FortiOS v5.2.1
Release Notes

FortiOS v5.2.1 Release Notes

October 27, 2015

01-521-250991-20151027

Fortinet Document Library	docs.fortinet.com
Fortinet Video Libarary	video.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log

Date	Change Description
2014-09-15	Initial release.
2014-09-16	Added FortiManager support information.
2014-09-17	Updated FortiManager support information.
2014-09-19	Removed references to the SSL VPN standalone client for Mac OS X.
2014-09-23	Added 0254898 to Known Issues.
2014-10-14	Corrected Microsoft Hyper-V Server support information.
2014-10-31	Added 0244926 to Known Issues.
2015-02-02	Added FG-3700DX to supported models.
2015-02-03	Added 0251919 to Known Issues.
2015-10-27	Updated Upgrade Information.

Introduction

This document provides the following information for FortiOS v5.2.1 build 0618:

- Supported models
- What's new in FortiOS v5.2.1
- Special Notices
- Upgrade Information
- Product Integration and Support
- Resolved Issues
- Known Issues
- Limitations

See the Fortinet Document Library for FortiOS documentation.

Supported models

FortiOS v5.2.1 supports the following models.

Table 1: Supported 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-POE, FG-70D, FG-80C, FG-80CM, FG-80D, FG-90D, FGT-90D-POE, 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-3950B, FG-3951B, FG-5001A, FG-5001B, FG-5001C, and 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-POE, FWF-80CM, FWF-81CM, FWF-90D, and FWF-90D-POE.
FortiGate Rugged	FGR-100C
FortiGate VM	FG-VM32, FG-VM64, FG-VM64-HV, FG-VM64-KVM, and FG-VM64-XEN.
FortiSwitch	FS-5203B

The following model is supported on a branch based off build 0618:

Table 2: Support model

FortiGate	FG-3700DX	Build 4776

What's new in FortiOS v5.2.1

For a comprehensive list of new features and enhancements that have been made in FortiOS v5.2.1 see the *What's New for FortiOS 5.2* document available in the Fortinet Document Library.

Default configuration changes

- The `set virtual-switch-vlan` CLI command is enabled by default for all FG-100D series and FG-200D series models.
- The maximum number of IPv6 NDP entries has been increased. The kernel holds 65,536 entries.
- Changed the 30D series default UI to the full Web-based Manager.
- Added a default DHCP server for the management port on FG-100D and FG-140D models.
- Bridged the WiFi interface and internal interfaces by default.
- Enabled HA (via CLI) on all 30D series models.
- Increased the `router.policy` value to 512 for all 1U appliances and 2048 for all 2U appliances.
- Renamed *Virtual WAN Link* to *WAN Link Load Balance.*

CLI changes

- Added a CLI command for `arp-max-entry` and `br-fdb-max-entry` in `system global setting`.
- `global antivirus service` settings were moved into `profile-protocol-options` settings.

Endpoint Control

- When the FortiClient license expires it will be marked as expired.
- Added a clear all option in Endpoint Control registration.
- Added SSOMA state into the Endpoint Control protocol.
- The `forticlient-reg-key endpoint` setting now supports up to 128 bytes.

Firewall

- NAT64 UDP TFTP service support.
- Implemented a policy tree in IPv6 to improve the iprope6 checking performance.
- TLS 1.2 support for SSL offload, WAN Optimization, SSL inspection, and SIP SSL.
- The RTA_HA_SES_DURATION information will be included when sending the session to the peer.
- Captive portal support in the block notification page.
- Allow virtual IP with port forwarding enabled to permit ICMP.

HA

- `session-sync-dev` is now used to enhance GTP HA sync.

Log & Report

- Botnet / IP Reputation log updates.

- An event log is generated when the maximum FortiClient license limit is reached during FortiClient registration sync.
- Changed the subtype for routing related logs.
- Cleaned up the `user` and `wireless` event log fields.
- Log ID field update.
- Bandwidth and setup rate statistics are now included in the event log.

System

- Implemented a `diagnose` command to test flash SSD
- Added netflow support for NP6 and XLP
- `execute telnet` now displays a message after disconnecting.

