



FortiOS v5.0.9  
Release Notes



FortiOS v5.0.9

January 28, 2015

01-509-249816-20150128

Copyright© 2015 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Fortinet Document Library	<a href="http://docs.fortinet.com">docs.fortinet.com</a>
Fortinet Video Library	<a href="http://video.fortinet.com">video.fortinet.com</a>
Customer Service & Support	<a href="http://support.fortinet.com">support.fortinet.com</a>
Training Services	<a href="http://training.fortinet.com">training.fortinet.com</a>
FortiGuard	<a href="http://fortiguard.com">fortiguard.com</a>
Document Feedback	<a href="mailto:techdocs@fortinet.com">techdocs@fortinet.com</a>

# Table of Contents

<b>Change Log</b> .....	<b>5</b>
<b>Introduction</b> .....	<b>6</b>
Supported models .....	6
<b>Special Notices</b> .....	<b>8</b>
FG-300D and FG-500D nTurbo Support .....	8
FG-3600C hardware compatibility.....	8
SCTP firewall support .....	8
New FortiOS Carrier features.....	8
Changes to licensing.....	8
Changes to GPRS Tunneling Protocol (GTP) support .....	9
Changes to MMS scanning.....	9
TFTP boot process .....	9
Monitor settings for Web-based Manager access .....	9
Before any upgrade .....	10
After any upgrade .....	10
Using wildcard characters when filtering log messages .....	10
Default setting/CLI changes/Max values changes .....	11
IPS algorithms.....	11
Disk logging disabled by default on some models (Log to FortiCloud instead) ....	12
FG-60D/FWF-60D logging to disk .....	12
WAN Optimization .....	12
MAC address filter list.....	13
Spam filter profile.....	13
Spam filter black/white list.....	13
DLP rule settings.....	13
Limiting access for unauthenticated users .....	13
Use case - allowing limited access for unauthenticated users.....	14
Use case - multiple levels of authentication .....	14
FG-100D upgrade and downgrade limitations .....	14
32-bit to 64-bit version of FortiOS .....	15
Internal interface name/type change .....	15
FG-100D hardware compatibility.....	16
<b>Upgrade Information</b> .....	<b>17</b>
Upgrading from FortiOS v5.0.6 or later .....	17
Upgrading an HA cluster.....	17
HA Virtual MAC Address Changes .....	17
Dynamic profiles must be manually converted to RSSO after upgrade .....	17

Zone-related policies may be deleted when upgrading to FortiOS v5.0.4 and later.....	17
Captive portal.....	17
Reports .....	22
SSL VPN web portal .....	22
Virtual switch and the FG-100D.....	22
DHCP server reserved IP/MAC address list .....	22
Upgrading from FortiOS v4.3.....	23
Table size limits.....	23
SQL logging upgrade limitation .....	23
SSL deep-scan .....	23
Profile protocol options.....	24
Upgrade procedure.....	27
SQL database error.....	27
Downgrading to previous FortiOS versions .....	27
FortiGate VM firmware .....	28
Firmware image checksums .....	28
<b>Product Integration and Support .....</b>	<b>29</b>
FortiOS v5.0.9 support .....	29
Language support.....	30
Module support.....	31
SSL VPN support .....	32
SSL VPN standalone client .....	32
SSL VPN web mode .....	33
SSL VPN host compatibility list .....	33
Explicit web proxy browser support .....	34
Default Behavior/Config Change .....	34
<b>Resolved Issues.....</b>	<b>35</b>
Web-based Manager .....	35
<b>Known Issues.....</b>	<b>36</b>
FG-1500D and FG-3700D.....	36
FG-80D .....	36
FG-100D .....	37
FG-300D and FG-500D.....	37
WAN Optimization and explicit proxy .....	37
Upgrade .....	37
Web-based Manager and CLI.....	38
<b>Limitations.....</b>	<b>39</b>
Add device access list .....	39
Citrix XenServer limitations.....	40
Open Source Xen limitations .....	40

# Change Log

Date	Change Description
2014-08-01	Initial release.
2014-08-07	Updated upgrade information. Updated virtualization environment support information.
2014-08-13	Added the FG-94D to support models. Updated FortiManager support information.
2014-08-26	Updated FortiManager support information. Updated FortiAnalyzer support information. Updated FortiClient support information.
2014-09-09	Updated SSL VPN standalone client information.
2014-10-07	Updated known issues. Removed Mac OS X from SSL VPN support. Added FG-1200D to support models.
2014-11-12	Added bug ID 0254084 in known issues. Added FG-98D-POE to support models.
2014-11-17	Added FG-100D hardware compatibility special notice.
2014-11-24	Added FGR-90D to support models.
2014-12-23	Removed FG-92D and FWF-92D from supported models.
2015-01-28	Added FG-3200D to support models.

# Introduction

This document provides the following information for FortiOS v5.0.9 build 0292:

- [Introduction](#)
- [Special Notices](#)
- [Upgrade Information](#)
- [Product Integration and Support](#)
- [Resolved Issues](#)
- [Known Issues](#)
- [Limitations](#)

For more information on upgrading your FortiOS device, see the *FortiOS 5.0 Handbook* at <http://docs.fortinet.com>.

