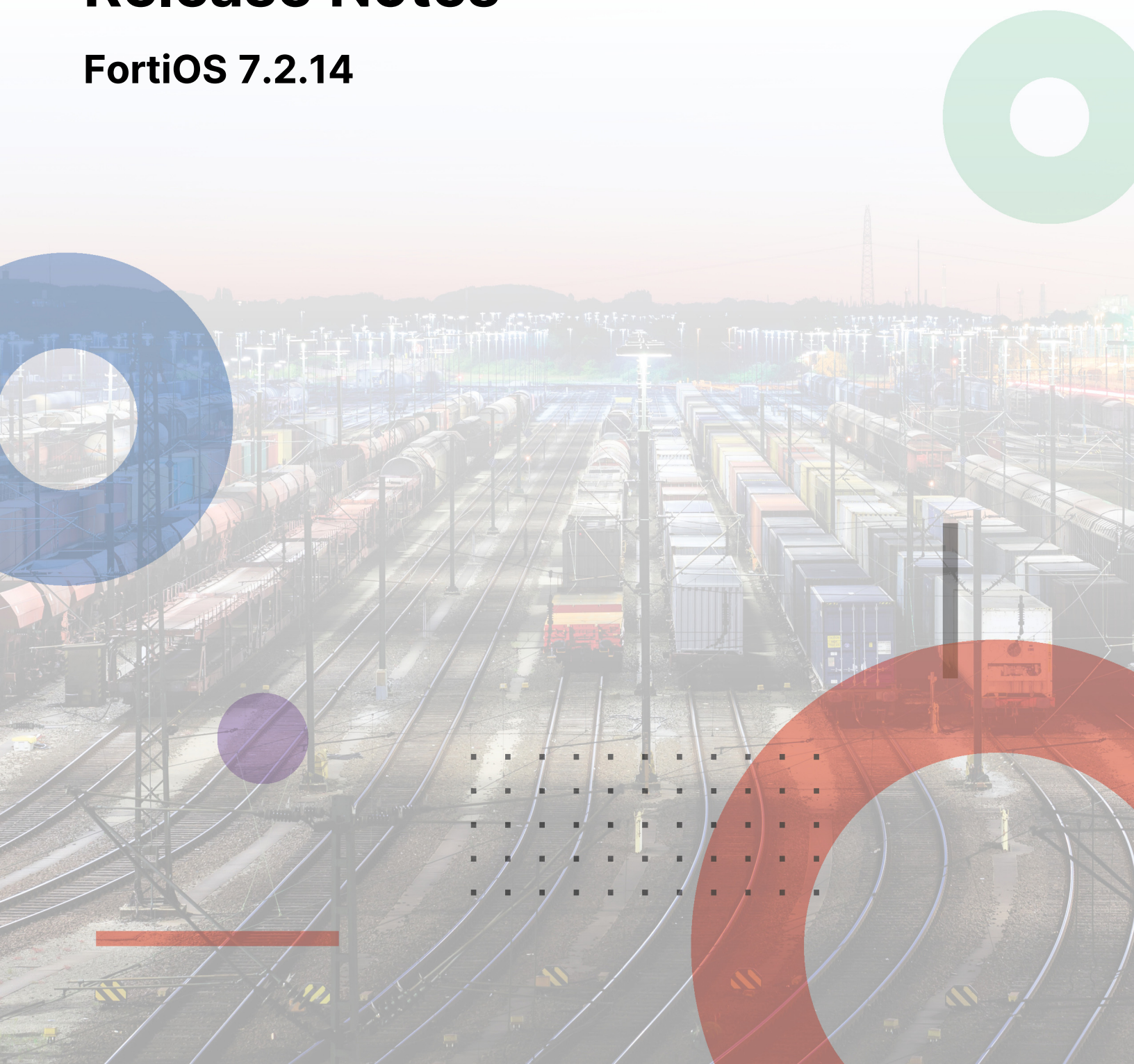
FORTINET

Release Notes

FortiOS 7.2.14



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 7.2.14 Release Notes

TABLE OF CONTENTS

Change Log **5**
Introduction and supported models **6**
Supported models 6
Special branch supported models 7
FortiGate 6000 and 7000 support 7
Special notices **8**
IPsec phase 1 interface type cannot be changed after it is configured 8
FortiGate 6000 and 7000 incompatibilities and limitations 8
Hyperscale incompatibilities and limitations 9
SMB drive mapping with ZTNA access proxy 9
Console error message when FortiGate 40xF boots 9
Hyperscale NP7 hardware limitation 9
Changes to NP7 traffic shaping 10
GUI cannot be accessed when using a server certificate with an RSA 1024 bit key 10
SSL VPN not supported on FortiGate G-series Entry-Level models 11
SAML certificate verification 11
Upgrade information **12**
Fortinet Security Fabric upgrade 12
Downgrading to previous firmware versions 14
Firmware image checksums 14
Strong cryptographic cipher requirements for FortiAP 14
FortiGate VM VDOM licenses 15
VDOM link and policy configuration is lost after upgrading if VDOM and VDOM link have the same name 15
FortiGate 6000 and 7000 upgrade information 15
Upgrade error message 16
FortiGates with ULL ports may expereince status down on active ports 17
SLBC FG-5001E primary blade fails to install image 17
Admin Access Lockout Risk when upgrading or downgrading from versions with PBKDF2 support 17
Traffic loss during graceful upgrade on SLBC HA with override enable due to premature failover 18
30G series upgrade from 7.2.11 to 7.2.12 18
Product integration and support **19**
Virtualization environments 20
Language support 20
SSL VPN support 21
SSL VPN web mode 21
Resolved issues **22**
Firewall 22
FortiGate 6000/7000 Platform 22

HA 22
Switch Controller 23
System 23
User and Authentication 23
VM 23
Known issues 24
New known issues 24
Existing known issues 24
Explicit Proxy 24
Anti Virus 25
Explicit Proxy 25
FortiGate 6000 and 7000 platforms 25
FortiView 27
GUI 27
HA 28
Hyperscale 29
IPsec VPN 29
REST API 29
Routing 30
Security Fabric 30
SSL VPN 30
Switch Controller 31
System 31
Upgrade 32
User & Authentication 32
VM 32
Web Filter 32
