FortiOS v5.0 Patch Release 3
Release Notes

FortiOS v5.0 Patch Release 3 Release Notes

December 3, 2013

01-503-207000-20131203

Technical Documentation	docs.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
2013-11-03	Added FG-1500D and 3700D to “Supported models” on page 7. Added FortiGae-1500D and 3700D known issues to “FortiGate-1500D and 3700D” on page 45.
2013-09-25	Added FG-280D-POE to “Supported models” on page 7.
2013-07-23	Added Google Chrome version 25 to supported browsers table. Added FG-30D and FWF-30D to supported models.
2013-07-09	Added FG-90D and FWF-90D to supported models.
2013-06-27	Added FG-140D, FG-140D-POE, and FG-140D-POE-T1 to supported models.
2013-06-19	Updated summary of enhancements.
2013-06-11	Added FG-200D and FG-240D to supported models. Added IPS algorithms note in Special Notices chapter. Added bugs 208231, 209008, 208428, 207870, 208649 to the Known Issues chapter.
2013-06-06	Added bug 208740 to Known Issues chapter.
2013-06-04	Corrected typographic errors. Added features to Summary of Enhancements. Added bug 204129 to Known Issues chapter.
2013-06-03	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 3 build 0208. 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 3.

FortiGate

FG-20C, FG-20C-ADSL-A, FG-40C, FG-60C, FG-60C-POE, FG-60D, FG-80C, FG-80CM, FG-100D, FG-110C, FG-111C, FG-200B, FG-200B-POE, 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-3600C, FG-3810A, FG-3950B, FG-3951B, FG-5001A, FG-5001B, FG-5001C, and FG-5101C.

FG-30D

This model is released on a special branch based off of FortiOS v5.0 Patch Release 3. As such, the build number found in the *System* > *Dashboard* > *Status* page and the output from the `get system status` CLI command displays `4245` 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 `0208`.

FG-90D

This model is released on a special branch based off of FortiOS v5.0 Patch Release 3. As such, the build number found in the *System* > *Dashboard* > *Status* page and the output from the `get system status` CLI command displays `4263` 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 `0208`.

FG-140D, FG-140D-POE, FG-140D-POE-T1

This model is released on a special branch based off of FortiOS v5.0 Patch Release 3. As such, the build number found in the *System* > *Dashboard* > *Status* page and the output from the `get system status` CLI command displays `4243` 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 `0208`.

FG-200D

This model is released on a special branch based off of FortiOS v5.0 Patch Release 3. As such, the build number found in the *System* > *Dashboard* > *Status* page and the output from the `get system status` CLI command displays `4233` 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 `0208`.

FG-240D

This model is released on a special branch based off of FortiOS v5.0 Patch Release 3. As such, the build number found in the *System* > *Dashboard* > *Status* page and the output from the `get system status` CLI command displays `4233` 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 `0208`.

FG-280D-POE

This model is released on a special branch based off of FortiOS v5.0 Patch Release 3. As such, the build number found in the *System* > *Dashboard* > *Status* page and the output from the `get system status` CLI command displays `4323` 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 `0208`.

FG-1500D

This model is released on a special branch based off of FortiOS v5.0 Patch Release 3. As such, the build number found in the *System* > *Dashboard* > *Status* page and the output from the `get system status` CLI command displays `4358` 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 `0208`.

FG-3700D

This model is released on a special branch based off of FortiOS v5.0 Patch Release 3. As such, the build number found in the *System* > *Dashboard* > *Status* page and the output from the `get system status` CLI command displays `4358` 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 `0208`.

FortiWiFi

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

FWF-30D

This model is released on a special branch based off of FortiOS v5.0 Patch Release 3. As such, the build number found in the *System* > *Dashboard* > *Status* page and the output from the `get system status` CLI command displays `4245` 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 `0208`.

FWF-90D

This model is released on a special branch based off of FortiOS v5.0 Patch Release 3. As such, the build number found in the *System* > *Dashboard* > *Status* page and the output from the `get system status` CLI command displays `4263` 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 `0208`.

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 3 build 0208.

