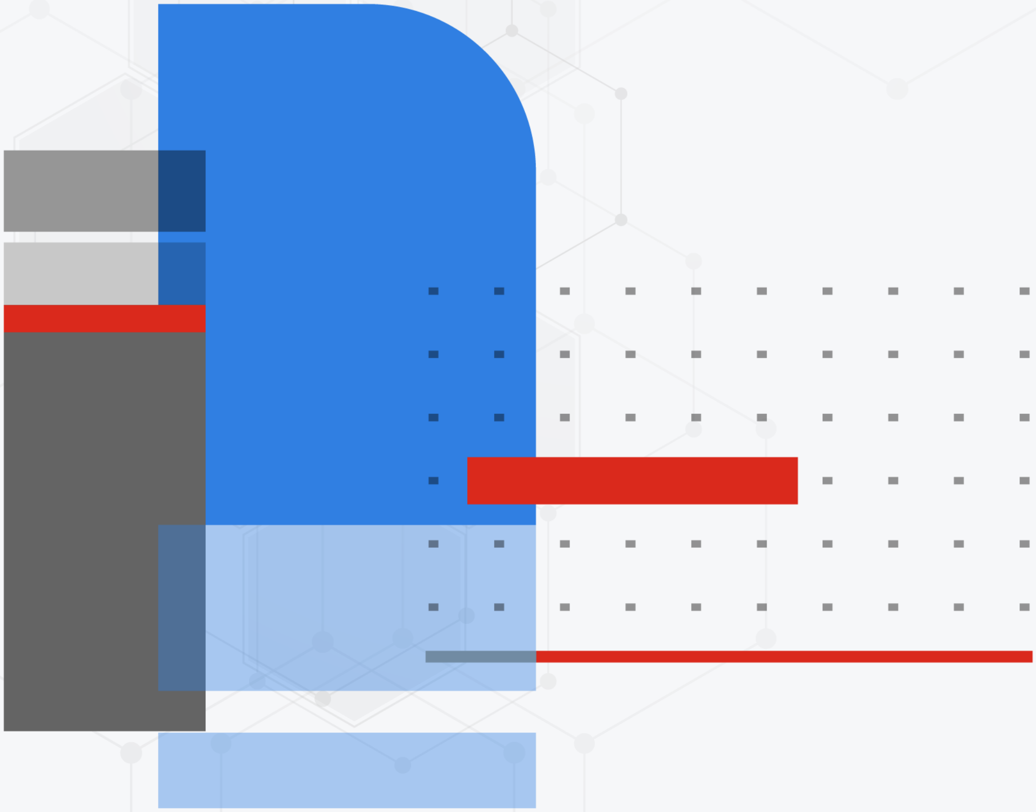
New Features

FortiAIOps 2.1.0



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

October 08, 2024
FortiAIOps 2.1.0 New Features
83-210-1021248-20241008

TABLE OF CONTENTS

Change log

Date	Change description
2024-10-08	FortiAIOps 2.1.0 release document.
2025-02-07	Added FortiAIOps 500G Hardware Support

FortiAIOps 500G Hardware Support

This release of FortiAIOps supports the FortiAIOps 500G (FAO-500G) appliance. The FAO-500G hardware platform comes with FortiAIOps pre-installed.

- Initial Configuration
- Accessing the GUI
- Licensing
- Recommendations and Special Notes

Initial Configuration

After setting up and mounting the appliance on the rack, connect to the FortiAIOps 500G CLI using the console port and perform the following steps. See, *FortiAIOps 500G Quick Start Guide*.

1. On the console Log in as an admin user with the username admin. A password is not required. You will be prompted to configure a new password after the initial login.

   This CLI password is separate from the GUI password. The default GUI credentials are *admin*/*admin*.

2. Verify the dynamically assigned IP address using the command: `get system interface`
3. Configure a static IP address (recommended) using the command: `config system interface`

Accessing the GUI

After completing the initial CLI configuration, you can access the FortiAIOps GUI.

1. Open a web browser and enter the following URL.

   `https://<fortiaiops_server_IP>`

   Replace `<fortiaiops_server_IP>` with the static IP address you configured.
2. Log in using the default GUI credentials.

   admin/*admin*

Licensing

Manual license upload is not required. FortiAIOps automatically synchronizes the license from *Fortinet Support*.

To initiate an immediate license and definition update, navigate to **System > FortiGuard** and click the **Update License and Definitions Now**.

Recommendations and Special Notes

- FortiAIOps supports RAID levels *0*, *1*, *5*, and *10*. The default configuration uses RAID 5 for HDDs and RAID 1 for SSDs.

- For a fresh configuration, completely erase all existing configurations from the hard disks. A factory reset is recommended to ensure all configurations are removed.
- Back up your configuration data before RAID rebuild and migration operations, as these processes are susceptible to errors.
- The 10 Gbps port does not support 1 Gbps data speeds.
- RAID rebuild and migration operations cannot be performed concurrently. However, simultaneous rebuild operations are supported for SSDs and HDDs.
- The system supports the failure of only one HDD and one SSD at a time. Simultaneous failures of multiple HDDs or SSDs may lead to data loss.

Enhanced AI/ML Model

FortiAIOps is now based upon a deployment-specific and adaptive learning AI/ML model, that automatically adjusts whenever there are changes in the Radio Frequency (RF) environment. This is an enhancement from the static AI/ML model of the previous releases. The system runs a weekly (on each Saturday) analysis, to detect any RF changes based on the past week's collected data, and assess if accuracy improvements are possible. If improvements are identified, the AI/ML model is updated to better align with your RF environment. All AI/ML model changes are notified via a local log event message.

SD-WAN SLA

The SD-WAN SLA monitors and measures the health of links that are connected to SD-WAN member interfaces based on the latency, jitter, and packet loss metrics. This enables the selection of an optimal link for traffic routing, that prevents traffic from being sent to broken links and getting lost. Thereby, enhancing network performance and reliability.

The **SD-WAN** page provides detailed link quality measurements with advanced AI insights, to forecast potential issues in the SD-WAN links. It summarizes the overall network health and provides performance data in terms of statistics and trends of latency, jitter, and packet loss metrics.

FortiAIOps base-lines the acceptable link performance of the deployed network to detect and report anomalies in case of SLA breaches. The range and baseline of performance metrics is identified based on historical data, to forecast and report any deviations. This ability of FortiAIOps to forecast the performance of the network, prepares you to effectively handle performance issues that might affect the network health.

FortiAIOps monitors and forecasts latency, jitter, and packet loss for the upcoming week based on available SLAs. It monitors the real time performance of the network to report any changes in the SD-WAN link performance.

- Pre-requisites
- Recommendations

Pre-requisites

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 Link Health Monitor.

Recommendations

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

- Use a time interval of 60 seconds for `sla-fail-log-period` and `sla-pass-log-period` for high accuracy.
- Enable `ntp sync` for accurate SD-WAN forecast and anomaly detection.

