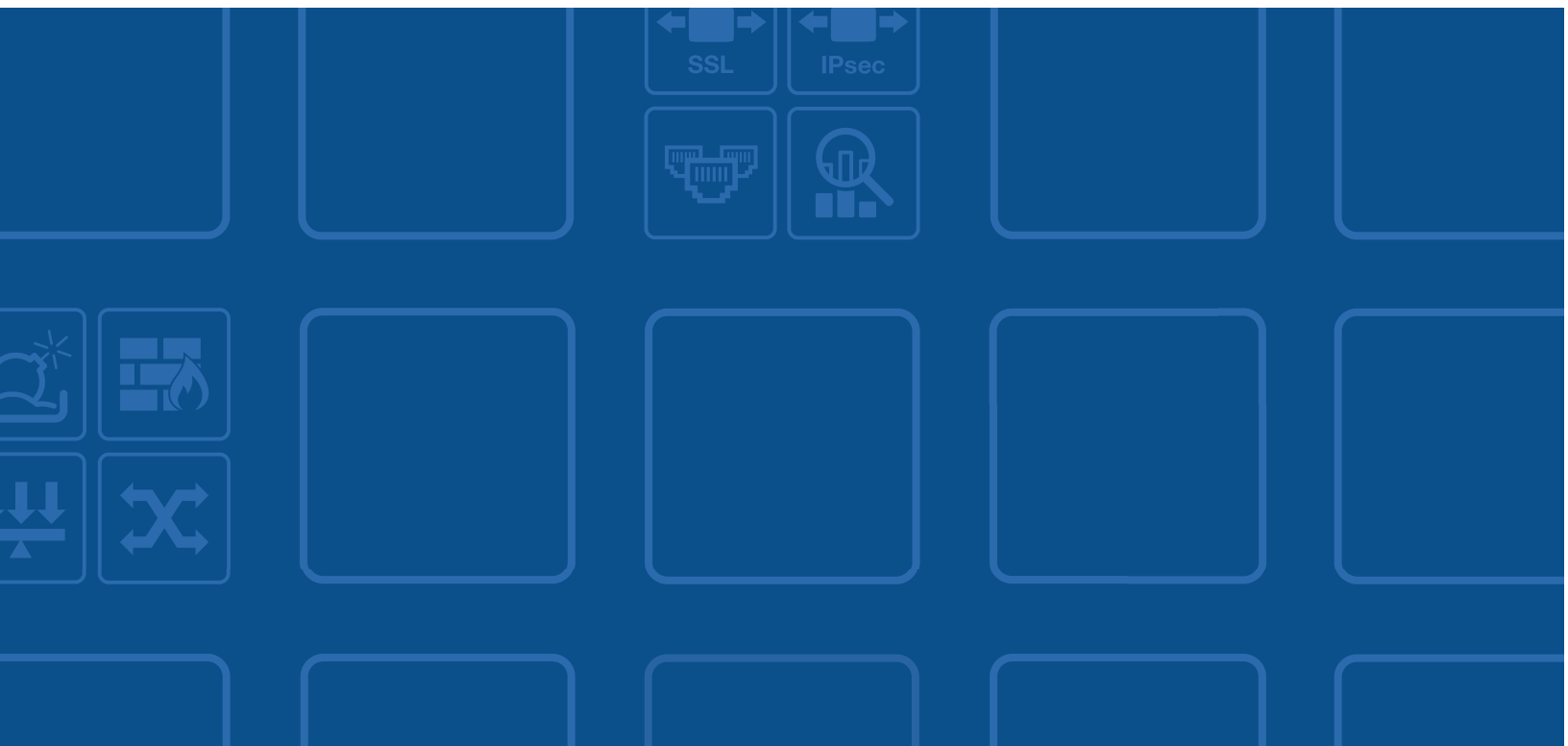
FORTINET
High Performance Network Security

FortiOS - Release Notes

VERSION 5.2.12



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

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

November 10, 2017

FortiOS 5.2.12 Release Notes

01-5212-455615-20171110

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-10-26	Initial release of 5.2.12.
2017-11-03	Added 421739 to *Resolved Issues* > *Common Vulnerabilities and Exposures* and corrected Mantis 440744 to 408239 in the same section.
2017-11-10	Deleted 380974 from *Known Issues* as it's a resolved issue.

Introduction

This document provides the following information for FortiOS 5.2.12 build 0760:

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

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 5.2.12 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-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-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-400D, FG-500D, FG-620B, FG-620B-DC, FG-621B, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-1500DT, FG-3000D, FG-3100D, FG-3040B, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3810D, FG-3815D, FG-3950B, FG-3951B
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-VM64, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN
FortiSwitch	FS-5203B
FortiOS Carrier	FCR-3950B and FCR-5001B FortiOS Carrier 5.2.12 images are delivered upon request and are not available on the customer support firmware download page. FortiOS Carrier firmware image file names begin with *FK*.

