

Release Notes

FortiAnalyzer-BigData 7.4.2



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



June 02, 2026

FortiAnalyzer-BigData 7.4.2 Release Notes

58-742-1084097-20260602

TABLE OF CONTENTS

Change Log	4
FortiAnalyzer-BigData version 7.4.2	5
Supported models	5
New features and enhancements	5
Features available in FortiAnalyzer-BigData 7.4.2+, but not in FortiAnalyzer 7.4.4	5
FortiAnalyzer-BigData 7.4.1: Main Host HA support added	6
Special Notices	8
Main Host HA support added in 7.4.1	8
Active-Passive operation mode for Main Host HA is deprecated	8
Chart Builder issues in FortiAnalyzer-BigData	8
Ports	9
Log Files	9
Product Integration and Support	10
Firmware Upgrade Paths	11
Fortinet Security Fabric	11
Resolved Issues	12
Common Vulnerabilities and Exposures	13
Known Issues	14
FortiAnalyzer-BigData-4500G limitations	15

Change Log

Date	Change Description
2024-10-23	Initial release.
2025-01-21	Removed reference to FortiAnalyzer-BigData-VM.
2025-02-06	Updated New features and enhancements on page 5 .
2025-03-11	Updated Resolved Issues on page 12 .
2025-08-08	Updated New features and enhancements on page 5 .
2025-10-15	Updated New features and enhancements on page 5 .
2025-11-03	Updated New features and enhancements on page 5 .
2026-01-29	Updated New features and enhancements on page 5 .
2026-06-02	Updated FortiAnalyzer-BigData-4500G limitations on page 15 .

FortiAnalyzer-BigData version 7.4.2

This document provides information about FortiAnalyzer-BigData version 7.4.2 build 0933.

FortiAnalyzer-BigData 7.4.2 also supports features in FortiAnalyzer 7.4.4. For more information about FortiAnalyzer features, see the [FortiAnalyzer documentation](#).

There are some features available in FortiAnalyzer-BigData 7.4.2 that are not available in FortiAnalyzer 7.4.4. For details, see [New features and enhancements on page 5](#).

Note that some FortiAnalyzer 7.4.4 features, such as "Fabric of FAZ", are not supported in FortiAnalyzer-BigData 7.4.2.



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 7.4.2 supports the following models:

FortiAnalyzer-BigData	FAZBD-4500F, FAZBD-4500G
------------------------------	--------------------------

New features and enhancements

For more information about what's new in FortiAnalyzer-BigData and supported by FortiAnalyzer-BigData 7.4.2, see the [FortiAnalyzer 7.4 New Features Guide](#).

Features available in FortiAnalyzer-BigData 7.4.2+, but not in FortiAnalyzer 7.4.4

The following feature is available in FortiAnalyzer-BigData 7.4.2 and later but not available in FortiAnalyzer 7.4.4.

Administrators with privacy masking enabled can download logs from Log View:

In FortiAnalyzer-BigData 7.4.2 and later, administrators with a *Privacy Masking*-enabled Admin Profile can download logs from *Log View*. The masked data is excluded from the output.

FortiAnalyzer-BigData 7.4.1: Main Host HA support added

Main Host HA support is introduced in FortiAnalyzer-BigData 7.4.1, enabling an Active-Active HA mode for Main Hosts across both chassis, providing high availability and scalability. This guide outlines the steps for recommissioning Blade 1 in the extender chassis within a chassis-stacked FortiAnalyzer-BigData 7.4.1 or later setup that has been upgraded from version 7.2.

If you are scaling out after upgrading to or deploying FortiAnalyzer-BigData 7.4.1 or later, see [How to scale out](#) in the FortiAnalyzer-BigData Administration Guide.

To recommission Blade 1 in the extender chassis for a 4500F model:

1. With Blade 1 in the extender chassis (Chassis2-Blade1) powered off, upgrade from 7.2 to 7.4.1 or later.
2. After the upgrade is complete, go to *Cluster Manager > Services > Core*, and stop the *Catalog* service.
3. Verify that the *Catalog* service has stopped, then power on Blade 1 in the extender chassis (Chassis 2-Blade 1).