WiFi Controller 33
ZTNA 33
Built-in AV Engine 34
Built-in IPS Engine 35
Limitations 36
Citrix XenServer limitations 36
Open source XenServer limitations 36
Limitations on HA cluster formation between different FortiGate Rugged 60F and 60F 3G4G models 36

Change Log

Date	Change Description
2026-10-22	Initial release.

Introduction and supported models

This guide provides release information for FortiOS 7.2.14 build 1778.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.2.14 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-70F, FG-71F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-DSL, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-90G, FG-91E, FG-91G, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-120G, FG-121G, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-400F, FG-401F, FG-500E, FG-501E, FG-600E, FG-601E, FG-600F, FG-601F, FG-800D, FG-900D, FG-900G, FG-901G, FG-1000D, FG-1000F, FG-1001F, FG-1100E, FG-1101E, FG-1500D, FG-1500DT, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3000F, FG-3001F, FG-3100D, FG-3200D, FG-3200F, FG-3201F, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3700F, FG-3701F, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-4800F, FG-4801F, FG-5001E, FG-5001E1, FG-6000F, FG-7000E, FG-7000F
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-80F-2R-3G4G-DSL, FWF-81F-2R, FWF-81F-2R-3G4G-DSL, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-60F, FGR-60F-3G4G, FGR-70F, FGR-70F-3G4G
FortiFirewall	FFW-1801F, FFW-2600F, FFW-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-SVM, FG-VM64-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-XEN

Special branch supported models

The following models are released on a special branch of FortiOS 7.2.14. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1778.

FG-30G	is released on build 6695
FG-31G	is released on build 6695
FG-70G	is released on build 6694
FG-70G-POE	is released on build 6694
FG-71G	is released on build 6694
FG-71G-POE	is released on build 6694
FG-200G	is released on build 6692
FG-201G	is released on build 6692
FWF-30G	is released on build 6695
FWF-31G	is released on build 6695
FWF-70G	is released on build 6694
FWF-70G-POE	is released on build 6694
FWF-71G	is released on build 6694