Web-based Manager

- Allow export of collected emails in the *Collected Email Addresses* page.
- Online help improvements
- Added Web-based Manager support for displaying FortiExtender supported 3G/4G modem list.
- FortiView time slice drill down and FortiView unknown application handling improvements
- Rogue AP monitor and SSID list updates
- Interface list update and switch modes
- Configurable syslog server setting in the Web-based Manager for FG-3600C, FG-3950B, and FG-3700D.
- Added a half duplex indication to interface panel
- Added a reset password link to the FortiCare login dialog
- Added a wizard summary, client instructions, and FortiCloud information
- Export collected emails in `.csv` format
- FortiCloud wizard activation for the following models: FG-30D, FG-30D-POE, FWF-30D, FWF-30D-POE, FG-60D, FG-60D-POE, FWF-60D, FWF-60D-POE, FG-70D, FG-80D, FG-90D, FG-90D-POE, FWF-90D, FWF-90D-POE
- LDAP tree browse interface and user group dialog improvements
- New LDAP tree browser design in the *User Wizard* and *User Group* pages
- Added column settings.

Web Filter

- Improved URL filter list usability by using dialog to create and edit. Introduced paging and search to the table.

WiFi

- Ekahau Blink protocol support and re-organization for `station-locate`
- Suppress probe responses based on the threshold value.

Special Notices

FortiCarrier

FortiCarrier images are delivered upon request and are not available in the Customer Service & Support firmware download page.

Before any firmware upgrade

To minimize network interruptions, plan the upgrade during a maintenance window. This allows you to properly upgrade, test, and implement the firmware upgrade without disrupting network traffic.

Save a copy of your FortiGate configuration prior to upgrading. To backup your FortiGate configuration, go to *System* > *Dashboard* > *Status*. In the *System Information* widget select *Backup* under *System Configuration* and save the configuration file to your local hard drive.

After any firmware upgrade

If you are using the FortiGate Web-based Manager, after a firmware upgrade, clear your browser cache prior to logging in to ensure the GUI is displayed properly.

The AV and IPS engines and definitions included with a firmware upgrade may be older than ones currently available from FortiGuard. You should update the AV and IPS engines and definitions right after a firmware upgrade by going to *System* > *Config* > *FortiGuard,* selecting the blue triangle next to *AV & IPS Download Options* and selecting the *Update Now* button.

Upgrade Information

Upgrading from FortiOS v5.2.0

FortiOS v5.2.1 officially supports upgrade from v5.2.0.

Upgrading from FortiOS 5.0.6 or later

FortiOS v5.2.1 officially supports upgrade from v5.0.6 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 FortiOS 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 VM environments:

Citrix XenServer and Open Source Xen

- `.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 Xen.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the Citrix Xen 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. To verify the integrity of the download, select the *Checksum* link next to the *HTTPS* download link. A dialog box will be displayed with the image file name and checksum code. Compare this checksum with the checksum of the firmware image.

Product Integration and Support

FortiOS v5.2.1 support

The following table lists FortiOS v5.2.1 product integration and support information.

Table 3: FortiOS v5.2.1 support information

Web Browsers	• Microsoft Internet Explorer version 11 • Mozilla Firefox version 30 • Google Chrome version 36 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	• v5.0.7 and later • v5.2.0 and later You should upgrade your FortiManager prior to upgrading the FortiGate.
FortiAnalyzer	• v5.0.7 and later • v5.2.0 and later You should upgrade your FortiAnalyzer prior to upgrading the FortiGate.
FortiClient Microsoft Windows and FortiClient Mac OS X	• v5.2.1
FortiClient iOS	• v5.2.0
FortiClient Android and FortiClient VPN Android	• v5.2.3

Table 3: FortiOS v5.2.1 support information (continued)

FortiAP	• v5.2.1 • v5.0.8 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 Web-based Manager. 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	• v2.0.3 Supported models: FS-28C, FS-324B-POE, FS-348B, and FS-448B
FortiSwitch ATCA	• v5.0.3 Supported models: FS-5003A and FS-5003B
FortiController	• v5.0.3 Supported model: FCTL-5103B
FortiSandbox	• v1.4.0 and later • v1.3.0
Fortinet Single Sign-On (FSSO)	• v4.3 build 0159 The following operating systems are supported: • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 Standard Edition • Microsoft Windows Server 2008 R2 64-bit • Microsoft Windows Server 2008 (32-bit and 64-bit) • Microsoft Windows Server 2003 R2 (32-bit and 64-bit) • Novell eDirectory 8.8 FSSO does not currently support IPv6.
FortiExplorer	• v2.4 build 1075 and later.
FortiExplorer iOS	• v1.0.4 build 0126 and later
FortiExtender	• v1.0.0 build 0024 Supported models: FEX-20B, FEX-100A, and FEX-100B
AV Engine	• v5.156
IPS Engine	• v3.051
Virtualization Environments	

Table 3: FortiOS v5.2.1 support information (continued)

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 • Hyper-V Server 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 FortiOS language support information.

Table 4: FortiOS language support

Language	Web-based Manager	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 v5.2.1 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.

