FortiOS v5.0 Patch Release 4
Release Notes

FortiOS v5.0 Patch Release 4 Release Notes

February 5, 2014

01-504-211272-20140205

Copyright© 2014 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance 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 the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. 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.

Technical Documentation	docs.fortinet.com
Video Guides	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
2014-02-05	Re-wrote the following two sections so that they are the same for FortiOS Release 5.0 Patches 4, 5 and 6: • "Disk logging disabled by default on some models (Log to FortiCloud instead)" on page 12 • "FG-60D/FWF-60D logging to disk" on page 13
2013-11-22	Added FG-60D-POE and FWF-60D-POE to "Supported models" on page 7.
2013-08-27	Added known issue "214643" on page 47.
2013-08-23	Added known issue "214935" on page 47.
2013-08-16	Renamed section "Upgrading from FortiOS v5.0 Patch Release 2 or later" on page 16. Corrected the description of resolved issue "203063" on page 37.
2013-08-09	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 4 build 0228. 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 following models are supported on FortiOS v5.0 Patch Release 4.

FortiGate

FG-20C, FG-20C-ADSL-A, FG-30D, FG-40C, FG-60C, FG-60C-POE, FG-60D, FG-80C, FG-80CM, FG-90D, FGT-90D-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-300C, FG-310B, FG-310B-DC, FG-311B, FG-600C, FG-620B, FG-620B-DC, FG-621B, FG-800C, FG-1000C, FG-1240B, FG-3016B, FG-3040B, FG-3140B, FG-3240C, FG-3810A, FG-3950B, FG-3951B, FG-5001A, FG-5001B, FG-5001C, and FG-5101C.

FG-3600C

This model is released on a special branch based off of FortiOS v5.0 Patch Release 4. As such, the build number found in the *System* > *Dashboard* > *Status* page and the output from the `get system status` CLI command displays `6311` as the build number.

To confirm that you are running the proper build, the output from the `get system status` CLI command has a `Branch point` field that should read `0228`.

FG-60D-POE and FWF-60D-POE

These models are released on a special branch based off of FortiOS v5.0 Patch Release 4. As such, the build number found in the *System* > *Dashboard* > *Status* page and the output from the `get system status` CLI command displays `4350` as the build number.

To confirm that you are running the proper build, the output from the `get system status` CLI command has a `Branch point` field that should read `0228`.

FortiGate Rugged

FGR-100C

FortiWiFi

FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-80CM, FWF-81CM, FWF-90D, and FWF-90D-POE.

FortiGate VM

FG-VM32, FG-VM64, and FG-VM64-XEN.

FortiSwitch

FS-5203B.

See http://docs.fortinet.com/fgt.html for additional documentation on FortiOS v5.0.

Summary of enhancements

The following is a list of enhancements in FortiOS v5.0 Patch Release 4 build 0228.

Not all features/enhancements listed below are supported on all models.

FortiGate VM

- Can include one managed access point with the 15-day embedded evaluation license.

Firewall

- Configure a security policy to send a TCP reset when a specific application session times out.

```
config firewall policy/policy6
  edit 0
    set timeout-send-rst {disable | enable}
```

- Support the FortiSandbox product for sandbox inspection.

IPsec

- Dial-up IPsec VPN wizard for FortiClient and the built-in iOS IPsec client.
- Support multiple L2TP/IPSec clients behind a NAT device.

System

- Display last successful and last failed administrator login attempts.
- Configurable idle timeout for console sessions (RS-232 and USB).
- Add spanning tree support to the FortiGate 100D and 140D when managing remote FortiSwitch units.

- IPoA support for DSL based devices.

Routing

- IPv6 packets can be filtered according to existing extension headers in the packets. using the command `configure firewall ipv6-eh-filter`.

User authentication

- You can configure up to four accounting servers for each RADIUS server. User accounting messages are sent to all of the accounting servers.

Wireless

- Addition of the wireless health monitor.

FortiClient

- New scheme for FortiClient to detect the existence of a FortiGate unit.

Logging & Report

- Merged Invalid Packet log into Local or Forward Traffic log.

CLI

- From the CLI you can use a contextual grep command when showing the configuration to display specific configuration details. The following example shows how to show a security policy that contains the gaming console device group:

```
show firewall policy | grep -f gaming
  config firewall policy
    edit 36
      set srcintf "any"
      set dstintf "any"
      set srcaddr "all"
      set action accept
      set comments "device identity"
      set identity-based enable
      set identity-from device
      set nat enable
        config identity-based-policy
          edit 1
            set schedule "schrec1"
            set logtraffic all
            set dstaddr "any-a1"
            set service "ALL_ICMP"
            set action deny
            set devices "devg1" "gaming-console" <---
          next
      end
  next
end
```