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

AV Engine

- Advanced Threat Protection (ATP) extensions

Endpoint profile

- Added support for multiple alternative update IP addresses
- Backup and restore registered client configuration
- Endpoint profile details can be displayed in the FortiClient registration dialog
- New endpoint profile feature: Custom endpoint profile portal pages for different device types (iOS, Mac, Windows, Android, etc.)
- Assign endpoint profiles based on user authentication

Firewall

- Support DSS and ECDSA certificates for the following features: HTTPS/SSL deep scanning, HTTPS/SSL server load balancing, HTTPS/SSL offloading, and HTTPS over the explicit web proxy

FortiGuard Services

- FortiGuard Subscription Services have been reorganized and renamed
  - Next Generation Firewall (NGFW) includes IPS & Application Control
  - Advanced Threat Protection (ATP) Services include Antivirus and Web Filtering
  - Other Services include Vulnerability Scan, Email Filtering, and Messaging

IPS

- Changes to IPS algorithms: “low” mode is now more efficient for FortiGate units with less memory (512 MB or less) and new “super” mode improves performance for FortiGate units with lots of memory (more than 4 GB)

Logging & Reporting

- New charts added to the daily FortiGate System Report based on data collected by event logs
- Memory logging is available on all models, but is disabled by default and can be enabled from the CLI
- Enabled logging to flash on the FG-60D and FWF-60D

Routing

- Increased the OSPF summary address limit from 10 to 25
- More routing community lists can be configured

SSO/FSSO

- Virtual IP support for integration with Citrix 6.0 or later
- FSSO authentication for the explicit web proxy supports port-range-based Citrix Terminal Services agent
- Failover from SSO/FSSO to default authentication for the explicit web proxy

VPN

- The maximum IPsec VPN preshared key length has been increased to 128 characters (was 80)
- The MTU for an IPsec VPN interface will now be the same as the MTU for the physical interface that the IPsec VPN interface is added to (in previous versions, the MTU was limited to 1500 for IPv6 IPsec VPN interfaces)
- 512 IPsec VPN phase 2 selectors can be associated with a single phase 1 (was 128)
- Increased the maximum length of the IPsec VPN banner string to 1024 characters

WAN Optimization & Web Proxy

- URL based web proxy forwarding

Web-based Manager

- When configuring an interface-based IPsec phase 1, select Mode Config to configure the DNS server and IP address range to assign IPsec VPN clients.
- Configure IPS signatures to exempt selected IP addresses from IPS protection
- More ways to customize the features available in the Web-based Manager. Includes a Features dashboard widget and security features presets.
- Improved user creation wizard, LDAP server options, and user monitor pages
- Intelligent object searching added to more Web-based Manager pages
- Threat History widget
- Web Site filter (formerly URL filter) allows you to add URLs to filter directly to web filter profiles
- Advanced Threat Protection Statistics dashboard widget
- Traffic History dashboard widget improvements
- IPS and Application Control sensor improvements

WiFi

- CAPWAP administrative access option for all interfaces. You must enable CAPWAP administrative access on an interface if you are managing a FortiAP device connected to it. You must also enable CAPWAP on a FG-100D interface used to manage a FortiSwitch device. You can manage multiple FortiAP and FortiSwitch devices from the same FortiGate interface. CAPWAP is supported in IPv4 only.
- Increased the maximum number of supported wireless access points
- Use RADIUS authentication to dynamically route authenticated wireless user traffic to a VLAN. The name of the VLAN is added to the user's RADIUS record (dynamic VLANs).
- Dynamic VLAN support
- Auto-detect the best firmware version for the FortiAP devices managed by a FortiGate device

- Report all wireless devices found by a FortiAP, even if the device does not attempt to connect or is not able to connect to the SSID hosted by the FortiAP
- Wireless Controller MIB support

Other

- FortiGate VM Xen support
- Certificate based URL filtering for HTTPS
- A single security policy can include multiple source and destination interfaces
- FortiCloud account creation using FortiCare registration information
- IPv6 DoS policy
- NAT46 support and support for IPv4 to IPv6/IPv6 to IPv4 destination address and port translation
- URL source tracking
- Set a FortiGate mgmt interface to be used for management only
- Deny option for split policy
- Configure hosts in an SNMP v1/2c community to send queries or receive traps
- Anti-spoof check for IPv6
- Support RFC 1853: IP in IP tunneling
- GTP-u acceleration on SP3 cards
- Support link aggregation for FortiController
- Support FortiGate 5001C with FortiController 5103B
- Added action options to each identity based policy
- Support STARTTLS/SMTPS in alertmail

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.

