FortiOS Release Notes

VERSION 5.2.3

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO LIBRARY

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

December 08, 2015

FortiOS 5.2.3 Release Notes

01-523-268616-20151208

TABLE OF CONTENTS

Change Log

Date	Change Description
2015-03-23	Initial release.
2015-03-25	Added known FortiSandbox issues.
2015-03-26	Added bug 258813 (Kernel section) to Resolved Issues. Made minor formatting changes.
2015-03-31	Added FG-3810D to Supported Models.
2015-04-02	Added a FG-3810D note to the Introduction.
2015-04-07	Added a bug to the Known Issues.
2015-04-10	Added bug 256100 to Resolved Issues. Added FG-3700DX - build number 4850, branch point 670 to Supported Models
2015-04-16	Minor typographic change.
2015-04-29	Added FG-1200D build number 4870, branch point 670 to Supported Models.
2015-05-01	Added FG-1000D build number 4873, branch point 670 to Supported Models.
2015-05-20	Added FG-400D build number 4906, branch point 670 to Supported Models.
2015-05-29	Added 279766 to Known Issues List. Updated What's New section with: Changes to FortiGate Models that support WAN Optimization.
2015-06-22	Added FG-600D build number 4944, branch point 670 to Supported Models.
2015-06-24	Added bug 276779 to Known Issues List.
2015-07-28	Added FG-3000D, FG-3100D, and FG-3200D build number 4955, branch point 670 to Supported Models.
2015-09-02	FSSO 4.3 build 0164 contact Support for download.
2015-09-03	Added bug 286162 to Known Issues List.
2015-10-27	Updated Upgrade Information.
2015-12-08	Added 268589 to Resolved Issues.
2016-03-22	Added 269094 to Resolved Issues.
2016-05-09	Added FortiManager 5.0.10 Support to Product Support & Integration.

Introduction

This document provides the following information for FortiOS 5.2.3 build 0670:

- Introduction
- Special Notices
- Upgrade Information
- Product Integration and Support
- Resolved Issues
- Known Issues
- Limitations

See the Fortinet Document Library for FortiOS documentation.

Supported models

FortiOS 5.2.3 supports the following models.

FortiGate	FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-SFP, FG-60C-POE, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-80C, FG- 80CM, FG-80D, FG-90D, FGT-90D-POE, FG-92D, FG-94D-POE, FG-100D, FG-110C, FG- 111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG- 200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-310B-DC, FG-311B, FG-500D, FG-600C, FG-620B, FG-620B-DC, FG- 621B, FG-800C, FG-1000C, FG-1240B, FG-1500D, FG-3016B, FG-3040B, FG-3140B, FG-3240C, FG-3600C, FG-3700D, FG-3810A, FG-3810D, FG-3700DX, FG-3950B, FG-3951B, FG-5001B, FG-5001C, FG-5001D, FG-5101C
FortiWiFi	FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-3G4G-VZW, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D
FortiGate Rugged	FGR-60D, FGR-100C
FortiGate VM	FG-VM32, FG-VM64, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN
FortiSwitch	FS-5203B
FortiOS Carrier	FCR-3810A, FCR-3950B, FCR-5001A-DW, and FCR-5001B FortiOS Carrier 5.2.3 images are delivered upon request and are not available on the customer support firmware download page

The following models are released on a special branch based off of FortiOS 5.2.3. As such, the *System> Dashboard > Status* page and the output from the `get system status` CLI command displays the build number.

FG-98D-POE	FortiGate 98D-POE is released on build 4843.
FG-400D	FortiGate 400D is released on build 4906.
FG-600D	FortiGate 600D is released on build 4944.
FG-1000D	FortiGate 1000D is released on build 4873.
FG-1200D	FortiGate 1200D is released on build 4870.
FG-3000D	FortiGate 3000D is released on build 4955.
FG-3100D	FortiGate 3100D is released on build 4955.
FG-3200D	FortiGate 3200D is released on build 4955.
FG-3700DX	FortiGate 3700DX is released on build 4850.
FG-3810D	FortiGate 3810D is released on build 4835.

To confirm that you are running the proper build, the output from the `get system status` CLI command has a **branch point field** that should read **0670**.

The FG-60D-3G4G-VZW model uses the FGT_60D_MC-v5-build0670-FORTINET.out image. The FWF-60D-3G4G-VZW model uses the FWF_60D_MC-v5-build0670-FORTINET.out image.

What's new in FortiOS 5.2.3

For a list of new features and enhancements that have been made in FortiOS 5.2.3 see the *What's New for FortiOS 5.2* document available in the Fortinet Document Library.

