FortiOS v5.2.0
Release Notes

FortiOS v5.2.0 Release Notes (Build 0589)

July 24, 2014

01-520-234298-20140724

Technical Documentation	docs.fortinet.com
Fortinet Video Libarary	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
july 24, 2014	Added section “OSPF MTU Mismatch” on page 19 Added bug id 248651 to “Known Issues” on page 28
July 17, 2014	Added bug id 246853 to “Known Issues” on page 28.
July 11, 2014	updated the section “FortiClient support (Windows, Mac OS X, iOS and Android)” on page 20
June 19, 2014	Simplified the section “FortiAP support” on page 20.
June 18, 2014	Added more information about allowing DNS to “Services required for authentication must be enabled in authentication policies” on page 16. Added hyper-v 2012 r2 to “Microsoft Hyper-V” on page 22. Edits and one addition to “Known Issues” on page 28.
June 13, 2014	Initial release.

New Feature Highlights

For complete details about all of the new Features in FortiOS v5.2.0, see *Whats New in FortiOS v5.2.0*.

Unified Policy Management

The options for creating user-identity, device identity, IPsec VPN and SSL VPN policies are merged into a single policy creation page. On this page you can select source addresses and also users and devices in a single policy. Authentication policies no longer require multiple nested authentication rules. This allows for greater control and customization of policies and the ability to impose user authentication and device identification on a single traffic stream.

Most IPSec and SSL VPN configuration has been moved to the VPN area of the GUI. Policy creation for these features is now simplified and easier to understand.

FortiView Dashboards

The *FortiView* dashboards integrate real time and historical dashboards into a single view that displays information on the following:

- Sources
- Applications
- Cloud applications
- Destinations
- Web sites
- Threats
- All sessions

SSL Inspection

Several changes have been made to how SSL inspection is handled by FortiOS v5.2.0. Certificate Inspection allows HTTPS traffic to be scanned without enabling deep inspection or causing certificate errors. Full SSL inspection unencrypts SSL traffic to identify potential threats inside the SSL streams. Full SSL inspection can result in certificate errors but a new exemption feature and the ability for uses to install the certificate used by FortiOS can reduce or eliminate them.

Web Filtering

Several new options have been added for web filtering:

- Restricting Google access to specific domains
- New protocols for warnings and authentication
- Modifying HTTP request headers
- Adding a referer to URL filters.
- Using FortiGuard rating checks for images, JavaScript, CSS, and CRL
- Additional replacement message variables

Application Control

Several new options have been added for application control:

- Deep inspection for cloud applications
- Traffic shaping settings
- 5-Point-Risk Ratings
- Replacement messages
- Support for SPDY protocol

IPsec VPN Wizard

The IPsec VPN wizard is the only web-based manager tool for creating interface- or route-based IPsec VPNs. All it takes is a few steps with the wizard to create a wide variety of interface-based IPsec VPN configurations. In addition to the IPsec settings the wizard creates all required routes and policies.

In FortiOS v5.2.0, expanded options have been added to the wizard, allowing it to be used for more types of VPN configurations. Tunnel templates have been created for popular configurations.

Captive Portal

Several new options have been added for captive portals:

- External captive portals
- Using groups from the security policy
- Exempting a policy
- Replacement messages
- New configuration options for wireless
- WPA personal security + captive portal for wireless

FortiAP Management

Several new options have been added for managing FortiAP units:

- Manually selecting AP profiles
- AP scanning
- Radio settings summary
- CLI console access
- Split tunneling for wireless traffic

Improved flow-based Antivirus

In FortiOS v5.2.0, flow-based AntiVirus has been improved to have the same enhanced performance as flow-based antivirus scanning in FortiOS 5.0 while providing the same accuracy and many of the extended features of proxy-based antivirus.

FortiExtender Support

FortiOS v5.2.0 supports FortiExtender, that allows you to remotely connect 4G/LTE USB modems to a FortiGate unit. The FortiGate unit can remained installed in a secure location while the FortiExtender is installed on a roof or near a window providing enhanced 4G/LTE modem reception.

Using a Virtual WAN Link for Redundant Internet Connections

A virtual WAN link consists of two or more interfaces that are connected to multiple ISPs. The FortiGate unit sees the virtual WAN link as a single interface so the FortiGate's security policy configuration no longer has be redundant to support dual Internet links. In addition, the virtual WAN link includes load balancing and new link health checking and settings.