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

For optimal performance of your FortiGate unit, disk logging will be disabled during upgrade to FortiOS v5.0 Patch Release 3. Fortinet recommends you enable logging to FortiCloud on this unit to use the extended logging and reporting capabilities. This change affects the following models:

- 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-80C, FWF-80C, FG-80CM, FWF-80CM
- FG-100D (PN: P09340-04 or earlier)
- FG-300C (PN: P09616-04 or earlier)
- FG-200B without SSD installed

A limitation in the code specific to the FG-80C, FG-80CM, FWF-80C, and FWF-80CM prevents a message from being displayed warning users that disk logging has been disabled upon upgrading to FortiOS v4.0 MR3 Patch Release 12. If you were using FortiCloud prior to upgrading, the settings are retained and the service continues to operate.

FG-60D/FWF-60D

Disk logging has been added back to the FG-60D and FWF-60D models. It is recommended to format the log disk after you enable this feature. To format the log disk, enter 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 3. 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 3. 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 3. 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 1 or later

FortiOS v5.0 Patch Release 3 build 0208 officially supports upgrade from FortiOS v5.0 Patch Release 1 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 3 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 3 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 3 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 3 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 3, 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 3.

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 3 build 0208 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 3 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 3 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 3 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.

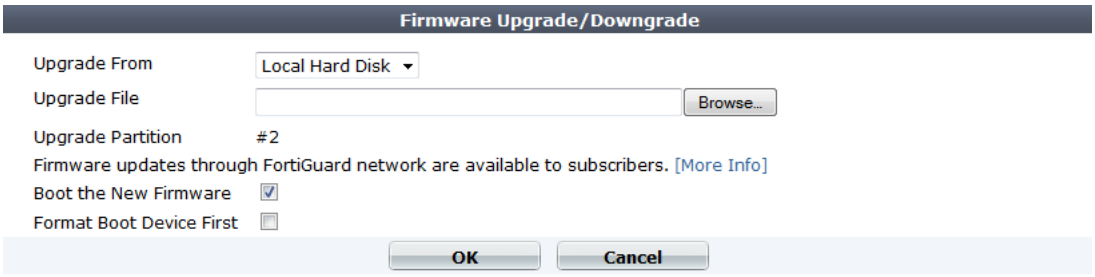
Save a copy of your FortiGate device configuration prior to upgrading. To backup your configuration, go to *System* > *Dashboard* > *Status*. In the *System Information* widget select *Backup* under *System Configuration*. Save the configuration file to your management computer.

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*.

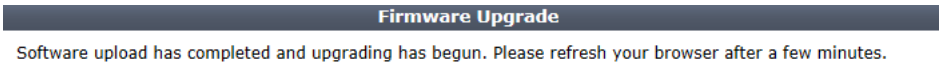
   The *Firmware Upgrade/Downgrade* window opens.

   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 3 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 3 is supported by FortiManager v5.0 Patch Release 3 or later.

FortiAnalyzer support

FortiOS v5.0 Patch Release 3 is supported by FortiAnalyzer v5.0 Patch Release 3 or later.

FortiClient support

FortiOS v5.0 Patch Release 3 is supported by the following FortiClient software versions:

- FortiClient (Windows) v5.0 Patch Release 4 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 4 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 4 Release Notes* for more information.

FortiClient iOS support

FortiOS v5.0 Patch Release 3 is supported by FortiClient (iOS) v5.0 Patch Release 1.

FortiAP support

FortiOS v5.0 Patch Release 3 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 4 build 0039 or later.

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

FortiSwitch support

FortiOS v5.0 Patch Release 3 supports the following FortiSwitch models:

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

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

FortiController support

FortiOS v5.0 Patch Release 3 supports the following FortiController models:

FCTL-5103B

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

Virtualization software support

FortiOS v5.0 Patch Release 3 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 3 is supported by FSSO v4.0 MR3 B0137 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 3 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 3 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 3 is supported by AV Engine v5.146 and IPS Engine v2.153.

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 on the drop-down menu.