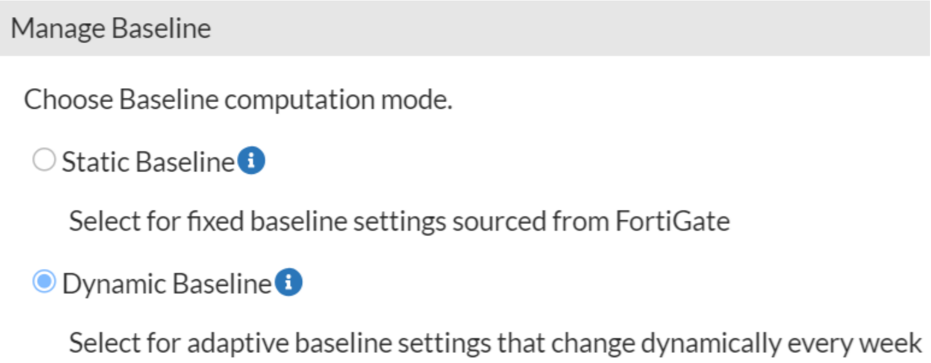
Navigate to **AI Insights > SD-WAN** and select the FortiGate, corresponding health check, and the interface that you want to analyze.

- Configure Baselines
- Performance Summary

- Health Check Trends
- Anomalies

Configure Baselines

Performance SLA baselines are used as the benchmark to analyze the network, forecast its performance, and detect anomalies. You can enable static or dynamic thresholds for assessing the performance of the SD-WAN links. Click **Manage Baselines**.



Manage Baseline

Choose Baseline computation mode.

○ Static Baseline

Select for fixed baseline settings sourced from FortiGate

● Dynamic Baseline

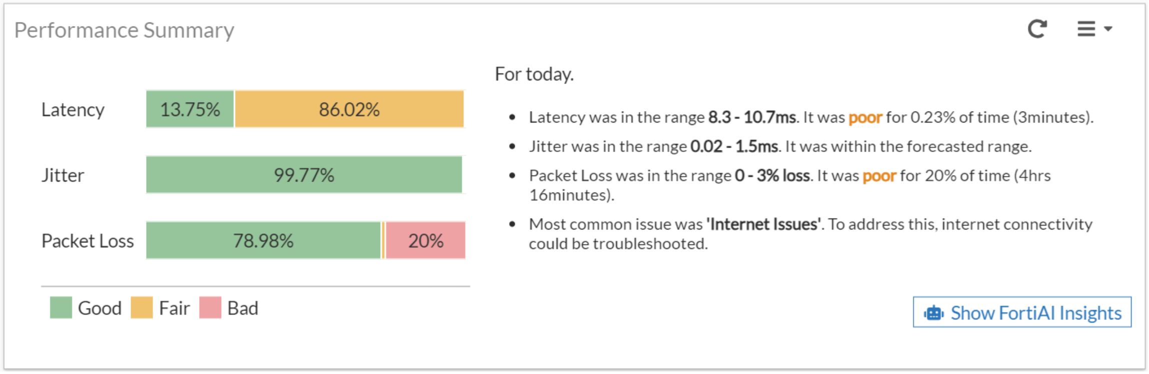
Select for adaptive baseline settings that change dynamically every week

- **Static Baseline** - These baselines are SLA targets configured in FortiGate or FortiAIOps default thresholds, for jitter, packet loss, and latency. If the SLA targets are not specified in FortiGate, then the following default baselines are used for all the 3 metrics.
  - Latency - 100 ms
  - Jitter - 30 ms
  - Packet Loss - 1 %
- **Dynamic Baseline** - These baseline values are calculated using real-time data from the previous week and are updated dynamically, every week, for jitter, packet loss, and latency. This is the default baseline mode.

Note: Fortinet recommends to use SLA targets for the Performance SLA, when static mode is used. The SLA targets are a set of constraints that are used in SD-WAN rules to control the paths that traffic takes. The constraints are configured using the FortiGate GUI and CLI. For more information, see Link health monitor.

Performance Summary

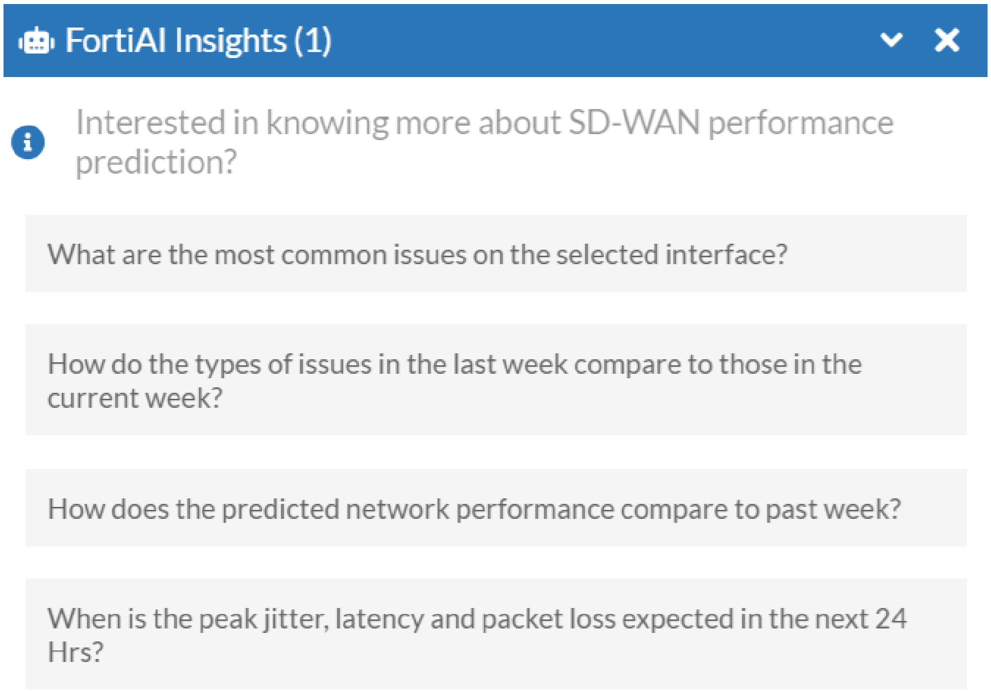
The **Performance Summary** panel provides the statistics for the WAN interface's performance based on the jitter, packet loss, and latency metrics. The events reported are categorized as good, fair, and bad, based on the metric performance with respect to the configured or calculated thresholds. This shows overall summary of the performance metrics, availability of network, and issues for the selected interval. Hover the cursor over the chart to see the break-up of the statistics.



For today.

- Latency was in the range **8.3 - 10.7ms**. It was poor for 0.23% of time (3minutes).
- Jitter was in the range **0.02 - 1.5ms**. It was within the forecasted range.
- Packet Loss was in the range **0 - 3% loss**. It was poor for 20% of time (4hrs 16minutes).
- Most common issue was **'Internet Issues'**. To address this, internet connectivity could be troubleshooted.

