

FortiAnalyzer Release Notes

VERSION 5.0.10

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



April 30, 2015

FortiAnalyzer 5.0.10 Release Notes

05-5010-265588-20150430

TABLE OF CONTENTS

Change Log	5
Introduction	6
Supported models	6
What's new in FortiAnalyzer version 5.0.10	6
Special Notices	7
SSLv3 on FortiAnalyzer-VM64-AWS	7
Limited support for remote SQL database	7
Log array disk quota after upgrade	7
Log Array conversion to HA cluster	7
Log database status widgets	8
Disk quota size on HA cluster	8
Report grouping	8
CLI commands to list or view reports in text	9
Changes to log aggregation	9
Log Array relocation	9
Log Arrays, devices, and VDOMs	9
Generate reports during the database rebuild	9
Special characters in report name	10
Required changes to dataset	10
FortiAnalyzer VM	10
Unregistered device table	10
Pre-processing logic of eptime	10
FortiAnalyzer VM license check	11
Extended UTM log for Application Control	11
ConnectWise Management Services Platform (MSP) support	11
Distributed upgrades	11
Upgrade Information	12
Upgrading from FortiAnalyzer version 5.0.6 or later	12
Upgrading from FortiAnalyzer version 5.0.5 or earlier	12
Downgrading to previous versions	12
FortiAnalyzer VM firmware	13
Firmware image checksums	13
SNMP MIB Files	14
Product Integration and Support	15

FortiAnalyzer version 5.0.10 support	15
Feature support	16
Language support	16
Supported models	17
Resolved Issues	25
Known Issues	27

Change Log

Date	Change Description
2015-01-30	Initial release.
2015-02-02	Corrected a typographic issue.
2015-02-04	Added remote SQL database special notice.
2015-02-13	Updated upgrade information section.
2015-03-10	Added video link for upgrade procedure.
2015-04-30	Updated VM Partition and Firmware Information in the Upgrade Information chapter. Added SSLv3 on FortiManager-VM64-AWS note to Special Notices.

Introduction

This document provides the following information for FortiAnalyzer version 5.0.10 build 0365:

- [Supported models](#)
- [What's new in FortiAnalyzer version 5.0.10](#)
- [Special Notices](#)
- [Upgrade Information](#)
- [Product Integration and Support](#)
- [Resolved Issues](#)
- [Known Issues](#)

Please review all sections in this document prior to upgrading your device. For more information on upgrading your device, see the *FortiAnalyzer Upgrade Guide*.

Supported models

FortiAnalyzer version 5.0.10 supports the following models:

FortiAnalyzer	FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-4000A, FAZ-4000B
FortiAnalyzer VM	FAZ-VM32, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN

What's new in FortiAnalyzer version 5.0.10

The following is a list of the new features and enhancements in FortiAnalyzer version 5.0.10.

Logging

- Added a progress bar to display the status of the SQL log database rebuild

Reports

- Report grouping

System

- Two new widgets have been added in *System Settings > Dashboard* to monitor the log database status: *Log Insert Lag Time* and *Insert Rate vs Receive Rate*.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer.

SSLv3 on FortiAnalyzer-VM64-AWS

Due to known vulnerabilities in the SSLv3 protocol, FortiAnalyzer-VM64-AWS only enables TLSv1 by default. All other models enable both TLSv1 and SSLv3. If you wish to disable SSLv3 support, please run:

```
config system global
    set ssl-protocol tlsv1
end
```

Limited support for remote SQL database

Starting with FortiAnalyzer software versions 5.0.7 and 5.2.0, remote SQL database support will only cover the insertion of log data into the remote MySQL database. Historical log search and reporting capabilities, which rely on the remote SQL data, will no longer be supported.

Those wishing to use the full set of FortiAnalyzer features are encouraged to switch as soon as possible to storing SQL data locally on the FortiAnalyzer. The local database can be built based upon existing raw logs already stored on the FortiAnalyzer.