FortiGate 6000 and 7000 support

FortiOS 7.2.14 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

- IPsec phase 1 interface type cannot be changed after it is configured on page 8
- FortiGate 6000 and 7000 incompatibilities and limitations on page 8
- Hyperscale incompatibilities and limitations on page 9
- SMB drive mapping with ZTNA access proxy on page 9
- Console error message when FortiGate 40xF boots on page 9
- Hyperscale NP7 hardware limitation on page 9
- Changes to NP7 traffic shaping on page 10
- GUI cannot be accessed when using a server certificate with an RSA 1024 bit key on page 10
- SSL VPN not supported on FortiGate G-series Entry-Level models on page 11
- SAML certificate verification on page 11

IPsec phase 1 interface type cannot be changed after it is configured

In FortiOS 7.2.0 and later, the IPsec phase 1 interface type cannot be changed after it is configured. This is due to the tunnel ID parameter (`tun_id`), which is used to match routes to IPsec tunnels to forward traffic. If the IPsec phase 1 interface type needs to be changed, a new interface must be configured.

FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 7.2.14 features.

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

Hyperscale incompatibilities and limitations

See Hyperscale firewall incompatibilities and limitations in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 7.2.14 features.

SMB drive mapping with ZTNA access proxy

In FortiOS 7.2.5 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.

Console error message when FortiGate 40xF boots

In FortiOS 7.2.5 and later, FortiGate 400F and 401F units with BIOS version 06000100 show an error message in the console when booting up.

The message, `Write I2C bus:3 addr:0xe2 reg:0x00 data:0x00 ret:-121.`, is shown in the console, and the FortiGate is unable to get transceiver information.

The issue is fixed in BIOS version 06000101.

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 90G and variants. Settings will not be upgraded from previous versions.

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

SAML certificate verification

For security purposes, in previous versions, FortiGate required a signature verification for both the SAML response message and the SAML assertion carried inside the SAML response. This means that the SAML response must have a valid signature, and the SAML assertion must also have a valid signature. If the Identity Provider (IdP) provides an invalid signature, or fails to sign one of these, the FortiGate will reject the SAML response.

This has now been loosened with the following configuration:

```
config user saml
    edit <name>
        set require-signed-resp-and-asrt <enable | disable>
    next
end
```

Option	Description
`enable`	Both response and assertion must be signed and valid.
`disable`	At least one of response or assertion must be signed and valid (default).

By default, the setting is disabled, which only requires one of the response or assertion to be signed and valid.

For more information, see Identify Providers.

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 12 and Upgrading Fabric or managed 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 7.2.14 greatly increases the interoperability between other Fortinet products. This includes:

FortiAnalyzer	• 7.2.12
FortiManager	• 7.2.12
FortiExtender	• 7.4.0 and later

FortiSwitch OS (FortiLink support)	• 6.4.6 build 0470 or later
FortiAP **FortiAP-S** **FortiAP-U** **FortiAP-W2**	• See Strong cryptographic cipher requirements for FortiAP on page 14
FortiClient* EMS	• 7.0.3 build 0229 or later
FortiClient* Microsoft Windows	• 7.0.3 build 0193 or later
FortiClient* Mac OS X	• 7.0.3 build 0131 or later
FortiClient* Linux	• 7.0.3 build 0137 or later
FortiClient* iOS	• 7.0.2 build 0036 or later
FortiClient* Android	• 7.0.2 build 0031 or 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 7.2.0, use FortiClient 7.2.0.

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. FortiAI

16. FortiTester
17. FortiMonitor
18. FortiPolicy



If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.2.14. When Security Fabric is enabled in FortiOS 7.2.14, all FortiGate devices must be running FortiOS 7.2.14.

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*.

Strong cryptographic cipher requirements for FortiAP

FortiOS 7.0.0 has removed 3DES and SHA1 from the list of strong cryptographic ciphers. To satisfy the cipher requirement, current FortiAP models whose names end with letter E or F should be upgraded to the following firmware versions:

- FortiAP (F models): version 6.4.3 and later
- FortiAP-S and FortiAP-W2 (E models): version 6.2.4, 6.4.1, and later
- FortiAP-U (EV and F models): version 6.0.3 and later

- FortiAP-C (FAP-C24JE): version 5.4.3 and later

If FortiGates running FortiOS 7.0.1 and later need to manage FortiAP models that cannot be upgraded or legacy FortiAP models whose names end with the letters B, C, CR, or D, administrators can allow those FortiAPs' connections with weak cipher encryption by using compatibility mode:

```
config wireless-controller global
    set tunnel-mode compatible
end
```

FortiGate VM VDOM licenses

FortiGate VMs with one VDOM license (S-series, V-series, FortiFlex) have a maximum number or two VDOMs. An administrative type root VDOM and another traffic type VDOM are allowed in 7.2.0 and later. After upgrading to 7.2.0 and later, if the VM previously had split-task VDOMs enabled, two VDOMs are kept (the root VDOM is an administrative type).

