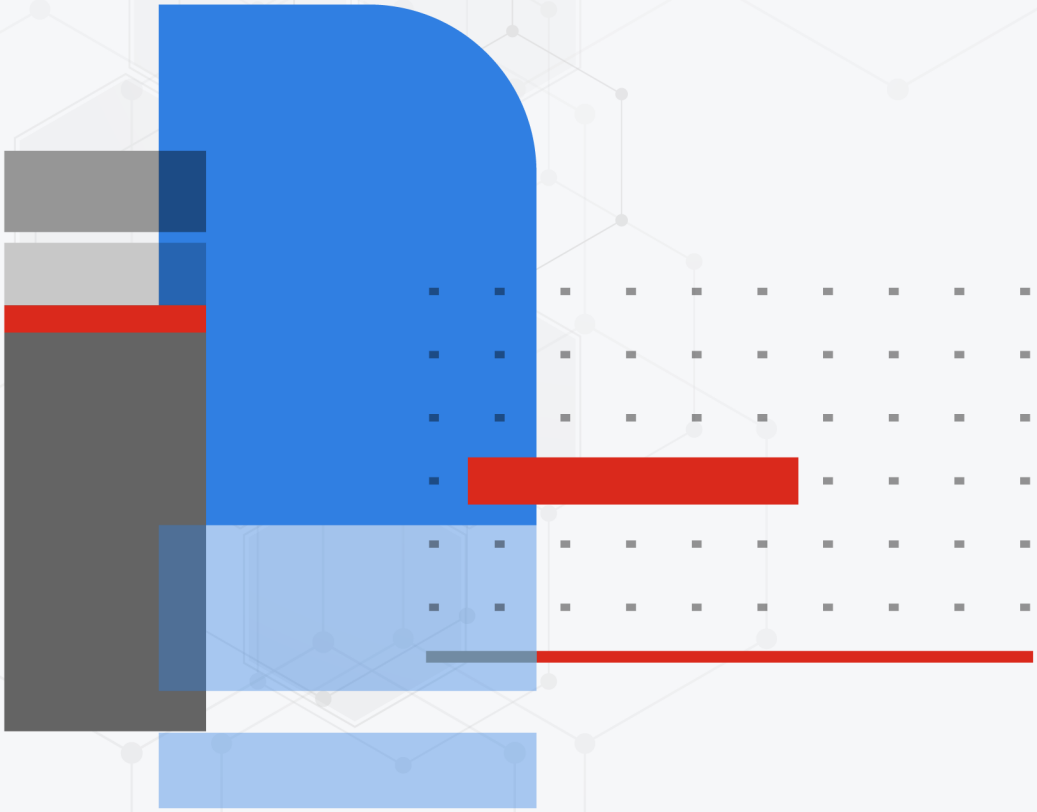
Release Notes

FortiAIOps 3.0.0



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

July 01, 2025
FortiAIOps 3.0.0 Release Notes
83-1171399-300-20250701

TABLE OF CONTENTS

Change log

Date	Change description
2025-07-01	FortiAIOps version 3.0.0 version.

About FortiAIOps 3.0.0

In this release, FortiAIOps delivers enhanced AI insights into your network and resolves key issues and vulnerabilities. For more information, see What's New, Common Vulnerabilities and Exposures and 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.
- The FortiAIOps subscription-based annual license is available as per the number of devices, and supports the following.
  - Monitoring
  - AI Insights
  - 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

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)

What's New

This release of FortiAIOps 3.0.0 delivers the following new features.

Feature	Description
FortiAI: Intelligent Network Assistance	This release introduces FortiAI, a generative AI assistant integrated into FortiAIOps. FortiAI simplifies network management by converting natural language questions into actionable intelligence, offering real-time diagnostics, performance monitoring, troubleshooting, and step-by-step configuration help across your wireless, wired, and SD-WAN environments. Its powerful AI/ML engine analyzes data from FortiGates, FortiAPs, and FortiSwitches to diagnose issues, identify root causes, and suggest clear remedies. FortiAI continuously recalculates performance baselines and SLA thresholds for precise anomaly detection, helping identify network slowdowns and bottlenecks to maximize uptime. Responses are now delivered in multiple formats, including tabular data and plain text, with information pulled directly from your FortiAIOps environment. **Note**: In this release, FortiAI is available to all customers as a **Beta** feature and includes a grant of 5 million tokens for use.
Customized Dashboards	FortiAIOps now enables you to create personalized dashboards, giving you the flexibility to customize your monitoring experience. You can now modify existing layouts by adding or deleting widgets, or create entirely new dashboards with your preferred widgets.
WIDS Security Analytics	This release introduces WIDS SLA, to monitor and report on potential Wireless Intrusion Detection System (WIDS) attempts across your network. It detects security threats and recommends corrective actions to maintain network integrity, ultimately enhancing security with real-time alerts and actionable insights for faster threat resolution.
SD-WAN SLA Enhancements	The SD-WAN SLA monitoring is now enhanced by introducing new sub-classifiers. The real-time FortiGate data is now used to provide deeper, more precise insights into critical performance and interface health issues. This allows for more targeted identification and resolution of problems, ultimately improving the network reliability and efficiency.
SD-WAN Monitoring and Insights	FortiAIOps now enables interface monitoring for SD-WAN devices. The following widgets in the SD-WAN dashboard (Dashboard > SD-WAN) provides a summarized view across multiple FortiGate devices: • FortiGates • SD-WAN Health Overview • SD-WAN Events • SD-WAN Insights • Top SLA Issues