New Feature

- VM License Check Time Extension

IPv6

- TFTP Session Helper

FortiLink

- FortiLink in FG-60D with FSR-112D-POE and FS-108D-POE with validation

SSL VPN

- Options added to allow the firewall address to be used in the routing table

System

- Cloud APT License
- NP6 - SYN Proxy

GUI

- Log Viewer improved
- Certificate GUI improved
- Admin login permissions for policies, addresses, services, and schedules corrected
- FOS interface was updated to make the FSW connection more user friendly. Users are allowed to change VDOM operation mode by improving the Certificate GUI
- FortiView and SSLVPN videos added to FortiOS GUI support for FSSO/Microsoft Exchange Server
- Source and destination interface added to FortiView
- FortiSandbox-FortiOS (FortiView) integrated
- FortiSwitch Management video added to the FortiOS GUI

Default Setting/CLI/Tablesize Change

- Split tunneling enabled with default FortiClient dialup IPsec VPN
- Redirect-URL parameter increased from 128 to 256
- Show switch controller by default when available (300D and below)
- 300D/500D factory default updated to include Sniffer ports (port 4 & 8 for 300D; port 5, 6, 13, 14 for 500D)
- `firewall.vip6` and `firewall.vipgrp6` values and missing tablesize details corrected.
- WF and App Profile tablesize aligned
- `VDOM.property` tablesize corrected
- Block notification changed from enabled to disabled
- SSLVPN hardware acceleration disabled and set Central Management to FortiGuard for FortiGate-92D
- WTP-profile capacity increasedto 1024 for FGT_VM8
- Default SSLVPN Server Certificate changed to Fortinet_Factory
- 300D/500D default app profile updated in the default Sniffer interface

Firewall

- Exemptions added to `SSL-deep-inspection` default profile for commonly used websites

FortiAP

- FortiAP LED dark support

FortiGate-5001D

- 4x10G interfaces in 5001D 40G port support

Logging and Report

- Admin permissions added to start or defer the file system check if the FGT was shutdown properly

Changes to FortiGate Models that support WAN Optimization

- See the FortiOS 5.2.3 Feature Platform Matrix for information about how FortiGate models support WAN Optimization.

FSSO

- FSSO agent support OU in group filters (requires FSSO v5.0)

Special Notices

Compatibility with FortiOS versions

The following units have a new WiFi module built-in that is not compatible with FortiOS 5.2.1 and lower. It is recommended to use FortiOS 5.2.2 and later for these units.

Affected models

Model	Part Number
FWF-60CX-ADSL	PN: 8918-04 and later

The following units have a memory compatibility issue with FortiOS 5.2.1 and lower. It is recommended to use FortiOS 5.2.2 and later for these units.

Affected models

Model	Part Number
FG-600C	PN: 8908-08 and later
FG-600C-DC	PN: 10743-08 and later
FG-600C-LENC	PN: 11317-07 and later

Default log setting change

For FG-5000 blades and FG-3900 series, log disk is disabled by default. It can only be enabled via CLI. For all 2U & 3U models (FG-3600/FG-3700/FG-3800), log disk is also disabled by default. For all 1U models and desktop models that supports STAT disk, log disk is enabled by default.

FG-5001D operating in FortiController or Dual FortiController mode

When upgrading a FG-5001D operating in FortiController or dual FortiController mode from version 5.0.7 (B4625) to FortiOS version 5.2.3, you may experience a back-plane interface connection issue. This is due to a change to the ELBC interface mapping ID. After the upgrade, you will need to perform a factory reset and then re-configure the device.

FortiGate units running 5.2.3

FortiGate units running 5.2.3 and managed by FortiManager 5.0.0 or 5.2.0 may report installation failures on newly created VDOMs, or after a factory reset of the FortiGate unit even after a retrieve and re-import policy.

Firewall services

Downgrading from 5.2.3 to 5.2.2 may cause the default protocol number in the firewall services to change. Double check your configuration after downgrading to 5.2.2.

FortiPresence

For FortiPresence users, it is recommended to change the FortiGate web administration TLS version in order to allow the connection.

```
config system global
   set admin-https-ssl-versions tlsv1-0 tlsv1-1 tlsv1-2
end
```

SSLVPN setting page

The default server certificate has been changed to the `Fortinet_Factory` option. This excludes FortiGate-VMs which remain at the `self-signed` option. For details on importing a CA signed certificate, please see the How to purchase and import a signed SSL certificate document.

Upgrade Information

Upgrading from FortiOS 5.2.1 or later

FortiOS version 5.2.3 officially supports upgrade from version 5.2.1 or later.

Upgrading from FortiOS 5.0.10 or later

FortiOS version 5.2.3 officially supports upgrade from version 5.0.10 or later.

When upgrading from releases prior to 5.0.11, if the source version is 5.0.10 with a configured HA cluster, you must schedule a down time; disable an uninterruptible upgrade; perform the upgrade; then, enable it back.

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
- VDOM parameters/settings
- admin user account
- session helpers
- system access profiles.

FortiGate VM firmware

Fortinet provides FortiGate VM firmware images for the following virtual environments:

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the QCOW2 file for Open Source XenServer.

- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains QCOW2 that can be used by `qemu`.

Microsoft Hyper-V

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.hyperv.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains three folders that can be imported by Hyper-V Manager on Hyper-V 2012. It also contains the file `fortios.vhd` in the Virtual Hard Disks folder that can be manually added to the Hyper-V Manager.

VMware ESX and ESXi

- `.out`: Download either the 32-bit or 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.ovf.zip`: Download either the 32-bit or 64-bit package for a new FortiGate VM installation. This package contains Open Virtualization Format (OVF) files for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

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 select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

Product Integration and Support

FortiOS 5.2.3 support

The following table lists 5.2.3 product integration and support information:

Web Browsers	• Microsoft Internet Explorer version 11 • Mozilla Firefox version 36 • Google Chrome version 40 • Apple Safari version 7.0 (For Mac OS X) Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Internet Explorer versions 8, 9, 10, and 11 • Mozilla Firefox version 27 • Apple Safari version 6.0 (For Mac OS X) • Google Chrome version 34 Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	• 5.2.1 and later • 5.0.10 You should upgrade your FortiManager prior to upgrading the FortiGate.
FortiAnalyzer	• 5.2.0 and later • 5.0.7 and later You should upgrade your FortiAnalyzer prior to upgrading the FortiGate.
FortiClient Microsoft Windows and FortiClient Mac OS X	• 5.2.2 and later
FortiClient iOS	• 5.2.0 and later
FortiClient Android and FortiClient VPN Android	• 5.2.4 and later

FortiAP	• 5.2.3 and later • 5.0.9 You should verify what the current recommended FortiAP version is for your FortiAP prior to upgrading the FortiAP units. You can do this by going to the *WiFi Controller* > *Managed Access Points* > *Managed FortiAP* page in the GUI. Under the *OS Version* column you will see a message reading *A recommended update is available* for any FortiAP that is running an earlier version than what is recommended.
FortiSwitch OS (FortiLink support)	• 3.2.0 Supported models: FS-108D-POE, FS-224D-POE, FSR-112D-POE • 3.0.1 and later Supported model: FS-224D-POE • 2.0.3 Supported models: FS-28C, FS-324B-POE, FS-348B, FS-448B
FortiSwitch-ATCA	• 5.0.3 and later Supported models: FS-5003A, FS-5003B
FortiController	• 5.2.0 Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C • 5.0.3 and later Supported model: FCTL-5103B
FortiSandbox	• 1.4.0 and later • 1.3.0

Fortinet Single Sign-On (FSSO)	• 5.0 build 0237 (needed for FSSO agent support OU in group filters)
	  • Windows Server 2008 64-bit
	  • Windows Server 2008 R2 64-bit
	  • Windows Server 2012 Standard
	  • Windows Server 2012 R2 Standard
	• 4.3 build 0164 (contact Support for download)
	The following operating systems are supported:
	  • Microsoft Windows Server 2003 R2 (32-bit and 64-bit)
	  • Microsoft Windows Server 2008 (32-bit and 64-bit)
	  • Microsoft Windows Server 2008 R2 64-bit
	  • Microsoft Windows Server 2012 Standard Edition
	  • Microsoft Windows Server 2012 R2
	  • Novell eDirectory 8.8
	FSSO does not currently support IPv6.

FortiExplorer	• 2.6 build 1083 and later. Some FortiGate models may be supported on specific FortiExplorer versions.
FortiExplorer iOS	• 1.0.6 build 0130 and later Some FortiGate models may be supported on specific FortiExplorer iOS versions.
FortiExtender	• 2.0.0 build 0003 • 1.0.0 build 0024
AV Engine	• 5.164
IPS Engine	• 3.072
Virtualization Environments	
Citrix	• XenServer version 5.6 Service Pack 2 • XenServer version 6.0 and later
Linux KVM	• CentOS 6.4 (qemu 0.12.1) and later
Microsoft	• Hyper-V Server 2008 R2, 2012, and 2012 R2
Open Source	• XenServer version 3.4.3 • XenServer version 4.1 and later
VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1 and 5.5

Language support

The following table lists language support information.

Language support

Language	GUI	Documentation
English	✔	✔
Chinese (Simplified)	✔	-
Chinese (Traditional)	✔	-
French	✔	-
Japanese	✔	-
Korean	✔	-
Portuguese (Brazil)	✔	-
Spanish (Spain)	✔	-

To change the FortiGate language setting, go to *System* > *Admin* > *Settings*, in *View Settings* > *Language* select the desired language from the drop-down menu.

Module support

FortiOS 5.2.3 supports Advanced Mezzanine Card (AMC), Fortinet Mezzanine Card (FMC), Rear Transition Module (RTM), and Fortinet Storage Module (FSM) removable modules. These modules are not hot swappable. The FortiGate unit must be turned off before a module is inserted or removed.

