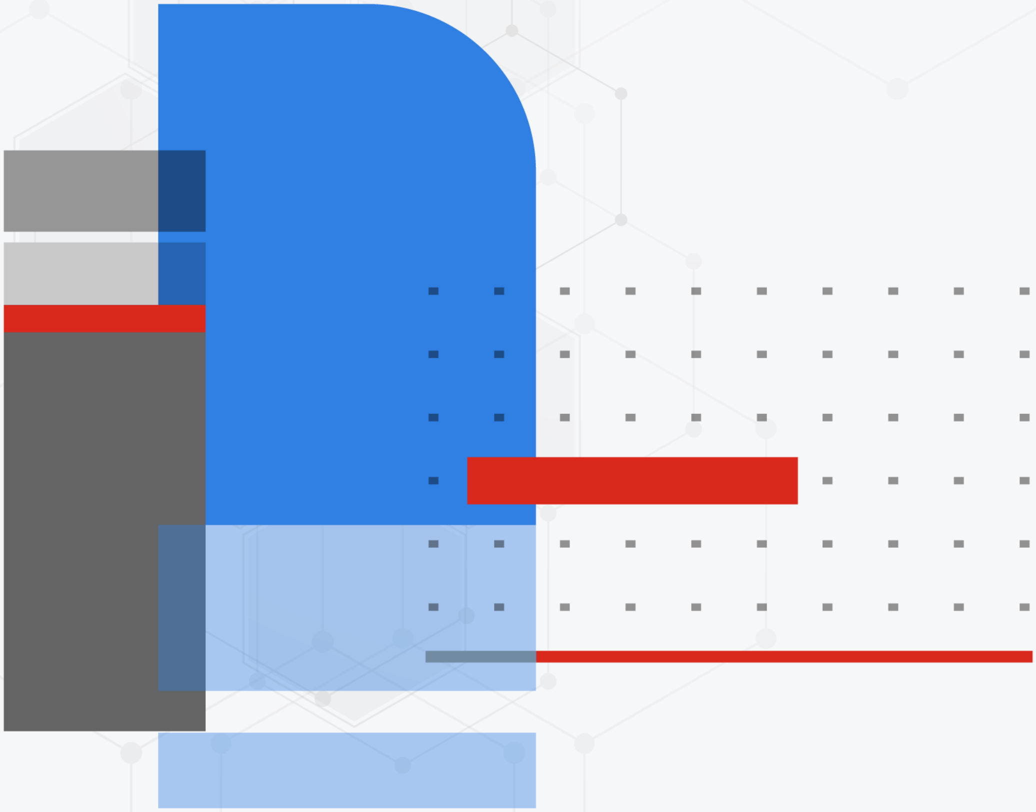
New Features

FortiAIOps 3.0.0



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 01, 2025
FortiAIOps 3.0.0 New Features
83-300-1145597-20250701

TABLE OF CONTENTS

Change log 4
FortiAI: Intelligent Network Assistance 5
Customizable Dashboards 12
WIDS Security Analytics 16
SD-WAN SLA Enhancements 20
SD-WAN Monitoring and Insights 21
SD-WAN Events Chart in SD-WAN Dashboard 29
Channel Summary 31
Export Table in Different Formats 37
Remote Admin Authentication 38
CLI and GUI Profile Consistency 45
Time Range Updates for AI Insights Pages 46
Intelligent Anomaly Detection for Wired SLA 47
Quick Cable Testing for Switches in AI Insights 48
Switch Monitoring Enhancements 49
User Sessions Management 50
Dashboard and Navigation Enhancements 51
Diagnostic Tool from CLI 52
Others 53

Change log

Date	Change description
2025-07-01	FortiAIOps 3.0.0 release document.

FortiAI: Intelligent Network Assistance

FortiAI is a generative AI assistant integrated into the FortiAIOps platform. It simplifies network management by translating your natural language questions into actionable intelligence. From real-time diagnostics and performance monitoring to complex troubleshooting and step-by-step configuration help, FortiAI provides comprehensive support across your entire wireless, wired, and SD-WAN environments.

Following are some of the key capabilities of FortiAI:

- Utilize natural language to monitor network health, identify stability issues like port flaps, troubleshoot specific client or device problems, and receive step-by-step configuration guidance using simple queries. Responses are delivered in multiple formats, including tabular data and plain text, with information pulled directly from your FortiAIOps environment.
- Leverage a powerful AI and Machine Learning (ML) engine that ingests and analyzes data from FortiGates, FortiAPs, and FortiSwitches. FortiAI uses this information to diagnose network issues, identify potential root causes, and to suggest clear, remedial steps to accelerate resolution.
- Continuously recalculate performance baselines and SLA thresholds for the network, client connection quality, and the Radio Frequency (RF) environment. This allows for precise, context-aware anomaly detection that adapts to network changes over time.
- Identify network slowdowns, throughput bottlenecks, and potential configuration issues to maximize network uptime. The mean time to diagnose and resolve issues is greatly reduced, freeing up critical administrative resources.

In this release, FortiAI is available to all customers as a **Beta** feature and includes a grant of 5 million tokens for use.

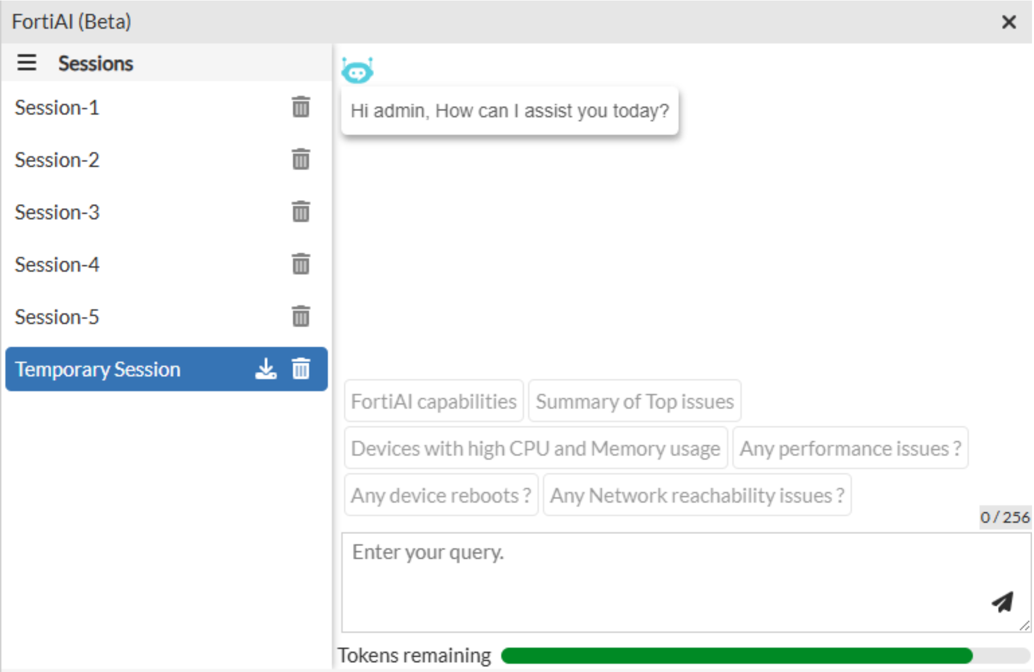
This section includes the following topics:

- Accessing FortiAI
- FortiAI Capabilities
- FortiAI Pane
- FortiAI Example Tasks

Accessing FortiAI

Note: FortiAI requires an active internet connection and a valid DNS configuration to function correctly.

Click the **FortiAI** icon located in the FortiAIOps GUI banner to open the assistant pane.



Hi admin, How can I assist you today?

Note: If you log out, close, or reload your session, you will not be able to continue your current thread in the Temporary Session. History is retained in the other sessions.

FortiAI Capabilities

The capabilities of FortiAI in FortiAIOps can be categorized into the following areas:

Category	Description
Wireless Troubleshooting	Monitor access point health (power, CPU, performance), troubleshoot specific client connectivity issues, and analyze the RF environment for interference.
Wired Network Diagnostics	Diagnose physical layer issues such as port flaps, down ports, and cable faults, while also monitoring overall switch bandwidth and throughput performance.
SD-WAN Health	Track real-time SD-WAN health by identifying top issues, overlay failures, interface performance degradation, and recent SLA health check breaches.
Configuration and Task Support	Receive instructions for common administrative tasks, and platform configuration.

FortiAI Pane

The FortiAI pane includes the following:

Section	Description
Sessions	Continuous conversation that maintains context, allowing you to ask follow-up questions about previously discussed information until the session ends

Section	Description
	by logging out, closing the window, or reloading.
Thread	A chronological record of prompts and responses within a single session of the FortiAI assistant.
Prompt	An instruction or question you provide to the FortiAI assistant. It can be a query that you type yourself, or a pre-defined suggestion that you select to request common information or actions.
Token remaining	Displays your current token usage out of your total allotment.

FortiAI Example Tasks

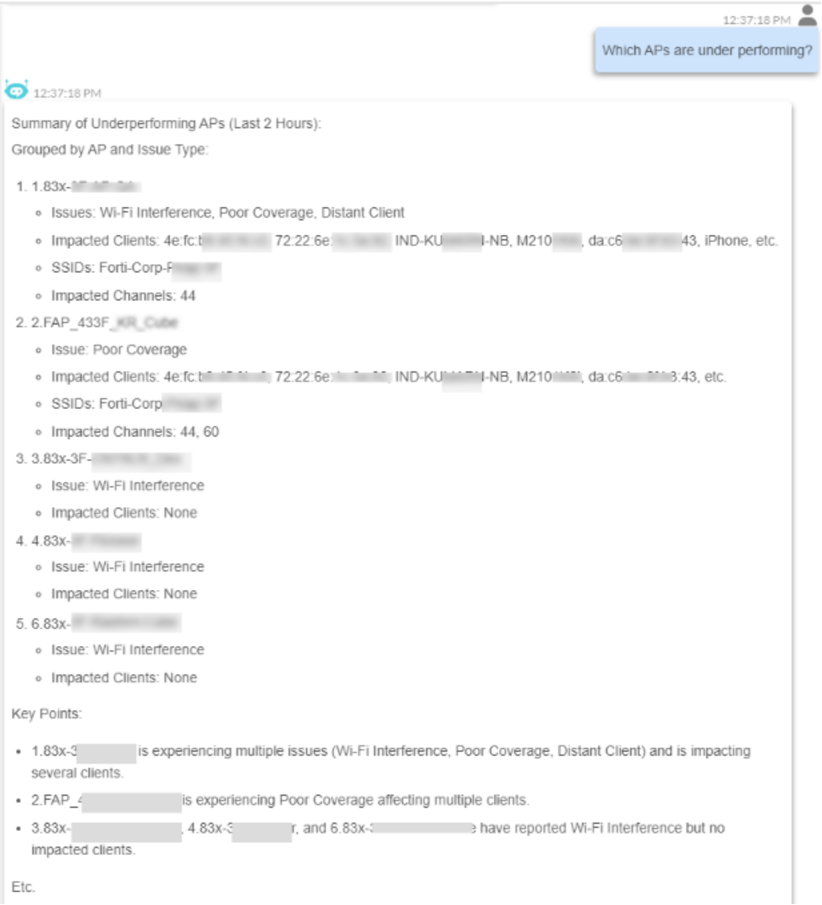
The following are some example tasks that can be performed using the FortiAI assistant:

Example 1: Finding under performing Access Points

Use FortiAI to identify which active Access Points (APs) are causing a poor user experience.

FortiAI analyzes a wide range of performance metrics for every AP and compares them against a performance baseline. It then flags any AP that deviates significantly from these healthy norms.

Prompt: Which APs are under performing?



12:37:18 PM

Which APs are under performing?

12:37:18 PM

Summary of Underperforming APs (Last 2 Hours):

Grouped by AP and Issue Type:

1. 1.83x-[redacted]
   - Issues: Wi-Fi Interference, Poor Coverage, Distant Client
   - Impacted Clients: 4e:fc:b[redacted] 72:22:6e[redacted] IND-KU[redacted]-NB, M210[redacted], da:c6[redacted]43, iPhone, etc.
   - SSIDs: Forti-Corp-[redacted]
   - Impacted Channels: 44
2. 2.FAP_433F[redacted]
   - Issue: Poor Coverage
   - Impacted Clients: 4e:fc:b[redacted] 72:22:6e[redacted] IND-KU[redacted]-NB, M210[redacted], da:c6[redacted]3:43, etc.
   - SSIDs: Forti-Corp[redacted]
   - Impacted Channels: 44, 60
3. 3.83x-3F-[redacted]
   - Issue: Wi-Fi Interference
   - Impacted Clients: None
4. 4.83x-[redacted]
   - Issue: Wi-Fi Interference
   - Impacted Clients: None
5. 6.83x-[redacted]
   - Issue: Wi-Fi Interference
   - Impacted Clients: None

Key Points:

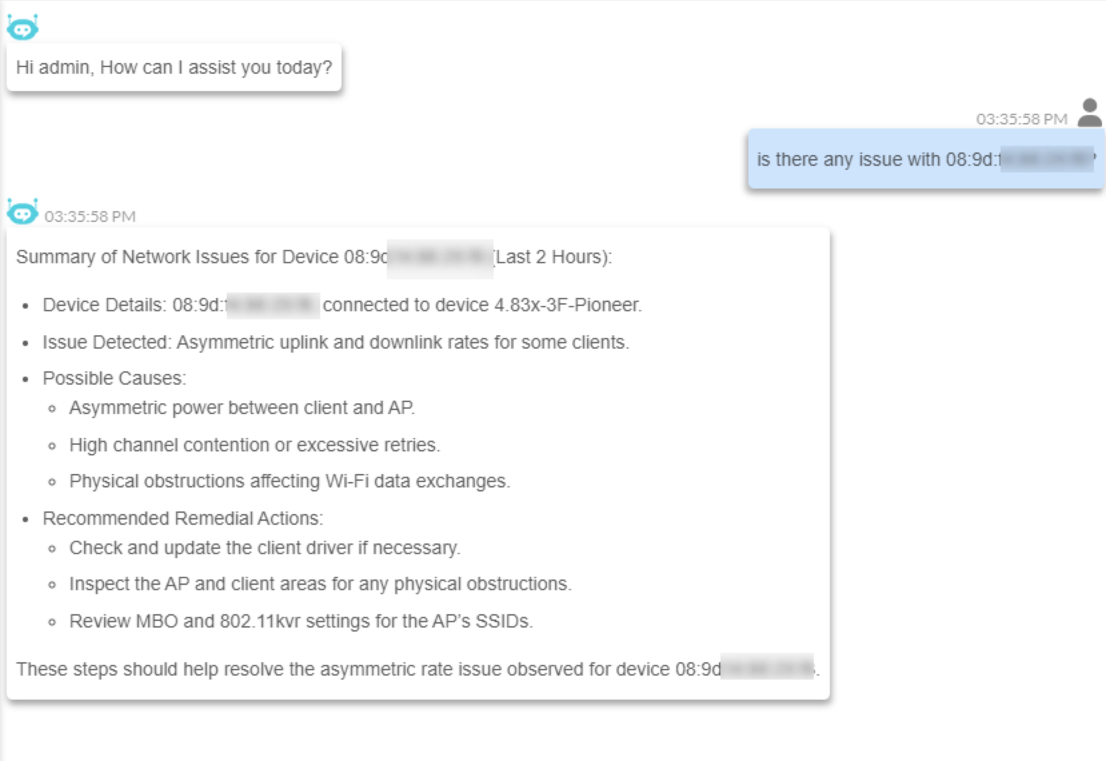
- 1.83x-[redacted] is experiencing multiple issues (Wi-Fi Interference, Poor Coverage, Distant Client) and is impacting several clients.
- 2.FAP_[redacted] is experiencing Poor Coverage affecting multiple clients.
- 3.83x-[redacted], 4.83x-[redacted], and 6.83x-[redacted] have reported Wi-Fi Interference but no impacted clients.

Etc.

Example 2: Diagnosing Device-Specific Issues

You can use FortiAI to diagnose network issues affecting a specific device. FortiAI will identify if a problem exists, provide a list of possible root causes, and recommend actionable steps to resolve the issue.

Prompt: Is there any issue with <MAC address>?



Hi admin, How can I assist you today?

03:35:58 PM

is there any issue with 08:9d:[redacted]

03:35:58 PM

Summary of Network Issues for Device 08:9d[redacted] (Last 2 Hours):

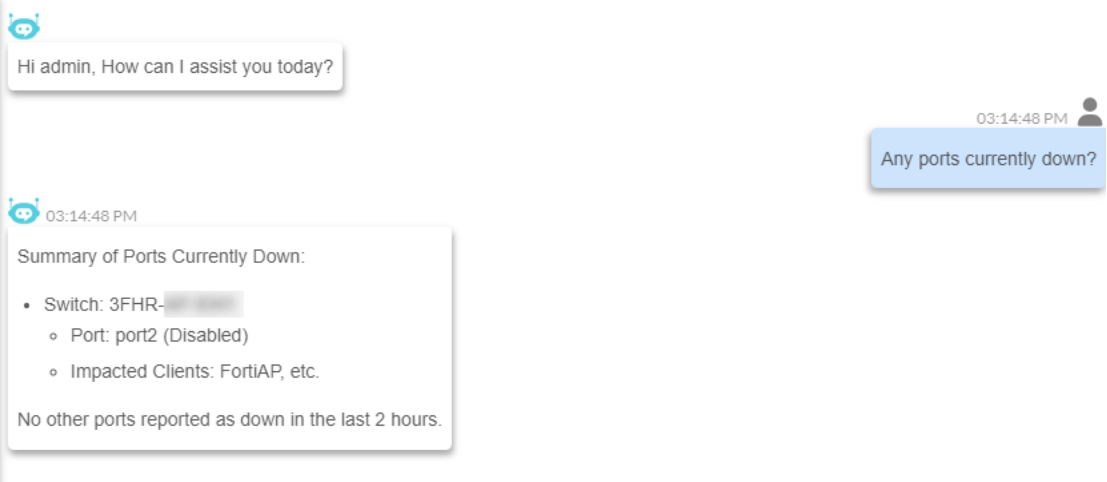
- Device Details: 08:9d:[redacted] connected to device 4.83x-3F-Pioneer.
- Issue Detected: Asymmetric uplink and downlink rates for some clients.
- Possible Causes:
  - Asymmetric power between client and AP.
  - High channel contention or excessive retries.
  - Physical obstructions affecting Wi-Fi data exchanges.
- Recommended Remedial Actions:
  - Check and update the client driver if necessary.
  - Inspect the AP and client areas for any physical obstructions.
  - Review MBO and 802.11kvr settings for the AP's SSIDs.

These steps should help resolve the asymmetric rate issue observed for device 08:9d[redacted].

Example 3: Outage Detection and Impact Analysis

FortiAI reports when any network component such as a device, port, access point, or SD-WAN link is down. The information includes specific details of the offline component and an analysis of the impact caused by the outage.