## Supported models

FortiOS v5.0.9 supports the following models:

<b>FortiGate</b>	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-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3810A, FG-3950B, FG-3951B, FG-5001A, FG-5001B, FG-5001C, FG-5101C
<b>FortiGate Rugged</b>	FGR-100C, FGR-90D
<b>FortiWiFi</b>	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
<b>FortiGate VM</b>	FG-VM32, FG-VM64, FG-VM64-XEN, FG-VM64-KVM, FG-VM64-HV
<b>FortiSwitch</b>	FS-5203B
<b>FortiOS Carrier</b>	FCR-3810A, FCR-3950B, FCR-5001A-DW, FCR-5001B  FortiOS Carrier v5.0.9 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 0292:

<b>FG-98D-POE</b>	The FortiGate 98D-PoE is released on build number 4687.
<b>FG-1200D</b>	The FortiGate 1200D is released on build number 4664.

---

**FG-3200D**

The FortiGate 3200D is released on build number 4758.

---

**FGR-90D**

The FortiGate Rugged 90D is released on build number 4681.

---

# Special Notices

## 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 v5.0.6 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 v5.0.6 or later and cannot be downgraded to FortiOS v5.0.5 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 5.0 and FortiOS Carrier 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 5.0, only FortiCarrier-specific hardware could run FortiOS Carrier 4.0. Starting with FortiOS 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 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 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 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 5.0.2 or later, it can be upgraded to FortiOS Carrier 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 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.

## TFTP boot process

The TFTP boot process erases all current firewall configuration and replaces it with the factory default settings.

## Monitor settings for Web-based Manager access

Fortinet recommends setting your monitor to a screen resolution of 1280x1024. This allows for all the objects in the Web-based Manager to be viewed properly.

## Before any upgrade

Upgrade your FortiOS device during a maintenance window. To minimize any adverse impact your users and your network, plan the firmware upgrade during a maintenance window. This allows you to properly upgrade, test, and implement the firmware upgrade.

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.



In VMware environments, it is recommended that you take a *Snapshot* of the VM instance prior to upgrading. In the event of an issue with the firmware upgrade, use the *Snapshot Manager* to revert to the *Snapshot*. To create a *Snapshot*, right-click the VM instance and select *Snapshot > Take Snapshot*.



In Citrix XenServer environments, it is recommended that you take a *Snapshot* of the VM instance prior to upgrading. In the event of an issue with the firmware upgrade, use *Virtual Machines Snapshots* to revert to the *Snapshot*. To create a *Snapshot*, right-click the VM instance and select *Take a Snapshot*.



Open Source Xen does not natively support *Snapshots*. You can create a backup of LVM partitions with the *LVM Snapshots* feature and then restore this backup. You can also use Linux commands to backup and restore a virtual machine.

---

## After any upgrade

If you are using the Web-based Manager, clear your browser cache prior to login on the FortiGate to ensure the Web-based Manager screens are displayed properly.

The AV and IPS engine and definitions included with a firmware upgrade may be older than ones currently available from the FortiGuard Distribution Server (FDS). Fortinet recommends performing an *Update Now* after upgrading. Go to *System > Config > FortiGuard*, select the blue triangle next to *AV & IPS Download Options* to reveal the menu, and select the *Update Now* button. Consult the *FortiOS v5.0 Handbook* for detailed procedures.

## 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.

## Default setting/CLI changes/Max values changes

- Increased site-to-site tunnel numbers for 2U and 3U models. (230577)
  - 2U -- 20,000
  - 3U and up --- 40,000
- To improve GUI performance, Section View is disabled in the firewall policy page if a large number of policies exist (231219)
- Increased the maximum number of certificates on FortiGate models 1000 and up (2U models) to 500.
- Increased the maximum number of members in a firewall address group on FortiGate models 1000 and up (2U models and up) to 1500.
- New maximum value for the number of FSSO polling entries. The values are 5 for desktop models, 20 for 1U models, 100 for 2U models and up.
- FortiGate-VM8 now supports 500 VDOMs.
- Adjustments to the following max values for low end models:
  - Application list: root will have 3 default, new VDOM will have 1 (previous is 3).
  - IPS sensor: root will have 6 default, new VDOM will have 1 (previous is 6).
  - Web Filter profile: root will have 4 default, new VDOM will have 1.
  - Antivirus profile: root will have 2 default, new VDOM will have 1.
  - DLP profile: root will have 6 default, new VDOM will have 1.
  - Email Filtering profile: root will have 1 default, new VDOM will have 1.

## 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 (512 MB or less)
- super: This algorithm works best on FortiGate models with more memory (more than 4 GB)

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 (Log to FortiCloud instead)

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

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

If you were logging to FortiCloud prior to upgrading to FortiOS v5.0.9, 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 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 v5.0 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 v5.0.9. 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 v5.0.9. 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 v5.0.9. 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.

