FortiOS - Release Notes

VERSION 5.0.12

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

October 27, 2015

FortiOS 5.0.12 Release Notes

01-5012-278841-20151027

TABLE OF CONTENTS

Change Log

Date	Change Description
2015-05-15	Initial release.
2015-07-17	Added 279577 to Known Issues List.
2015-08-13	Added a note to Upgrading from FortiOS version 4.3.16 or later about obtaining FortiGuard services from FortiManager
2015-09-10	Added 284891 to Known Issues List.
2015-10-05	Added FGV-40D2 and FGV-70D4 to Supported Models List.
2015-10-27	Updated Upgrade Information. Added FK-3810A and FK-3950B to Supported Models List.
2016-01-27	Added FortiOS 5.0 Supported Upgrade Path note to Upgrade Information

Introduction

This document provides the following information for FortiOS version 5.0.12 build 0318:

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

See the Fortinet Document Library for FortiOS documentation.

Supported models

FortiOS version 5.0.12 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, 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-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-5001D, FG-5101C
FortiWiFi	FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D
FortiGate Rugged	FGR-60D, FGR-100C
FortiGate VM	FG-VM32, FG-VM64, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN
FortiSwitch	FS-5203B
FortiOS Carrier	FCR-3810A, FCR-3950B, FCR-5001A-DW, and FCR-5001B FortiOS Carrier version 5.0.12 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 a branch point of build 0318:

FGR-90D	FortiGate Rugged 90D is released on build 4905.
FG-98D-POE	FortiGate 98D-POE is released on build 4904.
FG-1000D	FortiGate 1000D is released on build 4901.
FG-1200D	FortiGate 1200D is released on build 4903.
FGV-40D2	FortiGate Voice 40D2 is released on build 5066.
FGV-70D4	FortiGate Voice 70D4 is released on build 5067.
FG-VM64-AWS	FortiGate VM for Amazon AWS is released on build 8441.
FG-VM64-AWSONDEMAND	FortiGate VM for Amazon AWS On Demand is released on build 8441.

Special Notices

Default log setting change

For FortiGate 2U and 3U models (FG-3600, FG-3700, FG-3800, and FG-3900 series devices) and 5000 series blades, the log disk is disabled by default. It can only be enabled via the Command Line Interface (CLI). For all 1U and desktop models that support SATA disk, the 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

You must use FortiCarrier specific firmware to upgrade your FortiCarrier hardware. 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 5.0.12, 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 5.0.12. 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 5.0.12. 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 5.0.12. 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.

Upgrade Information

Upgrading from FortiOS version 5.0.10 or later

FortiOS version 5.0.12 supports upgrading from version 5.0.10 or later.

When upgrading from a firmware version beyond those mentioned in the Release Notes, a recommended guide for navigating the upgrade path can be found on the Fortinet documentation site.

There is 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 5.0 Supported Upgrade Paths

HA Virtual MAC addresses are created for each FortiGate interface based on the interface index number. Between FortiOS 5.0.9 and 5.0.10 interface indexing changed. After upgrading a cluster to FortiOS 5.0.0, the Virtual MAC addresses assigned to individual FortiGate interfaces may be different. You can use the `get hardware nic <interface name>` CLI command to view the Virtual Mac address of each FortiGate Interface

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.

Upgrading from FortiOS version 4.3.16 or later

FortiOS version 5.0.12 supports upgrading from version 4.3.16 or later.

Tablesize limits

FortiOS 5.0 has changed the maximum allowable limits on some objects. As a result, the configuration for some objects may be lost. These include:

- Application list
- DLP sensor
- DLP sensor filter
- Firewall VIP
- IPS sensor

For more information, see the *Maximum Values Table* for FortiOS 5.0 on the Fortinet Document Library website.

FortiOS 5.0 changed how users configure their FortiGate to obtain FortiGuard services from FortiManager.

In FortiOS 4.3, users added FortiManagers as FortiGuard override servers. When upgrading from FortiOS 4.3.x to 5.0.x, the FortiGuard override settings are lost and users have to add a FortiManager to the Central Management configuration and select the option to use the FortiManager for FortiGuard communications.

The CLI syntax is:

```
config system central-management
set fortimanager-fds-override enable/disable
end
```

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.

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. 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 version 5.0.12 support

The following table lists FortiOS version 5.0.12 product integration and support information.

