FortiOS v5.0 Patch Release 2
Release Notes

FortiOS v5.0 Patch Release 2 Release Notes

May 08, 2013

01-502-198042-20130508

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
2013-03-18	Initial release.
2013-03-19	Corrected typographic errors. Updated FortiAP support information.
2013-03-20	Updated summary of enhancements.
2013-03-22	Added bug ID 200867 to Resolved Issues chapter. Added FG-3600 special build information. Updated VMware support information. Updated FortiExplorer support information.
2013-03-27	Added FG-60D/FWF-60D special build information. Updated summary of enhancements. Updated FortiExplorer/FortiExplorer iOS support information.
2013-03-28	Added FortiGate 100D special notice. Added 201698 to Known Issues chapter.
2013-04-11	Minor document update to Upgrade Information chapter.
2013-04-29	Minor document update.
2013-05-08	Corrected FSSO support information.

Introduction

This document provides a summary of new features, support information, installation instructions, integration, resolved and known issues in FortiOS v5.0 Patch Release 2 build 0179.

Supported models

The following models are supported on FortiOS v5.0 Patch Release 2.

FortiGate

FG-20C, FG-20C-ADSL-A, FG-40C, FG-60C, FG-60C-POE, 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-3810A, FG-3950B, FG-3951B, FG-5001A, FG-5001B, FG-5001C, and FG-5101C.

FG-60D

This model is released on a special branch based off of FortiOS v5.0 Patch Release 2. As such, the build number found in the *System* > *Dashboard* > *Status* page and the output from the `get system status` CLI command displays `4162` 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 `0179`.

FG-3600C

This model is released on a special branch based off of FortiOS v5.0 Patch Release 2. As such, the build number found in the *System* > *Dashboard* > *Status* page and the output from the `get system status` CLI command displays `6184` 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 `0179`.

FortiWiFi

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

FWF-60D

This model is released on a special branch based off of FortiOS v5.0 Patch Release 2. As such, the build number found in the *System* > *Dashboard* > *Status* page and the output from the `get system status` CLI command displays `4162` 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 `0179`.

FortiGate VM

FG-VM32 and FG-VM64.

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 2 build 0179.

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

Endpoint control and FortiClient support

- Added FortiClient license upload feature to FG-60C series and FG-80C series platforms
- Added option for FortiClient to upload logs with or without SSL
- Added support for mode-cfg unity save-password. Added attributes to allow FortiClient to save password, auto-connect and keep-alive.
- Endpoint security replacement messages are customized for each device type
- Extend FortiClient registration license to allow unlimited expiry time
- FortiClient console customization options for registered clients
- FortiClient log support for VDOMs
- FortiClient registration with redundant gateways
- FortiClient can be configured to upload traffic, event and vulnerability scan logs to your FortiAnalyzer or FortiManager device via the *Endpoint Profile*
- FortiClient can be configured to receive FortiGuard updates from your FortiManager device via the *Endpoint Profile*
- FortiClient upgrade license
- iOS .mobileconfig file deployment over Endpoint Control. Requires FortiClient (iOS) v5.0 Patch Release 1.
- Multiple endpoint profiles
- Support FortiClient for iOS in endpoint profiles
- Web category filtering safe search support

Logging and reporting

- Added the option to enable FortiCloud logging during activation
- Changes to customizing and running reports
- Combine domains in charts
- Disk log is disabled by default for all desktop models
- Enable traffic logging for UTM events or all sessions in security policies

- FortiAnalyzer client reputation report

UTM

- Block infections to botnet servers available in both proxy-based and flow-based antivirus profiles
- *FortiGuard Analytics* requires a FortiCloud account

Authentication

- Improvement for FSSO server configuration
- PPPoE for FG-100/FG-200 series platforms
- Support LDAP user with workstation names in FSSO authentication
- Wizard for creating locally mapped LDAP users

VPN

- FortiClient IPsec VPN enhancements
- SSL VPN portal configuration enhancements
- Support for multiple custom SSL VPN logins
- Support SSL VPN MAC address host check
- Synchronize FortiClient VPN elements; `save password`, `autoconnect`, and `always up`; with the FortiGate

Dashboard

- Added application column to top destination widget
- Added intelligent search capabilities to the firewall address list
- Added log-based *Traffic History* dashboard widget
- Added support for redirecting administrator logins from HTTP to HTTPS
- *AntiMalware Statistics* dashboard widget
- Combined domains in top destinations dashboard
- USB modem dashboard widget

Wireless

- Broadcast suppression
- Custom mesh downlink SSIDs
- Icon for local bridge SSIDs
- QoS for wireless via FortiAP
- Wireless client mode improvements

Other

- Added a new command to force session synchronization for standalone `sessionsync`
- Added IKE support for RSA certificate chains
- Added support to allow denied session in the session table
- ECMP support for BGP and IPv6
- Event log for XH0 modules
- FortiGate units can provide NTP services

- RADIUS based MAC address authentication
- IPv6 PIM sparse mode multicast routing
- Safari web browser support
- FortiCarrier upgrade license
- Generate an event log message when a one-time schedule is about to expire
- The SIP ALG can receive SIP traffic on multiple TCP and UDP ports
- SSL next-proto-negotiation extension
- FGFM protocol to upgrade FortiAP firmware
- Policy routing by source port
- USB encrypted configuration file support

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*. On the *System Information* widget select *Backup* under *System Configuration* and save the configuration file to your local hard drive.

