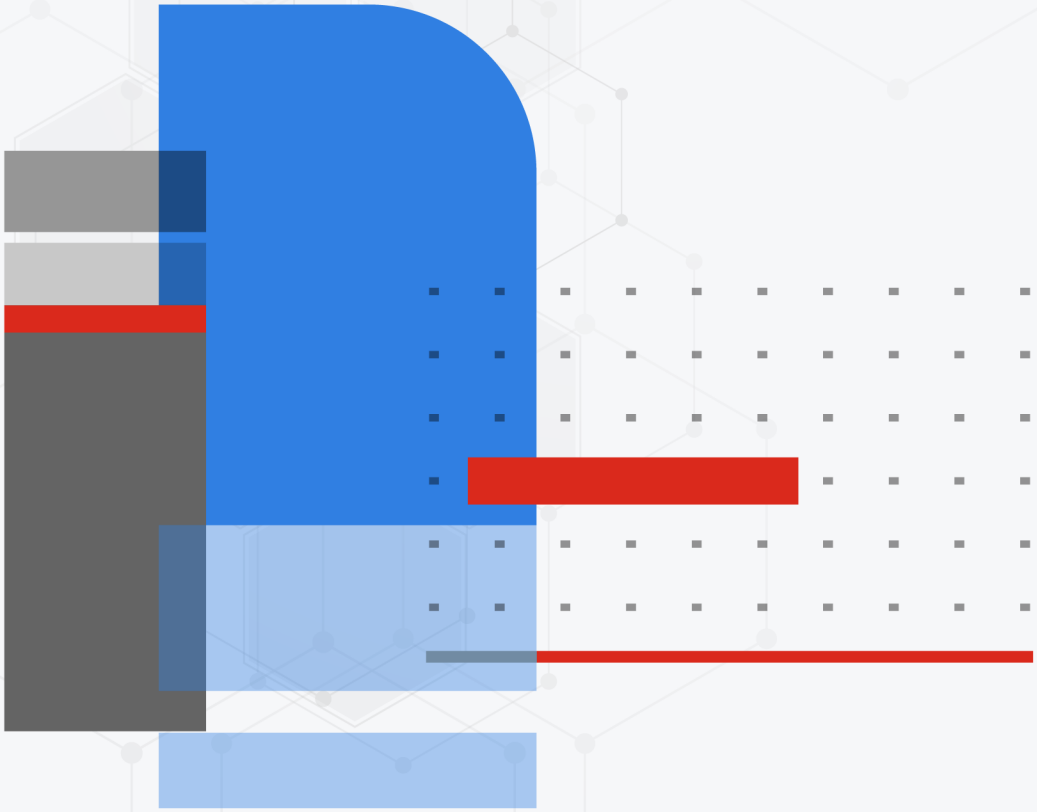
Release Notes

FortiAIOps 3.2.0



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

Feb 05, 2026
FortiAIOps 3.2.0 Release Notes
83-1235343-320-20260205

TABLE OF CONTENTS

Change log

Date	Change description
2025-12-15	FortiAIOps version 3.2.0 version.
2026-02-05	Updated What's New section.

About FortiAIOps 3.2.0

This release enhances network automation with AI-ARRP for channel optimization and expanded AI Insights for health monitoring. It also features an upgraded Wi-Fi Maps interface and a dedicated FortiExtender diagnostics, plus new capabilities for alert acknowledgement and packet capture analysis.

For more information, see What's New.

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.
- 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

The following versions are supported with this release of FortiAIOps.

Software	Supported Versions
FortiOS	• 7.6.5 • 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

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 3.2.0 delivers the following new features.

Feature	Description
AI-Driven Automated Radio Resource Provisioning (AI-ARRP)	This release introduces AI-ARRP, an advanced AI-driven system that automates and optimizes wireless channel distribution across Access Points monitored by FortiAIOps. By leveraging historical telemetry and network insights, the AI engine makes precise, data-driven channel decisions. Once enabled on the FortiGate, the engine analyzes RF conditions to select the optimal channel and automatically pushes the recommendation to the FortiGate for application to the FortiAPs. The new AI-ARRP window includes four widgets to help you understand radio health and why channel changes occurred: • Impacted Radio Forecast • Radio Health Summary • Channel Change Events • Channel Change Reason You can also perform the following actions manually: • Optimize: Instantly triggers channel planning for a specific radio. • Enable AI-ARRP: Activates the AI feature for standard radios that have reported issues in the last hour. • View Details: Opens a panel with in-depth statistics for a selected Access Point.
Enhanced Wi-Fi Maps	This release introduces Wi-Fi Maps, a significant upgrade to the previous mapping feature. It offers a modern, standard interface consistent with other Fortinet products and provides real-time visualization of FortiAP status on custom floor plans. Key improvements include full compatibility with **Ekahau**, enabling the seamless import and export of .esx files for site, building, and AP management. Additionally, an enhanced **Locate** feature allows administrators to instantly pinpoint Access Points and wireless clients on the map from any wireless management screen.
FortiExtender Monitoring and Diagnostics	This release introduces the Managed FortiExtenders window, providing a comprehensive dashboard for monitoring device health through high level summaries and in depth diagnostics. The interface is organized into four primary tabs: • **FortiExtenders**: Features visual summaries via donut charts alongside a detailed device table. • **FortiExtender SSIDs**: Lists configuration details, including Name, SSID, Type, Security, IP/Netmask, and associated FortiGate information. • **Profiles**: Displays profile settings such as Name, Model, Mode, and

