FortiOS v5.0 Patch Release 8
Release Notes

FortiOS v5.0 Patch Release 8

May 25, 2016

01-508-248040-20160525

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
May 25, 2016	Added bug id 238959 to resolved issues under HA.
November 17, 2014	Added bug id 254084 as known issue in "Web-based Manager and CLI" on page 48 Added "FortiOS identity base policy behavior change" and "FortiGate-100D hardware compatibility" in "Special Notices" on page 9
September 24 2014	Updated "SSL VPN standalone client" on page 34
August 26, 2014	Corrected "FortiManager support" on page 30 Corrected "FortiAnalyzer support" on page 30 Corrected "FortiClient support (Windows, Mac OS X, iOS and Android)" on page 30 Added new issues to "Resolved Issues" on page 37
August 20, 2014	Corrected "FortiManager support" on page 30.
August 8, 2014	Added new resolved issues to "FortiGate 200D" on page 38.
August 01, 2014	Updated "Virtualization software support" on page 31. Updated "Upgrading from FortiOS v5.0 Patch Release 6 or later" on page 18
July 30, 2014	Added new issues to "Resolved Issues" on page 37. Corrected "FortiManager support" on page 30 Added new LTE-related features to "Summary of Enhancements" on page 8.
July 28, 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 8. 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 8.

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-60D-POE, FG-70D, FG-80C, FG-80CM, FG-80D, FG-90D, FGT-90D-POE, FG-94D-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-300D, FG-310B, FG-310B-DC, FG-311B, FG-500D, FG-600C, FG-620B, FG-620B-DC, FG-621B, FG-800C, FG-1000C, FG-1240B, FG-1500D, FG-3016B, FG-3040B, FG-3140B, FG-3240C, FG-3600C, FG-3700D, FG-3810A, FG-3950B, FG-3951B, FG-5001A, FG-5001B, FG-5001C, 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-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, and FWF-90D-POE.

FortiGate VM

FG-VM32, FG-VM64, 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 8 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

Firewall

- Support IPv6 DoS policy on XLP (211082)

System

- LTE Daemon support for Novatel U679 (Bell) (225531,234743)
- Port kernel profiling function (237984)

```
# dia sys profile  cpumask 0xffffffff
# dia sys profile  start
# dia sys profile  stop
# dia sys profile  show
```

- Support IPv6 DoS policy on XLP. (186581)
- Add SPAN support for FG-200D/240D/280D. (217060)
- When a crash occurs, generate an event log to record some brief information about it. (238137)
- New MIB entities for USB LTE Modem and changed USB MODEM widget GUI. (237150)
- New LTE modem CLI commands. (249631)

```
# config system global
     usb-wan-auth-type
     usb-wan-extra-init
     usb-wan-passwd
     usb-wan-username
```

Wireless

- FAP 11ac radio support for DARRP. (243332)
- Radius Accounting for Wireless. (228497, 224968)

Special Notices

FortiGate-300D and FortiGate-500D nTurbo Support

The FortiGate-300D and FortiGate-500D do not support nTurbo for IPS acceleration. The option for this feature has been disabled by default. Enabling it may result in a performance degradation. The CLI commands are shown below.

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

If `np-accel-mode` is set to `none`, then nTurbo IPS acceleration is disabled.

FortiGate-3600C hardware compatibility

FortiOS v5.0 Patch Release 6 contains a compatibility issue with certain FortiGate-3600C units. Units that are affected have a system part number of P12090-03 and later. You can view the system part number on the bottom of the unit or from the get system status CLI command.

FortiGate-3600C units with part number P12090-03 and later must run FortiOS v5.0 Patch Release 6 or later and can't be downgraded to FortiOS v5.0 Patch Release 5 or earlier.

SCTP firewall support

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

New FortiOS Carrier features

Changes to licensing

Prior to FortiOS 5.0, only FortiCarrier-specific hardware could run FortiOS Carrier 4.0. Starting with FortiOS 5.0 Patch Release 2, the FortiOS Carrier Upgrade License can be applied to selected FortiGate models to activate FortiOS Carrier features. There is no support for FortiOS Carrier features in FortiOS 5.0 GA and 5.0 Patch Release 1.

