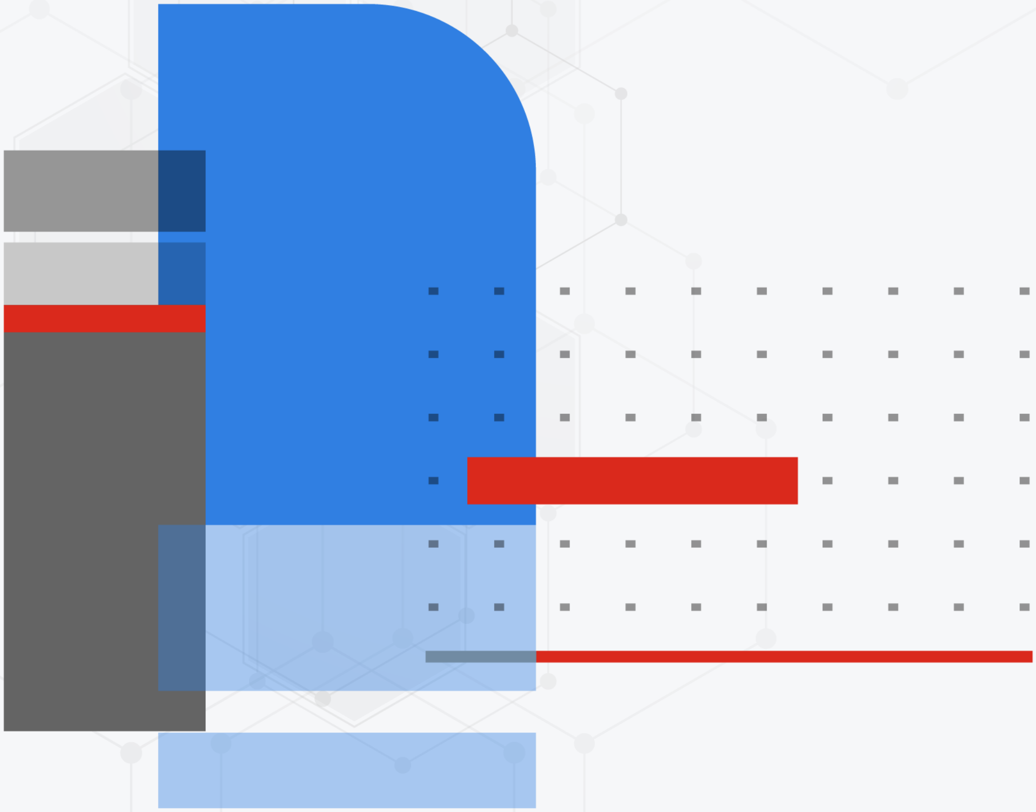
Release Notes

FortiAIOps 3.2.1



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
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/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

Feb 23, 2026
FortiAIOps 3.2.1 Release Notes
83-1250262-321-20260223

TABLE OF CONTENTS

Change log

Date	Change description
2026-02-23	FortiAIOps version 3.2.1 version.

About FortiAIOps 3.2.1

This release enables support for the FAO-100G hardware platform and adds data export capabilities to the Impacted SLA window. This update also delivers key performance optimizations and stability improvements for a smoother experience. For more information, see What's New.

FortiAIOps 3.2.1 expands upon the robust capabilities established in version 3.2.0. For a comprehensive list of features from the previous release, see FortiAIOps Documentation Library.

Notes:

- Upgrade to the current release is supported only from version 2.0.0/2.0.1/2.0.2/2.1.0/3.0.0/3.0.1/3.2.0.
- The FortiAIOps subscription-based annual license is available as per the number of devices, and supports the following.
  - Monitoring
  - Monitoring and AI Insights
  - SD-WAN

Overview

FortiAIOps enables you to proactively monitor the health of your entire wireless, wired, and SD-WAN network, and provides insights into key health statistics, based on the Artificial Intelligence (AI) and Machine Learning (ML) architecture that it is built upon. FortiAIOps ingests data for analysis and automated event correlation to precisely detect anomalies that impact the clients' network experience. It learns from numerous sources such as FortiGates, FortiAPs, FortiSwitches, and FortiExtenders to report statistics on a series of comprehensive and simple dashboards, providing visibility and deep insight into your network. This predictable network infrastructure enables you to swiftly identify the root cause with the highest probability of association to actual issues, and its resolution.

Supported Hardware and Software

The following are the hardware and software requirements for FortiAIOps.

- Software requirements
- Hardware requirements
- FortiAIOps 500G (FAO-500G)
- FortiAIOps 100G (FAO-100G)
- Supported web browsers

Software requirements

The following versions are supported with this release of FortiAIOps.