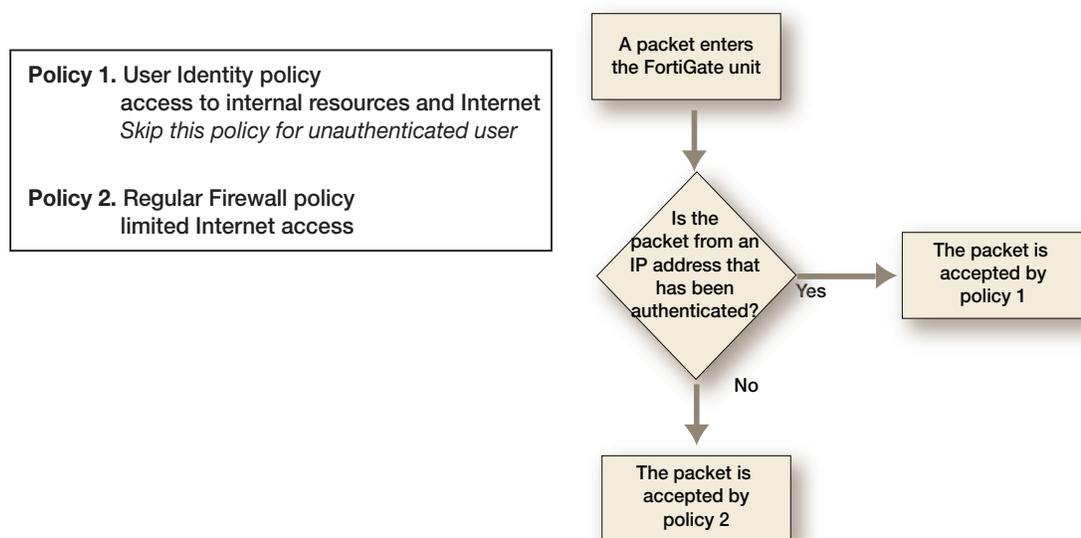
To support these different levels of access you can add a user identity policy to the top of the policy list that allows authenticated users to access internal resources and to have unlimited access to the Internet. In this policy, select *Skip this policy for unauthenticated user*.

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.

Figure 1 shows how the FortiGate unit handles packets received from authenticated and unauthenticated users.

**Figure 1:** Packet flow for authenticated and unauthenticated users



## 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 FortiGate 100D model when upgrading from FortiOS v4.3 to FortiOS v5.0.0 or later.

## 32-bit to 64-bit version of FortiOS

With the release of FortiOS v5.0.0 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 v5.0.0 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 v5.0.0 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 v5.0.0 or later with a FG-100D upgraded from FortiOS v4.0 MR3, 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 v5.0.0 to v5.0.7, 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 v5.0.8 or later.

# Upgrade Information

## Upgrading from FortiOS v5.0.6 or later

FortiOS v5.0.9 officially supports upgrading from FortiOS v5.0.6 or later.



Please review the [Special Notices](#), [Product Integration and Support](#), [Known Issues](#), and [Limitations](#) chapters prior to upgrading. For more information on upgrading your FortiOS device, see the *FortiOS 5.0 Handbook* at <http://docs.fortinet.com>.

### Upgrading an HA cluster

When upgrading a high availability cluster to FortiOS v5.0.9, if uninterruptable-upgrade is enabled you must always upgrade to FortiOS v5.0.6 before upgrading to v5.0.9. If you skip this step the firmware upgrade will fail.

### HA Virtual MAC Address Changes

HA virtual MAC addresses are created for each FortiGate interface based on that interface's index number. Between FortiOS v4.3 and v5.0 interface indexing changed. After upgrading a cluster to FortiOS v5.0 the virtual MAC addresses assigned to individual FortiGate interfaces may be different. You can use the `get hardware nic <interface-name>` command to view the virtual MAC address of each FortiGate interface.

### Dynamic profiles must be manually converted to RSSO after upgrade

After upgrading from FortiOS v4.3 to FortiOS v5.0, dynamic profile configurations are lost and you must manually create new RADIUS Single Sign On (RSSO) configurations to maintain the old dynamic profile functionality.

### Zone-related policies may be deleted when upgrading to FortiOS v5.0.4 and later

Policies that include interfaces that are members of a zone could be deleted when upgrading to FortiOS v5.0.4 and later. As of v5.0.4 you cannot create policies that include interfaces that have been added to zones. The reason for this restriction is that if you have policies for interfaces added to zones and policies for zones it may not be clear which policy to match with traffic that is received by the interface.

To avoid this problem, review your policies before the upgrade and re-configure policies that include interfaces that have been added to zones.

### Captive portal

The captive portal configuration has changed in FortiOS v5.0.9 and upon upgrading the previous configuration may be lost or changed. Review the following configuration examples before upgrading.

## Endpoint control

The following examples detail an endpoint control configuration to allow all compliant Microsoft Windows and Mac OS X computers network access. All non-compliant computers will be sent to the captive portal.

### **Example FortiOS v5.0.0 configuration:**

```
edit 3
  set srcintf "internal"
  set dstintf "wan1"
  set srcaddr "all"
  set action accept
  set identity-based enable
  set identity-from device
  set nat enable
  config identity-based-policy
    edit 1
      set schedule "always"
      set dstaddr "all"
      set service "ALL"
      set devices "windows-pc" "mac"
      set endpoint-compliance enable
    next
    edit 2
      set schedule "always"
      set dstaddr "all"
      set service "ALL"
      set devices all
      set action capture
      set devices "windows-pc" "mac"
      set captive-portal forticlient-compliance-enforcement
    next
  end
next
```

The new `set forticlient-compliance-enforcement-portal enable` and `set forticlient-compliance-devices windows-pc mac` CLI commands have been added to the master policy. Sub-policy 2 has been removed.

