FortiAIOps

Highlights

- Extensive Network Visibility
- AI-powered Insights
- Robust Troubleshooting Tools
- Reduced Trouble Tickets
- Reported Results
- Lower TCO

Artificial Intelligence and Machine Learning Enhance Network Operations

FortiAIOps simplifies LAN and WAN network management and leverages artificial intelligence with machine learning for enhanced network operations.

FortiAIOps delivers a simple and easy means to manage a Fortinet networking stack (FortiAP, FortiSwitch, FortiGate, and FortiExtender). Network monitoring functionality gives visibility and in-depth understanding at your fingertips. From Layer 1 diagnostic information to Layer 7 application visibility, FortiAIOps covers Wi-Fi, Ethernet, SD-Wan, and 5G/LTE Gateway. Built-in troubleshooting tools enable active testing of network components to find faults and verify functionality.

The built-in Artificial Intelligence engine uses machine learning to catch issues, solve problems, and prevent network degradation. Artificial Intelligence can systematically consume the extensive amount of data being produced throughout the Security Fabric, correlate it, and analyze the results with Machine Learning so that you don't have to.

FortiAIOps is available as a virtual machine. In all deployment scenarios it works natively with Fortinet NOC and SOC tools to unify and simplify the way you manage the Fortinet Security Fabric.

Available in

Virtual

Key Features and Benefits

- Extensive Network Visibility: Monitoring and reporting of WLAN, LAN, SD-WAN, 5G/LTE Gateway

- AI-Powered Insights: Cross correlate events and data from across the deployment to quickly identify issues

- Robust Troubleshooting Tools: Built in tools to validate your deployment at any network level

- Reduced Trouble Tickets: Identify and correct issues before they start impacting users

- Reported Results: Delivers reporting and historical visibility

- Lower TCO: Reduce the amount of time staring at management screens or trying to resolve issues

Monitoring

Key Functions

- Comprehensive real-time and historical performance trends dashboards including RF metrics for a centralized view

- Quick and easy navigation with information no more than two clicks away

- Real-time network visualization enables remote management and saves on-site truck-roll expenses

- Current and historical metrics enable rapid resolution of issues by rewinding and recreating past state

- Customized dashboards allow any time, anywhere management of the network

Simplified Dashboard

- With a simplified dashboard setup, FortiAIOps allows the user to quickly get a read on their network health including Wi-Fi, Ethernet, and SD-WAN, and whether there is anything that needs attention.

Monitor Desired Service Levels

Use trending information and configured SLAs determine the good or bad health of your network

Minimal Network Impact

FortiAIOps leverages the same logs that FortiAnalyzer is already collecting, meaning there is no additional overhead on your network to add Artificial Intelligence to the Security Fabric. This activity is another benefit of a combined platform approach to Security-Driven Networking.

Topology Navigation

FortiAIOps leverages Fortinet Security Fabric integration to give you a visualization of your network at the point of an issue to understand the scope and implications of issues found.
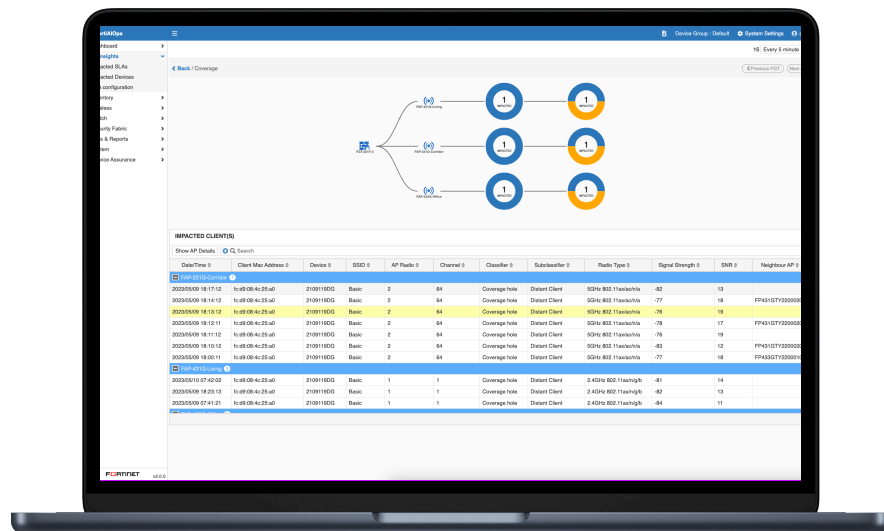
Network Heatmaps

