FortiOS v5.0 Patch Release 6

Release Notes

FortiOS v5.0 Patch Release 6 Release Notes

February 5, 2014

01-506-228788-20140205

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

Table of Contents

Change Log

Date	Change Description
February 5, 2014	Re-wrote the following two sections so that they are the same for FortiOS Release 5.0 Patches 4, 5 and 6: • "Disk logging disabled by default on some models (Log to FortiCloud instead)" on page 13 • "FG-60D/FWF-60D logging to disk" on page 14 Added a new feature about selecting services for SSL VPN configurations to "Summary of enhancements" on page 8. Added a new item about section view on the firewall policy page to "Default setting/CLI changes/Max values changes" on page 13.
January 31, 2014	Added resolved issue "224725" on page 39.
January 24, 2014	Initial release.

Introduction

This document provides a summary of enhancements, support information, and installation instruction to upgrade your device to FortiOS v5.0 Patch Release 6 build 0271. 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 6.

FortiGate

FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-80C, FG-80CM, FG-90D, FGT-90D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-240D, FG-280D-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.

FortiGate Rugged

FGR-100C

FortiWiFi

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

FortiGate VM

FG-VM32, FG-VM64, and FG-VM64-XEN, FG-VM64-KVM, and FG-VM64-HV

FortiSwitch

FS-5203B

FortiCarrier

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

FortiOS v5.0 Patch Release 6 FortiCarrier images are delivered upon request and are not available on the customer support firmware download page. See "Upgrading older FortiCarrier specific hardware" on page 10.

Summary of enhancements

The following is a list of enhancements in FortiOS v5.0 Patch Release 6 build 0271. For more information about new features in FortiOS v5.0 Patch Release 6 see Whats New in FortiOS 5.0.

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

- When creating an SSL VPN policy you no longer select a service in the policy. Instead services are selected as part of the SSL VPN portal configuration (231200).
- Endpoint Control: FortiClient Licence Limit Increased

  The number of FortiClient licences per FortiGate unit has increased from 8k to 16k.

  To reduce the performance impact of the increased number of licenses some efficiency changes were made to how Endpoint Control handles data. As a result of these changes you can configure FortiClient keepalive and full-keepalive timeouts using the following command:

  ```
  config endpoint-control settings
    set forticlient-keepalive-interval <interval>
    set forticlient-sys-update-interval <interval>
  end
  ```

  where:

  `forticlient-keepalive-interval` is the interval between two KeepAlive messages from FortiClient (in seconds).

  `forticlient-sys-update-interval` is the interval between two system update messages from FortiClient (in minutes).

  Setting these intervals higher reduces the Endpoint Control performance demands on the FortiGate CPU but can reduce how accurately the FortiGate unit can track FortiClient status.
- Disable Disk Logging on FortiGate-3000 and 5000 products

  Logging to disk can affect FortiGate performance, plus some units log to flash drives that may have a shorter life expectancy from constant access to save log messages. When a FortiGate-3000 or 5000 series model running FortiOS v5.0 Patch Release 6 is set to factory defaults the system is set to log to memory. You can enable disk logging from the CLI.

Upgrading a FortiGate unit to FortiOS v5.0 Patch Release 6 does not change the logging configuration.

- Control the number of miglogd child processes from the CLI

  You can use the following command to configure the maximum number of miglogd child processes that can run at a time. miglogd is the FortiOS logging daemon. FortiOS can increase the number of miglogd child processes running to keep up with logging requirements. Running more miglogd child processes can affect FortiGate performance. You can use the following command to change the maximum number of allowed miglogd child processes:

  ```
  config sys global
    set miglogd-children <integer>
  end
  ```

  The default number of child processes is 8. The range is 0 to 15. Reduce the number to reduce the system resources being used for logging. Log messages are not lost if you reduce the number of child processes.

- Non-block CRL update over SCEP added.
- New CLI commands to change some IPS hardware acceleration settings for network processors (NPx) and content processor (CPx). Previously one command was available for changing hardware acceleration settings:

  ```
  config ips global
    set hardware-accel-mode {engine-pick | none | CP-only | NP-only
         | NP+CP}
  end
  ```

  The functionality of this command has been separated into two commands:

  ```
   config ips global
    set np-accel-mode {none | basic}
    set cp-accel-mode {none | basic | advanced}
  end
  ```

  The network processor acceleration modes are:

  `none`: Network Processor acceleration disabled

  `basic`: Basic Network Processor acceleration enabled

  The network processor acceleration modes are:

  `none`: Content Processor acceleration disabled

  `basic`: Basic Content Processor acceleration enabled

  `advanced`: Advanced Content Processor acceleration enabled

- All CRL and SCEP features support IPv6, including IPv6 URLs in certificates.
- The extended IPS signature database is now available on D-series desktop model FortiGate models.
- The wireless controller (max. 2 APs) is now available for the FortiGate-30D series.
- FWF-30D, FGT-30D, FWF-30D-POE, and FGT-30D-POE models can now act as wireless controllers and manage one or two FortiAPs.

Special Notices

New FortiOS Carrier features

Changes to licensing

Prior to FortiOS 5.0, only FortiCarrier-specific hardware could run FortiOS Carrier 4.0. Starting with FortiOS 5.0.2, the FortiOS Carrier Upgrade License can be applied to selected FortiGate models to activate FortiOS Carrier features. There is no support for FortiOS Carrier features in FortiOS 5.0 GA and 5.0 Patch Release 1.

At this time the FortiOS Carrier Upgrade License is supported by FortiGate models FG-3240C, FG-3950B, FG-5001B, FG-5001C, and FG-5101C. The license can also be applied to a FortiGate virtual machine (FG-VM). Future 3000, 5000, and VM series models are also expected to support FortiOS Carrier.

You can obtain a FortiOS Carrier license from your Fortinet distributor. On a FortiGate model that supports FortiOS Carrier and that is running FortiOS 5.0 Patch Release 2 or later you can use the following command to activate FortiOS Carrier features:

```
execute forticarrier-license <license-key>
```

The license key is case-sensitive and includes dashes. When you enter this command, FortiOS attempts to verify the license with the FortiGuard network. Once the license is verified the FortiGate unit reboots. When it restarts it will be running FortiOS Carrier with a factory default configuration.