Prompt: Are any ports currently down?



Hi admin, How can I assist you today?

03:14:48 PM

Any ports currently down?

03:14:48 PM

Summary of Ports Currently Down:

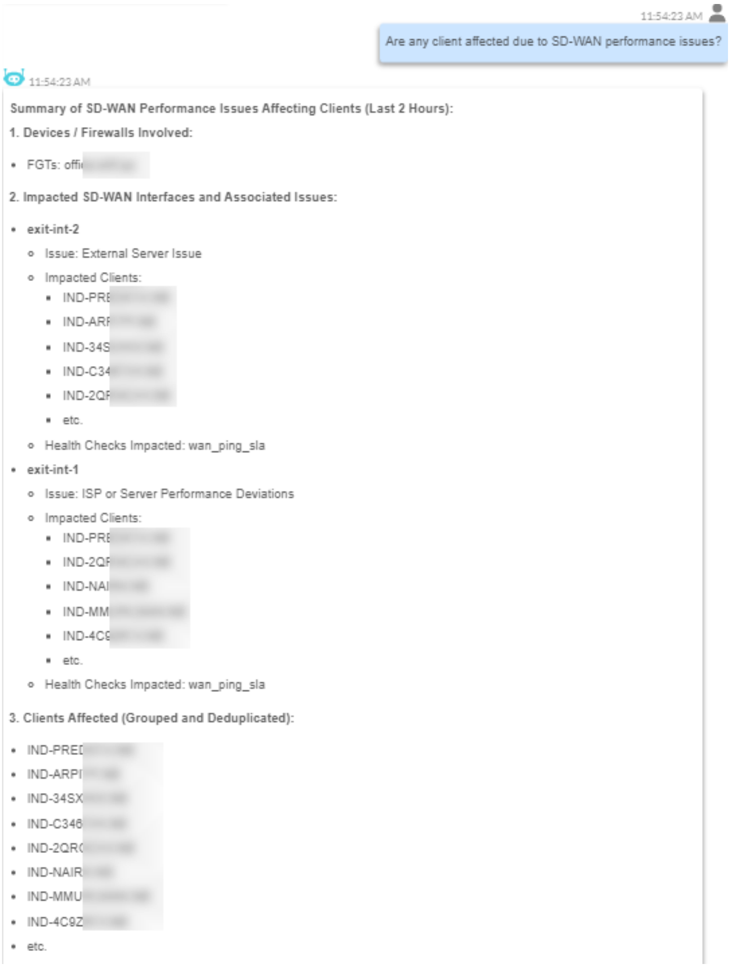
- Switch: 3FHR-[redacted]
  - Port: port2 (Disabled)
  - Impacted Clients: FortiAP, etc.

No other ports reported as down in the last 2 hours.

Example 4: Analyze Client Impact due to SD-WAN Performance Issue

FortiAI can determine how specific SD-WAN performance issues impact clients. It reports the type of performance issue, devices impacted and the list of clients impacted by the issue. This information is grouped by the SD-WAN issue for clear, concise analysis and efficient troubleshooting.

Prompt: Are any clients affected due to SD-WAN performance issues?



11:54:23 AM

Are any client affected due to SD-WAN performance issues?

11:54:23 AM

Summary of SD-WAN Performance Issues Affecting Clients (Last 2 Hours):

1. Devices / Firewalls Involved:

- FGTs: offi[redacted]

2. Impacted SD-WAN Interfaces and Associated Issues:

- **exit-int-2**
  - Issue: External Server Issue
  - Impacted Clients:
    - IND-PRE[redacted]
    - IND-ARF[redacted]
    - IND-34S[redacted]
    - IND-C34[redacted]
    - IND-2QF[redacted]
    - etc.
  - Health Checks Impacted: wan_ping_sla
- **exit-int-1**
  - Issue: ISP or Server Performance Deviations
  - Impacted Clients:
    - IND-PRE[redacted]
    - IND-2QF[redacted]
    - IND-NAI[redacted]
    - IND-MM[redacted]
    - IND-4C9[redacted]
    - etc.
  - Health Checks Impacted: wan_ping_sla

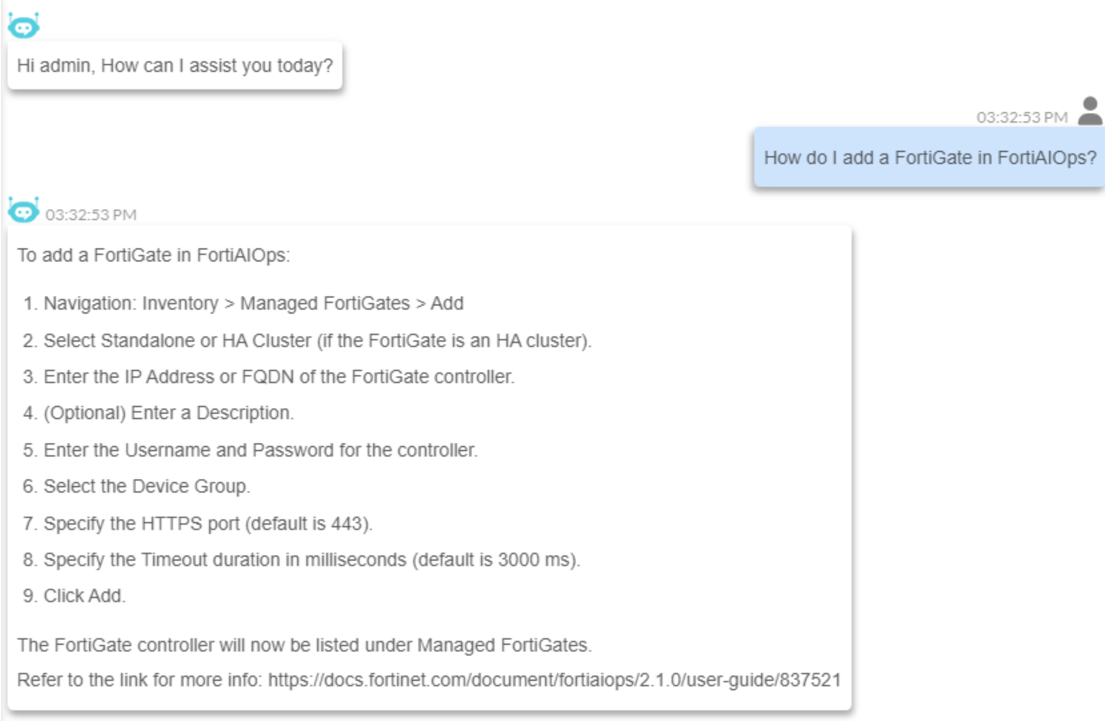
3. Clients Affected (Grouped and Deduplicated):

- IND-PRED[redacted]
- IND-ARPI[redacted]
- IND-34SX[redacted]
- IND-C346[redacted]
- IND-2QR[redacted]
- IND-NAIR[redacted]
- IND-MMU[redacted]
- IND-4C9Z[redacted]
- etc.

Example 5: Assistance with Device Setup

FortiAI can provide step-by-step instructions for adding a device, sourcing this information directly from the FortiAIOps documentation. It lists all the necessary steps and includes a link to the relevant documentation for further details.

Prompt: How do I add a FortiGate in FortiAIOps?



Hi admin, How can I assist you today?

03:32:53 PM

How do I add a FortiGate in FortiAIOps?

03:32:53 PM

To add a FortiGate in FortiAIOps:

1. Navigation: Inventory > Managed FortiGates > Add
2. Select Standalone or HA Cluster (if the FortiGate is an HA cluster).
3. Enter the IP Address or FQDN of the FortiGate controller.
4. (Optional) Enter a Description.
5. Enter the Username and Password for the controller.
6. Select the Device Group.
7. Specify the HTTPS port (default is 443).
8. Specify the Timeout duration in milliseconds (default is 3000 ms).
9. Click Add.

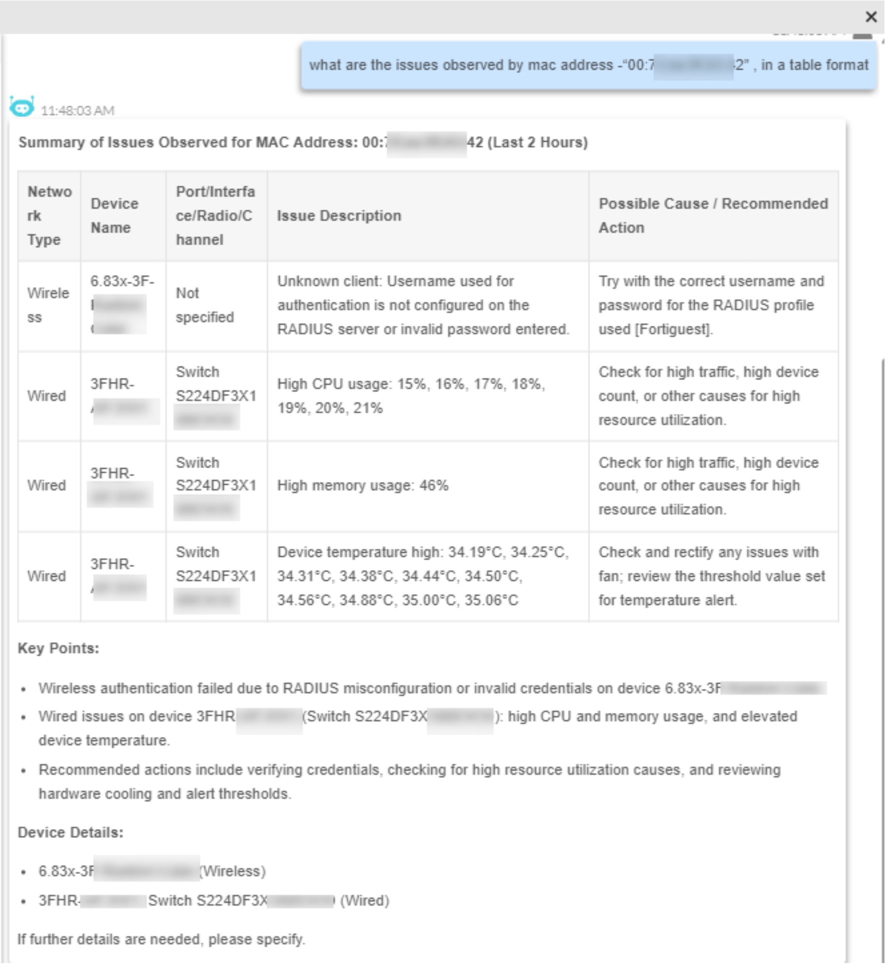
The FortiGate controller will now be listed under Managed FortiGates.

Refer to the link for more info: https://docs.fortinet.com/document/fortiaiops/2.1.0/user-guide/837521

Example 6: Tabular Format Display

FortiAI can provide the necessary details and analysis in a table format for easier handling of data. The complex network data is presented in a more user-friendly that minimizes effort and maximizes understanding of the information.

Prompt: What are the issues observed by mac address <IP address> in a table format?



what are the issues observed by mac address -“00:7[redacted]2” , in a table format

Summary of Issues Observed for MAC Address: 00:7[redacted]42 (Last 2 Hours)

Network Type	Device Name	Port/Interface/Radio/Channel	Issue Description	Possible Cause / Recommended Action
Wireless	6.83x-3F-[redacted]	Not specified	Unknown client: Username used for authentication is not configured on the RADIUS server or invalid password entered.	Try with the correct username and password for the RADIUS profile used [Fortiguest].
Wired	3FHR-[redacted]	Switch S224DF3X1[redacted]	High CPU usage: 15%, 16%, 17%, 18%, 19%, 20%, 21%	Check for high traffic, high device count, or other causes for high resource utilization.
Wired	3FHR-[redacted]	Switch S224DF3X1[redacted]	High memory usage: 46%	Check for high traffic, high device count, or other causes for high resource utilization.
Wired	3FHR-[redacted]	Switch S224DF3X1[redacted]	Device temperature high: 34.19°C, 34.25°C, 34.31°C, 34.38°C, 34.44°C, 34.50°C, 34.56°C, 34.88°C, 35.00°C, 35.06°C	Check and rectify any issues with fan; review the threshold value set for temperature alert.

Key Points:

- Wireless authentication failed due to RADIUS misconfiguration or invalid credentials on device 6.83x-3F[redacted]
- Wired issues on device 3FHR[redacted](Switch S224DF3X[redacted]): high CPU and memory usage, and elevated device temperature.
- Recommended actions include verifying credentials, checking for high resource utilization causes, and reviewing hardware cooling and alert thresholds.

Device Details:

- 6.83x-3F[redacted](Wireless)
- 3FHR-[redacted] Switch S224DF3X[redacted] (Wired)

If further details are needed, please specify.

Customizable Dashboards

This release introduces personalized dashboards. You now have the flexibility to customize your dashboard experience—modify existing layouts by adding or deleting widgets, or create entirely new dashboards with your preferred widgets.

The following customization options are available:

- Create a New Dashboard
- Modify an Existing Dashboard
- Delete a Dashboard
- Rearrange the Dashboards
- Reset Dashboard Section

Note: Customizations are saved across navigations, logouts, reboots, and upgrades, and are specific to each user.

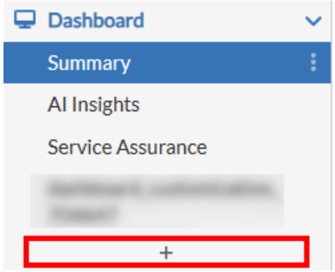
The widget library has also been improved for a more seamless user experience. For more information, see Manage Dashboard Widgets.

Create a New Dashboard

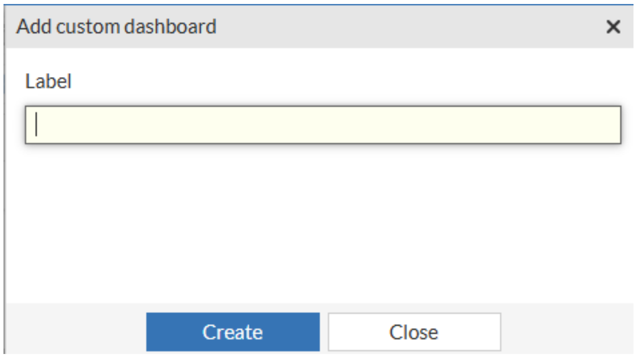
You can now create new custom dashboards and add widgets from the widget library.

To create a new dashboard:

1. On the left navigation pane, select **Dashboard** and click **+**.



2. In the **Add custom dashboard** pane, enter a name for the dashboard in the **Label** field.



3. Click **Create**.
   Add widgets to the newly created dashboard. See Modify an Existing Dashboard.

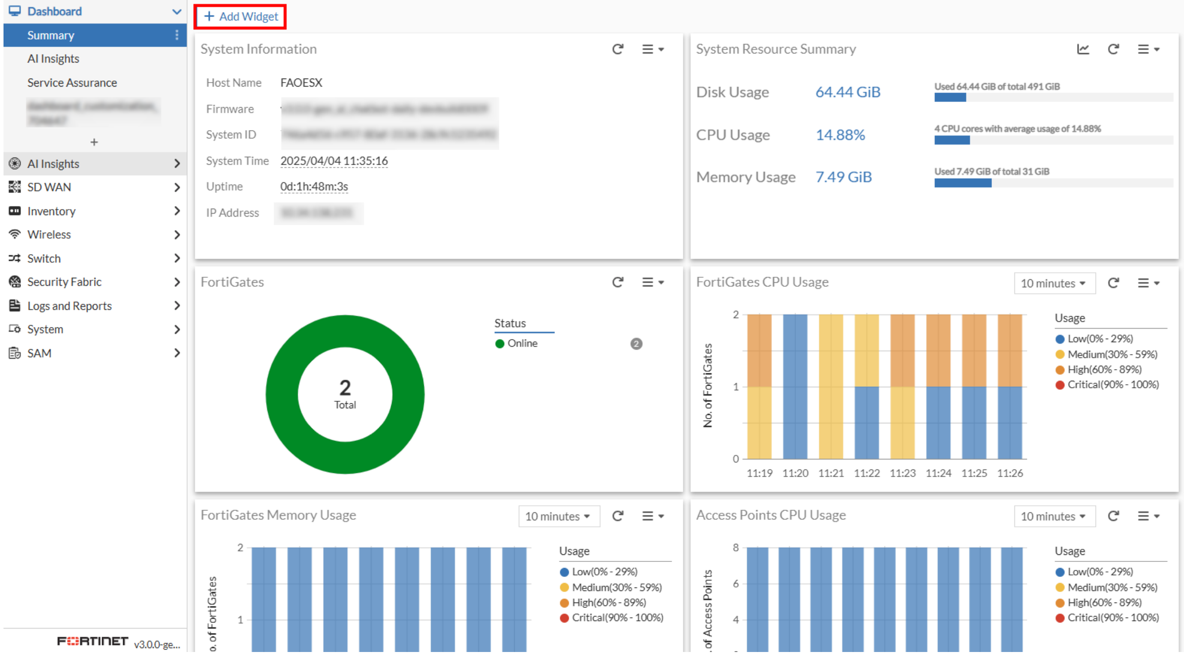
Modify an Existing Dashboard

You can customize both existing dashboards and default dashboards by adding/deleting widgets or renaming the dashboards.

Note: You can add a maximum of 20 widgets in a dashboard.

To add a widget to the dashboard:

1. Select the dashboard you want to modify.
2. On the right pane, click **Add Widget** to add required widgets from the widget library.



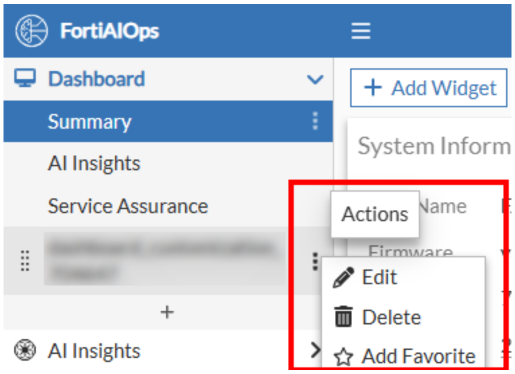
Host Name FAOESX
Firmware [redacted]
System ID [redacted]
System Time 2025/04/04 11:35:16
Uptime 0d:1h:48m:3s
IP Address [redacted]

Disk Usage 64.44 GiB — Used 64.44 GiB of total 491 GiB
CPU Usage 14.88% — 4 CPU cores with average usage of 14.88%
Memory Usage 7.49 GiB — Used 7.49 GiB of total 31 GiB

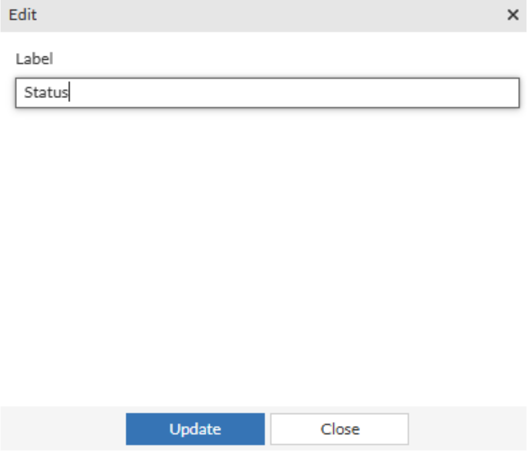
3. In the the **Manage Dashboard Widgets** pane, hover on the widget name to select the required widget and click +.
   For more information on widget library, see Manage Dashboard Widgets
4. Click **Close** to close the pane once the widgets are selected.
5. Click **Reset dashboard layout** to clear all the widgets added to the dashboard.