Get visibility into the current state of your deployment with live heatmaps. Various network metrics can be visualized including signal strength, Throughput, Loss, Channel Utilization, or Number of Stations. Set thresholds to view only those areas passing important criteria or roll back the clock to see how things looked in the past.
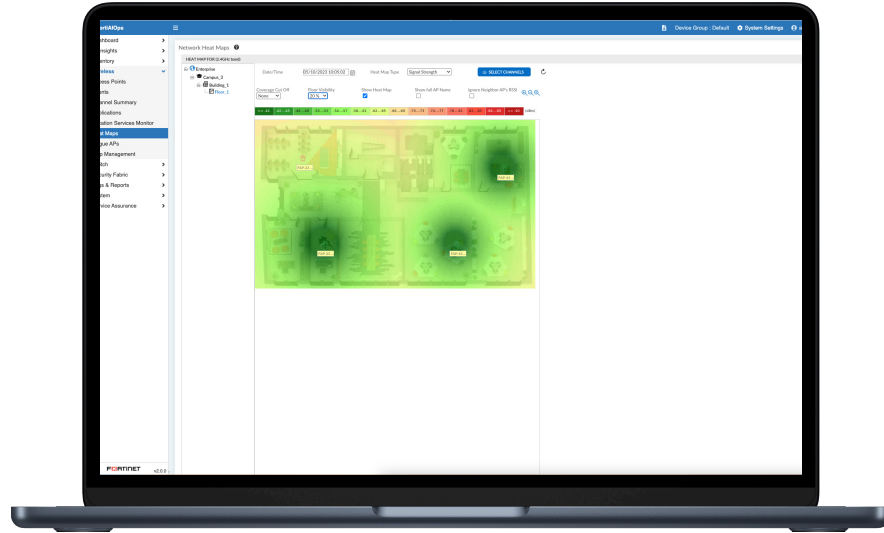
Application Monitoring

Get insights into what people are doing on your network with FortiAIOPs's DPI Application Monitoring feature. All detected or blocked applications will be listed with trend views available.
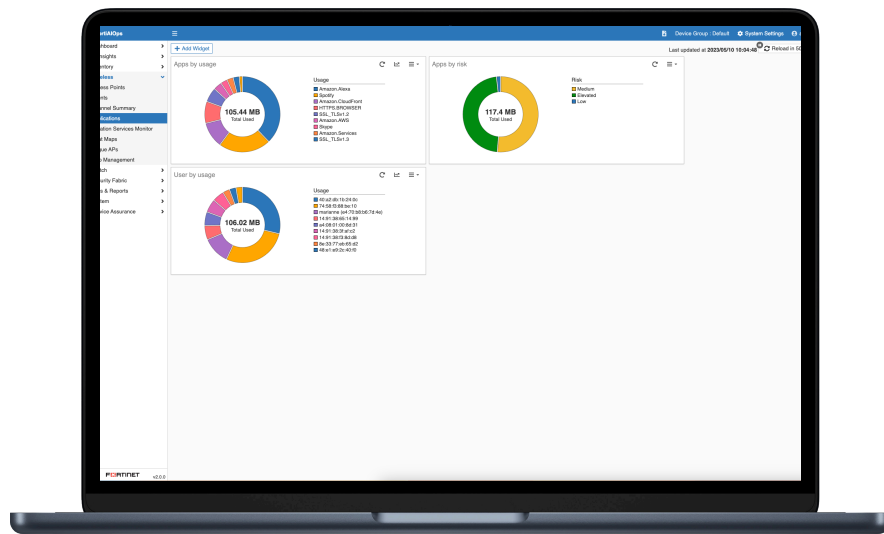
Troubleshooting

Key Functions

- Network testing toolkit allows for issue research and verification of performance
- Service Assurance testing validates that SLAs are being met, even across wireless medium
- Deep information analysis down to the port or RF level

Get Answers Quick or See Details if Desired

With the tools available within, you can quickly get remediation suggestions for detected network issues. But if you want to dive in further, FortiAIOps will take you directly to the information you're interested in and let you dive as deep as you want into logged information about the device.