Web-based Manager

- Logs sent to a FortiAnalyzer or FortiManager unit from a FortiGate unit can be encrypted.
- Apply the same AP profile to multiple managed APs in one step.
- The Log monitor has been renamed the Log Volume monitor, and now displays log data more effectively.
- Log viewer improvements.
- Policy-based IPsec can be hidden on the Web-based Manager.
- Dynamic VLANs can now be used to divide a single SSID into several VLANs. In Patch 4 Dynamic VLANs are supported for both tunnel and bridge mode SSIDs.
- Explicit web proxy traffic can be load balanced among multiple forwarding servers.
- IPv6 NAT GUI Extensions for following features (IPv6 IP Pool, VIP6/VIP64/VIP46, VIPGRP6/VIPGRP64/VIPGRP46, NAT64 Policy, NAT.
- Policies and Virtual IPs for NAT46 and NAT64 can now be configured from the web-based manager. For these options to appear in the web-based manager, this feature must be enabled using Feature Select.
- Administrators can now add web filtering overrides that affect all web filtered traffic.
- Enhancements to security policy list contextual menus.
- Added the extended version of the top utility.
- Improved “member” display in lists.
- More filter options for IPS and Application Control.
- Added ability to clone ATP/WF/IPS/AC profiles.

Special Notices

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.

Default setting/CLI changes

The VIP and VIP64 maximum value has been changed to 512 on desktop FortiGate models.

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 4, 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 4. 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 4. 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 4. The DLP rule settings have been moved inside the DLP sensor.

ID-based firewall policy

If you have enabled `fall-through-unauthenticated` in the identity-based policy, the following logic will apply:

- For unauthenticated users: if none of the accepted policies are matched and an identity-based policy has been hit, the normal authentication process will be triggered based on specific settings.
- For authenticated users: if an identity-based policy is matched, the traffic will be controlled by this policy. If none of the sub-rules are matched, the traffic will get dropped.

To enable/disable `fall-through-unauthenticated` in the identity-based policy, enter the following CLI command:

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

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 2 or later

FortiOS v5.0 Patch Release 4 build 0228 officially supports upgrade from FortiOS v5.0 Patch Release 2 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.

Captive portal

The captive portal configuration has changed in FortiOS v5.0 Patch Release 4 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 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 4 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 4 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 4 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 4, 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 FortiGate 60C variants and lower models only one SSL VPN web portal is retained after upgrading to FortiOS v5.0 Patch Release 4.

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.

Upgrading from FortiOS v4.0 MR3

FortiOS v5.0 Patch Release 4 build 0228 officially supports upgrade from FortiOS v4.0 MR3 Patch Release 12 and v4.0 MR3 Patch Release 14.

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 4 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 4 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 4 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.

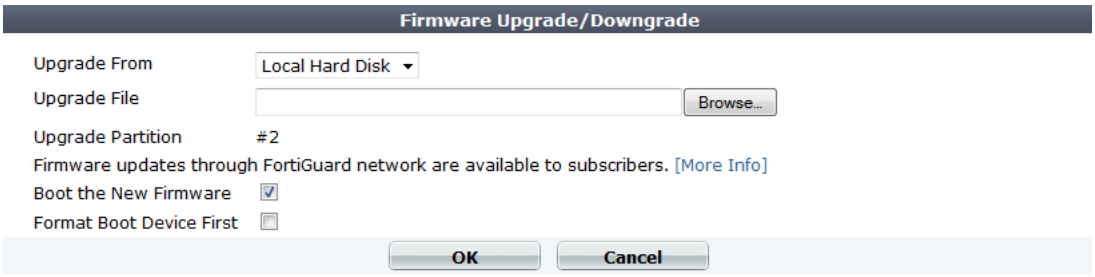
Save a copy of your FortiGate device configuration prior to upgrading. To backup your configuration, go to *System* > *Dashboard* > *Status*. In the *System Information* widget select *Backup* under *System Configuration*. Save the configuration file to your management computer.

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*.

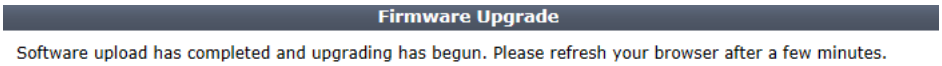
   The *Firmware Upgrade/Downgrade* window opens.

   Figure 1: 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 2: 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/fgt50.html.

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 4 supports the following web browsers:

- Microsoft Internet Explorer versions 8 and 9
- Mozilla Firefox versions 21
- Google Chrome version 25
- 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 4 is supported by FortiManager v5.0 Patch Release 4 or later.

FortiAnalyzer support

FortiOS v5.0 Patch Release 4 is supported by FortiAnalyzer v5.0 Patch Release 4 or later.

FortiClient support

FortiOS v5.0 Patch Release 4 is supported by the following FortiClient software versions:

- FortiClient (Windows) v5.0 Patch Release 5 or later
  - Windows 8 (32-bit and 64-bit)
  - Windows 7 (32-bit and 64-bit)
  - Windows Vista (32-bit and 64-bit)
  - Windows XP (32-bit)
- FortiClient (Mac OS X) v5.0 Patch Release 5 or later
  - Mac OS X v10.8 Mountain Lion
  - Mac OS X v10.7 Lion
  - Mac OS X v10.6 Snow Leopard

See the *FortiClient v5.0 Patch Release 5 Release Notes* for more information.