In VM environments, it is recommended that you take a *Snapshot* of the VM instance. 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*.

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 virus and attack 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* (*System* > *Config* > *FortiGuard* > *AntiVirus and IPS Options*) after upgrading. Consult the *FortiOS v5.0 Handbook* or *FortiOS v5.0 Carrier Handbook* for detailed procedures.

Disk logging

For optimal performance of your FortiGate unit, disk logging will be disabled during upgrade to FortiOS v5.0 Patch Release 2. Fortinet recommends you enable logging to FAMS (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-60D, FWF-60D
- 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.

Table size changes

FortiOS v5.0 Patch Release 2 changes the following table size values:

- Application list
- DHCP server
- Multicast address
- IPS sensor
- Profile
- DHCP server
- VIP
- Policy routes
- URL filter

See the *Maximum Values Table for FortiOS 5.0* for more information.

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 2. 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 2. 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 2. The DLP rule settings have been moved inside the DLP sensor.

ID-based firewall policy

If you have enabled `fail-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 `fail-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 v5.0.0 or later

FortiOS v5.0 Patch Release 2 build 0179 officially supports upgrade from FortiOS v5.0.0 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 2 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 2 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 2 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 2 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 2, 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 2.

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 2 build 0179 officially supports upgrade from FortiOS v4.0 MR3 Patch Release 10 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.

