FortiOS v5.0 Patch Release 7
Release Notes

FortiOS v5.0 Patch Release 7

August 21, 2014

01-507-238147-20140821

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

Table of Contents

Change Log

Date	Change Description
August 21, 2014	Added FortiGateVoice section to “Supported models” on page 8
August 11, 2014	Added the FG-5001D to “Supported models” on page 8 Updated product integration section “FortiClient support (Windows, Mac OS X, iOS and Android)” on page 33
July 31, 2014	Update upgrade section “Upgrading from FortiOS v5.0 Patch Release 7 or later” on page 21
July 08, 2014	Added bug id 0243960 to the Upgrade issues.
June 06, 2014	Updated the build number for FG-300D, FG-500D and FG-1500D and added new models FG-60D-MC and FWF-60D-MC to “Supported models” on page 7.
May 26, 2014	Added the FG-1500D and 3700D to “Supported models” on page 7. Added the section “FortiGate-1500D and 3700D” on page 38. Added section “HA Virtual MAC Address Changes” on page 19.
May 15, 2014	Added the FG-80D to “Supported models” on page 7. Added the section “FortiGate-80D” on page 39.
May 9, 2014	Added the FG-300D and FG-500D to “Supported models” on page 7. Added the section “FortiGate-300D and FortiGate-500D nTurbo Support” on page 11. Added the section “FortiGate-100D” on page 39.
April 17, 2014	Added new build number for the FG-60D-POE, FWF-60D-POE, and FG-3600C to “Supported models” on page 7. Removed the FG-1500D and FG-3700D.
April 16, 2014	New format for listing supported FortiGate, FortiWiFi and FortiGate-VM models, build numbers and branch points. See “Supported models” on page 7. Added new build numbers and branch points for FG-30D, FG-60D, FWF-30D, FWF-30D-POE, FWF-60D, FG-90D, FG-90D-POE, FG-94D-POE, FG-1500D, and FG-3700D to “Supported models” on page 7. Corrected the CentOS and Unbutu Firefox version numbers in “SSL VPN web mode” on page 35. Added a note about IPv6 support to “SSL VPN standalone client” on page 35.

Date	Change Description
April 11, 2014	Added the FortiGate-200D to “Supported models” on page 7. Added FG-VM64-AWS to “FortiGate VM” on page 10.
April 9, 2014	Initial release.

Introduction

This document provides a summary of enhancements, support information, and installation instruction to upgrade your device to FortiOS v5.0 Patch Release 7. Please review all sections in this document prior to upgrading your device. For more information on upgrading your FortiOS device, see the *FortiOS 5.0 Handbook* at http://docs.fortinet.com.

This document includes the following sections:

Supported models

The models listed in the following sections are supported on FortiOS v5.0 Patch Release 7. For most models FortiOS v5.0 Patch Release 7 has build number 3608 and branch point 271. Some models are released on a special branch based off of FortiOS v5.0 Patch Release 7. As such they will have a different build number and possibly a different branch point.

From the GUI you can go to *System* > *Dashboard* > *Status* to confirm the Firmware Version build number. From the CLI, the output of the `get system status` command displays the build number and branch point.

FortiGate

Table 1: FortiGate models supported FortiOS v5.0 Patch Release 7

Model	Build Number	Branch Point
FG-20C FG-20C-ADSL-A	3608	271
FG-30D FG-30D-POE	4459	271
FG-40C FG-60C FG-60C-POE FG-60C-SFP	3608	271

Table 1: FortiGate models supported FortiOS v5.0 Patch Release 7 (continued)

Model	Build Number	Branch Point
FG-60D	4459	271
FG-60D-MC	4522	271
FG-60D-POE	4457	271
FG-80C FG-80CM	3608	271
FG-80D	4500	271
FG-90D FG-90D-POE	4459	271
FG-94D-POE	4458	271
FG-100D	4429	271
FG-110C FG-111C	3608	271
FG-140D FG-140D-POE	4429	271
FG-140D-POE-T1 FG-200B FG-200B-POE FG-200D FG-240D	3608	271
FG-200D-POE FG-240D-POE	4562	271
FG-280D-POE	4439	271
FG-300C	3608	271
FG-300D	4520	271
FG-310B FG-310B-DC FG-311B	3608	271
FG-500D	4520	271

Table 1: FortiGate models supported FortiOS v5.0 Patch Release 7 (continued)