The following models are released on a special branch based off of FortiOS 5.2.12. As such, the *System* > *Dashboard* > *Status* page and the output from the `get system status` CLI command displays the build number.

FG-VM64-AWS/AWSONDEMAND	Released on build 9782.
FG-VM64-AZURE	Released on build 6008.
FG-5001B	Released on build 7631.
FG-5001C	Released on build 7631.
FG-5001D	Released on build 7631.
FG-5101C	Released on build 7631.

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 0760.

The FG-60D-3G4G-VZW model uses the FGT_60D_MC-v5-build0760-FORTINET.out image. The FWF-60D-3G4G-VZW model uses the FWF_60D_MC-v5-build0760-FORTINET.out image.

Last Release of Software

Due to the device flash size limitations, the following FortiGate models' last release of software is FortiOS version 5.2.5. These devices have already entered their end-of-life cycle. Further details and exact dates are in Fortinet Customer Support.

Affected Products:

- FortiGate FG-3016B
- FortiGate FG-3810A
- FortiGate FG-5001A SW & DW
- FortiCarrier FK-3810A
- FortiCarrier FK-5001A SW & DW

Special Notices

Local report customization removed

Local report customization has been removed from FortiOS 5.2. You can still record and view local reports, but you can no longer customize their appearance. For more control over customizing local reports, you can use FortiAnalyzer or FortiCloud.

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. We recommend using 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. We recommend using 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

Removed WANOPT, NETSCAN, FEXP features from USB-A

The following features have been removed from the FortiGate and FortiWiFi 80C, 80CM, and 81CM:

- WAN Optimization
- Vulnerability scanning
- Using FortiExplorer on a smartphone to manage the device by connecting to the USB-A port

Router Prefix Sanity Check

Prior to FortiOS 5.2.4 under the config router prefix table, if there are any `le` and `ge` settings that have the same prefix length as the prefix, you may lose the prefix rule after upgrading to FortiOS 5.2.4 or later.

WAN Optimization in FortiOS 5.2.4

In FortiOS 5.2.4:

- If your FortiGate does not have a hard disk, WAN Optimization is not available.
- If your FortiGate has a hard disk, you can configure WAN Optimization from the CLI.
- If your FortiGate has two hard disks, you can configure WAN Optimization from the GUI.

See the FortiOS 5.2.4 Feature Platform Matrix to check the availability for your FortiGate model.

Built-In Certificate

FortiGate and FortiWiFi D-series and above have a built in Fortinet_Factory certificate that uses a 2048-bit certificate with the 14 DH group.

FortiGate-92D High Availability in Interface Mode

The FortiGate-92D may fail to form an HA cluster and experience a spanning tree loop if it is configured with the following:

- operating in interface mode
- at least one of the interfaces, for example *interface9*, is used has the HA heartbeat interface
- a second interface is connected to an external switch

Workaround: use either WAN1 or WAN2 as the HA heartbeat device.

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 SATA disk, log disk is enabled by default.

FortiGate units running 5.2.12

FortiGate units running 5.2.12 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.

For the latest information, see the FortiManager and FortiOS Compatibility.