Module support

FortiOS v5.0 Patch Release 3 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 3 supports the SSL VPN tunnel client standalone installer build 2289 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 Google Chrome version 25
Microsoft Windows 7 64-bit SP1	Microsoft Internet Explorer versions 8, 9 and 10 Mozilla Firefox version 19 Google Chrome version 25
Linux CentOS version 5.6 and Ubuntu version 12.0.4	Mozilla Firefox version 3.6 Google Chrome version 25
Mac OS X v10.7 Lion	Apple Safari version 6 Google Chrome version 25

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	✔	✔

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

Product	Antivirus	Firewall
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 3 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 3 build 0208. For inquires about a particular bug, please contact Customer Service & Support.

Email Filtering

Table 7: Resolved email filtering issues

Bug ID	Description
158658	`scanunitd` daemon signal 11 crash with antispam engine.
186330	The spam scan is not completed for email which has an irregular line in the mail header.
192554	The SMTP proxy should correctly enter the block state when an archive block occurs.
203465	The `antispam-score-threshold` range should be enforced in the CLI.

Data Loss Prevention

Table 8: Resolved data loss prevention issues

Bug ID	Description
196879	DLP file pattern does not match values in `ftp-over-http` proxy mode.
201540	DLP fails to detect credit card information in PDFs.
202685	Added memory usage limit for the `dlpstatd` daemon.
203016	DLP does not check the converted `utf8` buffer for DLP regular expression.

ELBC

Table 9: Resolved ELBC issues

Bug ID	Description
200276	Disabling the ELBC `graceful-upgrade` option in the CLI may not disable this feature.

Endpoint Control

Table 10: Resolved endpoint control issues

Bug ID	Description
199334	FortiGate does not send the `broadcast-forticlient-discovery` message for the secondary IP in the interface.

Firewall

Table 11: Resolved firewall issues

Bug ID	Description
186292	`sslworker` daemon memory leak.
188248	`urlfilter` daemon memory leak.
189626	In some situations, the `proxyworker` daemon experiences high CPU and traffic is blocked.
192856	Removed the limitation that only one wildcard admin user is permitted in each VDOM.
192977	Added FortiAP information to RADIUS accounting information.
194628	The `service-ttl` value does not have priority over the `policy session-ttl` value.
197032	Rx/Tx counters are reporting incorrect values when above 4 TB.
201556	RPC unreachable issue caused by the authentication packet being changed, resulting in an integrity check failure.
202811	Unable to access FortiGate local services over a different interface.
202962	`proxyworker` daemon crash caused by stack corruption in HTTP replacement message generation.
203376	Garbled replacement message in the quarantine section if the file name is longer than 23 characters.
203549	Updated the maximum number of load balance virtual and real servers.
204409	IP translation does not occur for SCTP INIT received for an existing session.
205221	SSL acceptor memory leak.
205342	No source NAT IP address in traffic log for ICMP destination unreachable packets when using source NAT in firewall policy.
205343	Server unreachable LDAP error when trying to access a load balancer VIP from the FortiGate.
205939	NAT64 is not recording source NAT properly.
206229	WSSO authenticated users cannot be listed in the *User and device* > *Monitor* > *Firewall* page.

Table 11: Resolved firewall issues (continued)

Bug ID	Description
206338	SMTP MTA timeout caused by SMTP splice mode changes related to SMTP body filter bypass changes.
Multiple	Several issues in the `scanunit` MIME parser. Bug ID: 202697, 202579, 202947, 202566, 202561, 200832, 202179, 201924, 202346, 202681, 202102, 202700
Multiple	Improved kernel support for firewall authentication. Bug ID: 192267, 201192, 195546, 192214, 192238, 197554, 196222, 202476, 190995, 194758

FortiCarrier

Table 12: Resolved FortiCarrier issues

Bug ID	Description
201887	The proxyworker daemon crashes when handling certain MMS messages

FortiGate VM

Table 13: Resolved FortiGate VM issues

Bug ID	Description
196421	Cannot set the MTU size to larger than 1500 with the VMXNET2 firmware image.
201737	New memory limits for FG-VM models. See FortiGate VM for more information.

High Availability

Table 14: Resolved high availability issues

Bug ID	Description
177810	IPsec tunnel is up in `vsys_ha` even if HA encryption and authentication are disabled.
200729	The FortiGate HA master is not upgraded when the slave is upgraded.
201838	Errors when restoring a VDOM configuration to Virtual Cluster2.
202764	When the FortiAnalyzer is unreachable the `hasync` process on a FortiGate slave unit causes multiple issues.
203940	Ensure the aggregate MAC address is propagated to aggregated devices when in HA mode.
205754	The `execute ha ignore-hardware-revision` CLI command does not work.

