FortiOS Release Notes

VERSION 5.0.10

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

November 04, 2015

FortiOS 5.0.10 Release Notes

01-5010-262521-20151104

TABLE OF CONTENTS

Change Log

Date	Change Description
2014-12-16	Initial release.
2014-12-18	Minor document update.
2014-12-19	Added FortiSwitch-ATCA version 5.2.0 support information,
2014-12-23	Minor document update.
2015-01-06	Added FG-92D, FWF-92D, FGR-90D, FG-98D-POE, FG-VM64-AWS, and FG-VM64-AWSONDEMAND to supported models.
2015-01-07	Corrected the SSL VPN standalone client installer version.
2015-01-09	Added known issues.
2015-01-14	Added FG-1000D and FG-1200D to supported models.
2015-11-04	Added FK-5001B to Supported Models.

Introduction

This document provides the following information for FortiOS 5.0.10 build 0305:

See the Fortinet Document Library for FortiOS documentation.

Supported models

FortiOS 5.0.10 supports the following models:

FortiGate	FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-POE, FG-70D, FG-80C, FG-80CM, FG-80D, FG-90D, FGT-90D-POE, 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-240D, 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-1200D, 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, 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, FWF-90D-POE
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, FCR-5001B, and FK-5001B FortiOS Carrier 5.0.10 images are delivered upon request and are not available on the customer support firmware download page.

The following models are supported on branches based off build 0305:

FG-92D	The FortiGate 92D is released on build number 4726.
FWF-92D	The FortiWiFi 92D is released on build number 4726.
FGR-90D	The FortiGate Rugged 90D is released on build number 4724.
FG-98D-POE	The FortiGate 98D-PoE is released on build number 4730.
FG-1000D	The FortiGate 1000D is released on build number 4755.
FG-1200D	The FortiGate 1200D is released on build number 4754.
FG-VM64-AWS	The FortiGate VM for Amazon AWS is released on build number 8167.
FG-VM64-AWSONDEMAND	The FortiGate VM for Amazon AWS On Demand is released on build number 8167.

What's new in FortiOS 5.0.10

For a list of new features and enhancements that have been made in FortiOS 5.0.10 see the *What's New for FortiOS 5.0* document available in the Fortinet Document Library.

- Added support for 32,000 plus FortiClient configuration distribution through Endpoint Control Network Access Control.
- ZTE MF667 modem support
- Enable dedicated management CPU for FG-1000D/FG-1500D/FG-3700D
- Enable FortiClient license for FG-3040B
- TLS support for explicit proxy
- New model support: FG-92D, FWF-92D, FGR-90D, FG-98D-POE, FG-VM64-AWS, FG-VM64-AWSONDEMAND

Special Notices

Default log setting change

For FortiGate 5000 series blades and 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.

FG-300D and FG-500D nTurbo support

The FG-300D and FG-500D do not support nTurbo for IPS acceleration. The option for this feature has been disabled by default. Enabling it may result in a performance degradation. The CLI commands are shown below.

```
config ips global
   set np-accel-mode {basic | none}
end
```

If `np-accel-mode` is set to `none`, then nTurbo IPS acceleration is disabled.

FG-3600C hardware compatibility

FortiOS version 5.0.6 contains a compatibility issue with certain FG-3600C units. Units that are affected have a system part number of P12090-03 and later. You can view the system part number on the bottom of the unit or from the get system status CLI command.

FG-3600C units with part number P12090-03 and later must run FortiOS version 5.0.6 or later and cannot be downgraded to FortiOS version 5.0.5 or earlier.

SCTP firewall support

LTE networks require support for the SCTP protocol to transfer control plane data between evolved NodeBs (eNBs) and the Mobility Management Entity (MME), as well as between the MME and the Home Subscriber Server (HSS). SCTP firewall support is included in FortiOS version 5.0 and FortiOS Carrier version 5.0. SCTP traffic is accepted by FortiOS and FortiOS Carrier and you can create SCTP services and security policies that use these services. All other security features can also be added as required to security policies for SCTP services.

New FortiOS Carrier features

Changes to licensing

Prior to FortiOS version 5.0, only FortiCarrier-specific hardware could run FortiOS Carrier version 4.0. Starting with FortiOS version 5.0.2, the FortiOS Carrier Upgrade License can be applied to selected FortiGate models to activate FortiOS Carrier features. There is no support for FortiOS Carrier features in FortiOS versions 5.0.0 and 5.0.1.