FortiClient iOS support

FortiOS v5.0 Patch Release 4 is supported by FortiClient (iOS) v5.0 Patch Release 1.

FortiAP support

FortiOS v5.0 Patch Release 4 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 5 build 0047 or later.

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

FortiSwitch support

FortiOS v5.0 Patch Release 4 supports the following FortiSwitch model:

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

The FortiSwitch device must be running FortiSwitchOS v2.0 Patch Release 2 build 0010 or later.

FortiController support

FortiOS v5.0 Patch Release 4 supports the following FortiController models:

FCTL-5103B

The FCTL-5103B is supported by the FG-5001C.

Virtualization software support

FortiOS v5.0 Patch Release 4 supports the following virtualization software:

- VMware ESX versions 4.0 and 4.1
- VMware ESXi versions 4.0, 4.1, 5.0, and 5.1
- Citrix XenServer versions 5.6 Service Pack 2 and 6.0
- Open Source Xen versions 3.4.3 and 4.1

See “FortiGate VM” for more information.

Fortinet Single Sign-On (FSSO) support

FortiOS v5.0 Patch Release 4 is supported by FSSO v4.0 MR3 B0142 for the following operating systems:

- Microsoft Windows Server 2012 Standard Edition
- Microsoft Windows Server 2008 (32-bit and 64-bit)
- Microsoft Windows Server 2008 R2 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 (Microsoft Windows/Mac OS X) support

FortiOS v5.0 Patch Release 4 is supported by FortiExplorer v2.3 build 1052 or later. See the *FortiExplorer v2.3 build 1052 Release Notes* for more information.

FortiExplorer (iOS) support

FortiOS v5.0 Patch Release 4 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 4 is supported by AV Engine v5.146 and IPS Engine v2.161.

Language support

The following table lists FortiOS language support information.

Table 1: 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 4 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 2: 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

Table 2: Supported modules and FortiGate models (continued)

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 Patch Release 4 supports the SSL VPN tunnel client standalone installer build 2292 for the following operating systems:

- Microsoft Windows 8, Windows 7, and Windows XP in `.exe` and `.msi` formats
- Linux CentOS and Ubuntu in `.tar.gz` format
- Mac OS X v10.7 Lion in `.dmg` format
- Virtual Desktop in `.jar` format for Microsoft Windows 7

Table 3: Supported operating systems

Operating System Support		
Microsoft Windows 8 64-bit	Linux CentOS version 5.6	Mac OS X v10.7 Lion
Microsoft Windows 8 32-bit	Linux Ubuntu version 12.0.4	
Microsoft Windows 7 64-bit		
Microsoft Windows 7 32-bit		
Microsoft Windows XP SP3		
Virtual Desktop Support		
Microsoft Windows 7 32-bit SP1		

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

SSL VPN web mode

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

Table 4: Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 32-bit SP1	Microsoft Internet Explorer versions 8, 9, and 10 Mozilla Firefox version 19
Microsoft Windows 7 64-bit SP1	Microsoft Internet Explorer versions 8, 9 and 10 Mozilla Firefox version 19
Linux CentOS version 5.6 and Ubuntu version 12.0.4	Mozilla Firefox version 3.6
Mac OS X v10.7 Lion	Apple Safari version 6

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

SSL VPN host compatibility list

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

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	✔	✔

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

Product	Antivirus	Firewall
Panda Internet Security 2011	✔	✔
Sophos Security Suite	✔	✔
Trend Micro Titanium Internet Security	✔	✔
ZoneAlarm Security Suite	✔	✔
Symantec Endpoint Protection Small Business Edition 12.0	✔	✔

Explicit web proxy browser support

The following web browsers are supported by FortiOS v5.0 Patch Release 4 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

The resolved issues tables listed below do not list every bug that has been corrected with FortiOS v5.0 Patch Release 4 build 0228. For inquires about a particular bug, please contact Customer Service & Support.

Email Filtering

Table 7: Resolved email filtering issues

Bug ID	Description
207401, 206338	SMTP proxy with terminator could cause splice mode to not work and also impact performance.
210979	Incorrect SMTP spam tag insertion on multi-line non-ASCII subjects.

Data Loss Prevention

Table 8: Resolved data loss prevention issues

Bug ID	Description
160386	DLP regex on URL encoded posts.
211429	Exif-JPEG file not recognized by DLP sensors.

ELBC

Table 9: Resolved ELBC issues

Bug ID	Description
194406	Fabric interfaces (internal and external) do not show correct statistics.
203229	Prevent ELBC mode related changes before the user has confirmed an ELBC mode change.
207002	Standalone session sync failed when a blade is rebooted and a new session is created.
208202	The `confsynchbd` daemon crashes on ForitGate when a static trunk is created on FortiController.