Model	Build Number	Branch Point
FG-600C FG-620B FG-620B-DC FG-621B FG-800C FG-1000C FG-1240B	3608	271
FG-1500D	3763	271
FG-3016B FG-3040B FG-3140B FG-3240C	3608	271
FG-3600C	3483	271
FG-3700D	3745	271
FG-3810A FG-3950B FG-3951B FG-5001A FG-5001B FG-5001C FG-5101C	3608	271
FG-5001D	4625	271

FortiGate Rugged

FGR-100C (Build number 3608, branch point 271)

FortiWiFi

Table 2: FortiWiFi models supported FortiOS v5.0 Patch Release 7

Model	Build Number	Branch Point
FWF-20C FWF-20C-ADSL-A	3608	271

Table 2: FortiWiFi models supported FortiOS v5.0 Patch Release 7 (continued)

Model	Build Number	Branch Point
FWF-30D FWF-30D-POE	4459	271
FWF-40C FWF-60C FWF-60CM FWF-60CX-ADSL-A	3608	271
FWF-60D	4459	271
FWF-60D-MC	4522	271
FWF-60D-POE	4457	271
FWF-80CM FWF-81CM	3608	271
FWF-90D FWF-90D-POE	4459	271

FortiGate VM

Table 3: FortiGate VM models supported FortiOS v5.0 Patch Release 7

Model	Build Number	Branch Point
FG-VM32 FG-VM64	3608	271
FG-VM64-AWS	4456	271
FG-VM64-XEN FG-VM64-KVM FG-VM64-HV	3608	271

FortiSwitch

FS-5203B (Build number 3608, branch point 271)

FortiCarrier

FCR-3810A, FCR-3950B, FCR-5001A-DW, and FCR-5001B

FortiOS v5.0 Patch Release 7 FortiCarrier images are delivered upon request and are not available on the customer support firmware download page. See “Upgrading older FortiCarrier specific hardware” on page 14.

FortiGateVoice

FGV-70D4 (Build number 4637, branch point 271)

Special Notices

FortiGate-300D and FortiGate-500D nTurbo Support

The FortiGate-300D and FortiGate-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.

FortiGate-3600C hardware compatibility

FortiOS v5.0 Patch Release 6 contains a compatibility issue with certain FortiGate-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.

FortiGate-3600C units with part number P12090-03 and later must run FortiOS v5.0 Patch Release 6 or later and can't be downgraded to FortiOS v5.0 Patch Release 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 Patch Release 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 GA and 5.0 Patch Release 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 Patch Release 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 Patch Release 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

- To improve GUI performance, Section View is disabled in the firewall policy page if a large number of policies exist (231219)
- Increase the maximum number of certificates on FortiGate models 1000 and up (2U models) to 500.
- Increase 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 Patch Release 7, 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 Patch Release 7. 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 Patch Release 7. 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 Patch Release 7. 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.

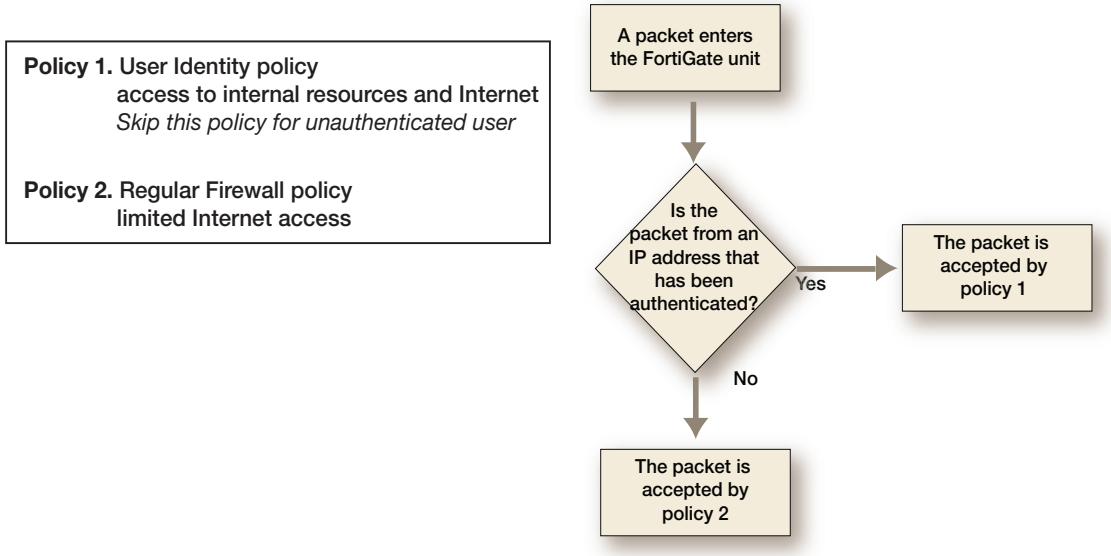
To support these different levels of access you can add a user identity policy to the top of the policy list that allows authenticated users to access internal resources and to have unlimited access to the Internet. In this policy, select *Skip this policy for unauthenticated user*.

