



Release Notes

FortiAI Ops 2.0.1



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 26, 2024

FortiAIOps 2.0.1 Release Notes

83-1017460-201-20240526

TABLE OF CONTENTS

- Change log 4**
- About FortiAI Ops 2.0.1 5**
- Overview 6**
- Supported Hardware and Software 7**
- What's New 9**
- Recommendations and Special Notes 11**
- Common Vulnerabilities and Exposures 13**
- Fixed Issues 14**
- Known Issues 15**

Change log

Date	Change description
2024-04-16	FortiAI Ops version 2.0.1 version.
2024-04-23	Updated the list of new FortiAPs supported in this release. See What's New
2024-05-06	Added Nutanix support. See What's New
2024-05-26	Updated Known Issues .

About FortiAI Ops 2.0.1

In this release, FortiAI Ops delivers key new features such as, elevated artificial intelligence and machine learning capabilities to enhance user experience for wireless access and the support of public Cloud platforms for deploying FortiAI Ops. For detailed information on the new features of this version, see [What's New](#).

Notes:

- Upgrade to the current release is supported only from version 2.0.0.
- The license is now applied as soon as FortiGate is added to the inventory. The delay in license application from the previous release is eliminated.
- The FortiAI Ops 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

FortiAI Ops 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. FortiAI Ops 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 FortiAI Ops.

Software	Supported Versions
FortiOS	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 7.0.x and above
Access Points	<ul style="list-style-type: none"> FortiAP 6.4.x and above FortiAP-U 6.2.4 and above
FortiExtender	<ul style="list-style-type: none"> 7.2.2 and above

The following are the recommended resource requirements for FortiAI Ops.

Maximum device count	Recommended Hardware	Supported Mode
<ul style="list-style-type: none"> FortiGates - 30 FortiSwitches - 90 FortiExtenders - 30 FortiAPs - 180 Clients - 3000 	<ul style="list-style-type: none"> CPU - 4 Memory - 32 GB Storage - 1 TB 	AI Insights and Monitoring
<ul style="list-style-type: none"> FortiGates - 200 FortiSwitches - 600 FortiExtenders - 200 FortiAPs - 1200 Clients - 10000 	<ul style="list-style-type: none"> CPU - 4 Memory - 32 GB Storage - 1 TB 	Monitoring only
<ul style="list-style-type: none"> FortiGates - 1000 FortiSwitches - 3000 FortiExtenders - 1000 FortiAPs - 6000 Clients - 25000 	<ul style="list-style-type: none"> CPU - 40 Memory - 128 GB Storage - 4 TB 	AI Insights and Monitoring
<ul style="list-style-type: none"> FortiGates - 2500 FortiSwitches - 7500 FortiExtenders - 2500 FortiAPs - 15000 Clients - 60000 	<ul style="list-style-type: none"> CPU - 24 Memory - 128 GB Storage - 4 TB 	Monitoring only
<ul style="list-style-type: none"> FortiGates - 5000 	<ul style="list-style-type: none"> CPU - 104 	AI Insights and Monitoring

Maximum device count	Recommended Hardware	Supported Mode
<ul style="list-style-type: none">• FortiSwitches - 15000• FortiExtenders - 5000• FortiAPs - 30000• Clients - 100000	<ul style="list-style-type: none">• Memory - 256 GB• Storage - 8 TB	

The following web browsers are tested to access the FortiAI Ops GUI.

Web Browser	Version
Google Chrome	123.0.6312.106
Mozilla Firefox	123
Microsoft Edge	123.0.2420.81
Safari	17.4.1

What's New

This release of FortiAI Ops 2.0.1 delivers the following new features.