To learn more about the SD-WAN interface performance prediction based on the FortiAI insights, click **Show FortiAI Insights**.



FortiAI Insights (1)

Interested in knowing more about SD-WAN performance prediction?

What are the most common issues on the selected interface?

How do the types of issues in the last week compare to those in the current week?

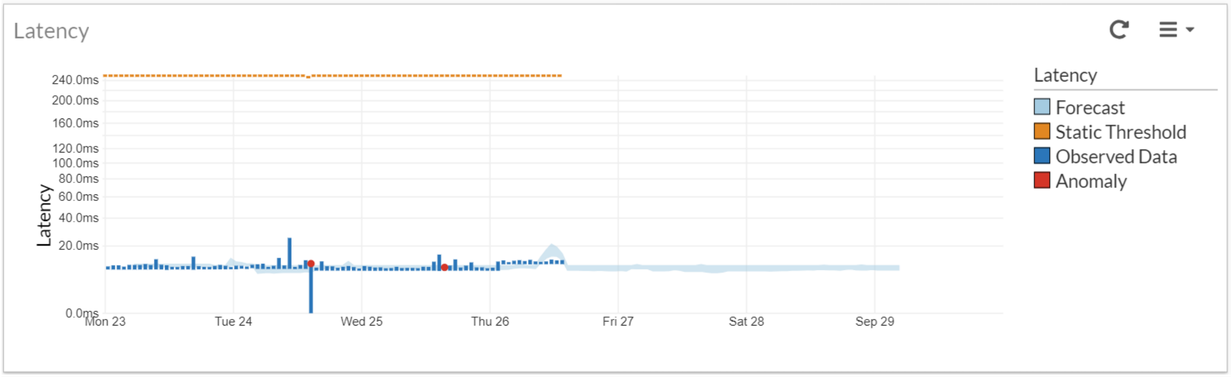
How does the predicted network performance compare to past week?

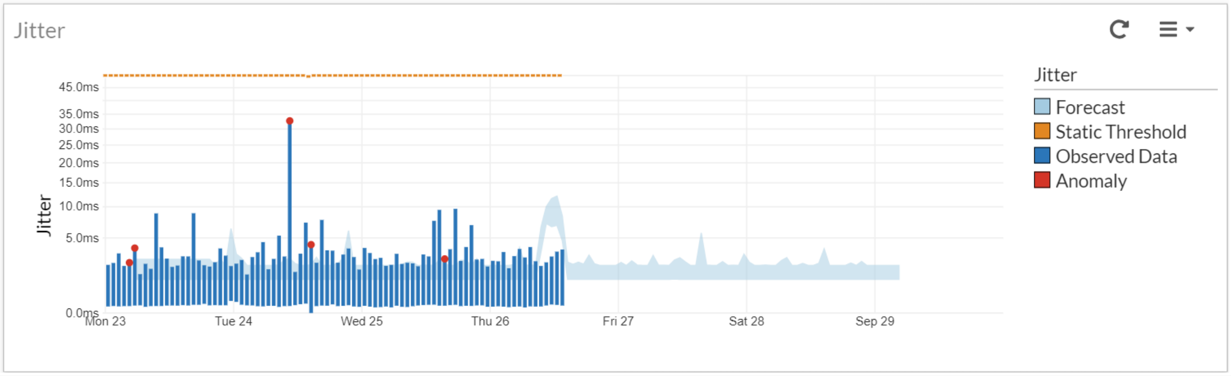
When is the peak jitter, latency and packet loss expected in the next 24 Hrs?

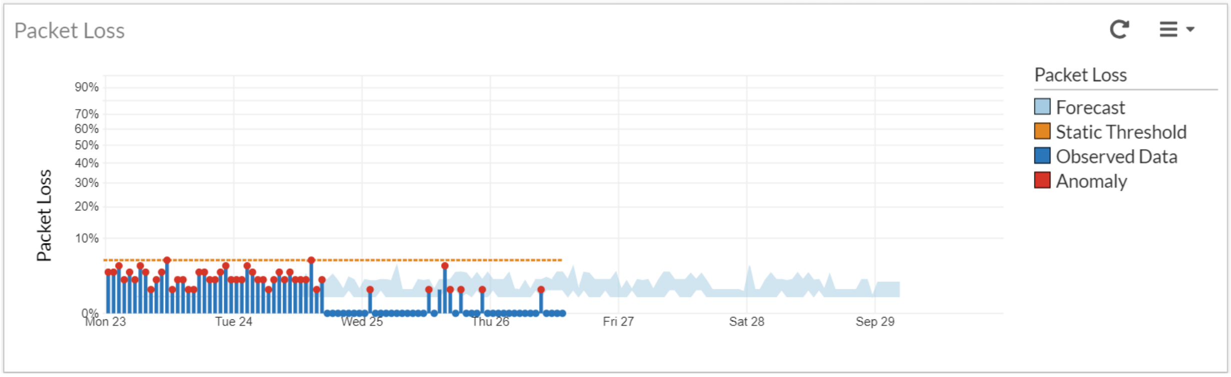
Health Check Trends

The health check graphs display the performance trends for packet loss, latency, and jitter against the predicted/forecasted values, with the anomalies for the selected interface. A comparative view between the following statistics is offered.

Note: The trends displayed are on an hourly basis.