Supported modules and FortiGate models

Module	FortiGate Model
Module: ASM-S08 Type: Storage	FG-310B, FG-620B, FG-621B, FG-3016B, FG-3810A, FG-5001A
Module: FSM-064 Type: Storage	FG-200B, FG-311B, FG-1240B, FG-3040B, FG-3140B, FG-3951B
Module: ASM-FB4 Type: Accelerated interface	FG-310B, FG-311B, FG-620B, FG-621B, FG-1240B, FG-3016B, FG-3810A, FG-5001A

Module	FortiGate Model
Module: ADM-XB2 Type: Accelerated interface	FG-3810A, FG-5001A
Module: ADM-FB8 Type: Accelerated interface	FG-3810A, FG-5001A
Module: ASM-FX2 Type: Bypass	FG-310B, FG-311B, FG-620B, FG-621B, FG-1240B, FG-3016B, FG-3810A, FG-5001A
Module: ASM-CX4 Type: Bypass	FG-310B, FG-311B, FG-620B, FG-621B, FG-1240B, FG-3016B, FG-3810A, FG-5001A
Module: ASM-CE4 Type: Security processing	FG-1240B, FG-3810A, FG-3016B, FG-5001A
Module: ADM-XE2 Type: Security processing	FG-3810A, FG-5001A
Module: ADM-XD4 Type: Security processing	FG-3810A, FG-5001A
Module: ADM-FE8 Type: Security processing	FG-3810A
Module: RTM-XD2 Type: Rear transition	FG-5001A
Module: ASM-ET4 Type: Security processing	FG-310B, FG-311B
Module: RTM-XB2 Type: Rear transition	FG-5001A
Module: FMC-XG2 Type: Security processing	FG-3950B, FG-3951B
Module: FMC-XD2 Type: Accelerated interface	FG-3950B, FG-3951B
Module: FMC-F20 Type: Accelerated interface	FG-3950B, FG-3951B

Module	FortiGate Model
Module: FMC-C20 Type: Accelerated interface	FG-3950B, FG-3951B
Module: FMC-XH0 Type: Security processing	FG-3950B

SSL VPN support

SSL VPN standalone client

The following table lists SSL VPN tunnel client standalone installer for the following operating systems.

Operating system and installers

Operating System	Installer
Microsoft Windows XP Service Pack 3(32-bit) Microsoft Windows 7 (32-bit & 64-bit) Microsoft Windows 8 (32-bit & 64-bit) Microsoft Windows 8.1 (32-bit & 64-bit)	2312
Linux CentOS 6.5 (32-bit & 64-bit) Linux Ubuntu 12.0.4 (32-bit & 64-bit)	2312
Virtual Desktop for Microsoft Windows 7 Service Pack 1 (32-bit)	2312

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

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 32-bit SP1	Microsoft Internet Explorer versions 9, 10 and 11 Mozilla Firefox version 33

Operating System	Web Browser
Microsoft Windows 7 64-bit SP1	Microsoft Internet Explorer versions 9, 10, and 11 Mozilla Firefox version 33
Linux CentOS version 5.6	Mozilla Firefox version 5.6
Linux Ubuntu version 12.0.4	Mozilla Firefox version 5.6

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

SSL VPN host compatibility list

The following table lists the antivirus and firewall client software packages that are supported.

Supported Microsoft Windows XP antivirus and firewall software

Product	Antivirus	Firewall
Symantec Endpoint Protection v11	✔	✔
Kaspersky Antivirus 2009	✔	
McAfee Security Center v8.1	✔	✔
Trend Micro Internet Security Pro	✔	✔
F-Secure Internet Security 2009	✔	✔

Supported Microsoft Windows 7 32-bit and 64-bit antivirus and firewall software

Product	Antivirus	Firewall
CA Internet Security Suite Plus Software	✔	✔
AVG Internet Security 2011		
F-Secure Internet Security 2011	✔	✔
Kaspersky Internet Security 2011	✔	✔
McAfee Internet Security 2011	✔	✔
Norton 360™ Version 4.0	✔	✔

Product	Antivirus	Firewall
Norton™ Internet Security 2011	✔	✔
Panda Internet Security 2011	✔	✔
Sophos Security Suite	✔	✔
Trend Micro Titanium Internet Security	✔	✔
ZoneAlarm Security Suite	✔	✔
Symantec Endpoint Protection Small Business Edition 12.0	✔	✔

Resolved Issues

The following issues have been fixed in version 5.2.3. For inquires about a particular bug, please contact Customer Service & Support.

DLP

Bug ID	Description
262764	When the DLP blocks email, the email subject should be over-writable with the configured replacement message.
260647	Provide more precise detection for MOV files.
261567	Outlook Web Access files should be detectable.
270108	The DLP may not detect the SSN correctly.

ELBC

Bug ID	Description
258954	Traffic destined for the SSLVPN tunnel network should always be sent to the master worker-blade (SLBC).