To change the name/label of the dashboard:

1. Select a dashboard and from the Actions menu click **Edit**.



2. Change the name of the dashboard in the **Label** field and click **Update**.

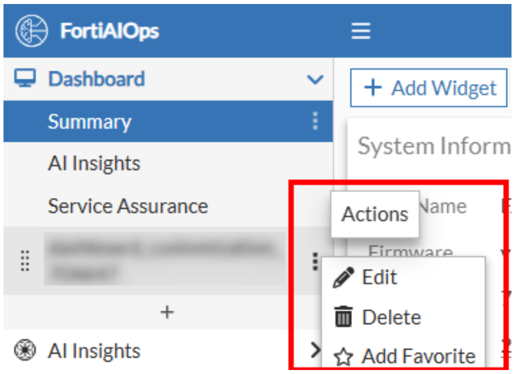


Status

Delete a Dashboard

Both default dashboards and user-added dashboards can be deleted.

Select the dashboard to be deleted and from the **Actions** menu click **Delete**.



Note: Dashboards once deleted cannot be recovered.

Rearrange the Dashboards

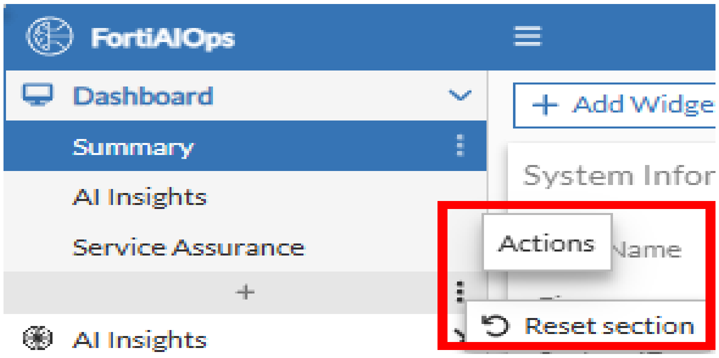
You can move a dashboard up or down to rearrange the dashboard list.

To rearrange your dashboards, click and drag a dashboard up or down in the list.

Reset Dashboard Section

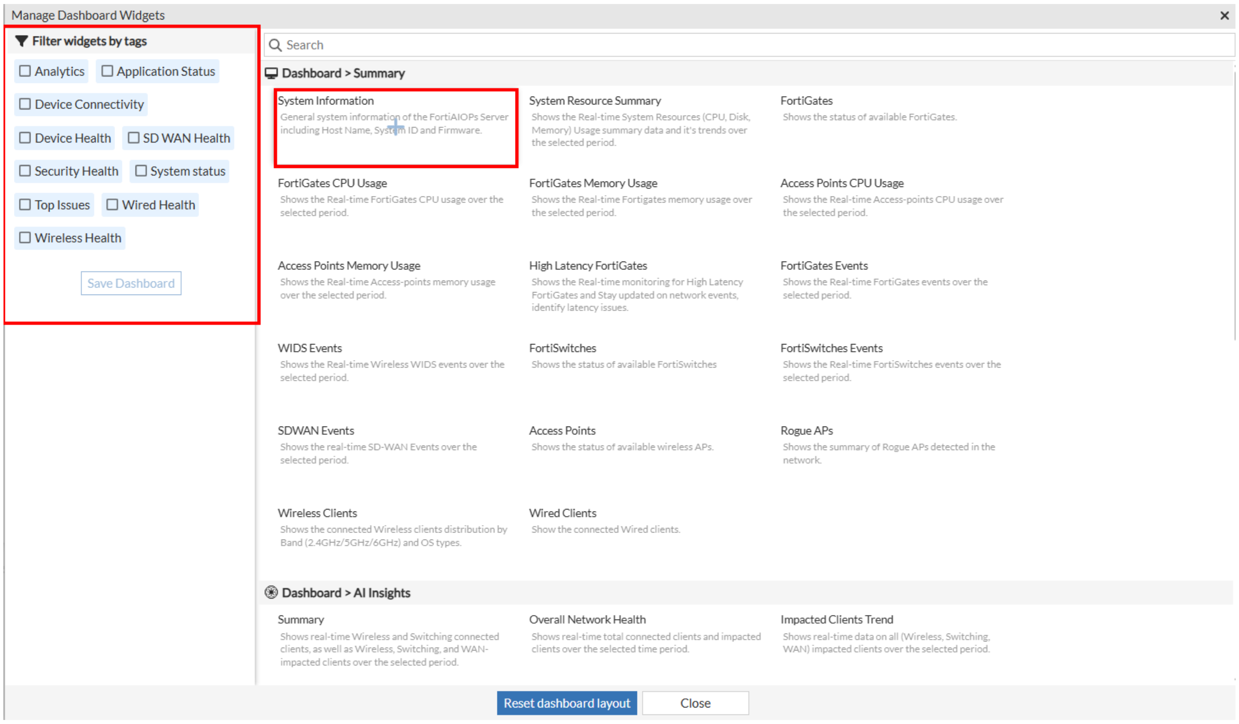
You can remove all your customized dashboards and revert to the default view.

Hover over **+** and from the **Actions** menu, click **Reset section**.



Manage Dashboard Widgets

The Manage Dashboard Widgets window is now enhanced for an improved user experience. The window now lists all available widgets for your dashboard in one place. Widgets are organized into categories such as Monitoring, AI-Insights, Service Assurance, SD-WAN, and Licensing. The left pane offers pre-defined filters to help you quickly locate the widgets you are looking for.



Dashboard > Summary

System Information

General system information of the FortiAIOPs Server including Host Name, System ID and Firmware.

System Resource Summary

Shows the Real-time System Resources (CPU, Disk, Memory) Usage summary data and it's trends over the selected period.

FortiGates

Shows the status of available FortiGates.

FortiGates CPU Usage

Shows the Real-time FortiGates CPU usage over the selected period.

FortiGates Memory Usage

Shows the Real-time Fortigates memory usage over the selected period.

Access Points CPU Usage

Shows the Real-time Access-points CPU usage over the selected period.

Access Points Memory Usage

Shows the Real-time Access-points memory usage over the selected period.

High Latency FortiGates

Shows the Real-time monitoring for High Latency FortiGates and Stay updated on network events, identify latency issues.

FortiGates Events

Shows the Real-time FortiGates events over the selected period.

WIDS Events

Shows the Real-time Wireless WIDS events over the selected period.

FortiSwitches

Shows the status of available FortiSwitches

FortiSwitches Events

Shows the Real-time FortiSwitches events over the selected period.

SDWAN Events

Shows the real-time SD-WAN Events over the selected period.

Access Points

Shows the status of available wireless APs.

Rogue APs

Shows the summary of Rogue APs detected in the network.

Wireless Clients

Shows the connected Wireless clients distribution by Band (2.4GHz/5GHz/6GHz) and OS types.

Wired Clients

Show the connected Wired clients.

Dashboard > AI Insights

Summary

Shows real-time Wireless and Switching connected clients, as well as Wireless, Switching, and WAN-impacted clients over the selected period.

Overall Network Health

Shows real-time total connected clients and impacted clients over the selected time period.

Impacted Clients Trend

Shows real-time data on all (Wireless, Switching, WAN) impacted clients over the selected period.

To clear all the widgets added to the dashboard, click **Reset dashboard layout**.

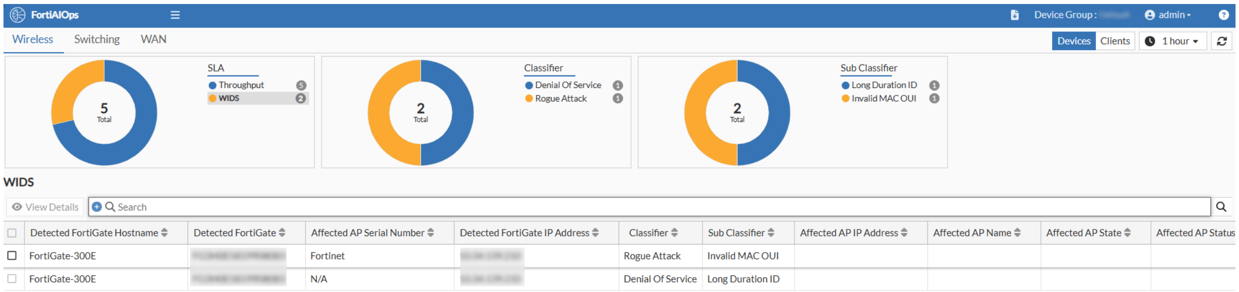
WIDS Security Analytics

This release introduces WIDS SLA which monitors and reports on potential events detected within the network by the WIDS (Wireless Intrusion Detection System) system. It detects security threats and recommends corrective actions to maintain network integrity, enhancing security with real-time alerts and actionable insights for faster threat resolution.

The following types of intrusion detection is available:

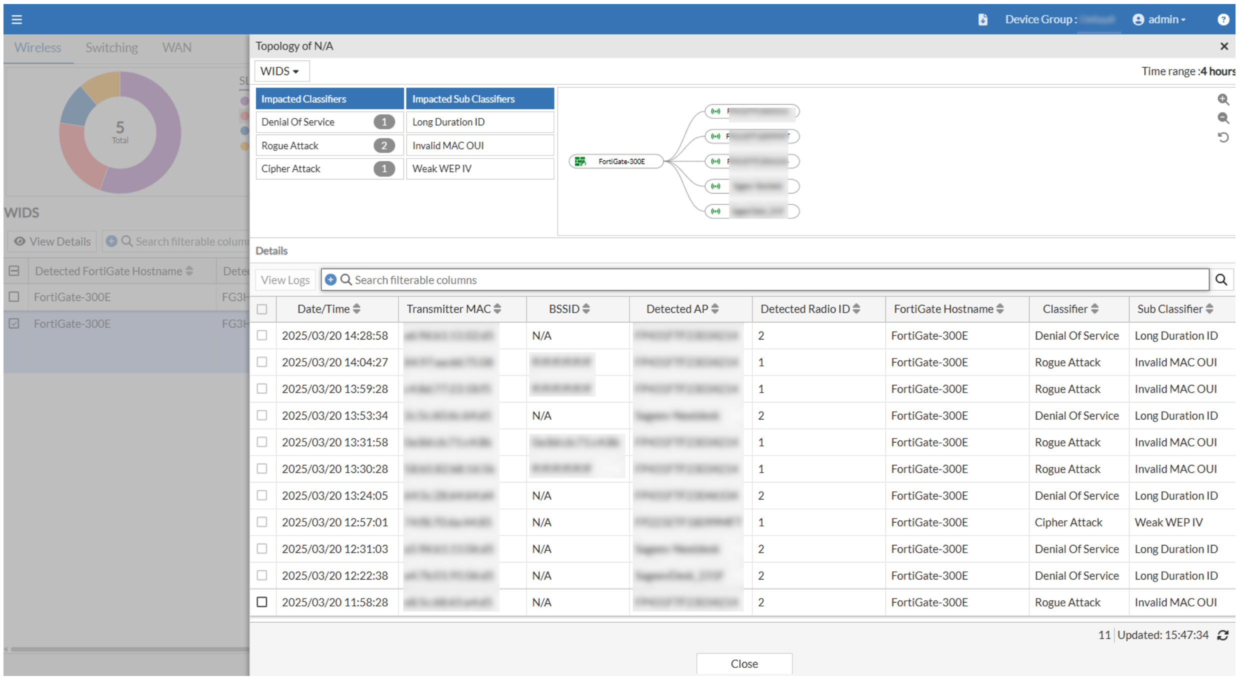
Intrusion Type	Description
Broadcast Deauthentication	This is a type of Denial of Service attack. A flood of spoofed de-authentication frames forces wireless clients to de-authenticate, then re-authenticate with their AP.
Long Duration ID	To share radio bandwidth, WiFi devices reserve channels for brief periods of time. Excessively long reservation periods can be used as a denial of service attack. You can set a threshold between 1000 and 32 767 microseconds. The default is 8200.
Authentication Frame Flood	A Denial of Service attack using a large number of association requests. The default detection threshold is 30 requests in 10 seconds.
Association Frame Flood	A Denial of Service attack using a large number of association requests. The default detection threshold is 30 requests in 10 seconds.
Deauthentication Spoof	Spoofed de-authentication frames are a denial of service attack. They cause all clients to disconnect from the AP.
EAPOL Flood attacks	Extensible Authentication Protocol over LAN (EAPOL) packets are used in WPA and WPA2 authentication. Flooding the AP with these packets can be a denial of service attack. Several types of EAPOL packets are detected: EAPOL-FAIL, EAPOL-LOGOFF, EAPOL-START, EAPOL-SUCC.
Wireless Bridge Intrusion	WiFi frames with both the fromDS and ToDS fields set indicate a wireless bridge. This will also detect a wireless bridge that you intentionally configured in your network.
Null SSID Probe Response	When a wireless client sends out a probe request, the attacker sends a response with a null SSID. This causes many wireless cards and devices to stop responding.
Invalid Mac OUI	Some attackers use randomly-generated MAC addresses. The first three bytes of the MAC address are the Organizationally Unique Identifier (OUI), administered by IEEE. Invalid OUIs are logged.
Weak WEP IV	A primary means of cracking WEP keys is by capturing 802.11 frames over an extended period of time and searching for patterns of WEP initialization vectors (IVs) that are known to be weak. WIDS detects known weak WEP IVs in on-air traffic.
ASLEAP Attack	ASLEAP is a tool used to perform attacks against LEAP authentication.

Navigate to **Dashboard** > **Wireless.** WIDS SLA is displayed under **Wireless Insights** Widget or Donut



☐	Detected FortiGate Hostname	Detected FortiGate	Affected AP Serial Number	Detected FortiGate IP Address	Classifier	Sub Classifier	Affected AP IP Address	Affected AP Name	Affected AP State	Affected AP Status
☐	FortiGate-300E	[redacted]	Fortinet	[redacted]	Rogue Attack	Invalid MAC OUI				
☐	FortiGate-300E	[redacted]	N/A	[redacted]	Denial Of Service	Long Duration ID				

Select WIDS SLA from the chart and from the **WIDS** table select a row and click **View Details**.



Impacted Classifiers		Impacted Sub Classifiers
Denial Of Service	1	Long Duration ID
Rogue Attack	2	Invalid MAC OUI
Cipher Attack	1	Weak WEP IV

☐	Date/Time	Transmitter MAC	BSSID	Detected AP	Detected Radio ID	FortiGate Hostname	Classifier	Sub Classifier
☐	2025/03/20 14:28:58	[redacted]	N/A	[redacted]	2	FortiGate-300E	Denial Of Service	Long Duration ID
☐	2025/03/20 14:04:27	[redacted]	[redacted]	[redacted]	1	FortiGate-300E	Rogue Attack	Invalid MAC OUI
☐	2025/03/20 13:59:28	[redacted]	[redacted]	[redacted]	1	FortiGate-300E	Rogue Attack	Invalid MAC OUI
☐	2025/03/20 13:53:34	[redacted]	N/A	[redacted]	2	FortiGate-300E	Denial Of Service	Long Duration ID
☐	2025/03/20 13:31:58	[redacted]	[redacted]	[redacted]	1	FortiGate-300E	Rogue Attack	Invalid MAC OUI
☐	2025/03/20 13:30:28	[redacted]	[redacted]	[redacted]	1	FortiGate-300E	Rogue Attack	Invalid MAC OUI
☐	2025/03/20 13:24:05	[redacted]	N/A	[redacted]	2	FortiGate-300E	Denial Of Service	Long Duration ID
☐	2025/03/20 12:57:01	[redacted]	N/A	[redacted]	1	FortiGate-300E	Cipher Attack	Weak WEP IV
☐	2025/03/20 12:31:03	[redacted]	N/A	[redacted]	2	FortiGate-300E	Denial Of Service	Long Duration ID
☐	2025/03/20 12:22:38	[redacted]	N/A	[redacted]	2	FortiGate-300E	Denial Of Service	Long Duration ID
☐	2025/03/20 11:58:28	[redacted]	N/A	[redacted]	2	FortiGate-300E	Rogue Attack	Invalid MAC OUI

WIDS SLAs are categorized based on the severity and potential impact of detected wireless intrusion events mentioned above. These events are classified into the following categories:

- Denial of Service
- Misconfigured Packet
- Rogue Attack
- Cipher Attack
- Tool Attack

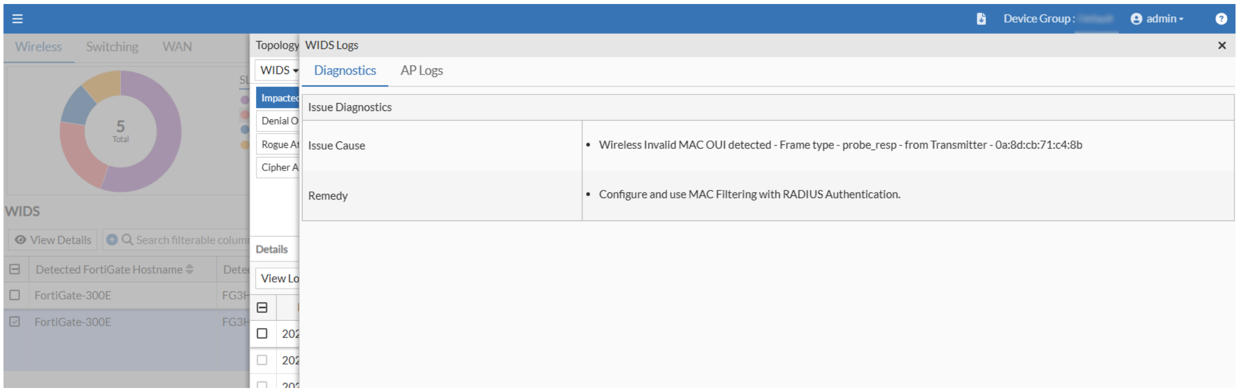
The **Details** table displays information such as the Detected FortiGate Hostname, Detected FortiGate, Affected AP Serial Number, Detected FortiGate IP Address, Classifier, Sub Classifier, Affected AP IP Address, Affected AP Name, Affected AP State, and Affected AP Status. Right-click on the header of the table to select the columns that you want to view.

