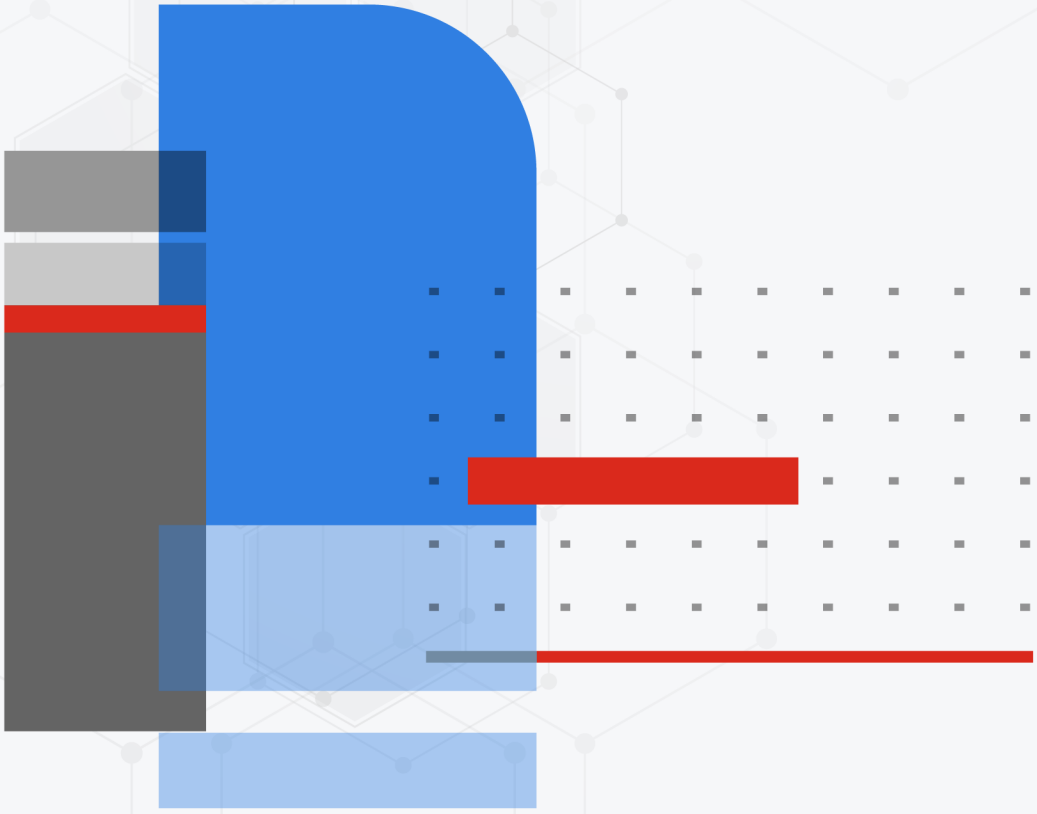
Release Notes

FortiAIOps 2.0.2



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

August 26, 2024
FortiAIOps 2.0.2 Release Notes
83-1069178-202-20240826

TABLE OF CONTENTS

Change log

Date	Change description
2024-08-26	FortiAIOps version 2.0.2 version.

About FortiAIOps 2.0.2

In this release, FortiAIOps delivers key vulnerability fixes and resolved issues. For more information, see Common Vulnerabilities and Exposures and Fixed Issues.

Notes:

- Upgrade to the current release is supported only from version 2.0.0/2.0.1.
- 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 • 7.2.0 and above • 7.4.0 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

The following are the recommended resource requirements for FortiAIOps.

Maximum device count	Recommended Hardware	Supported Mode
• FortiGates - 30 • FortiSwitches - 90 • FortiExtenders - 30 • FortiAPs - 180 • Clients - 3000	• CPU - 4 • 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 • 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	• CPU - 104	AI Insights and Monitoring

Maximum device count	Recommended Hardware	Supported Mode
• FortiSwitches - 15000 • FortiExtenders - 5000 • FortiAPs - 30000 • Clients - 100000	• Memory - 256 GB • Storage - 8 TB	

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

Web Browser	Version
Google Chrome	127.0.6533.120
Mozilla Firefox	129.0.2
Microsoft Edge	127.0.2651.105
Safari	17.6

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 or version 7.4.0 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 30 to 60 seconds. • 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.
- 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.
- 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.

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
1055642	FortiGate CPU and memory data is not displayed in FortiAIOps graph.
1060760	FortiAIOps Dashboard is not displaying FortiGate logs.

Known Issues

The following are known issues in FortiAIOps version 2.0.2. For inquiries about a particular issue, contact *Customer Support*.

Issue ID	Description	Workaround
984470	FortiAIOps docker fails to start on Google Cloud Platform (GCP) upon reboot.	
992173	In the **AI Insights** dashboard, the statistics for connected switch clients take longer (2.5 minutes approximately) to display, only for a duration of 1 week.	
992778	Sometimes, SAM measured baseline tests fail due to time zone errors.	
995350	[AI Insights dashboard] The **Overall Network Health** and the **Impacted Clients** charts are not supported in the Firefox browser.	Use a supported browser, such as, Chrome, Edge, and Safari.
1000705	In **Wireless > Clients**, the trend data displayed for more than 12 hours is inaccurate.	
1011884	Interfering SSID data reported by radio 3 is not displayed in the **Channel Summary**.	
1013904	In **Wireless > applications**, the data in the **User**, **Access Points**, and **SSID** columns for bridge SSID profiles is incorrect in all widgets.	
1014527	Currently, there is a delay in the switch SLA data in the **Impacted SLA** and **Impacted Devices** pages.	
1020336	FortiAIOps does not detect FaceTime application due to signature issues in FortiGuard.	

Issue ID	Description	Workaround
1034404	FortiGates managed by FortiAIOps lose connectivity on upgrade.	FortiAIOps rigorously scrutinizes the certificate chain. On upgrading (when using the *Fortinet_GUI_Server* certificate), if FortiGate ignores the CA certificate in FortiAIOps, then it loses connectivity. To restore the FortiGate's online status, perform any of the following. • Download the CA certificate from FortiGate and upload it into FortiAIOps (**System > CA certificates**). • Switch to a custom certificate like *Let's Encrypt* and add the CA certificate in FortiAIOps.

www.fortinet.com