Log array disk quota after upgrade

The disk quota of a log array may exceed the total disk size after upgrade. You should manually adjust the disk quota to the appropriate size on each of the log array members.

Log Array conversion to HA cluster

If you have been using log array to manage your HA device disk quota, migrate from log array to HA cluster for easier management. Refer to the *HA Cluster for Log Conversion* section in the *FortiAnalyzer Upgrade guide* version 5.0.10.

You can also watch the following video: http://forti.net/faz_upgrade for detailed instructions.

Log database status widgets

FortiAnalyzer version 5.0.10 introduces two new widgets in *System Settings > Dashboard: Log Insert Lag Time* and *Insert Rate vs Receive Rate*. After upgrade, the new widgets are not displayed by default for the existing administrators. The new widgets can be added manually.

Disk quota size on HA cluster

When adding a registered FortiGate device to an HA cluster, the default disk quota size on the HA cluster is the sum of all disk quotas allocated on the HA cluster members.

Report grouping

If you are running a large number of reports which are very similar, you can significantly improve report generation time by grouping the reports. Report grouping can reduce the number of hcache tables and improve auto-hcache completion time and report completion time.

Step 1: Configure report grouping

To group reports whose titles contain the string `Security_Report` and are grouped by device ID and VDOM, enter the following CLI commands:

```
config system report group
  edit 0
    set adom root
    config group-by
      edit devid
      next
      edit vd
      next
    end
    set report-like Security_Report
  next
end
```

Notes:

1. The `report-like` field is the name pattern of the report that will utilize the `report-group` feature. This string is case-sensitive.
2. The `group-by` value controls how cache tables are grouped.
3. To see a listing of reports and which ones have been included in the grouping, enter the following CLI command:

```
execute sql-report list-schedule <ADOM>
```

Step 2: Initiate a rebuild of hcache tables

To initiate a rebuild of hcache tables, enter the following CLI command:

```
diagnose sql rebuild-report-hcache <start-time> <end-time>
```


Where `<start-time>` and `<end-time>` are in the format: `<yyyy-mm-dd hh:mm:ss>`.

Step 3: Perform an hcache-check for a given report

Perform an hcache-check for a given report to ensure that the hcache tables exactly match the start and end time frame for the report time period. Enter the following CLI command:

```
execute sql-report hcache-check <adom> <report_id> <start-time> <end-time>
```

If you do not run this command, the first report in the report group will take a little longer to run. All subsequent reports in that group will run optimally.

CLI commands to list or view reports in text

Two CLI commands have been added in FortiAnalyzer version 5.0.10 to list and view reports in text. To list reports, run `execute sql-report list <adom> [days-range] [layout-name]`. To view reports, run `execute sql-report view <data-type> <adom> <report-name>`.

Changes to log aggregation

In FortiAnalyzer version 5.0.9, new functionality was added to log aggregation to allow for multiple devices to be uploaded concurrently.

As a result, more information is included in the log aggregation negotiation messages. Both client and analyzer should be upgraded together to ensure log aggregation continues to work.

Log Array relocation

Log Array has been relocated to *Log View* under the *FortiView* module from the *Device Manager* module.

Log Arrays, devices, and VDOMs

In FortiAnalyzer version 5.0.6 or earlier, when creating a Log Array with both devices and VDOMs, you need to select each device and VDOM to add it to the Log Array. In FortiAnalyzer version 5.0.7 or later, when selecting to add a device with VDOMs, all VDOMs are automatically added to the Log Array.

Generate reports during the database rebuild

After your device is upgraded, the system may need to rebuild databases due to schema changes. Please note that the ability to generate accurate reports will be affected until the rebuild is complete.

Special characters in report name

FortiAnalyzer version 5.0.7 and later does not support the following special characters in report's name:

`\ / ' " > < & , |`

If you wish to import a report, please make sure the above special characters are not used. Otherwise, your device may not display the name properly.