Table size limits

FortiOS v5.0 Patch Release 2 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 2 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 2 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
```

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 2 supports the following web browsers:

- Microsoft Internet Explorer versions 8 and 9
- Mozilla Firefox versions 18
- Google Chrome version 25
- Apple Safari versions 5.1 and 6

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

FortiManager support

FortiOS v5.0 Patch Release 2 is supported by FortiManager v5.0 Patch Release 2 or later.

FortiAnalyzer support

FortiOS v5.0 Patch Release 2 is supported by FortiAnalyzer v5.0 Patch Release 2 or later.

FortiClient support

FortiOS v5.0 Patch Release 2 is supported by the following FortiClient software versions:

- FortiClient (Windows) v5.0.0 build 0194 or later
- FortiClient (Mac OS X) v5.0.0 build 0081 or later

The following features require FortiClient v5.0 Patch Release 2 or later:

- Endpoint control registration with redundant gateways
- FortiClient uploads traffic, event, and vulnerability logs to FortiAnalyzer/FortiManager
- Synchronize VPN elements; `save password`, `autoconnect`, and `always up`; with the FortiGate

See the *FortiClient v5.0 Patch Release 2 Release Notes* for more information.

FortiClient iOS support

FortiOS v5.0 Patch Release 2 is supported by FortiClient (iOS) v5.0 Patch Release 1.

FortiAP support

FortiOS v5.0 Patch Release 2 supports the following FortiAP models:

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

The FortiAP device must be running FortiAP v5.0 Patch Release 2 build 0030 or later.

FortiSwitch support

FortiOS v5.0 Patch Release 2 supports the following FortiSwitch models:

FS-348B

The FortiSwitch device must be running FortiSwitch v1.0 Patch Release 2 build 4030 or later.

Virtualization software support

FortiOS v5.0 Patch Release 2 supports VMware ESX / ESXi 4.0, 4.1, 5.0, and v5.1. See "FortiGate VM" for more information.

Fortinet Single Sign-On (FSSO) support

FortiOS v5.0 Patch Release 2 is supported by FSSO v4.0 MR3 B0129 for the following operating systems:

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

FSSO does not currently support IPv6.

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

FortiExplorer (Microsoft Windows/Mac OS X) support

FortiOS v5.0 Patch Release 2 is supported by FortiExplorer v2.2 build 1046 or later. See the *FortiExplorer v2.2 build 1046 Release Notes* for more information.

FortiExplorer (iOS) support

FortiOS v5.0 Patch Release 2 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 2 is supported by AV Engine v5.00032 and IPS Engine v2.000137.

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 2 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

Table 2: Supported modules and FortiGate models (continued)

Accelerated Interface Module 8xSFP Double-Width AMC (ADM-FB8)	FG-3810A, FG-5001A
Bypass Module 2x1000 Base-SX Single-Width AMC (ASM-FX2)	FG-310B, FG-311B, FG-620B, FG-621B, FG-1240B, FG-3016B, FG-3810A, FG-5001A
Bypass Module 4x10/100/1000 Base-T Single-Width AMC (ASM-CX4)	FG-310B, FG-311B, FG-620B, FG-621B, FG-1240B, FG-3016B, FG-3810A, FG-5001A
Security Processing Module 2x10/100/1000 SP2 Single-Width AMC (ASM-CE4)	FG-1240B, FG-3810A, FG-3016B, FG-5001A
Security Processing Module 2x10-GbE XFP SP2 Double-Width AMC (ADM-XE2)	FG-3810A, FG-5001A
Security Processing Module 4x10-GbE SFP+ Double-Width AMC (ADM-XD4)	FG-3810A, FG-5001A
Security Processing Module 8xSFP SP2 Double-Width AMC (ADM-FE8)	FG-3810A
Rear Transition Module 10-GbE backplane fabric (RTM-XD2)	FG-5001A
Security Processing Module (ASM-ET4)	FG-310B, FG-311B
Rear Transition Module 10-GbE backplane fabric (RTM-XB2)	FG-5001A
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 2 supports the SSL VPN tunnel client standalone installer build 2285 for the following operating systems:

- Microsoft Windows XP, Windows 7, and Windows 8 in .exe and .msi format
- 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 5.6	Mac OS X v10.7 Lion
Microsoft Windows 8 32-bit	Linux Ubuntu 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 5.6 and Ubuntu 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 Microsoft Windows XP antivirus and firewall software

Product	Antivirus	Firewall
Symantec Endpoint Protection v11	✔	✔
Kaspersky Antivirus 2009	✔	
McAfee Security Center v8.1	✔	✔
Trend Micro Internet Security Pro	✔	✔
F-Secure Internet Security 2009	✔	✔

Table 6: Supported Microsoft Windows 7 32-bit and 64-bit antivirus and firewall software

Product	Antivirus	Firewall
CA Internet Security Suite Plus Software	✔	✔
