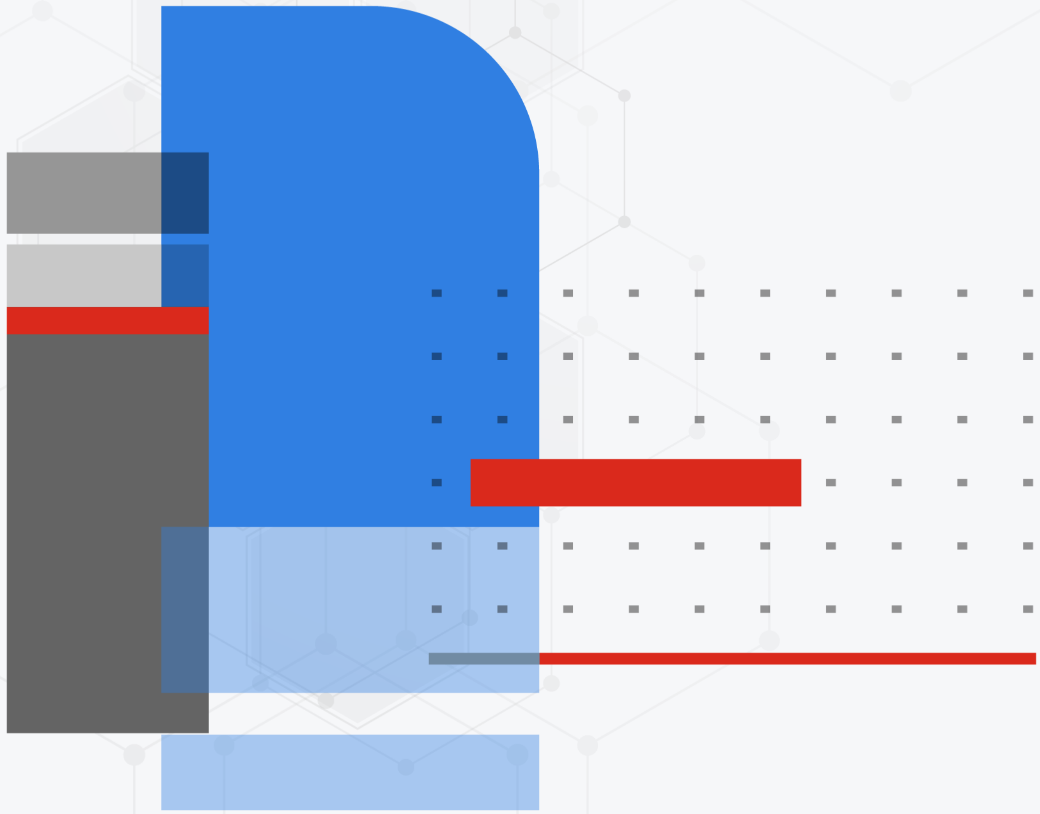
FORTINET

Release Notes

FortiAIOps 3.0.1



Aug 20, 2025
FortiAIOps 3.0.1 Release Notes
83-1187328-301-20250820

TABLE OF CONTENTS

Change log

Date	Change description
2025-08-20	FortiAIOps version 3.0.1 version.

About FortiAIOps 3.0.1

In this release, FortiAIOps resolves a few key issues. For more information, see Fixed Issues.

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.
- 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)
- Supported web browsers

Software requirements

The following versions are supported with this release of FortiAIOps.

Software	Supported Versions
FortiOS	• 7.0.6 and above • 7.2.0 and above • 7.4.0 and above • 7.6.0 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
• FortiGates - 1000	• CPU - 40	AI Insights and Monitoring

Maximum device count	Recommended Hardware	Supported Mode
• FortiSwitches - 3000 • FortiExtenders - 1000 • FortiAPs - 6000 • Clients - 25000	• Memory - 128 GB • Storage - 4 TB	
• 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 1	9.0 TB	18 TB

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

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)

Recommendations and Special Notes

- Recommendations
- 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 and above, 7.4.0, or 7.6.0 are 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

Note the following when using FortiAIOps.

- [SD-WAN] Upgrade to the current release sets the baseline configuration mode to dynamic, by default.
- [SD-WAN] Interfaces that were impacted before the upgrade will not be visible after the upgrade. However, any new impacts detected after the upgrade will be shown properly.
- [SD-WAN] SD-WAN license is required to view SD-WAN forecast and monitoring data, and Analytics license is necessary to view SD-WAN insights.
- [Switching] Ensure that all L2 security features, such as, BPDU guard, loop guard, DHCP snooping, root guard are enabled on the switch port to detect STP and DHCP failures.
- FortiAP and FortiSwitch events/logs are displayed randomly for both primary and secondary FortiGates in a cluster.
- When a FortiGate is deleted and added in a new device group, 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.
- This release supports the backup and restore function 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 HA mode.
- SAM works with F-series, G-series, and K-series FAPs, bridge mode SSIDs, and WPA2 PSK security mode only.
- Currently only radio1 (2.4GHz) and radio 2 (5GHz) are supported for SAM operations.
- SAM test results are not displayed in the baseline view details/trends page after the restore operation.
- FortiAnalyzer version 7.4.1 is not supported due to an incorrect log format.
- Time to Connect and Connection Failure SLA - WPA3 SAE and Enterprise modes are not supported.
- The backup and restore operation is supported from version 2.0.0. This operation is not supported from 1.x version.

Common Vulnerabilities and Exposures

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

Fixed Issues

This release of FortiAIOps resolves the issues described in this section.

Issue ID	Description
1177770	The **Dynamically Obtained Baselines Values** under **AI Insights** > **Wireless** > **Roaming** tab is not displayed even when the **Dynamic Baselines Configuration** is set up.
1005585	When the SMTP server is configured to receive reports by email, the reports are not delivered, and their delivery status is not captured in the `report.log` file.

www.fortinet.com