Endpoint Control

Table 10: Resolved endpoint control issues

Bug ID	Description
207101	FortiGate cannot detect Android OS when registered over Endpoint Control.
208387	FortiGate will not send the portal page to the client if Endpoint Control is enabled in the SSL VPN firewall policy.

Firewall

Table 11: Resolved firewall issues

Bug ID	Description
143961	FortiGate in HA A-A mode failed to connect with an ICAP server when the traffic falls on the slave FortiGate.
169930	Fix inaccurate DoS policy counters.
196907, 208885	SSL exempt problems when SSL `inspect-all` is enabled and SSL server-name cache.
201003	FortiGate unable to install full firewall policy when the firewall policy's address range has exceed the system size limit.
203335 204081	Fix VIP health check session is blocked because of extra ICMP reply packets that trigger the anti-reply function.
204388	FortiGate continues to increment duration in the Traffic log even though the session does not exists anymore after session timeout.
204398	Correct user credentials are required to input twice after wrong user name and password are input with `auth-http-basic` enabled.
205931	H.225 RAS's location requests are not natted by `session-helper` in the IP address field.
208630	Unable to set the broadcast address in the multicast address configuration.
208759	The `authd` daemon may experience high CPU usage for a long time if there are hundreds of firewall policies.
209370	Traffic can pass device based firewall policies when an empty device group is used.
210438	FortiGate keeps using IPsec VPN to connect to FortiAnalyzer after setting encrypt to disable.
211790	Port number is missing in the redirected URL after authentication on non-standard HTTP port with auth-secure-http enabled.

FortiCarrier

Table 12: Resolved FortiCarrier issues

Bug ID	Description
207312	MIME header parsing when no whitespace exists after the colon following the field name.
208181	FortiGate blocks traffic when `set remove-blocked` is enabled in the MMS profile.
208510	HTTP header parsing for MMS message address header.
208554	Console prints MMS error message in CLI when browsing in the MMS monitor Web-based Manager pages.

FortiGate VM

Table 13: Resolved FortiGate VM issues

Bug ID	Description
203649	Fix SSL VPN crash for FortiGate VM when using client certificate.

FortiGate 60D/FortiWiFi 60D

Table 14: Resolved FortiGate 60D/FortiWiFi 60D issues

Bug ID	Description
207759	SSL connection reset on FortiGate 60D and FortiWiFi 60D with RC4 Cipher Suite.

High Availability

Table 15: Resolved high availability issues

Bug ID	Description
201820	Ping traffic for `gwdetect` stops when HA failover occurs with vcluster.
204785	Fix hasysnc communication stop when socket is not closed properly and caused the hasync process unable to open new socket connection.
206258	Static route6 might not be restored after HA failover on the new master if there are IKE routes to be added through ZebOS.
208006	Cannot set MAC address of ethernet inter-VDOM link when HA is enabled.
208454	IPsec tunnel synced to the slave is not correct if NATT is enabled.
209296	The interface's IPv6 link-local address is incorrect after an HA failover.
209270	Fix MD5 authentication breaks after a HA failover.

Table 15: Resolved high availability issues (continued)

Bug ID	Description
210611	The `set gratuitous-arps disable` command does not take effect after rebooting the master when the HA configuration is set to transparent mode.

208928	Fix standalone session sync for set service filter does not exist for v5.0.
	`config system sesssion-sync`
	`edit 0`
	`config filter`
	`config custom-service`
	`edit 0`
	`set src-port-range 8080-8090`
	`set dst-port-range 8080-8090`
	`end`
	`end`

IPS

Table 16: Resolved IPS issues

Bug ID	Description
191529	Beta signature triggering should not be affected in quarantine action in the IPS Sensor.
207995	IPS extended database reloading issue after FortiGate reboot.
208231	IPSA compiler code does not check the number of rules added against the CP8 hardware limit.
208649	IPS Engine memory leak when configuration is changed.
210949	Fix XLP unable to support DOS anomaly periodical mode.
Multiple	Fix traffic flow issues for the nturbo enabled platforms (FortiGate-3240C and FG-3600C) if the number of IPS engines is changed, or nturbo is switched on or off. Bug ID: 209735, 209732, 190277, 200967, 200420, 200436

IPsec VPN

Table 17: Resolved IPsec VPN issues

Bug ID	Description
203063	Invalid SPI message appears during key-renewal when IPsec processing is offloaded by an NP4 processor.
205107	Restore ability to support IKE round-robin DDNS.
209002	DHCP relay over IPsec in interface mode does not function correctly.
209562	Failed to rekey IKE sa with strongSwan if both IPsec SA and IKE SA expire.