At this time the FortiOS Carrier Upgrade License is supported by FortiGate models FG-3240C, FG-3950B, FG-5001B, FG-5001C, and FG-5101C. Future 3000 and 5000 series models are also expected to support FortiOS Carrier.

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

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

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

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

Licensing and RMAs

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

Licensing and firmware upgrades, downgrades and resetting to factory defaults

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

Upgrading older FortiCarrier specific hardware

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

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

Changes to GPRS Tunneling Protocol (GTP) support

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

Changes to MMS scanning

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

TFTP boot process

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

Monitor settings for Web-based Manager access

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

Before any upgrade

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

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

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

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

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

After any upgrade

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

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

Using wildcard characters when filtering log messages

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

logged

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

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

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

Default setting/CLI changes/Max values changes

- Increase site-to-site tunnel numbers for 2U and 3U models. (230577)
  - 2U -- 20,000
  - 3U and up --- 40,000
- 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 8, 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 8. 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 8. 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 8. 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.

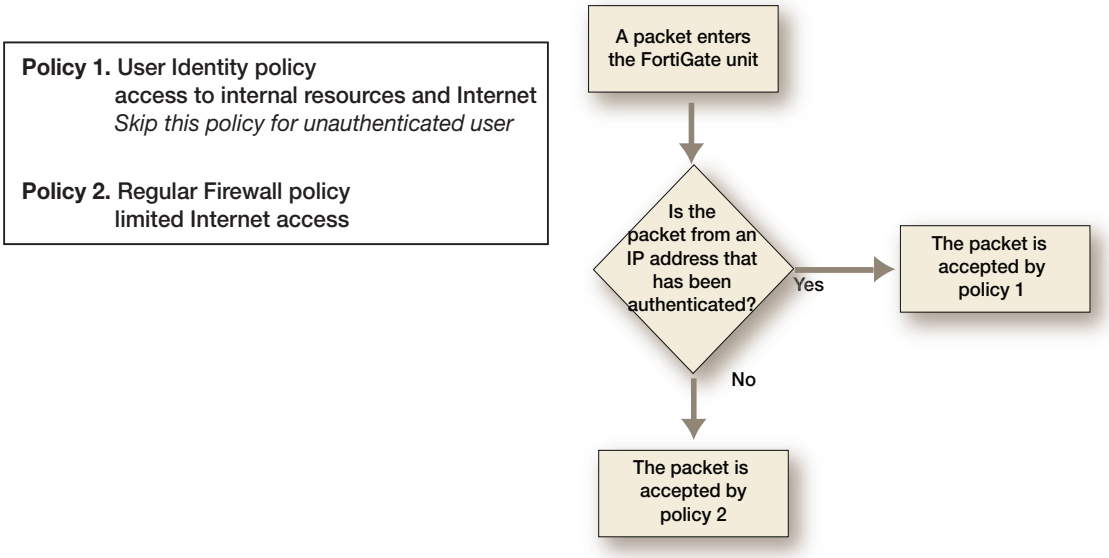
To support these different levels of access you can add a user identity policy to the top of the policy list that allows authenticated users to access internal resources and to have unlimited access to the Internet. In this policy, select *Skip this policy for unauthenticated user*.