Required changes to dataset

Due to database schema changes in FortiAnalyzer version 5.0.7, the following rules must be followed by any existing or new datasets:

- If your dataset references any IP related data, such as `srcip` or `dstip`, please use the `ipstr('...')` function to convert an IP address for proper display. For example, `ipstr('srcip')` returns the source IP in a string.
- The column, `status`, has been changed to `action`. Please replace `status` with `action` in dataset query for proper status.

FortiAnalyzer VM

In VM environments, upgrade your VM server to latest stable update and patch release offered by the VM host server provider before installing or upgrading FortiAnalyzer VM.

Unregistered device table

In FortiAnalyzer version 5.0.4 or earlier releases, the `config system global set unregister-pop-up` command is enabled by default. When a FortiGate device is configured to send logs to FortiAnalyzer, the unregistered device table will be displayed. You can decide to promote the device now or at a later date.

In FortiAnalyzer version 5.0.5 or later, the `config system global set unregister-pop-up` command is disabled by default. When a FortiGate device is configured to send logs to FortiAnalyzer, the unregistered device table will not be displayed. Instead, a new entry *Unregistered Devices* will appear in the Device Manager tab under *All FortiGate*. You can then promote devices to specific ADOMs or use the right-click menu to delete the device.

Pre-processing logic of ebtime

Logs with the following conditions met are considered usable for the calculation of estimated browsing time:

Traffic logs with `logid` of 13 or 2, when `logid == 13`, `hostname` must not be empty. The `service` field should be either `HTTP, 80/TCP` or `443/TCP`.

If all above conditions are met, then `devid`, `vdom`, and `user` (`srcip` if `user` is empty) are combined as a key to identify a user. For time estimation, the current value of `duration` is calculated against history session start and end time, only un-overlapped part are used as the `ebtime` of the current log.

In FortiAnalyzer version 5.0.5 or later, Explicit Proxy logs (`logid=10`) are checked when calculating the estimated browsing time.

FortiAnalyzer VM license check

As a part of the license validation process FortiAnalyzer VM compares its IP address with the IP information in the license file. If the IP address does not match, FortiAnalyzer VM returns the error `IP does not match` within CLI command `get system status` output. If a new license has been imported or the FortiAnalyzer VM's IP address has been changed, the FortiAnalyzer VM must be manually rebooted in order for the system to validate the change and operate with a valid license.

Extended UTM log for Application Control

Upon upgrading to FortiAnalyzer version 5.0.10, the application control log is not visible until you enable the extended UTM log in the FortiOS CLI.

To enable extended UTM log, use the following CLI command:

```
config application list
  edit <name>
    set extended-utm-log enable
  end
```

ConnectWise Management Services Platform (MSP) support

ConnectWise Management Services Platform (MSP) is not supported in FortiAnalyzer version 5.0.

Distributed upgrades

For Collector/Analyzer architecture upgrades, Fortinet recommends upgrading the Analyzer first.



Upgrading the Collector first could impact the Analyzer's performance.

Upgrade Information



For more information on upgrading your device, see the *FortiAnalyzer Upgrade Guide*.

Upgrading from FortiAnalyzer version 5.0.6 or later

FortiAnalyzer version 5.0.10 supports upgrade from version 5.0.6 or later.

FortiAnalyzer version 5.0.7 or later has re-sized the flash partition storing system firmware. If your FortiAnalyzer is running 5.0.6, you will need to change the hard disk provisioned size to more than 512 MB in your VM environment before powering on the FortiAnalyzer VM. The secondary firmware and System Settings stored in the partition is lost after upgrade. Please reconfigure System Settings as needed.



Upgrading your FAZ-400B to version 5.0.10 requires you to use an interim step. You **MUST** upgrade to version 5.0.7 before upgrading to 5.0.10. For more information see the *FortiAnalyzer 5.0.7 Release Notes*. The upgrade path looks like this:
5.0.5 or earlier > 5.0.6 > 5.0.7 > 5.0.10

Upgrading from FortiAnalyzer version 5.0.5 or earlier

In order to accommodate the re-sizing of the flash partition, you **MUST** upgrade to version 5.0.6 first.