Web Browsers	• Microsoft Internet Explorer version 11 • Mozilla Firefox version 37 • Google Chrome version 42 • Apple Safari version 7.1 (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	• 5.2.3 and later
FortiClient iOS	• 5.2.2 build 037
FortiClient Android and FortiClient VPN Android	• 5.2.5 build 103

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 GUI. Under the *OS Version* column you will see a message reading *A recommended update is available* for any FortiAP that is running an earlier version than what is recommended.
FortiSwitch OS (FortiLink support)	• 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
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 • 5.0 build 0239 The following operating systems are supported: • Windows Server 2008 64-bit • Windows Server 2008 R2 64-bit • Windows Server 2012 Standard • Windows Server 2012 R2 Standard FSSO does not currently support IPv6. The FSSO agent supports OU in group fiters. This feature has been added for FortiOS 5.2. (OU in group filters is not supported by FortiOS 5.0.)

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.
AV Engine	• 5.163
IPS Engine	• 2.199
Virtualization Environments	
Citrix	• XenServer version 5.6 Service Pack 2 • XenServer version 6.0 and later
Linux KVM	• CentOS 6.4 (qemu 0.12.1) and later
Microsoft	• Hyper-V Server 2008 R2 • 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, 5.5, and 6.0

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	GUI	Documentation
English	✓	✓
Chinese (Simplified)	✓	-
Chinese (Traditional)	✓	-

Language	GUI	Documentation
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 5.0.12 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.

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	FortiGate Model
Module: ADM-XE2 Type: Security processing	FG-3810A, FG-5001A
Module: ADM-XD4 Type: Security processing	FG-3810A, FG-5001A
Module: ADM-FE8 Type: Security processing	FG-3810A
Module: RTM-XD2 Type: Rear transition	FG-5001A
Module: ASM-ET4 Type: Security processing	FG-310B, FG-311B
Module: RTM-XB2 Type: Rear transition	FG-5001A
Module: FMC-XG2 Type: Security processing	FG-3950B, FG-3951B
Module: FMC-XD2 Type: Accelerated interface	FG-3950B, FG-3951B
Module: FMC-F20 Type: Accelerated interface	FG-3950B, FG-3951B
Module: 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	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)	2313

Operating System	Installer
Linux CentOS 6.5 (32-bit & 64-bit) Linux Ubuntu 12.0.4 (32-bit & 64-bit)	2313
Virtual Desktop for Microsoft Windows 7 Service Pack 1 (32-bit)	2313

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.

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	✓	✓
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 FortiOS version 5.0.12. For inquires about a particular bug, please contact Customer Service & Support.

Antivirus

Bug ID	Description
266432	Corruption handling by the AV-Engine and AV Database may not work as expected.

DLP

Bug ID	Description
261567	DLP and virus scan of attachments for on-premises version of OWA may not work as expected.

ELBC

Bug ID	Description
261371	`capwap` for MAC lookup in Cluster Mode may not work as expected.

FIPS-CC

Bug ID	Description
272012	After rebooting backup box, `fips-cc vpn config test failure` may occur.

Firewall

Bug ID	Description
269863	If the response code is not 200, the Connection Upgrade Case Proxy may bypass the session.

FortiGate-3040/3140-B

Bug ID	Description
249749	In SGMII mode, users may not be able to program the SFP.

FortiGate-5001C

Bug ID	Description
271652	The Blade may stop passing traffic and restarts unexpectedly.

FortiGate-VM

Bug ID	Description
250054	When there is a license status change or a warning occurs, the FortiGate-VM License Alert may not appear in the Event Log.

FSSO

Bug ID	Description
268460	The FSSO may drop users before retrieving the complete list.

GUI

Bug ID	Description
259349	The Network Interface page may display incorrectly.
262171	Users may still be able to delete Firewall Policies in Read Only Mode.
267396	In some cases, the Top Sources widget may only report traffic only for root VDOM.

HA

Bug ID	Description
232458	The TCP session may not clear on `a-p slave`.
247725	After a default timeout expiration occurs, the session duration timer on the slave may reset.
254388	HA Packet loss may occur when there is high CPU usage
263737	The `hasync` may stop synchronizing the configuration if the file descriptor is exhausted.
264836	When editing the default admin account in the CLI, it may not sync in the HA environment.
265606	The `debugzone` and `checksum` under the `HA checksum` may not match.

Bug ID	Description
267249	After a `vcluster1 failover`, the `vcluster2 VMAC` on the VLAN interface may not persist.