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.

FortiGate 100D upgrade and downgrade limitations

The following limitations affect the FortiGate 100D model when upgrading from FortiOS v4.0 MR3 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 FortiGate 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 FortiGate 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 FortiGate 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 FortiGate 100D shipped with FortiOS v5.0.0 or later with a FortiGate 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
```

Upgrade Information

Upgrading from FortiOS v5.0 Patch Release 7 or later

FortiOS v5.0 Patch Release 7 officially supports upgrading from FortiOS v5.0 Patch Release 4 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 patch 7, if uninterruptable-upgrade is enabled you must always upgrade to FortiOS v5.0 Patch 4 before upgrading to patch 7. 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 4.3 and 5.0 interface indexing changed. After upgrading a cluster to FortiOS 5.0 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 v4.0 MR3 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 Patch Release 4, 5, 6, or 7

Policies that include interfaces that are members of a zone could be deleted when upgrading to FortiOS v5.0 Patch Release 4, 5, 6, or 7. As of patch release 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 Patch Release 7 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 Patch Release 7 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 Patch Release 7 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 Patch Release 7 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 Patch Release 7, 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 Patch Release 7.

Virtual switch and the FortiGate-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 Patch Release 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 5.0 Patch Release 5. If you have configured reserved IP/MAC addresses using this command, they will be lost when you upgrade to FortiOS 5.0 Patch Release 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 v4.0 MR3

FortiOS v5.0 Patch Release 7 officially supports upgrade from FortiOS v4.0 MR3 Patch Release 14 and v4.0 MR3 Patch Release 15.

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 Patch Release 7 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 Patch Release 7 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 MR3.

Example FortiOS v4.3 MR3 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
```

```
        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 Patch Release 7 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.

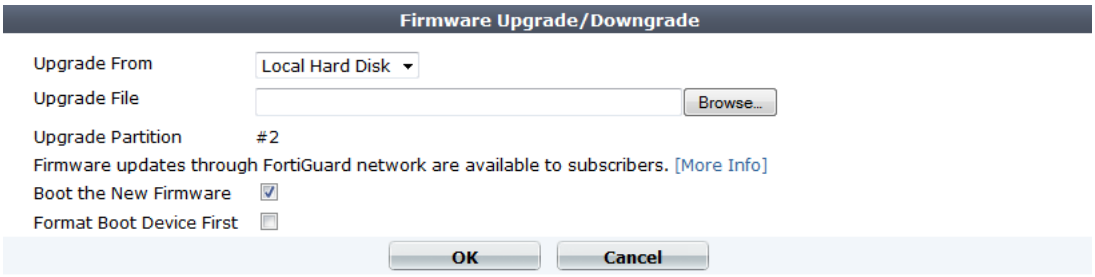
Save a copy of your FortiGate device configuration prior to upgrading. To backup your configuration, go to *System* > *Dashboard* > *Status*. In the *System Information* widget select *Backup* under *System Configuration*. Save the configuration file to your management computer.

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*.

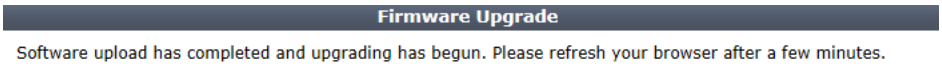
   The *Firmware Upgrade/Downgrade* window opens.

   Figure 2: Firmware upgrade/downgrade window



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.

   Figure 3: Firmware upgrade dialog box



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 Patch Release 7, 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.

Product Integration and Support

Web browser support

FortiOS v5.0 Patch Release 7 supports the following web browsers:

- Microsoft Internet Explorer versions 9 and 10