At this time the FortiOS Carrier Upgrade License is supported by FortiGate models FG-3240C, FG-3950B, FG-5001B, FG-5001C, and FG-5101C. Future 3000 and 5000 series models are also expected to support FortiOS Carrier.

You can obtain a FortiOS Carrier license from your Fortinet distributor. On a FortiGate model that supports FortiOS Carrier and that is running FortiOS version 5.0.2 or later you can use the following command to activate FortiOS Carrier features:

```
execute forticarrier-license <license-key>
```

The license key is case-sensitive and includes dashes. When you enter this command, FortiOS attempts to verify the license with the FortiGuard network. Once the license is verified the FortiGate unit reboots. When it restarts it will be running FortiOS Carrier with a factory default configuration.

You can also request that Fortinet apply the FortiOS Carrier Upgrade license prior to shipping a new unit, as part of Professional Services. The new unit will arrive with the applied license included.

Licensing and RMAs

When you RMA a FortiGate unit that is licensed for FortiOS Carrier, make sure that the FortiCare support representative handling the RMA knows about the FortiOS Carrier license. This way a new FortiOS Carrier license will be provided with the replacement unit.

Licensing and firmware upgrades, downgrades and resetting to factory defaults

After a firmware upgrade from FortiOS version 5.0.2 or later you should not have to re-apply the FortiOS Carrier license. However, the FortiOS Carrier license may be lost after a firmware downgrade or after resetting to factory defaults. If this happens, use the same command to re-apply the FortiOS Carrier license. FortiGuard will re-verify the license key and re-validate the license.

Upgrading older FortiCarrier specific hardware

Previous versions of FortiOS Carrier run on FortiCarrier specific hardware. This includes FCR-3810A, FCR-3950B, FCR-5001A-DW, and FCR-5001B.

As long as the FortiCarrier hardware can be upgraded to FortiOS version 5.0.2 or later, it can be upgraded to FortiOS Carrier version 5.0.2 or later without purchasing a new FortiOS Carrier Upgrade License. You must use FortiCarrier firmware to upgrade this hardware and this firmware may not be available from the Fortinet Support Site. Please work with your Fortinet representative to ensure a smooth upgrade of these FortiCarrier models.

Changes to GPRS Tunneling Protocol (GTP) support

FortiOS Carrier version 5.0 supports GTP-C v2, which is the control plane messaging protocol used over 4G-LTE 3GPP R8 software interfaces, as well as between LTE networks and older 2G/3G networks with general packet radio service (GPRS) cores.

Changes to MMS scanning

MMS scanning now includes data leak prevention (DLP) to detect fingerprinted and/or watermarked files transferred via MMS, as well as data pattern matching for data such as credit cards and social security numbers.

Using wildcard characters when filtering log messages

While using filtering in the log message viewer you may need to add * wildcard characters to get the search results that you expect. For example, if you go to *Log & Report* > *Event Log* > *System* to view all messages with the word “logged” in them you can select the Filter icon for the *Message* list and enter the following:

logged

Including both * wildcard characters will find all messages with “logged” in them. “logged” can be at the start or the end of the message or inside the message.

If you only want to find messages that begin with the search term you should remove the leading *. If you only want to find messages that end with the search term you need to remove the trailing *.

It does not work to add a * wildcard character inside the search term. So searching for *lo*ed* will not return any results.

IPS algorithms

For optimal performance on your FortiGate unit, the IPS algorithm can be configured via the CLI. Select one of the following modes:

- engine-pick: The IPS engine picks the best algorithm to use.
- high: This algorithm fits most FortiGate models
- low: This algorithm works best on FortiGate units with less memory (512MB or less)
- super: This algorithm works best on FortiGate models with more memory (more than 4GB)

To configure the algorithm, use the following CLI commands:

```
config ips global
   set algorithm [engine-pick | high | low | super]
end
```

Disk logging disabled by default on some models

For the following FortiGate and FortiWiFi models, disk logging is disabled by default and Fortinet recommends logging to FortiCloud instead of logging to disk:

FortiGate	FG-20C, FG-20C-ADSL-A, FG-40C, FG-60C, FG-60C-POE, FG-60D, FG-60D-POE, FG-80C, FG-80CM, FG-100D (PN: P09340-04 or earlier), FG-300C (PN: P09616-04 or earlier), FG-200B, FG-200B-POE (if flash is used as storage)
FortiWiFi	FWF-20C, FWF-20C-ADSL-A, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60DM, FWF-60DX-ADSL-A, FWF-80C, FWF-80CM,

If you were logging to FortiCloud prior to upgrading to FortiOS version 5.0.10, the settings are retained and logging to FortiCloud continues to operate normally. If you were logging to disk prior to upgrading, logging to disk may be disabled during the upgrade process.