IPS

Table 15: Resolved IPS issues

Bug ID	Description
199286, 199429	`ips view-map` memory usage and performance issue when cache searching.
201156	XH0 DoS policy is not bound to zone when configured for syn proxy.
201422	IPS engine memory usage increases over time causing the device to enter conserve mode.
205030	IPS drops original direction packets after 5 minutes idle time when NP4 offloading is enabled.

IPsec VPN

Table 16: Resolved IPsec VPN issues

Bug ID	Description
128491	CLI should control the maximum value for phase2 parameter `keylifekbs`.
193361	IKEv2 cannot connect to third party device due to a selector matching error.
197597	A VPN authenticated by certificate was successful without importing a CA certificates.
197896	Error counter issue during IPsec test with CP6/CP7/CP8 driver.
198121	FortiGate responds to the IKE initiator first message with source port 4500 instead of 500.
202211	The `iked` daemon crashes when using RSA certificates with no CA in peer entry.
202780	IKE memory leak when using RSA certificates.
203499	Allow IPsec MTU larger than 1500.
203631	The CLI command `set fragmentation enable | disable` is not available for interface-mode IPsec.
203916	Increased the maximum phase2 selectors per phase1 from 128 to 512.
204059	When *Full Cone NAT* is enabled, PPTP VPN connections fail to establish.
204324	Added a new CLI command to enable/disable VPN hardware-acceleration for the FG-60D and FWF-60D.
205497	Site-to-site incorrect phase2 selector match error.

Logging and Reporting

Table 17: Resolved logging and reporting issues

Bug ID	Description
157212	Added memory logging back on all platforms. This feature is disabled by default and CLI only.
188767	Added new UTM event category `app-ctrl` for IPS UTM traffic log.
193312, 193273	Added log support for FortiGuard Sandbox to `explicit web-proxy`, `explicit ftp-proxy`, and `mapi`.
194329	Missing logs in Poll Active Directory server.
202622	Garbled Japanese character are displayed in the filename field of the UTM (AV/DLP) log.
203140	Added control and checks for FortiCloud daily volume.
203910	Added `dlpsensor` field to UTM traffic log.

Routing

Table 18: Resolved routing issues

Bug ID	Description
172674	Traffic cannot pass through a GRE tunnel which is established over a loopback interface.
186469	Changing the OSPF NBMA interface priority caused the hello interval to ne changed causing a neighbor down.
200476	Actual hello interval does not match configured `hello-interval` for the OSPF NBMA interface.
202246	The `gwdetect` daemon fails to take down IPSEC routing.

SSL VPN

Table 19: Resolved SSL VPN issues

Bug ID	Description
165402	The SSL VPN web portal does not handle Sage CRM websites.
193668	Improved the renew password page when authenticating with LDAP.
195202, 179445	Citrix applications can not be launched if the Citrix receiver `CitrixReceiverWeb` is used in client PC.
196956	Users are not forced to logout when the SSL VPN client fails to login due to the MAC address check.
198415	Web server does not work correctly with SSL VPN bookmarks.

Table 19: Resolved SSL VPN issues (continued)

Bug ID	Description
201689	Unable to access RDP through SSL VPN web mode bookmarks.
201834	PKI user can not login if multiple authentication rules are included in one policy.
202459	Added event/crash log entry for SSL VPN conserve mode.
203135	SSL VPN parser for setting cookie in web mode.
204521	Incorrect SSL VPN portal is displayed after renewing the password through LDAPS.
206172	The second SSL VPN firewall policy is not checked if the first firewall policy does not match the source IP.