Endpoint Control

Bug ID	Description
256717	Current VDOM settings in the EC daemon with multiple concurrent FortiClient connections, may cause a race condition to occur.

Firewall

Bug ID	Description
263901 262173 259156 214301 254366 252606	Improve per-VDOM firewall authentication.
261745	Using Akamai, restore the support for HTTP Cookie Load-Balance.
265375	In deep-inspection mode , the server certificate chain validation may not be handled correctly.

Bug ID	Description
199253	When a HTTP message is sent to the ICAP server, duplicate ICAP requests may be sent.
257807	The default UDP custom service may have the `tcp-portrange 0:0` in its definition.
258976	Ensure the IPLD VIP List is consistent with the current *firewall.vip* configuration.
264723	Improve the SMTP, POP3, NNTP and FTP protocol detection.
259942	The *scanunit daemon* may be able to handle raw, deflate, encoding, and decompression without a header.
261506	TCP statuses *timeout* and *close* may not be added in the IPv6 log session, and may not reflect the TCP status in the IPv6 traffic logs.
256488	If there is a firewall policy change, the TCP session may disconnect.
260044	If the SSLVPN policy is configured, the WCCP may not configure.
257797	The unbounded proxy log queue size may be incorrect.
266482	If you restart the unit, the natip setting may reset.
266592	For admission request messages, the RAS helper may not start the NAT process.
263289	Using the server load-balance, allow the HTTP POST to be larger than 4GB.
257521	The SSL Offload may not be able to talk to SSL 3.0 Only Server.
267038	The Server Load Balance VIP with proxy-based UTM may drop the session when it is balanced to the slave unit.
264125	The HTTP Proxy may not properly identify a chunked encoding terminator.
264756	Bypass on Session Ticket for Certificate Inspection mode may not be handled as expected.
182015 239522	Workers may not be able to release unused memory back to the kernel. New proxy counters and malloc trim calls may not be implemented.
259681	In full SSL mode, a high amount of HTTPS transactions may not work as expected. A *SSL decryption failure* message may appear.
267600	The RSSO agent may not insert user information from the Accounting Request.
241945	The traffic quota in the Fortinet Bar may not be supported.
268460	The FSSO may drop users before retrieving the complete list.
267773	If the IPv6 source address uses the same port for NAT, the NAT64 session may not work.

Bug ID	Description
260470	The SSL Persistence Support in SSL Offload via `SessionTickets` may not be restored.

FortiCarrier

Bug ID	Description
266695	The `replacemsg-group` for MM1 messages may be incorrect.

FortiGate VM

Bug ID	Description
264912	FGT-VM option to select the strongest Cipher Suite in Client Hello is now available.
258718	HyperV network driver may not support the promiscuous mode.
250054	When there is a license status change or a warning has occurred, the FGT-VM license alert may not appear on the event log.

FortiGate 60C POE

Bug ID	Description
265510	There may be a booting issue caused by the LTE-Modem.

FortiGate-1500D

Bug ID	Description
240001	There may not be a 10G full duplex option.

FSSO

Bug ID	Description
265608	Korean character ID may not work as expected.

GUI

Bug ID	Description
264705	Importing *.crt files* with multiple *x.509 certs* on a single line may cause the *httpsd* to stop working.
257344	If there are over 1000 entries, the Policy List may not remember the last view mode.
260342	The DOS Policy ID may be missing in the GUI.
230125	Addressed with different associated interface may be added to the same group via the GUI.
263799	When the address is in use, users may be able to change associated interfaces.
255424	On a customer configuration with 40,000 address objects, the address section may not be displayed by the GUI.
257356	In the object usage dialog, long item lists may be displayed.
244979	The GUI may trim string value `set-monitor` to 64 characters.
261925	In the GUI, policies with large digit IDs may not be able to be reordered.
264983	When trying to edit the Display Zone from the GUI, the Member Interface List may be slow to display.
262171	The Context Menu in the Firewall Policy may be set to `read-only`.
260342	In the GUI, the DOS Policy may be missing.
265263	Th FortiView Destination Interface Filter may not work properly.
265481	When editing the SSL VPN setting and applying it, a *Permission Denied. Insufficient Privileges.* error message may appear.
264210	Japanese usernames from failed login attempts may appear truncated.
266824	Overlong 2 byte UTF-8 sequence may be detected when decoding string.
257356	In the Object Usage or View Details Pop Up, there may be missing data.
266559	When editing a user, an *Error 404: The web page cannot be found.* message may appear.
268676	In HA Clusters, the *Last Used* Time of Policies may be inconsistent.
269897	The Static Schedule and Service Objects may not be supported.
266438	You may not be able to skip loopback interfaces for Virtual IP or Virtual IP groups.
244043	If no disks are installed, you may not be able to hide the disk usage in the *Sysres* widget.