AVG Internet Security 2011		
F-Secure Internet Security 2011	✔	✔
Kaspersky Internet Security 2011	✔	✔
McAfee Internet Security 2011	✔	✔
Norton 360™ Version 4.0	✔	✔
Norton™ Internet Security 2011	✔	✔
Panda Internet Security 2011	✔	✔
Sophos Security Suite	✔	✔
Trend Micro Titanium Internet Security	✔	✔
ZoneAlarm Security Suite	✔	✔
Symantec Endpoint Protection Small Business Edition 12.0	✔	✔

Explicit web proxy browser support

The following web browsers are supported by FortiOS v5.0 Patch Release 2 for the explicit web proxy feature:

- Microsoft Internet Explorer versions 8 and 9
- Mozilla Firefox versions 18 and 19
- 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 2 build 0179. For inquires about a particular bug, please contact Customer Service & Support.

Antispam

Table 7: Resolved antispam issues

Bug ID	Description
170139	The antispam engine causes the `scaunitd` daemon to crash.
174190	When parsing email the `scanunitd` daemon consumes 99% CPU until aborted by the alarm clock.

CLI

Table 8: Resolved CLI issues

Bug ID	Description
194737	Merged the `fdsmgmtd` daemon with the `forticldd` daemon.

Client Reputation

Table 9: Resolved client reputation issues

Bug ID	Description
192459	Client reputation does not report statistics for web filter DNS mode.
194084	Count URLs blocked by FortiGuard to client reputation.

Email Filtering

Table 10: Resolved email filtering issues

Bug ID	Description
197291	Spam submission link issue on 64-bit FortiGate models.

Firewall

Table 11: Resolved firewall issues

Bug ID	Description
147699	DLP full content archive can be bypassed with SMTP.
167304	Control concurrent user authentication in identity based policies.
171261	Custom replacement message images are not displayed by web filtering in flow-based inspection mode.
181530	Fortinet top bar does not display application control messages if the rule is set to `reset`.
184809, 190973	High CPU usage issue with the VSD process when passing traffic.
190534, 182481	Enable POP3 and IMAP detection in transparent mode for IPv6.
190735	Users should not be allowed to delete the default UTM profile.
191660	Antivirus failopen support for the `sslworker` process when using SSL `inspect-all`.
191755	HTTPS deep scan does not work when `inspect-all` is enabled.
191987	A virus is passed when the spam filter banned word is matched and tagged.
192744	The IPS daemon retrieves configuration via policy ID for level 7 packets without IPS view information.
194158	High CPU issue caused by IPS when `deep-inspection` is enabled with `inspection all`.
194526	HTTP content length parsing for values exceeding 32-bits.
194601	TCP `inspect-all` option issue.
194703	Antivirus proxy mode blocks specific internet radio stations.
195285	The XH0 module crashed with heavy traffic load.
195832	Load balancer packet loss issue.
195838	A session is not created for certain ICMPv6 messages.
196556	Add `remove attachment` support to `DLP filepattern`.
200867	The `proxyworker` daemon may crash if a URL with a length of zero traverses the firewall.

FortiCarrier

Table 12: Resolved FortiCarrier issues

Bug ID	Description
173623	Add support for the `remove infected` feature for MMS. This includes reporting multiple DLP-blocked files instead of just one for the whole transfer so `proxy` can remove each file.
174862	The `log field` is incorrect for DLP sensor MMS filtering.
183611	MM1 carrier endpoint filtering causes a `scanunit` process crash.

High Availability

Table 13: Resolved high availability issues

Bug ID	Description
163505	HA synchronization of source visibility and VCM signatures does not work.
178289	Transparent mode HA failover could cause a G-ARP storm.
183986	Added new OIDs to get HA configuration synchronization related information.
184052	High latency and dropped sessions during HA active-active failover.
186520	HA configuration synchronization failure when a USB device is attached.
189793	The NPU offload flag is incorrectly synchronized to the slave.
190567	Blades become unresponsive in a four blade active-active cluster.
192192	The `standalone-config-sync enable` CLI command breaks session synchronization.
196400	When the master switches to slave, the kernel should try to delete offloaded sessions in the NPU.
196771	The switch interface does not act as a HA management port properly.
197737	`ips-sp` and `ips-sp2` are unable to synchronize.

IPS

Table 14: Resolved IPS issues

Bug ID	Description
189432	Added check for `app_cat/category` option in the signature.
195856	IPS custom defined signatures do not work correctly after making configuration changes.

IPsec VPN

Table 15: Resolved IPsec VPN issues

Bug ID	Description