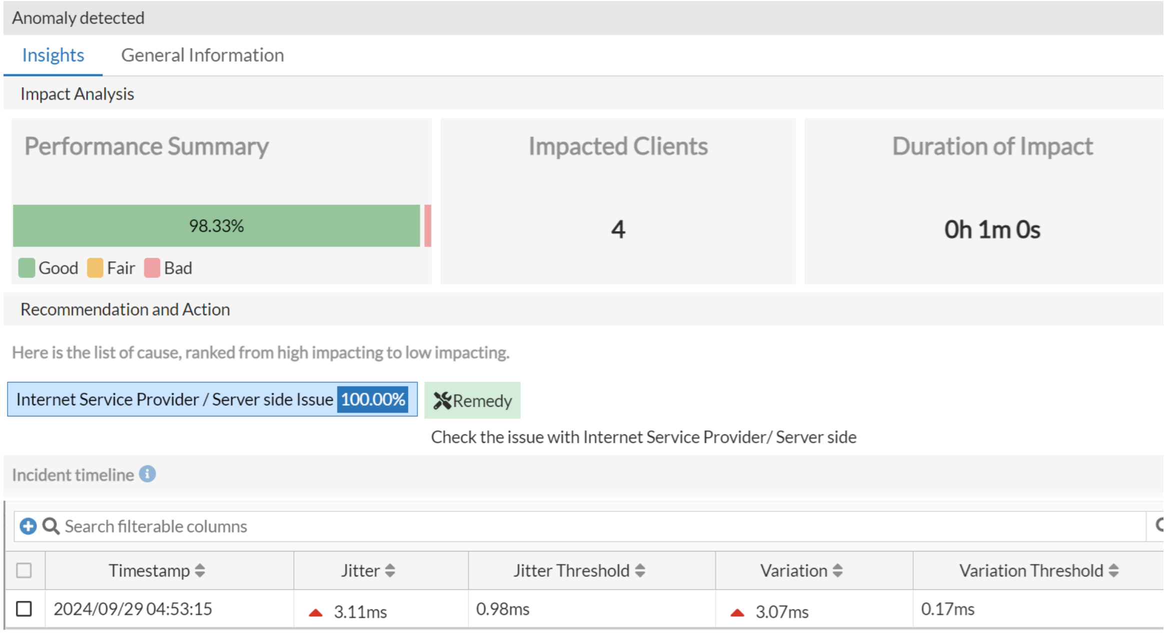




- **Forecast** - This is indicative of the range predicted by FortiAIOps based on historical statistics.
- **Observed Data** - This is the range of real time statistics observed in a given hour.
- **Anomaly** - Anomalies are reported when FortiAIOps observes a deviation in the data exceeding the usual variation in the network, or exceeds the static/dynamic baselines.
- **Static Threshold** - Static SLA baselines are SLA targets that are configured in FortiGate or FortiAIOps default thresholds.

Hover the cursor over the graph to view the statistics for each performance metric. Clicking on anomaly point in the trend graph displays the details.

- **Insights** - This provides the impact analysis for the anomaly that includes the performance summary categorizing the events as good, bad, and fair, the statistics for the impacted clients and the duration of the impact. FortiAIOps lists the cause of the anomaly with the recommended action. The incident timeline provides statistics for when the metric exceeds the threshold values and the observed variation thresholds.



Anomaly detected

Insights | General Information

Impact Analysis

Performance Summary	Impacted Clients	Duration of Impact
98.33% 🟩 Good 🟨 Fair 🟥 Bad	4	0h 1m 0s

Recommendation and Action

Here is the list of cause, ranked from high impacting to low impacting.

Internet Service Provider / Server side Issue 100.00% | Remedy

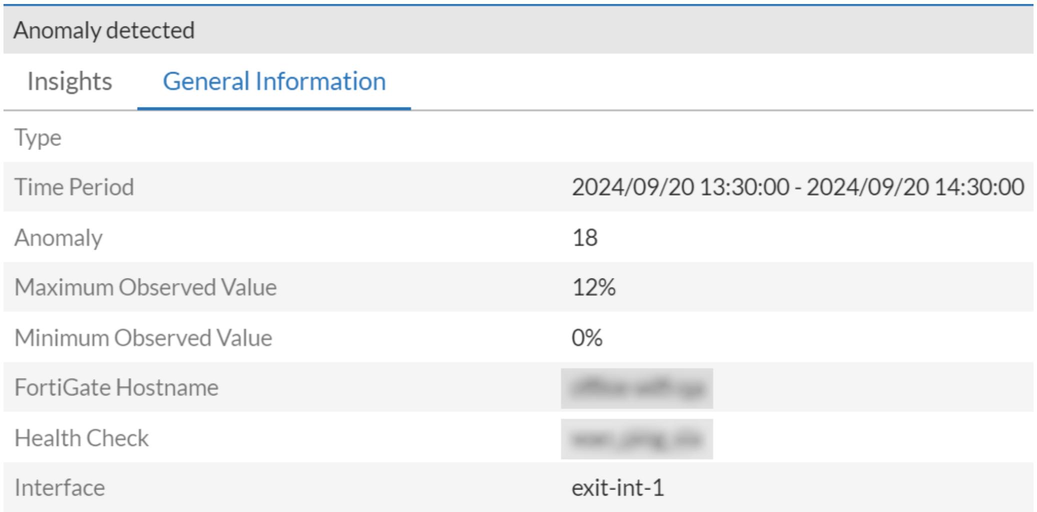
Check the issue with Internet Service Provider/ Server side

Incident timeline

Search filterable columns

□	Timestamp	Jitter	Jitter Threshold	Variation	Variation Threshold
□	2024/09/29 04:53:15	▲ 3.11ms	0.98ms	▲ 3.07ms	0.17ms

- **General Information** - This provides general information about the detected anomaly such as, the duration, the FortiGate host name, interface, configured health check, and so on.



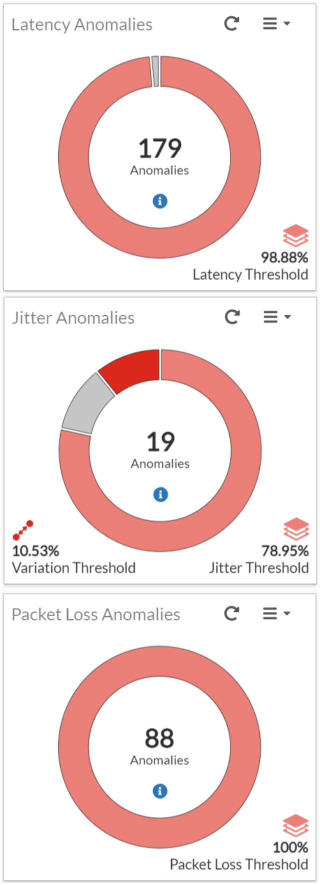
Anomaly detected

Insights | General Information

Type	
Time Period	2024/09/20 13:30:00 - 2024/09/20 14:30:00
Anomaly	18
Maximum Observed Value	12%
Minimum Observed Value	0%
FortiGate Hostname	[redacted]
Health Check	[redacted]
Interface	exit-int-1

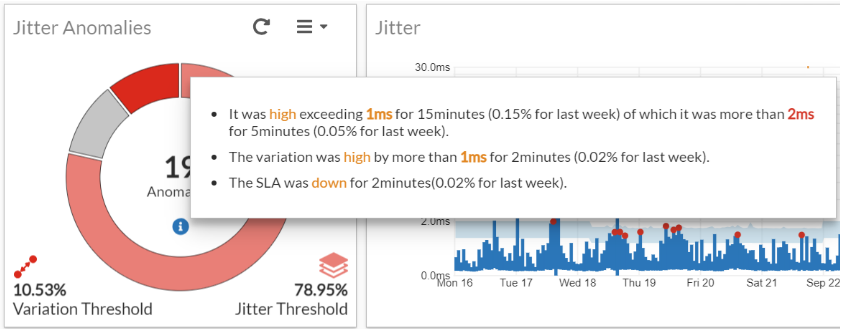
Anomalies

As mentioned earlier, anomalies are reported when a **High Variation** in performance is detected as compared to the usual variations in the network or when the performance exceeds the configured **Upper Threshold** for static or dynamic baselines. The details of these anomalies is displayed in the trend graphs, offering an in-depth analysis of the overall health of the jitter, latency, and packet loss metrics.



Using the anomaly charts, you can view the total number of anomalies classified into high variation, SLA down, and above expected thresholds for the selected duration. Click on the ⓘ icon for additional information.