IPSEC

Bug ID	Description
263428	Tunnels may go down after 420 days of uptime.
266115	When handling `IKEv2 SA_INIT Packet` as a Responder, the `iked` may stop working.

IPSEngine

Bug ID	Description
273164	A memory leak may occur in the SMB2 decoder.

Logging & Report

Bug ID	Description
232768	`unknown-0` interface may be displayed in the log.
242425	After a `HA failover` with multiple ISPs, the FortiAnalyzer logging over IPSec may stop working.
254899	When the Source is a FortiAnalyzer, Traffic Logs may not be displayed.

Routing

Bug ID	Description
275894	If OSPF type 3 routes are obtained from multiple ABRs, some of the routes may not be installed after selected ABR flushes its type 3 routes.

SSLVPN

Bug ID	Description
247112, 265504	After `sslvpn idle-timeout expire` and `portal re-login occurs`, the `RDPnative` may not work.
271439	When a website is accessed through the SSLVPN Web Mode Bookmark, users may not be able to upload files.

System

Bug ID	Description
237288	Due to VDOM isolation, the System Admin `remote group` may be modified incorrectly.
240001	10G full speed option may not be available for FortiGate-1500D.
259681	HTTPS Transactions may not work.
260381	When there is a `null trusthost` betwen the `valid trusthosts`, the Admin User may not be able to login to the FortiGate.
261669	Due to ARP Requests and NP Accelerated Sessions, high CPU usage may occur.
264367	When trying to obtain the Admin Profile from Radius, the SCP backup may not work as expected.
264983	When users try to edit the Display Zone from the GUI, the Display Zone with the Member Interface List may be slow to load.
265245	There may not be a corresponding policy for the `keepalive portal`, and the redirect address may be set to the local IP. This may cause the `location.href` to be the IP address instead of the `auth-redirect-addr` thatis configured in the policy.
267131	AV-Engine and AV Database corruption handling may occur.
268654	During bootup, the System and Console may be slow to respond.
272967, 273375	Application Control and IPS UTM Profiles may be limited to only 500.
276191	In some cases, the Radius Authentication may not work.

WAN Optimization & Webproxy

Bug ID	Description
253682	When the Webcache is enabled and it receives the 304 Message from the Server, the `wad process` may stop working.
265129	When going through two Explicit Proxies, the *None Standard HTTPS Page* may not load as expected.

Webfilter

Bug ID	Description
182863	In some cases, the `URLFilter` may become stuck in the *No Correct FortiGuard Information* state.

Upgrade

Bug ID	Description
259334	After upgrading to 5.0, the HA Cluster may be out of sync.
261562	After upgrading from 4.3 to 5.0, the TCP Reset Settings may have changed.
274251	After upgrading to 5.0.11 or 5.2.3, the Explicit Proxy Service may not be correctly created when using the GUI.

Known Issues

The following issues have been identified in FortiOS version 5.0.12. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

FG-80D

Bug ID	Description
235525	The link and speed LEDs remain on after shutting down the unit using the `execute shutdown command`.
239619	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-1500D and FG-3700D

Bug ID	Description
239968	IP tunneling (SIT tunneling) does not work when offloaded to NP6. Workaround: Disable `auto-asic-offload` in SIT tunnel configurations.
240789	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.
240945	Reply traffic is not offloaded when shared traffic shaping is enabled on policies for accelerated inter-VDOM links using the `npu_vdom` interface.
241646	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.
242012	IPsec VPN traffic throughput is highly unstable. Workaround: Do not use IPsec VPN over a 40G LAG.
242298	When the FortiGate unit experiences high CPU usage, IPsec VPN packets may be lost.

GUI

Bug ID	Description
231086	A firewall policy may be deleted after a reboot if it uses an empty FSSO group.

Bug ID	Description
254084	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.

Routing

Bug ID	Description
228800	After enabling `capability-default-originate`, BGP will not insert the default route learnt from a different neighbor.

System

Bug ID	Description
233419	The `initXXX` daemon may cause high CPU usage.

Upgrade

Bug ID	Description
243960	Antivirus profile errors after upgrade from 4.3
263340	The source address is lost and SNAT is disabled in a multicast policy after upgrading from 4.3.
269249	When upgrading from 4.0 to 5.0 firmware, the LB VIP option `set http-ip-header enable` may not be preserved.
284891	Users may not be able to upgrade to 5.0.12 due to the impact of the VIPs no longer working when making requests internally to the external IP addresses.

Limitations

This section outlines the limitations in FortiOS version 5.0.12.

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.