### **Example FortiOS v5.0.9 configuration:**

```
edit 3
  set srcintf "internal"
  set dstintf "wan1"
  set srcaddr "all"
  set action accept
  set forticlient-compliance-enforcement-portal enable
  set forticlient-compliance-devices windows-pc mac
  set identity-based enable
  set identity-from device
  set nat enable
  config identity-based-policy
    edit 1
      set schedule "always"
      set dstaddr "abc"
      set service "ALL"
      set devices "windows-pc" "mac"
      set endpoint-compliance enable
    next
  end
next
```

After the upgrade, you may experience a configuration loss with the removal of sub-policy 2. If this occurs, you have to enter the following CLI commands:

```
set forticlient-compliance-enforcement-portal enable
set forticlient-compliance-devices windows-pc mac
```

### **Device detection**

The following examples detail a device detection configuration to allow Android, Blackberry, and iPhone devices network access. The captive portal is used to optionally learn the device type, or send back a replacement message if device type cannot be determined.

### **Example FortiOS v5.0.0 configuration:**

```
edit 3
  set srcintf "internal"
  set dstintf "wan1"
  set srcaddr "all"
  set action accept
  set identity-based enable
  set identity-from device
  set nat enable
  config identity-based-policy
    edit 1
      set schedule "always"
      set dstaddr "all"
      set service "ALL"
      set devices "android-phone" "blackberry-phone" "ip-phone"
    next
  edit 2
```

```

        set schedule "always"
        set dstaddr "all"
        set service "ALL"
        set devices all
        set action capture
        set captive-portal device-detection
    next
end
next

```

The new `set device-detection-portal enable` CLI command has been added to the master policy. Sub-policy 2 has been removed.

**Example FortiOS v5.0.9 configuration:**

```

edit 3
    set srcintf "internal"
    set dstintf "wan1"
    set srcaddr "all"
    set action accept
    set device-detection-portal enable
    set identity-based enable
    set identity-from device
    set nat enable
    config identity-based-policy
        edit 1
            set schedule "always"
            set dstaddr "abc"
            set service "ALL"
            set devices "android-phone" "blackberry-phone" "ip-phone"
        next
    end
next

```

After the upgrade, you may experience a configuration loss with the removal of sub-policy 2. If this occurs, you have to enter the following CLI command:

```

set device-detection-portal enable

```

**Email collection**

The following examples detail an email collection configuration which would allow all devices for which an email-address has been collected network access. Any device which has not had an email collected would be directed to the captive portal.

**Example FortiOS v5.0.0 configuration:**

```

edit 3
    set srcintf "internal"
    set dstintf "wan1"
    set srcaddr "all"
    set action accept
    set identity-based enable
    set identity-from device

```

```

set nat enable
config identity-based-policy
edit 1
    set schedule "always"
    set dstaddr "all"
    set service "ALL"
    set devices email-collection
next
edit 2
    set schedule "always"
    set dstaddr "all"
    set service "ALL"
    set devices all
    set action capture
    set captive-portal email-collection
next
end
next

```

The new `set email-collection-portal enable` CLI command has been added to the master policy. Sub-policy 2 has been removed.

**Example FortiOS v5.0.9 configuration:**

```

edit 3
    set srcintf "internal"
    set dstintf "wan1"
    set srcaddr "all"
    set action accept
    set email-collection-portal enable
    set identity-based enable
    set identity-from device
    set nat enable
    config identity-based-policy
        edit 1
            set schedule "always"
            set dstaddr "abc"
            set service "ALL"
            set devices "collected-emails"
        next
    end
next

```

After the upgrade, you may experience a configuration loss with the removal of sub-policy 2. If this occurs, you have to enter the following CLI command:

```

set email-collection-portal enable

```

## Reports

Before you run a report after upgrading to v5.0.9, you must enter the following CLI commands:

```
execute report-config reset
This will reset report templates to the factory default.
All changes to the default report will be lost!
Do you want to continue? (y/n)y
Report configuration was reset to the factory default.
```

```
execute report recreate-db
This will recreate the report database from the log database.
Do you want to continue? (y/n)y
Request to recreate report database is successfully sent.
```

## SSL VPN web portal

For FG-60C variants and lower models only one SSL VPN web portal is retained after upgrading to FortiOS v5.0.9.

## Virtual switch and the FG-100D

The name *Virtual Switch* is used by different objects on the Web-based Manager and the CLI. On the Web-based Manager *Virtual Switch* refers to an interface type and is used for the FortiSwitch controller feature. This instance of *Virtual Switch* maps to the CLI command `config switch-controller vlan`.

The second instance of *Virtual Switch* in the CLI, `config system virtual-switch` is used to configure the hardware switch. This command maps to the Web-based Manager hardware switch interface type.

## DHCP server reserved IP/MAC address list

Up to FortiOS v5.0.4 you could use the following command to add a system-wide reserved IP/MAC address list for all DHCP servers.

```
config system dhcp reserved-address
```

This command has been removed in FortiOS v5.0.5. If you have configured reserved IP/MAC addresses using this command, they will be lost when you upgrade to FortiOS v5.0.5. To keep these IP/MAC address pairs you must add them to individual DHCP server configurations, for example:

```
config system dhcp server
edit 1
config reserved-address
edit 0
config ip 172.20.120.137
config mac 00:09:0F:E7:61:40
end
```

## Upgrading from FortiOS v4.3

FortiOS v5.0.9 officially supports upgrade from FortiOS v4.3.16 and v4.3.17.



