGate devices	Manual update	Use the procedure in this topic. See also Upgrading individual devices in the FortiOS Administration Guide.
	Automatic update based on FortiGuard upgrade path	See Enabling automatic firmware updates in the FortiOS Administration Guide for details
Multiple FortiGate devices in a Fortinet Security Fabric	Manual, immediate or scheduled update based on FortiGuard upgrade path	See Fortinet Security Fabric upgrade on page 13 and Upgrading all devices in the FortiOS Administration Guide.

To view supported upgrade path information:

1. Go to the Fortinet Document Library at https://docs.fortinet.com/product/fortigate.
2. From the right side-bar, go to *Tools & Resources* and select *Upgrade Path Tool*.
3. Check that *Choose a product* is *FortiGate / FortiOS*.
4. In the *Product Model* list, select your model.
5. In the *Current Version* list, select the FortiOS version you are currently running.
6. In the *Target Upgrade Version* list, select the target FortiOS version for the upgrade.
7. Click *Go* to view the upgrade path.

Fortinet Security Fabric upgrade

FortiOS 8.0.2 is verified to work with these Fortinet products. This includes:

FortiAnalyzer	• 8.0.2
FortiManager	• 8.0.2
FortiExtender	• 7.4.0 and later
FortiSwitch OS (FortiLink support)	• 6.4.6 build 0470 and later
FortiAP	• 7.2.2 and later

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

* If you are using FortiClient only for IPsec VPN, 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 8.0.0, use FortiClient 8.0.0.

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 8.0.2. When Security Fabric is enabled in FortiOS 8.0.2, all FortiGate devices must be running FortiOS 8.0.2.

Downgrading to previous firmware versions

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

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

Firmware image checksums

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

FortiGate 6000 and 7000 upgrade information

To make sure a FortiGate 6000 or 7000 firmware upgrade is successful, before starting the upgrade, Fortinet recommends you use health checking to make sure the FIMs and FPMs are all synchronized and operating as expected.

If you are following a multi-step upgrade path, you should re-do health checking after each upgrade step to make sure all components are synchronized before the next step.

You should also perform a final round of health checking after the firmware upgrade process is complete.

For recommended health checking commands, see the Fortinet community article: Technical Tip: FortiGate-6000/7000 Chassis health check commands.

Both management boards and all of the FPCs in a FortiGate 6000 FGCP HA cluster run the same firmware image. You upgrade the firmware from the primary FortiGate 6000 management board. The firmware image is copied to the FPCs and all components upgrade at the same time.

All of the FIMs and FPMs in a FortiGate 7000 FGCP HA cluster also run the same firmware image. You upgrade the firmware from the primary FIM in the primary FortiGate 7000. The firmware image is copied to the secondary FIM and the FPMs and all components upgrade at the same time.

A graceful firmware upgrade of a FortiGate 6000 or 7000 FGCP cluster only causes minimal traffic interruption. Use the following command to enable graceful upgrade.

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

The `uninterruptible` option is enabled by default. To improve session synchronization during a graceful upgrade, you can also enable `session-pickup`:

```
config system ha
   set session-pickup enable
end
```



For the FortiGate 7000F platform, enabling session pickup requires using the `session-sync-dev` option to select one or more interfaces to use for session synchronization. The recommended session synchronization configuration is to add two 100Gbps FIM management interfaces to a LAG and configure the HA `session-sync-dev` option to use this LAG for session synchronization. The recommended interfaces to use for this LAG are the M1 interface of the FIM in slot 1 and the M1 interface of the FIM in slot 2. You should use a switch to connect the LAGs in the two chassis. To support graceful upgrade with session synchronization:

```
config system ha
   set upgrade-mode uninterruptible
   set session-syn-dev <lag>
   set session-pickup enable
end
```

During a graceful firmware upgrade the secondary FortiGate 6000 or 7000 upgrades its firmware first, traffic then fails over to the secondary FortiGate 6000 or 7000 and then the primary FortiGate 6000 or 7000 firmware is upgraded. A FortiGate 6000 or 7000 firmware upgrade can take a few minutes, the amount of time depending on the hardware and software configuration and whether DP or NP7 processor software is also upgraded.

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

Normally, you would want to set `upgrade-mode` to `uninterruptible` to minimize traffic interruptions. If a traffic interruption is not going to cause any problems, you can set `upgrade-mode` to `simultaneous` so that the firmware upgrade process takes less time.

As well, some firmware upgrades may not support setting `upgrade-mode` to `uninterruptible`. Make sure to review the release notes before running a firmware upgrade to verify whether or not setting `upgrade-mode` to `uninterruptible` is supported to upgrade to that version.

Password policy enforcement

After upgrade to FortiOS 7.6.5 or later, the password policy is enforced, and your password must meet the requirements before you can log in to FortiOS. Passwords must contain:

- 1 uppercase letter
- 1 lowercase letter
- 1 special character
- 1 number (0-9)
- A minimum length of 12 characters

If your password meets the requirements, you can log in to FortiOS after upgrade.

If your password does not meet the requirements, you must change your password before you can log in to the GUI or CLI.

FortiGate VM upgrade requirement

Starting in FortiOS 8.0.1, FortiGate VM models support signatures in CMS (Cryptographic Message Syntax) format, and the support introduces a required intermediate upgrade step.