Software	Supported Versions
FortiOS	• 7.6.0 and above • 7.4.0 and above • 7.2.0 and above • 7.0.6 and above
FortiWiFi	All devices with FortiOS version 7.0 and above.
FortiSwitchOS	• 7.0.x and above
Access Points	• FortiAP 6.4.x and above • FortiAP-U 6.2.4 and above
FortiExtender	• 7.2.2 and above

Hardware requirements

The following are the recommended resource requirements for FortiAIOps on VM platforms.

Maximum device count	Recommended Hardware	Supported Mode
• FortiGates - 30 • FortiSwitches - 90 • FortiExtenders - 30 • FortiAPs - 180 • Clients - 3000	• CPU - 8 • Memory - 32 GB • Storage - 1 TB	AI Insights and Monitoring
• FortiGates - 200 • FortiSwitches - 600 • FortiExtenders - 200 • FortiAPs - 1200 • Clients - 10000	• CPU - 4 • Memory - 32 GB • Storage - 1 TB	Monitoring only

Maximum device count	Recommended Hardware	Supported Mode
• FortiGates - 1000 • FortiSwitches - 3000 • FortiExtenders - 1000 • FortiAPs - 6000 • Clients - 25000	• CPU - 40 • Memory - 128 GB • Storage - 4 TB	AI Insights and Monitoring
• FortiGates - 2500 • FortiSwitches - 7500 • FortiExtenders - 2500 • FortiAPs - 15000 • Clients - 60000	• CPU - 24 • Memory - 128 GB • Storage - 4 TB	Monitoring only
• FortiGates - 5000 • FortiSwitches - 15000 • FortiExtenders - 5000 • FortiAPs - 30000 • Clients - 100000	• CPU - 104 • Memory - 256 GB • Storage - 8 TB	AI Insights and Monitoring

FortiAIOps 500G (FAO-500G)

The following are the maximum devices supported in FortiAIOps 500G hardware.

Maximum device count	Supported Mode
• FortiGates - 1000 • FortiSwitches - 3000 • FortiExtenders - 1000 • FortiAPs - 6000 • Clients - 25000	AI Insights and Monitoring
• FortiGates - 2500 • FortiSwitches - 7500 • FortiExtenders - 2500 • FortiAPs - 15000 • Clients - 60000	Monitoring only

FortiAIOps supports RAID levels *0*, *1*, *5*, and *10*. The default configuration uses RAID 5 for HDDs and RAID 1 for SSDs. The following are the storage capacities for RAID levels in the default and maximum FortiAIOps 500G hardware configurations.

RAID Level	FortiAIOps 500G Hardware Configuration	
	Default (4 HDDs, 2 SSDs)	Maximum (8 HDDs, 4 SSDs)
RAID 0	18 TB	36 TB

RAID Level	FortiAIOps 500G Hardware Configuration	
	Default (4 HDDs, 2 SSDs)	Maximum (8 HDDs, 4 SSDs)
RAID 1	9.0 TB	18 TB
RAID 5	13 TB	31 TB
RAID 10	9.0 TB	18 TB

FortiAIOps 100G (FAO-100G)

The following are the maximum devices supported in FortiAIOps 100G hardware.

Maximum device count	Supported Mode
• FortiGates - 30 • FortiSwitches - 90 • FortiExtenders - 30 • FortiAPs - 180 • Clients - 3000	AI Insights and Monitoring
• FortiGates - 200 • FortiSwitches - 600 • FortiExtenders - 200 • FortiAPs - 1200 • Clients - 10000	Monitoring only

Supported web browsers

The following web browsers are tested to access the FortiAIOps GUI.

Web Browser	Version
Google Chrome	137.0.7151.120
Mozilla Firefox	139.0.4
Microsoft Edge	137.0.3296.83
Safari	18.5 (20621.2.5.11.8)

What's New

This release of FortiAIOps 3.2.1 delivers the following new features.

Feature	Description
FAO-100G Hardware Platform Support	You can now deploy FortiAIOps on the FAO-100G platform. For detailed instructions on deployment and configuration, see the *FortiAIOps User Guide* for release 3.2.1.
Export Impacted SLA Data	FortiAIOps now supports exporting tabular data directly from the **AI Insights** > **Impacted SLA** window. You can save this data in multiple formats, including CSV, JSON, Plaintext, and PDF.

Recommendations and Special Notes

Recommendations

Fortinet ***recommends*** the following versions and configurations to use with FortiAIOps.