Internet Key Exchange (IKE)

Several new options have been added for how IKE is supported on a FortiGate:

- Multiple interfaces
- Mode-configuration
- Certificates groups
- Authentication methods
- Inheriting groups from the security policy
- Assigning client IP addresses using the DHCP proxy
- Transform matching
- Cookie notification
- Message ID sync for High Availability

SSL VPN Creation

SSL VPN configuration has been simplified with new settings and portal creation pages. Most SSL VPN settings can be configured on one GUI page. Additional settings only involve simplified policy creation.

On-Net Status for FortiClient Devices

A new status option, On-Net, has been added for FortiClient devices that show if that device has been registered with the FortiGate unit.

Supported Models

The following models are supported by FortiOS v5.2.0 build 0589.

FortiGate

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

FortiGate VMs

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

All FortiGate VMs can be licensed at the following levels: FG-VM00, FG-VM01, FG-VM02, FG-VM04, and FG-VM08.

FortiSwitch

FS-5203B

FortiCarrier

FortiOS v5.2.0 FortiCarrier images are delivered upon request and are not available on the customer support firmware download page.

Upgrading to FortiOS v5.2.0 build 0589

This chapter describes how to upgrade FortiOS v5.2.0 build 0589 and describes known issues that you should be aware of after upgrading.

This chapter includes the following sections:

Supported upgrade paths to FortiOS v5.2.0 build 0589

This section lists the supported upgrade paths from the most recent versions of FortiOS to FortiOS v5.2.0 build 0589. For a complete list of upgrade paths see the latest Upgrade Paths document (*http://docs.fortinet.com/d/upgrade-paths-to-fortios-5.2.0*)

- FortiOS 5.0 Patch Release 6 and 7 (supported)

Before any firmware upgrade

To minimize network interruptions, plan the upgrade during a maintenance window. This allows you to properly upgrade, test, and implement the firmware upgrade without disrupting network traffic.

Check the sections in this chapter for important information about upgrading to FortiOS v5.2.0.

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, Citrix XenServer and Microsoft Hyper-V environments you can also take a snapshot of or backup your current VM before upgrading to the latest version. You can revert to the snapshot or backup if the new firmware does not function properly.

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 firmware upgrade

If you are using the FortiGate GUI (web-based manager), after a firmware upgrade, clear your browser cache prior to logging in to ensure the GUI is displayed properly.

The AV and IPS engines and definitions included with a firmware upgrade may be older than ones currently available from FortiGuard. You should update the AV and IPS engines and definitions right after a firmware upgrade by going to *System* > *Config* > *FortiGuard,* selecting the blue triangle next to *AV & IPS Download Options* and selecting the *Update Now* button.

Firmware Image Checksums

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

Upgrading your FortiGate unit to FortiOS v5.2.0 build 0589

Use the following steps to upgrade your FortiGate unit or FortiGate VM to FortiOS v5.2.0 build 0589. Make sure you have reviewed the notes in this chapter before upgrading.

You can upgrade your firmware directly from the FortiGuard network. From the GUI, go to *System* > *Dashboard* > *Status* > *System Information Widget* and selecting *Update* beside *Firmware Version*. Set *Upgrade From* to *FortiGuard Network*, select the Firmware Version to upgrade to and select *OK*. If FortiOS v5.2.0 build 0589 is not yet available on the FortiGuard network you can use the following procedure to download a firmware image file from http://support.fortinet.com.

To upgrade the firmware from the GUI:

1. Download the FortiOS v5.2.0 build 0589 firmware from http://support.fortinet.com.
2. Log into the web-based manager using an administrator account that can upgrade firmware.
   a. If you are using FortiAnalyzer AND you are using the “store and upload” transfer method:
      i. You MUST upgrade the FortiAnalyzer unit to v5.0.7 or v5.2.0 prior to upgrading the FortiGate.
      ii. You MUST run the command `execute log roll` and `execute log upload` to sync the latest logs to the FortiAnalyzer prior to upgrading the firmware.
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.
5. Select *Browse* and locate the firmware image on your local hard disk and select *Open*.
6. Select *OK*. The FortiGate unit uploads the firmware image file, upgrades to the new firmware version.
7. Clear your browser cache and refresh your browser after a few minutes and log back into your FortiGate device.
8. Update the AV and IPS engines and definitions by going to *System* > *Config* > *FortiGuard,* selecting the blue triangle next to *AV & IPS Download Options* and selecting the *Update Now* button.
   a. If you are using FortiAnalyzer AND you are using the “store and upload” transfer method:
      i. You MUST run the command `execute formatlogdisk` to delete the old logs. Failing to run this command may cause log uploading to stop working after upgrade.