You can also request that Fortinet apply the FortiOS Carrier Upgrade license prior to shipping a new unit, as part of Professional Services. The new unit will arrive with the applied license included.

Licensing and RMAs

When you RMA a FortiGate unit that is licensed for FortiOS Carrier, make sure that the FortiCare support representative handling the RMA knows about the FortiOS Carrier license. This way a new FortiOS Carrier license will be provided with the replacement unit.

Licensing and firmware upgrades, downgrades and resetting to factory defaults

After a firmware upgrade from FortiOS 5.0 Patch Release 2 or later you should not have to re-apply the FortiOS Carrier license. However, the FortiOS Carrier license may be lost after a firmware downgrade or after resetting to factory defaults. If this happens, use the same command to re-apply the FortiOS Carrier license. FortiGuard will re-verify the license key and re-validate the license.

Upgrading older FortiCarrier specific hardware

Previous versions of FortiOS Carrier run on FortiCarrier specific hardware. This includes FCR-3810A, FCR-3950B, FCR-5001A-DW, and FCR-5001B.

As long as the FortiCarrier hardware can be upgraded to FortiOS 5.0.2 or later, it can be upgraded to FortiOS Carrier 5.0.2 or later without purchasing a new FortiOS Carrier Upgrade License. You must use FortiCarrier firmware to upgrade this hardware and this firmware may not be available from the Fortinet Support Site. Please work with your Fortinet representative to ensure a smooth upgrade of these FortiCarrier models.

Changes to GPRS Tunneling Protocol (GTP) support

FortiOS Carrier 5.0 supports GTP-C v2, which is the control plane messaging protocol used over 4G-LTE 3GPP R8 software interfaces, as well as between LTE networks and older 2G/3G networks with general packet radio service (GPRS) cores.

Changes to MMS scanning

MMS scanning now includes data leak prevention (DLP) to detect fingerprinted and/or watermarked files transferred via MMS, as well as data pattern matching for data such as credit cards and social security numbers.

SCTP firewall support

LTE networks require support for the SCTP protocol to transfer control plane data between evolved NodeBs (eNBs) and the Mobility Management Entity (MME), as well as between the MME and the Home Subscriber Server (HSS). SCTP firewall support is included in FortiOS 5.0 and FortiOS Carrier 5.0. SCTP traffic is accepted by FortiOS Carrier and you can create SCTP services and security policies that use these services. All other security feature can also be added as required to security policies for SCTP services.

TFTP boot process

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

Monitor settings for Web-based Manager access

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

Before any upgrade

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

Save a copy of your FortiGate configuration prior to upgrading. To backup your FortiGate configuration, go to *System* > *Dashboard* > *Status*. In the *System Information* widget select *Backup* under *System Configuration* and save the configuration file to your local hard drive.

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

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

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

After any upgrade

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

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

Using wildcard characters when filtering log messages

While using filtering in the log message viewer you may need to add * wildcard characters to get the search results that you expect. For example, if you go to *Log & Report* > *Event Log* > *System* to view all messages with the word “logged” in them you can select the Filter icon for the *Message* list and enter the following:

logged

Including both * wildcard characters will find all messages with “logged” in them. “logged” can be at the start or the end of the message or inside the message.

If you only want to find messages that begin with the search term you should remove the leading *. If you only want to find messages that end with the search term you need to remove the trailing *.

It does not work to add a * wildcard character inside the search term. So searching for *lo*ed* will not return any results.

Default setting/CLI changes/Max values changes

- To improve GUI performance, Section View is disabled in the firewall policy page if a large number of policies exist (231219)
- Increase the maximum number of certificates on FortiGate models 1000 and up (2U models) to 500.
- Increase the maximum number of members in a firewall address group on FortiGate models 1000 and up (2U models and up) to 1500.
- New maximum value for the number of FSSO polling entries. The values are 5 for desktop models, 20 for 1U models, 100 for 2U models and up.
- FortiGate-VM8 now supports 500 VDOMs.
- Adjustments to the following max values for low end models:

  Application list: root will have 3 default, new VDOM will have 1 (previous is 3).

  IPS sensor: root will have 6 default, new VDOM will have 1 (previous is 6).

  Web Filter profile: root will have 4 default, new VDOM will have 1.

  Antivirus profile: root will have 2 default, new VDOM will have 1.

  DLP profile: root will have 6 default, new VDOM will have 1.

  Email Filtering profile: root will have 1 default, new VDOM will have 1.

IPS algorithms

For optimal performance on your FortiGate unit, the IPS algorithm can be configured via the CLI. Select one of the following modes:

- engine-pick: The IPS engine picks the best algorithm to use.
- high: This algorithm fits most FortiGate models
- low: This algorithm works best on FortiGate units with less memory (512 MB or less)
- super: This algorithm works best on FortiGate models with more memory (more than 4 GB)

To configure the algorithm, use the following CLI commands:

```
config ips global
  set algorithm [engine-pick | high | low | super]
end
```

Disk logging disabled by default on some models (Log to FortiCloud instead)

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

- FG-20C, FWF-20C
- FG-20C-ADSL-A, FWF-20C-ADSL-A
- FG-40C, FWF-40C
- FG-60C, FWF-60C, FG-60C-POE, FWF-60CM, FWF-60CX-ADSL-A
- FG-60D, FWF-60D, FG-60D-POE, FWF-60DM, FWF-60DX-ADSL-A
- FG-80C, FWF-80C, FG-80CM, FWF-80CM
- FG-100D (PN: P09340-04 or earlier)

- FG-300C (PN: P09616-04 or earlier)
- FG-200B/200B-PoE (if flash is used as storage)

If you were logging to FortiCloud prior to upgrading to FortiOS v5.0 Patch Release 6, the settings are retained and logging to FortiCloud continues to operate normally. If you were logging to disk prior to upgrading, logging to disk may be disabled during the upgrade process.