For FortiOS 8.0, you must upgrade the FortiGate VM to 8.0.1 before you can upgrade to 8.0.2 or later.

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

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

Product integration and support

The following table lists FortiOS 8.0.2 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 0337 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	• 8.0018
IPS Engine	• 8.0050

See also:

- Virtualization environments on page 19
- Language support on page 19
- Agentless VPN support on page 20

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 2022
Windows Hyper-V Server	• Microsoft Hyper-V Server 2022
Open source XenServer	• Version 3.4.3 • Version 4.1 and later
VMware ESXi	• Versions 6.5, 6.7, 7.0, 8.0, and 9.0.

Language support

The following table lists language support information.

Language support

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

Agentless VPN support

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

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.

Resolved issues

The following issues have been fixed in version 8.0.2. To inquire about a particular bug, please contact Customer Service & Support.

Intrusion Prevention

Bug ID	Description
1328306	Local-in Virtual Patch fails to inspect traffic when using the HA-MGMT interface.

Known issues

Known issues are organized into the following categories:

- New known issues on page 22
- Existing known issues on page 22

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

New known issues

Currently no new issues have been reported in 8.0.2.

Existing known issues

The following issues have been identified in a previous version of FortiOS and remain in FortiOS 8.0.2.

AntiVirus

Bug ID	Description
1307848	Eicar passes when two security policies are configured, first one denies application and second one enables AV scan. **Workaround**: Use wildcard policies to block AV reliably

FortiGate 6000/7000 Platform

Bug ID	Description
1130491	Traffic disruption occurs when WCCP is enabled on FortiGate **Workaround**: Direct all related traffic to master FPC
1131269	UESP packet drop occurs when VPN peer uses different source ports for IKE-NATT and UESP **Workaround**: Add a flow rule to work around the issue
1250240	Traffic disruption occurs when kernel routes are not synchronized across the FPM.

Bug ID	Description
	Workaround: Run diag test application chlbd 3 on the slot that's missing routes to trigger a manual routes redownload.
1292637	6000F / 7000F support Multipath IPsec feature #1235059
1336373	7121F-2 (FIM-7941)/b0245: 100G FR transceiver link fails when RS-FEC is enabled on 1-P4, but works with FEC disabled

GUI

Bug ID	Description
1102594	HA status on the Global Dashboard changes unexpectedly during hard refresh
1190683	Fabric Connector status shows as DOWN in GUI after failover on Azure SDN Connector cluster **Workaround**: Logout and login again to the GUI
1205102	Traffic logs cannot be viewed when Resolve unknown applications is enabled **Workaround**: Disable Resolve unknown applications under the global settings of log settings
1232828	Unresponsive GUI occurs when httpd is fully loaded on the forward traffic page **Workaround**: Disable Resolve unknown applications in the log settings
1237136	Dynamic VLANs are not visible on the GUI when a port-security-policy is applied
1249752	Incorrect HA status occurs when switching to mgmt-vdom vdom on FortiGate-6001F
1262047	Connection loss occurs when web-svc-perf is enabled under log settings **Workaround**: Disable web-svc-perf under log setting
1265107	Blank page displays in GUI when vdom_admin logs in but lacks root access
1265177	Display issues occur in FortiView widgets when FIPS-CC mode is enabled **Workaround**: Create another super-admin profile to assign to the new admin.
1265862	On FortiFirewall, GUI displays incorrect log traffic status when firewall policy is configured via CLI **Workaround**: Use set logtraffic all/disable instead of unset logtraffic
1274560	Non-resolvable FQDN objects intermittently show a red box around the object name when filtered by FQDN type in the Policy & Objects section on FortiGate.

HA

Bug ID	Description
1246177	Warning pop-up is not displayed on FGCP cluster members in clusters with more than 2 members
1249251	TCP session failover fails when using NGFW policy-based mode after HA failover.
1273324	SNAT uses incorrect IP address after HA failover **Workaround**: Delete and re-add the secondary IP configuration manually
1285091	Config sync failure occurs when standalone-config-sync is enabled

HyperScale

Bug ID	Description
1200885	Renaming an ippool in a FortiGate setup with VDOMs results in unintended behavior affecting network traffic.
1262881	Hw session sync dev goes out of sync due to the discrepancy in lag driver between primary and secondary

IPsec VPN

Bug ID	Description
1238675	Connection fails to establish when FortiClient VPN Android connects to FortiGate IPsec IKEv1

REST API

Bug ID	Description
1267118	Filters are ignored when using the /firewall/sessions API call

Routing

Bug ID	Description
1260891	BFD packet transmission issues occur when a port member of the aggregate interface is shut down and then brought back up on the switch side. **Workaround**: Change bfd-detect-mult to 7 on both sides.

Upgrade

Bug ID	Description
1343135	Upgrading to 8.0.1 GA.F configuration with names beginning with a period "." will be lost **Workaround**: Before upgrading, rename any configurations whose names begin with a period (.).

User and Authentication

Bug ID	Description
1241530	LDAP authentication fails when password is not sent in bind request

Built-in AV Engine

AV Engine 8.0018 is released as the built-in AV Engine.

Built-in IPS Engine

IPS Engine 8.0050 is released as the built-in IPS Engine.

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.



www.fortinet.com

Copyright© 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.