Table 17: Resolved IPsec VPN issues (continued)

Bug ID	Description
209570	FortiGate does not re-transmit SA_INIT_RESPONSE when detecting re-transmit SA_INIT.
209966	OSFP one way traffic over point-to-point IPsec VPN with npu-offload enabled on SoC2 FWF-60D.
210540	Fix crypto errors that occurred when using aggregate mode.
211649	FortiOS IKE v2 keeps rekeying with strongSwan.
211879	Fix IPsec dev index is wrong after changing phase1 interface to loopback.

Logging and Reporting

Table 18: Resolved logging and reporting issues

Bug ID	Description
175029	SSH proxy logs are not displayed in the Web-based Manager.
194888	Restore the `diag log test` command to the previous behavior.
197709	The IPS packet log is not sent to the VDOM FortiAnalyzer override when all 3 global FortiAnalyzer servers are disabled.
203039	The event log format in relating to uploading disk logs related log event.
207154	FortiGate will not upload logs when the FTP server replies the login banner message.
207986	The Threat History widget does not display the IPS attack name, application name or website URL in the threat field.
208035	The Threat History widget show type as IPS for matching geo-location traffic.
208110	The wrong `src-ip` field is sent for the av-analytics in explicit web proxy.
209975	Reliable log sent to the FortiAnalyzer is not encrypted when `enc-algorithm` is enabled.
213662	Add Attack ID and Virus ID field to traffic log for proxy base.
Multiple	Several report related bug fixes. Bug ID: 187478, 197955, 200081, 202736, 203281, 203285, 206385, 208465, 209061, 210006.

Routing

Table 19: Resolved routing issues

Bug ID	Description
205789	Issue with the `diag ip router pim-sm level info` command; unable to `set pim-sm debug level` to `info`.
208344	OSPFv3 area 0.0.0.0 should not allow to set to type nssa or stub.
213798	Fix bgpd segmentation fault crash if `diag ip router bgp nsm enable` and bfd is enabled for bgp.

SSL VPN

Table 20: Resolved SSL VPN issues

Bug ID	Description
201423	Unable to login to OWA 2013 in SSL VPN web mode.
204649	Parser for CMS portal in SSL VPN web mode.
206185	Unsigned application warnings when running RPD applet on newest Java update.
207410	Web page has no scroll bar in SSL VPN web mode.
208431	The password for SSL VPN RDP personal bookmark will be lost when edit the bookmark.
205356	Fix cannot connect to SSL VPN portal when subnet overlap is enabled and two interfaces have same IP address.
206606	Fix unable to open specific page on FortiAnalyzer page in SSL VPN web mode.
208600	SSL VPN client cannot login when the user belongs two user groups in the identity based policy in the ssl.root interface.
209779	SSL VPN stops working after ping over connection tool to domain name.
210509	Fix SSL VPN leaks memory in SSL VPN web mode.
211470	Fix SSL VPN portal automatic SSO for SMB bookmark authentication fails for non DC shared.
211153	Fix Firefox version 22 does not show tunnel mode on and SSL VPN portal.
212074	Fix SSL VPN web tunnel does not work under Google Chrome.

System

Table 21: Resolved system issues

Bug ID	Description
169930	Fix inaccurate DoS policy counters.
174959	Syn proxy feature does not work for XG2 NPU-cascade mode.
185027	The loopback interface should not be listed as an interface type candidate in TP mode.
194199	Statistics errors in FSSO polling feature.
195661	ForitGate does not check the firewall service when a user restores an invalid service such as `any` in the configuration.
195970	B0147: SSL VPN portal bookmarking isn't limited. For more information, see *Maximum Values Table for FortiOS 5.0*.
197237	Analytics stays on when switching antivirus to flow-based.
201905	Unable to telnet to FortiAP if telnet-admin-port setting is modified.
202955	Excessive memory usage by the dhcpd daemon causes the FortiGate to enter conserve mode.
203068	Limit `exec` commands for read_only administrators.
203203	The `dhcpd` daemon consumes high CPU usage and stops leasing DHCP addresses.
203549	Update the maximum number of load balance virtual and real servers. For more information, see *Maximum Values Table for FortiOS 5.0*.
203871	Kernel error info is outputted and crashes after executing the `diag sys modem com` command.
204475	The logging function is not enabled for pre-defined UTM profiles in FIPS-CC mode.
204525	Fix 802.1X and spanning tree does not work on FWF-60D/FG-60D models.
204757	Fix remote logging to faz stop working when primary connection fail in dual wan scenario.
205268	CRL commands are not adding double quotes when sending to FortiManager devices, so the FortiManager unit cannot check in updated CRLs.
206175	Proxy generated packets should not be sent out if the session is not available.
206966	FCS/MTU error occurs using `100half fixed` setting on NP interfaces.
207021	FortiGate allows the creation of a VDOM with an invalid VDOM name and is unable to delete it afterwards.
207147	Static ARP entry is not able to be created with a software switch interface.
207199	Support local CRL check in LDAPS authentication.