- **Latency/Jitter/Packet Loss Threshold** - Anomaly observed due to data exceeding the expected threshold.
- **Variation Threshold** - Anomaly observed due to variation exceeding the expected variation.
- **SLA Down** - Anomaly observed due to performance SLA being down.



- It was high exceeding 1ms for 15minutes (0.15% for last week) of which it was more than 2ms for 5minutes (0.05% for last week).
- The variation was high by more than 1ms for 2minutes (0.02% for last week).
- The SLA was down for 2minutes(0.02% for last week).

Switching SLA

This release introduces **Throughput** and **Network** SLAs, and also enhances the existing SLAs of **Switch Health and Uptime** and **Switch Connection Failure**.

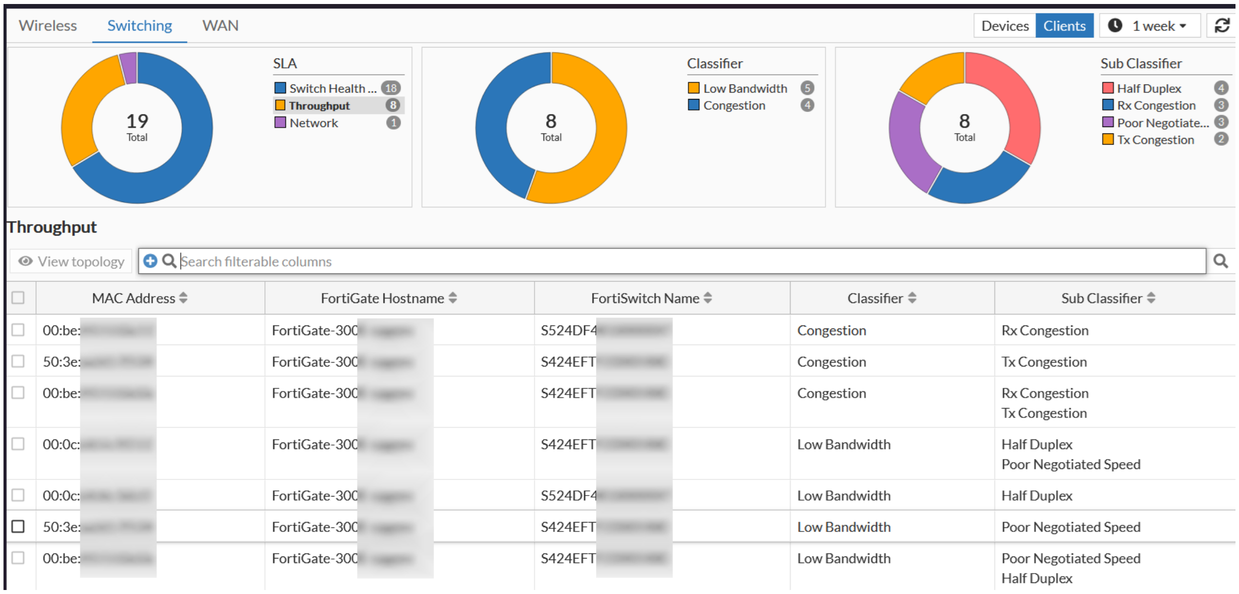
- Throughput
- Network
- Switch Health and Uptime
- Switch Connection Failure

Notes:

- Ensure that all L2 security features, such as, BPDU guard, loop guard, DHCP snooping, root guard are enabled on the switch port to detect STP and DHCP failures.
- DHCP failures are reported only for DHCP configurations in the FortiSwitch, such as, DHCP client blocked, DHCP lease full.

Throughput

This SLA monitors your wired network at the system and client level, to identify potential low throughput conditions and categorizes them based on the underlying issue type, into different classifiers and sub-classifiers. Low throughput is reported based on traffic congestion due to high inbound/outbound traffic, storm conditions, low wired bandwidth conditions leading to network slowdowns, packet drops, and increased latency. Navigate to **Dashboard > AI Insights** and in the **Switching** panel, you can view the details of the throughput SLA.



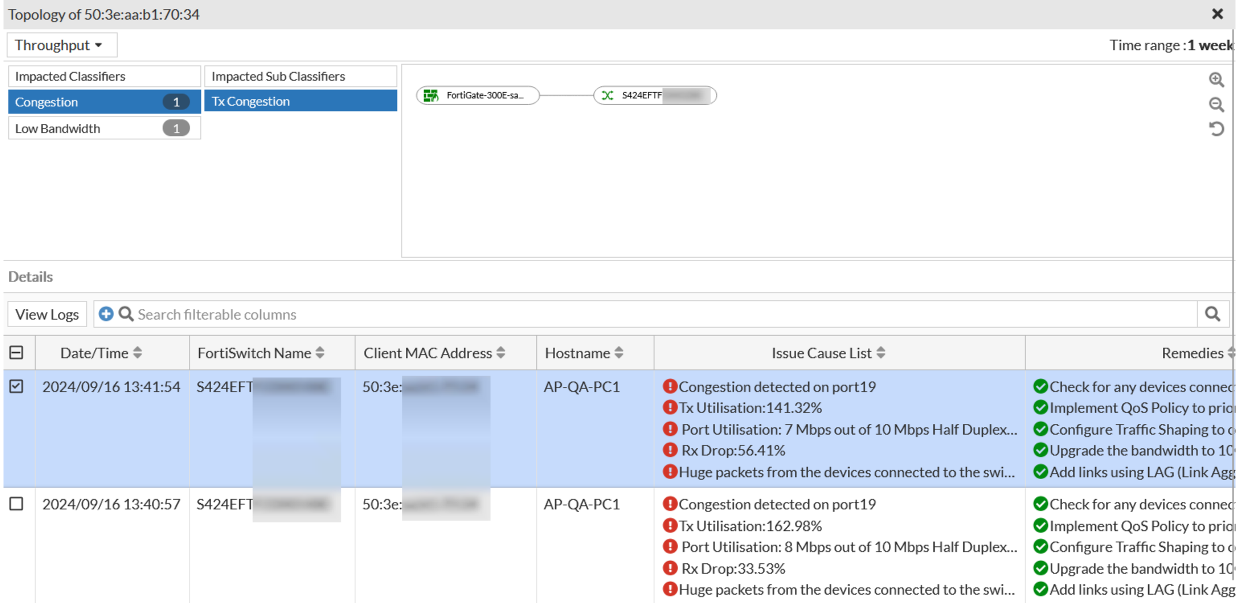
Throughput

□	MAC Address	FortiGate Hostname	FortiSwitch Name	Classifier	Sub Classifier
□	00:be:[redacted]	FortiGate-300[redacted]	S524DF4[redacted]	Congestion	Rx Congestion
□	50:3e:[redacted]	FortiGate-300[redacted]	S424EFT[redacted]	Congestion	Tx Congestion
□	00:be:[redacted]	FortiGate-300[redacted]	S424EFT[redacted]	Congestion	Rx Congestion Tx Congestion
□	00:0c:[redacted]	FortiGate-300[redacted]	S424EFT[redacted]	Low Bandwidth	Half Duplex Poor Negotiated Speed
□	00:0c:[redacted]	FortiGate-300[redacted]	S524DF4[redacted]	Low Bandwidth	Half Duplex
□	50:3e:[redacted]	FortiGate-300[redacted]	S424EFT[redacted]	Low Bandwidth	Poor Negotiated Speed
□	00:be:[redacted]	FortiGate-300[redacted]	S424EFT[redacted]	Low Bandwidth	Poor Negotiated Speed Half Duplex

The **Throughput** table displays information such as the client MAC address, the associated FortiSwitch details, and port details for the reported classifiers and sub classifiers, issue description and the suggested remediation measure, and so on are displayed. Right-click on the header of the table to select the columns that you wish to view.