Table 5: Supported modules and FortiGate models

AMC/FMC/FSM/RTM 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: 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

Table 5: Supported modules and FortiGate models (continued)

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: 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.

Table 6: Operating system and installers

Operating System	Installer
Microsoft Windows 8.1 (32-bit & 64-bit) Microsoft Windows 8 (32-bit & 64-bit) Microsoft Windows 7 (32-bit & 64-bit) Microsoft Windows XP Service Pack 3(32-bit)	2304
Linux CentOS 6.5 (32-bit & 64-bit) Linux Ubuntu 12.0.4 (32-bit & 64-bit)	2304
Virtual Desktop for Microsoft Windows 7 Service Pack 1 (32-bit)	2304

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.

Table 7: 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 31
Microsoft Windows 7 64-bit SP1	Microsoft Internet Explorer versions 9, 10, and 11 Mozilla Firefox version 31
Linux CentOS version 5.6	Mozilla Firefox version 5.6
Linux Ubuntu version 12.0.4	Mozilla Firefox version 5.6
Mac OS X v10.9 Mavericks	Apple Safari version 7

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.

Table 8: Supported 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	✔	✔

Table 9: Supported 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	✔	✔
Norton™ Internet Security 2011	✔	✔

Table 9: Supported Windows 7 32-bit and 64-bit antivirus and firewall software (continued)

Product	Antivirus	Firewall
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 FortiOS v5.2.1. For inquires about a particular bug, please contact Customer Service & Support.

Data Leak Prevention

Table 10: Data Leak Prevention

Bug ID	Description
0240623	DLP filters can be either a file or message type. And FortiGate decides whether the received data should treated as file or message and applies the corresponding filters. To avoid these issues, all received packets are treated the same as files and are submitted to the AV engine as required. If the file type cannot be detected by the AV engine, packets are checked against the DLP message filters.
0244347	Handle tabs in headers in the MIME parser to properly extract and display attribute values in the Web-based Manager.

Endpoint Control

Table 11: Endpoint Control

Bug ID	Description
0250451	FortiClient does not get VPN settings via Endpoint Control if a special character is entered in PSK.

Firewall

Table 12: Firewall

Bug ID	Description
0217481	SSL inspection stops some applications from running.
0217637	STP forwarding problem in one-arm transparent mode firewall configuration. Added an STP forwarding option in the CLI.
0230181	The `proxyworker` process closes the field descriptor but does not remove it from the `epoll` process. As a result in will crash in `epoll` because the corresponding connection structure has already been released.
0242957	DCE-RPC session helper should open expectations and negotiated high ports should be allowed by FortiGate.
0244393	Device based policies do not work after a reboot when source is VLAN interface.
0244552	Some traffic may pass through a higher firewall policy and matches with a lower policy.

Table 12: Firewall (continued)

Bug ID	Description
0245121	sFlow stops sending raw packet samples.
0245748	SCTP multihome INIT or INIT_ACK packets matching expectation sessions do not get NAT'ed.
0247568	A RADIUS accounting stop message is sent for users when the FSSO CA connection is established.
0247954	The `ftpd` daemon hangs in BUFFER_DOWNLOAD_STATE.
0248396	All policies are grouped in a long list so that lookup takes long time and consumes CPU.

FortiGate VM

Table 13: FortiGate VM

Bug ID	Description
0244695	RDP sessions between the windows VM in the same VM host fails with data encryption error. Enabled the large receive offload (LRO) feature in the VMXNET3 driver.
0250054	When the license status cannot be validated for more than 4 hours or it changes, FortiGate VM should create an event log entry.

High Availability

Table 14: High Availability

Bug ID	Description
0214401	An administrative user on a remote authentication server cannot login via the HA management interface.
0233107	In active-active clusters, the load balancing session from FortiGate to the backend server is not load balanced to the slave.
0246480	Directly connected routes are lost after port based allocation and/or Sflow is enabled on the FG-1500D.
0247563	A non-admin account is unable to connect to the `ha-mgmt-interface`, after reboot.
0250721	The slave times out when receiving the master configuration if the master has hundreds of VDOMs.

IPS

Table 15: IPS

Bug ID	Description
0211967	Beta signatures are created by IPS analysts to test false positives and are reported to FDS statistics only. These should not be displayed in the Web-based Manager or system statistics.
0229356	IPS does detect intrusions after upgrade.
0236752, 0247149	Changed IPS signature categorization.
0250112	Support certificate chaining in the server certificate payload.