Table 21: Resolved system issues (continued)

Bug ID	Description
207356, 207608	AMC-XE2 will block traffic if UTM (Application Control) is enabled in an IPv6 IPsec policy.
207507	H.323 call drops when the session is removed from the session table.
207572	Fix Unit crash intermittently with no crashdump.
207615	FortiGate is unable to forward traffic and console access when locked by the `newlic` process.
207745	FortiGate hang caused by restoring a configuration file with non-existent interfaces in the firewall policy.
207814	Fix secondary IP still works after changing the interface mode to DHCP
207952	Not generate *disk failure is imminent* event log when SMART is not supported.
208233	High `miglogd` daemon CPU usage caused when `miglogd` sends hostname sync messages when slave does not exist.
208353	Fix FortiGate is unable to establish link when setup with MS-CHAP v1.
208528	Fix multicast lag session are not redistributed after a port member changed from up to down.
208565	Incorrect USB Modem information is being displayed on the Web-based Manager widget and in the CLI for the FG-3810A and FCR-3810A.
208626	FortiGate's USB auto-install always works even when it is disabled.
208636	Fix the link status is not updated after physical device has turned off for NP4 platform.
208901	The ForitGate unit is unable to send update requests for FortiGuard AV and IPS services when it encounters SSL connection errors or is stuck while installing updates.
208908	DNS64 proxy does not always resolve DNS queries properly.
209008	IPSA failure after updating the signature while passing traffic.
209337	IPS database update SNMP trap is always triggered when there was no IPS related updates.
209366	The mgmt interface can be selected in a multicast policy after it has been dedicated to management only.
209398	DHCP replay over IPsec does no work properly while adding or modifying DHCP server.
209439	Traffic history value is not shown for FortiGate-3950B 1G ports.
209957	The FortiGate unit failed to use FAT32 formatting for a storage size above 2GB.

Table 21: Resolved system issues (continued)

Bug ID	Description
210173	The snmpwalk fails at the end with an invalid child entry when querying against FORTINET-FORTIGATE-MIB::fgHwSensors.
210246	The FortiGate unit generates inaccurate event logs during a scheduled update.l
210340	Synproxy does not work with a XH0 lag on a FortiGate-3950B
210708	Intermittent high CPU usage of newcli process.
210710	Fix GRE tunnel stop passing traffic caused by PPPOE renew/flapping.
211231	Fix FortiCarrier license overwrites other factory licenses.
211313	Huawei E367 USB 3G modem disconnects when receiving an lAT&V command.
211431	System interface VLAN gets deleted after executing factoryreset2.
211432	Should not be able to add a Firewall Address with Non-UTF8 characters.
211441	sflow interface index issue.
211594	`show full-configuration` CLI command gives duplicate entries.
212160	The FortiGate unit does not flush the routing cache when firewall ippool is changed.
212257	If the traffic to CPU is too high, the CPU will be always busy processing packets and left no cpu cycles for other tasks.
212626	AirCard 340U not dialing.
212695	Iegbe network driver resports RX/TX counters as 32 bit integers.
212792	FortiGate source NAT Interface does not reply Ident RST packet when ident accept is disable.
214251	Newcli crashed when adding the interface to SP3-port.

Upgrade

Table 22: Resolved upgrade issues

Bug ID	Description
167269	The new modem version is overridden after a firmware upgrade.
204831	The IPS extended database is always reset to null during a firmware upgrade.
205791	The `dlp-sensor` configuration is changed after the first reboot of a firmware upgrade.
206822	When upgrading from build 0179, extend-db stops working until the user either manually updates or schedules an update.

Table 22: Resolved upgrade issues (continued)

Bug ID	Description
208321	When upgrading from v4.0 MR3 the web filter UTM log setting will be disabled (`extend-utm-log` and `http-url-log`) regardless of the setting before upgrading.
208740	Mobile FortiToken keys get rejected after upgrading.
209842	Pantech UML290 modem stopped working after upgrade from v5.0 Patch Release 2 to v5.0 Patch Release 3.

WAN Optimization and Explicit Web and FTP Proxy

Table 23: Resolved WAN optimization and explicit proxy issues

Bug ID	Description
187729	Firewall policies with webcache and inspect-all enabled can be lost after rebooting.
207310	Enabled PAC file download by bypassing DNS lookup when the host header of HTTP request matches `proxy-fqdn`.
209029, 209825, 210703	A wad segmentation fault occurs when the explicit proxy traffic includes deep inspection, moderate stress, or when encountering SSL decryption failure situations.
209567	The explicit web proxy did not check the request port before treating it as SSL port when performing the connection request.
213123	Fix explicit proxy NTLM authentication does not work with Apple Safari on iOS.
210305	There is a 502 Bad Gateway Error issue when accessing groupsms.starhubgee.com.sg through the explicit web proxy.
211426	Explicit web proxy users are not able to authenticate using HTTPS form based authentication.
209581	The WAN Optimization daemon continuously crashes, disrupting explicit web proxy traffic.