If required, you can enable disk logging from the CLI using the following command:

```
config log disk setting
  set status enable
end
```

If you enable disk logging on the models listed above, the CLI displays a message reminding you that enabling disk logging impacts overall performance and reduces the lifetime of the unit.

A code limitation specific to the FG-80C, FG-80CM, FWF-80C, and FWF-80CM models prevents the warning message from being displayed.

FG-60D/FWF-60D logging to disk

If you enable logging to disk for FG-60D and FWF-60D models, Fortinet recommends that you format the log disk using the following CLI command:

```
execute formatlogdisk
Log disk is /dev/sda1.
Formatting this storage will erase all data on it, including logs,
     quarantine files; WanOpt caches; and require the unit to reboot.
Do you want to continue? (y/n) [Enter y to continue]
```

WAN Optimization

In FortiOS 5.0, WAN Optimization is enabled in security policies and WAN Optimization rules are no longer required. Instead of adding a security policy that accepts traffic to be optimized and then creating WAN Optimization rules to apply WAN Optimization, in FortiOS v5.0 you create security policies that accept traffic to be optimized and enable WAN Optimization in those policies. WAN Optimization is applied by WAN Optimization profiles which are created separately and added to WAN Optimization security policies.

MAC address filter list

The `mac-filter` CLI command under the `config wireless-controller vap` setting is not retained after upgrading to FortiOS v5.0 Patch Release 6. 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 6. 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 6. The DLP rule settings have been moved inside the DLP sensor.

Limiting access for unauthenticated users

When configuring User Identity policies, if you select the option *Skip this policy for unauthenticated user* the policy will only apply to users who have already authenticated with the FortiGate unit. This feature is intended for networks with two kinds of users:

- Single sign-on users who have authenticated when their devices connected to their network
- Other users who do not authenticate with the network so are “unauthenticated”

Sessions from authenticated users can match this policy and sessions from unauthenticated users will skip this policy and potentially be matched with policies further down the policy list. Typically, you would arrange a policy with *Skip this policy for unauthenticated user* at the top of a policy list.

You can also use the following CLI command to enable skipping policies for unauthenticated users:

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

Use case - allowing limited access for unauthenticated users

Consider an office with open use PCs in common areas. Staff and customers do not have to log in to these PCs and can use them for limited access to the Internet. From their desks, employees of this office log into PCs which are logged into the office network. The FortiGate unit on the office network uses single sign-on to get user credentials from the network authentication server.

The open use PCs have limited access to the Internet. Employee PCs can access internal resources and have unlimited access to the Internet.

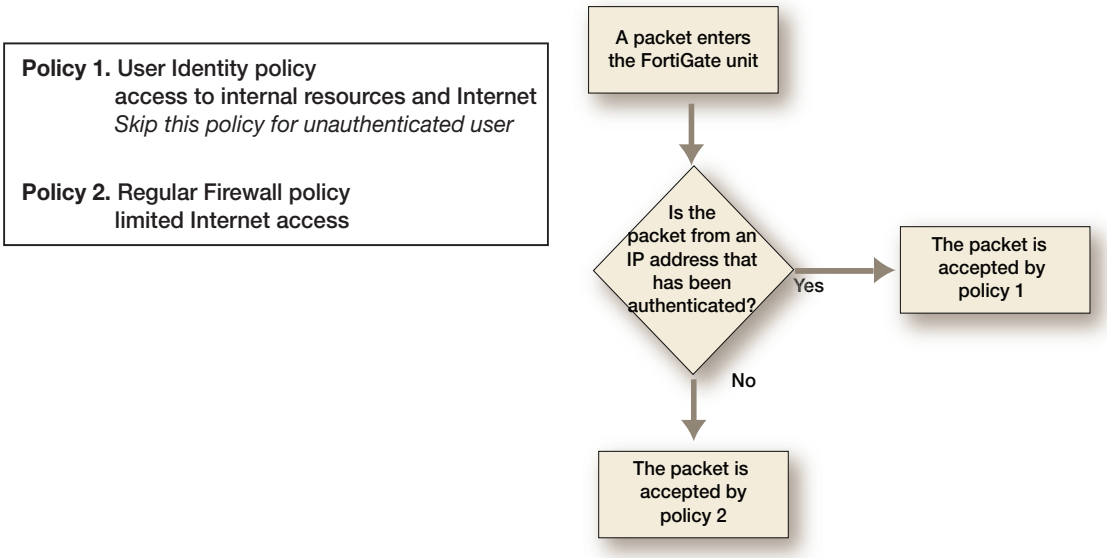
To support these different levels of access you can add a user identity policy to the top of the policy list that allows authenticated users to access internal resources and to have unlimited access to the Internet. In this policy, select *Skip this policy for unauthenticated user*.

Add a normal firewall policy below this policy that allows limited access to the Internet.

Sessions from authenticated PCs will be accepted by the User Identity policy. Sessions from unauthenticated PCs will skip the User Identity policy and be accepted by the normal firewall policy.

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

Figure 1: Packet flow for authenticated and unauthenticated users



Use case - multiple levels of authentication

As a variation of the above use case, Policy 2 could be a User Identity policy and *Skip this policy for unauthenticated user* would not be selected. Sessions from unauthenticated users that are accepted by Policy2 would now require users to authenticate before traffic can connect through the FortiGate unit. The result is different levels of authentication: Single sign on for some users and firewall authentication for others.

FortiGate 100D upgrade and downgrade limitations

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

32-bit to 64-bit version of FortiOS

With the release of FortiOS v5.0.0 or later, the FortiGate 100D will run a 64-bit version of FortiOS. This has introduced certain limitations on upgrading firmware in a high availability (HA) environment and downgrading.

When performing an upgrade from a 32-bit FortiOS version to a 64-bit FortiOS version and the FortiGate 100Ds are running in a HA environment with the uninterruptable-upgrade option enabled, the upgrade process may fail on the primary device after the subordinate devices have been successfully upgraded. To work around this situation, users may disable the uninterruptable-upgrade option to allow all HA members to be successfully upgraded. Without the uninterruptable-upgrade feature enabled, several minutes of service unavailability are to be expected.