Please review the [Special Notices](#), [Product Integration and Support](#), [Known Issues](#), and [Limitations](#) chapters prior to upgrading. For more information on upgrading your FortiOS device, see the *FortiOS 5.0 Handbook* at <http://docs.fortinet.com>.

### Table size limits

FortiOS v5.0.9 has changed the maximum allowable limits on some objects. As a result, the configuration for some objects may be lost. These include:

- dlp sensor
- firewall vip
- application list
- dlp sensor filter
- ips sensor

For more information, see the *Maximum Values Table for FortiOS 5.0* at <http://docs.fortinet.com>.

### SQL logging upgrade limitation

For the following units, after upgrading to FortiOS v5.0.9 SQL logging will be retained based on the total size of the RAM available on the device. Logs will use up to a maximum of 10% of the RAM. Once passed that threshold, any new logs will overwrite older logs. The historical report generation will also be affected based on the SQL logs that are available for query.

- FG-100D
- FG-300C

### SSL deep-scan

A new SSL/SSH inspection option has been added to include all SSL protocols. The protocol status in SSL/SSH inspection will default to *disable* for the SSL protocols. The SSL/SSH inspection should be modified to enable the SSL protocols wherever inspection is required.

#### Before upgrade

- The antivirus, web filter, and antispam profiles had separate protocol settings for the SSL and non-SSL protocols.
- For HTTPS deep-scanning to be done, deep-scan needed to be enabled for HTTPS in the UTM proxy options.

#### After upgrade

- The settings for the SSL protocols in the antivirus, web filter, and antispam profiles have been removed. Instead, the non-SSL options will apply to both the SSL and non-SSL versions of each protocol. The SSL/SSH inspection options now includes an enable/disable

option for each protocol. This is used to control which protocols are scanned and which SSL enabled protocols are decrypted.

- To use HTTPS non-deep (SSL handshake) inspection, HTTPS needs to be enabled in the SSL/SSH inspection options. A web filter profile with `https-url-scan` enabled needs to be applied in the policy with the SSL/SSH inspection options. The web filter profile option changes the inspection mode to non-deep scan. AV will not be performed if this option is enabled. The web filter profile option does not apply if `SSL inspect-all` is enabled in the SSL/SSH inspection options.

## Behavior

- After upgrade, all the SSL related settings in the antivirus, web filter, and antispam profiles will be lost. The non-SSL settings will be retained and applied to the related SSL protocols if they are enabled in the SSL/SSH inspection options. The protocol status in the SSL/SSH inspection options will default to enable for the non-SSL protocols and will default to disable for the SSL protocols. The SSL/SSH inspection options should be modified to enable the SSL protocols wherever inspection is required.
- Any profiles requiring non-deep HTTPS inspection will need to be modified to include a web filter profile and SSL/SSH inspection options with the settings as described above. The original HTTPS deep-scan settings will be lost upon upgrade.

## Profile protocol options

Deep inspection status configurations are not retained for FTPS/IMAPS/POP3S/SMTPS after upgrading from FortiOS v4.3.

### Example FortiOS v4.3 configuration:

```
config firewall profile-protocol-options
  edit "default"
    set comment "all default services"
    config http
      set port 80
      set port 8080
      set options no-content-summary
      unset post-lang
    end
    config https
      set port 443
      set port 8443
      set options allow-invalid-server-cert
      unset post-lang
      set deep-scan enable
    end
    config ftp
      set port 21
      set options no-content-summary splice
    end
    config ftps
      set port 990
      set options no-content-summary splice
      unset post-lang
    end
  end
```

```

config imap
    set port 143
    set options fragmail no-content-summary
end
config imaps
    set port 993
    set options fragmail no-content-summary
end
config pop3
    set port 110
    set options fragmail no-content-summary
end
config pop3s
    set port 995
    set options fragmail no-content-summary
end
config smtp
    set port 25
    set options fragmail no-content-summary splice
end
config smtps
    set port 465
    set options fragmail no-content-summary splice
end
config nntp
    set port 119
    set options no-content-summary splice
end
next
end

```

**Example FortiOS v5.0.9 configuration:**

```

config firewall profile-protocol-options
    edit "default"
        set comment "all default services"
        config http
            set ports 80 8080
            set options no-content-summary
            unset post-lang
        end
        config ftp
            set ports 21
            set options no-content-summary splice
        end
        config imap
            set ports 143
            set options fragmail no-content-summary
        end
        config mapi

```

```

        set ports 135
        set options fragmail no-content-summary
    end
    config pop3
        set ports 110
        set options fragmail no-content-summary
    end
    config smtp
        set ports 25
        set options fragmail no-content-summary splice
    end
    config nntp
        set ports 119
        set options no-content-summary splice
    end
    config dns
        set ports 53
    end
next
end

config firewall deep-inspection-options
edit "default"
    set comment "all default services"
    config https
        set ports 443 8443
        set allow-invalid-server-cert enable
    end
    config ftps
        set ports 990
        set status disable
    end
    config imaps
        set ports 993
        set status disable
    end
    config pop3s
        set ports 995
        set status disable
    end
    config smtps
        set ports 465
        set status disable
    end
next
end

```

## Upgrade procedure

Plan a maintenance window to complete the firmware upgrade to ensure that the upgrade does not negatively impact your network. Prepare your FortiGate device for upgrade and ensure other Fortinet devices and software are running the appropriate firmware versions as documented in the [Product Integration and Support](#) section.