Attribute	Description
MAC Address	The MAC address of the impacted client device.
FortiGate Hostname	The hostname of the FortiGate associated with the FortiSwitch/impacted client.
FortiSwitch Name	The name of the FortiSwitch that the impacted client associated with.
Classifier	The classifier of the issue reported for the SLA.
Sub Classifier	The sub-classifier of the issue for the reported classifier.
Connecting From	The IP address of the FortiSwitch.
FortiGate Serial Number	The serial number of the FortiGate associated with the FortiSwitch/impacted client.
FortiSwitch Serial Number	The serial number of the FortiSwitch associated with the FortiSwitch/impacted client.
OS Version	The OS version of the FortiSwitch.
Port Name	The FortiSwitch port details.
Status	The status of the FortiSwitch (online/offline).
State	The state of the FortiSwitch (authorized/unauthorized).

Select a row and click **View Topology**. The **Details** table displays the following information.



Topology of 50:3e:aa:b1:70:34 ✕

Throughput ▾ Time range :**1 week**

Impacted Classifiers		Impacted Sub Classifiers
Congestion	1	Tx Congestion
Low Bandwidth	1	

Details

View Logs | Search filterable columns

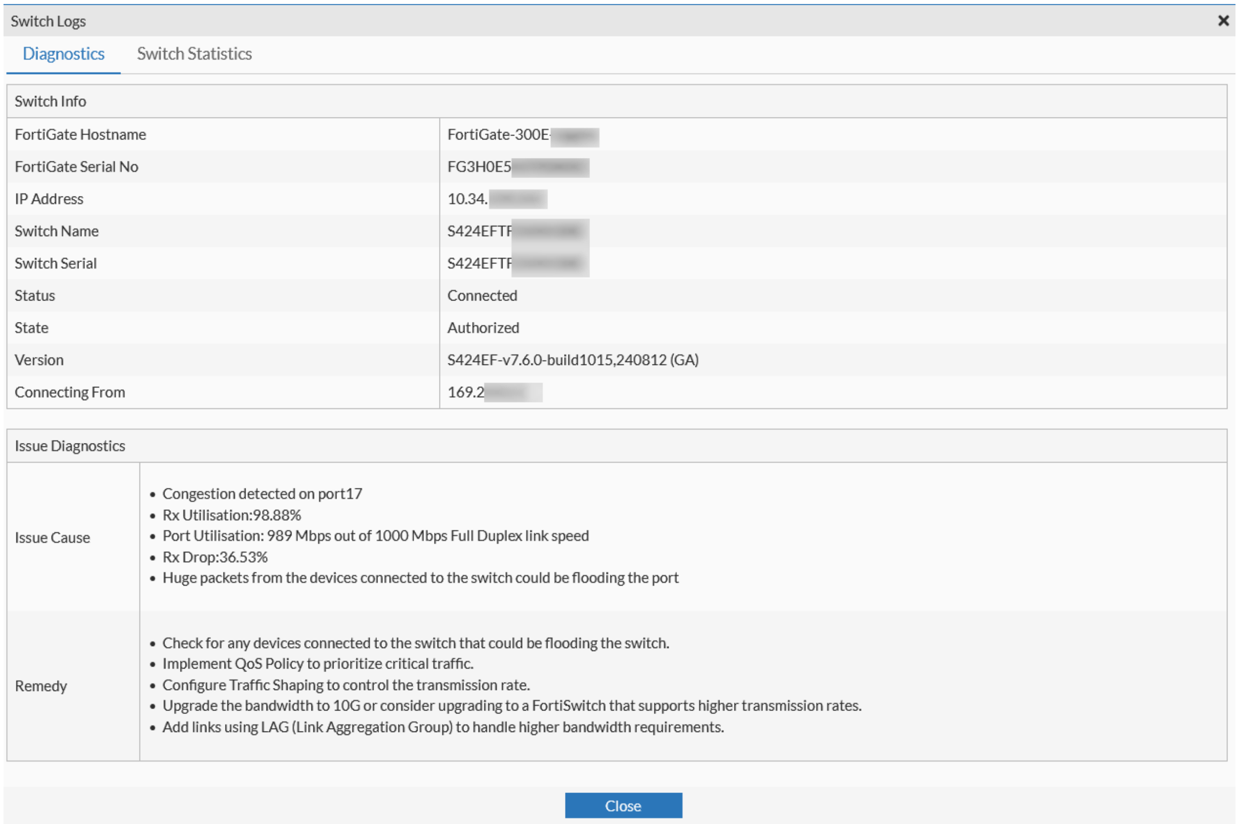
⊟	Date/Time	FortiSwitch Name	Client MAC Address	Hostname	Issue Cause List	Remedies
☑	2024/09/16 13:41:54	S424EFT[redacted]	50:3e:[redacted]	AP-QA-PC1	Congestion detected on port19 Tx Utilisation:141.32% Port Utilisation: 7 Mbps out of 10 Mbps Half Duplex... Rx Drop:56.41% Huge packets from the devices connected to the swi...	Check for any devices connec Implement QoS Policy to prio Configure Traffic Shaping to c Upgrade the bandwidth to 10 Add links using LAG (Link Agg
☐	2024/09/16 13:40:57	S424EFT[redacted]	50:3e:[redacted]	AP-QA-PC1	Congestion detected on port19 Tx Utilisation:162.98% Port Utilisation: 8 Mbps out of 10 Mbps Half Duplex... Rx Drop:33.53% Huge packets from the devices connected to the swi...	Check for any devices connec Implement QoS Policy to prio Configure Traffic Shaping to c Upgrade the bandwidth to 10 Add links using LAG (Link Agg

Right-click on the header of the table to select the columns that you wish to view.

Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
FortiSwitch Name	The name of the impacted switch.