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
```

SSL VPN 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, see How to purchase and import a signed SSL certificate.

Use of dedicated management interfaces (*mgmt1* and *mgmt2*)

For optimum stability, use management ports (*mgmt1* and *mgmt2*) for management traffic only. Do not use management ports for general user traffic.

Upgrade Information

Upgrading from FortiOS 5.2.10 or 5.2.11

FortiOS version 5.2.12 officially supports upgrading from version 5.2.10 or 5.2.11.

Upgrading from FortiOS 5.0.13 or later

FortiOS version 5.2.12 officially supports upgrading from version 5.0.13 or later.

When upgrading from a firmware version not mentioned in the Release Notes, see the Fortinet Document Library for the recommended upgrade path.

There is a separate version of the guide describing the safest upgrade path to the latest patch of each of the supported versions of the firmware. To upgrade to this build, go to FortiOS 5.2 Supported Upgrade Paths.

Web filter log options change from disabled to enabled after upgrade

After upgrading from FortiOS 5.0.13 or 5.0.14 to FortiOS 5.2.12, all log options for web filter change from disabled to enabled, except the `log-all-url` option.

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 Customer Service & Support. After logging in click *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and click *Get Checksum Code*.

Product Integration and Support

FortiOS 5.2.12 support

The following table lists 5.2.12 product integration and support information:

Web Browsers	• Microsoft Internet Explorer version 11 • Mozilla Firefox version 42 • Google Chrome version 46 • 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	For the latest information, see the FortiManager and FortiOS Compatibility. You should upgrade your FortiManager prior to upgrading the FortiGate.
FortiAnalyzer	For the latest information, see the FortiAnalyzer and FortiOS Compatibility. You should upgrade your FortiAnalyzer prior to upgrading the FortiGate.
FortiClient Microsoft Windows and FortiClient Mac OS X	• 5.4.0 and later • 5.2.5 and later
FortiClient iOS	• 5.4.1 • 5.2.2 and later
FortiClient Android and FortiClient VPN Android	• 5.2.8 • 5.2.7

FortiAP	• 5.2.5 and later • 5.0.10 Before upgrading FortiAP units, verify that you are running the current recommended FortiAP version. To do this in the GUI, go to the *WiFi Controller* > *Managed Access Points* > *Managed FortiAP*. If your FortiAP is not running the recommended version, the *OS Version* column displays the message: *A recommended update is available*.
FortiSwitch OS (FortiLink support)	• 3.4.2 build 0192 Supported models: all FortiSwitch D models.
FortiSwitch-ATCA	• 5.0.3 and later Supported models: FS-5003A, FS-5003B
FortiController	• 5.2.0 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C • 5.0.3 and later Supported model: FCTL-5103B
FortiSandbox	• 2.2.1 • 2.1.0

Fortinet Single Sign-On (FSSO)	• 5.0 build 0264 or later (needed for FSSO agent support OU in group filters)
	  • Windows Server 2008 (32-bit or 64-bit)
	  • Windows Server 2008 R2 64-bit
	  • Windows Server 2012 Standard
	  • Windows Server 2012 R2 Standard
	  • Windows Server 2016 Server Edition
	  • Windows Server 2016 Datacenter
	  • Novell eDirectory 8.8
	• 4.3 build 0164 (contact Support for download)
	  • Windows Server 2003 R2 (32-bit and 64-bit)
	  • Windows Server 2008 (32-bit and 64-bit)
	  • Windows Server 2008 R2 64-bit
	  • Windows Server 2012 Standard Edition
	  • Windows Server 2012 R2
	  • Novell eDirectory 8.8
	FSSO does not currently support IPv6.
	For Windows 10 clients, the FSSO agent forwards the sign-on information to FortiGate.

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	• 3.0.0 build 0069 • 2.0.0 build 0003 and later
AV Engine	• 5.177
IPS Engine	• 3.174
Virtualization Environments	
Citrix	• XenServer version 5.6 Service Pack 2 • XenServer version 6.0 and later
Linux KVM	• RHEL 7.1/Ubuntu 12.04 and later • 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, 5.5 and 6.0

Language support

The following table lists language support information.

Language support

Language	GUI
English	✔
Chinese (Simplified)	✔
Chinese (Traditional)	✔

Language	GUI
French	✔
Japanese	✔
Korean	✔
Portuguese (Brazil)	✔
Spanish (Spain)	✔

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 SP3 (32-bit) Microsoft Windows 7 (32-bit & 64-bit) Microsoft Windows 8 (32-bit & 64-bit) Microsoft Windows 8.1 (32-bit & 64-bit)	2328
Microsoft Windows 10 (64 bit)	2333
Linux CentOS 6.5 (32-bit & 64-bit) Linux Ubuntu 12.0.4 (32-bit & 64-bit)	2334
Virtual Desktop for Microsoft Windows 7 SP1 (32-bit)	2328

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 SP1 (32-bit)	Microsoft Internet Explorer versions 9, 10, and 11 Mozilla Firefox version 33
Microsoft Windows 7 SP1 (64-bit)	Microsoft Internet Explorer versions 9, 10, and 11 Mozilla Firefox version 33
Microsoft Windows 8/8.1 (32bit/64bit)	Microsoft Internet Explorer versions 10 and 11 Mozilla Firefox version 42
Microsoft Windows 10 (64 bit)	Microsoft Internet Explorer version 11 Mozilla Firefox version 52 Google Chrome version 57
Mac OS 10.9	Safari version 7
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 11	✔	✔