System

Table 20: Resolved system issues

Bug ID	Description
131874	Importing a CRL via LDAP does not work in VDOM mode.
139918	The `authd` daemon crashes after adding or deleting a VDOM.
167264	Modem update could not be synchronized between HA members.
170385	Unable to link at 1000full on all interface ports.
171529	`sFlow` does not work correctly with NPU interfaces.
182127	FortiGate L2TP client data flow fails on RPF check.
186859	The OSPF MD5 key is not encrypted in the configuration file.
188769	ICMPv6 ping traffic is not blocked when there is no firewall policy on the interface.
192341	10 half-duplex issue with unusual packet loss.
192970	FortiGuard Web filtering and Email filtering services should be displayed as *Unreachable* rather than *Not Registered.*
194861	Improved the WCCP daemons VDOM change handling function.
195058	Allow SNMP v1/v2 host to specify whether it can accept queries or send traps.
195900	Resolved host-names do not work on widgets when the non-root VDOM is the management VDOM.
197923	FortiGate did not free `rtcache` memory after high `hping3` stress attack.
198375	P2P sessions cannot be traffic shaped.

Table 20: Resolved system issues (continued)

Bug ID	Description
200519	NP-offloaded sessions flows over the backup redundant interface after the primary interface is back online.
200639	Mobile FortiToken authentication code delivery should not use the FortiGuard email service.
200819	In non-root VDOMs, the modem interface cannot register to `iprope` when getting its IP address.
201142	Inter-VDOM routing fails at the fifth VDOM.
201496	Added a description field for `reserved-address` of DHCP server.
201523	DHCP offer blocked by FortiGate `dhcp-relay`.
201567	Hardware switch interface is down after upgrading to FortiOS v5.0 Patch Release 2.
201690	XH0 memory problem after initialization or conserve mode.
201695	XH0 initialization issue with high memory usage.
201825	3G modem PIN logic change request.
202100	Interface lost after running the `execute factoryreset2` CLI command when in interface mode.
202602	Added a `never` option to the FSSO logon history parameter.
202658	Changing to ELBC service group mode should not cause `miglogd` daemon errors.
202844	Cannot enter a FortiClient license on a FG-60D or FWF-60D.
202922	The output of the `show` CLI command is inconsistent.
203205	Multicast traffic does not flow through all IPsec tunnels when using XH0/SP3.
203486	Login with a remote wildcard administrator does not work after reboot.
203609	IPv6 packets are dropped sporadically between VLAN interface and IPsec interface on FSM-XG2 modules.
203719	Updated maximum values for NAT64 objects.
203844	FDS connection problem when SSL write was not completed.
204056	The CLI command `diagnose sys session6 list` should include IPv4 NAT message on NAT64 function.
205080	CLI scripts output the `Configuration file error` message.
205272	Table size changed for router community list. See the *Maximum Values Table for FortiOS 5.0* for more information.
205495	DoS sensor activation on XH0.

Table 20: Resolved system issues (continued)

Bug ID	Description
206507	FortiGate does not buffer logs if the FortiAnalyzer connection is lost.
207521	The FG-3600C status LED does not turn on.

Upgrade

Table 21: Resolved upgrade issues

Bug ID	Description
190948	A wireless-controller.wids-profile was added by default. This profile is not available when upgrading from previous builds.
198895	Corrected the upgrade code for the `voip extended-utm-log` feature.
199674	The `11g-only wtp-profile` is kept after upgrading from FortiOS v4.0 MR3 Patch Release 12.
201931	After upgrading from FortiOS v4.0 MR3 Patch Release 11 to v5.0 Patch Release 2, FortiGate is unable to form HA properly.

WAN Optimization and Explicit Proxy

Table 22: Resolved WAN optimization and explicit proxy issues

Bug ID	Description
182964	The `WAD` daemon crashes when processing multiple range HTTP requests from a single database read.
201021	`WAD` daemon memory leak in SSL mode.
201483	The `fnbamd` process crashes frequently.
202907	Replacement message is not shown using explicit web proxy with SSL inspection and HTTPS URL scan.
203187	Web pages do not fully load when webcache is enabled.
204242	Dynamically generated files (server-side) do not pass through explicit proxy.
205826	The `WAD` SSL module crashes and memory leaks are observed when the module is stressed with different kinds of SSL traffic.

Web-based Manager

Table 23: Resolved Web-based Manager issues

Bug ID	Description
192463	HTTP ERROR 400 while navigating on FG-100D Web-based Manager.
193766	FSSO authenticated users are not displayed in the Web-based Manager.