Feature	Description
Enhanced AI Detection	<ul style="list-style-type: none"> In this release, FortiAI Ops uses elevated artificial intelligence and machine learning capabilities to enhance user experience for wireless access. This applies to throughput and coverage SLAs. FortiAI Ops also provides detailed analytics on the experience for specific conference applications, MS Teams, Google Meet, and Zoom. SSID down events detection is now supported.
Public Cloud Platforms	<p>FortiAI Ops can now be deployed on the following public Cloud platforms.</p> <ul style="list-style-type: none"> Microsoft Azure Google Cloud Platform Amazon Web Services
VM Platforms	<p>FortiAI Ops can now be deployed on Nutanix.</p>
Enhanced AI Insights Dashboard	<p>The following new widgets are now available in the AI insights dashboard.</p> <ul style="list-style-type: none"> Overall network health Impacted clients trends Top 3 impacted applications Top 5 problematic devices <p>The AI insights dashboard now displays data for a maximum of 1 week.</p>
Log Retention	<p>FortiAI Ops now dynamically allocates the duration to retain statistics data based on daily data accumulation and space available.</p>
New Topology	<p>This release provides a simplified topology with a visualization/illustration of the physical placement of devices, for ease of navigation and debugging.</p>
Enhanced GUI	<ul style="list-style-type: none"> New System Resource Summary, High Latency FortiGates, and FortiSwitches Events widgets are added in the Summary dashboard. Simplified physical and logical topologies are available in the Security Fabric. New and enhanced Channel Summary page in Wireless.
New FortiAP Support	<p>This release supports the following FortiAPs.</p> <ul style="list-style-type: none"> FAP- 231G FAP- 233G FAP- 234G FAP- 431G FAP- 432G FAP- 433G

Feature	Description
	<ul style="list-style-type: none">• FAP- 432R• FAP- 441K• FAP- 443K
Others	<ul style="list-style-type: none">• The LAN port statistics are now displayed for access points.• The AP health trends now monitor the temperature.• SMTP server configurations are added to receive email notifications for report generation.

Recommendations and Special Notes

- [Recommendations](#)
- [Special Notes](#)

Recommendations

Fortinet **recommends** the following versions and configurations to use with FortiAIOps.

Product	Recommendation
FortiAP	<ul style="list-style-type: none"> • FortiAP (FAP) version 7.2.2 and above is recommended to generate all events in FortiAIOps.
FortiOS	<ul style="list-style-type: none"> • FortiOS version 7.2.4 and above or version 7.4.0 are recommended to generate all events in FortiAIOps.
FortiGate	<ul style="list-style-type: none"> • [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 <i>Throughput</i> SLA - interference issues in FortiAIOps. To detect interfering SSIDs in FortiGate, configure the FortiAP profile to use <i>Radio Resource Provisioning</i> or a <i>WIDS</i> 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 <i>sla-fail</i> and <i>sla-pass</i> 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 FortiAI Ops is no longer vulnerable to the following.

- CVE-2023-48795
- CVE-2023-51384
- CVE-2023-51385
- CVE-2024-27782
- CVE-2024-27783
- CVE-2024-27784
- CVE-2024-27785
- CVE-2024-27786

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
941199	Sometimes, the discovery of FortiGate failed with errors in the diagnostic logs.
977236	FortiSwitch port status was <i>Down</i> in FortiAIOps but <i>Up</i> in FortiGate.
978275	FortiGates added through FortiAIOps GUI are not visible in GUI after a period of time.
982922	If the first time login failed after adding FortiGate in the HA mode, then the HA mode was not updated even after the FortiGate was successfully discovered.
982926	Sometimes, the GUI was not accessible due to some certificate issues.
1009655	FortiSwitch data was not displayed in the widgets in Switch > FortiSwitch .
1009660	Unable to add the second FortiAP in the heat map.

Known Issues

The following are known issues in FortiAI Ops version 2.0.1. For inquiries about a particular issue, contact *Customer Support*.

Issue ID	Description	Workaround
984470	FortiAI Ops 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	FortiAI Ops does not detect FaceTime application due to signature issues in FortiGuard.	

Issue ID	Description	Workaround
1034404	FortiGates managed by FortiAIOps lose connectivity on upgrade.	<p>FortiAIOps rigorously scrutinizes the certificate chain. On upgrading (when using the <i>Fortinet_GUI_Server</i> 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.</p> <ul style="list-style-type: none">• Download the CA certificate from FortiGate and upload it into FortiAIOps (System > CA certificates).• Switch to a custom certificate like <i>Let's Encrypt</i> and add the CA certificate in FortiAIOps.