180980	Unable to get an IP address via L2TP over an IPsec tunnel using Chrome OS.
189304	The destination of an IPv6 route bound to `ipsec_tunnel_common` changes to the IPsec interface when a physical link is down.
190285	IPsec traffic offloaded to NP4 is cleared after rekeying.
190598	Communication between spokes (route-based VPN) does not work when one spoke is a non-NPU platform and one is a NPU platform.
191550	Certificate validation failed with many IPsec dialup phase 1 configurations.
191909	DHCP relay issue over IPsec.
192347	A session is dropped with NP4/IPsec offload (hub and spoke, spoke to spoke) traffic.
193049	Invalid ESP errors for dialup clients.
193822	Empty certificate request payload causes IPsec VPN certificate authentication to fail.
194359	Extended username shown in the `diagnose vpn tunnel list` to 64 characters.
195941	Dynamic DNS VPN does not auto-negotiate after a WAN link fails and restarts.

Logging and Reporting

Table 16: Resolved logging and reporting issues

Bug ID	Description
177399	The IM/P2P application incorrectly displays the attack ID in the log.
180995	IPS packet archive cannot be displayed in the Web-based Manager log after running the `execute log roll` CLI command.
181375	Show the authenticated user in traffic logs for web filtering overrides.
185241	Transparent mode forwarded traffic does not have a session end log.
187695	Added UTM traffic log for the web filter module when using `flow-based` for the `inspection-mode`.
190434	The `miglogd` daemon is active without any active log devices.
191808	No logs for application control in explicit proxy.
191851	The event log from FortiCloud is incorrect when activating a FortiCloud account.
192758	Generating reports causes memory leak issues.

Table 16: Resolved logging and reporting issues (continued)

Bug ID	Description
195494	Local in policy traffic is not logged on the FortiGate.
195740	Removed FortiAnalyzer discovery functionality.
196583	The default report layout is not generated.
196840	Rebuild the report database if it becomes corrupted.
197962	Removed the client reputation chart from the default layout.
Multiple	Changed client reputation report behavior. Bug ID 181469, 190906, 191161, 191298, 191196, 169714, 176203, 152434
Multiple	Generate report database from log files instead of SQL logs. Bug ID: 193801, 188292, 188830, 192298, 189349, 189700, 192690

Routing

Table 17: Resolved routing issues

Bug ID	Description
193990	The `as-confed-seq` attribute is incorrectly sent when using `route-map` to prepend `as-path`.

SSL VPN

Table 18: Resolved SSL VPN issues

Bug ID	Description
119949	SSL VPN web mode is unable to load Oracle Java application forms.
184522	Fixed content handling type for images when it is not clear from the URL whether the request is for an image.
184710	The SSL VPN monitor displayed an incorrect remain time for RADIUS users when `session-timeout` was defined.
189087	RDP native and Citrix bookmarks have to be clicked twice to work on Microsoft Internet Explorer.
191278	A user cannot create `New` on OWA Agenda through the SSL VPN web portal on Microsoft Internet Explorer versions 7 and 8.
191672	The OA page displays incorrectly in SSL web proxy mode.
191725	SSL VPN is unable to renew a password when authenticated by LDAPS.
194653	An automatic SSL VPN tunnel policy is created with the incorrect source interface.

Table 18: Resolved SSL VPN issues (continued)

Bug ID	Description
195024	Removed the SSL/SSH inspection option from SSL VPN policy.
196581	Increased the SSL VPN password length for RADIUS user authentication to 128 characters.

System

Table 19: Resolved system issues

Bug ID	Description
165667	RADIUS `source-IP` does not work.
175193	DLP full archive is not available on the FG-5101C.
176071	Improved the speed for deleting entries from a table containing large number of entries.
178545	The `average network usage` is displayed incorrectly with XH0 modules.
180188, 168610	Sessions fail with IPS enabled on the XH0 module when CPU exceeds 60%.
183191	Sub-second flaps on SFP+ interfaces (ports 1-5) on FG-3140B, FG-3040B, FG-3950B, FG-3951B, and FG-5001B platforms.
185315	When the NMI Watchdog detect feature is enabled the system hangs.
185617	NTP and CRL update from passive node failing.
187210	Servers do not return valid registration information when FortiGuard services are registered.
187310	IPS traffic is blocked when multiple XH0 modules are used with FMC-C20 and FMC-F20 modules.
187871	An `execute factoryreset2` should not clear static routes.
189061	Dedicated sniffer mode is included for scheduled update.
189254	The `forticron` process caused system information to hang.