Downgrading a FortiGate 100D from FortiOS v5.0.0 or later is not supported due to technical limitations between 64-bit and 32-bit versions of FortiOS. The only procedure to downgrade firmware is by using the TFTP server and BIOS menu to perform the downgrade. In this case the configuration will need to be restored from a previously backed up version.

Internal interface name/type change

In FortiOS v5.0.0 or later the internal interface has been renamed `lan` and the type of the interface has changed to `hard-switch`. In order to create an HA cluster between a FortiGate 100D shipped with FortiOS v5.0.0 or later with a FortiGate 100D upgraded from FortiOS v4.0 MR3, you must first remove the `lan` interface and re-generate the `internal` interface to match the interface on the upgraded device.

Use the following CLI commands to remove the `lan` interface and re-generate the `internal` interface.

```
# config firewall policy
(policy) # purge
  This operation will clear all table!
  Do you want to continue? (y/n)y
(policy) # end

# config system dhcp server
(server) # purge
  This operation will clear all table!
  Do you want to continue? (y/n)y
(server) # end

# config system virtual-switch
(virtual-switch) # purge
  This operation will clear all table!
  Do you want to continue? (y/n)y
(virtual-switch) # end

# config system global
(global) # set internal-switch-mode switch
(global) # end
  Changing switch mode will reboot the system!
  Do you want to continue? (y/n)y
```

Upgrade Information

Upgrading from FortiOS v5.0 Patch Release 4 or later

FortiOS v5.0 Patch Release 6 build 0271 officially supports upgrading from FortiOS v5.0 Patch Release 4or later.

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

Upgrading an HA cluster

When upgrading a high availability cluster to FortiOS v5.0 patch 6, if uninterruptable-upgrade is enabled you must always upgrade to FortiOS v5.0 Patch 4 before upgrading to patch 6. If you skip this step the firmware upgrade will fail.

Dynamic profiles must be manually converted to RSSO after upgrade

After upgrading from FortiOS v4.0 MR3 to FortiOS v5.0, dynamic profile configurations are lost and you must manually create new RADIUS Single Sign On (RSSO) configurations to maintain the old dynamic profile functionality.

Zone-related policies may be deleted when upgrading to FortiOS v5.0 Patch Release 4, 5 or 6

Policies that include interfaces that are members of a zone could be deleted when upgrading to FortiOS v5.0 Patch Release 4, 5 or 6. As of patch release 4 you cannot create policies that include interfaces that have been added to zones. The reason for this restriction is that if you have policies for interfaces added to zones and policies for zones it may not be clear which policy to match with traffic that is received by the interface.

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

Captive portal

The captive portal configuration has changed in FortiOS v5.0 Patch Release 6 and upon upgrading the previous configuration may be lost or changed. Review the following configuration examples before upgrading.

Endpoint control

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

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

```
edit 3
```

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

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

***Example FortiOS v5.0 Patch Release 6 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 6 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 6 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 6, you must enter the following CLI commands:

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


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

SSL VPN web portal

For FG-60C variants and lower models only one SSL VPN web portal is retained after upgrading to FortiOS v5.0 Patch Release 6.

Virtual switch and the FortiGate-100D

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

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

DHCP server reserved IP/MAC address list

Up to FortiOS v5.0 Patch Release 4 you could use the following command to add a system-wide reserved IP/MAC address list for all DHCP servers.

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

This command has been removed in FortiOS 5.0 Patch Release 5. If you have configured reserved IP/MAC addresses using this command, they will be lost when you upgrade to FortiOS 5.0 Patch Release 5. To keep these IP/MAC address pairs you must add them to individual DHCP server configurations, for example:

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

Upgrading from FortiOS v4.0 MR3

FortiOS v5.0 Patch Release 6 build 0271 officially supports upgrade from FortiOS v4.0 MR3 Patch Release 14 and v4.0 MR3 Patch Release 15.

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

Table size limits

FortiOS v5.0 Patch Release 6 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 6 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 6 configuration:

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

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

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

Upgrade procedure

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

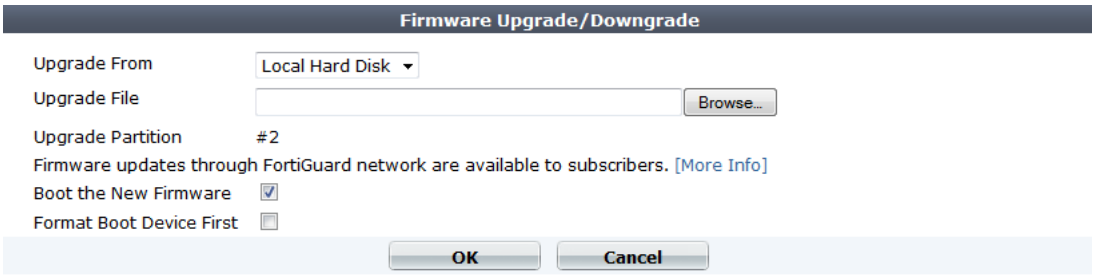
Save a copy of your FortiGate device configuration prior to upgrading. To backup your configuration, go to *System* > *Dashboard* > *Status*. In the *System Information* widget select *Backup* under *System Configuration*. Save the configuration file to your management computer.

To upgrade the firmware via the Web-based Manager:

1. Download the `.out` firmware image file from the Customer Service & Support portal FTP directory to your management computer.
2. Log into the Web-based Manager as the `admin` administrative user.
3. Go to *System* > *Dashboard* > *Status*.
4. In the *System Information* widget, in the *Firmware Version* field, select *Update*.

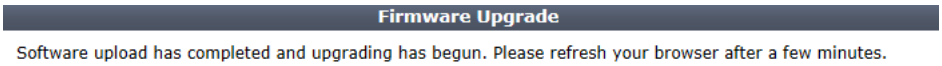
   The *Firmware Upgrade/Downgrade* window opens.

   Figure 2: Firmware upgrade/downgrade window

5. Select *Browse* and locate the firmware image on your management computer and select *Open*.
6. Select *OK*. The FortiGate unit uploads the firmware image file, upgrades to the new firmware version. The following message is displayed.