High Availability

Bug ID	Description
263753	If the link-monitor is configured on the VLAN interface, the High Availability failover may not be triggered.
264836	When editing the default admin account in the CLI, it may not synchronize with the High Availability environment.
265606	The slave *debugzone* and *checksum* may not match.
263080	After a failover is performed by the reboot master unit, the slave's PPP interface information may not synchronize with the master unit.
232253	In an IKE setup, dialup connections may not be added on the slave.
259508	When there are two ore more PPP interfaces, the master and slave may create them in different orders. The PPP devices may receive different names.
244702	When logging into the High Availability slave through the management interface, the FortiManager warning may not appear.
232458	When there is a session state change to local & redir between the `TCP_S_ESTABLISHED` and `TCP_S_CLOSE`, `TCP_S_CLOSE` may not synchronize with the `TCP_S_ESTABLISHED`.
260251	The *hasync high CPU* and *sync* may contain errors.
266149	When the kernel `session-sync-dev` is configured, the *sync daemon* session may become 100% busy.
267249	The vcluster2's VMAC on the VLAN Interface may not be persistent after vcluster1 failover.
259334	After upgrading to 5.0, clusters may be out of sync. One cluster unit may restart.
254388	Priority of LACP and HA packets may not be escalated.
261669	ARP Requests and NP Accelerated Sessions may cause high CPU usage.

IPS Engine

Bug ID	Description
265517	The RTCP packets may be blocked by the Application Control UTM.
268589	Some packets are dropped when `nturbo` is enabled.

IPsec VPN

Bug ID	Description
250815	If the embryonic limit is reached, the IPsec reconnection may stall.
261066	In the IPsec interface, there may be an error with the link-monitor feature.
257943	In some cases, the IPsec primary and secondary may start simultaneously.
263428	IPsec tunnels may go down after 420 days of uptime.
266115	When handling `IKEv2 SA_INIT` packet as a Responder, the `iked` may crash.

IPv6

Bug ID	Description
259322	If the BGP peer is deactivated and reactivated, the `as-override-flag` may not appear.
266573	If the `link-monitor` is renamed, it may stop working.

Kernel

Bug ID	Description
258813	If Avalanche is used to set up 1000 IPSec tunnels, and http traffic is sent over each tunnel, the kernel may stop working.

Log & Report

Bug ID	Description
265999	Sending, uploading, and storing logs may occur multiple times a day.
257694	When the application has `set log disable` applied, the Application Control Log may be still created.
265999	Store and Upload may send Logs multiple times a day.
264706	The Service Name Lookup for the IPv6 Traffic Log may be incorrect.
254899	When the Source is a FortiAnalyzer, Traffic Logs may not be displayed.
269094	`reportd daemon` not running after enabling report settings.

Routing

Bug ID	Description
252890	If there are two consecutive zero next headers, the pointer in the *icmpv6* parameter may not work as expected.
256369	Redistributed IPv6 routes may not be prevented, which may cause the Peer's address to be nexthop and may be advertised to the same BGP Peer.
267778	Upon receiving the `one-way hello` packet, the *OSPF Graceful Restart Helper Mode* may be exited.

Spam Filter

Bug ID	Description
260172	If the regular expression is used to check for URL syntax, the URLs may be identified in an email and sent to FortiGuard.

SSL VPN

Bug ID	Description
262256	If the SSLVPN portal does not set up `ip-pools` and is restarted, the SSLVPN portal configuration may be partially lost.
262156	In some cases, the SSLVPN may send a `sslvpnerrmsg` key or number to the FortiClient. When the FortiClient looks in the local map to find the corresponding message, English may be the only language supported.
259820	The SSLVPN web mode URL may not be able to handle the CGI character `/` as a variable.
247112 265504	If a SSLVPN `idle-timeout-expire` and `portal-relogin` occurs, the RDPnative may not work.
263597	SSLVPN authentication response duration may not be notified to the FortiClient.
261540	In some cases, a LDAP user with FortiToken may not be able to login via SSLVPN tunnel using FortiClient.
241883	SSLVPN soap address location link may not be rewritten to gain access through the proxy.
261759	If the DNS query is not correct, the SSLVPN links may not receive a data error.
262162	SSLVPN may not be able to gain access to the remote server though a forwarding port.
262964	The SSLVPN Web mode traffic may be sourced with a random IP.
261180	Some SSLVPN users may not be redirected to the NAC portal.

