

# Release Notes

## FortiAnalyzer-BigData 7.2.7



**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](mailto:techdoc@fortinet.com)



June 02, 2026

FortiAnalyzer-BigData 7.2.7 Release Notes

58-727-1011999-20260602

# TABLE OF CONTENTS

<b>Change Log</b> .....	<b>4</b>
<b>FortiAnalyzer-BigData version 7.2.7</b> .....	<b>5</b>
Supported models .....	5
New features and enhancements .....	5
<b>Special Notices</b> .....	<b>6</b>
Issue when applying a filter in Log View .....	6
Chart Builder issues in FortiAnalyzer-BigData .....	6
Ports .....	7
Log Files .....	7
<b>Product Integration and Support</b> .....	<b>8</b>
<b>Firmware Upgrade Paths</b> .....	<b>9</b>
Fortinet Security Fabric .....	9
<b>Resolved Issues</b> .....	<b>10</b>
Common Vulnerabilities and Exposures .....	11
<b>Known Issues</b> .....	<b>12</b>
<b>FortiAnalyzer-BigData-4500G limitations</b> .....	<b>14</b>

# Change Log

Date	Change Description
2024-04-10	Initial release.
2024-04-11	Updated <a href="#">Known Issues on page 12</a> .
2024-05-09	Added "Issue when applying a filter in Log View" to <a href="#">Special Notices on page 6</a> .
2024-11-14	Updated <a href="#">Resolved Issues on page 10</a> .
2025-01-21	Removed reference to FortiAnalyzer-BigData-VM.
2026-06-02	Updated <a href="#">FortiAnalyzer-BigData-4500G limitations on page 14</a> .

# FortiAnalyzer-BigData version 7.2.7

This document provides information about FortiAnalyzer-BigData version 7.2.7 build 0659.

FortiAnalyzer-BigData 7.2.7 also supports features in FortiAnalyzer 7.2.5. For more information about FortiAnalyzer features, see the [FortiAnalyzer documentation](#).



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 7.2.7 supports the following models:

<b>FortiAnalyzer-BigData</b>	FAZBD-4500F, FAZBD-4500G
------------------------------	--------------------------

## New features and enhancements

For more information about what's new in FortiAnalyzer-BigData and supported by FortiAnalyzer-BigData 7.2.7, see the [FortiAnalyzer 7.2 New Features Guide](#).

# Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer-BigData version 7.2.7.

## Issue when applying a filter in Log View

When using *Log View* in FortiAnalyzer-BigData 7.2.7 build 0659, applying a filter using a number value, such as *srcport*, *dstport*, or *avcount*, may cause the pane to gray out. To avoid this issue, use FortiAnalyzer-BigData build 8014 instead.

## Chart Builder issues in FortiAnalyzer-BigData

The following issues are present in *Chart Builder* for FortiAnalyzer-BigData 7.2.7, but not in regular FortiAnalyzer:

Bug ID	Description
653736	<i>Order By</i> does not work in <i>Tools &gt; Chart Builder</i> .
928222	The <i>Preview</i> in <i>Chart Builder</i> displays <code>sql</code> error when using the following settings: <ul style="list-style-type: none"><li>• <i>Columns</i> include <i>Date/Time</i> and <i>Application</i></li><li>• <i>Group By</i> = <i>Application</i></li></ul>
981966	Error occurs when <i>Chart Builder</i> in <i>LogView &gt; Syslog</i> .
1013368	<i>Preview</i> is always loading when <i>Chart Builder</i> for <i>Hyperscale</i> .

The following issues are present in *Chart Builder* for both FortiAnalyzer-BigData 7.2.7 and regular FortiAnalyzer:

Bug ID	Description
781210	When some filter is applied, the <i>preview</i> in <i>Chart Builder</i> always shows empty data and cannot create the charts.
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.

Bug ID	Description
927959	No query statement in <i>Chart Builder</i> when <i>Log View</i> displayed with more than the default columns.
1005887	<i>AnalysisException</i> occurred when using <i>Chart Builder</i> in <i>Log View</i> if select <i>Source Object</i> or <i>Destination Object</i> .

## 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 7.2.7 support of other Fortinet products is the same as FortiAnalyzer 7.2.5. For details, see the [FortiAnalyzer 7.2.5 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 7.0.0 or later to FortiAnalyzer 7.2.7.

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 6.4 or 7.0, see the corresponding FortiAnalyzer Upgrade Guide.