   Figure 3: Firmware upgrade dialog box

7. Refresh your browser and log back into your FortiGate device. Launch functional modules to confirm that the upgrade was successful.

For more information on upgrading your FortiGate device, see the *Install and System Administration for FortiOS 5.0* at http://docs.fortinet.com/fgt.html.

SQL database error

When upgrading to FortiOS v5.0 Patch Release 6, the FortiGate may encounter a *SQL Database Error*.

Workaround: After the upgrade, rebuild the SQL database.

Downgrading to previous FortiOS versions

Downgrading to previous FortiOS versions results in configuration loss on all models. Only the following settings are retained:

- operation modes
- interface IP/management IP
- route static table
- DNS settings
- VDOM parameters/settings
- admin user account
- session helpers
- system access profiles.

Product Integration and Support

Web browser support

FortiOS v5.0 Patch Release 6 supports the following web browsers:

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

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

FortiManager support

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

FortiAnalyzer support

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

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

FortiOS v5.0 Patch Release 6 is supported by the following FortiClient software versions:

- FortiClient (Windows) v5.0 Patch Release 7or later
  - Microsoft Windows 8.1 (32-bit and 64-bit)
  - Microsoft Windows 8 (32-bit and 64-bit)
  - Microsoft Windows 7 (32-bit and 64-bit)
  - Microsoft Windows Vista (32-bit and 64-bit)
  - Microsoft Windows XP (32-bit)
- FortiClient (Mac OS X) v5.0 Patch Release 7or later
  - Mac OS X v10.9 Mavericks
  - Mac OS X v10.8 Mountain Lion
  - Mac OS X v10.7 Lion
  - Mac OS X v10.6 Snow Leopard

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

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

FortiAP support

FortiOS v5.0 Patch Release 6 supports the following FortiAP models:

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

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

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

FortiSwitch support

FortiOS v5.0 Patch Release 6 supports the following FortiSwitch models:

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

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

FortiOS v5.0 Patch Release 6 supports the following FortiSwitch 5000 series models:

FS-5003B, FS-5003A

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

FortiController support

FortiOS v5.0 Patch Release 6 supports the following FortiController models:

FCTL-5103B

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

Virtualization software support

FortiOS v5.0 Patch Release 6 supports the following virtualization software:

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

See “About FortiGate VMs” on page 49 for more information.

Fortinet Single Sign-On (FSSO) support

FortiOS v5.0 Patch Release 6 is supported by FSSO v4.0 MR3 B0151 for the following operating systems:

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

FSSO does not currently support IPv6.

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

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

FortiOS v5.0 Patch Release 6 is supported by FortiExplorer v2.3 build 1052 or later. See the *FortiExplorer v2.3 build 1052 Release Notes* for more information.

FortiOS v5.0 Patch Release 6 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 6 is supported by AV Engine v5.146 and IPS Engine v2.179.

Language support

The following table lists FortiOS language support information.

Table 1: FortiOS language support

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

To change the FortiGate language setting, go to *System* > *Admin* > *Settings*, in *View Settings* > *Language* select the desired language from the drop-down menu.

Module support

FortiOS v5.0 Patch Release 6 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
Rear Transition Module 10-GbE backplane fabric (RTM-XB2)	FG-5001A

Table 2: Supported modules and FortiGate models (continued)

Security Processing Module 2x10-GbE SFP+ (FMC-XG2)	FG-3950B, FG-3951B
Accelerated Interface Module 2x10-GbE SFP+ (FMC-XD2)	FG-3950B, FG-3951B
Accelerated Interface Module 20xSFP (FMC-F20)	FG-3950B, FG-3951B
Accelerated Interface Module 20x10/100/1000 (FMC-C20)	FG-3950B, FG-3951B
Security Processing Module (FMC-XH0)	FG-3950B

SSL VPN support

SSL VPN standalone client

FortiOS v5.0 Patch Release 6 supports the SSL VPN tunnel client standalone installer build 2297 for the following operating systems:

- Microsoft Windows 8.1 (32-bit & 64-bit), 8 (32-bit & 64-bit), 7 (32-bit & 64-bit), and XP SP3 in `.exe` and `.msi` formats
- Linux CentOS and Ubuntu in `.tar.gz` format
- Mac OS X v10.9, 10.8 and 10.7 in `.dmg` format
- Virtual Desktop in `.jar` format for Microsoft Windows 7 SP1 (32-bit)

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

SSL VPN web mode

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

Table 3: Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 32-bit SP1	Microsoft Internet Explorer versions 8, 9, 10 and 11 Mozilla Firefox version 26
Microsoft Windows 7 64-bit SP1	Microsoft Internet Explorer versions 8, 9, 10 and 11 Mozilla Firefox version 26
Linux CentOS version 5.6 and Ubuntu version 12.0.4	Mozilla Firefox version 5.6
Mac OS X v10.9 Maverick	Apple Safari version 7

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

SSL VPN host compatibility list

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

Table 4: 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 5: Supported Windows 7 32-bit and 64-bit antivirus and firewall software

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

Explicit web proxy browser support

The following web browsers are supported by FortiOS v5.0 Patch Release 6 for the explicit web proxy feature:

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

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

Resolved Issues

This chapter describes issues with FortiOS v5.0 Patch Release 5 that have been resolved for FortiOS v5.0 Patch Release 6 build 0271. For inquires about a particular bug, please contact Customer Service & Support.

This chapter contains the following sections:

- Resolved Issues from FortiOS v5.0 Patch Release 5 Release Notes
- Resolved Issues in FortiOS v5.0 Patch Release 6

Resolved Issues from FortiOS v5.0 Patch Release 5 Release Notes

The following resolved issues were listed as known issues in the FortiOS v5.0 Patch Release 5 Release Notes.