The following table lists all the attributes listed in the **Details** table:

Attribute	Description
Detected FortiGate Hostname	The hostname of the FortiGate associated with AP detecting WIDS events.
Detected FortiGate	Name of the FortiGate in which AP detecting WIDS is connected.
Affected AP Serial Number	Serial number of Access Point detecting WIDS event.
Detected FortiGate IP Address	IP address of the FortiGate in which AP detecting WIDS is connected.
Classifier	The classifier of the issue reported for the SLA.
Sub Classifier	The sub-classifier of the issue for the reported classifier.
Affected AP IP Address	IP address of Access Point detecting WIDS event.
Affected AP Name	Name of Access Point detecting WIDS event.
Affected AP State	State of Access Point detecting WIDS event.
Affected AP Status	Status of Access Point detecting WIDS event.
Attribute	Description
Detected FortiGate Hostname	The hostname of the FortiGate associated with AP detecting WIDS events.
Detected FortiGate	Name of the FortiGate in which AP detecting WIDS is connected.
Affected AP Serial Number	Serial number of Access Point detecting WIDS event.

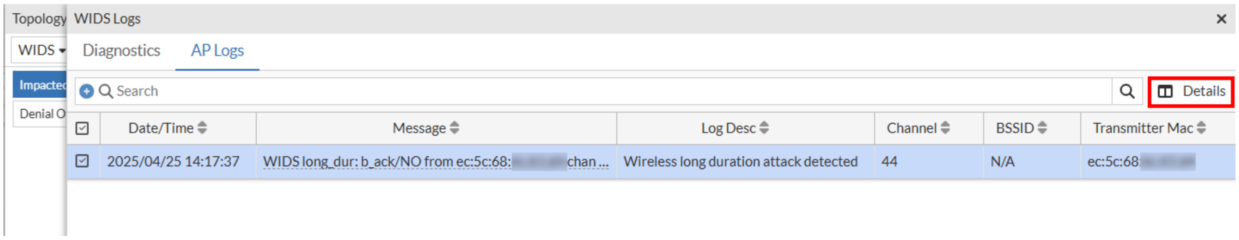
Select a specific row and click **View Logs**. The **WIDS Logs** window displays detailed logs in two tabs namely – **Diagnostics** and **AP Logs**.

The **Diagnostics** tab displays diagnostics details such as Issue Cause and Remedy suggested to resolve the issue.



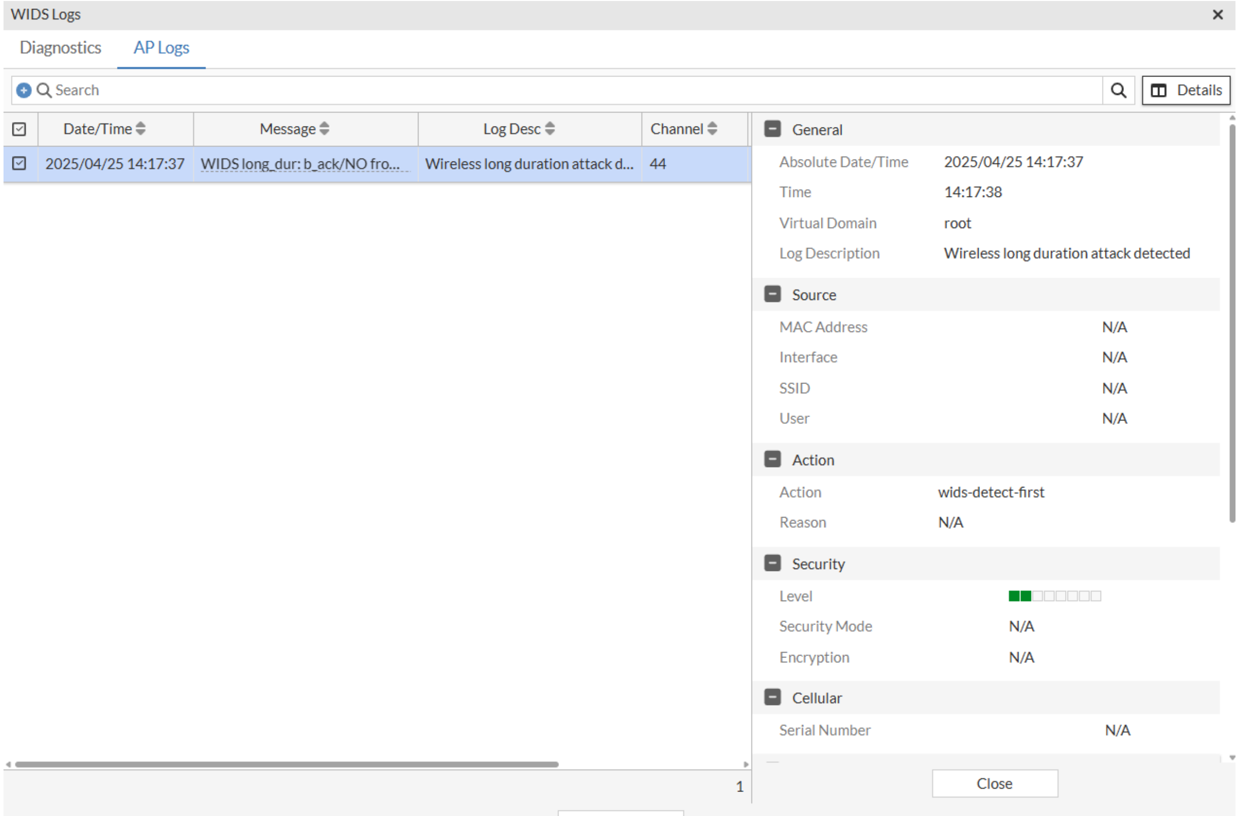
Issue Diagnostics	
Issue Cause	• Wireless Invalid MAC OUI detected - Frame type - probe_resp - from Transmitter - 0a:8d:cb:71:c4:8b
Remedy	• Configure and use MAC Filtering with RADIUS Authentication.

The **AP Logs** tab displays details of the event such as time of the event, error message and log of the event, and details of channel, BSSID, and Transmitter MAC address.



☑	Date/Time	Message	Log Desc	Channel	BSSID	Transmitter Mac
☑	2025/04/25 14:17:37	WIDS long_dur: b_ack/NO from ec:5c:68:[redacted]chan ...	Wireless long duration attack detected	44	N/A	ec:5c:68[redacted]

Select the log and click **Details** to view a more detailed log.



☑	Date/Time	Message	Log Desc	Channel
☑	2025/04/25 14:17:37	WIDS long_dur: b_ack/NO fro...	Wireless long duration attack d...	44

General

Absolute Date/Time	2025/04/25 14:17:37
Time	14:17:38
Virtual Domain	root
Log Description	Wireless long duration attack detected

Source

MAC Address	N/A
Interface	N/A
SSID	N/A
User	N/A

Action

Action	wids-detect-first
Reason	N/A

Security

Level	🟩🟩☐☐☐☐☐☐
Security Mode	N/A
Encryption	N/A

Cellular

Serial Number	N/A

1

Note: WIDS must be enabled on FortiGate to detect wireless attacks and receive logs for the WIDS SLA. By default, intrusion detection in WIDS profile is disabled. For more information, see FortiWiFi and FortiAP Configuration Guide.

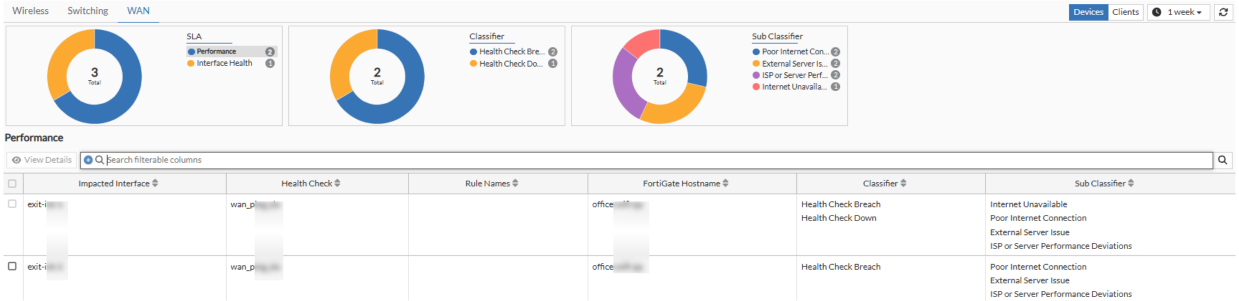
SD-WAN SLA Enhancements

This release enhances SD-WAN SLA monitoring by introducing a comprehensive set of sub-classifiers designed to provide deep insights into critical performance issues. By leveraging real-time logs and statistical data from FortiGate devices, these sub-classifiers enable more precise identification and resolution of potential challenges, ultimately improving network reliability and efficiency.

Previously, SD-WAN issues were primarily categorized as general performance problems triggered by health checks. However, this release introduces more use-case specific classifications for Performance SLAs, Interface Health SLAs and SD-WAN rule [Service] based SLAs. This enables to identify a wider range of performance and interface related problems within the SD-WAN network.

The SLA data tables lists the Impacted Interface, Health Check, Rule Name, FortiGate Hostname, Classifier, and Subclassifier.

Note: To ensure the charts display accurate values, configure the necessary prerequisites and consider the recommendations provided. For more information, see *FortiAIOps User Guide* for release 3.0.0



Performance

☐	Impacted Interface	Health Check	Rule Names	FortiGate Hostname	Classifier	Sub Classifier
☐	exit-i[redacted]	wan_p[redacted]		office[redacted]	Health Check Breach Health Check Down	Internet Unavailable Poor Internet Connection External Server Issue ISP or Server Performance Deviations
☐	exit-i[redacted]	wan_p[redacted]		office[redacted]	Health Check Breach	Poor Internet Connection External Server Issue ISP or Server Performance Deviations

Select any device listed in the tables and click on **View Details** for topology and other details.

SD-WAN Monitoring and Insights

The FortiAIOps Release 3.0.0 introduces interface monitoring for SD-WAN devices.

A new menu item **SD-WAN** is introduced in the main menu. The SD-WAN window provides two views: **Insights** and **Forecast**.

The **Insights** window contains widgets designed to highlight SD-WAN issues.

The **SD-WAN** window that was previously in the **AI Insights** > **Network Benchmarks** section, is now renamed to **Forecast** and moved directly under the SD-WAN menu for easier access.

Prerequisites

The following configurations are necessary to enable proper monitoring:

- The SD-WAN SLA monitors and measures the health of links that are connected to SD-WAN members based on SLA log messages (pass and fail), to predict the performance. Configure the SD-WAN health check in FortiGate as shown in the following example:
  ```
  config system sdwan
  config health-check
  edit "<Health Check Name>"
  set sla-fail-log-period 60
  set sla-pass-log-period 60
  ```
  For more details, see FortiGate Administration Guide.
- Enable Application Control to ensure accurate computation of SD-WAN traffic, along with detailed reporting of SD-WAN rule utilization, application usage, and bandwidth consumption. For more information, see FortiGate Administration Guide.

Recommendations

Fortinet recommends the following for best usage of the FortiAIOps capabilities:

- To ensure all health checks are accurately monitored by FortiAIOps, configure the SD-WAN Health Check parameters `sla-fail-log-period` and `sla-pass-log-period` on the FortiGate. It is recommended to set both to a 60-second interval for higher accuracy. For information, see FortiGate Administration Guide.
- Enable NTP sync for accurate SD-WAN forecast and anomaly detection.
- To enable accurate reporting of bandwidth consumption and capacity failures for SD-WAN interfaces, the estimated upstream and downstream bandwidth values must be configured. For information on how to configure, see FortiGate Administration Guide.
- SD-WAN Network Monitor license must be installed on the FortiGate to measure the estimated bandwidth accurately.

Insights

The Insights page provides valuable insights into your network's health and performance with the charts:

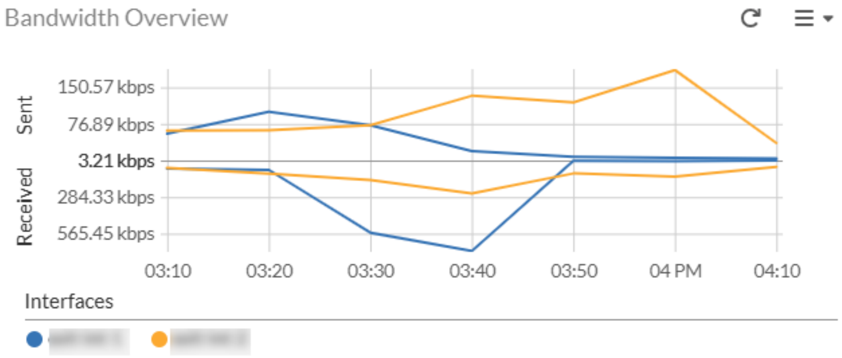
- Bandwidth Overview
- Available Bandwidth

- Used Bandwidth
- Performance Status
- Rules Utilization
- Applications Utilization
- MOS Score
- SLA Performance Issues

Bandwidth Overview

This chart displays the trend of bandwidth usage for both sent and received traffic for the selected duration for the selected/all SD-WAN interfaces on the selected FortiGate device.

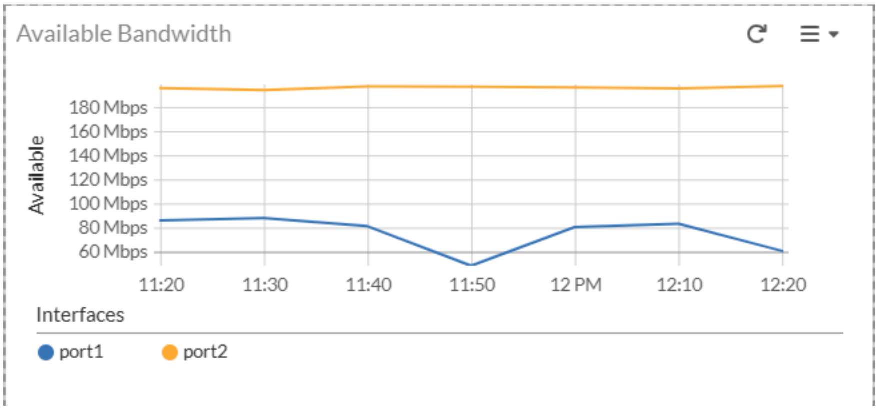
Hover over the points on graph to view sent/receive data.



Available Bandwidth

This chart shows the total bandwidth available for the SD-WAN Interfaces over time. This is based on the Estimated Bandwidth configured in SD-WAN Interface configuration and used to estimate the WAN Utilization.

Hover over the points on graph to view Available Bandwidth information.

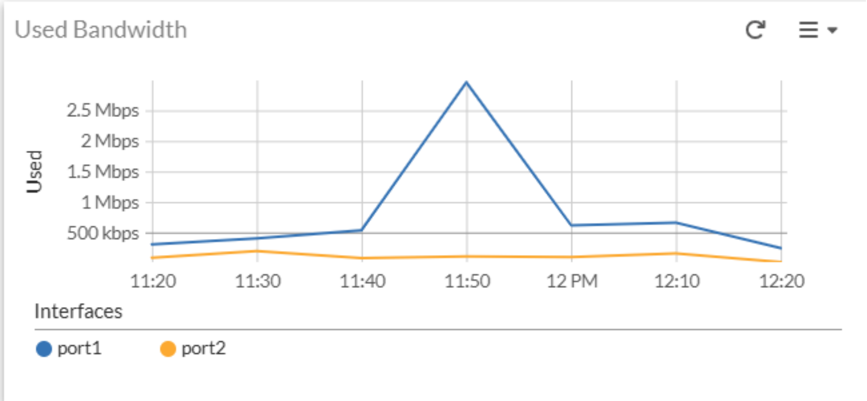


Note: Configure **Estimated Bandwidth** to estimate accurate WAN utilization. If not configured, the maximum capacity of the link is inserted as **Available Bandwidth**. For more information, see FortiGate Administration Guide.

Used Bandwidth

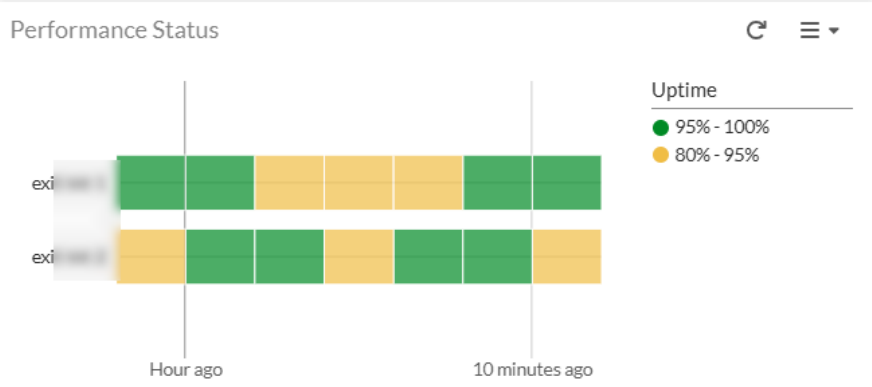
This chart displays the amount of bandwidth consumed by the SD-WAN interfaces over a period of time.

Hover over the points on graph to view Used Bandwidth information.



Performance Status

This chart shows the overall status of the SD-WAN interface for the selected FortiGate device, based on the uptime of each monitored health check within the specified time frame.



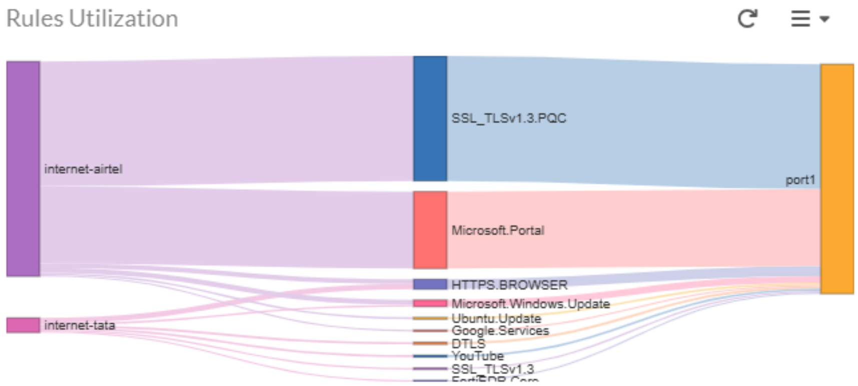
Color-coded indicators represent uptime percentages:

- Green – Up time of more than 95%
- Yellow – Up time between 80% to 95%
- Orange – Up time between 50% to 80%
- Red – Up time for less than 50%

For detailed information, click a health check status to open the **Details** pane, displaying FortiGate name, health check type, uptime, and interface. To view in-depth analytics, click the **Health Check** name to access the **Dashboard** > **SD-WAN** window.