Initial Version	Upgrade to	Log Database Rebuild
7.2.0 or later	To 7.2.7	No
7.0.0 or later	Latest 7.0 version, then to 7.2.7	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 7.2.7. To inquire about a particular bug, please contact [Customer Service & Support](#).

## Cluster Manager

Bug ID	Description
990762	Assign role failed due to timeout.
1006325	Assign role failed with Syntax Error.

## Common

Bug ID	Description
922340	Scale-out: The full configuration sync of the HA Cluster in a scale-out setting will overwrite the hidden user.
1008522	DNS settings does not sync from FortiAnalyzer blade down to the other blades.
1018759	Can't open the unauthorized window from FortiGate if the connected FortiAnalyzer-BigData is 4500G.

## FortiView

Bug ID	Description
794662	The values for some columns are displayed incorrect for <i>Monitors &gt; SD-WAN Events</i> .
941645	No data is returned when drill down from <i>Compromised Hosts</i> for <i>FML &gt; Emailfilter</i> .
1003601	No data is shown and error, "Facet not found:", in log when query some <i>FortiView</i> .
1014783	<i>FortiView</i> drill down Top sources or destinations keeps spinning with no outcome.

## LogView

Bug ID	Description
904122	Some fields value can't be shown in log details.
941126	Logdetail - threatcnts,threatlvl,threats,threattyps,threatwgts display with braces.

Bug ID	Description
949244	No archive file link on LogView > FortiGate > Security > Application Control.
962256	"Could not resolve column/field reference: devgrps" is shown in <i>Chart Builder</i> if select device group as filter.
968058	When using "Last N ..." filter, the "N" value is changing to the previous value while the search is performed.
977741	CSV export N days problem.
981057	Normal FortiAnalyzer logs and hyperscale logs of FG-4800F in <i>Log View</i> .
1003267	Hyperscale logs from FG-4401F sent to FortiAnalyzer.
1012910	<i>Last X &lt;time unit&gt;</i> does not update time interval upon a query refresh or new query filter.
1012954	<i>Log View</i> presents wrong results or no result at all (No record found).

## Reports

Bug ID	Description
965151	execute sql-report list <adom> empty result.
973037	Encountered: TIMESTAMP\nExpected: DEFAULT, IDENTIFIER\n\nCAUSED BY: Exception: Syntax error\n", "code": 2 when run report.
1009776	The hash ids for the report are different from that in "Retrieve Diagnostic" file.
1017149	Error is in log if add subnets in report settings for report <i>Situation Awareness Report</i> .

## System Setting

Bug ID	Description
885429	Logging Topology: Right click the device redirects to wrong type device in <i>Log View</i> .

# Common Vulnerabilities and Exposures

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

Bug ID	CVE references
1028283	FortiAnalyzer-BigData 7.2.7 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"> <li>CVE-2024-23666</li> </ul>

# Known Issues

The following issues have been identified in FortiAnalyzer-BigData version 7.2.7. To inquire about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

## Common

Bug ID	Description
938308	Upgrade: Error is shown when upgrade by <i>Upload File</i> method.
1011102	FortiAnalyzer-BigData upgrade fails if upgrade filename has special characters.
1019337	Improvement about authorizing hyperscale devices.

## Device Manager

Bug ID	Description
1017120	The newly added device won't automatically appear in the list.

## FortiSoC

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

## FortiView

Bug ID	Description
925815	No data is returned and error in log if add two <i>Threat Level</i> filters for <i>Top Threats</i> .
941638	The <i>Threat Count</i> is always 0 in the IOC rescan task and no entry in rescan task drill down for <i>FML &gt; Emailfilter</i> .
1004908	<i>FortiView</i> : The page is always loading and error in log when jump to <i>Session</i> if select more csf devices.
1005562	<i>Log View</i> : <i>Source Object</i> and <i>Destination Object</i> are always empty in <i>Log View</i> for <i>Traffic</i> .

## LogView

Bug ID	Description
1010465	Log import: logs duplicates and some of them missing after importing from GUI.
1013888	The new added column are empty in <i>Custom View</i> .
1019444	<i>Log View &gt; FortiGate &gt; Traffic</i> : "no record found" is shown after changing the position of columns.
1019473	<i>Log View &gt; FortiGate &gt; Security &gt; Application Control</i> : the page becomes grey when searching while switching filter mode.
1019499	<i>Log View &gt; Any event like FortiGate &gt; Traffic</i> : no data is shown after add or delete a column.

# 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](http://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.