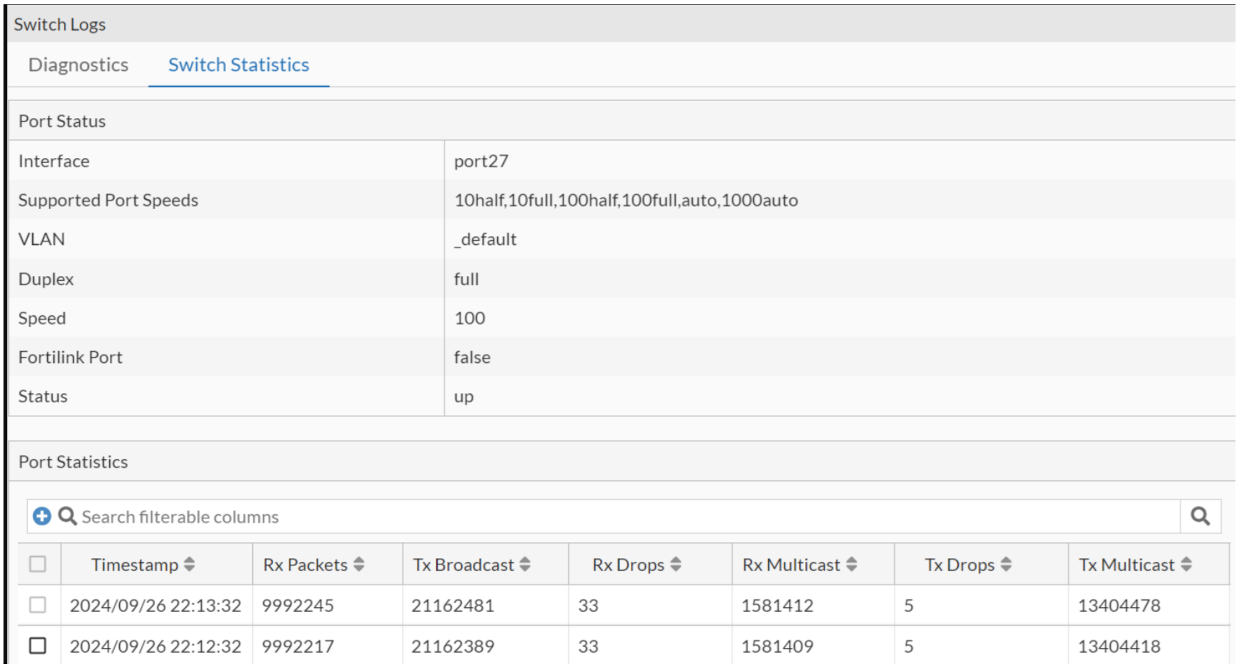
Attribute	Description
Client MAC Address	The MAC address of the impacted client device.
Hostname	The name of the device as configured by the user. If the name is not configured or available, then MAC address is displayed.
Issue Cause List	Detailed cause of the SLA breach that impacted the client/switch.
Remedies	The suggested remedy to resolve the issue.
Classifier	The classifier of the issue reported for the SLA.
Sub Classifier	The sub-classifier of the issue for the reported classifier.
FortiGate Hostname	The hostname of the FortiGate associated with the impacted client.
FortiGate Serial Number	The serial number of the FortiGate associated with the impacted client.
FortiSwitch Serial Number	The serial number of the impacted switch.
Port Name	The FortiSwitch port details.

To view the Switch logs, select a specific row of a **Throughput** event and click **View Logs**. You can view Switch details and diagnostics with the issue description and the suggested remediation, along with the FortiSwitch port statistics.



Switch Info	
FortiGate Hostname	FortiGate-300E-[redacted]
FortiGate Serial No	FG3H0E5[redacted]
IP Address	10.34.[redacted]
Switch Name	S424EFTF[redacted]
Switch Serial	S424EFTF[redacted]
Status	Connected
State	Authorized
Version	S424EF-v7.6.0-build1015,240812 (GA)
Connecting From	169.2[redacted]

Issue Diagnostics	
Issue Cause	• Congestion detected on port17 • Rx Utilisation:98.88% • Port Utilisation: 989 Mbps out of 1000 Mbps Full Duplex link speed • Rx Drop:36.53% • Huge packets from the devices connected to the switch could be flooding the port
Remedy	• Check for any devices connected to the switch that could be flooding the switch. • Implement QoS Policy to prioritize critical traffic. • Configure Traffic Shaping to control the transmission rate. • Upgrade the bandwidth to 10G or consider upgrading to a FortiSwitch that supports higher transmission rates. • Add links using LAG (Link Aggregation Group) to handle higher bandwidth requirements.



Port Status

Interface	port27
Supported Port Speeds	10half,10full,100half,100full,auto,1000auto
VLAN	_default
Duplex	full
Speed	100
Fortilink Port	false
Status	up

Port Statistics

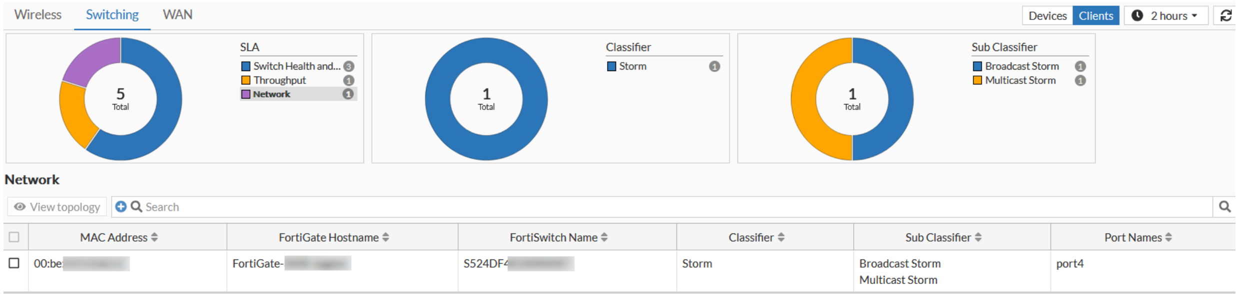
□	Timestamp	Rx Packets	Tx Broadcast	Rx Drops	Rx Multicast	Tx Drops	Tx Multicast
□	2024/09/26 22:13:32	9992245	21162481	33	1581412	5	13404478
□	2024/09/26 22:12:32	9992217	21162389	33	1581409	5	13404418

Network

This SLA monitors the deployed FortiSwitches to predict any potential network disruptions that may lead to poor connectivity. FortiAIOps detects such issues based on monitoring broadcast and multicast storms, possible IP address exhaustion in the DHCP server, or MCLAG issues such as hardware mismatch or peer communication glitches.

Note: The broadcast/multicast storm rate threshold is set to 500 packets per second, storm conditions are reported when this condition is detected. The storm conditions are detected based on this threshold, even if a different storm control policy is configured in FortiGate.

Navigate to **Dashboard > AI Insights** and in the **Switching** panel, you can view the details of the network SLA.