- Mozilla Firefox versions 24
- Google Chrome version 28
- Apple Safari versions 5.1 and 6.0

Other web browsers may function correctly, but are not supported by Fortinet.

FortiManager support

FortiOS v5.0 Patch Release 7 is supported by FortiManager v5.0 Patch Release 6.

FortiAnalyzer support

FortiOS v5.0 Patch Release 7 is supported by FortiAnalyzer v5.0 Patch Release 6.

FortiClient support (Windows, Mac OS X, iOS and Android)

FortiOS v5.0 Patch Release 7 is supported by the following FortiClient software versions:

- FortiClient (Windows) v5.0 Patch Release 7 or later
  - Microsoft Windows 8.1 (32-bit and 64-bit)
  - Microsoft Windows 8 (32-bit and 64-bit)
  - Microsoft Windows 7 (32-bit and 64-bit)
  - Microsoft Windows Vista (32-bit and 64-bit)
  - Microsoft Windows XP (32-bit)
- FortiClient (Mac OS X) v5.0 Patch Release 7 or later
  - Mac OS X v10.9 Mavericks
  - Mac OS X v10.8 Mountain Lion
  - Mac OS X v10.7 Lion

See the *FortiClient v5.0 Patch Release 7 Release Notes* for more information.

- FortiClient (iOS) v5.0 Patch Release 2.
- FortiClient (Android) v5.0 Patch Release 3.

FortiAP support

FortiOS v5.0 Patch Release 7 supports the following FortiAP models:

FAP-11C, FAP-14C, FAP-28C, FAP-112B, FAP-210B, FAP-220A, FAP-220B, FAP-221B, FAP-222B, FAP-223B, and FAP-320B

The FortiAP device must be running FortiAP v5.0 Patch Release 7 build 0064 or later.

The FAP-220A is supported on FortiAP v4.0 MR3 Patch Release 9 build 0228.

FortiSwitch support

FortiOS v5.0 Patch Release 7 supports the following FortiSwitch models:

FS-28C, FS-324B-POE, FS-348B, and FS-448B

The FortiSwitch device must be running FortiSwitchOS v2.0 Patch Release 3 or later.

FortiOS v5.0 Patch Release 7 supports the following FortiSwitch 5000 series models:

FS-5003B, FS-5003A

The FortiSwitch 5000 device must be running FortiSwitchOS v5.0 Patch Release 3 or later.

FortiController support

FortiOS v5.0 Patch Release 7 supports the following FortiController models:

FCTL-5103B

The FCTL-5103B is supported by the FG-5001B and FG-5001C. The FortiController device must be running FortiSwitch 5000 OS v5.0 Patch Release 3 or later.

Virtualization software support

FortiOS v5.0 Patch Release 7 supports the following virtualization software:

- VMware ESX versions 4.0 and 4.1
- VMware ESXi versions 4.0, 4.1, 5.0, 5.1 and 5.5
- Citrix XenServer versions 5.6 Service Pack 2 and 6.0 or later
- Open Source Xen versions 3.4.3 and 4.1 or later
- Microsoft Hyper-V Server 2008 R2 and 2012
- KVM - CentOS 6.4 (qemu 0.12.1) or later

See “About FortiGate VMs” on page 45 for more information.

Fortinet Single Sign-On (FSSO) support

FortiOS v5.0 Patch Release 7 is supported by FSSO v4.0 MR3 B0151 for the following operating systems:

- Microsoft Windows Server 2012 Standard Edition
- Microsoft Windows Server 2008 R2 64-bit
- Microsoft Windows Server 2008 (32-bit and 64-bit)
- Microsoft Windows Server 2003 R2 (32-bit and 64-bit)
- Novell eDirectory 8.8

FSSO does not currently support IPv6.

Other server environments may function correctly, but are not supported by Fortinet.

FortiExplorer support (Microsoft Windows, Mac OS X and iOS)

FortiOS v5.0 Patch Release 7 is supported by FortiExplorer v2.3 build 1052 or later. See the *FortiExplorer v2.3 build 1052 Release Notes* for more information.

FortiOS v5.0 Patch Release 7 is supported by FortiExplorer (iOS) v1.0.4 build 0118 or later. See the *FortiExplorer (iOS) v1.0.4 build 0118 Release Notes* for more information.

AV Engine and IPS Engine support

FortiOS v5.0 Patch Release 7 is supported by AV Engine v5.146 and IPS Engine v2.179.

