FORTINET

Release Notes

FortiAnalyzer-BigData 7.2.11

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

November 05, 2025
FortiAnalyzer-BigData 7.2.11 Release Notes
58-7211-1215331-20251105

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-11-05	Initial release.

FortiAnalyzer-BigData version 7.2.11

This document provides information about FortiAnalyzer-BigData version 7.2.11 build 0702.

FortiAnalyzer-BigData 7.2.11 also supports features in FortiAnalyzer 7.2.11. 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 7.2.11 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 7.2.11, 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 7.2.11.

Chart Builder issues in FortiAnalyzer-BigData

The following issues are present in *Chart Builder* for FortiAnalyzer-BigData 7.2.11, 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*

The following issues are present in *Chart Builder* for both FortiAnalyzer-BigData 7.2.11 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 7.2.11 support of other Fortinet products is the same as FortiAnalyzer 7.2.11. For details, see the FortiAnalyzer 7.2.11 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. 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	7.2.11	No
7.0.0 or later	Latest 7.0 version, then to 7.2.11	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 7.2.11. To inquire about a particular bug, please contact Customer Service & Support.

Common

Bug ID	Description
1097487	Admin session list tracks one source IP for multiple admin logins, causing user login failures.
1142125	*System Settings* > *Network* > create an interface with name of "`port1`" and a wrong ip address and GUI is down.
1145144	All facets are missing in BD side.
1166069	Upgrade failed due to "Failed to backup metastore".
1173804	Add more device platform for Hyperscale logs.
1178699	*Log View* randomly shows empty output and GUI shows errors `Internal Server Error / OutOfMemoryError`.
1182668	Improve error message when entering some modules from "main host" IP.
1215449	Setup failed for "start all services".
1218590	When Encryption is Enable, the login UI opens too early when upgrading is only finished 50%.

FortiView

Bug ID	Description
925815	No data is returned and error in log if adding two "Threat Level" filters for "Top Threats".
1076266	The "Detect Pattern" is wrong for some URLs for "Indicator of Compromise".
1095545	No data is shown and error in log when query *FortiView* after changing the System time zone.

LogView

Bug ID	Description
1144565	*Log View* > FortiGate (all types) > "null" should be counted in when the search condition is "not like XXX* "
1173438	*Log View* > *FortiGate* > *Security:DLP* > no Archive icons are displayed for the entries with Archive.
1187114	Missing "selectColums" in FAZ/LogView/Fortinet Logs/FortiFirewall/Hyperscale request.
1218444	*Log View* > *FortiAnalyzer* > *Application Control* > `faz_app_ctrl` is not a valid `Log Type` error occurs in backend.

Reports

Bug ID	Description
930841	Error is shown when validate or test dataset "apprisk-Malware-Total-Count".
1219939	The "360 Security Report" returns error when running with extended log filter auto cache turned on.

Known Issues

The following issues have been identified in FortiAnalyzer-BigData version 7.2.11. To inquire about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Common

Bug ID	Description
1088938	fazbd-log-export push failing to push to sftp / scp server.
1101183	Health alert missing and only show in the *Cluster Manager* tab.
1162669	4500F encryption power cycle: after power on, apply recommended config failed.

FortiView

Bug ID	Description
1097106	"Failed to retrieve FortiView data" is shown on FortiGate when query "Top Endpoint Vulnerabilities" to drill down.
1145795	*FortiView* > *Compromised Hosts* > select group device > "Server error: ERROR: function find_in_set..." occured.
1222016	*FortiView* VPN sessions data showing inaccurately.

LogView

Bug ID	Description
1099963	*Log View* > some log types > blank is showing for *Total Logs* on the bottom.
1099373	*Log View* > when a group nested, if an inner group has device(s) sibling, not able to select it partially.
1010465	*Log View* > Log import > logs duplicates and some of them missing after importing from GUI.

Reports

Bug ID	Description
1222053	Endpoint chart empty when extended filtering not enabled for report "360 Security Report".

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