

A decorative header section with a solid blue background. It features a pattern of white, concentric hexagonal outlines of varying sizes, some of which are slightly offset from each other, creating a sense of depth and movement.

# FortiAI Ops - Release Notes

Version 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](mailto:techdoc@fortinet.com)

June 22, 2021

FortiAIOps 1.0 Release Notes

# TABLE OF CONTENTS

- Change log ..... 4**
- Overview ..... 5**
- Supported FortiOS ..... 6**
- Enabling FortiAI Ops ..... 7**
- Known issues ..... 8**

## Change log

Date	Change description
2021-06-22	FortiAI Ops version 1.0 release version.

# Overview

FortiAIops aims at diagnosing and troubleshooting network issues by analyzing potential problems and suggesting remedial steps 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 on a comprehensive and simple dashboard, providing network visibility and deep insight into your network. Thus, enabling you to effectively manage your connected devices and resolve network issues swiftly with the help of AI/ML.

The FortiAIops Management Extension Application (MEA) container is hosted on the FortiManager integrated platform that provides centralized management of Fortinet products and other devices. For more information on FortiManager operations, see related [product documentation](#).

Some key features of FortiAIops supported in this release are as follows:

- Wireless SLA configurations
  - Successful Connects - Association, Authentication, DHCP, DNS
  - Time To Connect - Association, Authentication, DHCP, DNS
  - AP Health and Uptime
- Switching SLA configurations
  - Successful Connects - Authentication, MAC limit
  - Switch Health and Uptime
- Topology view of the impacted devices (wireless and switch)
- Top 3 and overall impacted FortiGates (wireless and switch)
- AP, switch, and station - issue identification and suggested remedies.

## Notes:

- FOS version 7.0.0 is recommended with FortiSwitch version 7.0.0 to generate all events.
- In FortiGate, configure the FortiManager IP in syslog.
- The FortiAIops - Time to Connect DNS is not supported.
- For wired SLA, only Linux devices are considered as end clients.
- Client data for FortiAIops topology is fetched only from the physical topology page of FortiGate.

The following scale deployment limits are supported for FortiAIops.

Devices	Maximum limit
FortiGate controllers	600
Access Points	600
Stations	12000

# Supported FortiOS

The following versions of FortiOS are supported with this release of FortiAI Ops.

- 6.4.3
- 6.4.4
- 6.4.5
- 7.0.0
- 7.0.1 (awaiting release)

# Enabling FortiAI Ops

Follow this procedure to enable FortiAI Ops.

1. Connect to the FortiManager GUI.
2. Navigate to **System Settings > Administrators > Admin** and set **JSON API Access** to **Read-Write**. This enables communication between FortiManager and FortiAI Ops.

The screenshot displays the FortiManager GUI's 'System Settings' section. On the left, a sidebar menu lists various settings, with 'Administrators' highlighted in blue. The main area is titled 'Edit Administrator' and shows configuration for the 'admin' user. Fields include 'User Name' (admin), 'Avatar' (A), 'Comments' (0/127), 'Admin Type' (LOCAL), 'Admin Profile' (Super\_User), 'Administrative Domain' (All ADOMs), 'Policy Package Access' (All Packages), 'JSON API Access' (Read-Write), 'Trusted Hosts' (OFF), and 'Meta Fields'. The 'JSON API Access' dropdown is highlighted with a red box. The 'Administrative Domain' and 'Policy Package Access' are also set to 'All ADOMs' and 'All Packages' respectively.

3. Navigate to **Management Extensions** and click the **FortiAI Ops** tile.

**Note:** Ensure that the DNS server is reachable.

## Known issues

The following issues are known in FortiAI Ops version 1.0. For inquiries about a particular issue, visit the [Fortinet Support](#) website.

Issue ID	Description
718461	DNS delays are not displayed in the Time to Connect SLA dashboard.
725228	Raw logs are not displayed for some of the AP related failure events.
720372	DHCP failure is not displayed when the client MAC address is blocked in the SSID.
721601	DNS-no-resp failure correlation and remediation reported is not proper.
722037	Clicking on classifiers on the donut chart does not filter log contents.
722241	The <b>Top 3 Sites</b> in the dashboard displays data for FortiGates with impacted clients only.
726342	Offline FortiSwitch directly connected to a FortiGate is not displayed in the topology.
723096	MAC addresses inserted in the database are not the stations for impacted switch.





Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.