Upgrade

Table 6: Resolved upgrade issues

Bug ID	Description
221412	Resolved an issue that caused a time out when upgrading from FortiOS v5.0 build 228 to FortiOS v5.0 Patch Release 5.
0222400	Resolved an issue that blocked access to WAN Optimization storage after a fresh install of FortiOS 5.0 Patch Release 5 on FG-60C and FWF-60C-ADSL models.
0221684	Dynamic Profile configurations must be upgraded manually to RSSO when upgrading from FortiOS v4.0 MR3 to v5.0.

Web-based Manager

Table 7: Resolved Web-based Manager issues

Bug ID	Description
0220056	The Web-based Manager now displays an application sensor properly when the sensor contains an application that is not found in either the built-in or custom application database.

Web Filtering

Table 8: Resolved Web FIltering issues

Bug ID	Description
0219352	Bing video SafeSearch now works as expected.

Wireless

Table 9: Resolved Wireless issues

Bug ID	Description
0212959	The FWF-80CM supports 7 local radio SSIDs.

Resolved Issues in FortiOS v5.0 Patch Release 6

The following issues have been resolved in FortiOS v5.0 Patch Release 6. These issues were not listed in the FortiOS v5.0 Patch Release 5 Release Notes. (Some or all of them may have been found and resolved after FortiOS v5.0 Patch Release 5 was released.)

AntiVirus

Table 10: Resolved antivirus issues

Bug ID	Description
184308	Improved HTTP header parsing when non-compliant line endings are used to mark the end of headers.
221385	The correct virus name now appears in botnet detection logs.

DLP

Table 11: Resolved DLP issues

Bug ID	Description
223555	DLP correctly detects social security or credit cards numbers in email subjects.
220013	DLP correctly parses filenames in SMTP email.
223765	The SSN and Credit card data field separation procedure used in DLP for docx files works correctly.

ELBC

Table 12: Resolved ELBC issues

Bug ID	Description
224481	Link state synchronization operates correctly on content-cluster worker blades.

Firewall

Table 13: Resolved firewall issues

Bug ID	Description
223330	Resolved an issue that caused High CPU and connection acceptance issues with the SSL proxy.
224604	Antivirus is correctly applied on HTTP PUT requests.
218871	Resolved an issue that caused session clashes.
221691	Resolved an issue that caused some VIPs to stop working after 30 to 60 minutes.
225558	Resolved an issue that caused the Fortinet bar to stop refreshing web pages after a successful logout.
202918	The transparent proxy now correctly handles 100 continue in POST method.
218174	Resolved an issue that caused high CPU and connection acceptance issues with the SSL proxy.
221388	Resolved an issue that caused Sflow traffic capture to show s incorrect frame lengths.
225480	FortiOS properly stores the message sent by a server in response to a client's DATA request.
224267	VIP addresses can be used for source NAT IPs when static VIPs and dynamic IP pools are combined and the VIP address as NAT source IP option is enabled.
225220	Resolved an issue that caused 'SCCP connection to a.b.c.d:2000 failed' messages.
212694	Resolved an issue that caused DLP file pattern extension match issues.
223332	Resolved an issue that caused FTP to stall due with some special file patterns.
222550	Resolved an issue that caused incorrect parsing of user names in the FTP proxy.
223953	Support deep inspection of sites with very long certificate chains.
225508	STARTTLS commands sent to a server are not modified by FortiOS.
220488	Resolved an issue that caused the proxy worker to crash with signal 11 due to a stack overflow when FortiGuard web filtering is enabled.
229085	Hairpin NAT now works correctly.

FortiOS Carrier

Table 14: Resolved FortiOS Carrier issues

Bug ID	Description
221890	Resolved an issue that caused "msisdn-prefix" basic filtering to stop working in "imsi" configuration of GTP profiles.
223944	Resolved an issue that caused GTP secondary context tear down problems when deleting primary context.
222437	Resolved an issue that caused reloading the config file or a FortiGate restart to loose the `set ovrd-scope-browser`. setting.

FortiGate-VM

Table 15: Resolved FortiGate-VM issues

Bug ID	Description
207881	Resolved an issue that caused the SSH key to remains on a LENC model after applying a license for full encryption.

High Availability

Table 16: Resolved high availability issues

Bug ID	Description
224103	FortiGate-3600C failover speed improved.
216574	RTP session are kept alive in TCP SIP traffic after HA failover.
228562	Resolved an issue that caused dedicated HA management interfaces to have the same virtual MAC on both cluster members after a failover.
224725	Resolved an issue that caused upgrading cluster firmware from FortiOS 4.3 to fail and CPU usage on the primary unit to stay at 99%.

IPsec VPN

Table 17: Resolved IPsec VPN issues

Bug ID	Description
221504	Traffic history now available for ipsec_phase1 and ipsec_manualkey interfaces in interface filter.
226825	Resolved an issue that caused IPv6 packets of IPsec with AH header to dropped by FortiOS without recording a log message.
213429	Resolved an issue that caused the iked daemon to crash when a dialup peer address was changed.
222822	Resolved an issue that caused 'Peertype' and 'Peerid' to be removed from the IPsec VPN configuration after a reboot.

IPv6

Table 18: Resolved IPv6 issues

Bug ID	Description
205024	Resolved an issue that caused NAT64 to use the external interface as source NAT IP when the configuration included an IPPOOL.

Logging and Reporting

Table 19: Resolved logging and reporting issues

Bug ID	Description
221752	Resolved an issue that removed web filtering information from traffic logs.
222665	Log setting views now match after enabling Client Reputation.
218865	Support NAT64 and NAT46 in compact v3 mode.
220137	Resolved an issue that caused FortiOS to send fragmented compact v3 logs to FortiAnalyzer.
226301	Resolved an issue that prevented log messages with custom traffic log fields from being sent to FortiAnalyzer.
205467	Traffic log message show correct service when there are multi-customer defined services that have same protocol/port.
220559	ICQ GUI setting and detected log have been corrected.
220407	The msg field has been added to router logs (Log id 20063).
140798	Log messages for SSL VPN tunnel traffic for both SSL VPN web and tunnel mode now include user names.
224373	IPSec event logs now include the IPsec tunnel type.