Downgrading your FortiGate unit to a previous FortiOS version

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

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

FortiOS v5.2.0 log messages are saved in a different format than FortiOS v5.0. If you downgrade from FortiOS v5.2.0 to FortiOS v5.0, logging will stop and you will not be able to view log messages that have been saved to disk. Before downgrading you MUST enter the command `execute log downgrade-log` to convert log messages from v5.2.0 to v5.0 format. After this command completes, you can downgrade to FortiOS v5.0 and you will be able to continue recording and viewing log messages. Also, if you do not run this command upgrading to v5.2.0 again at a later time may fail.

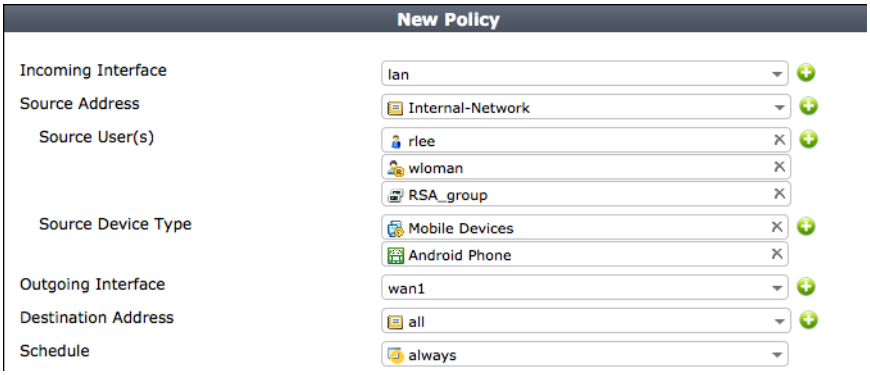
Firewall policy changes after upgrading to FortiOS v5.2.0 build 0589

Read the information in this section if your policy list includes user authentication policies. Because of changes to Firewall authentication in FortiOS v5.2.0, after upgrading your policy list may not be as secure as it was.

FortiOS 5.0 firewall policies require you to select the policy type (firewall or VPN) and an policy subtype (Address, User Identity, or Device Identity) resulting in address-based policies for general firewall control, user-based policies to require users to authenticate and device based policies to control access for different devices. You can also add multiple authentication rules to a user identity or device identity policy and use these multiple rules to apply different security features to different users, user groups, devices, or device groups.

FortiOS v5.2.0 removes the concept of different policy types. Instead, any policy can include source users and source devices. So a single policy can require users to authenticate and can also apply device access control. Of course you can also create policies with source addresses only, that do not require authentication or perform device control.

Figure 1: Example FortiOS v5.2.0 policy with a source address, source users, and source devices



In addition, in FortiOS v5.2.0 you no longer add multiple authentication rules to a user or device policy. Applying different access levels to different user groups or different devices requires creating multiple policies, one for each access type that you whish to apply.

This new method of configuring firewall authentication is a more industry-standard approach to incorporating user authentication and device control with firewall policies than the method used with FortiOS 5.0. FortiOS v5.2.0 policy lists could potentially contain more policies than corresponding FortiOS 5.0 policy lists. But each policy is simpler and does not contain nested authentication rules. In addition, this new FortiOS v5.2.0 policy method also allows user authentication and device control to work together since you can configure both user authentication and device control in the same policy.

What happens to FortiOS 5.0 user and device policies after upgrading to v5.2.0?