Please upgrade your FAZ-100C, FAZ-2000A, or FAZ-4000A via the Web-based Manager or command line interface. Upgrade via TFTP from BIOS is not supported for these models.

Downgrading to previous versions

FortiAnalyzer does not provide a full downgrade path. You can downgrade to a previous firmware release via the Web-based Manager or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset all-settings
execute format {disk | disk-ext4}
```

FortiAnalyzer VM firmware

Fortinet provides FortiAnalyzer VM firmware images for Amazon AWS, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

Amazon Web Services

- The 64-bits Amazon Machine Image (AMI) is available on the AWS marketplace.

Citrix XenServer and Open Source XenServer

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

Linux KVM

- `.out`: Download the 64-bits firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.out.kvm.zip`: Download the 64-bits package for a new FortiAnalyzer VM installation. This package contains QCOW2 that can be used by qemu.

Microsoft Hyper-V Server

- `.out`: Download the firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.hyperv.zip`: Download the package for a new FortiAnalyzer VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.

VMware ESX/ESXi

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



For more information see the FortiManager product data sheet available on the Fortinet web site, <http://www.fortinet.com/products/fortimanager/virtualappliances.html>. VM installation guides are available in the [Fortinet Document Library](#).

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, <https://support.fortinet.com>. To verify the integrity of the download, select the *Checksum* link next to the

HTTPS download link. A dialog box will be displayed with the image file name and checksum code. Compare this checksum with the checksum of the firmware image.

SNMP MIB Files

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiAnalyzer v5.00 file folder.

Product Integration and Support

FortiAnalyzer version 5.0.10 support

The following tables list FortiAnalyzer version 5.0.10 product integration and support information:

Web Browsers	<ul style="list-style-type: none">• Microsoft Internet Explorer version 11• Mozilla Firefox version 35• Google Chrome version 40 <p>Other web browsers may function correctly, but are not supported by Fortinet.</p>
FortiOS/FortiOS Carrier	<ul style="list-style-type: none">• 5.2.0 and later• 5.0.0 and later• 4.3.2 and later• 4.2.0 and later
FortiCache	<ul style="list-style-type: none">• 3.0.0 to 3.0.2
FortiClient	<ul style="list-style-type: none">• 5.2.0 and later• 5.0.4 and later
FortiMail	<ul style="list-style-type: none">• 5.2.0 to 5.2.2• 5.1.3 to 5.1.4• 5.0.6 to 5.0.7
FortiSandbox	<ul style="list-style-type: none">• 1.4.0 and later• 2.0.0
FortiWeb	<ul style="list-style-type: none">• 5.3.0 to 5.3.4• 5.2.3 to 5.2.4• 5.1.4• 5.0.6
Syslog	<ul style="list-style-type: none">• Standard syslog

Virtualization

- Amazon Webservice AMI, Amazon EC2, Amazon EBS
- Citrix XenServer 6.2
- Linux KVM Redhat 6.5
- Microsoft Hyper-V 2008 R2 and 2012
- OpenSource XenServer 4.2.5

VMware

- ESX version 4.1
- ESXi versions 4.1, 5.1, and 5.5

Feature support

The following table lists FortiAnalyzer feature support for log devices.

Platform	Logging	FortiView	Event Management	Reports
FortiGate	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓
FortiCache	✓			✓
FortiClient	✓			
FortiMail	✓			✓
FortiSandbox	✓			
FortiWeb	✓			✓
Syslog	✓			

Language support

The following table lists FortiAnalyzer language support information.

Language	Web-based Manager	Reports	Documentation
English	✓	✓	✓
Chinese (Simplified)	✓	✓	
Chinese (Traditional)	✓	✓	
French		✓	

Language	Web-based Manager	Reports	Documentation
Hebrew		✓	
Hungarian		✓	
Japanese	✓	✓	
Korean	✓	✓	
Portuguese		✓	
Russian		✓	
Spanish		✓	

To change the FortiAnalyzer language setting, go to *System Settings > Admin > Admin Settings*, in *Administrative Settings > Language* select the desired language on the drop-down menu. The default value is *Auto Detect*.

Russian, Hebrew, and Hungarian are not included in the default report languages. You can import language translation files for these languages via the command line interface using one of the following commands:

```
execute sql-report import-lang <language name> <ftp> <server IP address> <user name>
  <password> <file name>
execute sql-report import-lang <language name> <sftp> <server IP address> <user name>
  <password> <file name>
execute sql-report import-lang <language name> <scp> <server IP address> <user name>
  <password> <file name>
execute sql-report import-lang <language name> <tftp> <server IP address> <file name>
```

For more information, see the *FortiAnalyzer CLI Reference*.

Supported models

The following tables list which FortiGate, FortiGateVoice, FortiCarrier, FortiCache, FortiMail, FortiSandbox, and FortiWeb models and firmware versions can log to a FortiAnalyzer appliance running FortiAnalyzer. Please ensure that the log devices are supported before completing the upgrade.

Supported FortiGate models

Model	Firmware Version
<p>FortiGate</p> <p>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, FG-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-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-500D, FG-600C, FG-620B, FG-621B, FG-800C, FG-1000C, FG-1240B, FG-1500D, FG-3016B, FG-3040B, FG-3140B, FG-3240C, FG-3600C, FG-3700DX, FG-3810A, FG-3810D, FG-3950B, FG-3951B, FG-5001A, FG-5001B, FG-5001C, FG-5001D, FG-5101C</p>	5.2
<p>FortiGate DC</p> <p>FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3040B-DC, FG-3140B-DC, FG-3240C-DC, FG-3600C-DC, FG-3810A-DC, FG-3950B-DC, FG-3951B-DC</p>	
<p>FortiGate Low Encryption</p> <p>FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-310B-LENC, FG-600C-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC</p>	
<p>FortiWiFi</p> <p>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, FWF-90D-POE</p>	
<p>FortiGate Rugged</p> <p>FGR-60D, FGR-100C</p>	
<p>FortiGate VM</p> <p>FG-VM, FG-VM64, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN</p>	
<p>FortiSwitch</p> <p>FS-5203B</p>	

Model	Firmware Version
<p>FortiGate</p> <p>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-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, 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-200D-POE, FG-240D, FG-240D-POE, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-500D, FG-600C, FG-620B, FG-621B, FG-800C, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-3016B, FG-3040B, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3810A, FG-3950B, FG-3951B, FG-5001A, FG-5001B, FG-5001C, FG-5001D, FG-5101C, FG-5001D</p>	5.0
<p>FortiGate DC</p> <p>FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3040B-DC, FG-3140B-DC, FG-3240C-DC, FG-3600C-DC, FG-3810A-DC, FG-3950B-DC, FG-3951B-DC</p>	
<p>FortiGate Low Encryption</p> <p>FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-310B-LENC, FG-600C-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC</p>	
<p>FortiWiFi</p> <p>FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CM-3G4G-B, FWF-60CX-ADSL-A, FWF-60D-POE, FWF-60D, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D</p>	
<p>FortiGate Rugged</p> <p>FGR-60D, FGR-90D, FGR-100C</p>	
<p>FortiGate VM</p> <p>FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN</p>	
<p>FortiSwitch</p> <p>FS-5203B</p>	

Model	Firmware Version