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
```

FortiOS identity base policy behavior change

Before 5.0.8, unauthenticated users were prompted with fw authentication page after trying to access a particular website. In this case, FGT intercepted the HTTP/HTTPS request sent to server and replied on its behalf.

As of v5.0.8 and v5.0.9, unauthenticated users are redirected to the address of the interface they are connected to. They are also redirected to port 1000.

If Client PC is under NAT environment so, source ip address from Client PC to server change per each session, this behavior change affect customer.

FortiGate-100D hardware compatibility

FortiOS v5.0.0 to v5.0.7, inclusive contains a compatibility issue with FortiGate-100D units that have a system part number of P11510-04 and later. You can view the system part number on the bottom of the unit or with the get system status CLI command. Units with this system part number must run FortiOS v5.0.8 or later.

Upgrade Information

Upgrading from FortiOS v5.0 Patch Release 6 or later

FortiOS v5.0 Patch Release 8 officially supports upgrading from FortiOS v5.0 Patch Release 6 or later.

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

Upgrading an HA cluster

When upgrading a high availability cluster to FortiOS v5.0 patch 8, if uninterruptable-upgrade is enabled you must always upgrade to FortiOS v5.0 Patch 6 before upgrading to patch 8. If you skip this step the firmware upgrade will fail.

HA Virtual MAC Address Changes

HA virtual MAC addresses are created for each FortiGate interface based on that interface's index number. Between FortiOS 4.3 and 5.0 interface indexing changed. After upgrading a cluster to FortiOS 5.0 the virtual MAC addresses assigned to individual FortiGate interfaces may be different. You can use the `get hardware nic <interface-name>` command to view the virtual MAC address of each FortiGate interface.

Dynamic profiles must be manually converted to RSSO after upgrade

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

Zone-related policies may be deleted when upgrading to FortiOS v5.0 Patch Release 4, 5, 6, 7, or 8

Policies that include interfaces that are members of a zone could be deleted when upgrading to FortiOS v5.0 Patch Release 4, 5, 6, 7, or 8. 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 8 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 8 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 8 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 8 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 8, 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 8.

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 8 officially supports upgrade from FortiOS v4.0 MR3 Patch Release 16 and v4.0 MR3 Patch Release 17.

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 8 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 8 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 8 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.

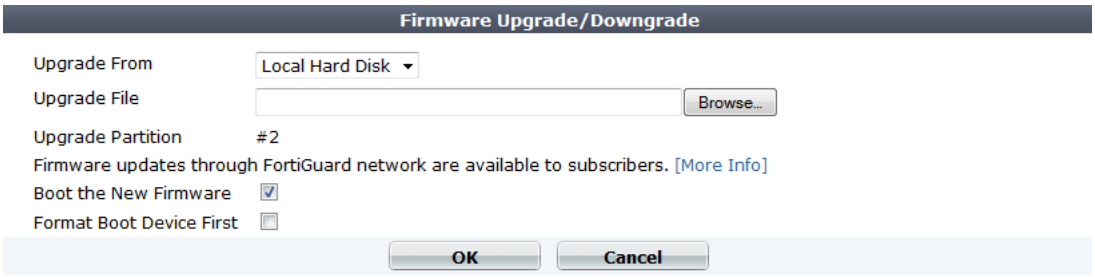
Save a copy of your FortiGate device configuration prior to upgrading. To backup your configuration, go to *System* > *Dashboard* > *Status*. In the *System Information* widget select *Backup* under *System Configuration*. Save the configuration file to your management computer.

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*.

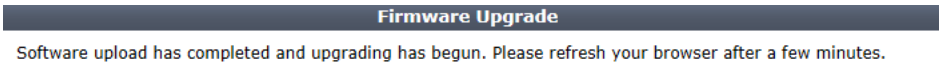
   The *Firmware Upgrade/Downgrade* window opens.

   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 8, 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 8 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 8 is supported by FortiManager v5.0 Patch Release 7 and later and FortiManager v5.2.0.

FortiAnalyzer support

FortiOS v5.0 Patch Release 8 is supported by FortiAnalyzer v5.0 Patch Release 6 and later.

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

FortiOS v5.0 Patch Release 8 is supported by the following FortiClient software versions:

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