If required, you can enable disk logging from the CLI using the following command:

```
config log disk setting
   set status enable
end
```

If you enable disk logging on the models listed above, the CLI displays a message reminding you that enabling disk logging impacts overall performance and reduces the lifetime of the unit.

A code limitation specific to the FG-80C, FG-80CM, FWF-80C, and FWF-80CM models prevents the warning message from being displayed.

FG-60D/FWF-60D logging to disk

If you enable logging to disk for FG-60D and FWF-60D models, Fortinet recommends that you format the log disk using the following CLI command:

```
execute formatlogdisk
Log disk is /dev/sda1.
Formatting this storage will erase all data on it, including logs, quarantine files;
    WanOpt caches; and require the unit to reboot.
Do you want to continue? (y/n) [Enter y to continue]
```

WAN Optimization

In FortiOS version 5.0, WAN Optimization is enabled in security policies and WAN Optimization rules are no longer required. Instead of adding a security policy that accepts traffic to be optimized and then creating WAN Optimization rules to apply WAN Optimization, in FortiOS version 5.0 you create security policies that accept traffic to be optimized and enable WAN Optimization in those policies. WAN Optimization is applied by WAN Optimization profiles which are created separately and added to WAN Optimization security policies.

MAC address filter list

The `mac-filter` CLI command under the `config wireless-controller vap` setting is not retained after upgrading to FortiOS version 5.0.10. It is migrated into both `config user device` and `config user device-access-list setting`.

Spam filter profile

The spam filter profile has been changed in FortiOS version 5.0.10. The `spam-emaddr-table` and `spam-ipbwl-table` have been merged into the `spam-bwl-table`. The `spam-bwl-table` exists in the spam filter profile.

Spam filter black/white list

The `config spamfilter emailbwl` and `config spamfilter ipbwl` commands are combined into `config spamfilter bwl`.

DLP rule settings

The `config dlp rule` command is removed in FortiOS version 5.0.10. The DLP rule settings have been moved inside the DLP sensor.

Limiting access for unauthenticated users

When configuring User Identity policies, if you select the option *Skip this policy for unauthenticated user* the policy will only apply to users who have already authenticated with the FortiGate unit. This feature is intended for networks with two kinds of users:

Single sign-on users who have authenticated when their devices connected to their network

Other users who do not authenticate with the network so are “unauthenticated”

Sessions from authenticated users can match this policy and sessions from unauthenticated users will skip this policy and potentially be matched with policies further down the policy list. Typically, you would arrange a policy with *Skip this policy for unauthenticated user* at the top of a policy list.

You can also use the following CLI command to enable skipping policies for unauthenticated users:

```
config firewall policy
   edit <id>
      set identity-based enable
      set fall-through-unauthenticated enable
      next
   end
```

Use case - allowing limited access for unauthenticated users

Consider an office with open use PCs in common areas. Staff and customers do not have to log in to these PCs and can use them for limited access to the Internet. From their desks, employees of this office log into PCs which are logged into the office network. The FortiGate unit on the office network uses single sign-on to get user credentials from the network authentication server.

The open use PCs have limited access to the Internet. Employee PCs can access internal resources and have unlimited access to the Internet.

To support these different levels of access you can add a user identity policy to the top of the policy list that allows authenticated users to access internal resources and to have unlimited access to the Internet. In this policy, select *Skip this policy for unauthenticated user*.

Add a normal firewall policy below this policy that allows limited access to the Internet.

Sessions from authenticated PCs will be accepted by the User Identity policy. Sessions from unauthenticated PCs will skip the User Identity policy and be accepted by the normal firewall policy.

Use case - multiple levels of authentication

As a variation of the above use case, Policy 2 could be a User Identity policy and *Skip this policy for unauthenticated user* would not be selected. Sessions from unauthenticated users that are accepted by Policy2 would now require users to authenticate before traffic can connect through the FortiGate unit. The result is different levels of authentication: Single sign on for some users and firewall authentication for others.