VDOM link and policy configuration is lost after upgrading if VDOM and VDOM link have the same name

Affected versions:

- FortiOS 6.4.9 and later
- FortiOS 7.0.6 and later
- FortiOS 7.2.0 and later

When upgrading to one of the affected versions, there is a check within the set `vdom-links` function that rejects `vdom-links` that have the same name as a VDOM. Without the check, the FortiGate will have a kernel panic upon bootup during the upgrade step.

A workaround is to rename the `vdom-links` prior to upgrading, so that they are different from the VDOMs.

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 7.2.14:

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

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

2. Download the FortiOS 7.2.14 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. Check the *Cluster Status* dashboard widget or use the `diagnose sys confsync status` command to confirm that all components are synchronized and operating normally.

Upgrade error message

The FortiGate console will print a `Fail to append CC_trailer.ncfg_remove_signature:error in stat` error message after upgrading from 7.2.4 to 7.2.5 or later. Affected platforms include: FFW-3980E, FFW-VM64, and FFW-VM64-KVM. A workaround is to run another upgrade to 7.2.5 or later.

FortiGates with ULL ports may expereince status down on active ports

After upgrading to FortiOS version 7.2.9, FortiGate platforms with ultra-low-latency (ULL) ports like 600F and 901G models may experience link status down on active ULL ports if the following conditions are met:

- The ULL port is set to 25G mode
- Forward error correcting (FEC) is enabled on the port
- Forward error correcting (FEC) is disabled on the connecting switch

This behaviour change is due to a fix in FortiOS 7.2.9 version for an issue where FEC feature was disabled even though it was enabled in the CLI. This allowed the FortiGate ULL port to still connect to the switch with FEC disabled. After the fix, FEC is activated on the ForitGate and caused a mismatch with the switch.

Workaround: User can disable FEC feature on the FortiGate ULL port to match with the connecting switch, or they can enable FEC feature on the switch to match with the FortiGate side.

```
config system interface
    edit <ULL port>
        set forward-error-correction disable
    next
end
```

SLBC FG-5001E primary blade fails to install image

For FG-5001E in a session-aware load balanced cluster (SLBC), all secondary blades install the image successfully. However, the primary blade fails, showing a `sync timeout` error, even with `graceful-upgrade` disabled.

Admin Access Lockout Risk when upgrading or downgrading from versions with PBKDF2 support

PBKDF2-based password hashing is supported starting in versions 7.2.11, 7.4.8, and 7.6.1. If a device is upgraded to one of these versions and administrator credentials are saved, then later upgraded or downgraded to a release prior to PBKDF2 support (for example, upgrading from 7.2.11 to 7.4.7), the admin login will fail, resulting in administrator access lockout.

Before upgrading or downgrading, make sure that the `login-lockout-upon-downgrade` command is disabled:

```
config system password-policy
    set login-lockout-upon-downgrade disable
end
```

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.

Workaround:

```
config system ha
    set override-wait-time 300
end
```

30G series upgrade from 7.2.11 to 7.2.12

For the FortiGate and FortiWiFi 30G and 31G devices:

- If trying to upgrade from 7.2.11 GA to 7.2.12 GA directly with BIOS security level High, the upgrade will fail.
- If trying to upgrade from 7.2.11 GA to 7.2.12 GA directly with BIOS security level Low, the upgrade works, but with the following error in the console:

```
****
Fail to append CC_trailer.ncfg_remove_signature:error in stat.
Fail to ncfg_remove_CC_trailer.
****
```

Product integration and support

The following table lists FortiOS 7.2.14 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 114 • Mozilla Firefox version 113 • Google Chrome version 114 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 114 • Mozilla Firefox version 113 • Google Chrome version 114 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 0335 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
	  • Windows Server 2008 64-bit (requires Microsoft SHA2 support package)
	  • Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package)
	  • Windows Server 2008 Core (requires Microsoft SHA2 support package)
	  • Novell eDirectory 8.8

AV Engine	• 6.00303
IPS Engine	• 7.00367

Virtualization environments

The following table lists hypervisors and recommended versions.

