

Release Notes

FortiAI Ops 1.1.0



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



July 18, 2022

FortiAIOps 1.1.0 Release Notes

TABLE OF CONTENTS

Change log	4
About FortiAI Ops 1.1.0	5
Overview	6
What's New	7
Supported Hardware and Software	10
Upgrading FortiAI Ops	11
Recommendations and Limitations	12
Fixed Issues	14
Known Issues	15
Common Vulnerabilities and Exposures	16

Change log

Date	Change description
2022-07-18	FortiAI Ops version 1.1.0 release version.

About FortiAI Ops 1.1.0

This release of FortiAI Ops delivers some new features and enhancements, see section [What's New](#)

Note: This release of FortiAI Ops requires FortiManager version 7.2.1.

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](#).

What's New

This release of FortiAI Ops 1.1.0 delivers the following new features.

- [SD-WAN SLA](#)
- [New Wireless SLAs](#)
- [Dynamic Baselines Configuration](#)
- [Dashboard Enhancements](#)
- [HA Cluster Support](#)

SD-WAN SLA

The minimum quality SLA strategy uses criteria that you configure to determine which SD-WAN links to use and to identify SD-WAN network issues. You can configure the SD-WAN threshold parameters and monitor them in the dashboard.

New Wireless SLAs

The 1.1.0 now allows you to monitor and analyze client data based on 3 new SLA thresholds, **Roaming**, **Coverage**, and **Throughput**. The Roaming SLA is configurable and you can set the required thresholds or enable FortiAI Ops to set the thresholds dynamically. The Throughput and Coverage SLA thresholds are not configurable and FortiAI Ops sets and applies these thresholds. You can monitor the impacted SLAs in the dashboard.

Dynamic Baselines Configuration

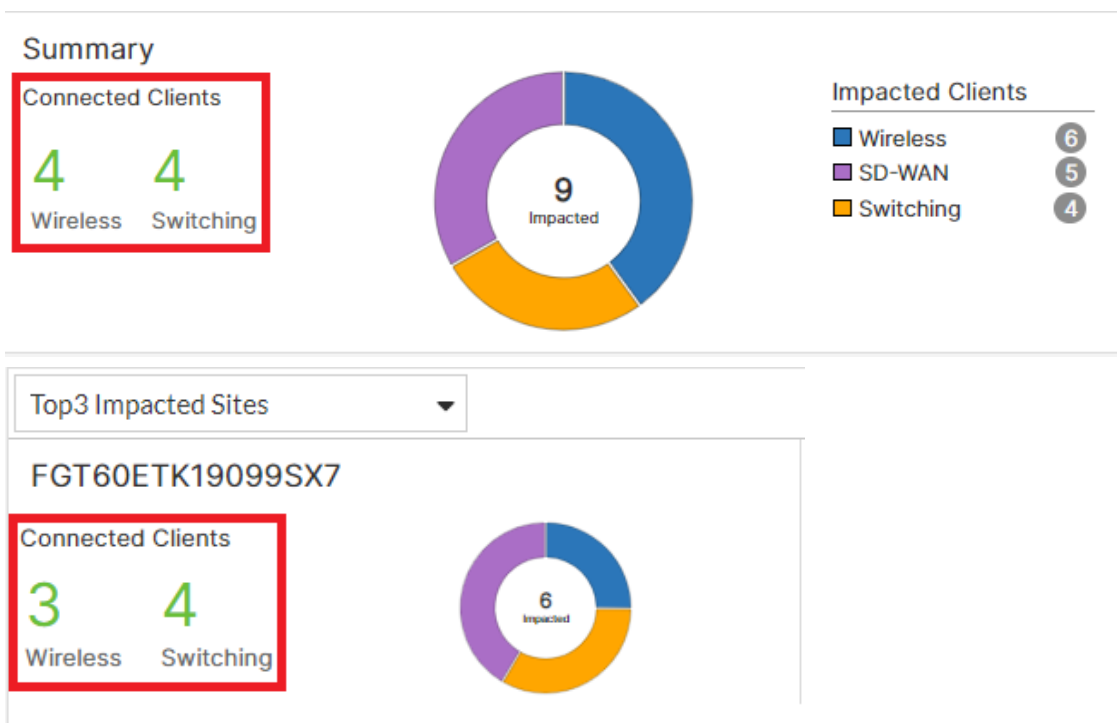
You can now allow FortiAI Ops to calculate the SLA thresholds/baselines dynamically using machine learning algorithms. This enables you to diagnose network issues based on accurate and latest client data trends. The AI driven algorithms are designed to learn new data regularly for changes in client activity, calculate thresholds, and report statistics.