FG-100D upgrade and downgrade limitations

The following limitations affect the FG-100D model when upgrading from FortiOS version 4.3 to FortiOS version 5.0.0 or later.

32-bit to 64-bit version of FortiOS

With the release of FortiOS version 5.0.0 or later, the FG-100D will run a 64-bit version of FortiOS. This has introduced certain limitations on upgrading firmware in a high availability (HA) environment and downgrading.

When performing an upgrade from a 32-bit FortiOS version to a 64-bit FortiOS version and the FG-100Ds are running in a HA environment with the uninterruptable-upgrade option enabled, the upgrade process may fail on the primary device after the subordinate devices have been successfully upgraded. To work around this situation, users may disable the uninterruptable-upgrade option to allow all HA members to be successfully upgraded. Without the uninterruptable-upgrade feature enabled, several minutes of service unavailability are to be expected.

Downgrading a FG-100D from FortiOS version 5.0.0 or later is not supported due to technical limitations between 64-bit and 32-bit versions of FortiOS. The only procedure to downgrade firmware is by using the TFTP server and BIOS menu to perform the downgrade. In this case the configuration will need to be restored from a previously backed up version.

Internal interface name/type change

In FortiOS version 5.0.0 or later the internal interface has been renamed `lan` and the type of the interface has changed to `hard-switch`. In order to create an HA cluster between a FG-100D shipped with FortiOS version 5.0.0 or later with a FG-100D upgraded from FortiOS version 4.3, you must first remove the `lan` interface and re-generate the `internal` interface to match the interface on the upgraded device.

Use the following CLI commands to remove the `lan` interface and re-generate the `internal` interface.

```
# config firewall policy
(policy) # purge
   This operation will clear all table!
   Do you want to continue? (y/n)y
(policy) # end

# config system dhcp server
(server) # purge
   This operation will clear all table!
   Do you want to continue? (y/n)y
(server) # end

# config system virtual-switch
(virtual-switch) # purge
   This operation will clear all table!
   Do you want to continue? (y/n)y
(virtual-switch) # end

# config system global
(global) # set internal-switch-mode switch
(global) # end
   Changing switch mode will reboot the system!
   Do you want to continue? (y/n)y
```

FG-100D hardware compatibility

FortiOS versions 5.0.0 to 5.0.7, inclusive contains a compatibility issue with FG-100D units that have a system part number of P11510-04 and later. You can view the system part number on the bottom of the unit or with the get system status CLI command. Units with this system part number must run FortiOS version 5.0.8 or later.

Product Integration and Support

FortiOS 5.0.10 support

The following table lists 5.0.10 product integration and support information.

Web Browsers	• Microsoft Internet Explorer version 11 • Mozilla Firefox version 34 • Google Chrome version 39 • 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	• 5.0.7 and later • 5.2.0 and later You should upgrade your FortiManager prior to upgrading the FortiGate.
FortiAnalyzer	• 5.0.7 and later • 5.2.0 and later You should upgrade your FortiAnalyzer prior to upgrading the FortiGate.
FortiClient Microsoft Windows and FortiClient Mac OS X	• 5.0.9 and later
FortiClient iOS	• 5.0.2
FortiClient Android and FortiClient VPN Android	• 5.0.3

FortiAP	• 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 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 (FortiLink support)	• 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	• 5.0.3 and later Supported model: FCTL-5103B • 5.2.0 Supported models: FTCL-5103B, FTCL-5903C, FTCL-5913C
Fortinet Single Sign-On (FSSO)	• 4.3 build 0161 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	• 2.3 build 1052 and later. Some FortiGate models may be supported on specific FortiExplorer versions.
FortiExplorer iOS	• 1.0.4 build 0118 and later Some FortiGate models may be supported on specific FortiExplorer iOS versions.
AV Engine	• 5.159
IPS Engine	• 2.196
Virtualization Environments	
Amazon	• Amazon Web Services AMI (Amazon EC2, Amazon EBS)

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

Always review the Release Notes of the supported platform firmware version before upgrading your FortiGate device.

Language support

The following table lists language support information.