IPsec VPN

Table 16: IPsec VPN

Bug ID	Description
0235304	IPsec over PPPoE (policy based IPsec) does not work since the DHCP packet did not go through the tunnel as an encrypted packet. Instead DHCP packets are broadcast as an unencrypted packet.
0244227	IPsec is sending too many dead peer detection probes.
0246085	`iked` daemon crashes when using Xauth with FortiToken.
0248916	Since the upgrade to v5.2.0 (from v5.0.7), PKI authentication in firewall policies is no longer working. When attempting authentication with a client certificate, the regular authentication prompt is returned.

IPv6

Table 17: IPv6

Bug ID	Description
0249361	IPv6 via PPPoE does not correctly use the default route learned from RA.

Log & Report

Table 18: Log & Report

Bug ID	Description
0241932	Missing important statistics in the performance statistics log.
0243465	Every `miglogd` process requests disk usage from FortiAnalyzer every 5 seconds.
0245480	Admin update log message cleanup.
0247483	Logs are not sent to FortiCloud on a FortiGate unit without a hard drive.

Table 18: Log & Report (continued)

Bug ID	Description
0248692	The `config log fortianalyzer override-setting` CLI command does not accept IP addresses from a FortiAnalyzer configured in global context.
0251714	The user event log action does not show the authentication method with explicit proxy.

Routing

Table 19: Routing

Bug ID	Description
0226987	FortiGate sends OSPF Hello packets with the VRRP IP address.
0250264	Probing to ping server does not restart if the interface is brought down and up administratively.

Spam Filter

Table 20: Spam Filter

Bug ID	Description
0246154	Improved the antispam speed when anti-phishing is enabled.

SSL VPN

Table 21: SSL VPN

Bug ID	Description
0223176	The internal IP address issued to the SSL VPN tunnel is not sent in the RADIUS accounting message.
0229880	SSL VPN web mode does not work with Nexpose application.
0234991	SSL VPN web mode navigation buttons for a specific web page do not work.
0243959	The `SVPNCOOKIE` does not follow the RFC6265 recommendation. There should be a space after each key/value pair and attribute.
0244967	Users should not need to enter the token twice for two-factor SMS authentication when the Windows RADIUS server is used.
0248425	Improper display of a webpage accessed through the bookmark in web mode.
0249074	FortiGate should recognize all groups for SSL VPN.

System

Table 22: System

Bug ID	Description
0161876, 0240650	Fixed the power supply unit alerting logic.
0228156	Adding overlapping `iplists` (VIP/ippool) fails without any error messages.
0235714	A sniffer policy on the DMZ port does not work in some configurations.
0237740	SP buffer leak for IPS traffic when sessions are synced.
0242454	Autoupdate tunnelling does not work after upgrade.
0244981	Backing up the FortiGate configuration file using a remote admin user (RADIUS, TACACS+) results in a small truncated file.
0246371	The DHCP server will not put the updated lease time in its `ACK` to client's renew request.
0246489	Unable to configure policy based VPNs when the virtual WAN link is configured.
0246884	The `get system source-ip status` CLI command does not show all `source-ip`.
0247258	SSH RSA fingerprint not calculated correctly from the actual used key.
0247260	The recovery of a fail-detect interface should move both interfaces up.
0247272	DHCP relay configuration is lost after reboot when an IP address is assigned to inter VDOM links.
0247718	The IP GEO database is not updated via FDS schedule update feature.
0247826	Increased the scheduled timeout to avoid random CPU15 peaks.
0248333	Unable to authenticate a VDOM admin using a RADIUS wildcard account.
0248460	Cloning an application control profile produces memory corruption errors.
0250813	There is no log entry for DHCP block events when it is not possible to determine which MAC address is blocked.

Upgrade

Table 23: Upgrade

Bug ID	Description
0250120	SCP configuration backup with RSA key authentication retrieves only the root VDOM configuration after upgrading from v5.0 to v5.2.0.
0250678	One of the SSIDs no longer broadcasts after upgrading to v5.2

WAN Optimization and Web Proxy

Table 24: WAN Optimization and Web Proxy

Bug ID	Description
0244856	FortiGate may generate a HTTP 502 response if it detects the HTTP server does not behave normally as per the HTTP RFC.
0246339	When using explicit proxy, web pages should load the same as when not using the proxy.
0246497	Parsing errors with some MAPI ROP commands.
0248416	HTTP POST request will get stuck on NTLM authentication if multipart content-type header is present.
0251178	Vimeo video is not cached as expected.