See the *FortiClient v5.0 Patch Release 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 8 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 8 build 0075 or later.

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

FortiSwitch support

FortiOS v5.0 Patch Release 8 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 8 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 8 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 8 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, 2012 and 2012-R2.
- KVM - CentOS 6.4 (qemu 0.12.1) or later

See "About FortiGate VMs" on page 52 for more information.

Fortinet Single Sign-On (FSSO) support

FortiOS v5.0 Patch Release 8 is supported by FSSO v4.0 MR3 B0157 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 8 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 8 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 8 is supported by AV Engine v5.155 and IPS Engine v2.189.

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 8 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 8 supports the SSL VPN tunnel client standalone installer build 2303 for the following operating systems:

- Microsoft Windows 8.1 (32-bit & 64-bit), 8 (32-bit & 64-bit), 7 (32-bit & 64-bit), and XP SP3 in `.exe` and `.msi` formats
- Linux CentOS 5.6 and Ubuntu 12.0.4 in `.tar.gz` format
- Virtual Desktop in `.jar` format for Microsoft Windows 7 SP1 (32-bit)

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

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

SSL VPN web mode

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

Table 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 28
Microsoft Windows 7 64-bit SP1	Microsoft Internet Explorer versions 8, 9, 10 and 11 Mozilla Firefox version 28
Linux CentOS version 5.6	Mozilla Firefox version 24
Linux Ubuntu version 12.0.4	Mozilla Firefox version 28
Mac OS X v10.9 Maverick	Apple Safari version 7

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

SSL VPN host compatibility list

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

Table 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 8 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.

Default Behavior/Config Change

The following table lists FortiOS default behavior/Config change.

Table 6: FortiOS default behavior/Config change

Bug ID	Description
247953	Add a default DHCP server for management port on 200D, 240D, 280D-POE, 100D and 140D.
247162	Hide switch controller on 600/800/1000 series.
246438	Change FG-30D default to full GUI.
246577	Configurable syslog server setting by WebGUI for 3600C, 3950B, 3700D.
247321	Move URL match list into explicit proxy page.
188763	Improvement to default mesh SSID.

Resolved Issues

This chapter describes issues with past releases of FortiOS v5.0 that have been resolved for FortiOS v5.0 Patch Release 8. For inquires about a particular bug, please contact Customer Service & Support.

DLP

Table 7: Resolved DLP issues

Bug ID	Description
227462	Fixed the DLP rule matching procedure for archived files.
238576	Fixed DLP does not detect batch files uploaded to a specific website.
229534	MPEG file type is not correctly detected by DLP.
227145	Support file pattern scanning inside archived files in DLP.
231677	Adding checks for To/CC in DLP regexp match for email header.
240958	SSN filter false positive resolved by considering the breaks in between numbers.

Firewall

Table 8: Resolved Firewall issues

Bug ID	Description
232532	Add STP/802.1X support and PCIe support for the FG-94D-POE.
245748	Endpoint IP addresses in SCTP multihome INIT or INIT_ACK packets may not be translated correctly by NAT.
229356	IPS DOS Sniffer stops working after change in IP Geo policy matching code.
244552	Rarely some traffic passes through higher firewall policy and matches with lower policy.
232598	Fixed scanunitd daemon not free memory when inflateInit2 fails.
217842	Fixed Device Definition Grouping Devices Incorrectly.
231568	Fixed 'GTPv2 Create Session Requests with PDN Type IPv6 are dropped'.