Language support

The following table lists FortiOS language support information.

Table 4: FortiOS language support

Language	Web-based Manager	Documentation
English	✔	✔
French	✔	-
Portuguese (Brazil)	✔	-
Spanish (Spain)	✔	-
Korean	✔	-
Chinese (Simplified)	✔	-
Chinese (Traditional)	✔	-
Japanese	✔	-

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 Patch Release 7 supports Advanced Mezzanine Card (AMC), Fortinet Mezzanine Card (FMC), Rear Transition Module (RTM), and Fortinet Storage Module (FSM) removable modules. These modules are not hot swappable. The FortiGate unit must be turned off before a module is inserted or removed.

Table 5: Supported modules and FortiGate models

AMC/FMC/FSM/RTM Module	FortiGate Model
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
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

Table 5: Supported modules and FortiGate models (continued)

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 Patch Release 7 supports the SSL VPN tunnel client standalone installer build 2300 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
- Mac OS X v10.9, 10.8 and 10.7 in `.dmg` format
- Virtual Desktop in `.jar` format for Microsoft Windows 7 SP1 (32-bit)

Other operating systems may function correctly, but are not supported by Fortinet.

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

SSL VPN web mode

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

Table 6: 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

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

SSL VPN host compatibility list

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

Table 7: 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 8: 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	✔	✔
Trend Micro Titanium Internet Security	✔	✔
ZoneAlarm Security Suite	✔	✔
Symantec Endpoint Protection Small Business Edition 12.0	✔	✔

Explicit web proxy browser support

The following web browsers are supported by FortiOS v5.0 Patch Release 7 for the explicit web proxy feature:

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

Other web browsers may function correctly, but are not supported by Fortinet.

Resolved Issues

This chapter describes issues with past releases of FortiOS v5.0 that have been resolved for FortiOS v5.0 Patch Release 7. For inquires about a particular bug, please contact Customer Service & Support.

Resolved OpenSSL Issue in FortiOS v5.0 Patch Release 7

Table 9: Resolved SSL issue

Bug ID	Description
237976	The OpenSSL library used for the FortiOS GUI and for SSL VPN has been upgraded to the most recent version (openssl 1.0.1g). An information disclosure vulnerability has been discovered in OpenSSL version 1.0.1 up to 1.0.1f. This vulnerability may allow an attacker to access sensitive information from memory by sending crafted TLS heartbeat requests. This vulnerability has been fixed in openssl 1.0.1g.

Known Issues

This chapter describes some known issues with FortiOS v5.0 Patch Release 7. Some of the issues listed below were also known issues for FortiOS v5.0 Patch Release 5. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

FortiGate-1500D and 3700D

Table 10: Known FortiGate-1500D and 3700D issues

Bug ID	Description
242793	If a link aggregation group (LAG) includes physical interfaces attached to different NP6 processors and if you apply Application Control and Traffic Shaping to the traffic using the LAG group the FortiGate CPU usage may reach 100% and the FortiGate unit may stop responding.