Web-based Manager

Table 24: Resolved Web-based Manager issues

Bug ID	Description
178075	Multi VDOM Dashboard Improvement.
191753	Windows AD group name is truncated in FSSO group configuration.
196754	Routing monitor not showing bgp routes for full BGP table.
199345	Loading time issue for the User SSO list page.

Table 24: Resolved Web-based Manager issues (continued)

Bug ID	Description
200687	Inactive and non selected IPv6 routes should not show up in routing monitor page.
203666	FortiGate requests the whole AD tree despite the DN level configured.
203682	The web-based manager does not hide the virtual switch menu when the switch controller is disabled.
207165	Test button in user LDAP config does not work for LDAPS.
207986	Drill down top threat for destination should not return all threats.
208205	Web-based manager display issue when accessing interface page that has a system zone with either one or any of the switch, aggregate, or redundant interface as its member.
208230	Setup wizard does not have proper interface setting when creating SSL VPN policies.
208248	Internal server error occurrence in LDAP user setting when using query button.
208251	When FAP has name string, FAP upgrade window cannot show Upgrade From FortiGuard.
208300	Default LDAP filter in Single User Creation Wizard does not work with standard user object classes in Open LDAP.
208566	No Threat History/Traffic History widget when RAID is enabled.
208574	Threat history time frame not updated after change system time.
208689	Added traffic history widget back as an non-default widget.
209566	Firewall policy6 identity based setting is not cleared when change identity based policy to deny, identity from won't be cleaned after change from device based policy to address policy.
209634	FortiGate shows unknown user reboot event in the log when it is rebooted by FortiManager.

Table 24: Resolved Web-based Manager issues (continued)

Bug ID	Description
210963	Fix VDOM admin privilege error message when trying to edit FortiGuard categories under webfilter.
Multiple	Several Web-based Manager fixes Bug ID: 153173, 166421, 166724, 181167, 193319, 199367, 199771, 199836, 200751, 200779, 204129, 204759, 206412, 206534, 206642, 207613, 207702, 208068, 208119, 208386, 208391, 208429, 208458, 208682, 208803, 208821, 208881, 208921, 208979, 209007, 209085, 209536, 209727, 209965, 172840, 212685, 182922, 211859, 164007, 176816, 205517, 208392, 174712, 209384, 185027, 202247, 211251, 211674, 201044, 208579, 200947, 198968, 179063, 194784, 208371, 208096, 212488, 195662, 212008, 180257, 204540, 210709, 212595, 206407, 206526, 140615, 205376, 211595, 203245, 190194, 208069, 211311, 202133, 160750, 185465, 208411, 180387, 186007, 205855, 206630, 203441, 159167, 212442, 208931, 212124, 207766, 198894, 185135, 175149, 212440, 201025, 211296, 201122, 113767, 212569, 196371, 213816, 204787, 205063, 198992, 205279, 210623, 209427, 178649, 209395, 126061, 171918, 205820,200396, 178818, 200745, 211004, 190233, 208079, 192639, 200105, 200681, 212930, 207183, 205986, 197373, 212054, 204966, 207894, 198976, 191238.

Web filtering

Table 25: Resolved web filtering issues

Bug ID	Description
154091	The web filter override does not work in the user group scope for the admin-level and user-level override.
199876	Web filter override redirect fails when the browser is configured with an HTTP proxy.
207253	The `ftgd-disable` option does not work in DNS based Web filter.
209334	Web filter blocks redirected website when the `redir-block` option is unset.

Wireless

Table 26: Resolved wireless issues

Bug ID	Description
173570	WiFi issue with Motorola barcode scanner MC30/31 repeatedly getting dropped.
183867	The WiFi log entry field *group* is empty for an authenticated user when WPA-Enterprise VAP uses the RADIUS Sever directly.
188065	Unable to configure both radios on the FortiAP 220B to the same band.
21322	Add Channel 52, 56, 60 and 64 to “-T” for Indoor.
214091	Expose DFS channels in wtp-profile for certified FAP-221B-E.

Known Issues

The known issues tables listed below do not list every bug that has been reported with FortiOS v5.0 Patch Release 4 build 0228. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Data Leak Prevention

Table 27: Known data leak prevention issues

Bug ID	Description
213295	DLP does not work for Gmail in proxy-mode.

Firewall

Table 28: Known firewall issues

Bug ID	Description
206225	SSL deep inspection causes browser error in load-balancing scenarios, due to different private key.

High Availability

Table 29: Known high availability issues

Bug ID	Description
213203	After split brain situation, gratuitous ARP is not sent by master unit.
214935	When operating in HA mode the FortiGate-3240C HA LED does not come on.
214643	When operating in HA mode the graphics on the HA cluster member web-based manager page and the unit operation dashboard widget do not display link status.

Logging and Reporting

Table 30: Known logging and reporting issues

Bug ID	Description
200724	Flow based does not generate a general email log when sending an email with SMTP TLS.

IPSec VPN

Table 31: Known IPSec VPN issues

Bug ID	Description
203349	6over4 IPsec does not work with NP4lite Fastpath enabled.
213451	Traffic cannot go through IPv6 over IPv4 IPsec with NP2 offload enable.