Language support information

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 version 5.0.10 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: 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	FortiGate Model
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: 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)	2308
Linux CentOS 6.5 (32-bit & 64-bit) Linux Ubuntu 12.0.4 (32-bit & 64-bit)	2308
Virtual Desktop for Microsoft Windows 7 Service Pack 1 (32-bit)	2308

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 8, 9, 10 and 11 Mozilla Firefox version 33
Microsoft Windows 7 64-bit SP1	Microsoft Internet Explorer versions 8, 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	✔	✔

Product	Antivirus	Firewall
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	✔	✔

Upgrade Information

Upgrading from FortiOS 5.0.6 or later

FortiOS version 5.0.10 supports upgrading from version 5.0.6 or later.

Upgrading from FortiOS 4.3.16 or later

FortiOS version 5.0.10 supports upgrading from version 4.3.16 or later.

Downgrading to previous firmware versions

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

- operation modes
- interface IP/management IP
- route static 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:

Amazon Web Services

- The 64-bit Amazon Machine Image (AMI) is available in the AWS marketplace. Download either the regular AWS image or the AWS On Demand image.

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*.

Resolved Issues

The following issues have been fixed in version 5.0.10. For inquires about a particular bug, please contact Customer Service & Support.

Antivirus

Bug ID	Description
0251398	Enabling FortiSandbox on an antivirus profile breaks the RPC connection.

Data Leak Prevention

Bug ID	Description
0244347	Handle tabs in headers in the MIME parser to properly extract and display attribute values in the Web-based Manager.

Device Visibility

Bug ID	Description
0244393	Device based policies do not work after a reboot when the source is a VLAN interface.

Endpoint Control

Bug ID	Description
0256732	An unexpected SSL connection shutdown from the client side causes the `fcnacd` daemon to consume CPU.

Firewall

Bug ID	Description
0230181	The `proxyworker` process closes the field descriptor but does not remove it from the `epoll` process. As a result, it will crash in `epoll` because the corresponding connection structure has already been released.
0235170	Self originating traffic should not use `identity-based-route`.
0246476	`FGTServer Set-Cookie` should not be added to a load-balance reply unless necessary.
0247568	A RADIUS accounting stop message is sent for users when the FSSO CA connection is established.

Bug ID	Description
0248419	FortiGate does not use the *User-Name* from the RADIUS response.
0249510	UDP VIP load balance session failover does not work.
0251394, 0252331	Traffic that passes the FortiGate twice is blocked in transparent mode when UTM is enabled.
0254366	A high CPU usage issue is caused by the `authd` daemon when there are a large number of policies.
0255623	TNS sessions hang when a VIP is defined for a mapped IP address shorter than the external IP address.
0256488	The TCP session disconnects when a firewall policy is changed.

FortiGate VM

Bug ID	Description
0250054	When the license status cannot be validated for more than 4 hours or it changes, FortiGate VM should create an event log entry.
0252306	FortiToken cannot be used for console login.

High Availability

Bug ID	Description
0231555	Traffic stops when `load-balance-all` is enabled in active-active HA.
0250721	The slave times out when receiving the master configuration if the master has hundreds of VDOMs.
0258356	Log upload to FortiAnalyzer fails for non-management VDOMs in HA.

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.

IPsec VPN

Bug ID	Description
0244227	IPsec sends too many DPD probes caused by long system up time.

Bug ID	Description
0248504	Fragmentation behavior of the IPsec interface changes when a session is offloaded.
0247729	NAT IPsec traffic is not decrypted by NP4lite/SoC2.
0251170	ESP replay packets are generated by the kernel.
0253221	IPsec offload feature for NP6 has been added.
0253680	Packets are tunnelled twice (ESP in ESP) by NP6 when the IPsec tunnel is terminated on an *npu-vlink* interface.
0256492	When IPsec interfaces belong to the same zone, all existing established IPsec SA are brought down with multiple configuration changes.

IPv6

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

Log & Report

Bug ID	Description
0241397	Updated session accounting after confirming the local-in IP packet in order to have proper logs.
0248692	The `config log fortianalyzer override-setting` CLI command does not accept IP addresses from a FortiAnalyzer configured in global context.
0250058	The command `execute log delete-old logs` does not work as expected.
0251714	The user event log action does not show the authentication method with explicit proxy.

Routing

Bug ID	Description
0252890	AS-override not taken into account when using the `set activate disable/enable` CLI command.

Spam Filter

Bug ID	Description
0257510	Added the .asia TLD as part of the URL so it can be recognized by spam filter.