Table 23: Resolved Web-based Manager issues (continued)

Bug ID	Description
199914	Changed style for *Top Bar* feature.
203427	Cannot access the Web-based Manager via HTTPS when FortiAnalyzer logging is enabled.
Multiple	Various traffic widget improvements. Bug ID: 199883, 196138, 201516
Multiple	Various Web-based Manager improvements. Bug ID: 182637, 161653, 161387, 195085, 203328, 201302, 193523, 201022, 153745, 202250, 189872, 204901, 201160, 202914, 195275, 207689, 148888, 207555, 203218, 201145
Multiple	Various log settings page improvements. Bug ID: 191465, 200661, 196715, 200694, 200793, 200012, 199444, 198508, 162046, 199305, 200960, 198805, 194951, 186890
Multiple	Various Web-based Manager performance and memory issues. Bug ID: 204124, 194117, 200748, 192578, 200592, 201456, 198607

Web filtering

Table 24: Resolved web filtering issues

Bug ID	Description
197973	Unable to display flow-based URL block page if FortiGuard is enabled and larger than 4 characters.
200350	When the Web Filter quota is assigned with more than three categories, the authentication keep alive page is not displayed.

Wireless

Table 25: Resolved wireless issues

Bug ID	Description
146103	The Web-based Manager should not delete the `ap-status` entry when changing the value.
192189	The FAP-223B radio-1 is a 5GHz single band and needs a separate profile.
202642	Incorrect AP status message.
206229	WSSO authenticated users could not be listed in the *User and device* > *Monitor* > *Firewall* page.

Known Issues

The known issues tables listed below do not list every bug that has been reported with FortiOS v5.0 Patch Release 3 build 0208. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

FortiGate-1500D and 3700D

Table 26: Known FortiGate-1500D and 3700D issues

Bug ID	Description
218425	NP6 syn-proxy do not work.
210890	IPv6 traffic over IP tunnel can not passthrough if offload enabled. Workaround: disable offload in tunnel configuration.
225640	IPS Engines crashed when viewing top widgets during stress test.
216235	Fragmented traffic fail to pass IPsec tunnel (4over6/6over6) with default MTU 1500. Workaround: disable NPU offload in IPSec phase1 setting.
223686	Traffic history widget can't report accurate traffic volume at high traffic load in IPS test.
216496	Multicast over inter-vdom-link does not offload to NP6.

Firewall

Table 27: Known firewall issues

Bug ID	Description
202460	Flow-based antivirus cannot be enabled in a firewall policy on the FG-3810A with an AMC-XE2 module.
206225	SSL deep inspection causes browser errors in load balancing scenarios, due to different private keys.

Logging and Reporting

Table 28: Known logging and reporting issues

Bug ID	Description
175029	SSH proxy logs are not displayed in the Web-based Manager.
204129	Test FortiAnalyzer connectivity always fails in the Web-based Manager when the management VDOM is not root.

System

Table 29: Known system issues

Bug ID	Description
203068	Read only administrators are able to run `execute` CLI commands.
203863	The FG-3240C cannot process DoS anomaly attacks in offload mode.
206480	Multicast encrypted packets are dropped by XLP in FastPath.
207870, 208649	The IPS engine may leak memory is the configuration is altered and saved frequently, for example by executing a script.
Multiple	The FortiGate unit may experience a temporary drop in performance during an IPS signature update. Bug ID: 208231, 209008, 208428

Web-based Manager

Table 30: Known Web-based Manager issues

Bug ID	Description
203666	FortiGate requests the whole AD tree instead of the DN level configured.
206780	Unable to configure/edit one-arm sniffer settings in the interface page. Workaround: Use the CLI to configure these settings.
206999	Policy filter on service does not list each policy within its associated interface pair menu.
207923	Cannot specify the FortiManager for update signature in the endpoint control profile in the Web-based Manager. Workaround: Use the CLI to configure these settings.
208251	When a FortiAP has name string, the FortiAP upgrade window does not show *Upgrade From FortiGuard*.

Upgrade

Table 31: Known upgrade issues

Bug ID	Description
206822	When upgrading from build 0179, `extend-db` stops working until the user either manually updates or schedules an update.
206895	Upgrading from v5.0 Patch Release 2 changes the following Web-based Manager display settings: `gui-dlp`, `gui-sslvpn-personal-bookmarks`, and `gui-sslvpn-realms`.