Hypervisor	Recommended versions
Citrix Hypervisor	• 8.1 Express Edition, Dec 17, 2019
Linux KVM	• Ubuntu 18.0.4 LTS • Red Hat Enterprise Linux release 8.4 • SUSE Linux Enterprise Server 12 SP3 release 12.3
Microsoft Windows Server	• 2012R2 with Hyper-V role
Windows Hyper-V Server	• 2019
Open source XenServer	• Version 3.4.3 • Version 4.1 and later
VMware ESXi	• Versions 6.5, 6.7, 7.0, and 8.0.

Language support

The following table lists language support information.

Language support

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

SSL VPN support

SSL VPN web mode

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

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 113 Google Chrome version 113
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 113 Google Chrome version 113
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 113 Google Chrome version 113
macOS Ventura 13	Apple Safari version 15 Mozilla Firefox version 113 Google Chrome version 113
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 7.2.14. To inquire about a particular bug, please contact Customer Service & Support.

Firewall

Bug ID	Description
1212608	FTP does not work in passive mode via the helper session.

FortiGate 6000/7000 Platform

Bug ID	Description
1202263	FQDN broadcast packets leave stale FQDN address entries in the firewall.
1211372	An error condition in confsyncd occurs when file sizes change between scans
1229458	A second file scan with a file size larger than the initial scan causes confsyncd to restart unexpectedly.

HA

Bug ID	Description
1032415	On the System > HA page, all HA vcluster device roles display as Primary in the Role column.
1225710	Mobile Token assignment fails on old models that don't support vSN when HA fail-over occurs

Switch Controller

Bug ID	Description
1170323	Interfaces cannot be enabled as FortiLink interfaces on FortiGate with hardware revision 2.

System

Bug ID	Description
1164174	Configuration loss on FGT-60F when FortiGate enters extreme conserve mode
1170282	FortiGate HA becomes out of sync after provisioning a certificate by using ACME protocol
1200604	Config backup to FGT Cloud fails when retrieving full config.

User and Authentication

Bug ID	Description
1196434	SAML authentication issues occur when LASSO_PROFILE_SIGNATURE_VERIFY_HINT_FORCE is set and the SAML response is not signed.

VM

Bug ID	Description
1224484	An error condition occurs in the diag daemon during image upgrade matrix operations

Known issues

Known issues are organized into the following categories:

- New known issues on page 24
- Existing known issues on page 24

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

New known issues

There are currently no new issues that have been identified in version 7.2.14.

Existing known issues

The following issues have been identified in a previous version of FortiOS and remain in FortiOS 7.2.14.

Explicit Proxy

Bug ID	Description
865828	Unexpected behavior occurs when configuring internet services with custom or ISDB entries, leading to failed negate options and issues with internet-service6 functionality.
890776	The GUI-explicit-proxy setting on the System > Feature Visibility page is not retained after a FortiGate reboot or upgrade.
894557	In some cases, the explicit proxy policy list can take a long time to load due to a delay in retrieving proxy stats. **Workaround**: User can restart WAD process, or temporarily disable the WAD debug process (need to disable again if the FortiGate reboots) dia wad toggle (using direct connect diagnose) This issue does not impact explicit-proxy functionality.
1059899	When setting sec-default-action to accept on an initial explicit web proxy configuration after a factory reset, incoming traffic does not match the proxy policy and allows all traffic to pass. **Workaround**: set sec-default-action to deny first in the CLI and then change the setting to accept.

Bug ID	Description
865828	Unexpected behavior occurs when configuring internet services with custom or ISDB entries, leading to failed negate options and issues with internet-service6 functionality.
890776	The GUI-explicit-proxy setting on the System > Feature Visibility page is not retained after a FortiGate reboot or upgrade.
894557	In some cases, the explicit proxy policy list can take a long time to load due to a delay in retrieving proxy stats. **Workaround**: User can restart WAD process, or temporarily disable the WAD debug process (need to disable again if the FortiGate reboots) dia wad toggle (using direct connect diagnose) This issue does not impact explicit-proxy functionality.
1059899	When setting sec-default-action to accept on an initial explicit web proxy configuration after a factory reset, incoming traffic does not match the proxy policy and allows all traffic to pass. **Workaround**: set sec-default-action to deny first in the CLI and then change the setting to accept.

