

Release Notes

FortiAnalyzer-BigData 7.0.4



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



January 21, 2025

FortiAnalyzer-BigData 7.0.4 Release Notes

58-704-816026-20250121

TABLE OF CONTENTS

Change Log	4
FortiAnalyzer-BigData version 7.0.4	5
Supported models	5
New features and enhancements	5
Special Notices	6
Ports	6
Log Files	6
Product Integration and Support	7
Firmware Upgrade Paths	8
Fortinet Security Fabric	8
Resolved Issues	9
Known Issues	11

Change Log

Date	Change Description
2022-08-25	Initial release.
2025-01-21	Removed reference to FortiAnalyzer-BigData-VM.

FortiAnalyzer-BigData version 7.0.4

This document provides information about FortiAnalyzer-BigData version 7.0.4 build 0145.



The recommended minimum screen resolution for the FortiAnalyzer-BigData GUI is 1920 x 1080. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

Supported models

FortiAnalyzer-BigData version 7.0.4 supports the following models:

FortiAnalyzer-BigData	FAZBD-4500F
------------------------------	-------------

New features and enhancements

For more information about what's new in FortiAnalyzer-BigData and supported by FortiAnalyzer-BigData 7.0.4, see the [FortiAnalyzer 7.0 New Features Guide](#).

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer-BigData version 7.0.4.

There are currently no special notices included for FortiAnalyzer-BigData 7.0.4.

Ports

Please be aware of the limitations for the following ports:

- Port 2055 reserved.
- Default Admin https port 443 cannot be customized.

Log Files

The log file rolling size setting should be smaller than the minimum ADOM cache allocation size of blade1.

Product Integration and Support

FortiAnalyzer-BigData 7.0.4 support of other Fortinet products is the same as FortiAnalyzer 7.0.4. For details, see the [FortiAnalyzer 7.0.4 Release Notes](#) in the Document Library.

Upgrade bootloader

If you are currently using FortiAnalyzer-BigData, we recommend upgrading bootloader.

To upgrade bootloader, connect to the Security Event Manager Controller and run the following command:

```
fazbdctl upgrade bootloader
```

Firmware Upgrade Paths

You can upgrade FortiAnalyzer-BigData 6.4.0 or later to FortiAnalyzer 7.0.4.

The following table identifies the supported FortiAnalyzer-BigData upgrade paths and whether the upgrade requires a rebuild of the log database. If you need information about upgrading to FortiAnalyzer 6.2 or 6.4, see the corresponding FortiAnalyzer Upgrade Guide.

Initial Version	Upgrade to	Log Database Rebuild
6.4.5 or later	Latest 6.4 version, then to latest 7.0 version	No
6.2.1 or later	Latest 6.2 version, then to latest 6.4 version	No



FortiGate units with logdisk buffer log data while FortiAnalyzer units are rebooting. In most cases, the buffer is enough to cover the time needed for FortiAnalyzer to reboot. However, Fortinet still recommends configuring multiple log destinations to ensure no logs are lost.

Fortinet Security Fabric

If you are upgrading the firmware for a FortiAnalyzer-BigData unit that is part of a FortiOS Security Fabric, be aware of how the FortiOS Security Fabric upgrade affects the FortiAnalyzer-BigData upgrade. You must upgrade the products in the Security Fabric in a specific order. For example, you must upgrade FortiAnalyzer-BigData to 7.0.0 or later before you upgrade FortiOS to 7.0.0 or later.

Resolved Issues

The following issues have been fixed in FortiAnalyzer-BigData version 7.0.4. For inquiries about a particular bug, please contact [Customer Service & Support](#).

GUI

Bug ID	Description
832703	<i>Device Manager</i> page does not display devices after upgrade when only ingesting Syslog.
807486	<i>Device Manager</i> page fails to load.

LogView

Bug ID	Description
814585	FortiAnalyzer-BigData only shows 10 pages in the <i>Log View</i> .
818415	Log data is not returned to FortiGate when it pulls with time range older than current day.
831761	<code>getLogTypes</code> API in setup page returns 500.
830504	FortiAnalyzer-BigData has Issues with Syslog devices.

FortiSoC

Bug ID	Description
834933	<code>scanioc</code> often shows Zombie state at top even after IOC is disabled.
833998	<i>No entry found</i> is returned when drilling down from the IOC rescan task.
728350	Incident & Event does not tag <code>Ioc_Rescan</code> for the rescanned <i>Compromised Host</i> .

FortiView

Bug ID	Description
831781	No data is returned and error in log when drilling down from <i>Compromised Hosts</i> .

Reports

Bug ID	Description
806312	Report breaks when all devices are not selected.
831797	Inaccurate report result (part 2) in <i>Traffic</i> statistics when a specific device is selected under the device filter.
831408	New ADOM has <i>Asset and Identity Report</i> with enabled auto-cache by default.
829170	<i>Throughput Utilization Billing Report</i> not working in FortiAnalyzer-BigData.
822364	Inefficient Temp Tables in Report Facet Formation.
818232	Report is lank when report period is last <i>N</i> day or <i>yesterday</i> .

System Setting

Bug ID	Description
836348	Upgrade failure: Blade 3 shows state: <i>upgrading</i> , status: <i>left [need upgrade]</i> .
834816	GUI access fails after upgrading to 0137 build.
758386	FortiAnalyzer-BigData support for Secure Protocol to transfer firmware image.

Common

Bug ID	Description
835942	Kudu skewness threshold value is not updated during job data upgrade
834082	Data re-balance all job improvement.
831367	Old environment cannot import job template which is exported from a newer system.
824453	Support remote shell from portal host page.

Known Issues

The following issues have been identified in FortiAnalyzer-BigData version 7.0.4. For inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

GUI

Bug ID	Description
836306	FortiAnalyzer-BigData Federation Global search displays the GUI error: <i>Cannot read properties of undefined (reading 'includes')</i> .

LogView

Bug ID	Description
837009	LogView cannot display data in FortiAnalyzer ADOM.

FortiView

Bug ID	Description
765976	Performance issues in FortiAnalyzer-BigData Multi-ADOM environments.

Monitors

Bug ID	Description
835276	Log error when user queries <i>Monitors > VPN(FortiFirewall) > Top Dialup VPN</i> .

Reports

Bug ID	Description
831630	Exception is thrown in logs when running the <i>FortiAI Breach Prevention Report</i> .

Common

Bug ID	Description
794932	FortiAnalyzer-BigData oftpd hangs and FortiGate is not able to pull logs.

Bug ID	Description
835191	FortiGate does load more than 5000 logs when pulling logs from FortiAnalyzer-BigData.
833496	FortiMail > Email filter logs should be supported by IOC.



www.fortinet.com

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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 Chief Legal Officer, 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. 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.