Table 31: Known 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	FortiToken mobile keys are rejected after upgrading to v5.0 Patch Release 3. Workaround: Deactivate each user token on the FortiGate and device. Reactivate each user token on the FortiGate and device.

Limitations

This section outlines the limitations in FortiOS v5.0 Patch Release 3.

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,

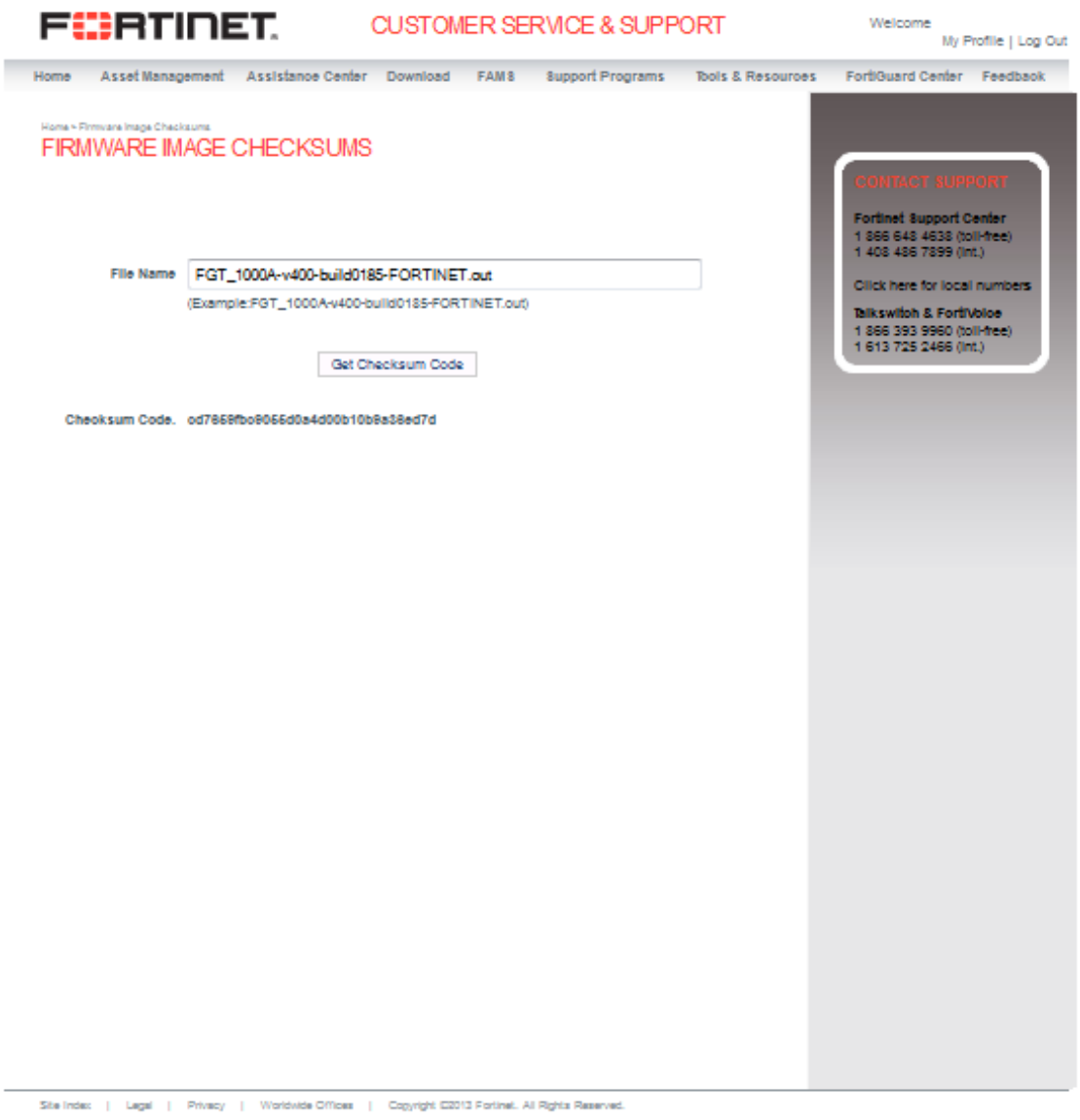
```
config user device
  edit "win"
    set mac 01:02:03:04:05:06
  next
end


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 32: 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.