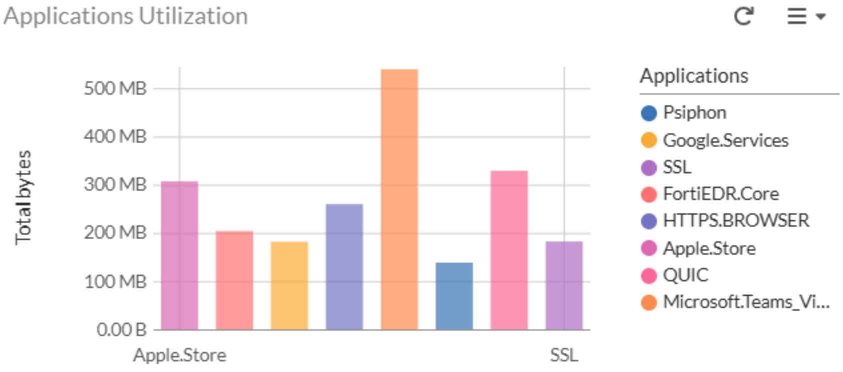
Rules Utilization

This chart shows how SD-WAN rules, which govern traffic routing across SD-WAN interfaces, are utilized. It presents a detailed view of traffic distribution, displaying data for both the interface through which the traffic flows and the applications generating the traffic. Hover your cursor over the data points for a more detailed information.



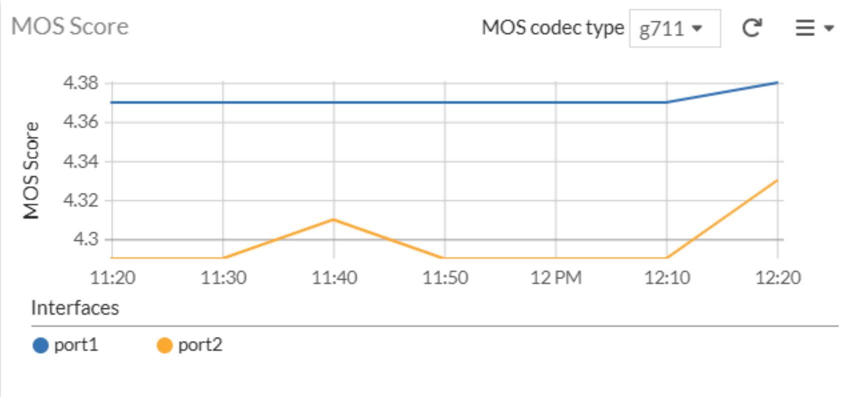
Applications Utilization

This chart displays a detailed overview of bandwidth consumption, showing the top 10 applications and their respective bandwidth distribution across the configured SD-WAN interfaces. Hover your cursor over the data points for a more detailed information.



MOS Score

The Mean Opinion Score (MOS) is used to evaluate the quality of voice and video transmissions, particularly in telecommunications applications like VoIP and video conferencing.



The MOS rating for the quality of video and Audio traffic through the SD-WAN Interface are listed below:

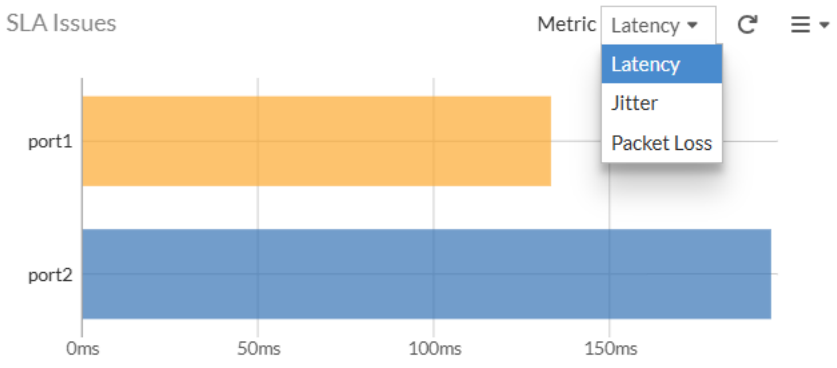
- MOS 4.3-5.0: Excellent
- MOS 4.0-4.3: Good
- MOS 3.6-4.0: Fair
- MOS 3.1-3.6: Poor
- MOS 2.6-1.0: Bad

The chart presents MOS score data for SD-WAN interfaces across a time frame, based on the selected **MOS codec type**.

SLA Performance Issues

The chart displays the maximum and average SD-WAN performance values for each metrics of Interfaces—Latency, Jitter, and Packet Loss for the selected time period.

Hover over to view performance metric value for selected time frame.



Select the desired **Metric** from the drop-down.

SD-WAN Dashboard

A new page, **SD-WAN** is introduced under the **Dashboard** menu. The **SD-WAN** page provides metric information for the FortiGate devices based on the SD-WAN Interfaces in the system. It provides a visual overview of network performance, application usage, and traffic distribution.

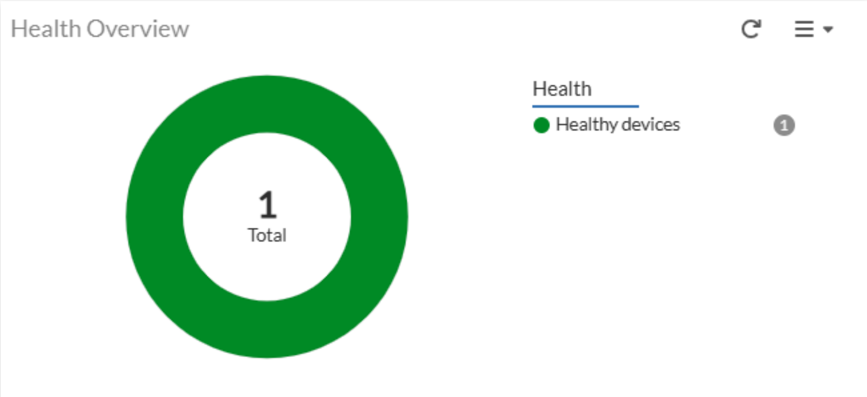
To ensure the charts display accurate values, configure the necessary Prerequisites and consider the Recommendations provided. If the prerequisites are not configured, both the SD-WAN dashboard and Forecast will appear empty.

The following new charts are available on the **SD-WAN** page:

- SD-WAN Health Overview
- Top SLA Issues
- Top Applications
- Top Talkers

The other additional charts available on the SD-WAN page are - FortiGates, SD-WAN Events, and SD-WAN Insights.

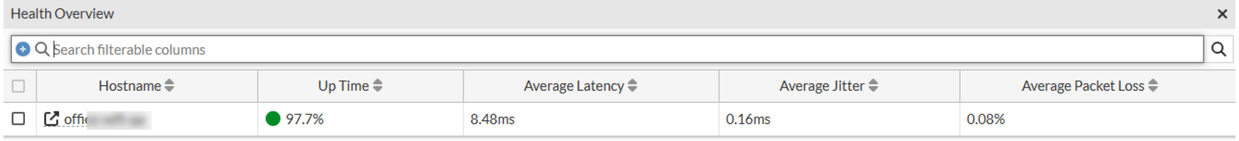
SD-WAN Health Overview



This chart summarizes the health status of FortiGates based on the health results of health checks configured for each interface. Depending on the health check uptime, FortiGates are classified as Critical, Major, or Healthy:

- Healthy Devices – Indicates the number of devices where there is no health check failure observed over the selected duration (Overall Health Check status is 95% to 100% for the given FortiGate device).
- Major Alerts Devices - Indicates the number of devices where there were health check failure observed over the selected duration (Overall Health Check status is 50% to 95% for the given FortiGate device).
- Critical Alert Devices - Indicates the number of devices where there were health check failure observed over the selected duration (Overall Health Check status is 0% to 50% for the given FortiGate device).

Clicking on each value displays a detailed table with information such as the hostname, up time, average latency, average jitter, and average packet loss.



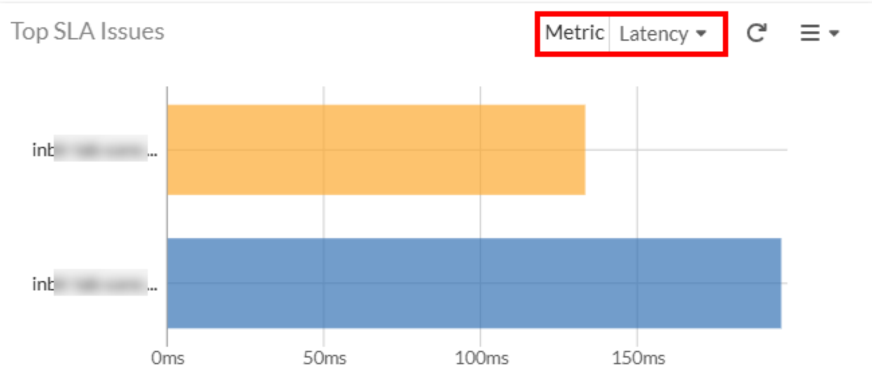
☐	Hostname	Up Time	Average Latency	Average Jitter	Average Packet Loss
☐	offi[redacted]	● 97.7%	8.48ms	0.16ms	0.08%

Clicking on a FortiGate name redirects to the **Insights** page, which displays various SD-WAN Insights for the associated interfaces. These insights are derived from the performance of configured health checks and include metrics such as bandwidth usage, SD-WAN rule utilization, application usage, and performance indicators like latency, jitter, and packet loss.

Top SLA Issues

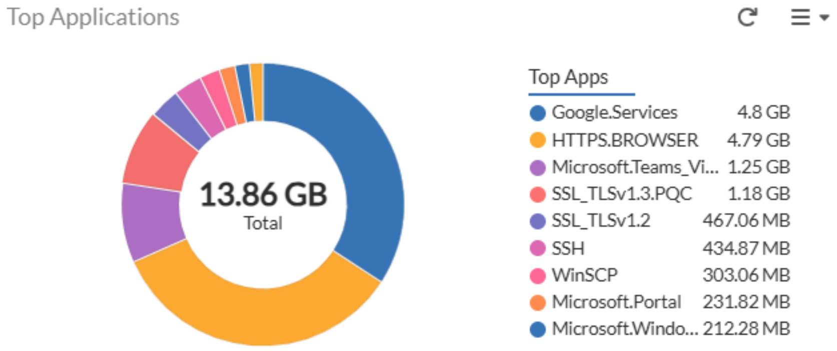
This chart displays the top 10 worst SD-WAN performance values for each metrics for Interfaces—Latency, Jitter, and Packet Loss for the selected time period.

You can select the SLA Performance Metrics from the **Metric** drop-down list.



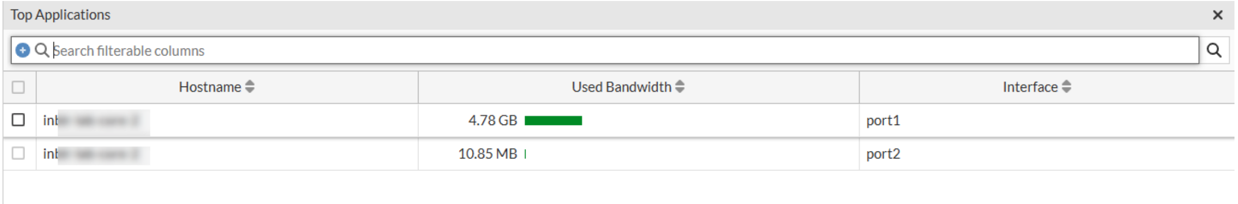
Top Applications

This chart displays the top 10 applications being used on the SD-WAN interfaces.



Hovering over each value displays the Application and Used Bandwidth.

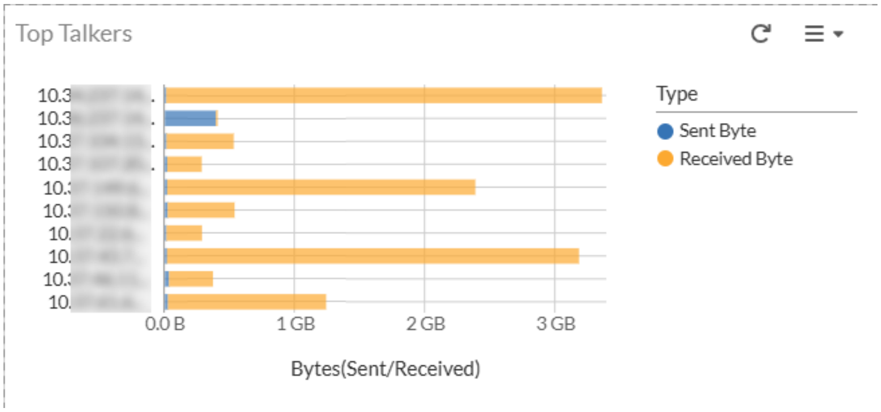
Clicking on each value opens the Top Applications detailed chart for the application displaying the FortiGate name, used bandwidth, and the interface.



☐	Hostname	Used Bandwidth	Interface
☐	int[redacted]	4.78 GB	port1
☐	int[redacted]	10.85 MB	port2

Top Talkers

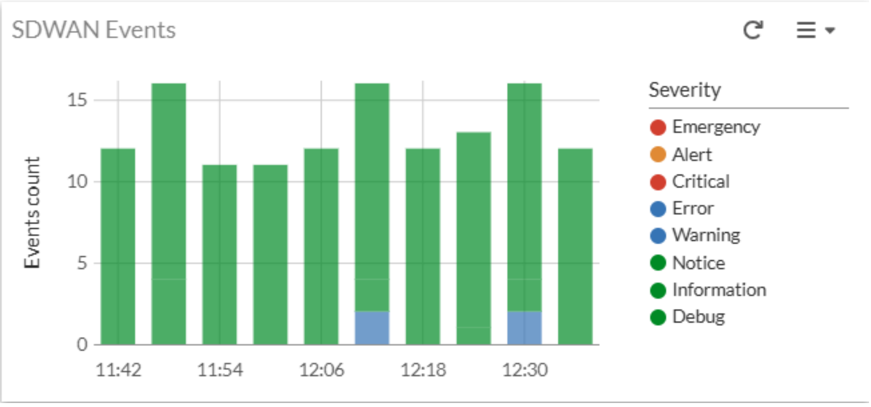
This chart displays the sources which have top 10 bandwidth usage (bytes sent and bytes received) on the SD-WAN interfaces across the FortiGates within a Device Group. Clicking on each value opens the Top Talkers detailed chart with information such as FortiGate name, interface, application, sent byte, and received byte.


Top Talkers
Type
● Sent Byte
● Received Byte
0.0 B
1 GB
2 GB
3 GB
Bytes(Sent/Received)

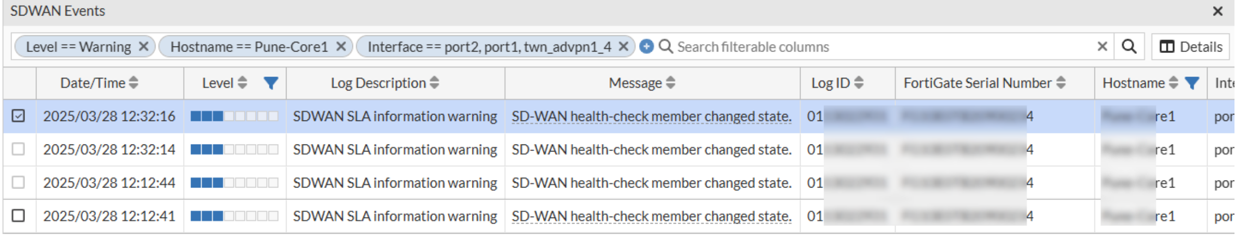
SD-WAN Events Chart in SD-WAN Dashboard

The **Dashboard** > **SD-WAN** window is updated with a new chart—SD-WAN Events.

This chart displays the number of SD-WAN events across various severity levels within a specified time frame.



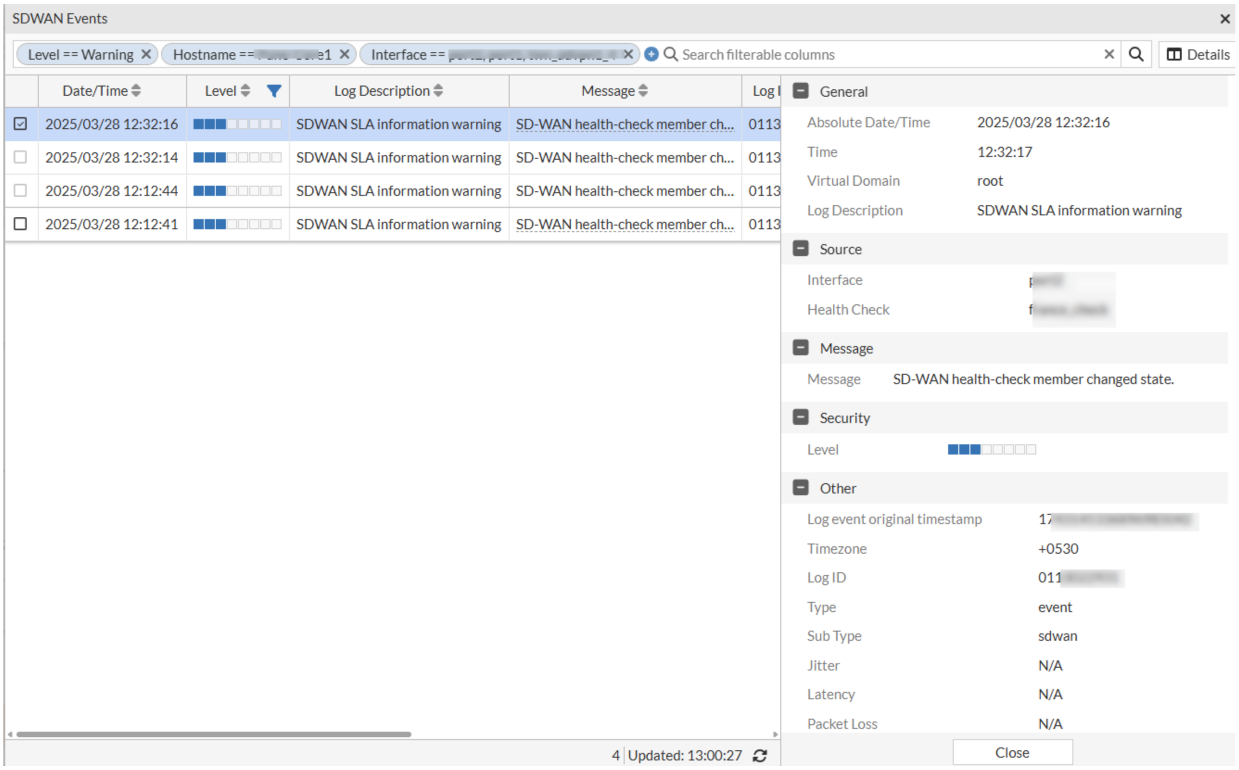
Click an event on the chart to view a detailed **SD-WAN Events** table, including time, severity, log description, message, log ID, FortiGate serial number, hostname, interface, health check, and VDOM.