System

Bug ID	Description
266456	If a remote login admin is used, and the *ssh client* closes the TCP session before the auto-backup is completed on the FortiGate, a temporary file on the memory disk may not be removable causing a memory leak.
253445	Removing FGT from a FMG backup ADOM may not remove all the FGT settings.
258881	In some cases, disabling the `client-log-when-on-net` may not work as expected.
262017	SNMPV3 linkUp/linkDown traps may be sent with an extra zero.
253396	The *Huawei E3276* and *E598* modems may not be supported.
257207	The system may not restore the interface configuration when an invalid interface is referenced.
250125	If the IPgeo database is updated, and there are duplicate geography IP addresses registered in the firewall, the kernel may not remove the registered address and reload the new geography IP addresses.
260381	If there is a null `trusthost` between valid `trusthost`, the admin user may not be able to login to the FGT.
266139	When recursive lookups are enabled, the FortiOS may not always set the *Recursion Available* to *true*.
260299	If the nested `config` command is applied, the `append` command in the CLI may not work.
265242	In some cases, the FortiGate may not backup the configuration onto a USB memory stick in the CLI.
190133	The set `enc-offload-antireplay`, `dec-offload-antireplay`, `offload-ipsec-host-enable/disable` functions for *np4* may not be removed.
255831	The `mod_time()` function warning may not be removed in the kernel.
263434	When the *standalone sync* is enabled, the kernel may check on the TCP sync paket.
258694	After 497 days of uptime, the ACD process and CPU may spike and crash with signal 6.
261349	FGT may be unable to read the UPN in SAN extension certificate.
264367	If the admin user has the `accprofile-override`enabled, when the *scp* checks the permissions, it only uses the `accprofile-config`in *cmdb* instead of the `accprofile-returned-from-remote`
253652	MAC Address learning on interfaces out of the Virtual Switch may not be disabled.
248912	Due to sequence number checking, the first data packet from the server may be dropped.

Bug ID	Description
267925	If the IPS is enabled, the DHCP Traffic in TP Mode may not pass the firewall.
267767	X509v3 Basic Constraints may be misplaced in generated Certificate Signing Request.
243840	When `include-default-servers` is enabled, the FGT may not be able to backup configurations to the FMG.
257909	After upgrading to v5.0.9, `admin-cert` may change from `Fortinet_Factory` to `Self-sign`.
267131	AVEngine and AV Database Corruption Handling may not work as expected.
242971	NP6 Shaping may be too aggressive for the TCP Flow.
257176	When adding FortiAPs to FortiGate-60C PoE, there may be a CPU increase.

Spam Filter

Bug ID	Description
260172	If the regular expression is used to check for URL syntax, the URLs may be identified in an email and sent to FortiGuard.

Server

Bug ID	Description
261870 260954	FortiGate/FortiWifi 40C and 100/200 series (FGT-40C, FWF-40C, FGT-100D, FGT-140D, FGT-140D-POE, FGT-140D-POE-T1, FGT-200D, FGT-200D-POE, FGT-240D, FGT-240D-POE, FGT-280D-POE) may not be included to the FortiDeploy process.
259823	Moscow and Minsk timezones may not be updated.
263301	When the broadcast flag is set to `DCHPDISCOVER`, `DCHPOFFER` may be sent as a broadcast from the DHCP server to the DHCP relay agent.
262881	The FSSO may send too many requests which may cause the DNS proxy service to crash.
267262	In some cases, the vip configuration in the CLI may not be able to change with profile admin permissions.
264948	If a reserved client belongs to another subnet, and sends a DHCP renew broadcast, the DHCP server may crash.
262817	*Port 444* in *VIP* or *admin-port* may not work.
259973	*Huawei E3372 Modem* may not be supported.

Upgrade

Bug ID	Description
261350	If the config is large, the interruptible upgrade may not work properly.
261622	If the master unit is restarted, the session may not synchronize back to the new slave.
261562	When upgrading from *v4.3* the TCP reset settings may change.
259980	After upgrading, the FGT-20C ADSL A WAN interface may be missing.
248293	After upgrading to *v5.2*, all failed queries may be logged.
263040	Upgrading from *v4.3.16* may cause a checksum mismatch in the *HAoC cluster*.
256100	If you downgrade from 5.0.9 to 5.0.7 then upgrade to 5.0.9 again, the Service Custom Protocol number may be incorrect.

VoIP

Bug ID	Description
250077	When receiving a SIP call from a specific number, the *IM Daemon* may crash.
261920	In Invite Message, the SIP ALG may not open a pinhole for the contact port.
269489	Sever `HelloRequest` may not be propagated to the client in SIP SSL.

WAN Optimization and Webproxy

Bug ID	Description
265129	When there are two explicit proxies, a standard HTTPS page may not load.
265634	If the session is closed, the `socket_port`may not close properly.
256489	If the destination interface is longer than 15 characters, the WAN Optimization tunnel may stop working.
266021	The FTP proxy may not handle multi-line responses correctly.
266178	When the `user-limit` is reached and NTLM authentication is used, the *WAD daemon* may stop working.
257265	The App Control Proxy may block the Explicit Proxy Policy.
268403	When the Header File has inconsistent content length and content range attributes, the explicit proxy may be incorrect.
262499	In Webproxy Mode, the reported protocol for the Traffic Log may be incorrect.