232285	Virtual server should only switch server if real-server is down.
238105	Alertemail for 'violation-traffic-logs' shows the wrong logid, subtype and missing date/time/devname/devid.
242245	DCE-RPC helper sometimes does not create expectation for ISystemActivator - RemoteCreateInstance method.

Table 8: Resolved Firewall issues (continued)

Bug ID	Description
230572	Fix memory leak in virtual-server when configuration changes.
234822	Fix virtual server crash when sending traffic to IPS.
224891	Sending a mail with an attached file fails via MAPI connection.
242957	DCE-RPC session helper does not open expectation.
234172	Chunked by pass should not bypass the whole session but only the chunked messages.
223885	Fix error in vsd test suite caused by new HTTP cookie length.
237639	Account for the use of an external proxy when exempting SSL connections from deep inspection.
234516	Unexpected session clash for GRE tunnel in event logs.
237640	Fnbamd logs into SSLVPN unauthorized PKI users when OCSP finishes after LDAP check.
223330	SSL worker is utilizing high CPU when deep scanning is enabled.
231201	Proxyworker outage after vdom creation/deletion.
223296	Sflow input interface value is set in sflow flow samples.
224001	Add accprofile override and vdom override function for Access-Challenge.

FortiGate 200D

Table 9: Resolved FortiGate-200D issues

Bug ID	Description
228966	Resolved an issue that made history widget statistics appear incorrect for the FGT200D family.
225812 228349	Resolved an issue that caused FG200/FG240D NPU IPsec offloading to block traffic.
234124	Resolved an issue that blocked the creation of 10 VDOMs on FGT200D models.

FortiGate VM

Table 10: Resolved FortiGate VM issues

Bug ID	Description
244695	Resolved an issue that caused RDP sessions between windows VMs in the same VM host to fail with data encryption errors.

HA

Table 11: Resolved HA issues

Bug ID	Description
246480	Directly Connect Routes are lost after Port Based allocation and/or Sflow is enabled on the FG1500D.
229235	FGT-HA failover sends invalid mgmt_id to FMG causing cluster member becomes unregistered device.
238541	Hasync does not sync to delete routes related to monitor interfaces.
233606	Routes lost on Master when Slave reboots.
220856	Master reports 1 more vdom than slave + ha global out of sync.
238454	For Carrier uninterruptible upgrade, daemon radiusd needs to sync its state during upgrade, then notify hatalk after sync. Master upgrade procedure can not continue if hatalk does not recv radiusd notification, that causes uninterruptible upgrade failure.
231808	Duplicates in HA global checksum triggers out of sync.
243656	Unable to lease dhcp addresses on HA cluster.
233107	Support the HA NAT change for A-A cluster with server-load-balance.
238959	The hasync daemon running on the slave unit may crash.

IPS

Table 12: Resolved IPS issues

Bug ID	Description
215622	Duplicate entries in user ban list suspected to cause the kernel to run at 80% on all CPU.
229356	IPS DOS Sniffer malfunction after change in IP geo policy matching code.

IPSec

Table 13: Resolved IPSec issues

Bug ID	Description
246085	Fix iked crashes when using xauth with FortiToken.
232091	Fix IKE seg fault with certificate authentication.
237275	Fix new IKEv2 SA is unexpectedly deleted after rekey.
235183	Fix for IKE diagnostic print commands crashing when dpd_mode flag is invalid.

Table 13: Resolved IPSec issues (continued)

Bug ID	Description
232253	Fix for IPsec traffic blocked after HA failover.
234003	RADIUS Framed-IP into accounting packets.

Logging & Report

Table 14: Resolved Logging & Report issues

Bug ID	Description
233876	Log message issues by WebFilter for invalid hostname is incorrect.
232443	Fix miglogd crash caused by the invalid vfid case.
227474	System Analysis Report Randomly displays a drop of traffic to 0.

Routing

Table 15: Resolved Routingissues

Bug ID	Description
230832	Not all redistributed routes are advertised to ISIS neighbors.
199589	OSPF may not reconverge after HA failover if the topology is changed during failover.