The **SD-WAN**, **Roaming**, and **Time To Connect** thresholds can be configured dynamically.

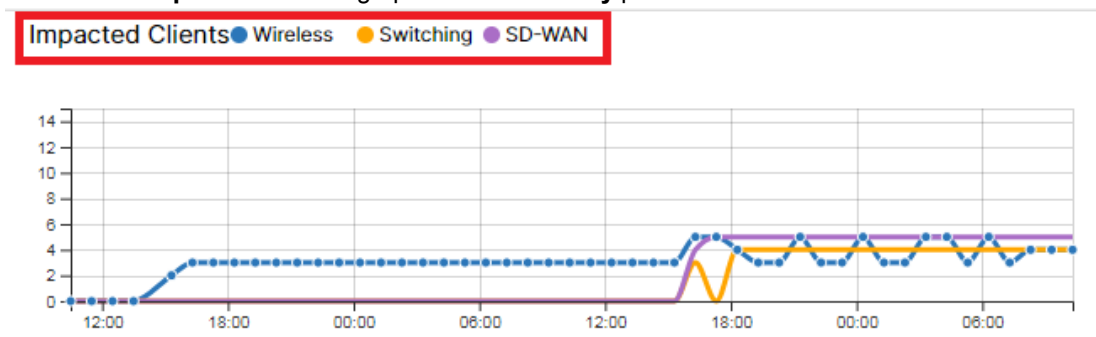
Dashboard Enhancements

This release delivers the following enhancements.

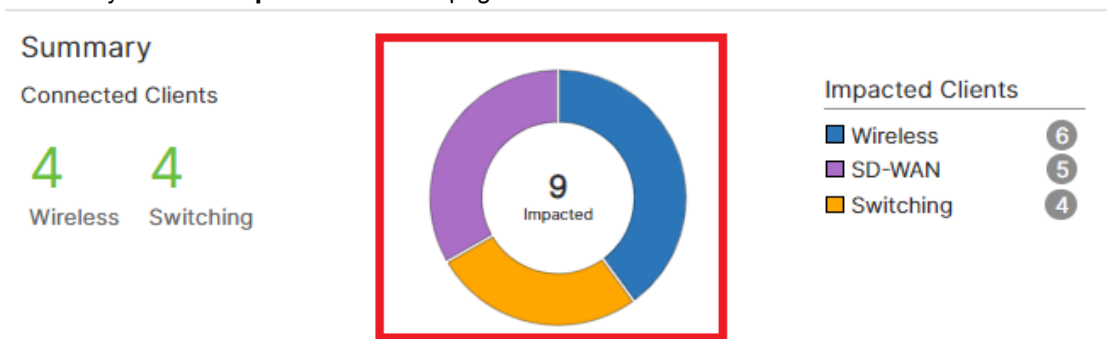
- These enhancements are added in the **Monitor > Overview** page.
 - Click on the connected client count in the **Summary** or **Top 3 Impacted Sites** panels to view the client details.



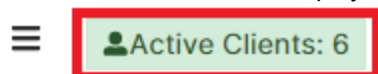
- Click on the **Impacted Clients** graph in the **Summary** panel to view the client details.



- Clicking on the impacted clients donut charts in the **Summary** or **Top 3 Impacted Sites** panel, redirects you to the **Impacted Devices** page.



- The **Active Client** count is displayed at the top, clicking on this displays the client details.



- The **Impacted Devices** dashboard provides details of the various devices in your network that are associated with impacted clients, that include the wireless, switching, and SD-WAN clients. You can view and analyze the SLA data based on the device type. The **Impacted SLA** dashboard displays the impacted wireless, switching, and SD-WAN clients, categorized based on SLAs, classifiers, and sub-classifiers. You can filter and view the SLAs as per specific categories.
- A toggle option is added for all the impacted SLA panels in the wireless, switching, and SD-WAN dashboards that allows you to toggle between the impacted client count and the impacted device/interface count.

HA Cluster Support

You can import FortiGate clusters in FortiAIOps, the HA configuration (Active-Active/Active-Passive) is preserved.