Webfilter

Bug ID	Description
265515	If there is a SSL Inspection exemption in the flow-base, the re-categorized page may be ignored.
259838	Flow-based FortiGuard webfilter statistics for SNMP monitoring may not be added.
263146	Incorrect certificate may be used for HTTPS site with web filter authentication.
260317	FortiGate may use default server certification in the web override message, even though it was configured to use a customized certification.
252749	The logo may not be displayed on the webfilter flow-based replacement message.
265515	In the SSL Inspection Exemption in `flow-base`, the Re-categorized page may be ignored.
182863	The URL Filter may be stuck in No Correct FortiGuard Information state.
267879	If an URL with CGI is configured as a Local Rating, the Web Filter may not be able to find this URL match in the Local Rating.
263146	An incorrect certificate may be used for HTTPS with the authenticate option selected on the Web Filter.

WiFi

Bug ID	Description
260645	If the user is not authenticated, traffic matching and split tunneling ACL may be able to still pass through.
260473	A Point to Point Wireless Bridge on 5GHz with 11 AC ARP may not be received on the station behind the leaf AP.
256087	Restarting a cluster of FGT200D may break the connection to FAP.
195093	For FortiAP-222B and 320-B WTP-Profiles, you may not be able to increase the TX Power to the maximum.

Known Issues

The following issues have been identified in version 5.2.3. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Firewall

Bug ID	Description
273909	SSL connection via LB VIP with SSL offloading may encounter a SSL handshake issue.

FortiGate-1000D

Bug ID	Description
279766	There may be an incorrect NP6 transmit traffic shaper on FortiGate 1000D.

FortiGate-5101C

Bug ID	Description
268727	After configuring `isf-acl`, the Kernel Panic Crash Log may be displayed.

FortiGate-VM

Bug ID	Description
272438	During the boot-up sequence, the FortiGate-VM device may encounter a harmless configuration error message.

FortiManager

Bug ID	Description
271059	FortiGate units running 5.2.3 and managed by FortiManager 5.0.0 or 5.2.0 may report installation failures on newly created VDOMs, or after a factory reset of the FortiGate unit even after a retrieve and re-import policy.
286162	FortiManager may not be able to install an administrator with a global scope access profile.

FortiSandbox

Bug ID	Description
269307	FortiGate devices with a free APT license might incorrectly submit more than 10 files to FortiSandbox prior to FortiSandbox acknowledging receipt of the files.
269830	The UTM log incorrectly reports a file has been sent to FortiSandbox. The *FortiView* > *FortiSandbox* still show files are submitted even after the daily upload quota has been reached.
270091	Some unsupported file types, such as javascript and shell script, are dropped from being scanned by FortiSandbox.
270234	*FortiView* > *FortiSandbox* "status" filter may not work correctly if multiple status results exist.
270403	*FortiView* > *FortiSandbox* drill-down details are not available on certain FortiSandbox detections.
270810	The `execute report sandbox-status` CLI help text is incorrect. The correct help text is the following: • -1 - Unknown • -2 - Pending • 0 - Clean • 1 - Malicious • 2 - Suspicious (High Risk) • 3 - Suspicious (Medium Risk) • 4 - Suspicious (Low Risk)
271906	FortiCloud may send an incorrect value for the analytics statistics.
272687	FortiSandbox statistics and analytics results may not appear once FortiCloud log quota has been reached.
273244	On the FortiGate device in *FortiView* > *FortiSandbox*, the analysis result may show pending and the FortiCloud side may show *unknown*.

FortiSwitch

Bug ID	Description
269213	The FortiGate may be unable to manage duo-uplink FortiSwitch and FortiLink creation.
266078	When all FortiSwitch ports are assigned to a customer-designed VLAN, the `vsw.root` may still be displayed for FortiSwitch-108D and FortiSwitch-224D.
266138	After 8021x client logs out, the FortiSwitch 224D-108D port may still be in the authorized status and still accessible.

Bug ID	Description
269448	After enabling the 1x Security Mode on the `vsw.root` on FortiGate-90D, the tunnel may disconnect.
270940	After you delete an authorized FortiSwitch, you may not be able to find it again.

GUI

Bug ID	Description
267957	The Top Interfering APs chart in the 5G Radio Spectrum Analysis Window may be empty.
268019	The VWL and link-monitor status may not be correctly indicated in the GUI.
268346	All Sessions: filter application, threat, and threat type may not work as expected.
271113	When creating an `id_based policy` with SSL enabled, and the set `gui-multiple-utm disable` is applied, an *Entry not found error message* may appear

HA

Bug ID	Description
276779	Access to `ha-mgmt-interface` can not be controlled via the Allow Access setting in the `ha-mgmt-interface`.

WiFi

Bug ID	Description
267904	If the Client is connecting to SSID with `WPA-Enterprise` and `User-group`, it may not be able to pass the traffic policy.
271246	If the local radio broadcast is on the default VAP interface, and the `override-profile` is enabled on the WiFi-92D, the `wtp-profile` may not work as expected.

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.