FORTINET

Release Notes

FortiAnalyzer-BigData 7.2.8

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

March 11, 2025
FortiAnalyzer-BigData 7.2.8 Release Notes
58-728-1066414-20250311

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-08-28	Initial release.
2024-11-14	Updated Resolved Issues on page 10.
2025-01-21	Removed reference to FortiAnalyzer-BigData-VM.
2025-02-11	Updated Resolved Issues on page 10.
2025-03-11	Updated Resolved Issues on page 10.

FortiAnalyzer-BigData version 7.2.8

This document provides information about FortiAnalyzer-BigData version 7.2.8 build 0674.

FortiAnalyzer-BigData 7.2.8 also supports features in FortiAnalyzer 7.2.7. 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 7.2.8 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 7.2.8, 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 7.2.8.

Chart Builder issues in FortiAnalyzer-BigData

The following issues are present in *Chart Builder* for FortiAnalyzer-BigData 7.2.8, but not in regular FortiAnalyzer:

Bug ID	Description
653736	*Order By* does not work in *Tools* > *Chart Builder*.
928222	The *Preview* in *Chart Builder* displays `sql error` when using the following settings: • *Columns* include *Date/Time* and *Application* • *Group By* = *Application*
981966	Error occurs when *Chart Builder* in *LogView* > *Syslog*.
1013368	Preview is always loading when *Chart Builder* for *Hyperscale*.

The following issues are present in *Chart Builder* for both FortiAnalyzer-BigData 7.2.8 and regular FortiAnalyzer:

Bug ID	Description
781210	When some filter is applied, the preview in *Chart Builder* always shows empty data and cannot create the charts.
888280	The *Preview* in *Chart Builder* displays the error "`Device not exist`" when device groups or log groups are selected in the device filter for *Log View*.
896553	The *Preview* in *Chart Builder* displays an error message when selecting *Device* for traffic.
927959	No query statement in *Chart Builder* when *Log View* displayed with more than the default columns.

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 7.2.8 support of other Fortinet products is the same as FortiAnalyzer 7.2.7. For details, see the FortiAnalyzer 7.2.7 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

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	7.2.8	No
7.0.0 or later	Latest 7.0 version, then to 7.2.8	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-BigDataupgrade. 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 7.2.8. To inquire about a particular bug, please contact Customer Service & Support.

Common

Bug ID	Description
938308	Error is shown when upgrade by "Upload File" method.
1011102	FortiAnalyzer-BigData upgrade fails if upgrade filename has special characters.

FortiSoC

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

FortiView

Bug ID	Description
1004908	The page is always loading and error in log when jumping to "Session" if select more CSF devices.
1056712	Secure SD-WAN Monitor only shows first 50 devices.

LogView

Bug ID	Description
1005562	"Source Object" and "Destination Object" are always empty in Log View for Traffic.
1013888	The newly added columns are empty in "Custom View".
1019444	Logview > FortiGate > Traffic > "no record found" is shown after changing the position of columns.
1019499	Log View > Any event such as FortiGate > Traffic > no data is shown after adding or deleting a column.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
1025021	FortiAnalyzer-BigData 7.2.8 is no longer vulnerable to the following CVE Reference: • CVE-2024-32117
1025025	FortiAnalyzer-BigData 7.2.8 is no longer vulnerable to the following CVE Reference: • CVE-2024-31496
1025026	FortiAnalyzer-BigData 7.2.8 is no longer vulnerable to the following CVE Reference: • CVE-2024-32118
1025029	FortiAnalyzer-BigData 7.2.8 is no longer vulnerable to the following CVE Reference: • CVE-2024-32116
1045351	FortiAnalyzer-BigData 7.2.8 is no longer vulnerable to the following CVE Reference: • CVE-2024-40584
1111847	FortiAnalyzer-BigData 7.2.8 is no longer vulnerable to the following CVE Reference: • CVE-2024-32123

Known Issues

The following issues have been identified in FortiAnalyzer-BigData version 7.2.8. 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.

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.
1068370	Sometimes "Failed loading data" for the device filter dropdown list for "Secure SD-WAN Monitor".

LogView

Bug ID	Description
1010465	Log View > Log import: logs duplicates and some of them missing after importing from GUI.
1027925	Log View > Traffic > filter search > searching keeps going on backend after the time counting stops.
1036317	LogView > All log types (such as FortiGate) > Traffic > no data is displayed when change device in realtime mode.
1062015	LogView > all devices are displayed when choosing an empty device group (different action from regular FortiAnalyzer).

Reports

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

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`

www.fortinet.com