189698	`xlp_xaui_tx_walk_around failed` error message on console reported on a FG-5101C.
189828	Added extra fields to RADIUS accounting; NAS-IP-Address(4), Called-Station-Id(30), Framed-IP-Address(8), Event-Timestamp(55).
190141	DHCPv6 server domain name cannot start with a number.
190142	A VLAN interface responds even though it is administratively down.
190749	Increased image storage limit for the FG-600C.
190829	RADIUS SSH authentication from FG-100D dedicated management interface failed.

Table 19: Resolved system issues (continued)

Bug ID	Description
191112	Failed to import a CRL which had an expiry date after 2038.
191119	FG-5101C XLP driver issue causes system kernel panic.
191184	Certain VLAN IDs (5,6,7,8) on the FortiGate do not place the ARP reply on the wire.
191268	WiFi guest management delivery via a custom SMS server does not work.
191502	Reset FortiClient license after a FortiGate factory reset.
191515	IPv4 to IPv6 IPsec traffic cannot pass through a FG-5101C when the SA is processed by XLP.
191724	Central NAT does not support wildcard addresses.
191972	Unable to login into FortiGate through FortiExplorer if trusted hosts are configured.
192085	Link aggregation interface inconsistent L2 hashing result for NPU sessions.
192360	Quarantine daemon memory usage control issue.
192580, 192582	PSU sensor false alarm issue due to hardware instability.
192598	The CLI command `icmp-redirect interface config` does not work.
192613	FG-3240C flash partition scheme is incorrect.
192686	The `newcli` process crashes when enabling VDOMs or creating a new VDOM.
192750	DHCP server incorrectly mirrors VCI information (option 60) from the request to the response.
192930	Failed to display logs after `filtering start-line.`
193104	FortiGate does not respond to the secondary IP when the primary IP is changed.
193187	SP3 ports are not accessible via telnet, SSH, and HTTP if IPS is enabled.
193399	Odd ports and HA1 on a FG-100D stop processing traffic.
194289	Push update does not work.
194412	RADIUS test authentication does not go through the source IP when configured.
194729	XLP process issues with multicast traffic.
194882	When `trusthost` is set, `iprope source address` is not set.
195027	The FortiToken seed server is unreachable after the FortiGate is registered.
195287	IPS packet real-time upload to FortiCloud does not work.

Table 19: Resolved system issues (continued)

Bug ID	Description
195982	CPU average calculation is incorrect.
196087	FG-311B kernel panic issue in a multi-homed SCTP traffic situation.
196308	Improved `crashlog` and monitor functions on XH0 modules.
196381	The `wccpd` daemon crashes when a new interface is added with `wccp` enabled.
196398	Image not showing with the replacement message.
196399, 197425	Flood and virtual switch issue with the FG-100D.
196410	The `get system performance status` is stuck after printing CPU statistics.
196418	CLI issue caused by the CLI command `execute dhcp6 lease-list`.
196772	BPDUs are not forwarded correctly in transparent mode.
196937	The `password field` in the CLI command `config system autoupdate tunneling` should be obfuscated.
197035	The timezone option is missing for Namibia.
197398	When performing a `factoryreset2` on an interface-mode FG-200B some interface configuration is lost.
197645	Removed the CLI command `execute fortiguard-log delete-log`.
197780	ISF-ACL does not work with XH0 modules.
197890, 197880	Removed the `auto-submit` feature from the `quarantine` daemon. CLI Changes: Removed `antivirus quarfilepattern` and `auto-submit` related attributes from `antivirus quarantine`.
198439	Disable revision history by default.
198443	Added log message for `ext2` errors.
200195	Unable to show the current network service mode using diagnose commands.

Upgrade

Table 20: Resolved upgrade issues

Bug ID	Description
190948	Several default profiles are not created after upgrade.
191099	*Firmware Details* comment is overwritten after upgrade.
191453	`Netscan` fails to run after upgrading from FortiOS v4.0 to FortiOS v5.0.

Table 20: Resolved upgrade issues (continued)

Bug ID	Description
191993	The multicast policy is lost if the source and destination interface are unset.
192177	Captive portal issue after upgrading.
192184	Deep inspection options for SSL VPN policy are missing after upgrading from FortiOS v5.0 build 0128.
192276	Web filter profile `log-all-url` options are incorrect after upgrading.
192919	The firewall protocol upgrade code causes the `cmdbsvr` process to crash.
192921	Multicast policy configuration issue after upgrading.
195574	After upgrading from FortiOS v5.0 build 0128, `policy-auth-concurrent` will reset to `0`.