223729	Route entry 0.0.0/32 makes BGP neighbor broken.
220841	OSPF: CLI displays negative OSPF tags.
230649	BGP AS Prepend doesn't show expected result when rules in route-map are not sequential.

Spamfilter

Table 16: Resolved Spamfilter issues

Bug ID	Description
229605	SMTP does not correctly handle oversized email in the splice mode when they need to be send out to the recipients.

SSLVPN

Table 17: Resolved SSLVPN issues

Bug ID	Description
215680	FortiGate to support FQDN in Address field in ICA file.
234245	Improve the SSL VPN password renewal page.

Table 17: Resolved SSLVPN issues (continued)

Bug ID	Description
229602	Added support for data URI scheme to the parser.
227146	404 Error when navigating FortiManager in SSL VPN web mode.
239550	Fixed SSL renegotiation possible when reqclientcert is enable.
228816 229631	SSL VPN parser did not construct relative URL properly.
231798	SSLVPN PortForward connection tool doesn't close session when it is closed on backend server.
237009	SSLVPN is restarted with all users every time updated CRL is downloaded.
224392	SSL VPN response failed when HTTP request size is larger than 4k.
232433	SSL-VPN idle timeout screen is garbled when it sets multi-byte language.
236992	Cannot log into SSL-VPN Web portal after deleting vlan/policy then configuring same vlan/policy again.
240916	Unable to launch Citrix application as ICA file is truncated.

System

Table 18: Resolved System issues

Bug ID	Description
245119	Resolved an issue that caused no interface statistics for VLANs of an NP6 LAG interface.
161876 240650	Correct PSU alerting logic.
245119	No interface statistics for VLANs of a NP6 LAG interface.
246371	FGT as dhcp server will give out wrong gateway info under some circumstance.
245121	sFlow stops sending raw packet samples after few minutes with possible race condition.
246367	No traffic flow on dialup tunnel when IPSec is accelerated in NP6 with Virtual cluster.
217637	STP forwarding problem in on-arm TP mode firewall.
247718	IP GEO database not updated via FDS schedule update.
247260	Fail-detect applied to VLAN interfaces causes flapping.
248333	Can't authenticate vdom admin using RADIUS wildcard account.
247708	Memory leaks when blocking pages with FortiGuard WF overrides enabled.

Table 18: Resolved System issues (continued)

Bug ID	Description
229220 231946	Slow down np4lite interrupt if system is overloaded by network traffic.
229293	Offload ESP/NAT-T (UDP 4500) passthrough traffic on XLR/XLP.
228805	Script restore from FortiCloud cannot be scheduled when timezone change to GMT+.
190894	Virtual-switch can't isolate floods broadcast packets correctly.
227998	Spoofed packet can lead to deletion of an existing session.
231800	Ensure aggregate HA status is set correctly.
231083	Ensure SNMP linkup/down trap to be sent after changing the snmp-index of interface.
235993	Capture packet fills RAM rapidly on diskless FortiGate.
235974	Fix possible disk issue when update.
223931	SNMP interface polling spikes CPU.
236817	Botnet database is not updated on cluster.
179613	port9-port12 of 3040B can't negotiate Huawei Router NE40.
222004	FWF-60CX-A modem crash with a specific config.
241715	SSH SCP not working with public key.
215988	Telnetd high CPU.
229746	Crash when importing CRL over GUI or CLI.
230364	Serial console prints lots of "NP4 accounting statistics" messages.
240631	Unable to dial & connect HUAWEI 3G Modem(E303H).
235841	Unit in transparent mode consumes 6 GB of shared memory and then removes sessions.
232600	DHCP server offered an expired lease with IP 0.0.0.0 when its IP range is exhausted.
224989	Traffic failing when offloaded to subordinate blade - No session matched.
236975	Rebooting unit, while the global setting for "cfg-save" is set to manual, breaks software switches displayed in GUI.
236797	Wrong IP address in update debug output, and wrong server trying order.
240627	PPPoE device now correctly handles concurrent connections for same AC that assign same sessID.
228156	Add warning message for failed iplist additions.