Product	Recommendation
FortiAP	• FortiAP (FAP) version 7.2.2 and above is recommended to generate all events in FortiAIOps.
FortiOS	• FortiOS version 7.2.4, 7.4.0, 7.6.0 or higher is recommended to generate all events in FortiAIOps.
FortiGate	• [FortiGate/FortiAnalyzer] Configure the FortiAIOps IP address in the FortiGate syslog or FortiAnalyzer to send events to FortiAIOps. • Ensure that you enable the detection of interfering SSIDs in FortiGate to allow reporting of *Throughput* SLA - interference issues in FortiAIOps. To detect interfering SSIDs in FortiGate, configure the FortiAP profile to use *Radio Resource Provisioning* or a *WIDS* profile with AP scan enabled. • SD-WAN Network Monitor license must be installed on the FortiGate to measure the estimated bandwidth accurately. • Configure the *sla-fail* and *sla-pass* log failure period, the recommended duration is 60 seconds for enhanced accuracy. • When the backup file is restored on a different machine, reconfigure the FortiAIOps IP address in the FortiGate syslog settings.
FortiAIOps 500G (FAO-500G)	• For a fresh configuration, completely erase all existing configurations from the hard disks. A factory reset is recommended to ensure all configurations are removed. • Back up your configuration data before RAID rebuild and migration operations, as these processes are susceptible to errors. • The 10 Gbps port does not support 1 Gbps data speeds. • RAID rebuild and migration operations cannot be performed concurrently. However, simultaneous rebuild operations are supported for SSDs and HDDs. • The system supports the failure of only one HDD and one SSD at a time. Simultaneous failures of multiple HDDs or

Product	Recommendation
	SSDs may lead to data loss.
Others	The FortiAIOps time and timezone should be synchronized with the NTP server.

Special Notes

AI-ARRP

AI-ARRP is only supported on FortiOS 7.6.5 or above, and FortiAP version 7.6.3.

SD-WAN

- Upon upgrading to the current release, the baseline configuration mode is automatically set to Dynamic.
- Interfaces that were impacted prior to the upgrade will not be visible post-upgrade. However, new impacts detected after the upgrade will display correctly.
- An SD-WAN license is required to view forecast and monitoring data, and an Analytics license is necessary to access SD-WAN Insights.

Service Assurance Manager (SAM)

- SAM is currently supported on F-series, G-series, and K-series FortiAPs using Bridge mode SSIDs with WPA2 PSK security only.
- Only Radio 1 (2.4 GHz) and Radio 2 (5 GHz) are supported for SAM operations.
- SAM test results are not displayed in the baseline view (details or trends) after a restore operation.

Backup and Restore

- Backup and restore is supported for version 2.0.0 and later. Migrating from version 1.x is not supported.
- The backup and restore function is supported only for FortiAIOps configuration. CLI configurations are saved using the execute backup config command and it does not include any FortiAIOps specific configurations.
- The Import option is not available for FortiGates deployed in High Availability (HA) mode.

Monitoring and SLAs

- To correctly detect STP and DHCP failures, ensure that L2 security features (BPDU Guard, Loop Guard, DHCP Snooping, Root Guard) are enabled on the switch ports.
- The "Time to Connect" and "Connection Failure" SLAs do not currently support WPA3 SAE or Enterprise modes.
- For FortiGate clusters, FortiAP and FortiSwitch events/logs may be displayed for both the primary and secondary units.
- When a FortiGate is deleted and added in a new ADOM, the AI-Insights data is still displayed in the older device group, only for the time period during which the device was part of that group.

Monitoring Dashboards

- The donut charts on the monitoring dashboards do not display correctly on smaller screens or when the browser window is resized. This issue impacts multiple Monitor pages (such as Managed FortiGate, Wireless Clients, Access Points, and others).
- All donut charts initially display `Refresh to Load Data` message after a page is reloaded.

System and Compatibility

- FortiAnalyzer version 7.4.1 is not supported due to an incorrect log format.

Common Vulnerabilities and Exposures

Visit https://www.fortiguard.com/psirt for information about vulnerabilities.

Known Issues

The following are known issues in FortiAIOps version 3.2.1. For inquiries about a particular issue, contact *Customer Support*.

Issue ID	Description
1230970	The location displayed for wireless clients on the floor map may not match their actual physical position.
1233982	**Diagnostics and Tools** window shows `No Data` for offline clients when accessed using the **Locate** feature (map view) for custom time ranges. **Workaround** Access the client details directly from the **Wireless Clients** page to view the data.
1229404	AI-ARRP channel validation does not account for neighbor AP RSSI, assigning the same channel to neighboring Access Points resulting in co-channel interference and reduced wireless performance.
1226216	AI-ARRP channel validation does not account for Neighbor AP channel bandwidth. When channel bonding is enabled, the system may assign channels that overlap with neighboring devices.

914708	Background scans on G-series and K-series FortiAPs do not correctly refresh DARRP data. The scanned AP list displays outdated information, and the system fails to detect when neighboring Access Points switch channels.
	Workaround
	For regular DARRP to work properly, you can enable ddscan. Following is a sample code:
	`edit "FAP231G-default"`
	`   config platform`
	`      set type 231G`
	`      set ddscan enable`
	`   end`

www.fortinet.com

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 General Counsel, 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.