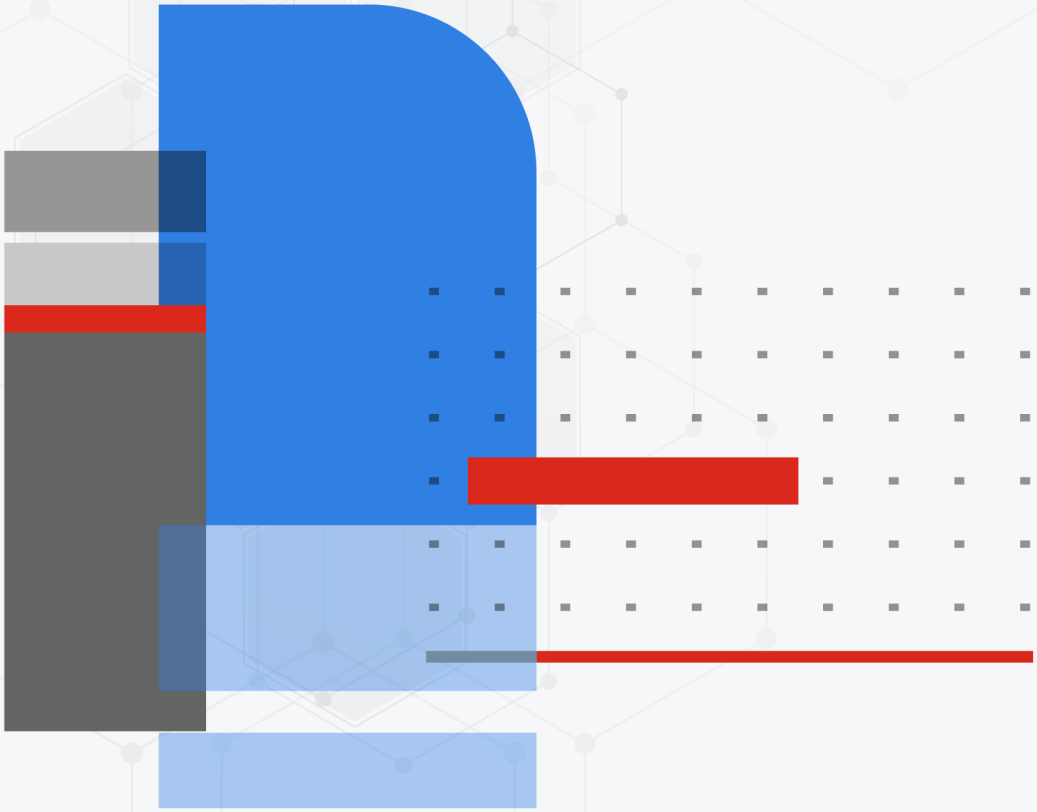
Release Notes

FortiAIOps 3.4.0



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

May 08, 2026
FortiAIOps 3.4.0 Release Notes
83-1288875-340-20260508

TABLE OF CONTENTS

Change log

Date	Change description
2026-05-08	FortiAIOps version 3.4.0 version.

About FortiAIOps 3.4.0

This release enables support for the FAO-2000G hardware platform. It introduces the new **Network Assurance Dashboard**, which provides comprehensive health scores for both the overall network and individual SLAs. Additionally, a new **Roaming** feature has been added, allowing administrators to visually track a wireless client's journey across the network.

For more information, see What's New.

Notes:

- Upgrade to the current release is supported only from version 3.0.0/3.0.1/3.2.0/3.2.1.
- 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	• 7.6.0 and above • 7.4.0 and above • 7.2.0 and above • 7.0.6 and above • 8.0.0 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
FortiManager	• 8.0.0 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	Monitoring and AI Insights
• FortiGates - 200 • FortiSwitches - 600	• CPU - 4 • Memory - 32 GB	Monitoring only

Maximum device count	Recommended Hardware	Supported Mode
• FortiExtenders - 200 • FortiAPs - 1200 • Clients - 10000	• Storage - 1 TB	
• FortiGates - 1000 • FortiSwitches - 3000 • FortiExtenders - 1000 • FortiAPs - 6000 • Clients - 25000	• CPU - 40 • Memory - 128 GB • Storage - 4 TB	Monitoring and AI Insights
• 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	Monitoring and AI Insights

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	Monitoring and AI Insights
• 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)
Default RAID (HDD - 5, SSD - 1)	13 TB	31 TB
RAID 0	18 TB	36 TB
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	Monitoring and AI Insights
• FortiGates - 200 • FortiSwitches - 600 • FortiExtenders - 200 • FortiAPs - 1200 • Clients - 10000	Monitoring only

FortiAIOps 2000G (FAO-2000G)

The following are the maximum devices supported in FortiAIOps 2000G hardware.