SSL VPN

Bug ID	Description
0229536	Not able to access SAP server bookmarks via web mode.
0243780	SSL VPN certificate based authentication without PKI users does not work with the SSL VPN client.
0229880	Web mode does not work with the Nexpose application.
0231666	Improved the submit button for editorial login page with SSO.
0231798	The PortForward connection tool should close the session as soon as it is closed by the backend server.
0234991	Web mode navigation buttons for a specific web page do not work.
0244399	Unable to handle remote web server return JavaScript as plain text type.
0247112	The `auto-tunnel-policy` is set to `disable` when a tunnel policy is added.
0248425	Improper display of a webpage accessed through the bookmark in web mode.
0251526	Login failure by a local user via internal routing when the policy's `srcintf` is `any`.
0252113	The username is incomplete when using user certificate authentication.
0254118	SSO bookmark for OWA page does not work when only HTTP/HTTPS is selected in webmode settings.
0254280	SSL VPN web mode is unable to access web pages due to a JavaScript error.
0259136	SSL proxy of SSL VPN can only use SSLv3 for the server side connection. TLS should be supported for the backend connection.

System

Bug ID	Description
0214401	An admin user on a remote authentication server cannot login via HA management interface.
0235841	Enhanced NP4 memory allocation to prevent system losing packets when under heavy load.
0237740	Possible memory leak for IPS traffic when sessions are synchronized.
0242454	Autoupdate tunneling does not work after upgrade.
0244082	To ensure nturbo works as expected, traffic should not be offloaded to NPU if there is an interface-based policy enabled.

Bug ID	Description
0244981	Backing up the FortiGate configuration file using remote admin user (RADIUS, TACACS+) results in a small truncated file.
0247062	FortiGate fails to update generic DDNS record when zone information is present in the server response.
0247563	Afte a reboot, a non-admin account is unable to connect to the HA management interface.
0247826	Increased the scheduled timeout to avoid random CPU15 peaks.
0248460	Cloning an application control profile produces memory corruption errors.
0248808	Cannot change group members of a nested address group.
0248912	On XR cards, the first data packet from a server can be dropped because the sequence number checking caused by anti-replay.
0250120	SCP configuration backup with RSA key authentication retrieves only the root VDOM configuration.
0252333	XLR crash when packets with priority bits are set in the VLAN tag.
0252455	Unexpected UDP port translation for NTP protocol.
0253221	IPsec pass through traffic is not accelerated by NP6.
0253694	`radiusd` daemon memory issueis caused by HA synchronization.
0253970	There is a long reboot time on a device with large configuration.
0256456	Fixed a memory leak in IPS and a crash issue in the AV Engine.
0256486	ADSL is unable to connect after upgrading to version 5.0.10.
0256491	Memory corruption in IPSA driver can cause a system freeze condition.
0256498	Improved how firewall policies are purged.
0256730	Changed the default digest method from SHA to SHA256 for certificate request generation.
0256899	Backing up the configuration may remove UTM related settings in the web proxy identity policy.
0257207	The system does not restore interface configuration that references an invalid interface.
0257343	Updated Israel's daylight savings time rules.
0257797, 0239522, 0182015	Added more counters to monitor proxyworker memory usage and release unused memory.

Bug ID	Description
0258251	Sessions are dropped when a VLAN interface description is changed.
0259973	Huawei E3372 modem support added.
0260155	DHCP does not request a new IP address on interfaces with IPsec after being brought back up.
0262017	SNMPv3 linkUp/linDown trap ID issue.
0262749	Improved performance with VLAN traffic.

Upgrade

Bug ID	Description
0249646	Two-factor configuration is lost for the system administrator after upgrading.
0258782	The admin login banner is not preserved during upgrade.
0259980	The FG-20C-ADSL-A's WAN interface is missing after upgrade.

VoIP

Bug ID	Description
0249511	SIP ALG crashes when using TLS renegotiation for SIP/TLS with MTLS.
0261920	SIP ALG fails to open a pinhole for the contact port in the invite message.

WAN Optimization and Web Proxy

Bug ID	Description
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.
0254020	Web proxy fails to connect server if the outgoing IP is configured.

Web-based Manager

Bug ID	Description
0214596	Allow saving multiple `dhcp-relay-ip` settings.
0230125	Prevent adding an IP address with different associated interfaces to the same group.
0231693	Imported local certificate overrides previously imported certificate.

Bug ID	Description
0238877	Issue with non-utf8 domain names that prevents the device list from displaying.
0250556	When creating a new custom service, the low source port initial value is incorrect.
0253649	Certain specific configurations can lead to VLANs being hidden from the VDOM interface list.