196228	FortiGuard is disabled in the web filter profile after upgrading.

WAN Optimization and Web Proxy

Table 21: Resolved WAN optimization and web proxy issues

Bug ID	Description
186823	ICAP does not work over web proxy response mode.
189266	Web proxy forward server forwards HTTP traffic to the wrong TCP port.
192222	In a forward server environment, HTTPS traffic caused a `wad` process crash.
194696	When processing HTTPS deep scan on explicit web proxy traffic the `wad` process crashed.
195367	Explicit proxy web filter requires `utm-extended log` to be enabled on the profile to display the hostname in logs.
195770	FSSO guest authentication group in explicit proxy issue.
196297	When web cache is enabled, the `wad` process causes a memory leak.
198826	Explicit SSL proxy for SSL negotiation with DH issue.

Web-based Manager

Table 22: Resolved Web-based Manager issues

Bug ID	Description
156340	The SSL re-negotiation feature can be used for a DoS attack.
164114	Packet capture display pane shrunk after switching between the log detail and archive tabs.
164544	Different checksum for virus log from the Web-based Manager.

Table 22: Resolved Web-based Manager issues (continued)

Bug ID	Description
165091	Cannot delete the `cache-exemption-list` from the Web-based Manager.
166103	IPv6 routing monitor page improvements.
170910	The *Traffic History* widget is displayed incorrectly in Google Chrome.
174180	Increased the length of the comment field to 256 characters.
176060	The Web-based Manager lists VLAN interfaces multiple times if it is associated with an IPsec tunnel interface.
178427	DHCP IP reservations are lost when adding or editing an invalid MAC address.
182386	The firewall VIP's real server cannot be displayed on the Web-based Manager if the virtual server name contains a space.
185378	The `log-all-url` field should not be shown in the threat column when the category is empty.
188936	Entry not found error after applying a user with accented characters in an identify-based policy.
189604	The select service search bar should not be movable.
190513	An administrative user with an *and* (&) sign in the name cannot log into the Web-based Manager.
191509	The web filter custom category should be disabled *per-profile* in the Web-based Manager.
192006	Web-based Manager display issue on DFS channel.
192055	The *System Resources* dashboard widget displays two different disk usage icons.
192113	A managed FortiSwitch cannot authorize or de-authorize using the right-click menu options.
192136	Issue loading a firewall policy when objects have slashes (/) in the name.
192514	The scroll-bar is missing on the *Historical Top Clients by Bandwidth* dashboard widget.
192745	Editing a rule via the Web-based Manager in a transparent mode VDOM with NAT configured results in a *Empty values are not allowed* error.
193700	*Entry not found error* when creating a web proxy policy.
195220	The software switch displays incorrect interfaces.
198122	Only show an alert console message for a new firmware upgrade.

Table 22: Resolved Web-based Manager issues (continued)

Bug ID	Description
Multiple	Multiple Web-based Manager dialog improvements. Bug ID: 193196, 183127, 157923, 190426, 162996, 197640, 165783, 167712, 196191, 177848, 173582, 192429, 182848, 194229, 187172
Multiple	Multiple Web-based Manager fixes. Bug ID: 197418, 197207, 192396, 182730, 195068, 196341, 194320, 163589, 197403, 196599, 182938, 197540, 182524, 194179, 190132, 198831, 189082, 195161, 198481, 194640, 196795, 195341, 188557, 191984, 189097, 189092, 191324, 189623, 182094, 193390, 197085, 180690, 195383

Web filtering

Table 23: Resolved web filtering issues

Bug ID	Description
121776	Rating issues when handling HTTP requests with a long path component.
164898	Ensure that filters can be set to *block* when the unrated category is in quota.
186322	When enabling IPS or application control, the DNS based web filter does not work.
188571	FortiGuard quota page does not display information until restarting the `urlfilter` process.
191120	The *Allow Websites When a Rating Error Occurs* does not work as expected.
192415	URL filter services are not able to connect to the FortiGate after a reboot.
193310	If `cookie-override` is allowed in web filter profile, the FortiGuard URL category will rated as *unrated.* There is no for FortiGuard web filter blocking.
194591	The `scanunit` process crashed when web filter content filtering is enabled.
196200	bing.com and yandex.com safe search issue.
196358	The FortiGuard web filter category authenticate action does not work with a proxy enabled browser.

Wireless

Table 24: Resolved wireless issues

Bug ID	Description