<p>FortiGate</p> <p>FG-20C, FG-20C-ADSL-A, FG-30B, FG-40C, FG-50B, FG-51B, FG-60B, FG-60C, FG-60C-POE, FG-60C-SFP, FG-80C, FG-80CM, FG-82C, FG-100A, FG-100D, FG-110C, FG-111C, FG-200A, FG-200B, FG-200B-POE, FG-224B, FG-300A, FG-300C, FG-310B, FG-311B, FG-400A, FG-500A, FG-600C, FG-620B, FG-621B, FG-800, FG-800C, FG-800F, FG-1000, FG-1000A, FG-1000AFA2, FG-1000C, FG-1240B, FG-3016B, FG-3040B, FG-3140B, FG-3240C, FG-3600, FG-3600A, FG-3810A, FG-3950B, FG-3951B, FG-5001, FG-5001A, FG-5001B, FG-5001C, FG-5001FA2, FG-5002A, FG-5002FB2, FG-5005FA2, FG-5101C</p> <p>FortiGate DC</p> <p>FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-620B-DC, FG-600C-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3040B-DC, FG-3140B-DC, FG-3240C-DC, FG-3810A-DC, FG-3950B-DC, FG-3951B-DC</p> <p>FortiGate Low Encryption</p> <p>FG-20C-LENC, FG-40C-LENC, FG-50B-LENC, FG-51B-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-310B-LENC, FG-600C-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC, FG-5001FA2-LENC, FG-5002A-LENC</p> <p>FortiWiFi</p> <p>FWF-20C, FWF-20C-ADSL-A, FWF-30B, FWF-40C, FWF-50B, FWF-60B, FWF-60C, FWF-60CM, FWF-60CM-3G4G-B, FWF-60CX-ADSL-A, FWF-80CM, FWF-81CM</p> <p>FortiGate Rugged</p> <p>FGR-100C</p> <p>FortiGate One</p> <p>FG-ONE</p> <p>FortiGate VM</p> <p>FG-VM, FG-VM64, FG-VM64-XEN</p> <p>FortiSwitch</p> <p>FS-5203B</p>	4.3

Model	Firmware Version
FortiGate FG-30B, FG-50B, FG-51B, FG-60B, FG-80C, FG-80CM, FG-80CM, FG-82C, FG-100A, FG-110C, FG-111C, FG-200A, FG-200B, FG-200B-POE, FG-224B, FG-300A, FG-300C, FG-310B, FG-311B, FG-400A, FG-500A, FG-620B, FG-621B, FG-800, FG-800F, FG-1000, FG-1000A, FG-1000AFA2, FG-1240B, FG-3016B, FG-3040B, FG-3140B, FG-3600, FG-3600A, FG-3810A, FG-3950B, FG-3951B, FG-5001, FG-5001A, FG-5001B, FG-5001FA2, FG-5002A, FG-5002FB2, FG-5005FA2	4.2
FortiGate DC FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-620B-DC, FG-621B-DC, FG-1240B-DC, FG-3040B-DC, FG-3140B-DC, FG-3810A-DC, FG-3950B-DC, FG-3951B-DC	
FortiGate Low Encryption FG-50B-LENC, FG-51B-LENC, FG-80C-LENC, FG-300C-LENC, FG-310B-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC, FG-5001FA2-LENC, FG-5002A-LENC	
FortiWiFi FWF-30B, FWF-50B, FWF-60B, FWF-60CX-ADSL-A, FWF-60CM, FWF-80CM, FWF-81CM, FWF-80CM, FWF-81CM	
FortiGate One FG-ONE	
FortiGate VM FG-VM	

Supported FortiGateVoice models

Model	Firmware Version
FortiGateVoice FGV-40D2, FGV-70D4	5.0

Supported FortiCarrier models

Model	Firmware Version
FortiCarrier FCR-3240C, FCR-3600C, FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5101C	5.2
FortiCarrier DC FCR-3240C-DC, FCR-3600C-DC, FCR-3810A-DC, FCR-3910B-DC, FCR-3950B-DC	
FortiCarrier Low Encryption FCR-5001A-DW-LENC	
FortiCarrier VM FCR-VM, FCR-VM64	
FortiCarrier FCR-3240C, FCR-3600C, FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5101C	5.0
FortiCarrier DC FCR-3240C-DC, FCR-3600C-DC, FCR-3810A-DC, FCR-3950B-DC, FCR-3910B-DC	
FortiCarrier Low Encryption FCR-5001A-DW-LENC	
FortiCarrier VM FCR-VM, FCR-VM64	
FortiCarrier FG-60B, FG-80C, FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001, FCR-5001A, FCR-5001B, FCR-5001FA2, FCR-5005FA2	4.3
FortiCarrier DC FCR-3810A-DC, FCR-3950B-DC, FCR-3910B-DC	
FortiCarrier Low Encryption FCR-5001A-DW-LENC	

Model	Firmware Version
FortiCarrier	4.2
FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001, FCR-5001A, FCR-5001B, FCR-5001FA2, FCR-5005FA2	
FortiCarrier DC	
FCR-3810A-DC, FCR-3950B-DC, FCR-3910B-DC	
FortiCarrier Low Encryption	
FCR-5001A-DW-LENC	

Supported FortiCache models