Save a copy of your FortiGate device configuration prior to upgrading. To backup your configuration, go to *System > Dashboard > Status*. In the *System Information* widget select *Backup* under *System Configuration*. Save the configuration file to your management computer.

### To upgrade the firmware via the Web-based Manager:

1. Download the .out firmware image file from the Customer Service & Support portal FTP directory to your management computer.
2. Log into the Web-based Manager as the `admin` administrative user.
3. Go to *System > Dashboard > Status*.
4. In the *System Information* widget, in the *Firmware Version* field, select *Update*.  
The *Firmware Upgrade/Downgrade* window opens.
5. Select *Browse* and locate the firmware image on your management computer and select *Open*.
6. Select *OK*. The FortiGate unit uploads the firmware image file, upgrades to the new firmware version. The following message is displayed.
7. Refresh your browser and log back into your FortiGate device. Launch functional modules to confirm that the upgrade was successful.

For more information on upgrading your FortiGate device, see the [Install and System Administration for FortiOS 5.0](#) at <http://docs.fortinet.com/fgt.html>.

## SQL database error

When upgrading to FortiOS v5.0.9, the FortiGate may encounter a *SQL Database Error*.

Workaround: After the upgrade, rebuild the SQL database.

## Downgrading to previous FortiOS 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:

### VMware

- `.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.

### 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.

### 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.

### 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`.

For more information see the FortiGate VM product datasheet available on the Fortinet web site, <http://www.fortinet.com/sites/default/files/productdatasheets/FortiGate-VM01.pdf>.

## Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal located at <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 v5.0.9 support

The following table lists FortiOS v5.0.9 product integration and support information.

**Table 1:** FortiOS v5.0.9 support

<b>Web Browsers</b>	<ul style="list-style-type: none"><li>• Microsoft Internet Explorer versions 9 and 10</li><li>• Mozilla Firefox versions 24</li><li>• Google Chrome version 28</li><li>• Apple Safari versions 5.1 and 6.0</li></ul> Other web browsers may function correctly, but are not supported by Fortinet.
<b>FortiManager</b>	<ul style="list-style-type: none"><li>• 5.0.7 and later</li><li>• 5.2.0</li></ul>
<b>FortiAnalyzer</b>	<ul style="list-style-type: none"><li>• 5.0.6 and later</li><li>• 5.2.0</li></ul>
<b>FortiClient Microsoft and FortiClient Mac OS X</b>	<ul style="list-style-type: none"><li>• 5.0.9 or later</li></ul>
<b>FortiClient iOS</b>	<ul style="list-style-type: none"><li>• 5.0.2</li></ul>
<b>FortiClient Android</b>	<ul style="list-style-type: none"><li>• 5.0.4</li></ul>
<b>FortiAP</b>	<ul style="list-style-type: none"><li>• 5.0.8 build 0075 and later</li></ul> Supported models: FAP-11C, FAP-14C, FAP-28C, FAP-112B, FAP-210B, FAP-220A, FAP-220B, FAP-221B, FAP-222B, FAP-223B, FAP-320B The FAP-220A is supported on FortiAP v4.3.9 build 0228.
<b>FortiSwitch</b>	<ul style="list-style-type: none"><li>• 2.0.3 and later</li></ul> Supported models: FS-28C, FS-324B-POE, FS-348B, FS-448B
<b>FortiSwitch ATCA</b>	<ul style="list-style-type: none"><li>• 5.0.3 or later</li></ul> Supported models: FS-5003B, FS-5003A
<b>FortiController</b>	<ul style="list-style-type: none"><li>• 5.0.3 or later</li></ul> Supported models: FCTL-5103B The FCTL-5103B is supported by the FG-5001B and FG-5001C.