SDWAN Events

Level == Warning ✕ Hostname == Pune-Core1 ✕ Interface == port2, port1, twn_advpn1_4 ✕

	Date/Time	Level	Log Description	Message	Log ID	FortiGate Serial Number	Hostname	Int
☑	2025/03/28 12:32:16	■■■□□□□	SDWAN SLA information warning	SD-WAN health-check member changed state.	01[redacted]	[redacted]4	[redacted]re1	por
☐	2025/03/28 12:32:14	■■■□□□□	SDWAN SLA information warning	SD-WAN health-check member changed state.	01[redacted]	[redacted]4	[redacted]re1	por
☐	2025/03/28 12:12:44	■■■□□□□	SDWAN SLA information warning	SD-WAN health-check member changed state.	01[redacted]	[redacted]4	[redacted]re1	por
☐	2025/03/28 12:12:41	■■■□□□□	SDWAN SLA information warning	SD-WAN health-check member changed state.	01[redacted]	[redacted]4	[redacted]re1	por

Double-click a row in the detailed table to view further details.



	Date/Time	Level	Log Description	Message	Log I
☑	2025/03/28 12:32:16	■■■□□□□□	SDWAN SLA information warning	SD-WAN health-check member ch...	0113
☐	2025/03/28 12:32:14	■■■□□□□□	SDWAN SLA information warning	SD-WAN health-check member ch...	0113
☐	2025/03/28 12:12:44	■■■□□□□□	SDWAN SLA information warning	SD-WAN health-check member ch...	0113
☐	2025/03/28 12:12:41	■■■□□□□□	SDWAN SLA information warning	SD-WAN health-check member ch...	0113

4 Updated: 13:00:27

General

Absolute Date/Time	2025/03/28 12:32:16
Time	12:32:17
Virtual Domain	root
Log Description	SDWAN SLA information warning

Source

Interface	p[redacted]
Health Check	f[redacted]

Message

Message	SD-WAN health-check member changed state.

Security

Level	■■■□□□□□

Other

Log event original timestamp	17[redacted]
Timezone	+0530
Log ID	011[redacted]
Type	event
Sub Type	sdwan
Jitter	N/A
Latency	N/A
Packet Loss	N/A

Channel Summary

Under the **Wireless** menu, the newly available **Channel Summary** page provides information categorized within the following sub-tabs

- Summary
- Events
- Insights

Summary

The **Summary** window displays information regarding channel distribution and power distribution.

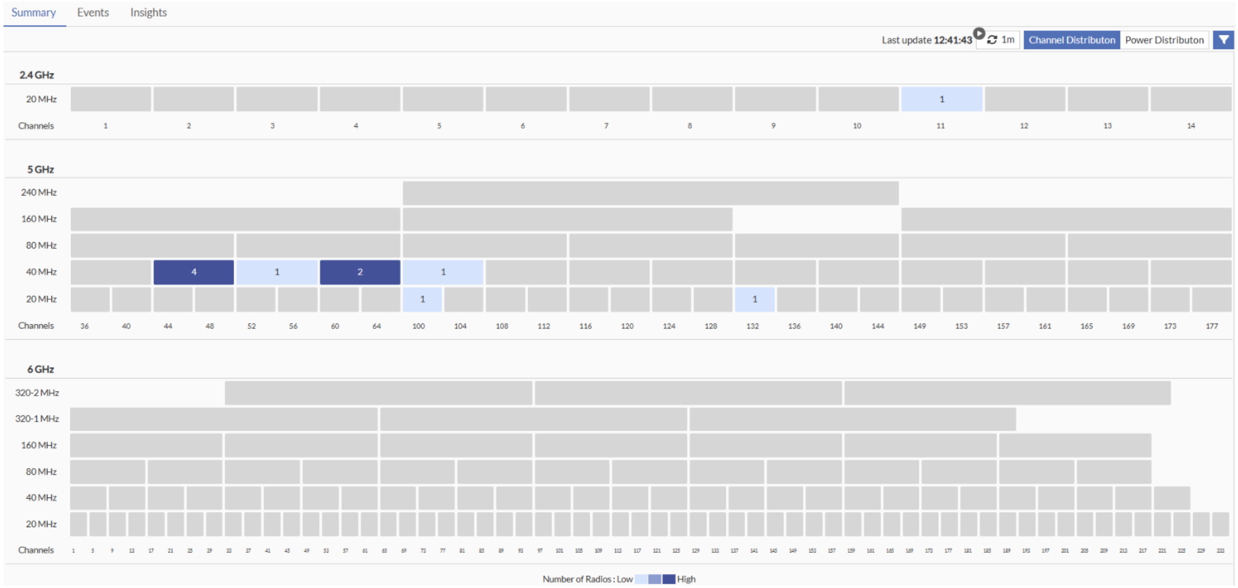
Toggle between the **Channel Distribution** and **Power Distribution** options for relevant information.

Channel Distribution

The **Channel Distribution** tab provides information about how the wireless network channels are utilized across different frequency bands. The information is categorized into three categories based on band namely – 2.4 GHz, 5 GHz, and 6GHz. Each band is further divided into different channel width - 20 MHz, 40 MHz, 80 MHz, 160 MHz, and so on. Hover over a channel number to view the number of radios operating on that channel.

The intensity of the channel colour indicates the number of radios present - a darker colour signifies more radios, and a lighter colour signifies fewer radios.

Use the **Filter** option to select FortiAPs and Radios at specific location such as Site, Building, and Floor.



Note:

- By default, data from all FortiAPs and radios within the logged-in device group is displayed.
- To view the data, you must have a valid monitoring license.

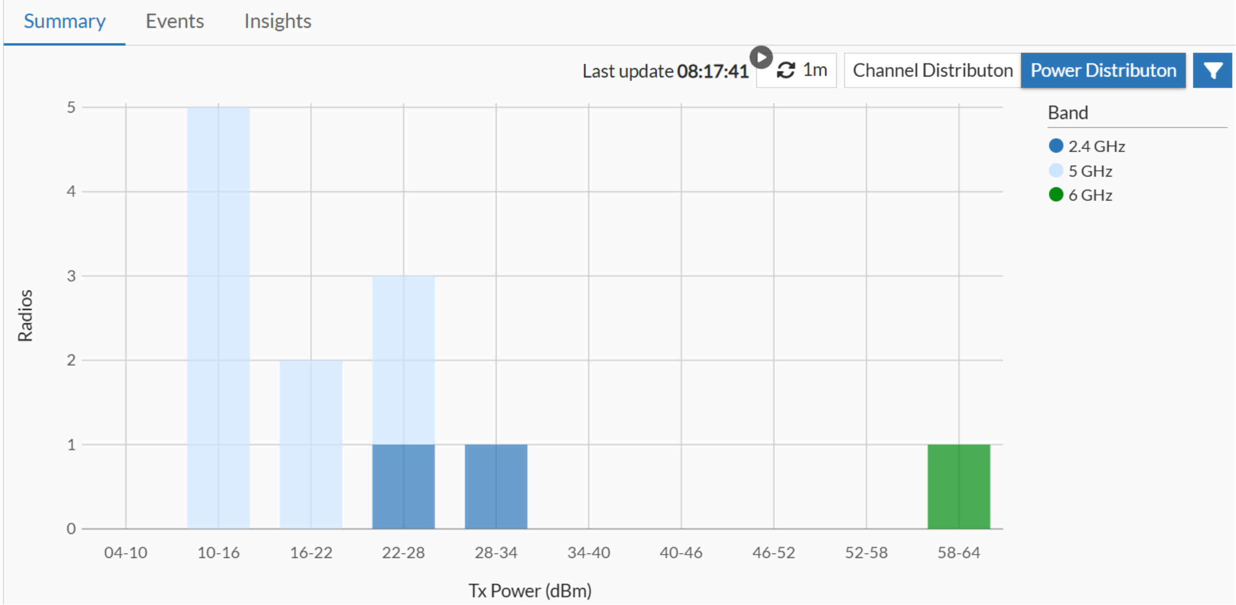
Power Distribution

Power distribution information shows how power is being used by the different radios in your access points. Each bar displays how many radios are transmitting at different power levels.

The vertical side (Y-axis) displays the number of radios operating at a specific power level and the horizontal side (X-axis) shows the amount of power each radio is using to send out signals, measured in dBm.

Power distribution is shown in three categories based on frequency band (2.4 GHz, 5 GHz, 6 GHz), with each band represented by a different colour.

Use the **Filter** option to select FortiAPs and Radios at specific location such as Site, Building, and Floor.

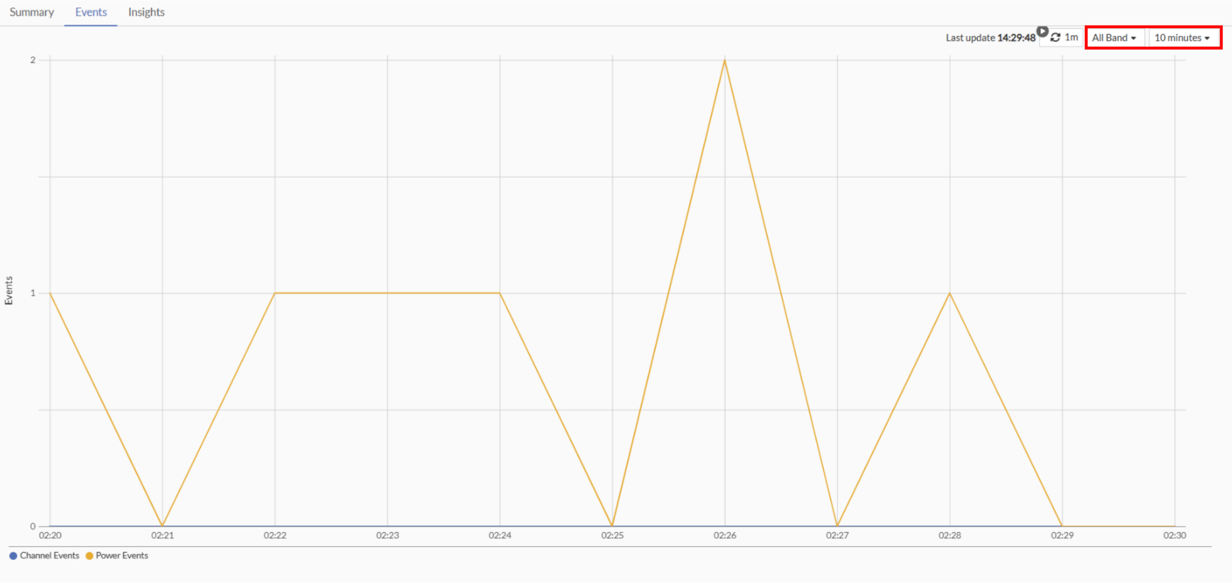


Note: By default, data from all FortiAPs and radios within the logged-in device group is displayed.

Events

The Events tab displays the channel and power change events over time using a bar chart.

To view the **Events** tab, navigate to **Wireless** > **Channel Summary** > **Events** tab.

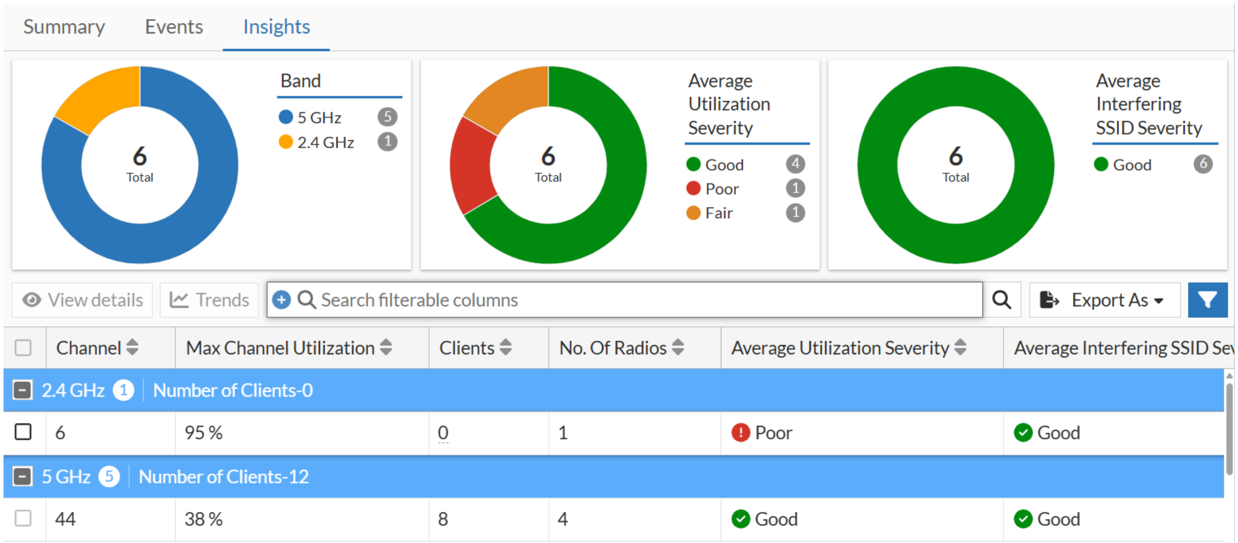


Select the desired bands and time period for the chart using the drop-down menus.

Insights

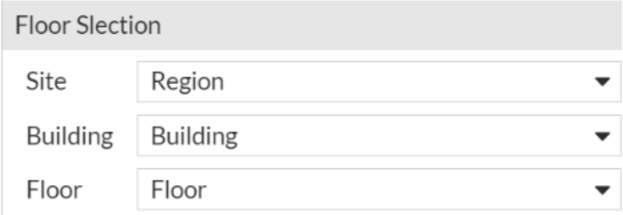
This page provides granular insights into the performance of each channel with key insights into critical statistics, that are key in determining the health of your wireless network. This facilitates effective resolution of any potential network stability issues due to the operating channel. FortiAIOps retrieves and aggregates all channel related statistics from the FortiAPs operating in your network and multiple radios operating on various channels.

Note: All data and trends displayed on this page are for the last 1 minute.



☐	Channel	Max Channel Utilization	Clients	No. Of Radios	Average Utilization Severity	Average Interfering SSID Se
⊟	2.4 GHz 1	Number of Clients-0				
☐	6	95 %	0	1	Poor	Good
⊟	5 GHz 5	Number of Clients-12				
☐	44	38 %	8	4	Good	Good

You can filter based on specific deployment locations such as **Site**, **Building**, and **Floor**.



Floor Slection

Site	Region
Building	Building
Floor	Floor

The following charts are available:

- Band
- Average Utilization Severity
- Average Interfering SSID Severity

Band

This chart provides channel count based on RF bands of 5 GHz, 2.4 GHz, and 6 GHz. The total number of channels for each band are displayed along with what percentage of the total channels used by the wireless network they comprise of. Click on any band to filter channel details and view them in the table below the charts.

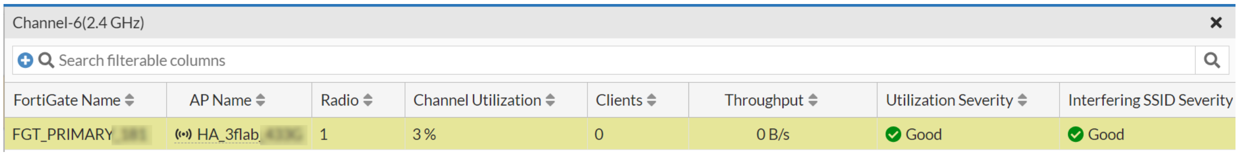
Average Utilization Severity

This chart provides the channel count based on the average utilization severity over the last 60 seconds. FortiAIOps automatically categorizes the channels as **Good** or **Poor**, and **Fair**. The total number of channels for each severity are displayed along with what percentage of the total channels used by the wireless network they comprise of. Click on any severity to filter channel details and view them in the table below the charts.

Average Interfering SSID Severity

This chart provides the channel count based on the average interfering SSID severity over the last 60 seconds. FortiAIOps automatically categorizes the channels as **Good** or **Poor**, and **Fair**. The total number of channels for each severity are displayed along with what percentage of the total channels used by the wireless network they comprise of. Click on any severity to filter channel details and view them in the table below the charts.

The channel data in the tabular format categorizes channels based on the RF band. To view radio level details for a particular channel number, select it and click **View details**.



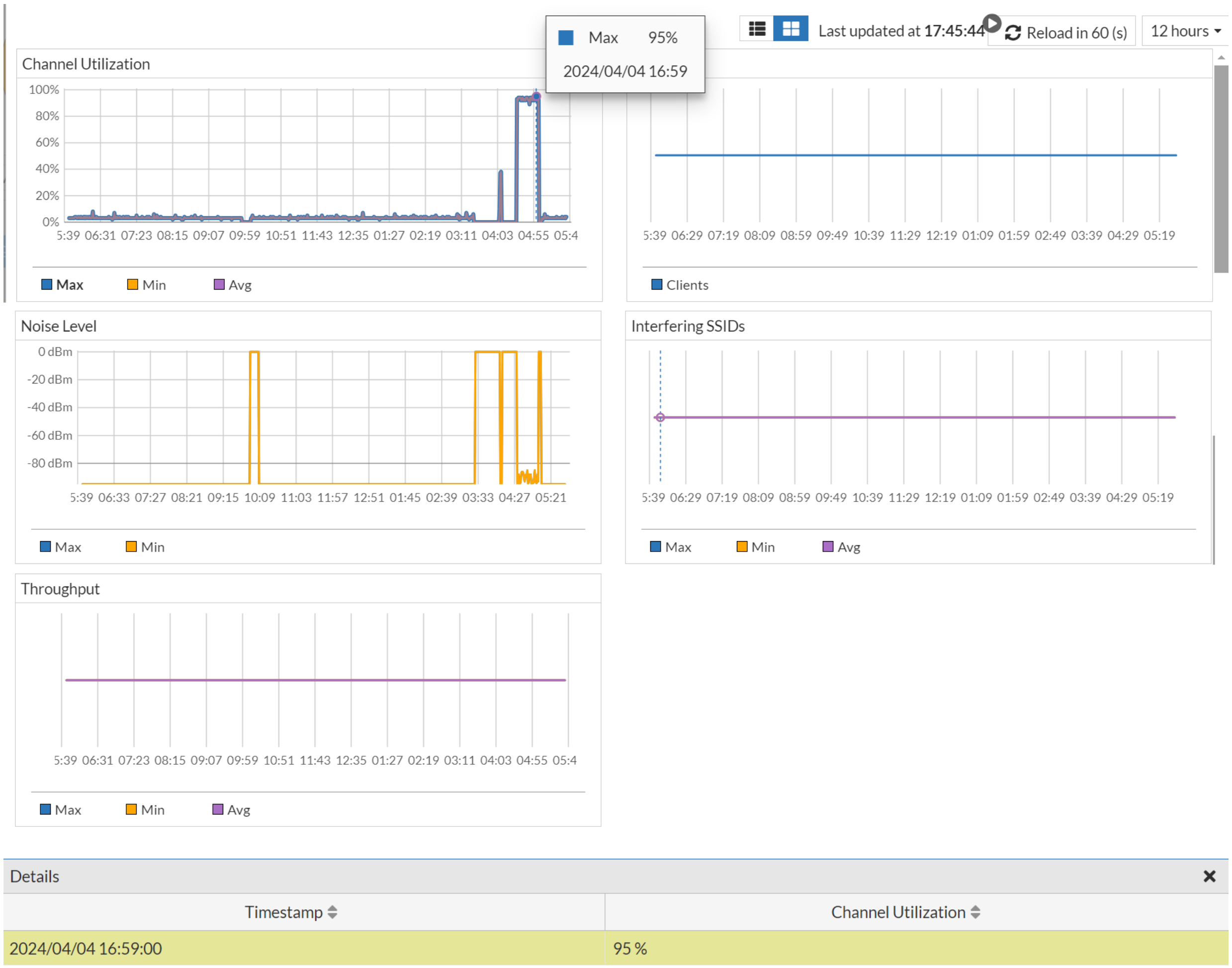
Channel-6(2.4 GHz)

FortiGate Name	AP Name	Radio	Channel Utilization	Clients	Throughput	Utilization Severity	Interfering SSID Severity
FGT_PRIMARY [redacted]	HA_3flab [redacted]	1	3 %	0	0 B/s	✓ Good	✓ Good

Field	**Description**
FortiGate Name and **AP Name**	The names of the FortiGate controller and FortiAP associated with the selected channel.
Radio	The radio operating on the selected channel.
Channel Utilization	Total channel utilization (in percentage) per radio.
Clients	The number of clients connected per radio.

