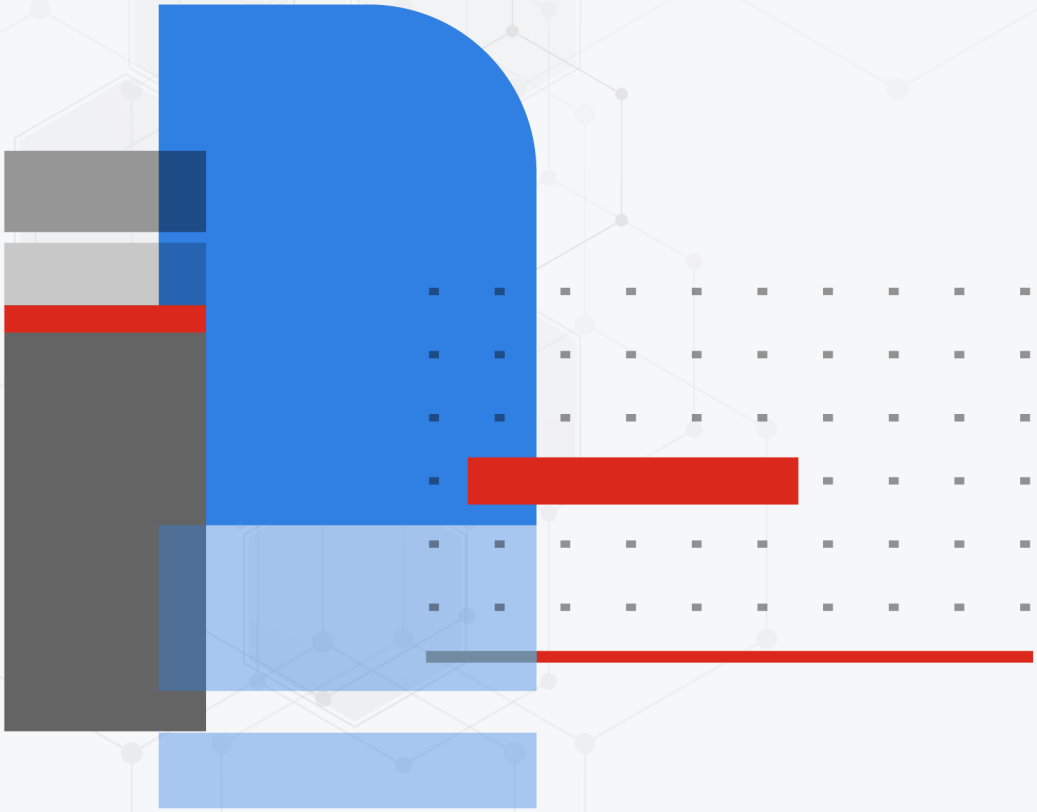
Release Notes

FortiAnalyzer-BigData 7.4.4



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

June 02, 2026
FortiAnalyzer-BigData 7.4.4 Release Notes
58-744-1173939-20260502

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-07-03	Initial release.
2025-08-08	Updated New features and enhancements on page 5.
2025-08-12	Updated Resolved Issues on page 13.
2025-09-04	Added "Prevent kudu corruption at upgrade" to Special Notices on page 8.
2025-10-15	Updated New features and enhancements on page 5.
2025-11-03	Updated New features and enhancements on page 5.
2025-12-04	Updated Known Issues on page 15.
2026-01-29	Updated New features and enhancements on page 5.
2026-06-02	Updated FortiAnalyzer-BigData-4500G limitations on page 17.

FortiAnalyzer-BigData version 7.4.4

This document provides information about FortiAnalyzer-BigData version 7.4.4 build 0959.

FortiAnalyzer-BigData 7.4.4 also supports features in FortiAnalyzer 7.4.7. For more information about FortiAnalyzer features, see the FortiAnalyzer documentation.

There are some features available in FortiAnalyzer-BigData 7.4.4 that are not available in FortiAnalyzer 7.4.7. For details, see New features and enhancements on page 5.

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 7.4.4 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 7.4.4, see the FortiAnalyzer 7.4 New Features Guide.

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 7.4.4.

Prevent kudu corruption at upgrade

Some environments may experience kudu failure immediately after upgrading FortiAnalyzer-BigData to 7.2.10, which may be in your upgrade path if you are upgrading to 7.4.4. This failure is potentially caused by auto remediation in the database health check, which occurs during the upgrade when kudu is not fully booted up.

Prior to upgrading to 7.2.10, enter the following command to disable the Repair Corrupted Tablets feature globally, preventing the job from breaking schema changes:

```
consul kv put services/bd-management-server/advanced_configuration "ansible.playbook.vars.command_
check_url=disabled"
consul kv get services/bd-management-server/advanced_configuration
kubectl rollout restart deployment/bd-management-server && kubectl rollout status deployment/bd-
management-server
kubectl rollout restart deployment/bd-management-task && kubectl rollout status deployment/bd-
management-task
```

Fabric of FortiAnalyzer requirement

To use the Fabric of FortiAnalyzer feature, you must install a special FortiAnalyzer image as a supervisor. Please contact your TAC or TAM support for more details. A GA release will be available later with this capability.