Routing

Table 20: Resolved routing issues

Bug ID	Description
221885	Resolved an issue that prevented BGP over IPv6 neighbor with password set may from working.
222255	Resolved an issue that prevented OSPF graceful restarts with multiple helpers.

SSL VPN

Table 21: Resolved SSL VPN issues

Bug ID	Description
225383	Resolved an issue that caused the sslvpnd daemon to enter conserve mode.
201689	Resolved an issue that prevented accessing RDP using SSL VPN web mode bookmarks.
226138	An SSL VPN host check successfully logs explicitly failed host check messages for unsupported OS/Browsers.
220872	SSL VPN parser works with the Dojo Toolkit.
224422	Resolved an issue with the parsec that caused high CPU usage by the SSL VPN daemon.
226088	Resolved an issue that caused memory corruption by jemalloc which resulted in SSL VPN sessions disconnecting intermittently.
226776	Resolved an issue that caused the SSL VPN Web Mode Tunnel Widget to hang when connecting to OSX

System

Table 22: Resolved System issues

Bug ID	Description
223323	SCP configuration restore command now consistent with backup command.
222647	Resolved an issue that caused a fnbamd memory leak.
224890	Resolved an issue where the NTP daemon tried to delete other sessions, including SSH and telnet sessions, instead of just NTP sessions.
227098	Resolved an issue that caused the telnetd daemon to be left as a zombie because its parent process doesn't call wait() on the child process when child process exits.
224362	Resolved an NPU switch chip issue that allowed multicast MAC addresses on FGT200D/240D/280DPOE
218106	Resolved possible flash issues with ext2_write_inode: unable to read inode block preceded by "scanunit=child exittype=exit code=255" error message.
209441	The MIB value fgProcessorPktDroppedCount is now calculated correctly.
224590	Japanese characters in replacement messages are no longer garbled after rebooting.
223293	The correct system time appears when the timezone is set to Rangoon.
225223	Resolved an issue that prevented HA management pings from being sent through the correct interface.
203547	Config pushed from FMG to FGT is no longer list after reboot.

Table 22: Resolved System issues (continued)

Bug ID	Description
190688	SNMP information can be sent over dedicated management interfaces.
226607	The RTSP helper no longer blocks the offload of a session using 7070/8554 as a source port.
207683, 204232	LACP renegotiation is no longer required after transient interface failures.
217637	Resolved an issue that caused an STP forwarding problem in one-arm Transparent mode firewalls.
217050	Resolved an issue that caused the modem interface distance and priority to be overwritten at runtime and also during system boot.
221291	Enable jumbo frames on FortiGate-60D/90D/200D internal interfaces.
222818	Timezone for Mexico (Chihuahua) GMT7 added.
221547	Resolved an issue that caused configuration backups to fail when any accprofile is named admin.
220274	Resolved an issue that caused ICMP packets to be dropped by Nturbo enabled platforms.
222680	Resolved an issue that prevented Huawei E169 from connecting due to 'PPP recv: IPCP Configure_Nak'
172475	PPPoE interface addresses are correctly output by the SNMP IP MIB.
220280	Gratuitous ARP going out from the wrong interface in Transparent mode.
226321	Resolved an issue that prevented IPv6 allow access settings from working with some configurations.
192636	Resolved an issue that prevented NP4 processors from forwarding traffic. Affected models: FortiGate-3040B, FMC-XD2, FortiGate-3240C.
224609	VLAN interface statistics are supported on XLP interfaces.
208529, 212222	Aggregate NPU session flushing improved.
227629	Resolved an issue that caused dhcpd memory leaks.
225048	Resolved an issue that caused the DSCP value to be set to 0 by switch chip on a FortiGate-100D VLAN interface.
213064	HA fail over support restored when `set lacp ha slave disable` is used.
228147	VDOM config restore correctly applies IPSec interface IPs.
227577	Resolved an issue that caused the DNS proxy to crash because it tried to insert into an entry that was found early but was freed because max limit was reached.

Table 22: Resolved System issues (continued)

Bug ID	Description
216108	Resolved an issue that caused NP4 interfaces on the FortiGate-800C to stop forwarding traffic periodically.
214737	FortiGate-3600C power supply failure SNMP trap added.
226611	Resolved an issue that caused trusted hosts to block traffic for other remote wildcard administrators.
222447	Remote wildcard admin users with `accprofile-override` can now restore the configuration on a cluster from the CLI.
221882	Resolved an issue that caused FWF-60CS-A PPPoA connections to go down after changing Allow Access settings on the ADSL interface.

Upgrade

Table 23: Resolved upgrade issues

Bug ID	Description
223515	Resolved an issue that caused an the error message “cli 38 die in an exception in line 1653” when upgrading from FortiOS 4 MR3 Patch 14 to FortiOS 5.0 MR5.

VDOM

Table 24: Resolved VDOM issues

Bug ID	Description
223932	VDOM administrators restricted to certain VDOMs can no longer see all VDOM names from the CLI.

WAN Optimization and Explicit Web and FTP Proxy

Table 25: Resolved WAN optimization and explicit proxy issues

Bug ID	Description
215001	FTP proxy replacement messages with multiple lines are now displayed correctly by FTP clients.
223223	Resolved an issue that caused a system crash when a property of a new session is not set correctly in the web-cache Transparent proxy.
219898	Resolved an issue that caused WAN Optimization to crash with signal 6 while processing IPS and HTTPS requests.
219895	Custom replacement message now load when Web caching is turned on in a policy.
017797	MAPI memory leak issues resolved.

Web-based Manager

Table 26: Resolved Web-based Manager issues

Bug ID	Description
215373	The traffic widget now displays data for PPPoE interfaces.
225375	Interfaces added to zones are now listed under Local Outgoing.
228003	Performance of system/interface DHCP reservation tables improved.
222046	VLAN interfaces are now available when configuring a policy if the parent physical interface is in a zone.
225886	Resolved issues that prevented the ability to create all to all multicast policies.
228430	Thew firewall monitor now displays the correct traffic volume for authenticated users.
227869	The option "Log Violation Traffic" can now be selected when creating a multicast policy.
228959	Policy NAT64 does not use IPv6 pool validation when adding a new pool from the GUI.