Spectrum Analyzer

Detect, classify, and manage wireless interference. Spectrum Manager gathers interference data from a network of dedicated sensors. It can also gather data from the APs which can dedicate one of its radios to act as a sensor.

Wireless Assurance

Validate the network from the RF side by using an AP as a client to attach to the network and verify all networking services are behaving as expected.
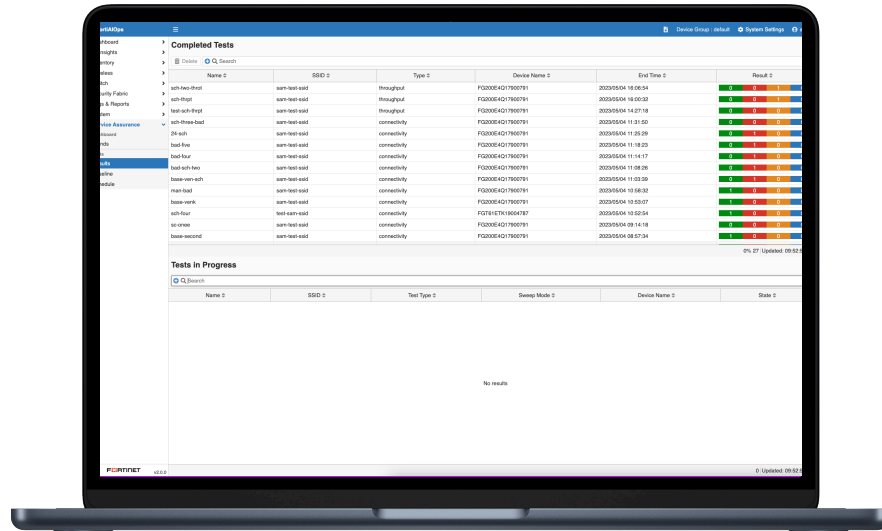
Cable Test

- Find the true problem in your wired network
- Eliminate bad cables as the source of frustrating performance problems. Wired Cable Test tool allows you to verify that the cabling in your installation is valid and doesn't have issues.

AI Insights with Machine Learning

The AI Engine combs through all your data and pulls out key items that need attention, giving you drill down focus on problems and easy solutions to complex issues. Machine Learning can determine what's normal for your network and your traffic, then keep that performance across time.
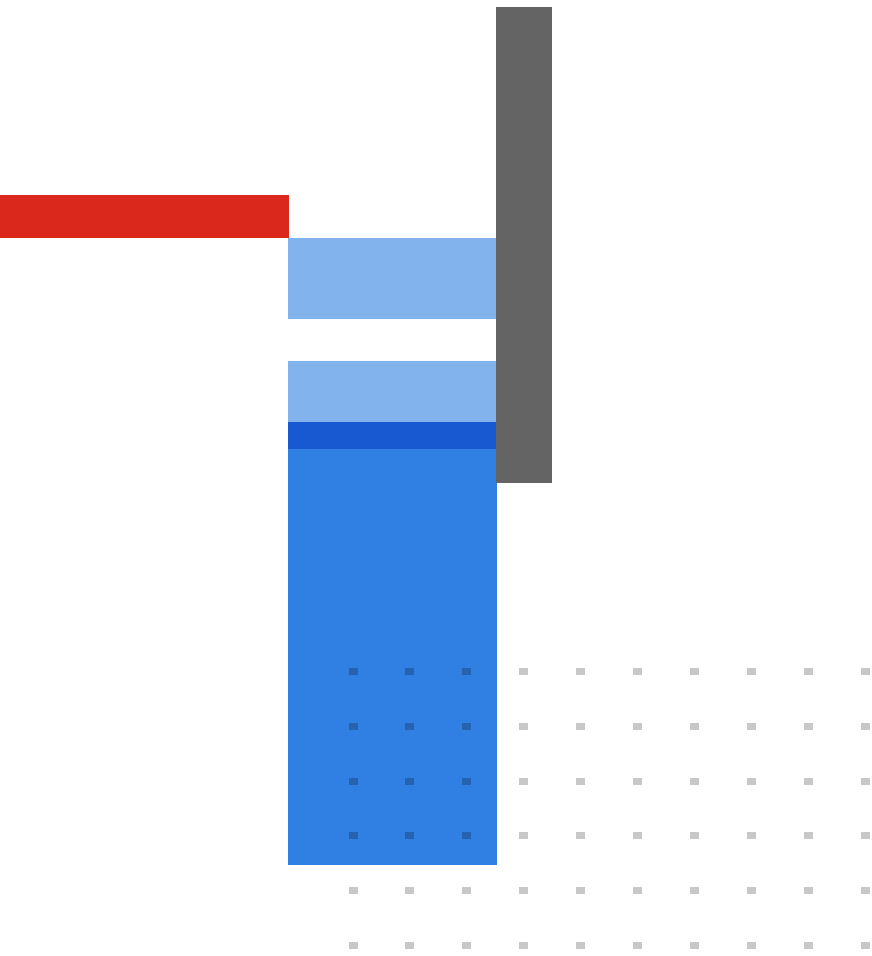
Ordering Information