Field	Description
Throughput	The total throughput of traffic passing per radio.
Utilization Severity	The average utilization severity of the selected channel.
Interfering SSID Severity	The average interfering SSID severity of the selected channel.
SSIDs	The SSIDs associated with the radio.
Noise Level	The noise level detected by the by the radio.
Health Assessment	FortiAIOps evaluates a assigns the health status of each radio.

To view trends and patterns to assess the performance of specific channels, select a channel and click **Trends**. You can view a graphical representation of the channel statistics over a period of time. These trends can be filtered for the last **10 minutes**, **1 hour**, or **12 hours**. Hover over the charts or click on a them to view the related statistics at a specific time. For example, the following image depicts a maximum channel utilization of 95% with the time stamp, clicking on this point provides similar data in a tabular format. You can filter the trends based on the selected duration or customized time slot; select a time window or define a **Custom range**. The custom range allows the selection of a minimum of 1 day and the maximum is the duration of log retention configured in **System > Settings**. The minimum, maximum, and average values are displayed when a time interval of more than 6 hours is selected.

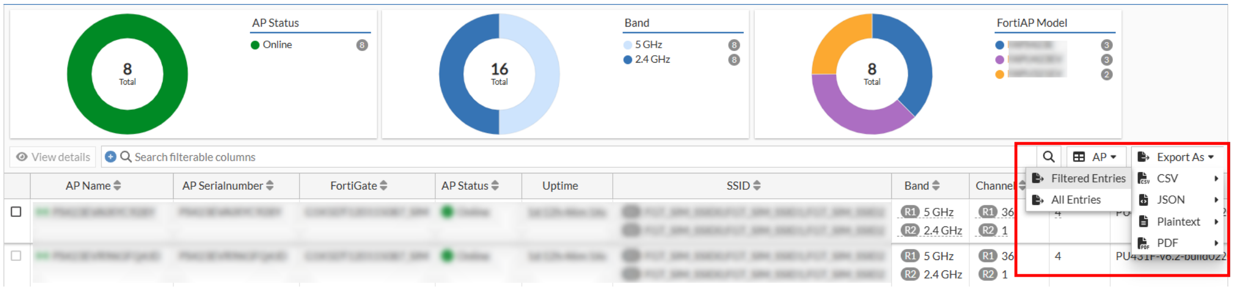


Timestamp	Channel Utilization
2024/04/04 16:59:00	95 %

Click **Export As** to export the table in CSV, JSON, Plaintext, or PDF format. You can export either filtered data or all data in the available formats.
Note: You customize your exports by choosing which columns to be included in the export. A maximum of 8 columns can be selected.

Export Table in Different Formats

FortiAIOps now enables you to export tabular data in CSV/JSON/plain text/PDF formats.



Export option is available in the following pages:

- Inventory > Managed FortiGates
- Wireless > Access Points (including Radio)
- Wireless > Wireless Clients
- Wireless > Channel Summary
- Wireless > Rogue APs
- Switch > FortiSwitches
- Switch > Wired Clients

You can download either filtered data or all data in the available formats.

Note: You customize your exports by choosing which columns to be included in the export. A maximum of 8 columns can be selected.

Remote Admin Authentication

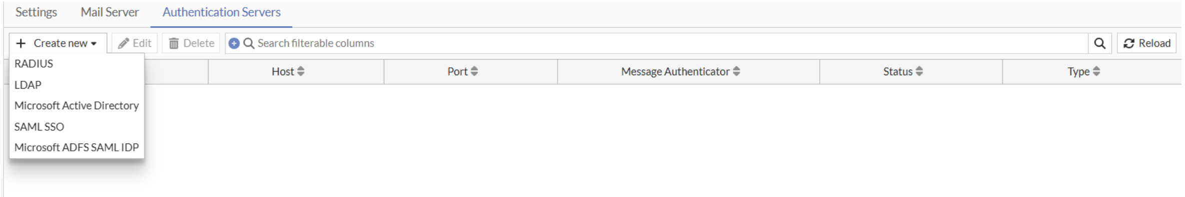
FortiAIOps now supports remote authentication. Previously supporting only local users, the system now supports remote authentication using a remote server.

To use remote authentication, you must first configure the appropriate servers for each authentication server in your network. Remote authentication servers can be added, edited, and deleted.

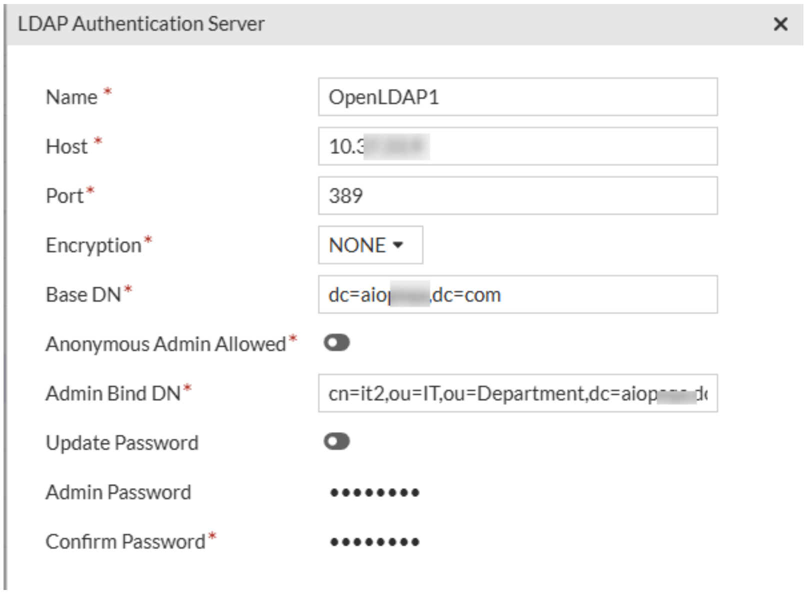
Managing Authentication Servers

To add an Authentication Server:

1. Navigate to **System** > **Settings** > **Authentication Servers** tab.
2. Click **Create New** and select the type of server to be added. Choose between **RADIUS**, **LDAP**, **Microsoft Active Directory**, **SAML SSO**, and **Microsoft ADFS SAML IDP**.



3. Configure the following settings for the server to be added:
   - **LDAP Server**:

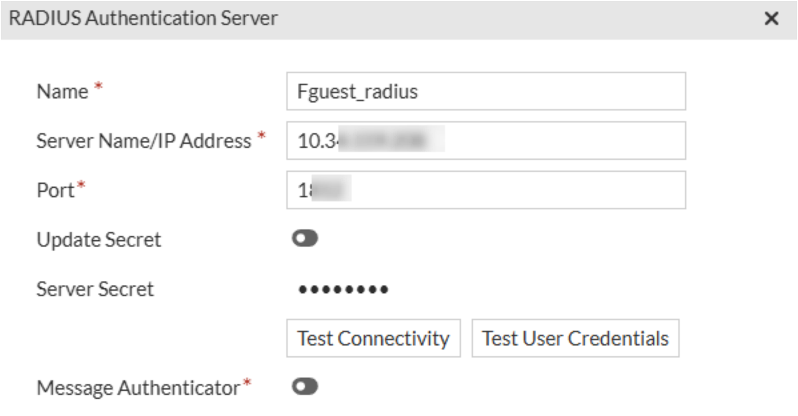


Name * OpenLDAP1
Host * 10.3[redacted]
Port * 389
Encryption * NONE
Base DN * dc=aio[redacted],dc=com
Anonymous Admin Allowed * ○
Admin Bind DN * cn=it2,ou=IT,ou=Department,dc=aiop[redacted]d
Update Password ○
Admin Password ••••••••
Confirm Password * ••••••••

Name	Enter a name to identify the LDAP server.
Host	Enter the IP address of the LDAP server.
Port	Enter the port for LDAP traffic. The

	default port is 389.
Encryption	Select encryption from the drop-down. Choose between NONE and LDAPS.
Base DN	Enter the base Distinguished Name (DN) for the LDAP server. This specific entry in the directory hierarchy acts as the starting point for the search operations in the LDAP server.
Anonymous Admin Allowed	Enable to allow anonymous admin user.
Admin Bind DN	Enter the Admin user Distinguished Name (DN).
Admin Password	Enter a password for admin user.
Confirm Password	Enter the password again to confirm.

- **RADIUS Server**:

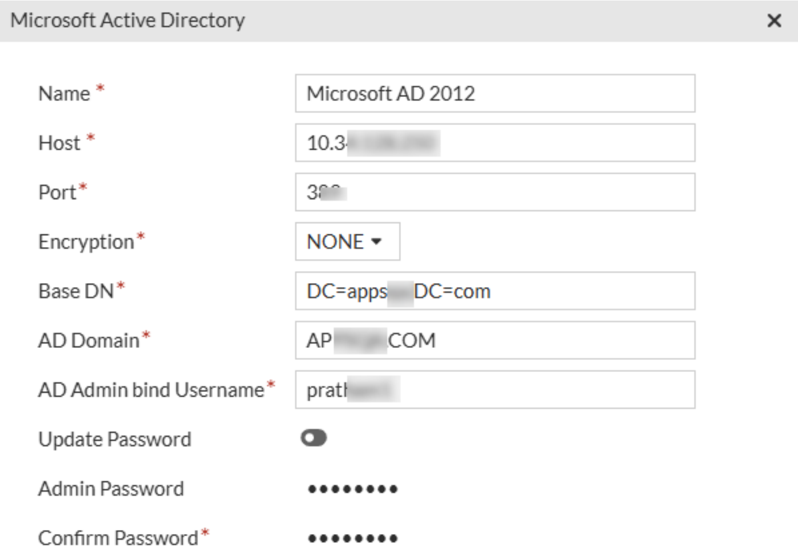


Name * Fguest_radius
Server Name/IP Address * 10.3[redacted]
Port * 1[redacted]
Update Secret
Server Secret ••••••••
Message Authenticator *

Name	Enter a name to identify the RADIUS server.
Server Name/IP Address	Enter the IP address or fully qualified domain name of the RADIUS server.
Port	Enter the port for RADIUS traffic. The default port is 1812. Some RADIUS servers use port 1645.
Update Secret	Enable to update Server Secret.
Server Secret	Enter the RADIUS server secret. Click the eye icon to Show or Hide the server secret.
Test Connectivity	Click Test Connectivity to test the connectivity with the RADIUS server.

Test User Credentials	Click Test User Credentials to test the user credentials.
Message Authenticator	Enable or disable message authentication as required.

- **Microsoft Active Directory (AD)**:

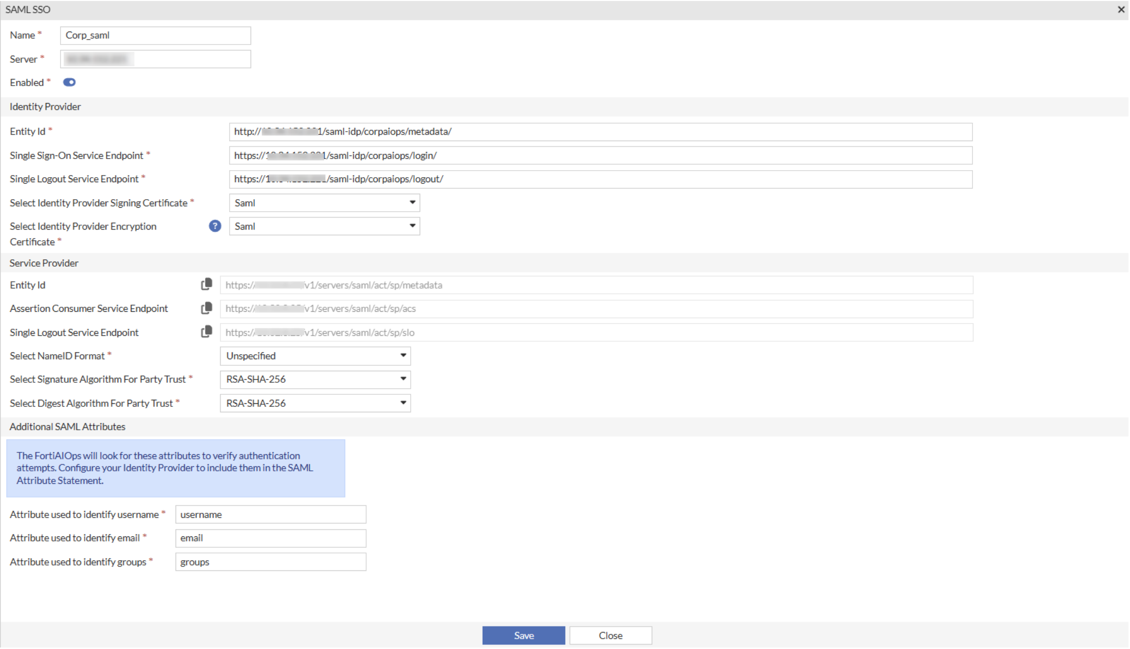


Name *	Microsoft AD 2012
Host *	10.3[redacted]
Port *	3[redacted]
Encryption *	NONE ▾
Base DN *	DC=apps[redacted]DC=com
AD Domain *	AP[redacted]COM
AD Admin bind Username *	prat[redacted]
Update Password	●
Admin Password	••••••••
Confirm Password *	••••••••

Name	Enter a name to identify the AD server.
Host	Enter the IP address of the AD server.
Port	Enter the port for network traffic. The default port is 389.
Encryption	Select encryption from the drop-down. Choose between NONE and LDAPS.
Base DN	Enter the base Distinguished Name (DN) for the LDAP searches within your AD server. This specific entry in the directory hierarchy acts as the starting point for the search operations.
AD Domain	Enter the name of your Active Directory domain.
AD Admin bind Username	Enter the username of the Active Directory account that your system will use to authenticate (bind) to the AD server.
Update Password	Enable to update the password.

Admin Password	Enter a password for admin user.
Confirm Password	Enter the password again to confirm.

- **SAML SSO**:



Name * Corp_saml

Server * [redacted]

Enabled *

Identity Provider

Entity Id * http://[redacted]/saml-idp/corpaiops/metadata/

Single Sign-On Service Endpoint * https://[redacted]/saml-idp/corpaiops/login/

Single Logout Service Endpoint * https://[redacted]/saml-idp/corpaiops/logout/

Select Identity Provider Signing Certificate * Saml

Select Identity Provider Encryption Certificate * Saml

Service Provider

Entity Id https://[redacted]v1/servers/saml/act/sp/metadata

Assertion Consumer Service Endpoint https://[redacted]v1/servers/saml/act/sp/acs

Single Logout Service Endpoint https://[redacted]v1/servers/saml/act/sp/slo

Select NameID Format * Unspecified

Select Signature Algorithm For Party Trust * RSA-SHA-256

Select Digest Algorithm For Party Trust * RSA-SHA-256

Additional SAML Attributes

The FortiAIOps will look for these attributes to verify authentication attempts. Configure your Identity Provider to include them in the SAML Attribute Statement.

Attribute used to identify username * username

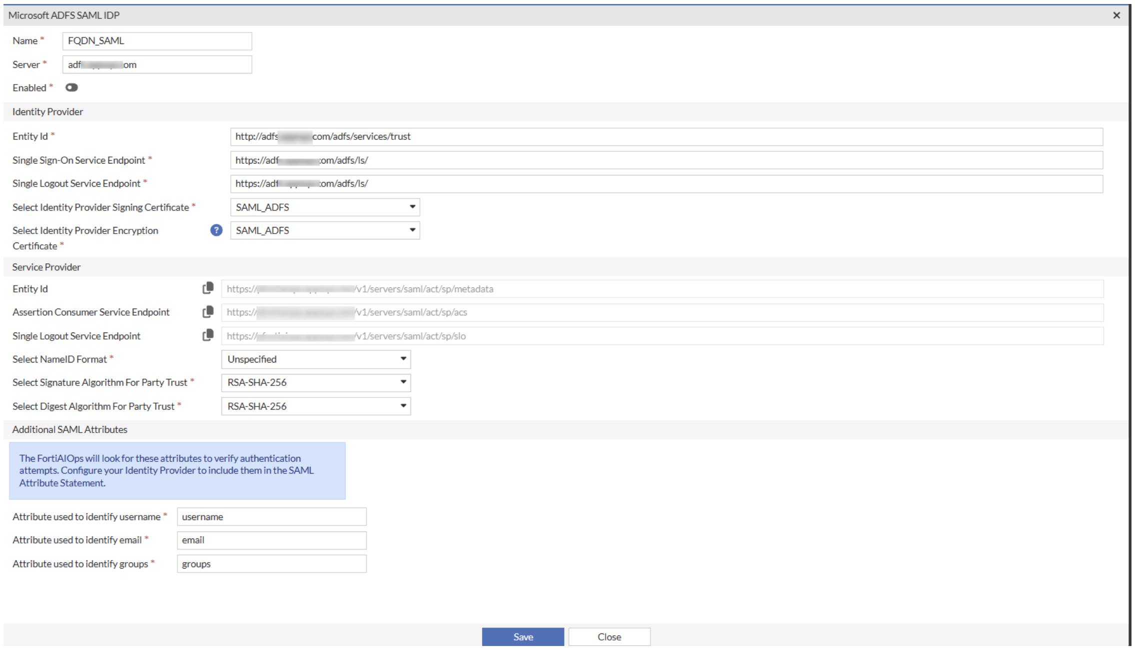
Attribute used to identify email * email

Attribute used to identify groups * groups

Name	A user-defined name to identify this SAML SSO configuration.
Server	The IP address or FQDN of the Identity Provider (IdP) server where SAML authentication requests will be sent.
Enabled	Toggle button to enable or disable this SAML SSO configuration. If enabled, SAML SSO is active. If disabled, configuration is saved but inactive.
Identity Provider	
Entity Id	The unique identifier URL for the Identity Provider. This is usually the IdP metadata URL. For example - `http://<IP address>/saml-idp/corpaiops/metadata/`
Single Sign-On Service Endpoint	The URL where FortiAIOps will redirect users for authentication (IdP SSO login URL). For example - `https://<IP address>/saml-idp/corpaiops/login/`
Single Logout Service Endpoint	The URL where FortiAIOps will send SAML logout requests to log the user out from IdP as well. For example - `https://<IP address>/saml-idp/corpaiops/logout/`

Select Identity Provider Signing Certificate	Select the IdP's certificate used to sign the SAML responses. This ensures message integrity and authenticity. This certificate has to be uploaded in Local certificate of the FortiAiops.
Select Identity Provider Encryption Certificate	Select the IdP's encryption certificate. The certificate must be uploaded under Local Certificate in FortiAIOps.
Service Provider	
Entity Id	The unique identifier URL for FortiAIOps as Service Provider (SP). For example - `https://<IP address>/v1/servers/saml/act/sp/metadata`
Assertion Consumer Service Endpoint (ACS URL)	The URL where IdP will post SAML assertions after authentication. For example - `https://<IP address>/v1/servers/saml/act/sp/acs`
Single Logout Service Endpoint	The URL where IdP can send logout requests to terminate FortiAIOps sessions. For example - `https://<IP address>/v1/servers/saml/act/sp/slo`
Select NameID Format	The format of NameID used by IdP to uniquely identify the user.
Select Signature Algorithm For Party Trust	The algorithm used to sign SAML requests. Both IdP and SP must support the selected algorithm. For example - RSA-SHA-256
Select Digest Algorithm For Party Trust	Specifies the hashing algorithm used to compute the message digest before signing the SAML messages. It ensures data integrity and is part of the digital signature process.The Identity Provider (IdP) and Service Provider (SP) must support the same digest algorithm to validate signatures correctly. For example - RSA-SHA-256
Additional SAML Attributes	
Attribute used to identify username	The name of the attribute in the SAML assertion provided by the Identity Provider (IdP) which holds the username. This attribute should match on both SP and IDP.
Attribute used to identify email	The name of the attribute in the SAML assertion provided by the Identity Provider (IdP) which contains the email address.
Attribute used to identify groups	The name of the attribute in the SAML assertion provided by the Identity Provider (IdP) which contains the user's group memberships.
Note: You can enter either the fixed keywords username, email and groups or specify the exact attribute names as configured in your Identity Provider.	