Anti Virus

Bug ID	Description
937375	Malware thread feeds can't be deleted from cli

Explicit Proxy

FortiGate 6000 and 7000 platforms

Bug ID	Description
790464	After a failover, ARP entries are removed from all slots when an ARP query of single slot does not respond.
951135	Graceful upgrade of a FortiGate 6000 or 7000 FGCP HA cluster is not supported when upgrading from FortiOS 7.0.12 to 7.2.5/7.2.6. Upgrading the firmware of a FortiGate-6000 or 7000 FGCP HA cluster from 7.0.12 to 7.2.5/7.2.6 should be done during a maintenance window, since the firmware upgrade process will disrupt traffic for up to 30 minutes. Before upgrading the firmware, disable uninterruptible-upgrade. Then perform a normal firmware upgrade. During the upgrade process the FortiGates in the cluster will not allow traffic until all components (management board and FPCs or FIMs and FPMs) are upgraded and both FortiGates have restarted. This process can take up to 30 minutes.

Bug ID	Description
951193	SLBC for FortiOS 7.0 and 7.2 uses different FGCP HA heartbeat formats. Because of the different heartbeat formats, you can't create an FGCP HA cluster of two FortiGate 6000s or 7000s when one chassis is running FortiOS 7.0.x and the other is running FortiOS 7.2.x. Instead, to form an FGCP HA cluster, both chassis must be running FortiOS 7.0.x or 7.2.x. If two chassis are running different patch releases of FortiOS 7.0 or 7.2 (for example, one chassis is running 7.2.5 and the other 7.2.6), they can form a cluster. When the cluster is formed, FGCP elects one chassis to be the primary chassis. The primary chassis syncs its firmware to the secondary chassis. As a result, both chassis will be running the same firmware version. You could also form a cluster if one chassis is running FortiOS 7.2.x and the other is running 7.4.x. For best results, both chassis should be running the same firmware version, although as described above, this is not a requirement.
954881	Unintended behavior occurs when FortiGate models perform a warm reboot without properly applying virtual domain configurations.
994241	On FortiGate 7000F using FGSP and FGCP, when TCP traffic takes an asymmetric path, the TCP ACK and data packets might be dropped in NP7.
1006759	After an HA failover, there is no IPsec route in the kernel. **Workaround**: Bring down and bring up the tunnel
1056894	On the FortiGate 6000 platform, IPv6 VRF routing tables appear under the new and old FPC primary units when the primary FPC slot is changed.
1062080	snmp query returns error when there are large no. of bgp routes

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 7000Fs in the cluster. When this happens, FortiManager may incorrectly change the VDOM of the management interfaces added to the `session-sync-dev` command from vsys_ha to mgmt-vdom 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.

1093412	For an FGSP configuration on the FortiGate 6000 and 7000 platforms, the `encryption` option of the `config system standalone-cluster` command does not encrypt session synchronization traffic. Enabling this option has no effect.

Bug ID	Description
1096156	GUI unreachable due to certificates and private keys mismatch in a HA setup.
1149342	BGP flapping occurs when concurrent IP address management causes unexpected source IP usage on outbound connections during FortiGate VDOM migrations.
1183735	Graceful upgrades lead to unintended primary claiming by FortiGate units during HA resynchronization.
1185528	Issue description: subscription license on the secondary chassis is missing after the graceful upgrade from 7.2.10 to 7.2.12 **Workaround**: run "execute update-now" again
1225359	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.
1349258	7KF/B2933: Uninterruptible-upgrade upgrade fails from 7.2.13 to 7.4.13

FortiView

Bug ID	Description
1123502	FortiView Threats: drill down to malicious website entry return Failed to retrieve FortiView data from disk