Maximum device count	Supported Mode
• FortiGates - 5000 • FortiSwitches - 15000 • FortiExtenders - 5000 • FortiAPs - 30000 • Clients - 100000	Monitoring and AI Insights

FortiAIOps supports RAID levels 0, 1, 5, and 10. The default configuration uses RAID 50 for HDDs and RAID 5 for SSDs. The following are the storage capacities for RAID levels in the default and maximum FortiAIOps 2000G hardware configurations.

RAID Level	FortiAIOps 2000G Hardware Configuration Default (8 HDDs, 4 SSDs)
Default RAID (HDD - 50, SSD - 5)	108 TB
RAID 0	144 TB
RAID 1	72 TB
RAID 5	123 TB
RAID 10	72 TB

Supported Web Browsers

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

Web Browser	Version
Google Chrome	147.0.7727.138
Mozilla Firefox	150.0.1
Microsoft Edge	147.0.3912.98
Safari	26.4

What's New

This release of FortiAIOps 3.4.0 delivers the following new features.

Feature	Description
Network Assurance Dashboard	This release introduces the Network Assurance Dashboard, located under the AI Insights menu. It provides a centralized interface for monitoring Service Level Agreement (SLA) performance and network health across Wireless, Switching, and WAN devices within a selected ADOM. Administrators can filter data by specific FortiGates, targeted SLAs, and custom timeframes (up to one week). The dashboard calculates health scores for both the overall network and individual SLAs, displaying them via a standard color-coded system. The information in the dashboard is divided into the following sections: • Network Health Score • SLA Performance • Lowest SLA Performing Devices • Network Device Health Status • Application Performance You can click on individual devices, clients, or data grids to open the Diagnostics and Tools pane for direct troubleshooting.
Wireless Client Roaming	This release introduces the **Roaming** graph trend analysis for Wireless Clients. The feature provides a graphical interface that allows administrators to visually track a wireless client's journey across the network and easily identify connectivity issues. You can view a client's roaming history using either of the following methods: • Navigate to **Wireless** > **Wireless Clients**, right-click a specific wireless device, and select **Roaming**. • Select a client and click **View Details** to open the **Diagnostics and Tools** pane, then click the **Roaming** button to open the client's roaming pane. The timeline provides a graphical representation of the client's connectivity with different Access Points (APs) over the chosen time period. It maps the journey using the following components: • Roaming Status • Roaming Types • Transient Association • Other Indicators The timeline is color-coded based on the Received Signal Strength Indicator (RSSI). The scale ranges from Red (-90 dBm), indicating a poor signal, to Green (-30 dBm), indicating an excellent signal. Clicking on an RSSI bar opens the Client Statistics pane, which provides detailed metrics such as RSSI information, Signal Strength/Noise, and Rx/Tx details (Bandwidth, Data Rate, and Rate MCS).