When you upgrade your firmware to FortiOS v5.2.0 all policies are converted to the v5.2.0 paradigm. In particular user and device identity policies will be split into multiple separate policies, one for each authentication rule. For example, consider the following FortiOS 5.0 user identity based policy that contains two authentication rules:

```
config firewall policy
  edit 3
    set srcintf "internal"
    set dstintf "wan1"
    set srcaddr "all"
    set action accept
    set log-unmatched-traffic enable
    set disclaimer enable
    set identity-based enable
    set nat enable
      config identity-based-policy
        edit 1
          set schedule "always"
          set groups "Group1"
          set dstaddr "all"
          set service "ALL_ICMP"
        next
        edit 2
          set schedule "always"
          set groups "Group2"
          set dstaddr "all"
```

```
            set service "ALL_TCP"
          next
        end
      next
    end
```

After upgrading to FortiOS v5.2.0 it becomes two policies as follows:

```
  config firewall policy
    edit 3
      set srcintf "internal"
      set dstintf "wan1"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ALL_ICMP"
      set groups "Group1"
      set disclaimer enable
      set nat enable
    next
    edit 5
      set srcintf "internal"
      set dstintf "wan1"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ALL_TCP"
      set groups "Group2"
      set disclaimer enable
      set nat enable
    next
```

What about the order of policies in the policy list?

After the upgrade the policies will be in the same order as before the upgrade. When a user or device policy is upgraded the resulting policies will appear in the same order as the authentication rules were and in the same place in the policy list as the original policy.

So after the upgrade my policy list should be good to go?

Possibly not. There are two changes to FortiOS v5.2.0 that may require you to review and change your policy list after upgrading to have it work as intended.

- Implicit fall-through feature for user authentication policies
- Services required for authentication must be enabled in authentication policies

Implicit fall-through feature for user authentication policies

In FortiOS v5.2.0 user authentication policies have an implicit fall-through feature that causes policy matching to fall through to a policy lower on the list that can also match the traffic. In other words the first user policy that is matched in the policy list, based on standard policy criteria, isn't the only policy that can be matched.

To illustrate implicit fall-through, consider a FortiOS v5.2.0 policy list consisting of the following two policies:

id 1: internal, (subnet1) ---> wan1, (all), service(all), has authentication

id 2: internal, (subnet1) ---> wan1, (all), service(all), no authentication

Since both policies have the same policy matching criteria the fall-through feature matches traffic with policy 2. The result of this policy list would be that no user would ever see a firewall authentication prompt.

This is not the intention of the fall-through feature but a policy list like this could be created unintentionally. Especially after a firmware upgrade since this configuration was acceptable for FortiOS v5.2.0.

Fall-through is intended to match users in different user groups with different policies. For example, consider an organization with two user groups where user group A requires a web filtering profile and user group B requires virus scanning. You could set up the following policy list:

id 1: internal, (subnet1) ---> wan1, (all), service(all), user group A, Web Filtering profile

id 2: internal, (subnet1) ---> wan1, (all), service(all), user group B, Antivrus profile

In this configuration, all users from subnet1 will see an authentication prompt. If the user is found in user group A the traffic is accepted by policy 1 and is filtered by the Web Filtering profile. If the user is found in user group B the traffic is accepted by policy 2 and is virus scanned.

The fall-through feature is required for users to be matched with policy 2. Without fall-through traffic would never be matched with policy 2.

Services required for authentication must be enabled in authentication policies

FortiOS allows authentication with the FortiGate unit using HTTP, HTTPS, FTP or Telnet. FortiOS 5.0 automatically allows HTTP, HTTPS, FTP, and Telnet services for any policy that includes user authentication, regardless of whether they are allowed on the policy or not. However, FortiOS v5.2.0 does not allow these services unless they are explicitly added to the authentication policy. So when you configure an authentication policy you must include the services that users need to be able to authenticate.

Furthermore, in some configurations, users will also need to be able to resolve host names through DNS lookups before authentication. In 5.0, DNS lookups are implicitly allowed before authentication on all authentication policies, regardless of whether the DNS service was defined in the policy. However, FortiOS v5.2.0 requires DNS to be explicitly allowed in the policy, for it to pass through before authentication.

To maintain the same functionality as FortiOS v5.0.7 you can add a policy to the top of the LAN to WAN policy list that allows all users to access DNS services.

Pre-upgrade policy list checks

Here is a brief list of things to check in your policy lists before upgrading to FortiOS v5.2.0:

1. How are the current firewall polices constructed?

2. Which identity policies use “fall-through-unauthenticated” and which do not?
3. Are there open-ended allow-all or deny-all policies behind the last identity-based policy? Do these need to be there?
4. How will behavior change when all user authentication polices become fall-through?
5. What about the maximum policy count? One identity policy will become multiple firewall policies.