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 `diagnose sniffer packet` on physical interface in TP 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. Don't use IPsec VPN over a 40G LAG.
240523	TCP traffic fails to pass through inter-VDOM links when NTurbo is enabled. Workaround: Disable `auto-asic-offload` in policies using inter-VDOM links.
240837, 240835, 240789	FortiGate-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 `auto-asic-offload` 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 npu_vdom interface.

FortiGate-80D

Table 11: Known FortiGate-80D issues

Bug ID	Description
235525	Link and speed LEDs remain “ON” on after shutting down the unit 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 up state.

FortiGate-100D

Table 12: Known FortiGate-100D issues

Bug ID	Description
232638	Allow option "Endpoint Registration" in VPN - SSL - Config deletes all firewall policies with srcintf "ssl.root".

FortiGate-300D and FortiGate-500D

Table 13: Known FortiGate-300D and FortiGate-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 `none`.
	`config ips global`
	`  set np-accel-mode none`
	`end`

238961	Link aggregation interfaces fail to come up. All members remain in *negotiating* status.
239485	Redundant interfaces do not work until the FortiGate-300D or 500D unit is rebooted. Workaround: reboot the FortiGate-300D or 500D unit after adding redundant interfaces.

FortiSwitch

Table 14: Known FortiSwitch issues

Bug ID	Description
220692	Traffic may be interrupted if you have created two physical links between a managed FortiSwitch and a FortiGate acting as the manager but only configured one of the links as an aggregate link member. Workaround: Remove one of the links or configure both of them.

WAN Optimization and explicit proxy

Table 15: 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 16: Known Upgrade issues

Bug ID	Description
0227984	FortiGate units with NP4 processes running in Transparent Mode may experience a Transparent mode L2 loop when upgrading to FortiOS 5.0 Patch Release 6. Workaround: Set the npu-vlink interface to be administratively down before upgrading to FortiOS 5.0 Patch 6. FortiOS 4.3 firmware does not support setting the npu-vlink interface down. In this case you should upgrade to a FortiOS 5.0 patch 4 and set the npu-vlink interface to be administratively down and then upgrade to FortiOS 5.0 Patch 6.
0243960	Antivirus profile errors after upgrade from 4.3

Web-based Manager

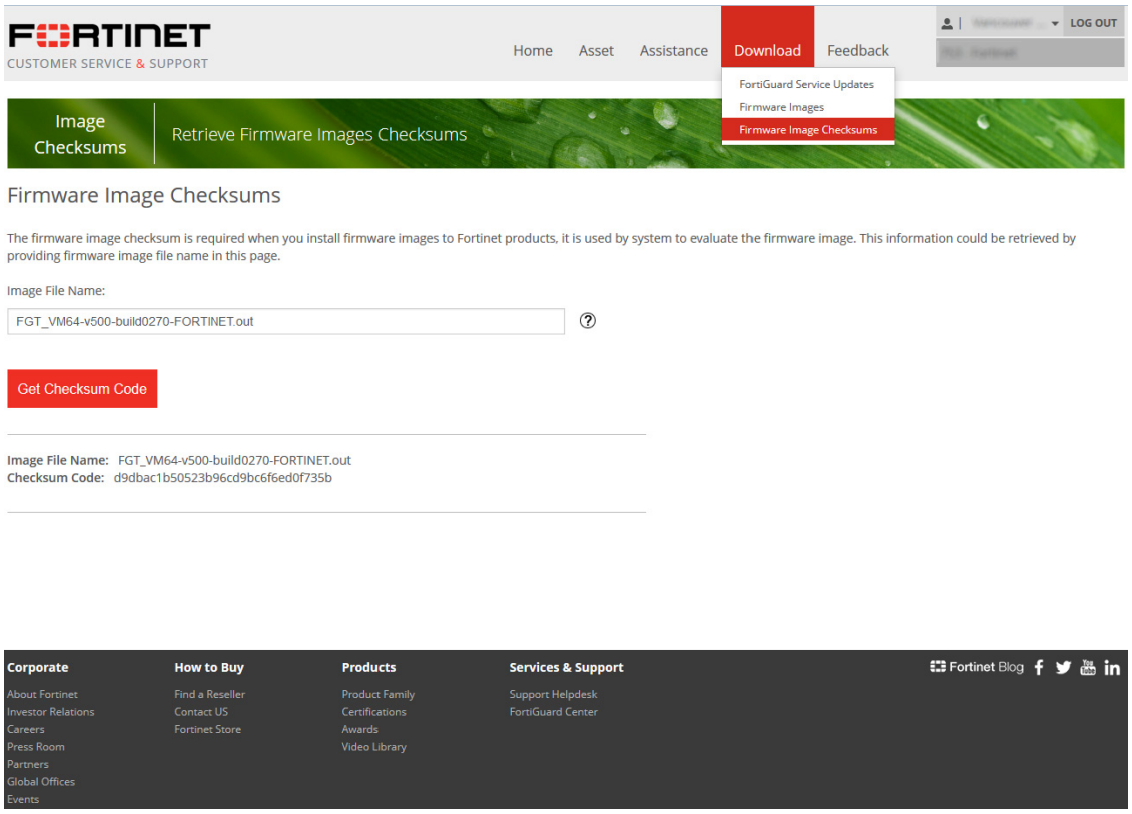
Table 17: Known Web-based Manager issues

Bug ID	Description
0220652 0217222	The Web-based Manager may incorrectly display a permission error when entering an incorrect password.

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. After logging in, select *Download* > *Firmware Image Checksum*, enter the image file name including the extension, and select *Get Checksum Code*.

Figure 4: Firmware image checksum tool



Limitations

This section outlines the limitations in FortiOS v5.0 Patch Release 7.

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.

Appendix A: About FortiGate VMs

FortiGate VM model information

Table 18: FortiGate VM model information

Technical Specification	VM-00	VM-01	VM-02	VM-04	VM-08
Virtual CPUs	1	1	1 or 2	1 to 4	1 to 8
Virtual Network Interfaces	2 to 10				
Memory Requirements (GB)	1	2	4	6	12
Storage	30 GB to 2 TB				
VDOMs	1	10	25	50	500
CAPWAP Wireless Access Points	32	32	256	256	1024
Remote Wireless Access Points	32	32	256	256	3072

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.

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`.

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.