4. Access the Controller and execute the following command to update the config:

```
fazbdadm config set config/network/faz/<Chassis2-Blade1 IP> <Chassis2-Blade1 IP>
```

For example:

```
fazbdadm config set config/network/faz/198.18.2.1 198.18.2.1
```

5. Ensure the FAZ image is located in controller (198.18.1.2) under `/mnt/boot/package/faz.out`.
6. Connect to the extender blade with the following command:

```
ssh admin@198.18.2.1
```

Provide password if required for log in.

7. Upgrade FAZ with the following command:

```
execute restore image ftp faz.out 198.18.1.2 anonymous ""
```

When you receive the following prompt, type `y` to continue the upgrade and eventual reboot.

```
This operation will replace the current firmware version and reboot the system!  
Do you want to continue? (y/n)
```

8. Connect back to the extender blade with the following command:

```
ssh admin@198.18.2.1
```
9. Run the following command to confirm the new version is displayed:

```
get system status
```
10. Configure FortiAnalyzer HA using the FortiAnalyzer GUI or CLI.
For more information, see [Set up Main Host HA in stacked FortiAnalyzer-BigData 4500F chassis](#) in the FortiAnalyzer-BigData Administration Guide.
11. In *Cluster Manager > Services > Core*, start the *Catalog* service.

To recommission Blade 1 in the extender chassis for a 4500G model:

1. With Blade 1 in the extender chassis (Chassis2-Blade1) turned off, upgrade from 7.2 to 7.4.1 or later.
2. After the upgrade is complete, access the Controller and execute the following command:

```
fazbdadm enable pxe-once
```

This enables the PXE server to allow the Chassis2-Blade1 to join.
3. Use the following steps to wipe Chassis2-Blade1 and PXE boot it from the Controller:
 - a. Turn on Chassis2-Blade1 and, **before** Chassis2-Blade1 boots into the OS, access its bootloader menu.
 - b. In the bootloader prompt, type `wipe` and confirm to wipe the host and get ready for PXE installation from the Controller.



Wipe is a hidden command that does not show on the bootloader menu. Use it with caution.

- c. After the wipe takes effect, the blade will start booting from PXE. **Before** it boots into the OS, access the bootloader menu to set `ChassisId=2` and `BladeId=1`, and then reboot.
 - d. Wait for the host to boot into the FortiAnalyzer-BigData OS.
4. In the Cluster Manager web GUI, go to the *Hosts* view and wait for the new host to appear in the table.
5. Once the new host appears, click *Assign Role* to assign the Main Host role to the new host. Main Host HA Active-Active mode should be configured automatically during the role assignment.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer-BigData version 7.4.2.

Main Host HA support added in 7.4.1

Main Host HA support is introduced in FortiAnalyzer-BigData 7.4.1, enabling an Active-Active HA mode for Main Hosts across both chassis, providing high availability and scalability.

For steps to recommission Blade 1 in the extender chassis within a chassis-stacked 7.4.1 or later setup that has been upgraded from version 7.2, see *FortiAnalyzer-BigData 7.4.1: Main Host HA support added* in [New features and enhancements on page 5](#).

For steps to scale out after upgrading to or deploying FortiAnalyzer-BigData 7.4.1 or later, see [How to scale out](#) in the FortiAnalyzer-BigData Administration Guide.

Active-Passive operation mode for Main Host HA is deprecated

Active-Passive operation mode for Main Host HA is deprecated in FortiAnalyzer-BigData 7.4.1.

If you are using Active-Passive in a previous version and upgrading to FortiAnalyzer-BigData 7.4.2, the mode should be switched to Active-Active automatically after upgrading.