Explicit Web proxy and FTP proxy policy changes after upgrading to FortiOS v5.2.0 build 0589

FortiOS v5.2.0 includes a new policy list for explicit Web proxy and explicit FTP proxy policies. The path for this new policy list is Policy & Objects > Policy > Explicit Proxy. After a firmware upgrade all explicit web and FTP proxy policies are moved to this policy list. You should check this policy list to make sure the configuration is working as intended.

In the CLI you configure explicit proxy policies using the `config firewall explicit-proxy-policy` command.

SSL VPN policy changes after upgrading to FortiOS v5.2.0 build 0589

Changes to web mode configurations

In FortiOS 5.0, SSL VPN web mode was configured by setting the policy type to VPN and adding SSL VPN authentication rules to that policy.

When upgraded to FortiOS v5.2.0 all SSL VPN policies become policies with source address set to ssl.root. The authentication rules from all the SSL VPN policies are added to SSL-VPN settings (*VPN* > *SSL* >*Settings* > *Authentication/Portal Mapping*).

Changes to tunnel mode configurations

In FortiOS 5.0 tunnel mode was configured by added a security policy that allowed access from the ssl.root interface to an internal network in addition to the SSL VPN policy required for web mode.

When upgraded to FortiOS v5.2.0 the web mode policy is changed as described above and the tunnel mode policy that allows access from the ssl.root interface to the internal network is not changed.

Default portal incorrectly set

If you have deleted the full-access portal from your FortiOS 5.0 configuration, after upgrading to FortiOS v5.2.0 the SSL VPN configuration will not include a default portal, You should use the following command to set a default portal:

```
config vpn ssl settings
  set default-portal <your-portal-name>
```

Preventing security certificate warnings caused by Full SSL inspection

When using Full SSL Inspection, FortiOS decrypts the SSL traffic flowing through the FortiGate unit to identify potential threats inside the SSL streams. Due to the nature of the SSL protocol, there are some things you need to be aware, to minimize the impact on end users:

- Certificate Trust: When visiting an SSL encrypted site, a certificate will be exchanged with the server. In the case of Full SSL Inspection, FortiOS is in the middle of this transaction and as a result, a certificate on the FortiGate unit is sent down to the client. This can cause the user's browser or other applications to produce certificate warnings. To avoid this, you can install the certificate used by FortiOS for encrypting SSL traffic on end user web browsers and other software (for example email clients) that may be affected. For an example cookbook recipe describing how to do this see: Preventing security certificate warnings when using SSL inspection.
- Exempting some applications and sites: Some Windows, Mac OS, iOS, Android or Linux applications may use specific criteria to establish secure SSL communications. For example, Windows Update uses only its built-in certificate (regardless of what other trusted certificates are installed in the Windows Cert Store). Because of this, Windows Updates fail Full SSL Inspection is enabled unless you add an exemption for them.

  Examples of addresses that you may want to exempt from SSL inspection include:

  - Apple addresses
    - *.appstore.com,
    - *.apple.com
    - *.itunes.apple.com
    - *.icloud.com
    - swscan.apple.com (Mac OS updates)
  - Dropbox
    - *.dropbox.com
  - Skype
    - *.messenger.live.com
  - Windows Updates
    - update.microsoft.com

  Add firewall addresses for the sites to exempt, then edit SSL/SSH profiles that are set to Full SSL Inspection and add these addresses to the Exempt from SSL Inspection list. A handy way to manage these addresses would be to create a firewall address group to add to the exempt list and then add that address group to the exempt list.
- To exempt large groups of sites you can select FortiGuard Categories. There are 3 of these categories preselected due to the high likelihood of issues with associated applications with the type of websites included in these categories.
  - Heath and Wellness
  - Personal Privacy
  - Finance and Banking

Disk logging and memory logging changes

On some FortiGate models, flash-based logging is not available in FortiOS v5.2.0. For these platforms, Fortinet recommends the free FortiCloud central logging & reporting service, as it offers higher capacity and extends the features available to the FortiGate. These models include:

- FG-100D (P09340-04 or earlier)
- FG-20C
- FG-20C_ADSL_A
- FG-200B/200B_POE (Without FSM)
- FG-300C_Gen1 (P09616-04 or earlier)