- **Microsoft ADFS SAML IDP**



Name * FQDN_SAML

Server * adf[redacted]om

Enabled *

Identity Provider

Entity Id * http://adfs[redacted]com/adfs/services/trust

Single Sign-On Service Endpoint * https://adf[redacted]om/adfs/ls/

Single Logout Service Endpoint * https://adf[redacted]om/adfs/ls/

Select Identity Provider Signing Certificate * SAML_ADFS

Select Identity Provider Encryption Certificate * SAML_ADFS

Service Provider

Entity Id https://[redacted]/v1/servers/saml/act/sp/metadata

Assertion Consumer Service Endpoint https://[redacted]/v1/servers/saml/act/sp/acs

Single Logout Service Endpoint https://[redacted]/v1/servers/saml/act/sp/slo

Select NameID Format * Unspecified

Select Signature Algorithm For Party Trust * RSA-SHA-256

Select Digest Algorithm For Party Trust * RSA-SHA-256

Additional SAML Attributes

The FortiAIOps will look for these attributes to verify authentication attempts. Configure your Identity Provider to include them in the SAML Attribute Statement.

Attribute used to identify username * username

Attribute used to identify email * email

Attribute used to identify groups * groups

Name	A user-defined name to identify this ADFS SAML IDP configuration.
Server	The IP address or FQDN of the Identity Provider (IdP) server where SAML authentication requests will be sent.
Enabled	Toggle button to enable or disable this ADFS SAML IDP configuration. If enabled, ADFS SAML IDP is active. If disabled, configuration is saved but inactive.
Identity Provider	
Entity Id	The unique identifier URL for the ADFS Identity Provider. This usually corresponds to the ADFS federation metadata address. For example - `https://<server>/adfs/services/trust`
Single Sign-On Service Endpoint	The URL to which FortiAIOps redirects users for authentication (the ADFS SSO login URL). For example - `https://<server>/adfs/ls/`
Single Logout Service Endpoint	The URL where FortiAIOps sends logout requests to sign out users from ADFS. For example - `https://<server>/adfs/ls/`
Select Identity Provider Signing Certificate	The certificate used by ADFS to sign SAML assertions. This certificate must be uploaded into FortiAIOps local certificate.
Select Identity Provider Encryption Certificate	The certificate used to encrypt SAML assertions from ADFS.This certificate must be uploaded into FortiAIOps local logs.

Service Provider	
Entity Id	The unique identifier for FortiAIOps as the Service Provider. For example - `https://<IP address>/v1/servers/saml/act/sp/metadata`
Assertion Consumer Service Endpoint (ACS URL)	The endpoint URL where ADFS will send SAML authentication responses after successful login. For example -`https://<IP address>/v1/servers/saml/act/sp/acs`
Single Logout Service Endpoint	The endpoint URL where ADFS can send logout requests to terminate the FortiAIOps user session. For example - `https://<IP address>/v1/servers/saml/act/sp/slo`
Select NameID Format	The format of the NameID used by ADFS to identify the user.
Select Signature Algorithm For Party Trust	The algorithm used for signing SAML messages. Both IdP and SP must support the same algorithm.
Select Digest Algorithm For Party Trust	Specifies the hashing algorithm used to compute the message digest before signing the SAML messages. It ensures data integrity and is part of the digital signature process. The Identity Provider (IdP) and Service Provider (SP) must support the same digest algorithm to validate signatures correctly.Ex - RSA-SHA-256
Additional SAML Attributes	
Attribute used to identify username	The name of the attribute in the SAML assertion provided by ADFS which contains the username.
Attribute used to identify email	The name of the attribute in the SAML assertion provided by ADFS which contains the email address.
Attribute used to identify groups	The name of the attribute in the SAML assertion provided by ADFS which contains the user's group memberships.
Note: You can enter either the fixed keywords username, email and groups or specify the exact attribute names as configured in your Identity Provider.	

4. Click **Save**.

Note:

- To make changes to an Authentication Server, choose the desired server and then select the **Edit** option.
- To remove a server from the configuration, select it and then choose the **Delete** option.
- After adding the authentication server details, configure user accounts to utilize this server for remote authentication. For more information, see *FortiAIOps User Guide*.

CLI and GUI Profile Consistency

User profiles within FortiAIOps are now consistent across both the Command Line Interface (CLI) and the Graphical User Interface (GUI). Users can use the same password for both CLI and GUI access.

Note:

- GUI usernames must begin with a lowercase letter or an underscore (_) and can include special characters like hyphens (-) or underscores (_), along with along with alphanumeric characters (a-z, A-Z, 0-9).
- After upgrading to version 3.0.0, GUI user names starting with a capital letter will be marked as invalid, preventing CLI synchronization.
- If a user that exists in both CLI and GUI have different passwords, they will retain their respective passwords even after the upgrade.
- Upon upgrading to release 3.0.0, all pre-existing user configurations will be automatically synchronized between the CLI and GUI.

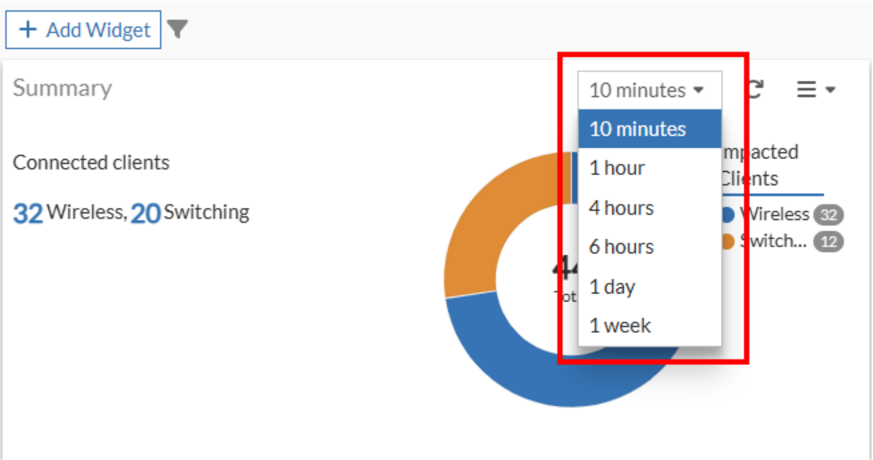
Time Range Updates for AI Insights Pages

Previously, the AI Insights Summary, Impacted SLAs, and Impacted Devices pages utilized the following time range options:

- 2 Hours
- 4 Hours
- 6 Hours
- 1 Day
- 2 Days
- 1 Week

These time ranges were inconsistent with those available in the Monitoring section. To ensure a unified and consistent user experience, the time range options for the AI Insights pages are now updated to the following:

- 10 minutes
- 1 hour
- 4 hours
- 6 hours
- 1 day
- 1 week



Connected clients

32 Wireless, 20 Switching

Intelligent Anomaly Detection for Wired SLA

FortiAIOps wired SLAs — Throughput and Network SLA have been upgraded for more accurate issue detection.

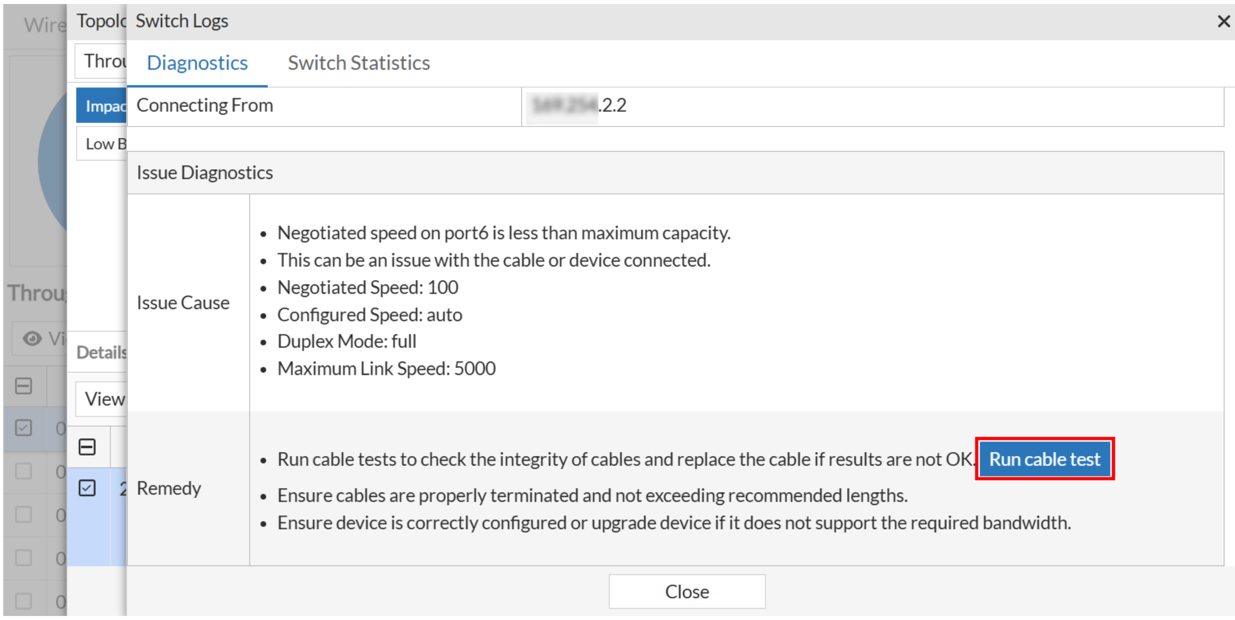
This release introduces intelligent machine learning to analyze recent switch port statistics instead of relying solely on fixed thresholds. By dynamically learning from recent data, the system can now identify unusual patterns and potential breaches with significantly improved accuracy.

Quick Cable Testing for Switches in AI Insights

A convenient shortcut to initiate cable tests on switches is now available within the AI Insights section for Throughput SLA with Classifier as low bandwidth and Sub-classifier as poor negotiated speed.

If the remedy contains the phrase `cable test`, a **Run Cable Test** button is displayed, allowing users to initiate a cable test on the affected port.

To access this feature, navigate to **Dashboard** > **Switch** > **Switching Insights** widget. Select a Topology, and click **View Details**. In the **Topology** pane, choose the desired Issues and click **View Logs**. You will now find a **Run Cable Test** option within the **Issue Diagnostics** section, allowing for faster troubleshooting of connectivity problems.



Connecting From	[redacted].2.2

Issue Diagnostics

Issue Cause	• Negotiated speed on port6 is less than maximum capacity. • This can be an issue with the cable or device connected. • Negotiated Speed: 100 • Configured Speed: auto • Duplex Mode: full • Maximum Link Speed: 5000
Remedy	• Run cable tests to check the integrity of cables and replace the cable if results are not OK. Run cable test • Ensure cables are properly terminated and not exceeding recommended lengths. • Ensure device is correctly configured or upgrade device if it does not support the required bandwidth.

Switch Monitoring Enhancements

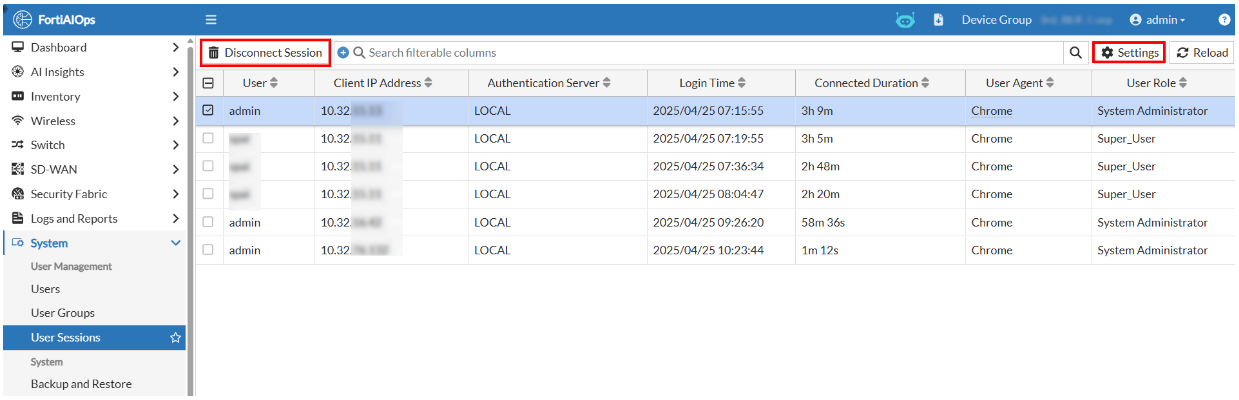
This release introduces enhanced Switch Health SLA monitoring with the following new sub-classifiers for more detailed insights:

- FSW ISL flap events
- Config sync failure
- Fan status correlated with temperature

User Sessions Management

The User Sessions sub-menu under **User Management**, provides a centralized view of all active user sessions. This window displays crucial details for each session, including the username, IP address, authentication server, login time, connection duration, user agent, and assigned role.

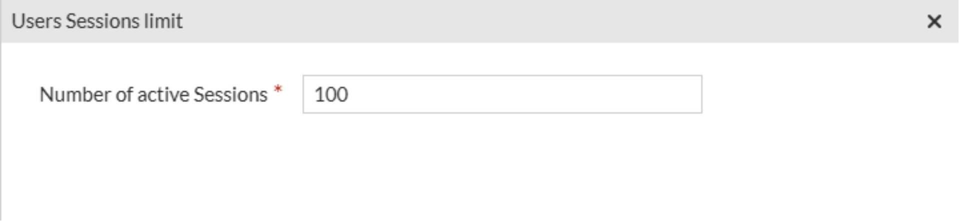
To access, navigate to **Systems** > **User Sessions**.



☐	User	Client IP Address	Authentication Server	Login Time	Connected Duration	User Agent	User Role
☑	admin	10.32.[redacted]	LOCAL	2025/04/25 07:15:55	3h 9m	Chrome	System Administrator
☐	[redacted]	10.32.[redacted]	LOCAL	2025/04/25 07:19:55	3h 5m	Chrome	Super_User
☐	[redacted]	10.32.[redacted]	LOCAL	2025/04/25 07:36:34	2h 48m	Chrome	Super_User
☐	[redacted]	10.32.[redacted]	LOCAL	2025/04/25 08:04:47	2h 20m	Chrome	Super_User
☐	admin	10.32.[redacted]	LOCAL	2025/04/25 09:26:20	58m 36s	Chrome	System Administrator
☐	admin	10.32.[redacted]	LOCAL	2025/04/25 10:23:44	1m 12s	Chrome	System Administrator

Administrators can now manually terminate active sessions. To disconnect a user, select their session from the displayed table and click the **Disconnect Session** button.

For enhanced control, you can limit the maximum number of concurrent active user sessions. Access this setting by clicking the **Settings** button.



Number of active Sessions * 100

In the **User Sessions Limit** pane, enter your desired value in the **Number of active Sessions** field.

Note:

1. By default 100 user sessions are supported.
2. The configurable user session limit is from 10 - 1000.

Dashboard and Navigation Enhancements

This release significantly enhances your dashboard experience with improved organization and new dashboards.

- The main **Dashboard** section now includes dedicated **Wireless**, **Switch**, and **SD-WAN** dashboards for streamlined monitoring.
- The **Dashboard** > **AI Insights** section has been removed. All dashboards previously found here have been relocated to their respective new dashboards under the main **Dashboard** menu.
- The **AI Insights** > **Network Benchmarks** section is now renamed **SLA Config**.
- The **AI Insights** > **Network Benchmarks** > **SD-WAN** section has been renamed Forecast and moved under the **SD-WAN** menu.
- **Switch** > **FortiSwitch Clients** is now renamed **Wired Clients**.
- The **Service Assurance** menu has been renamed to **SAM**.

Diagnostic Tool from CLI

Starting with this release, you can run the Diagnostics Tool from the command line interface (CLI).

Use the following command to run diagnostics using the CLI:

Command	Parameters	Description
`execute diagnostics`	`all System`	Executes all application and logs diagnostics.
	`download <ftp_server>[:port] [ftp_user] [ftp_passwd] [ftp_path]`	Download diagnostics file from the local system to a remote destination.

Others

The following are some additional enhancements delivered in this release.

REST API Polling Optimizations

The REST API polling mechanism is now optimized to minimize the utilization of CPU and memory resources on the FortiGate device.

GUI Responsiveness Improvements

The different pages have been refined and optimized to significantly boost GUI responsiveness. This ensures faster loading times, quicker reaction to user input, and an efficient interaction with the application.

www.fortinet.com

Copyright© 2025 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.