Wireless

Table 27: Resolved wireless issues

Bug ID	Description
225046	Resolved an issue that caused some FortiAP radio interfaces to randomly stop working and display an INTF_DOWN message.
221714	Added the correct country code and wireless settings for the Ukraine.

221301	Resolved WiFi performance and packet loss issues with Realtek RTL8188CE wireless clients. New command to configure 802_11g protection mode:
	`configure wireless-controller wtp-profile`
	`  config radio-1`
	`  set protection-mode {ctsonly| disable | rtscts}`
	`  end`
	Where
	`ctsonly` enables 802.11g protection CTS only mode.
	`disable` disables 802.11g protection mode.
	`rtscts` enables 802.11g protection RTS/CTS mode.

Known Issues

This chapter describes some known issues with FortiOS v5.0 Patch Release 6 build 0271. Some of the issues listed below were also known issues for FortiOS v5.0 Patch Release 5. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

FortiSwitch

Table 28: Known FortiSwitch issues

Bug ID	Description
0220692	Traffic may be interrupted if you have created two physical links between a managed FortiSwitch and a FortiGate acting as the manager but only configured one of the links as an aggregate link member. Workaround: Remove one of the links or configure both of them.

WAN Optimization and explicit proxy

Table 29: Known WAN Optimization and explicit proxy issues

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

Upgrade

Table 30: Known Upgrade issues

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

Web-based Manager

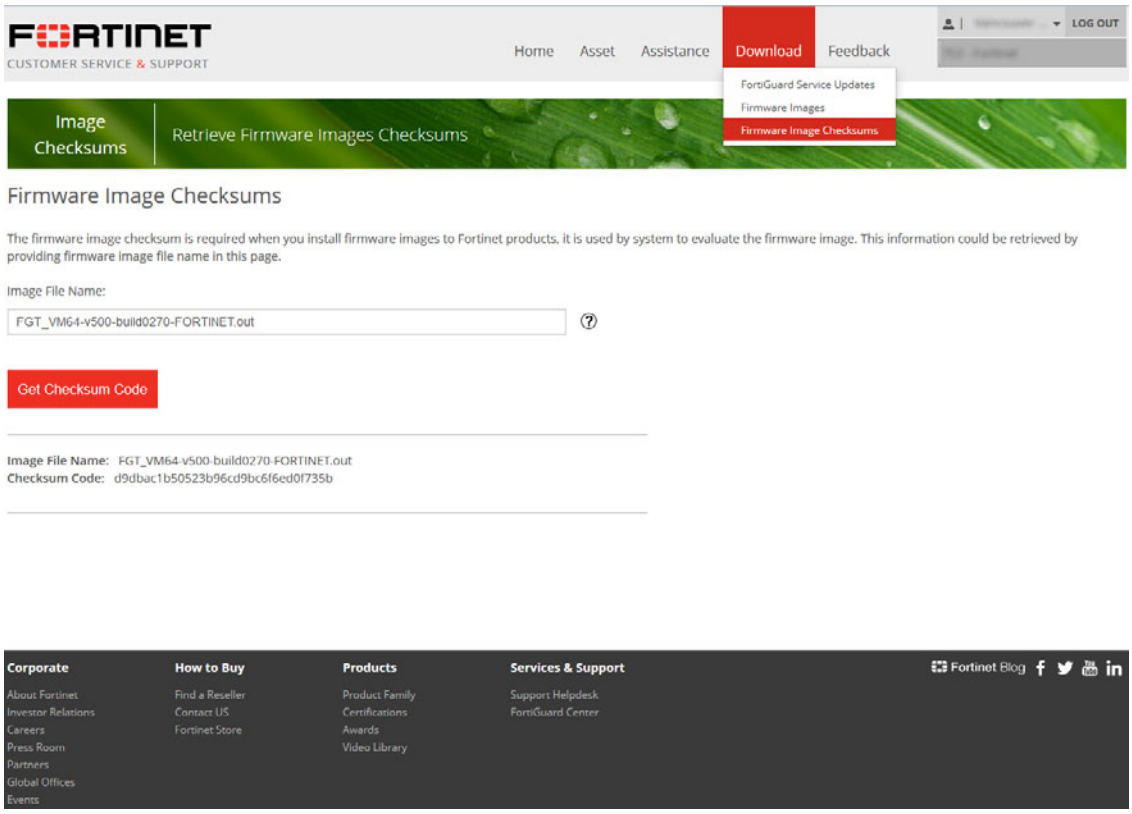
Table 31: Known Web-based Manager issues

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

Firmware Image Checksums

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

Figure 4: Firmware image checksum tool



Limitations

This section outlines the limitations in FortiOS v5.0 Patch Release 6.

Add device access list

If the `device-access-list` has the action set as `deny`, you will need to explicitly define a device in order to allow it to work.

For instance,

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


config user device-access-list
  edit "wifi"
    set default-action deny
      config device-list
        edit 1
          set action accept
          set device "windows-pc" <-the predefined device-category
        next
        edit 2
          set action accept
          set device "win" <-the custom device
        next
      end
    next
  end
```

As a result, the predefined `device-category` entry 1 will not have network access. Only the custom device entry 2 would be able to get network access.

Appendix A: About FortiGate VMs

FortiGate VM model information

Table 32: FortiGate VM model information

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

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

FortiGate VM firmware

Fortinet provides FortiGate VM firmware images for the following VM environments:

VMware

- `.out`: Download either the 32-bit or 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.ovf.zip`: Download either the 32-bit or 64-bit package for a new FortiGate VM installation. This package contains Open Virtualization Format (OVF) files for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

Xen

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the QCOW2 file for Open Source Xen.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the Citrix Xen Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Hyper-V

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.hyperv.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains three folders that can be imported by Hyper-V Manager on Hyper-V 2012. It also contains the file `fortios.vhd` in the Virtual Hard Disks folder that can be manually added to the Hyper-V Manager.

KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains `qcow2` that can be used by `qemu`.

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

Open Source Xen limitations

When using Ubuntu version 11.10, Xen version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.