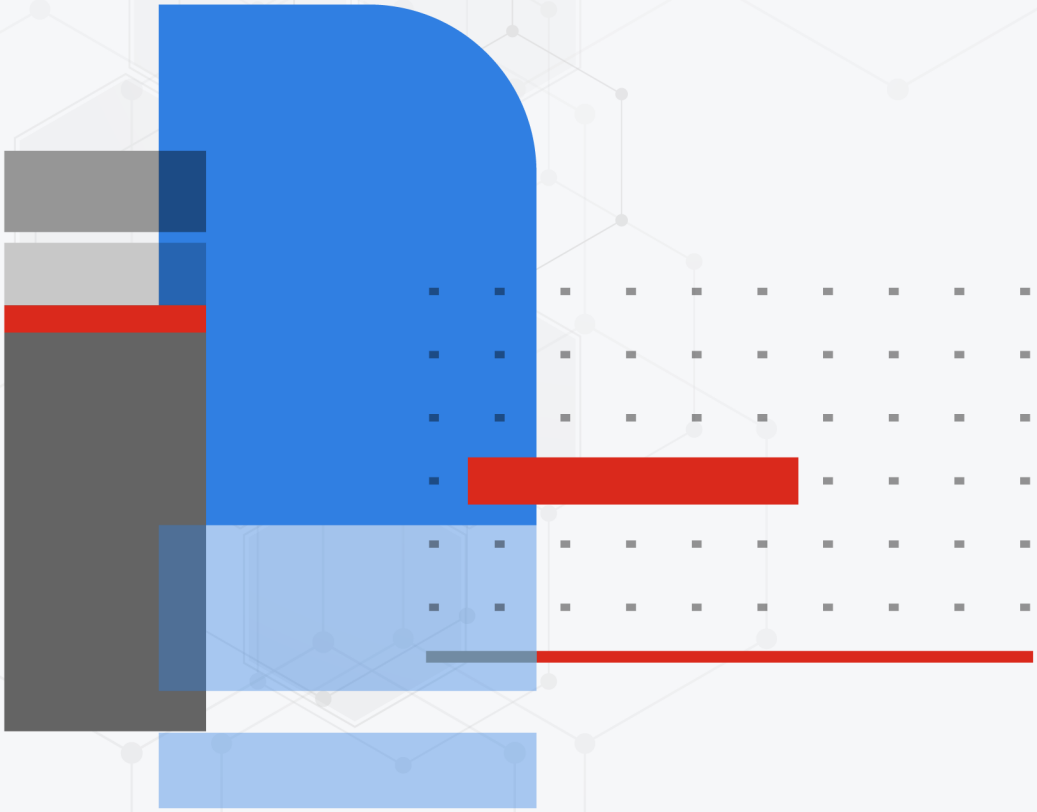
# Release Notes

FortiAIOps 2.0.0



**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

November 16, 2023
FortiAIOps 2.0.0 Release Notes
83-905872-200-20231116

# TABLE OF CONTENTS


**Change log** ..... **4**
**About FortiAIOps 2.0.0** ..... **5**
**Overview** ..... **6**
**Supported Hardware and Software** ..... **7**
**Recommendations and Special Notes** ..... **9**
**Known Issues** ..... **11**

# Change log

| Date | Change description |
| --- | --- |
| 2023-11-16 | FortiAIOps version 2.0.0 version. |

# About FortiAIOps 2.0.0

This release of a standalone FortiAIOps bundles the network monitoring feature and AI insights. For more information, see the *FortiAIOps 2.0.0 User Guide*.

**Note**: 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 view and monitor the status 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 learns from your network data to report statistics, providing visibility and deep insight into your network, and it monitors integrated wireless, wired, and SD-WAN networks by managing and monitoring of FortiGate controllers.

# Supported Hardware and Software

The following versions are supported with this release of FortiAIOps.

| Software | Supported Versions |
|---|---|
| **FortiOS** | • 7.0.6 and above<br>• 7.2.0 and above<br>• 7.4.0 and above |
| **FortiWiFi** | All devices with FortiOS version 7.0 and above. |
| **FortiSwitchOS** | • 7.0.x and above |
| **Access Points** | • FortiAP 7.2.0 and above<br>• FortiAP-U 6.2.4 and above |
| **FortiExtender** | • 7.2.2 and above |

The following are the recommended resource requirements for FortiAIOps.

| Maximum device count | Recommended Hardware | Supported Mode |
|---|---|---|
| • FortiGates - 30<br>• FortiSwitches - 90<br>• FortiExtender - 30<br>• FortiAPs - 180<br>• Clients - 3000 | • CPU - 4 CPU<br>• Memory - 32 GB<br>• Storage - 1 TB | AI Insights and Monitoring |
| • FortiGates - 200<br>• FortiSwitches - 600<br>• FortiExtender - 200<br>• FortiAPs - 1200<br>• Clients - 10000 | • CPU - 4 CPU<br>• Memory - 32 GB<br>• Storage - 1 TB | Monitoring only |
| • FortiGates - 600<br>• FortiSwitches - 1800<br>• FortiExtender - 600<br>• FortiAPs - 3600<br>• Clients - 15000 | • CPU - 24 CPU<br>• Memory - 128 GB<br>• Storage - 4 TB | AI Insights and Monitoring |

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

| Web Browser | Version |
|---|---|
| Google Chrome | 119.0.6045.124 |
| Mozilla Firefox | 119 |

| Web Browser | Version |
| --- | --- |
| Microsoft Edge | 119.0.2151.58 |
| Safari | 17 |

# 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 7.2.6 and above 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.<br>• 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.<br>• To receive SD-WAN logs, ensure that the SD-WAN monitoring license is applied in FortiGate. This is to generate congestion logs.<br>• Configure the *sla-fail* and *sla-pass* log failure period, the recommended duration is 30 to 60 seconds.<br>• When the backup file is restored on a different machine, reconfigure the FortiAIOps IP address in the FortiGate syslog settings. |
| **Others** | The FortiAIOps time and timezone should be synchronized with the NTP server. |

## Special Notes

Note the following when using FortiAIOps.

- 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.
- Upgrading FortiAIOps is supported only via the CLI mode.
- 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.

- 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.
- For wired SLA, only personal computers devices are considered as end clients (other network devices are not displayed).
- Spectrum Analysis is supported on all FAP models, except the G-series access points.
- SAM works with F-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.

# Known Issues

The following issues are known is FortiAIOps version 2.0.0. For inquiries about a particular issue, contact *Customer Support*.

| Issue ID | Description |
|---|---|
| 900200 | New models of G and F series FortiAPs are not supported in the RF planner. |
| 904803/972319/900413 | Filtering and sorting of columns is not working, for some fields, in the Wireless (APs and clients) and FortiSwitch clients pages. |
| 911547 | Spectrum analysis is not supported on G-series FortiAPs. Also, incorrect radio IDs are displayed. |
| 915755 | SAM test runs in an unresponsive state if FortiAIOps upgraded or restarted. |
| 919050 | Filtering and sorting is not available for the rogue AP table columns. |
| 935970 | The AI Insights dashboard data is not filtered accurately based on the selected FortiGate. |
| 941199 | FortiGate cannot be added in FortiAIOps if the pre login banner is enabled on FortiOS. |
| 945366 | AP power supply anomalies are not reported in FortiAIOps. |
| 947772/948194 | Wired clients and FortiSwitch health statistics and logs related events are not displayed accurately in FortiAIOps. |

www.fortinet.com