Table 18: Resolved System issues (continued)

Bug ID	Description
229762	Port1 through Port8 going down at the same time.
235714	Sniffer policy on dmz port does not under certain scenario.
231087	Only first packet captured for firewall policy in a transparent VDOM.
234117	FortiGate DHCP server detects erroneous IP conflict.
207048	SCTP multi home INIT collision in NAT environment is not resolved correctly.
229745	Kernel panic triggered by traffic on FG240D.
234193	Interfaces still alive with gwdetect configured even if halt status.
235041	Radius Accounting Stop sent for user when creating new vdom.
231204	Fix total freeze in less than 3 days.
231801	Revert system.interface default distance back to original value of 5.
233289	Removing restriction on having dots in interface names when packet capture is issued.
232053	Offloading enabled for Oracle TNS sessions.
223323	SCP configuration restore command syntax not consistent with backup command.
237415	Multiple console admin sessions without human intervention.

Upgrade

Table 19: Resolved Upgrade issues

Bug ID	Description
227984	TP-mode L2 loop occurs between npu-vlink itself when upgrading.
231797	Inconsistent behavior for logtraffic after upgrade from 4.3.15.

VoIP

Table 20: Resolved Wanopt & Webproxy issues

Bug ID	Description
231678	Fix One Way audio with SIP ALG.

Wanopt & Webproxy

Table 21: Resolved Wanopt & Webproxy issues

Bug ID	Description
240918	Fixed learning of FQDN firewall address from configuration in explicit proxy.
244856	Prevent 502 Bad gateway when using explicit proxy.
234404	MAPI AV: Outlook2003 in a particular PC does not start up by MAPI parsing error.
224638 235946	Fixed bug web-cache related crashes in WAD.
229929	Explicit proxy local-in policy disappears after a reboot with units having one STATIC and one PPPoE WAN setup.
231978	HTTP response with invalid format may not pass through WAD when scan is on.
233407	Improve MAPI session expectation handling to remove potential conflict among multiple MAPI clients to the same server.
226724	SSL Inspection automatically performed on Explicit Proxy for webfilter blocked categories.
227765	Fixed WAD crashes caused by SSL requests,
234406	MAPI AV: Outlook2007 not responding when a message is saved
246339	Fix HTTP response processing on naked body without HTTP headers.
233090	Improve MAPI read/write stream, MAPI FastTransfer stream handling code so that content cannot bypass scanning using different transferring modes.

Webfilter

Table 22: Resolved Webfilter issues

Bug ID	Description
228240	Fixes the issue issue that urlfilter does not have a log for monitor action.
232404	Safari browser is not stable with web override when using proxy policy.

Web-based Manager

Table 23: Resolved Web-based Manager issues

Bug ID	Description
225780	Events are logged with the incorrect user when making changes in jsconsole with a wildcard user.
216078	Adding DHCP server options with hex value causes the interface to no longer be edited in the GUI.

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

Bug ID	Description
241538	Custom Admin Profile - Log and Report -> Report Access issues.
244219	SNMP community setting was removed when confirmed on GUI.
239368	Fix Internal 500 Server Error after login.
220056	Application control GUI entries are blank when one entry uses a rule ID that doesn't exist.
219095	All interfaces of vdoms are displayed if a "CLI Console" on GUI is detached.
242622	GUI LDAP test connection and DN Query fail when using STARTTLS.
236729	Error occurred when using setup wizard on FWF_20C-ADSL-A.
217684	Query button for LDAPS in LDAP config GUI does not work.
221874	When the VCM plugins update failed, the error message is not correct.
216347	LDAP Test button does not use set source-ip x.x.x.x.
244509	Webfilter doesn't work on sniffer policy, unless webfilter profile applied on a non-sniffer policy.
239549	New created service in policy is not displayed.
218303	LDAP query in LDAP config GUI does not display an AD OU container that contains a large number of objects.