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 100K entries.
974988	FortiGate GUI should not show a license expired notification due to an expired device-level FortiManager Cloud license if it still has a valid account-level FortiManager Cloud license (function is not affected).
989512	Dashboard > Firewall User monitor widget: When the number of users exceed 2000, the page will no longer display the search bar, filter columns or graphs. This is due to results being lazily loaded, which do not support these GUI features.
993890	The Node.JS restarts and causes a kill ESRCH error on FortiGate after an upgrade.
999972	Security Profiles > Intrusion Prevention > IPS Signatures and filters: IP Exemption edits made more than once via the GUI are not saved

Bug ID	Description
1055197	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.
1143734	Network > SD-WAN > SD-WAN Rules: When editing a rule, inline edit from the omniselect is not available for Application Group entries. **Workaround**: is to edit the application from Security Profiles > Application Signatures > Group or via the command line.

HA

Bug ID	Description
781171	When performing HA upgrade via the GUI, if the secondary unit takes several minutes to bootup, 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.
970316	When adding new vcluster, link-failure value of the newly added vcluster is not updated, causing wrong master selection.
988944	The Fabric Management page displays inconsistent information when accessed through secondary HA units on some FortiGate models.

1072440	Special branch supported models FortiGate HA cluster with empty HA password - Upgrade from special build GA version (v7.0.x) to official GA version (i.e v7.2.9/v7.2.10) can cause the primary member fail to upgrade.
	Impacted models: Please see a full list of "Special branch supported models" for FortiOS v7.0.15 here https://docs.fortinet.com/document/fortigate/7.0.15/fortios-release-notes/760203/introduction-and-supported-models
	Workaround: User can configure valid HA password for the cluster before the upgrade, or manually upgrade the member that was impacted.
	`config system ha`
	`  set password <new-password>`
	`end`
	Note that setting the password will cause a HA cluster re-election to occur.

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.
1231480	LACPDU transmission issues occur when HA failover is triggered by a monitoring port disconnect

Hyperscale

Bug ID	Description
802182	After successfully changing the VLAN ID of an interface from the CLI, an error message similar to "cmdb_txn_cache_data(query=log.npu-server,leve=1) failed" may appear.
824071	IPv6 traffic fails to load balance across multiple virtual domains when using Equal-cost Multipath (ECMP) in NAT mode on FortiGate devices.
843197	The npu-session list fails to display policy-route information when traffic is routed through a policy route on FortiGate models using NPU acceleration.
853258	Traffic drops occur after Failover in HA A-P setups using hardware-only sessions.
872146	The "diagnose sys npu-session list" command displays incorrect policy IDs when traffic uses intra-zone policies.
920228	nat46 npu session lost and traffic dropped when ha failover
1170648	"diag firewall ippool list pba" command is executed in a hyperscale device may result in high cpu no workaround available
1178585	Traffic outage occurs when making ip-pool group changes on hyperscale vdoms.
1223321	IP pools got stuck when session-ttl changes are made

IPsec VPN

Bug ID	Description
944600	CPU usage issues occurred when IPSec VPN traffic was received on the VLAN Interface of NP7 vlink
1128662	BGP peering fails to establish when a race condition occurs between FortiGate OS and NPU driver during IPsec SA updates for dynamic hub-to-static spoke VPNs.

REST API

Bug ID	Description
1004136	Fetching logs via a REST API GET request returns a maximum of 1000 logs.

Routing

Bug ID	Description
896090	SD-WAN Performance SLA health checks fail when FortiGuard is configured as the server due to lack of HTTP support on FortiGuard servers
903444	Command 'diagnose ip rtcache list' is no longer supported in FortiOS 4.19 kernel
924693	On the Network > SD-WAN > SD-WAN Rules page, member interfaces that are down are incorrectly shown as up. The tooltip on the interface shows the correct status.
1025201	FortiGate encounters a duplication issue in a hub and spoke configuration with set packet-duplication force enabled on a spoke and set packet-de-duplication enabled on the hub.

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, ForriSwitches, FortiAPs and endpoint device traffic. This is a GUI only display issue and does not impact operations of downstream devices.
1011833	When multiple admins login to the GUI at the same time, node process may experience a spike in CPU usage if there are many downstream devices in the Security Fabric. This can result in slow loading time for multiple GUI pages. **Workaround**: Disconnect the other concurrent admin sessions to avoid overloading node process.
1120652	Fabric topology - 2 devices on different vdoms but behind same router show wrong vdom data on tooltip **Workaround**: : disable device-identification on that interface

SSL VPN

Bug ID	Description
795381	FortiClient windows cannot be launched via sslvpn web portal
941676	Incorrect character entered when using Shift+2 on Japanese keyboard during RDP session in SSL-VPN web mode.