**Table 1:** FortiOS v5.0.9 support (continued)

<b>Fortinet Single Sign-On (FSSO)</b>	<ul style="list-style-type: none"> <li>FSSO 4.3 build 0157 <ul style="list-style-type: none"> <li>Microsoft Windows Server 2012 Standard Edition</li> <li>Microsoft Windows Server 2008 R2 64-bit</li> <li>Microsoft Windows Server 2008 (32-bit and 64-bit)</li> <li>Microsoft Windows Server 2003 R2 (32-bit and 64-bit)</li> <li>Novell eDirectory 8.8</li> </ul> </li> </ul> <p>FSSO does not currently support IPv6.</p>
<b>FortiExplorer</b>	<ul style="list-style-type: none"> <li>FortiExplorer 2.3 build 1052 or later.</li> </ul> <p>See the <a href="#">FortiExplorer v2.3 build 1052 Release Notes</a> for more information.</p>
<b>FortiExplorer iOS</b>	<ul style="list-style-type: none"> <li>FortiExplorer (iOS) 1.0.4 build 0118 or later.</li> </ul> <p>See the <a href="#">FortiExplorer (iOS) v1.0.4 build 0118 Release Notes</a> for more information.</p>
<b>AV Engine</b>	<ul style="list-style-type: none"> <li>5.155</li> </ul>
<b>IPS Engine</b>	<ul style="list-style-type: none"> <li>2.189</li> </ul>
<b>Virtualization Environments</b>	
<b>Citrix</b>	<ul style="list-style-type: none"> <li>XenServer version 5.6 Service Pack 2</li> <li>XenServer version 6.0 or later</li> </ul>
<b>Linux KVM</b>	<ul style="list-style-type: none"> <li>CentOS 6.4 (qemu 0.12.1) or later</li> </ul>
<b>Microsoft</b>	<ul style="list-style-type: none"> <li>Hyper-V Server 2008 R2, 2012 and 2012-R2</li> </ul>
<b>Open Source</b>	<ul style="list-style-type: none"> <li>XenServer version 3.4.3</li> <li>XenServer version 4.1 or later</li> </ul>
<b>VMware</b>	<ul style="list-style-type: none"> <li>ESX versions 4.0 and 4.1</li> <li>ESXi versions 4.0, 4.1, 5.0, 5.1 and 5.5</li> </ul>

## Language support

The following table lists FortiOS language support information.

**Table 2:** FortiOS language support

Language	Web-based Manager	Documentation
English	✓	✓
Chinese (Simplified)	✓	-
Chinese (Traditional)	✓	-
French	✓	-
Japanese	✓	-

**Table 2:** FortiOS language support

Language	Web-based Manager	Documentation
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 v5.0.9 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 3:** Supported modules and FortiGate models

AMC/FMC/FSM/RTM Module	FortiGate Model
Storage Module 500GB HDD Single-Width AMC (ASM-S08)	FG-310B, FG-620B, FG-621B, FG-3016B, FG-3810A, FG-5001A
Storage Module 64GB SSD Fortinet Storage Module (FSM-064)	FG-200B, FG-311B, FG-1240B, FG-3040B, FG-3140B, FG-3951B
Accelerated Interface Module 4xSFP Single-Width AMC (ASM-FB4)	FG-310B, FG-311B, FG-620B, FG-621B, FG-1240B, FG-3016B, FG-3810A, FG-5001A
Accelerated Interface Module 2x10-GbE XFP Double-Width AMC (ADM-XB2)	FG-3810A, FG-5001A
Accelerated Interface Module 8xSFP Double-Width AMC (ADM-FB8)	FG-3810A, FG-5001A
Bypass Module 2x1000 Base-SX Single-Width AMC (ASM-FX2)	FG-310B, FG-311B, FG-620B, FG-621B, FG-1240B, FG-3016B, FG-3810A, FG-5001A
Bypass Module 4x10/100/1000 Base-T Single-Width AMC (ASM-CX4)	FG-310B, FG-311B, FG-620B, FG-621B, FG-1240B, FG-3016B, FG-3810A, FG-5001A
Security Processing Module 2x10/100/1000 SP2 Single-Width AMC (ASM-CE4)	FG-1240B, FG-3810A, FG-3016B, FG-5001A
Security Processing Module 2x10-GbE XFP SP2 Double-Width AMC (ADM-XE2)	FG-3810A, FG-5001A

**Table 3:** Supported modules and FortiGate models (continued)

Security Processing Module 4x10-GbE SFP+ Double-Width AMC (ADM-XD4)	FG-3810A, FG-5001A
Security Processing Module 8xSFP SP2 Double-Width AMC (ADM-FE8)	FG-3810A
Rear Transition Module 10-GbE backplane fabric (RTM-XD2)	FG-5001A
Security Processing Module (ASM-ET4)	FG-310B, FG-311B
Rear Transition Module 10-GbE backplane fabric (RTM-XB2)	FG-5001A
Security Processing Module 2x10-GbE SFP+ (FMC-XG2)	FG-3950B, FG-3951B
Accelerated Interface Module 2x10-GbE SFP+ (FMC-XD2)	FG-3950B, FG-3951B
Accelerated Interface Module 20xSFP (FMC-F20)	FG-3950B, FG-3951B
Accelerated Interface Module 20x10/100/1000 (FMC-C20)	FG-3950B, FG-3951B
Security Processing Module (FMC-XH0)	FG-3950B

## SSL VPN support

### SSL VPN standalone client

FortiOS v5.0.9 supports the SSL VPN tunnel client standalone installer build 2303 for the following operating systems:

- Microsoft Windows 8.1 (32-bit & 64-bit), 8 (32-bit & 64-bit), 7 (32-bit & 64-bit), and XP SP3 in `.exe` and `.msi` formats
- Linux CentOS 5.6 and Ubuntu 12.0.4 in `.tar.gz` format
- Virtual Desktop in `.jar` format for Microsoft Windows 7 SP1 (32-bit)

The SSL VPN client for Microsoft Windows supports IPv6 addresses but the Linux clients support only IPv4 addresses.

The SSL VPN standalone client for Mac OS X is not released and FortiClient installer is provided for Mac OS X users.

## SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

**Table 4:** 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 28
Microsoft Windows 7 64-bit SP1	Microsoft Internet Explorer versions 8, 9, 10 and 11 Mozilla Firefox version 28
Linux CentOS version 5.6	Mozilla Firefox version 24
Linux Ubuntu version 12.0.4	Mozilla Firefox version 28
Mac OS X v10.9 Maverick	Apple Safari version 7

## SSL VPN host compatibility list

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

**Table 5:** 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 6:** 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	✓	✓
Panda Internet Security 2011	✓	✓
Sophos Security Suite	✓	✓

**Table 6:** Supported Windows 7 32-bit and 64-bit antivirus and firewall software (continued)

Product	Antivirus	Firewall
Trend Micro Titanium Internet Security	✓	✓
ZoneAlarm Security Suite	✓	✓
Symantec Endpoint Protection Small Business Edition 12.0	✓	✓

## Explicit web proxy browser support

- Microsoft Internet Explorer versions 8, 9, and 10
- Mozilla Firefox version 21
- Apple Safari version 6.0
- Google Chrome version 25

## Default Behavior/Config Change

The following table lists FortiOS default behavior/configuration change.

**Table 7:** FortiOS default behavior/configuration change

Bug ID	Description
247953	Add a default DHCP server for management port on FG-200D, FG-240D, FG-280D-POE, FG-100D and FG-140D.
247162	Hide switch controller on 600/800/1000 series.
246438	Change FG-30D default to full Web-based Manager.
246577	Configurable syslog server setting in the Web-based Manager for FG-3600C, FG-3950B, FG-3700D.
247321	Move URL match list into explicit proxy page.
188763	Improvement to default mesh SSID.

# Resolved Issues

The following issues have been fixed in FortiOS v5.0.9. For inquiries about a particular bug, please contact [Customer Service & Support](#).

## Web-based Manager

**Table 8:** Resolved Web-based Manager issues

Bug ID	Description
231885	Insufficient sanitization of TELNET and SSH usernames when displayed in the web administration interface

# Known Issues

The following issues have been identified in FortiOS v5.0.9. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

## FG-1500D and FG-3700D

**Table 9:** Known FG-1500D and FG-3700D issues

Bug ID	Description
242298	When the FortiGate unit is very busy with high CPU usage, IPsec VPN packets may be lost.
241646	Traffic may not be able to pass through a VLAN interface added to a link aggregation group (LAG) in a transparent mode VDOM. Workaround: Run <code>diagnose sniffer packet</code> on physical interface in the transparent VDOM or reboot the FortiGate unit.
242012	IPsec VPN traffic throughput is highly unstable. Workaround: this only happens on IPsec interface added to a 40G LAG. Do not use IPsec VPN over a 40G LAG.
240789	FG-3700D: LAG groups configured on low latency interfaces (port25 to port32) (NP6_0 and NP6_1) do not function correctly. Workaround: Only use either low-latency-mode or LAG for traffic on port25 to port32) (NP6_0 and NP6_1).
239968	IP tunneling (SIT tunnelling) not working when offload to NP6. Workaround: Disable <code>auto-asic-offload</code> in sit-tunnel configurations.
240945	Reply traffic is not offloaded when shared traffic shaping is enabled on policies for accelerated inter-VDOM links using the <code>npu_vdom</code> interface.

## FG-80D

**Table 10:** Known FG-80D issues

Bug ID	Description
235525	Link and speed LEDs remain <i>ON</i> on after shutting down the unit after shutting down the unit using the <code>execute shutdown</code> command.
239619	The r8168 driver is unable to shutdown power of the port and will keep the link of the other end in up state.

## FG-100D

**Table 11:** Known FG-100D issues

Bug ID	Description
232638	Allow option Endpoint Registration in <i>VPN &gt; SSL &gt; Config</i> deletes all firewall policies with <code>srcintf ssl.root</code> .

## FG-300D and FG-500D

**Table 12:** Known FG-300D and FG-500D issues

Bug ID	Description
239434	nTurbo for IPS acceleration fails to accelerate traffic. Fortinet recommends keeping this option set to the default value of <code>none</code> . <pre>config ips global   set np-accel-mode none end</pre>
238961	Link aggregation interfaces fail to come up. All members remain in <i>negotiating</i> status.
249324	NAT IPsec TCP traffic can not go through when <code>npu-offload</code> is enabled.
249996	FG-500D: Link status for ports 5,6,7 and 8 on the unit are unable to come up Work around: Set the speed of the ports to <code>1000full</code> first then switch it back to <code>auto</code> after the link has come up.

## WAN Optimization and explicit proxy

**Table 13:** Known WAN Optimization and explicit proxy issues

Bug ID	Description
0195564	Application control does not always work as expected for HTTPS traffic over the explicit web proxy.

## Upgrade

**Table 14:** Known upgrade issues

Bug ID	Description
0243960	Antivirus profile errors after upgrading from version 4.3

## Web-based Manager and CLI

**Table 15:** Known Web-based Manager issues

Bug ID	Description
0220652 0217222	The Web-based Manager may incorrectly display a permission error when entering an incorrect password.
172567	The vulnerability scanner appears in the Web-based Manager and CLI when the FortiGate unit is in transparent mode but the vulnerability scanner does not work in transparent mode.
254084	When using Microsoft Internet Explorer 9, new firewall policies are not displayed in the Policy page. The content pane toolbar is not displayed in this page.

# Limitations

This section outlines the limitations in FortiOS v5.0.9.

## 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 Xen limitations

When using 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.