- FG-40C
- FG-60C
- FG-60C-POE
- FG-60C-SFP
- FG-70D
- FG-60D
- FG-80C/80CM (P05403-05, P05446-05)
- FW-20C
- FW-40C
- FW-20C_ADSL_A
- FW-60CX_A
- FW-60C
- FW-60CM (P08962-04 or later)
- FW-60CX_ADSL-A
- FW-60D
- FW-60D-POE
- FW-80CM (P05405-06 or later)

OSPF MTU Mismatch

If you are upgrading from FortiOS v4.3 or FortiOS v5.0 to FortiOS v5.2 and you have OSPF over IPsec configured, the OSPF adjacencies fail to form after the upgrade. The reason for this is a mismatched MTU between FortiGate units running different FortiOS versions. You must change the MTU on the FortiGate device running v5.2 with the following command:

```
config router ospf
   config ospf-interface
       edit "R1_IPSEC"
            set mtu <integer-value>
       next
   end
end
```

Product Integration and Support

Web browser support

FortiOS v5.2.0 build 0589 supports the latest versions of the following web browsers:

- Microsoft Internet Explorer version 10, 11
- Mozilla Firefox version 29.01
- Google Chrome version 34
- Apple Safari version 5.1

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

FortiManager and FortiAnalyzer support

FortiOS v5.2.0 is supported by the following FortiManager and FortiAnalyzer software versions:

- FortiManager v5.0.7
- FortiManager v5.2.0
- FortiAnalyzer v5.0.7
- FortiAnalyzer v5.2.0

You should upgrade the FortiManager and/or FortiAnalyzer prior to upgrading the FortiGate.

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

FortiOS v5.2.0 supports the following versions of FortiClient:

- FortiClient (Windows) v5.0.9 and v5.2.0
- FortiClient (Mac OS X) v5.0.9 and v5.2.0
- FortiClient (iOS) v5.0.9 and v5.2.0
- FortiClient (Android) v5.0.9 and v5.2.0

FortiAP support

FortiOS v5.2.0 supports the following FortiAP software versions:

- FortiAP v5.2.0
- FortiAP v5.0.7

FortiSwitch support

FortiOS v5.2.0 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 build 0018 or later.

FortiOS v5.2.0 supports the following FortiSwitch-5000 series models:

FS-5003B, FS-5003A

The FortiSwitch-5000 device must be running FortiSwitchOS v5.0 Patch Release 3 build 0020 or later.

FortiController support

FortiOS v5.2.0 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 build 0020 or later.

FortiGate VM support

FortiOS v5.2.0 supports the following VM environments:

VMware

- VMware ESX versions 4.0 and 4.1
- VMware ESXi versions 4.0, 4.1, 5.0, 5.1 and 5.5

Fortinet provides the following firmware images for the 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.

Citrix XenServer and Open Source Xen

- 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

Fortinet provides the following firmware images for Citrix XenServer and Open Source Xen:

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

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

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

Open Source Xen limitations

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

Microsoft Hyper-V

- Microsoft Hyper-V Server 2008 R2, 2012, and 2012 R2

Fortinet provides the following firmware images for Microsoft 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.

Linux KVM

- KVM - CentOS 6.4 (qemu 0.12.1) or later

Fortinet provides the following firmware images for Linux 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`.

Fortinet Single Sign-On (FSSO) support

FortiOS v5.2.0 is supported by FSSO v4.0 MR3 B0156 for the following operating systems:

- Microsoft Windows Server 2012 R2
- 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 v5.2.0 is supported by FortiExplorer v2.4 build 1075 or later.

FortiOS v5.2.0 is supported by FortiExplorer (iOS) v1.0.4 build 0126 or later.

FortiExtender support

FortiOS v5.2.0 is supported by FortiExtender models FEX-20B, FEX-100A, and FEX-100B running FortExtender v1.0.0 build 0024.

AV Engine and IPS Engine support

FortiOS v5.2.0 is supported by AV Engine v5.154 and IPS Engine v3.038.

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 v5.2.0 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
Security Processing Module 2x10-GbE SFP+ (FMC-XG2)	FG-3950B, FG-3951B
Accelerated Interface Module 2x10-GbE SFP+ (FMC-XD2)	FG-3950B, FG-3951B

Table 2: Supported modules and FortiGate models (continued)

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 v5.2.0 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 and Ubuntu 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.