Model	Firmware Version
FortiCache	3.0
FCH-400C, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D	
FortiCache VM	
FCH-VM64	

Supported FortiMail models

Model	Firmware Version
FortiMail	5.1
FE-100C, FE-200D, FE-400B, FE-400C, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5001A, FE-5002B	
FortiMail VM	
FE-VM64	
FortiMail	5.0
FE-100C, FE-200D, FE-400B, FE-400C, FE-1000D, FE-2000A, FE-2000B, FE-3000C, FE-3000D, FE-4000A, FE-5001A, FE-5002B	
FortiMail VM	
FE-VM64	

Supported FortiSandbox models

Model	Firmware Version
FortiSandbox	2.0
FSA-1000D, FSA-3000D, FSA-VM	1.4

Supported FortiWeb models

Model	Firmware Version
FortiWeb	5.3
FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-	5.2
3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-4000C, FWB-	5.1
4000D	5.0
FortiWeb VM	
FWB-VM64	

Resolved Issues

The following issues have been fixed in FortiAnalyzer version 5.0.10. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Device Manager

Bug ID	Description
0257037	Unable to load devices properly when there are several thousand devices.

Event Management

Bug ID	Description
0218025	The additional information field does not show very relevant data for web filter and application control.

FortiView

Bug ID	Description
0252751	When explicit proxy is enabled on FortiGate, FortiView's top web sites are not populated.
0255869	The SQL insertion rate may not be sufficient for rendering many historical logs.
0265368	Filtering on <i>Device Name</i> returns no records found.

Reporting

Bug ID	Description
0257514	VPN related reports may not work after upgrading.
0260639	All log entries are downloaded if <i>Now</i> is selected at the end time on a custom time period.
0253212, 0253806	Cannot save configuration changes for the header and footer.
0258224	After upgrade, all custom reports in the root VDOM may disappear.

System Settings

Bug ID	Description
0252762	The log file format may not be consistent.

Others

Bug ID	Description
0252933	Backup configuration fails with a <code>get all_backup_mutex not success error</code> .
0257160	The <code>sqlrplugind</code> daemon may not function properly after upgrading.
0259522	Reports and output profiles may be lost after upgrading.
0259523	The OFTP daemon may crash after upgrading.

Known Issues

The following issues have been identified in FortiAnalyzer version 5.0.10. For inquires about a particular bug or to report a bug, please contact [Customer Service & Support](#).

FortiView

Bug ID	Description
0265977	Administrators cannot open DLP archived files after downloading them from FortiAnalyzer.

Reporting

Bug ID	Description
0262593	Japanese characters in a PDF formatted report are displayed in an unexpected format.
0264445	The scheduled report start time is incremented by two hours after making changes to report configuration.

Others

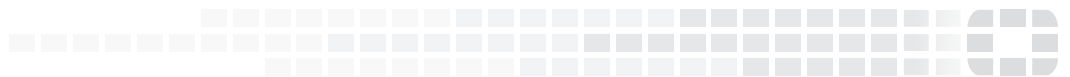
Bug ID	Description
0265095	The <code>fwd-min-level</code> setting should be enforced for each <code>aggregation-client</code> .

System Settings

Bug ID	Description
0267488	After creating a new administrator, the <i>Insert Rate vs Receive Rate</i> widget and the <i>Log Insert Lag Time</i> widget do not show any graphs. Workaround: Please refresh the widgets



High Performance Network Security



Copyright© 2015 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.