Feature	Description
FAO-2000G Hardware Platform Support	You can now deploy FortiAIOps on the FAO-2000G platform. For detailed instructions on deployment and configuration, see the *FortiAIOps User Guide for release 3.4*.
FortiAI Tokens	Your monthly FortiAI token allocation is now determined directly by your purchased FortiAIOps license. If you require additional tokens beyond this standard limit, you can purchase FortiAI Assistant token top-up licenses. For exact allocation details regarding both regular and top-up licenses, refer to the *FortiAIOps Ordering Guide*.
Fabric Connectors: FortiManager Deployment Mode	**FortiManager** is now available as a **Deployment Mode**. By using the Fabric Connector, FortiAIOps connects directly to FortiManager instead of communicating with devices individually. This integration embeds FortiAIOps analytics directly into the FortiManager dashboard. Clicking any widget navigates you to the FortiAIOps GUI for detailed analysis. This architecture ensures network settings are continuously synchronized. When FortiAIOps pushes configuration updates (such as AI-ARRP channel adjustments or client quarantine statuses) directly to FortiGates, the connector instantly synchronizes the changes with FortiManager. For configuration details, see the *FortiAIOps User Guide for release 3.4*.
SD-WAN Interface Monitoring and AI Insights	A new **SD-WAN Interfaces** tab and advanced **AI Insights** are now available to help administrators analyze performance, troubleshoot issues, and identify root causes. The **SD-WAN Interfaces** tab lists all available interfaces for a selected device (accessible via **Inventory** > **Managed FortiGates** > **View Details**). From this list, selecting a specific interface and clicking **View Details** opens the **Diagnostics and Tools** pane. Within this pane, you can use the **AI Insights** tab to perform an in-depth analysis of the interface's performance.
AI Insights for FortiExtenders	A new **AI Insights** tab is now available in the **Diagnostics and Tools** pane, specifically tracking the **FortiExtender Health** SLA. This tab provides detailed device metrics, root-cause analysis, and performance tracking. To access it, navigate to **Extenders** > **FortiExtenders**, view the details of a specific device, and select the **AI Insights** tab.
Sub-classifier Alarms	Once an acknowledgment is configured, alarms from the following sub-classifiers are now suppressed and automatically marked as **Acknowledged**: • Client Type • Asymmetric Data Rates • Incomplete Connection • Server Unresponsive and Firewall Policy • Load Balancing Denied • Server Unresponsive - Wrong or Missing Cfg Events • Wrong Credentials • Capability Mismatch

Feature	Description
	• No Domain To ensure metric accuracy, all acknowledged issues are explicitly excluded from network and device health score computations. Administrators retain the ability to manually edit or delete these alarms. Navigate to **AI Insights** > **Event Acknowledgement** window. Select and acknowledgement from the list to **Edit** or **Delete**.

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) and **FortiAIOps 2000G (FAO-2000G)**	• 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. • *(FAO-500G Only)*The 10 Gbps port does not support 1 Gbps data speeds. • *(FAO-2000G Only)* The 25 Gbps port does not support 1 Gbps data speeds. • RAID rebuild and migration operations cannot be performed concurrently. However, simultaneous rebuild operations are

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

Special Notes

REST API

FortiAIOps REST APIs now exclusively use JSON Web Tokens (JWT) for authentication and authorization. Session ID tokens are no longer supported. You must use the `aiops-token` to authorize Swagger.

Certificates

For FortiGates using default certificates, the device may not be recognized after an upgrade or reboot due to a fingerprint change. In such cases, disable certificate checks via the CLI.

The recommended best practice is to use custom certificates.

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.

Fixed Issues

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

Issue ID	Description
1034404	Managed FortiGates become unmanaged following an upgrade from FortiOS 7.4.3 to 7.4.4. The devices disconnect with an `Unknown CA` error, requiring administrators to manually import the CA certificate into FortiAIOps.
1250229	FortiSwitch information is not displayed under the General and Faceplate expandable sections within the **Diagnostics and Tools** view.
1257836	SD-WAN license is only consumed if SD-WAN was enabled on the root VDOM.

Known Issues

The following are known issues in FortiAIOps version 3.4.0. For inquiries about a particular issue, contact *Customer Support*.

Issue ID	Description
1275690	Filtering and sorting functions do not work correctly in the device list when drilling down from the Network Health Score and SLA Performance sections in the Network Assurance Dashboard.
1283459	When the score is 0%, the Network Health Score section is not visible or appears empty.
1285301	Transient association icons are misaligned in the Roaming trend graph, appearing slightly below the AP line overlapping with the Roaming Type line.
1278869	The Transient drill-down view occasionally displays empty data caused by an incorrect time calculation that set the start and end times to the exact same value.
1281907	The Roaming Type line and Roaming icon are not displayed between a Transient association and the subsequent Stable association in the Roaming trend graph.
1275213	When using the Safari browser on macOS, icons incorrectly overlap with the Activity bar in the Roaming Trend graph.

www.fortinet.com

Copyright© 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. 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.