Web-based Manager

Table 25: Web-based Manager

Bug ID	Description
0197598	The interface status tooltip for port1-8 in the *Unit Operation* widget is not displayed.
0219095	All VDOM interfaces are displayed if a *CLI Console* in the Web-based Manager is detached.
0225780	Events are logged with the incorrect user when making changes in jsconsole with a wildcard user.
0230692	An internal server error message is generated when filtering logs with more than 10 source IP addresses.
0239368	An internal server error message is generated after log in.
0244219	The SNMP community setting is removed when confirmed in the Web-based Manager.
0245722	Updated the disk management *Format* button to *Format Disk*.
0246743	The VIP object is not displayed in the Web-based Manager when creating a firewall policy.
0247321	The *WAN Opt. & Cache* menu is displayed when the feature is disabled.
0247477	Added a checkbox to hide the source port selection by default when creating new service.
0249007	Interface aliases not displayed in global view.
0249023	An internal server error message is generated when editing a Korean language address, address group, or policy name.
0250042	VIP address load-balance type not visible in the Web-based Manager.

Table 25: Web-based Manager (continued)

Bug ID	Description
0250100	Unable to load an application control list in the Web-based Manger if the same application is specified in more than one filter.
0250556	When creating new custom service, the low source port initial value is incorrect.

Web Filter

Table 26: Web Filter

Bug ID	Description
0244839	The `set ovrd-auth-port-warning` CLI command does not allow ports above 32767.
0249622	The load time of a URL filter list with 50,000 entries should be shorter.
0249899	The RSSO user name length shows only 31 characters in the web filter log.

Wireless

Table 27: Wireless

Bug ID	Description
0155391	Memory leak observed between the `cmdbsvr` process and the wireless controller during associations.
0249045	Cannot forward multicast traffic when DTLS encryption is enabled for CAPWAP.

Known Issues

The following issues have been identified in FortiOS v5.2.1. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Endpoint Control

Table 28: Endpoint control

Bug ID	Description
0248014	FortiGate and FortiClient have a discrepancy in displaying their On-Net/Off-Net status.

Firewall

Table 29: Firewall

Bug ID	Description
0253505	Changing the `dedicated-management-cpu` configuration may cause an unstable state. Workaround: Reboot the device after changing the CPU configuration. Affected model: FG-3700D
0253592	Firewall may ignore the deny policy rule when used with an authentication portal.
0254210	Failed to block an EICAR sample on SMB 1.0 and 2.0 protocol when nturbo is enabled.

IPsec VPN

Table 30: IPsec VPN

Bug ID	Description
0253651	FortiClient may encounter an IPsec traffic issue with a FortiGate that has NP6 NPU offload enabled.
0254898	An IPsec tunnel interface may not come up after the FortiGate unit reboots if the tunnel is using DHCP mode. Workaround options: • Option 1. After rebooting the FortiGate, manually restart the IPsec daemon with the following CLI command, `diag sys kill 11 <ipsec pid>` • Option 2. Change the IPsec tunnel interface mode from DHCP to static.

SSL VPN

Table 31: SSL VPN

Bug ID	Description
0244926	Unable to launch the Linux SSL VPN standalone client in Centos v5.6 due to a GLIBC error.

System

Table 32: System

Bug ID	Description
0241646	Traffic may not go through VLAN interfaces based on LAG in transparent VDOMs. Workaround: After finish the configuration, perform a reboot operation.
0246126	IPv4 multicast traffic over an IPsec interface cannot be offloaded to NP6.
0246224	SCTP traffic cannot be offloaded on NP6.
0250534	Adding or unsetting a member of an aggregation interface can cause the peer switch's interface to be down.
0251221	The hardware switch span port does not work on FG-200D-POE and FG-240D-POE models.
0251919	Enable `block-notification` by default for firewall policy.
0252947	With a FortiGate previously registered to both FortiManager and FortiCloud, it will still send management traffic to FortiManager even after it is unregistered from the FortiManager. Workaround: Log out and reactivate the FortiCloud account on the FortiGate after unregistering from FortiManager.
0253641	The `inbandwidth` limit does not work on NP6 interfaces.

Upgrade

Table 33: Upgrade

Bug ID	Description
0251511	Upgrades to v5.2.1 will encounter a configuration error with the antivirus service and HTTPS/FTPS/POP3S/IMAPS/SMTPS protocols because such configurations do not exist in `profile-protocol-options`.

Web-based Manager

Table 34: Web-based Manager

Bug ID	Description
0253573	Unable to properly create a new remote user group using the local user creation wizard due to a missing *OK* button.
0254300	The FortiSwitch 5203B label is FortiGate 5203B in the main header.
0254301	The FortiGateRugged 100C label is FortiGate 100C in the main header.

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, Xen version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.