157663	WiFi channel bonding caused irregular radio behavior.
181467	When the physical interface captive portal was changed the WiFi interface was also changed.
185830	The `device-acl` does not deny the `all` category on WiFi interfaces.

Table 24: Resolved wireless issues (continued)

Bug ID	Description
189725	WiFi controller default working channel display issue.
191295	The console printed out a 802.1X authentication procession when a client attempted to connect to a WPA-Enterprise virtual AP.
192574	When the `echo-interval` value was changed the FortiAP disconnected.
192789	A phone hot-spot was detected as a rogue AP on-wire even though it was offline.
193679	A kernel panic occurred when client mode was configured.
195462	WiFi MAC address filtering does not work switch interfaces.
195753	`ca_acd` daemon memory leak issue.

Known Issues

The known issues tables listed below do not list every bug that has been reported with FortiOS v5.0 Patch Release 2 build 0179. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

IPS

Table 25: Known IPS issues

Bug ID	Description
197454	FG-3240C will not offload either interface policy or DoS Policy for either of the ingress or the egress interfaces to the NP4 interface. Instead, traffic is handled by the IPS Engine on the CPU side.

Logging and Reporting

Table 26: Known logging and reporting issues

Bug ID	Description
200750	FortiGate generates duplicate reports when the report option is set to *weekly*.

System

Table 27: Known system issues

Bug ID	Description
176884	SNMP `ifindex` changed dynamically when deleting an interface.
193148	The interfaces for the ASM-CE4 module may fail to be recognized on the FG-310B, FG-620B, and FG-3016B.
195221	Traffic cannot pass a FG-100D shared port when connected to a FortiSwitch.
200564	The `diag sys ha status` CLI command prints duplicate HA related messages. ***Workaround***: Press *CTRL+C* to exit the command.

Web-based Manager

Table 28: Known Web-based Manager issues

Bug ID	Description
199555	A VDOM *prof_admin* user encounters a *Permission denied* error when trying to create or edit interface.
199779	User may encounter HTTP issue when editing the HA settings from the Web-based Manager.
200301	Unable to complete device registration in *System* > *Config* > *FortiGuard*.

Upgrade

Table 29: Known upgrade issues

Bug ID	Description
196717	The Web-based Manager default log-device setting on the FG-60C is changed to disk during an upgrade from FortiOS v4.0 MR3 build 0656 to FortiOS v5.0 build 0175. When upgrading from FortiOS v5.0 build 0147 to build 0175 the disk log setting is changed to disabled.
200057	An uninterruptible upgrade will not work with FG-100D when upgrading from FortiOS v4.0 MR3 to FortiOS v5.0. ***Workaround***: Disable the `uninterruptible-upgrade` setting before the upgrade. See FortiGate 100D upgrade and downgrade limitations.
200286	When upgrading from FortiOS v4.0 MR3 to v5.0 the `config log fortianlyzer` setting will be lost if `set fp-device` is enabled.
201698	Unable to create an HA cluster between a FG-100D running FortiOS v5.0.0 or later and a FG-100D upgraded from FortiOS v4.0 MR3 to v5.0.0 or later. ***Workaround***: Remove the `lan` interface and re-generate the `internal` interface. See FortiGate 100D upgrade and downgrade limitations.

Limitations

This section outlines the limitations in FortiOS v5.0 Patch Release 2.

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,

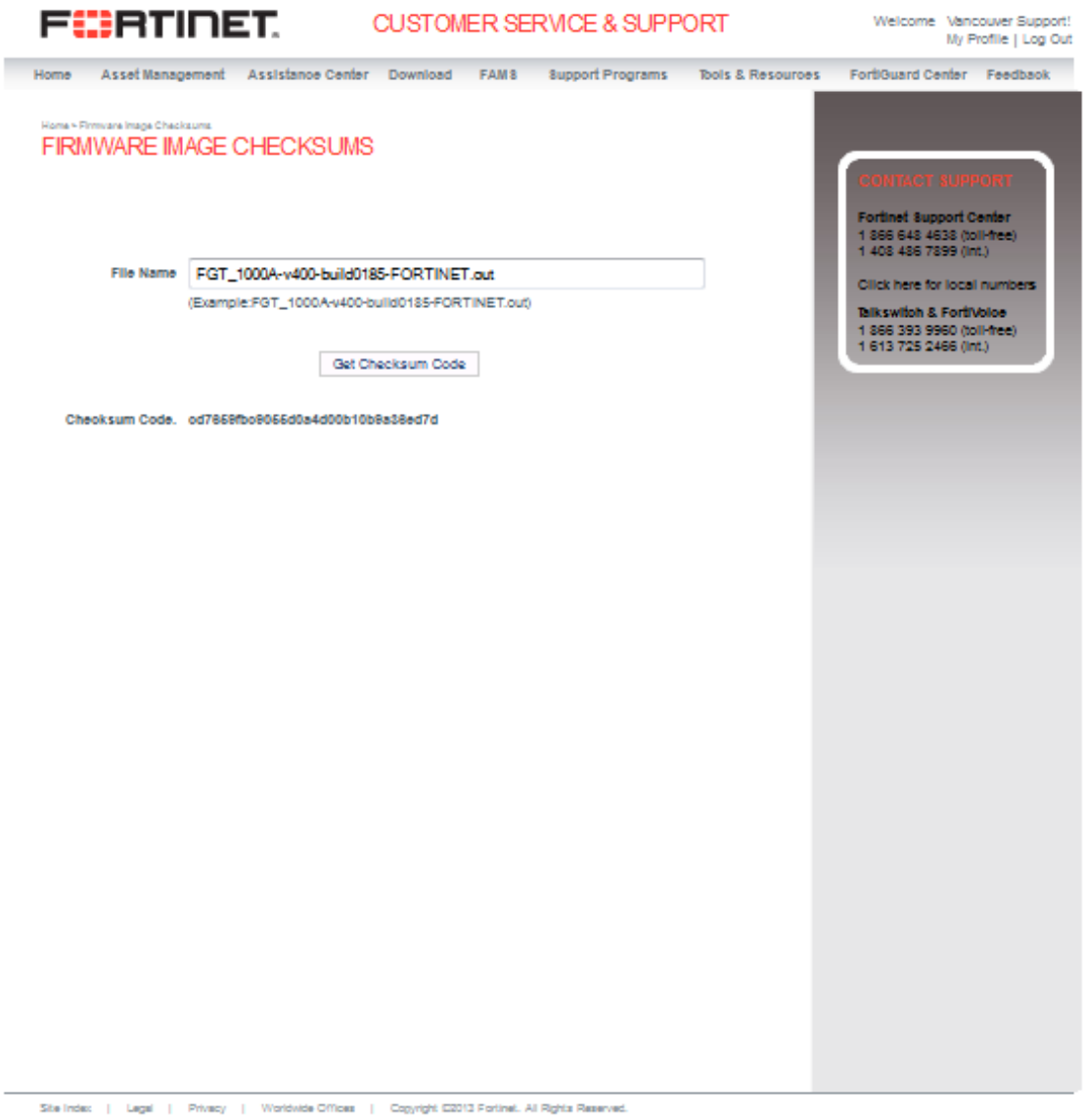
```
config user device
  edit "win"
    set mac 01:02:03:04:05:06
  next
end


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.

Image Checksum

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support website located at https://support.fortinet.com. After logging in, click on *Download* > *Firmware Image Checksum*, enter the image file including the extension, and select *Get Checksum Code*.

Figure 1: Firmware image checksum tool



Appendix A: FortiGate VM

FortiGate VM system requirements

The following table provides a detailed summary on FortiGate VM system requirements.

Table 30: FortiGate VM system requirements

Technical Specifications	Requirement
Hypervisor Support	VMware ESX / ESXi 4.0, 4.1, 5.0, and 5.1
Virtual Machine Form Factor	Open Virtualization Format (OVF)
Virtual CPUs Supported (Minimum / Maximum)	1 / 8
Virtual NICs Supported (Minimum / Maximum)	2 / 10
Storage Support (Minimum / Maximum)	30GB / 2TB
Memory Support (Minimum / Maximum)	512GB / 12GB (varies per VM level)
High Availability 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 FortiOS VM firmware images in two formats:

- `.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.