Kaspersky Antivirus 2009	✔	
McAfee Security Center 8.1	✔	✔
Trend Micro Internet Security Pro	✔	✔
F-Secure Internet Security 2009	✔	✔

Supported Microsoft Windows 7 32-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	✔	✔
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 5.2.12. For inquires about a particular bug, please contact Customer Service & Support.

Firewall

Bug ID	Description
388040	Creating address object shows errors but still creates the object.

Proxy

Bug ID	Description
445374	`DSCP` field on IP header should be preserved after passing SIP proxy.

Router

Bug ID	Description
368417	FortiOS parse route-map correctly if full configuration is applied.

SSL VPN

Bug ID	Description
380974	Possible root cause of SSL VPN fail on `error:0B080074:...X509_check_private_key:key values mismatch...ApacheSSLSetCertStuff failed`.
412850	SSL VPN Portal redirect not working. Fails with a javascript error.
423452	Citrix XenApp not working properly via SSL VPN Web Portal.

System

Bug ID	Description
437550	System time is not synchronized with NTP Server.
385455	Inconsistent `trustedhost` behavior.

User & Authorization

Bug ID	Description
438758	A CRL update on FortiGate does not trigger an auto-update on FortiManager.
378207	The `authd` process uses high CPU when only RSSO logging is configured.

Common Vulnerabilities and Exposures

Bug ID	Description
409913	FortiOS 5.2.12 is no longer vulnerable to the following CVE References: • 2017-3130 Visit https://fortiguard.com/psirt for more information.
414418	FortiOS 5.2.12 is no longer vulnerable to the following CVE References: • 2017-3131 • 2017-3132 • 2017-3133 Visit https://fortiguard.com/psirt for more information.
421739	FortiOS 5.2.12 is no longer vulnerable to the following CVE References: Visit • 2017-7735 https://fortiguard.com/psirt for more information.
440744	FortiOS 5.2.12 is no longer vulnerable to the following CVE References: • 2017-7739 Visit https://fortiguard.com/psirt for more information.
408239	FortiOS 5.2.12 is no longer vulnerable to the following CVE References: • 2016-5766 • 2016-6132 • 2016-6207 • 2016-6128 • 2016-5767 • 2015-8874 • 2016-9317 • 2016-6912 • 2016-10166 • 2016-10167 • 2016-10168 Visit https://fortiguard.com/psirt for more information.

Bug ID	Description
446892	FortiOS 5.2.12 is no longer vulnerable to the following CVE References: • 2017-13077 • 2017-13078 • 2017-13079 • 2017-13080 • 2017-13081 Visit https://fortiguard.com/psirt for more information.

Known Issues

The following issues have been identified in version 5.2.12. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Anti-spam

Bug ID	Description
374283	Spamfilter does not leave Anti-Spam log for the exempted traffic by bwl matching.

FortiGate 3810D

Bug ID	Description
285429	Traffic may not be able to go through the NPU VDOM link with traffic shaper enabled on FG-3810D TP mode.

FortiGate 3815D

Bug ID	Description
385860	FG-3815D does not support 1GE SFP transceivers.

FortiSandbox

Bug ID	Description
269830	The UTM log may incorrectly report a file that has been sent to FortiSandbox. *FortiView* > *FortiSandbox* may still show files are submitted even after the daily upload quota has been reached.

GUI

Bug ID	Description
215890	Local-category status display may not change after running `unset category-override` in the CLI.
246546	Adding an override application signature may cause all category settings to be lost.
268346	*All sessions: filter application*, *threat*, and *threat type* may not work as expected.

Bug ID	Description
271113	When creating an `id_based policy` with SSL enabled, and the set `gui-multipleutm disable` is applied, an *Entry not found* error message may appear.
278638	Explicit policy may be automatically reset to log security events.
285813	When navigating `FortiView > Application` some security action filters may not work.
286226	Users may not be able to create new address objects from the Firewall Policy.
310930	LDAP browser in `LDAP-group-GUI` may not respect group filter from LDAP server.

System

Bug ID	Description
285520	On NP4 platforms, TCP traffic may not be able to be offloaded in the decryption direction.
285981	Adding more than eight members to `LACP get np6_lacp_add_slave` may result in an error.
302272	Medium type may be shown incorrectly on shared ports.
416005	GUI should not allow read-only admin to back up configuration.

VoIP

Bug ID	Description
272278	SIP calls may be denied when using a combination of `SIP ALG`, `IPS`, and `AppCtrl`.

Webfilter

Bug ID	Description
284661	If the requested URL has port number, the URL filter may not block properly.
378277	YouTube header injection (replacement for YouTube for Schools) was deleted.
380119	Webfilter static URL filter blocks additional domains with similar names.

WiFi

Bug ID	Description
267904	If the client is connecting to an SSID with WPA-Enterprise and User-group, it may not be able to pass the traffic policy.
355335	SSID may stop broadcasting.

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 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 require manual configuration before the first power on process.

Open Source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.

FORTINET

High Performance Network Security