Routing

Table 32: Known routing issues

Bug ID	Description
209766	IGMP Leave Group does not work.

SSL VPN

Table 33: Known SSL VPN issues

Bug ID	Description
212329	SSL VPN cacheclean plugin warning message shows up in Firefox version 22 even though the plugin has been installed.

System

Table 34: Known system issues

Bug ID	Description
214392	Fail to edit assigned token user, get *Token does not below to this device* error.

Web-based Manager

Table 35: Known web-based manager issues

Bug ID	Description
206586	Unresponsive script when editing address group with many members.
214596	Multiple existing dhcp-relay-ip addresses get lost when making any Web-based Manager change for the related interface.

Limitations

This section outlines the limitations in FortiOS v5.0 Patch Release 4.

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,

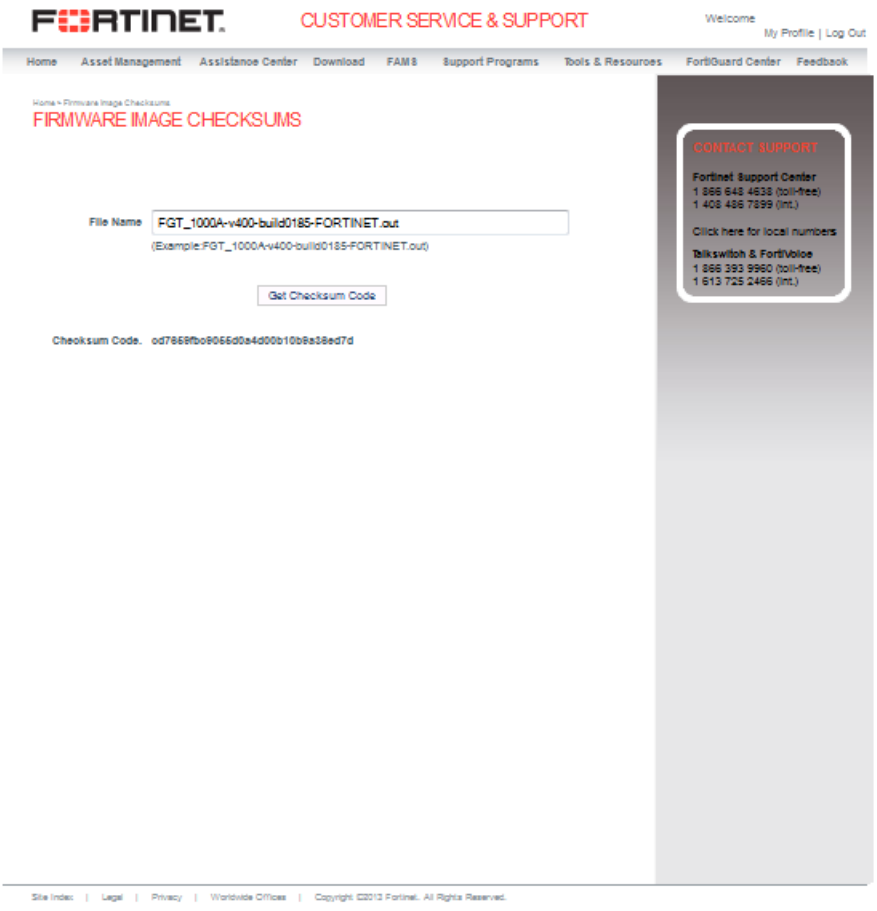
```
config user device
  edit "win"
    set mac 01:02:03:04:05:06
  next
end


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.

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 3: Firmware image checksum tool



Appendix A: FortiGate VM

FortiGate VM model information

The following table provides a detailed summary on FortiGate VM models.

Table 36: FortiGate VM model information

Technical Specification	VM-00	VM-01	VM-02	VM-04	VM-08
Hypervisor Support	VMware ESX versions 4.0, and 4.1 VMware ESXi versions 4.0, 4.1, 5.0, and 5.1 Citrix XenServer versions 5.6 SP2 and 6.0 Open Source Xen versions 3.4.3 and 4.1				
Virtual CPU (Min / Max)	1 / 1	1 / 1	1 / 2	1 / 4	1 / 8
Virtual Network Interfaces (Min / Max)	2 / 10				
Memory Support (Min / Max)	512 MB / 1 GB	512 MB / 2 GB	512 MB / 4GB	512 MB / 6GB	512 MB / 12 GB
Storage Support (Min / Max)	30 GB / 2 TB				
VDOM Support (Default / Max)	1 / 1	10 / 10	10 / 25	10 / 50	10 / 250
Wireless Access Points Controlled (CAPWAP + Remote)	64 (32 + 32)	64 (32 + 32)	512 (256 + 256)	512 (256 + 256)	4,096 (1024 + 3072)
HA Support	Yes				

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 both VMware and Xen 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.

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.