Feature	Description
	• Top Talkers • Top Applications The following widgets under the SD-WAN menu (SD-WAN > Insights) provide insights into your network's health and performance: • Bandwidth Overview • Available Bandwidth • Used Bandwidth • Performance Status • Rules Utilization • Applications Utilization • MOS Score • SLA Performance Issues
SD-WAN Events Chart	A new SD-WAN Events chart is introduced which captures the number of SD-WAN events across various severity levels within a specified time frame. The severity levels are classified as Emergency, Alert, Critical, Error, Warning, Notice, Information, and Debug.
Channel Summary	The **Channel Summary** page under the **Wireless** menu is now enhanced, offering detailed insights into your wireless network. You can now see how channels are utilized across different frequency bands, how power is being used by various radios in your access points, and channel and power change events over time represented in a bar chart.
Remote Admin Authentication	FortiAIOps now supports remote authentication. In the older releases, only local users were supported. You can now authenticate users through a remote server. To enable this, configure the appropriate remote servers within your network.
Export Table in Different Formats	FortiAIOps now allows you to export tabular data in various formats, including CSV, JSON, plain text, and PDF. You can choose to download either filtered data or all available data in your preferred format. Export option is available in the following pages: • Inventory > Managed FortiGates • Wireless > Access Points (including Radio) • Wireless > Wireless Clients • Wireless > Channel Summary • Wireless > Rogue APs • Switch > FortiSwitches • Switch > Wired Clients
CLI and GUI Profile Consistency	User profiles within FortiAIOps are now consistent across both the Command Line Interface (CLI) and the Graphical User Interface (GUI). This means you can use the same password for both CLI and GUI access. Upon upgrading to release 3.0.0, all your existing user configurations will be automatically synchronized between the CLI and GUI.

Feature	Description
Time Range Updates for AI Insights Pages	The time ranges used in the Impacted SLAs, Impacted Devices, and SLA Config pages were inconsistent with those available in the Monitoring section. To ensure a unified and consistent user experience, the time range options for the AI Insights pages are now updated to the following: • 10 minutes • 1 hour • 4 hours • 6 hours • 1 day • 1 week
AI-Driven Anomaly Detection for Wired SLA	The wired SLAs for Throughput and Network have been upgraded for more accurate issue detection. This release introduces intelligent machine learning that analyzes recent switch port statistics. By dynamically learning from recent data, the system can now identify unusual patterns and potential breaches with significantly improved accuracy.
Quick Cable Testing for Switches in AI Insights	A shortcut to initiate cable tests on switches is now available in the **Dashboard** > **Switch** section for Throughput SLA with Classifier as low bandwidth and Sub-classifier as poor negotiated speed. If the remedy contains the phrase `cable test`, a **Run Cable Test** button is displayed, enabling you to initiate a cable test on the affected port.
Switch Monitoring Enhancements	This release introduces enhanced Switch Health SLA monitoring with the following new sub-classifiers for more detailed insights: • FSW ISL flap events • Config sync failure • Fan status correlated with temperature
User Sessions Management	A new **User Sessions** sub-menu is now available under **User Management**, giving you a centralized view of all active user sessions. This window displays crucial details for each session, such as username, IP address, authentication server, login time, connection duration, user agent, and assigned role.
REST API Polling Optimizations	The REST API polling mechanism is now optimized to minimize the utilization of CPU and memory resources on the FortiGate device.
GUI Responsiveness Improvements	The different pages have been refined and optimized to significantly boost GUI responsiveness. This ensures faster loading times, quicker reaction to user input, and an efficient interaction with the application.
Dashboard and Navigation Enhancements	This release significantly enhances your dashboard experience with improved organization and new dashboards. • The main **Dashboard** section now includes dedicated **Wireless**, **Switch**, and **SD-WAN** dashboards for streamlined monitoring. • The **Dashboard** > **AI Insights** section has been removed. All dashboards previously found here have been relocated to their

Feature	Description
	respective new dashboards under the main Dashboard menu. • The **AI Insights** > **Network Benchmarks** section is now renamed **SLA Config**. • The **AI Insights** > **Network Benchmarks** > **SD-WAN** section has been renamed **Forecast** and moved under the SD-WAN menu. • **Switch** > **FortiSwitch Clients** is now renamed **Wired Clients**. • The **Service Assurance** menu has been renamed to **SAM**.

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 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
1103759	High Availability (HA) devices disappear if the clusters have same name.
1032005	Connected clients are not visible in the **Wireless** > **Location Services Monitor** window for G and K series FortiAP even though they are available in database.
1142198	When redirecting a FortiAP from FortiGate 1 to FortiGate 2 (belonging to a different Device Group), the FortiAP does not appear in FortiGate 2 Device Group, and hence cannot be added to **Map Management** in the GUI.
1115099	After importing a new certificate, the GUI is inaccessible with the following error message displayed: `Please wait while the FortiAIOps server is coming up.`

Known Issues

The following are known issues in FortiAIOps version 3.0.0. For inquiries about a particular issue, contact *Customer Support*.

Issue ID	Description
1167312	FortiAI: MAC address in some formats (for example: `30e3.a43b.d2d3`, `30-e3-a4-3b-d2-d3`, `30-E3-A4-3B-D2-D3`) is not recognized.
1162803	FortiAI: Follow-up questions regarding the names of classifiers or sub-classifiers does not work.
1129666	SD-WAN: Misalignment between static threshold, observed value, and forecast data in graph.
1134856	SD-WAN Monitor: Bar graphs appear inverted in Safari on macOS.

www.fortinet.com