Release Notes

FortiAIOps 2.1.0

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 19, 2025
FortiAIOps 2.1.0 Release Notes
83-1069178-210-20241008

TABLE OF CONTENTS

Change log

Date	Change description
2024-10-08	FortiAIOps version 2.1.0 version.
2025-02-07	Updated document to include support for the FortiAIOps 500G (FAO-500G) hardware platform.
2025-05-19	Updated Supported Hardware and Software section.

About FortiAIOps 2.1.0

In this release, FortiAIOps delivers enhanced AI insights into your network and resolves key issues and vulnerabilities. For more information, see What's New on page 10, 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. This does not apply to FortiAIOps 500G (FAO-500G) hardware, as it comes pre-installed with version 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
- 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
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	129.0.6668.71
Mozilla Firefox	130.0.1
Microsoft Edge	129.0.2792.65
Safari	18

What's New

This release of FortiAIOps 2.1.0 delivers the following new features.

Feature	Description
Hardware Platform	FortiAIOps can now be deployed on the new FortiAIOps 500G (FAO-500G) hardware platform.
Enhanced AI/ML Model	FortiAIOps is now based upon a deployment-specific and adaptive learning AI/ML model, that automatically adjusts to your RF environment.
SLA Enhancements	This release introduces enhancements in switching and SD-WAN SLAs for advanced AI insights. • [**SD-WAN**] FortiAIOps now offers detailed baselining of performance metrics using historical data, along with network performance forecasting and improved anomaly detection. Additionally, new enhanced dashboards provide an overall summary for each interface and SLA. • [**Switching**] Additional SLAs of **Throughput** and **Network** are now supported for switching. The existing switching SLAs of **Switch Health and Uptime** and **Switch Connection Failure** are enhanced for improved monitoring and reporting of issues.
Wireless Enhancements	This release provides additional Access Point statistics in the user interface to enable better assessment of network issues.
VDOM Support	You can now add and manage FortiGate VDOMs in FortiAIOps.
Network Interfaces	You can configure FortiAIOps with 4 active physical interfaces for VM deployments.
Summary Dashboard Enhancements	The following enhancements are delivered in the summary dashboard. • The **Access Points CPU** and **Memory Usage** widgets are added. • The **WIDS Events** widget is added. • The **Wireless Clients** panel now provides representation for clients based on the OS type. • The **System Resource Summary** panel now displays usage for both HDD and SSD.
Upgrade via GUI	You can now upgrade FortiAIOps via the GUI.
FortiGuard Updates	You can now enable automatic updates for the FortiGuard Distribution Network (FDN) license, for accurate license data synchronization.
Additional Settings	The following additional settings are added in this release. • You can select and apply a certificate that was generated/imported. • You can now configure forwarding FortiAIOps local logs to a remote machine.
Local Logs	This release of FortiAIOps introduces the local logs that provide key

Feature	Description
	insights into the system, configuration, reports, license, SAM, and mail events.
Time Range Selection	This feature allows you to view data based on the selected duration or customized time slot, on some pages of the FortiAIOps user interface.
CLI Enhancements	Additional commands to manage *DNS No Domain* events and LLDP transitions are added.
Public Cloud Platforms	FortiAIOps can now be deployed on the Oracle Cloud Infrastructure (OCI).
VM Platforms	FortiAIOps can now be deployed on Proxmox.
Others	The following are some additional enhancements delivered in this release. • The FAP-241K and FAP-243K models are now supported. • You can now export the wireless and FortiSwitch clients' data in a *.csv* file. • FortiAIOps is now Swagger compliant that enhanced API accessibility. • FortiOS NAC discovery is now supported via the LLDP and DHCP options.

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. • To receive SD-WAN logs, ensure that the SD-WAN monitoring license is applied in FortiGate. This is to generate congestion logs. • 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

Product	Recommendation
	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

Note the following when using FortiAIOps.

- [SD-WAN] Upgrade to the current release sets the baseline configuration mode to dynamic, by default.
- [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.
- By default, there is no password for logging into the CLI mode for the first time. However, you are prompted to change the password after logging in. The default login credentials (username/password) for the GUI are admin/admin. Configuring the CLI password does not modify the GUI password.
- The FortiAIOps CLI and GUI users are different.
- 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.
- The *Time to Connect* - DNS delay is not supported.
- 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

This release of FortiAIOps is no longer vulnerable to the following.

- CVE-2024-6387
- CVE-2024-39894

Visit https://www.fortiguard.com/psirt for more information.

Fixed Issues

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

Issue ID	Description
818888	Wired Client negotiating 100 MB links were not reported in FortiAIOps.
913525	FortiGate Memory and CPU usage graph and data were not stable.
987484	FortiAIOps should support user deletion from the GUI.
1040104	Warning message is required when creating SAM.
1055642	FortiGate CPU and memory data was not displayed in the FortiAIOps graph.
1058680	FortiAIOps VDOM clients view was empty.
1060760	The FortiAIOps dashboard did not display logs from FortiGate.
1072752	Devices not displayed in the location services dashboard.

Known Issues

The following are known issues in FortiAIOps version 2.1.0. For inquiries about a particular issue, contact *Customer Support*.

Issue ID	Description	Workaround
1082349	The custom range selection of **Today**, does not display wireless and switching clients data.	The options to filter data for 10 minutes, 2 hours, 6 hours, and 1 day are available.
1085839	After a failback or failover, the status of existing access points added to FortiAIOps may display as *Unknown* due to a synchronization delay between the primary and secondary FortiGate.	Reboot the access point.
1070637	After restoring a 2.0.0 backup file, the unique station report is empty for longer hours.	
1075458	In the switching SLA, uplink congestion is reported as port congestion.	
1076554	SAM tests details are not displayed in the dashboard after FortiAIOps upgrade/reboot.	
1079915	SD-WAN data is displayed 1 hour after FortiGate or a new performance SLA is added.	
1081501	Pre-upgrade performance SLA failures upto 2 hours are marked as *good* after upgrade in SDWAN UI.	
1083226	SD-WAN Performance metrics comparison with historical data, can have minor variation in anomaly detection for 30, 45 and 15 timezone offsets.	

www.fortinet.com

Copyright© 2025 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.