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">• 7.0.5• 7.2.0• 7.2.1
FortiSwitchOS	<ul style="list-style-type: none">• 7.0.4• 7.2.0• 7.2.1

The following are the recommended resource requirements for FortiAI Ops. For more information, see the [FortiManager Release Notes](#).

Maximum devices (FortiGate/FortiSwitches/APs/Clients)	Recommended Hardware (FortiManager)
30/30/60/600	4 CPU/16 GB RAM/500 GB storage
100/100/200/4000	6 CPU/16 GB RAM/500 GB storage
600/600/1200/24000	8 CPU/32 GB RAM/2 TB storage
1600/1600/3200/64000	16 CPU/64 GB RAM/2 TB storage

Upgrading FortiAI Ops

Run the `diagnose docker upgrade fortiaios` command in the FortiManager CLI to upgrade FortiAI Ops to the latest version. Ensure that FortiAI Ops is enabled and a new version is available for installation.

Recommendations and Limitations

- [Recommendations](#)
- [Limitations](#)

Recommendations

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

Product	Recommendation
FortiManager	<ul style="list-style-type: none"> • This release of FortiAI Ops requires FortiManager version 7.2.1. • The ADOM version supports FortiOS version 7.0.x and 7.2.x. • Configure and enable syslog.
FortiAP/FortiAP-U	<ul style="list-style-type: none"> • FortiAP (FAP) version 7.2.0 and FortiAP-U (FAP-U) version 6.2.4 are recommended.
FortiSwitch	<ul style="list-style-type: none"> • FortiSwitch OS version 7.2.1 is recommended.
FortiOS	<ul style="list-style-type: none"> • FortiOS version 7.2.1 is recommended to generate all events in FortiAI Ops.
FortiGate	<ul style="list-style-type: none"> • [FortiGate/FortiAnalyzer] Configure the FortiManager IP address in the FortiGate syslog or FortiAnalyzer to send events to FortiAI Ops. • Ensure that you enable the detection of interfering SSIDs in FortiGate to allow reporting of <i>Throughput</i> SLA - interference issues in FortiAI Ops. 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.

Limitations

The following **limitations** apply to FortiAI Ops.

- The Time to Connect DNS is not supported.
- For wired SLA, only Linux/Windows/MacBook devices are considered as end clients.
- Backup and restore operations are not supported.
- All *Throughput* SLAs are not supported in FortiAI Ops, if the FortiOS/FortiAP/FortiAP-U deployed are below the recommended versions.
- Currently FortiAI Ops evaluates only some de-authentication reasons.
- Configuring the *set sla-fail-log-period* to less than 30 seconds generates many SD-WAN logs. Also, this may overload FortiAI Ops.
- Currently FortiAI Ops receives the channel utilization data excluding WiFi and non-WiFi interference

utilization data.

- Retry information is not available for these FortiAP models, FAP-43xF, FAP-U43xF, FAP-23xF.

Fixed Issues

This release of FortiAI Ops resolves the issues described in this section.

Issue ID	Description
740904	Mismatch between the wireless impacted client data displayed in the trend graph and the data in the SSID bubble/ SLA data.
743441	Toggling between the failure events displayed incorrect data in the topology donut chart.
743700	On clicking the classifier donut chart, only related sub-classifier donuts should be displayed.

Known Issues

The following issues are known in FortiAI Ops version 1.1.0. For inquiries about a particular issue, contact *Customer Support*.

Issue ID	Description
721121	[Scale deployment] A sudden drop is observed in the last sample of the impacted client trend graph, also, the count display in the Y axis is not correct.
783916	The impacted client details displayed in the graph and pop-up window do not match, in the dashboard.
785303	Starting or upgrading FortiAI Ops can take approximately 15 minutes due to large product image size.
795205	[Scale deployment] Active client count displayed in the dashboard is not accurate.
805319	Impacted clients graphs in the Summary and Wireless panels display incorrect data when the client roams across SSIDs/bands.
807253	Some older data is not available in FortiAI Ops after upgrading.
819651	Incorrect association time is displayed in <i>View Details</i> client drill down view in the overview dashboard page.

Common Vulnerabilities and Exposures

This release of FortiAI Ops is no longer vulnerable to the following.

Vulnerability	Description
CVE-2022-22963	In Spring Cloud Function versions 3.1.6, 3.2.2 and older unsupported versions, when using routing functionality it is possible for a user to provide a specially crafted SpEL as a routing-expression that may result in remote code execution and access to local resources.

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



www.fortinet.com

Copyright© 2022 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.