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 7.4.4, but not in regular FortiAnalyzer:

Bug ID	Description
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 7.4.4 and regular FortiAnalyzer:

Bug ID	Description
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.

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 7.4.4 support of other Fortinet products is the same as FortiAnalyzer 7.4.7. For details, see the FortiAnalyzer 7.4.7 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
```

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	7.4.4	No
7.2.0 or later	Latest 7.2 version, then to 7.4.4  FortiAnalyzer-BigData 7.2.10GA upgrade to 7.4.3GA with siem enabled may fail. See 1149063 in the FortiAnalyzer-BigData 7.4.3 Release Notes > Known Issues.	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-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 7.4.4. To inquire about a particular bug, please contact Customer Service & Support.

Common

Bug ID	Description
1094710	"Kafka Consumer Lag" keeps increasing for more ADOMs on 4500F.
1097487	Admin session list tracks one source IP for multiple admin logins, causing user login failures.
1114416	External Storage Maintenance failure.
1127751	Last result health check file naming includes one hour offset time.
1129105	DB query returns empty result after single node failure.
1129600	Improving Bootloader upgrade. Failed Kudu T-Serever could trigger bootloader upgrade to hang.
1129984	Lack of diagnostics dterminating bad disk's ID.
1130226	Setup failed when "Apply recommended configurations".
1130233	`diagnose system disk` failed on 4500F.
1137916	All the healthy check and jobs are in "Queued" Status.
1139232	Third-party component upgrade required for security reasons: tomcat to 8.5.100/9.0.99/10.1.35/11.0.3.
1139657	Setup failed for restart SIEM because of clickhouse-sinker crash.
1139658	"cluster-federation" should not be shown in Hosts list.
1144026	Setup failed due to "Unable to finish setup, it took too long to respond."
1145144	All facets are missing in bd side.
1157442	No facets are registered after resetting cluster.
1162669	4500F encryption graceful power cycle; after power on apply recommended config failed
1165112	Some pods are crash or ERROR.
1166012	4500F encryption upgrade from 7.4.3GA to 7.6.0GA, xfs_quota creation failed.
1166069	Upgrade from 7.4.3 to 7.6.0 failed due to "Failed to backup metastore".
1167528	HA: 50 mins logs lost when the extender chassis power off.

Bug ID	Description
1169080	Upgrade failed due to "Aborted syncing due to abnormally long duration. Please retry".
1173804	Add more device platform for Hyperscale logs.

FortiView

Bug ID	Description
925815	No data is returned and error in log if add two "Threat Level" filters for "Top Threats".

LogView

Bug ID	Description
1121506	Log filter devname is not applied when is used at the begginning of the log filter.

Reports

Bug ID	Description
1118546	Error in log when enabled *Extended Log Filtering* for report *Security Analysis*.
1119004	Error in bd log if enabled *Extended Log Filtering* for report *DNS Report*.
1137771	Some reports stay in "initializing" stage for a few minutes before running.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
1130330	FortiAnalyzer-BigData 7.4.4 is no longer vulnerable to the following CVE Reference: • CVE-2025-26466

Known Issues

The following issues have been identified in FortiAnalyzer-BigData version 7.4.4. To inquire about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Common

Bug ID	Description
1114171	External storage retention job failure.
1118126	FAZBD JSON API login event now showing original IP.
1121394	Some device load balance settings are lost after shut down primary faz.
1166607	No data is shown for "Endpoint Vulnerability".
1172403	4500F power cycle spark driver node, catalog server is pending.
1176053	Top right toolbar > Question Mark menu > Video Tutorials > Whitelabel Error Page.
1208417	Ingestion stopped on FAZBD after changing storage pool type from sparse to default.

Fabric of FortiAnalyzer

Bug ID	Description
1113582	The performance issue for *Log View* and *FortiView*.
1118020	High CPU usage on BD member when query *Log View*/*FortiView*/*Report* on Supervisor.
1119962	The values of line chart Y-axis between supervisor and member are different for *FortiView*.

FortiView

Bug ID	Description
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*.
1117068	No data is returned for "Top Cloud Users" > "Video" > drill down to *Log View*.

LogView

Bug ID	Description
1125039	*Log View* >FortiGate > "Custom View" is related to parent log view configuration.
1176209	*Log View* > FortiCASB > Session ID > Internal error.
1176419	FortiFirewall of *Log View* display error"Internal Error" when turn to Security:Intrusion Prevention.
1176692	"No Device Selected" for the device filter when query Hyperscale in FortiFirewall ADOM.
1176696	The *Log View* menu should be FortiFirewall if there is only Hyperscale logs for FortiFirewall.
1176703	No device in *Device* dropdown for FortiFirewall/FortiFirewallCarrier in Fabric ADOM if only Hyperscale.

Reports

Bug ID	Description
1104840	Query error when run built-in report of *What is New Report* for specific device.

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