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 v10.7 Lion	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 v5.2.0 for the explicit web proxy feature:

- Microsoft Internet Explorer versions 8, 9, 10, and 11
- Mozilla Firefox version 27
- Apple Safari version 6.0
- Google Chrome version 34

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

Resolved Issues

This chapter describes issues with FortiOS v5.2.0 (beta 3 and previous) that have been resolved for FortiOS v5.2.0. If you would like to see a more complete list of resolved issues for this release you can request one by emailing techdoc@fortinet.com.

Resolved issues from FortiOS v5.2.0 beta forums

This section lists some of the issues that posted on the beta forums and resolved. Each issue includes a link to the original beta forum post for more information about the issue.

- The `auto-vpn-when-off-net` option is set to `disable` when the FortiGate does not have a FortiClient 5.2 License (241912) (Beta Forum: 108966)
- Interfaces configured with PPPoE can be added to Virtual WAN Links. (232871) (Beta Forum: 108782)
- Zone interface or zone member can be SSL VPN Interfaces. (238336) (Beta Forum: 107570)
- Normal CPU usage in cmdbsvr and httpsd after cache build-up. (217083) (Beta Forum: 106932 and 106740)
- Webfilter URL filter lists upgrade successfully. (239764) (Beta Forum: 108492)
- The AirCard 340U modem is compatible with FortiOS v5.2.0. (235435) (Beta Forum: 108894)
- Zone interfaces are available for Local-in policies. (237697) (Beta Forum: 107584)

Known Issues

This chapter lists some known issues with FortiOS v5.2.0 build 0589.

- FortiGate units may be unable to authorize dual link FortiSwitches. (244849)

  Workaround: Enable *Dedicate to Extension Device* on the FortiGate interface connected to the FortiSwitch and remove the IP address from the FortiGate interface. Then add manually add the FortiSwitch to the FortiGate.
- Application control cloud-based signatures do not appear. (239938)
- The application control signature categories *File.Sharing* and *Special* have been removed but may still visible on the GUI. (237471)
- If you change a policy from proxy-based Web Filtering to flow-based Web Filtering, users who receive HTTPS traffic may see an invalid certificate error message in their web browser.

  This happens because of how proxy-based and flow-based HTTPS web filtering generates CA certificates. (227441)

  Workaround: This issue is rare and will not be fixed. It should only happen if the policy is changed while it is processing traffic. Users need to delete the CA Certificate on their browsers and accept the new certificate.
- Inspection mode for the default antivirus profile after upgrade will have different attributes than the default configuration. (225956)
- Customized charts lost in default report layout after upgrade. (236568)
- SSL VPN portals can be deleted even if they are added to the Authentication/Portal Mapping list on the SSL VPN settings page. If a portal selected in the portal mapping list on the SSL VPN settings page is deleted you cannot save SSL VPN settings. (243367)

  Workaround: Select a portal for all entries in the portal mapping list. Add more portals if required.
- Filter applied in any of the FortiView widgets also affects other FortiView widgets. (243930)
- GUI will encounter Internal Server Error when modifying log setting page if FAZ is connect via IPSec. (214372)
- The FortiGate fails to reserve an IP address for a client once added through the DHCP monitor. (235425)
- Custom defined application signatures belonging to a certain category may fail to be detected. (235762)
- Restoring a VDOM configuration through the GUI fails. (240148)
- Create multiple custom categories consecutively may result in the second to fail. (241364)
- The FGT-70D may fail to boot when changing from switch mode to interface mode. (243747)
- The pyfcgid daemon may crash when browsing FortiView. (244439)
- The traffic log shows `utmaction=allow` when spam is blocked. (244886)
- The FortiGate fails to show login history in SSL-VPN web mode. (245027)
- Client fails to receive firewall email authentication page if email-collection is enabled in the policy. (245287)
- An installed FMC-XG2 card intermittently may block traffic (245338)
- Downgrading from v5.2.0 to v5.0 and then upgrading to v5.2.0 again will fail unless you run the `execute log downgrade-log` command before downgrading to v5.0. (244039)
- FWF_30D cannot boot up after changing config. (246853)

- OSPF over IPsec will fail upon upgrading due to MTU mismatch. (248651)