FortiAIOps offers subscriptions for Monitoring, AI Insights, or SD-WAN. For Monitoring or AI Insights, licensing is by number of extension devices (FortiSwitch or FortiAP), for SD-WAN licensing is by FortiGate devices. A bundle of both Monitoring and AI Insights is available as well.

Service Category	SKU	Description
FortiAIOps Monitoring	FC1-10-AOVMS-668-01-DD	FortiAIOps Monitoring subscription for 25 extension device. Includes FortiCare Premium
	FC2-10-AOVMS-668-01-DD	FortiAIOps Monitoring subscription for 500 extension device. Includes FortiCare Premium
	FC3-10-AOVMS-668-01-DD	FortiAIOps Monitoring subscription for 2000 extension device. Includes FortiCare Premium
	FC4-10-AOVMS-668-01-DD	FortiAIOps Monitoring subscription for 10000 extension device. Includes FortiCare Premium
FortiAIOps AI Insights	FC1-10-AOVMS-669-01-DD	FortiAIOps AI Insights subscription for 25 extension device. Includes FortiCare Premium
	FC2-10-AOVMS-669-01-DD	FortiAIOps AI Insights subscription for 500 extension device. Includes FortiCare Premium
	FC3-10-AOVMS-669-01-DD	FortiAIOps AI Insights subscription for 2000 extension device. Includes FortiCare Premium
	FC4-10-AOVMS-669-01-DD	FortiAIOps AI Insights subscription for 10000 extension device. Includes FortiCare Premium
FortiAIOps Monitoring and AI Insights Bundle	FC1-10-AOVMS-670-01-DD	FortiAIOps Monitoring and AI Insights subscription BUNDLE for 25 extension device. Includes FortiCare Premium
	FC2-10-AOVMS-670-01-DD	FortiAIOps Monitoring and AI Insights subscription BUNDLE for 500 extension device. Includes FortiCare Premium
	FC3-10-AOVMS-670-01-DD	FortiAIOps Monitoring and AI Insights subscription BUNDLE for 2000 extension device. Includes FortiCare Premium
	FC4-10-AOVMS-670-01-DD	FortiAIOps Monitoring and AI Insights subscription BUNDLE for 10000 extension device. Includes FortiCare Premium
FortiAIOps SD-WAN	FC1-10-AOVMS-671-01-DD	FortiAIOps SD-WAN subscription for 25 FortiGate device. Includes FortiCare Premium
	FC2-10-AOVMS-671-01-DD	FortiAIOps SD-WAN subscription for 500 FortiGate device. Includes FortiCare Premium
	FC3-10-AOVMS-671-01-DD	FortiAIOps SD-WAN subscription for 2000 FortiGate device. Includes FortiCare Premium
	FC4-10-AOVMS-671-01-DD	FortiAIOps SD-WAN subscription for 10000 FortiGate device. Includes FortiCare Premium

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.

May 17, 2023