234369	Interface address setting by setup wizard was removed after the device reboot.
230692	Pyfcgid crashed and got internal server error.
231219	Section View is disabled in the policy page after upgrading to 5.0.6.
237291	Right click on a policy count nothing shows in section view.
237636	Firewall policy count is sometimes showing values of all 0.
233558	Improve policy page loading time.
238225	Fixed login HTML code discloses IPS_version.
197598	The tooltip for interface status for port1-8 on "Unit Operation" Widget does not show.
237696	Unable to add comment to vip using GUI.
242096	Changing a firewall policy from identity to normal in the GUI doesn't free up objects.
239224	LDAP browser in LDAP-group-GUI does not respect group filter from LDAP server.
230257	PSec Monitor filter with '%' will lock column filters

WiFi

Table 24: Resolved WiFi issues

Bug ID	Description
236818	Fixed cw_acd crash reported in crash log.
240307	Removing the oldest DEAD rogue AP entry if the table is full
235477	Fixed cw_acd crash every days caused by invalid read memory

Known Issues

This chapter describes some known issues with FortiOS v5.0 Patch Release 8. Some of the issues listed below were also known issues for FortiOS v5.0 Patch Release 5. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

FortiGate-1500D and 3700D

Table 25: Known FortiGate-1500D and 3700D issues

Bug ID	Description
242298	When the FortiGate unit is very busy with high CPU usage, IPsec VPN packets may be lost.
241646	Traffic may not be able to pass through a VLAN interface added to a link aggregation group (LAG) in a Transparent Mode VDOM. Workaround: Run `diagnose sniffer packet` on physical interface in TP vdom, or reboot the FortiGate unit.
242012	IPsec VPN traffic throughput is highly unstable. Workaround: this only happens on IPsec interface added to a 40G LAG. Don't use IPsec VPN over a 40G LAG.
240789	FortiGate-3700D: LAG groups configured on low latency interfaces (port25 to port32) (NP6_0 and NP6_1) do not function correctly. Workaround: Only use either low-latency-mode or LAG for traffic on port25 to port32) (NP6_0 and NP6_1).
239968	IP tunneling (SIT tunnelling) not working when offload to NP6. Workaround: Disable `auto-asic-offload` in sit-tunnel configurations.
240945	Reply traffic is not offloaded when shared traffic shaping is enabled on policies for accelerated inter-VDOM links using the npu_vdom interface.

FortiGate-80D

Table 26: Known FortiGate-80D issues

Bug ID	Description
235525	Link and speed LEDs remain “ON” on after shutting down the unit after shutting down the unit using the `execute shutdown` command.
239619	The r8168 driver is unable to shutdown power of the port and will keep the link of the other end in up state.

FortiGate-100D

Table 27: Known FortiGate-100D issues

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

FortiGate-300D and FortiGate-500D

Table 28: Known FortiGate-300D and FortiGate-500D issues

Bug ID	Description

239434	nTurbo for IPS acceleration fails to accelerate traffic. Fortinet recommends keeping this option set to the default value of `none`.
	`config ips global`
	`  set np-accel-mode none`
	`end`

238961	Link aggregation interfaces fail to come up. All members remain in *negotiating* status.
249324	Nat IPSec TCP traffic can not go through when npu-offload is enabled.

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
0243960	Antivirus profile errors after upgrade from 4.3

Web-based Manager and CLI

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.

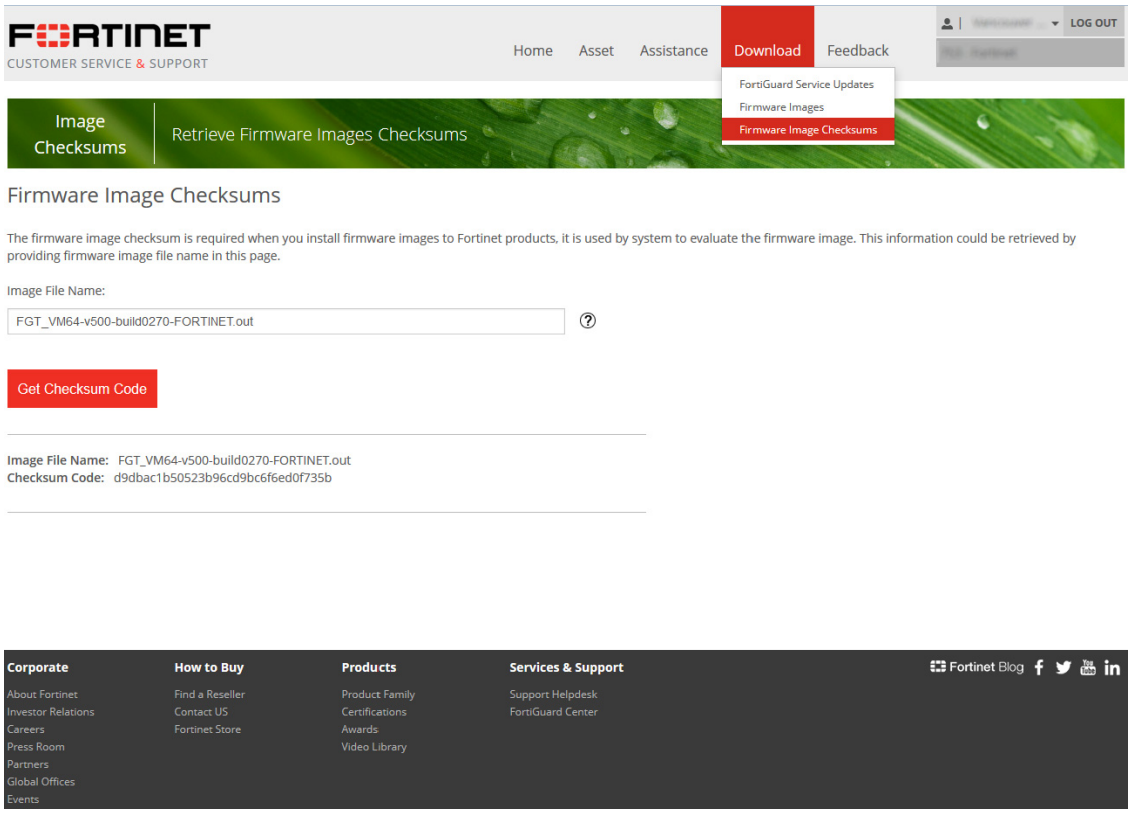
Table 31: Known Web-based Manager issues (continued)

Bug ID	Description
172567	The vulnerability scanner appears on the GUI and CLI when the FortiGate unit is in Transparent mode but the vulnerability scanner does not work in Transparent mode.
254084	When using IE9, created firewall policies are not displayed on "Policy" page. Also the content pane toolbar is not displayed on this page.

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 8.

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.