Web Filter

Bug ID	Description
0249622	The load time of a URL filter list with 50,000 entries should be shorter.
0255209	In transparent mode, if FortiGuard categories have the action set to *Warning*, the client's connection is reset and unable to reach the requested URL.

Wireless

Bug ID	Description
0249045	Cannot forward multicast traffic when DTLS encryption is enabled for CAPWAP.

Known Issues

The following issues have been identified in version 5.0.10. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Data Leak Prevention

Bug ID	Description
0261567	DLP cannot detect files in Microsoft Outlook Web Access over HTTPS.

Firewall

Bug ID	Description
0254388	FortiGate may experience an HA failover issue caused by high CPU usage.
0259681	Users may experience a HTTPS transaction failure on a load balanced VIP in full SSL mode.

FG-1500D and FG-3700D

Bug ID	Description
0242298	When the FortiGate unit experiences high CPU usage, IPsec VPN packets may be lost.
0241646	Traffic may not pass through a VLAN interface added to a link aggregation group (LAG) in a transparent mode VDOM. Workaround: Run a diagnose sniffer packet on the physical interface in the transparent mode VDOM or reboot the FortiGate unit.
0242012	IPsec VPN traffic throughput is highly unstable. Workaround: Do not use IPsec VPN over a 40G LAG.
0240789	FG-3700D: LAG groups configured on low latency interfaces (port25 to port32, and NP6_0 to NP6_1) do not function correctly. Workaround: Only use either low-latency-mode or LAG for traffic on these interfaces.
0239968	IP tunneling (SIT tunneling) does not work when offloaded to NP6. Workaround: Disable `auto-asic-offload` in SIT tunnel configurations.
0240945	Reply traffic is not offloaded when shared traffic shaping is enabled on policies for accelerated inter-VDOM links using the *npu_vdom* interface.

FG-80D

Bug ID	Description
0235525	The link and speed LEDs remain on after shutting down the unit using the `execute shutdown` command.
0239619	The r8168 driver is unable to shutdown power of the port and will keep the link of the other end in an up state.

FG-140D-POE

Bug ID	Description
0264029	Only the first PoE port is able to provide power to PoE devices.

FSSO

Bug ID	Description
0232434	The collector agent flushes all authenticated users after a TSAgent restart and a new user logon event.

High Availability

Bug ID	Description
0263737	Hasync stops synchronizing the configuration due to a file descriptor exhausted issue.

IPsec VPN

Bug ID	Description
0263428	The IPsec VPN may lose connectivity when connecting to the FortiGate Web-based Manager or SSH.

Routing

Bug ID	Description
0228800	After enabling `capability-default-originate`, BGP will not insert the default route learnt from a different neighbor.

System

Bug ID	Description
0233419	The `initXXX` daemon may cause high CPU usage.

Upgrade

Bug ID	Description
0263463	After upgrading, the slave may fail to synchronize with the master due to the firewall service group.
0243960	Antivirus profile errors after upgrade from 4.3

WAN Optimization and Web Proxy

Bug ID	Description
0265129	A non-standard HTTPS page fails to load when passing through two explicit proxies.

Web-based Manager

Bug ID	Description
0172567	The vulnerability scanner appears in the Web-based Manager and CLI when the FortiGate unit is in transparent mode. This feature does not work in transparent mode by design.
0254084	When using Microsoft Internet Explorer 9, created firewall policies are not displayed in the *Policy* page. The content pane toolbar is not displayed in this page.
0262171	An administrator with read-only permission is able to delete firewall policies.
0231086	A firewall policy may be deleted after a reboot if it uses an empty FSSO group.

Limitations

This section outlines the limitations in FortiOS 5.0.10.

Add device access list

If the `device-access-list` has the action set as `deny`, you will need to explicitly define a device in order to allow it to work.

For instance,

```
config user device
   edit "win"
      set mac 01:02:03:04:05:06
   next
end


config user device-access-list
   edit "wifi"
      set default-action deny
         config device-list
            edit 1
               set action accept
               set device "windows-pc" <-the predefined device-category
            next
            edit 2
               set action accept
               set device "win" <-the custom device
            next
         end
      next
   end
```

As a result, the predefined `device-category` entry 1 will not have network access. Only the custom device entry 2 would be able to get network access.

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.