Chart Builder issues in FortiAnalyzer-BigData

The following issues are present in *Chart Builder* for FortiAnalyzer-BigData 7.4.2, but not in regular FortiAnalyzer:

Bug ID	Description
928222	The <i>Preview</i> in <i>Chart Builder</i> displays sql error when using the following settings: <ul style="list-style-type: none">• <i>Columns</i> include <i>Date/Time</i> and <i>Application</i>• <i>Group By</i> = <i>Application</i>

The following issues are present in *Chart Builder* for both FortiAnalyzer-BigData 7.4.2 and regular FortiAnalyzer:

Bug ID	Description
888280	The <i>Preview</i> in <i>Chart Builder</i> displays the error "Device not exist" when device groups or log groups are selected in the device filter for <i>Log View</i> .
896553	The <i>Preview</i> in <i>Chart Builder</i> displays an error message when selecting <i>Device</i> for traffic.

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 7.4.2 support of other Fortinet products is the same as FortiAnalyzer 7.4.4. For details, see the [FortiAnalyzer 7.4.4 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
```

You can also upgrade bootloader from the GUI. For more information, see [Bootloader in the FortiAnalyzer-BigData Administration Guide](#).

Firmware Upgrade Paths

The following table identifies the supported FortiAnalyzer-BigData upgrade paths and whether the upgrade requires a rebuild of the log database.

Initial Version	Upgrade to	Log Database Rebuild
7.4.0 or later	7.4.2	No
7.2.0 or later	Latest 7.2 version, then to 7.4.2	No
7.0.0 or later	Latest 7.0 version, then to latest 7.2 version	No
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 7.2.0 or later before you upgrade FortiOS to 7.2.0 or later.

Resolved Issues

The following issues have been fixed in FortiAnalyzer-BigData version 7.4.2. To inquire about a particular bug, please contact [Customer Service & Support](#).

Common

Bug ID	Description
1038201	Failed to download FortiCare Debug Report.

FortiSoC

Bug ID	Description
1013880	No data is returned and error in log when add filter "Source IP" or "Destination IP" in <i>Threat Hunting</i> .

FortiView

Bug ID	Description
1006427	No data is shown and error in backend response when query "Top Endpoint Vulnerabilities" on FortiGate.

LogView

Bug ID	Description
1036317	Log View > All log type (such as FortiGate) > Traffic: no data is displayed when change device in realtime mode.

Reports

Bug ID	Description
1038438	Error in log when running "Secure SD-WAN Report" if "Generate separate report per-device/VDOM" is enabled.

Common Vulnerabilities and Exposures

Visit <https://fortiguard.com/psirt> for more information.

Bug ID	CVE references
1111847	FortiAnalyzer-BigData 7.4.2 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2024-32123

Known Issues

The following issues have been identified in FortiAnalyzer-BigData version 7.4.2. To inquire about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

Common

Bug ID	Description
1035817	Upload file in upgrade process is interrupted and cannot be resumed if GUI is switched.
1088938	fazbd-log-export push failing to push to sftp / scp server.
1090630	The "Date"/"Logs/Sec" and the items are not aligned in the alert details.

FortiView

Bug ID	Description
925815	No data is returned and error in log if add two "Threat Level" filters for "Top Threats".
941638	The "Threat Count" is always 0 in the IOC rescan task and no entry in rescan task drill down for FortiMail > Email filter.
1031177	No data is shown for "Threat Map" if you select historical time filter.
1076266	The "Detect Pattern" is wrong for some URLs in "Indicators of Compromise".

LogView

Bug ID	Description
1086967	Missing "count total button" when <i>Log View</i> search result is less than search limit.
1089054	Log View > realtime download fail.
1090993	Log View > Custom View > Action and Source become empty after moving any columns.

Reports

Bug ID	Description
1090172	<i>Report Calendar</i> GUI issue cause clickable text box overlap.

FortiAnalyzer-BigData-4500G limitations

The following commands are altered or removed from FortiAnalyzer-BigData 4500G appliance:

- `config system interface`
- `config system route`
- `config system docker`
- `execute reset`
- `diagnose system interface`
- `diagnose system print interface`

FortiAnalyzer-BigData 4500G does not support log aggregation.



www.fortinet.com

Copyright© 2026 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.