Switch Controller

Bug ID	Description
947351	The FortiSwitch topology fails to load correctly and triggers Java errors in HTTPS logs when switches are connected via SFPs.
961142	An interface in FortiLink is flapping with an MCLAG FortiSwitch using DAC on an OPSFPP-T-05-PAB transceiver.

System

Bug ID	Description
782710	VLAN-over-VXLAN traffic was not being offloaded to NP7, causing performance issues due to increased CPU load.
882862	On 400F/600F/900G/3200F/3700F, LAG interface members are not shutting down when the remote end interface(one member in the LAG) is admin down.

901621	On the NP7 platform, setting the interface configuration using set inbandwidth <x> or set outbandwidth <x> commands stops traffic flow.
	Workaround: Change the NP7 "default-qos-type" setting from shaping to policing. This requires a restart of the device for the configuration to take effect.
	`config system npu`
	`  set default-qos-type policing`
	`end`

921604	601F the ports x7 had the link status as up/green with no cables attached
1045866	"node" daemon causes high CPU usage and memory consumption when many interfaces are being edited or created at once.
1078119	Traffic is intermittently interrupted on virtual-vlan-switch on Soc5 based platforms when a multicast or broadcast packet is received
1078541	FortiFirewall 2600F models may become stuck after a fresh image burn. Upgrading from a previous version stills works. **Workaround**: power cycle the unit.
1114594	On the FG-200G, sdns is not able to connect to FortiGuard servers. This issue only affects FG-200G. **Workaround**: use DNS instead of SDNS: FortiGate-201G # show sys dns config system dns set primary 96.45.45.45 set secondary 96.45.46.46 set protocol dot <<<<<<<<<< replace with cleartext
1121548	Enabling "device-identification" also get endpoint information even though intermediate router exist on FG and endpoints. **Workaround**: : disable device-identification on that interface

Upgrade

Bug ID	Description
1055486	Firmware and Registration page - When user performs Fabric Upgrade via the GUI for the whole Fabric topology that includes managed FortiAP and FortiSwitch, the root FortiGate may use an incorrect recommended image for FortiAP and FortiSwitch due to a parsing issue. **Workaround**: User can initiate Fabric Upgrade via the CLI command.

User & Authentication

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

VM

Bug ID	Description
899984	Should not downgrade to any GA earlier than 7.2.4 if FGTVM was deployed in UEFI bootup mode.
1094274	FortiOS becomes unresponsive when sending IPv6 traffic over MLX5 network adapters due to incorrect WQE handling.
1119140	Incorrect deployment of DLP configurations occurs when FortiGate VMs are deployed on hypervisors with Intel Skylake processors.

Web Filter

Bug ID	Description
885222	HTTP sessions are logged as HTTPS in web filter logs when using an HTTP VIP server, causing incorrect protocol identification.

WiFi Controller

Bug ID	Description
869106	The layer-3 roaming feature may not work when wireless controller is running multiple cw_acd processes (i.e. when the value of "acd-process-count" is not zero).
869978	In HA cluster of FGT-200F units with 'capwap-offload' enabled, traffic from tunnel SSID cannot pass after HA failover is triggered.
873273	The automatically connect option fails to function when the local radio connection is lost on some FortiGate models.
941691	Managed FortiSwitch detects multiple MACs using the same IP address.

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 6.00303 is released as the built-in AV Engine.

Built-in IPS Engine

IPS Engine 7.00367 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.

Limitations on HA cluster formation between different FortiGate Rugged 60F and 60F 3G4G models

FortiGate Rugged 60F and 60F 3G4G models have various generations defined as follows:

- Gen1
- Gen2 = Gen1 + TPM
- Gen3 = Gen2 + Dual DC-input
- Gen4 = Gen3 + GPS antenna
- Gen5 = Gen4 + memory

The following HA clusters can be formed:

- Gen1 and Gen2 can form an HA cluster.
- Gen4 and Gen5 can form an HA cluster.

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



www.fortinet.com

Copyright© 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.