Feature	Description
	VDOM details. • **Data Plans**: Tracks configured cellular plans, covering Carrier, APN, Capacity, Monthly Cost, Billing Date, and device association.
Advanced Alert Acknowledgement	This release introduces the ability to acknowledge alerts, giving you control over false positives and known issues. Acknowledging an event suppresses notifications and prevents it from negatively impacting SLA metrics. You can create time-bound rules to suppress specific events from **AI Insights** > **Impacted SLA** window. To view, edit, pause, or resume acknowledgement rules, a new window, namely **Event Acknowledgement** is now available. A new **Acknowledged Events** dashboard widget in the **Summary** dashboard provides a quick summary of suppressed alerts by type.
AI Insights for Network Health Monitoring	This release adds an **AI Insights** tab to the **Diagnostics and Tools** window for Access Points, Wireless Clients, and FortiSwitches. This feature analyzes performance metrics to identify root causes of network issues, helping administrators maintain high service levels. The system provides a high-level **SLA Health Score** categorized as follows: • Good for a score more 70 • Fair for a score between 30 and 70 • Bad for a score less than 30 The following metrics are available: • **Access Points** and **Wireless Clients**: AP Health, Roaming, Coverage, Throughput, Connection Failure, and Time To Connect. • **FortiSwitches**: Switch Network, Switch Throughput, Switch Health/Uptime, and Switch Connection Failure.

Enhanced Monitoring for Wireless Clients	This release introduces improved tools for tracking client performance trends and managing device access.
	Diagnostics and Tools
	The **Diagnostics and Tools** pane is updated with the following changes:
	• The **Performance** tab now includes an **RSSI Chart** to track signal strength trends and a **Data Rate Chart** to monitor uplink/downlink speeds.
	• The expand section now displays **Data Rate** summaries (including MCS Indexes) and **Roaming Capabilities** (Optimized, Fast, and Assisted).
	• **Action Buttons**:
	  • **Quarantine**: To add a device to the blocklist.
	  • **Disassociate**: To disconnect a client from its Access Point.

Feature	Description
	Wireless Dashboard The Wireless dashboard now features a Client Connectivity widget, designed to provide a quick overview of client connection health. It displays the total number of clients connected over a specified interval, categorized by their specific status or capabilities.
Packet Capture Analysis using FortiAI (Generative AI Assistant)	FortiAI is now enhanced to support packet capture analysis. You can upload PCAP or PCAPNG files directly to FortiAI to receive key observations and ask follow-up questions for deeper insights. Additionally, FortiAI can trigger real-time packet captures on specific interfaces, allowing you to download the resulting data for further use.
Fabric Connectors: Deployment Mode Selection	A new **Fabric Connectors** window is now introduced under **Security Fabric** to manage the deployment mode. Deployment Mode determines how FortiAIOps discovers and communicates with network devices. Two deployment modes are displayed: • **Standalone FortiGates**: In this mode, FortiAIOps operates independently and connects directly to individual FortiGates. **Note**: This is the default mode. • **FortiManager**: A centralized mode where FortiAIOps connects to FortiManager using the **Fabric Connector** rather than communicating with devices individually. **Note**: This mode requires FortiManager version 7.6.7 or 8.0.0, which will be released at a later date.
Remote Authentication	FortiAIOps now supports the automatic provisioning of admin accounts upon successful SAML authentication. This release introduces the **Auto Create Admin** setting, which requires the selection of a **Default Admin Profile**. Upon successful login, the system automatically generates an admin account with the assigned profile permissions. These accounts are persistent. They remain in the database indefinitely after logout and must be deleted manually if no longer required.
Dashboard Filter Persistence	Dashboard widget filters and layout configurations are now automatically saved to the user profile, ensuring a consistent, personalized view across sessions. Settings such as applied filters, widget sizing, and positioning persist through page reloads, logouts, browser changes, and when switching between ADOMs. These configurations are unique to the user account and remain unaffected by global navigation changes.

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

AI-ARRP

AI-ARRP is only supported on FortiOS 7.6.5 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.

Fixed Issues

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

Issue ID	Description
1162857	Users are unable to clear alert entries from the SLA history.
1179642	Certificates are not applied in FortiAIOps if the certificate name includes a space character.
1185725	The system must display historical data even after the current license is expired.
1198367	FortiGates managing more than 1000 connected FortiAPs incorrectly reports a licensing issue.
1198368	In Tunnel mode, `DHCP No Answer` events fail to trigger an SLA alert. Due to this, DHCP availability issues are not tracked or reported by the system.
1204667	`Error 500` displayed when drilling down into FortiSwitch details.
1204687	Spectrum Analyzer and VLAN Probe functionalities fail when using FortiGate firmware version 7.6.4.
1207166	Enhanced the SLA dashboard with additional insights required to ensure comprehensive network visibility.

Known Issues

The following are known issues in FortiAIOps version 3.2.0. 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`

1230483	AI-ARRP does not currently restrict or prioritize Preferred Scanning Channels (PSC) for the 6GHz band.
1236762	After restoring data from version 3.0.0 or 3.0.1 to version 3.2.0, users created on the restored server are not automatically assigned to the user group.

www.fortinet.com