Network

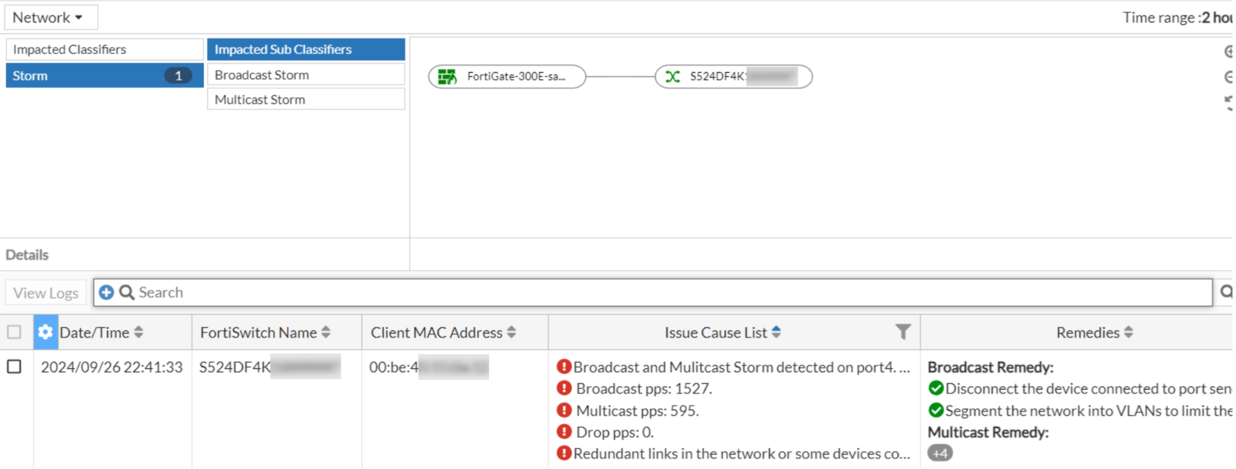
□	MAC Address	FortiGate Hostname	FortiSwitch Name	Classifier	Sub Classifier	Port Names
□	00:be[redacted]	FortiGate-[redacted]	S524DF4[redacted]	Storm	Broadcast Storm Multicast Storm	port4

The **Network** table displays information such as the client MAC address and the associated FortiSwitch details for the reported classifiers and sub classifiers, issue description and the suggested remediation measure, and so on are displayed. Right-click on the header of the table to select the columns that you wish to view.

Attribute	Description
MAC Address	The MAC address of the impacted client device.

Attribute	Description
FortiGate Hostname	The hostname of the FortiGate associated with the FortiSwitch/impacted client.
FortiSwitch Name	The name of the FortiSwitch that the impacted client associated with.
Classifier	The classifier of the issue reported for the SLA.
Sub Classifier	The sub-classifier of the issue for the reported classifier.
Connecting From	The IP address of the FortiSwitch.
FortiGate Serial Number	The serial number of the FortiGate associated with the FortiSwitch/impacted client.
FortiSwitch Serial Number	The serial number of the FortiSwitch associated with the FortiSwitch/impacted client.
OS Version	The OS version of the FortiSwitch.
Port Name	The FortiSwitch port details.
Status	The status of the FortiSwitch (online/offline).
State	The state of the FortiSwitch (authorized/unauthorized).

Select a row and click **View Topology**. The **Details** table displays the following information.



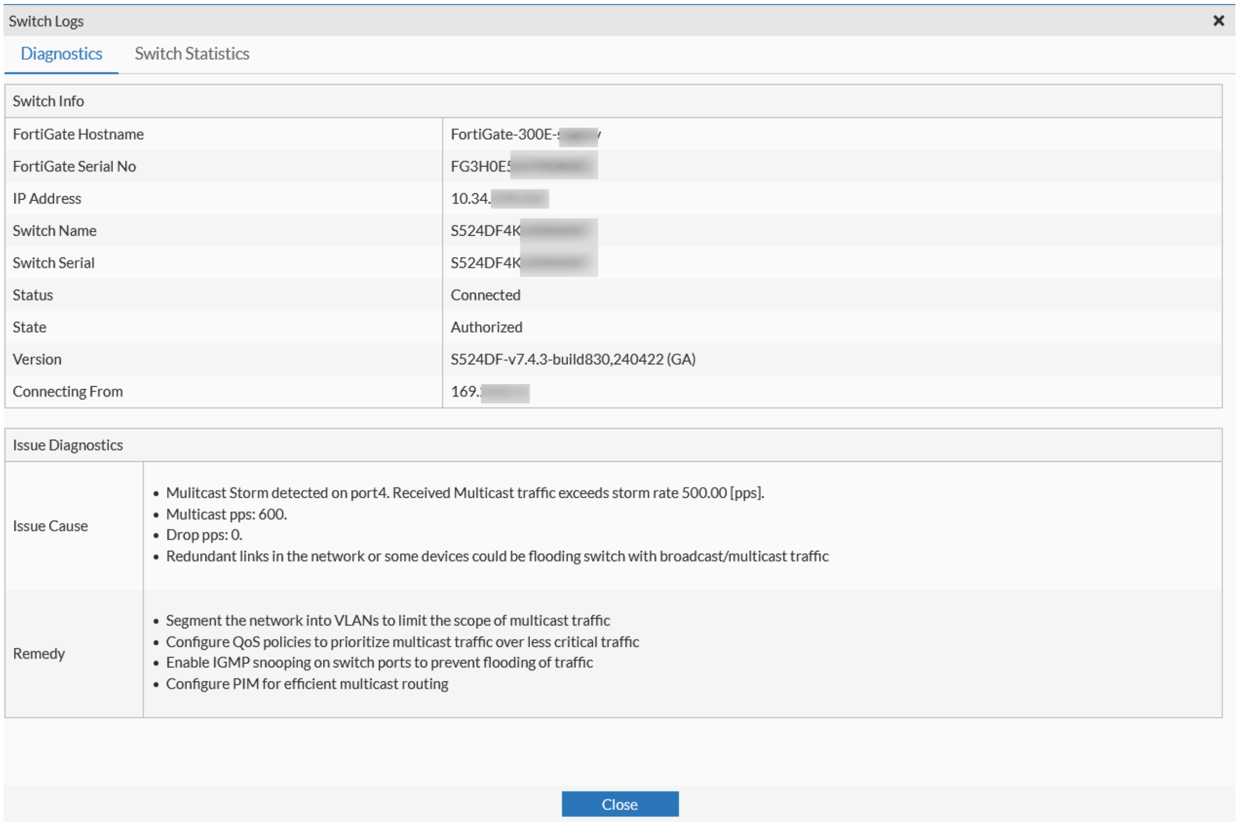
□	Date/Time	FortiSwitch Name	Client MAC Address	Issue Cause List	Remedies
□	2024/09/26 22:41:33	S524DF4K[redacted]	00:be:4[redacted]	Broadcast and Mulitcast Storm detected on port4. ... Broadcast pps: 1527. Multicast pps: 595. Drop pps: 0. Redundant links in the network or some devices co...	**Broadcast Remedy:** ✓ Disconnect the device connected to port sen ✓ Segment the network into VLANs to limit the **Multicast Remedy:** +4

Right-click on the header of the table to select the columns that you wish to view.

Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
FortiSwitch Name	The name of the impacted switch.
Client MAC Address	The MAC address of the impacted client device.
Hostname	The name of the device as configured by the user. If the name is not configured or available, then MAC address is displayed.

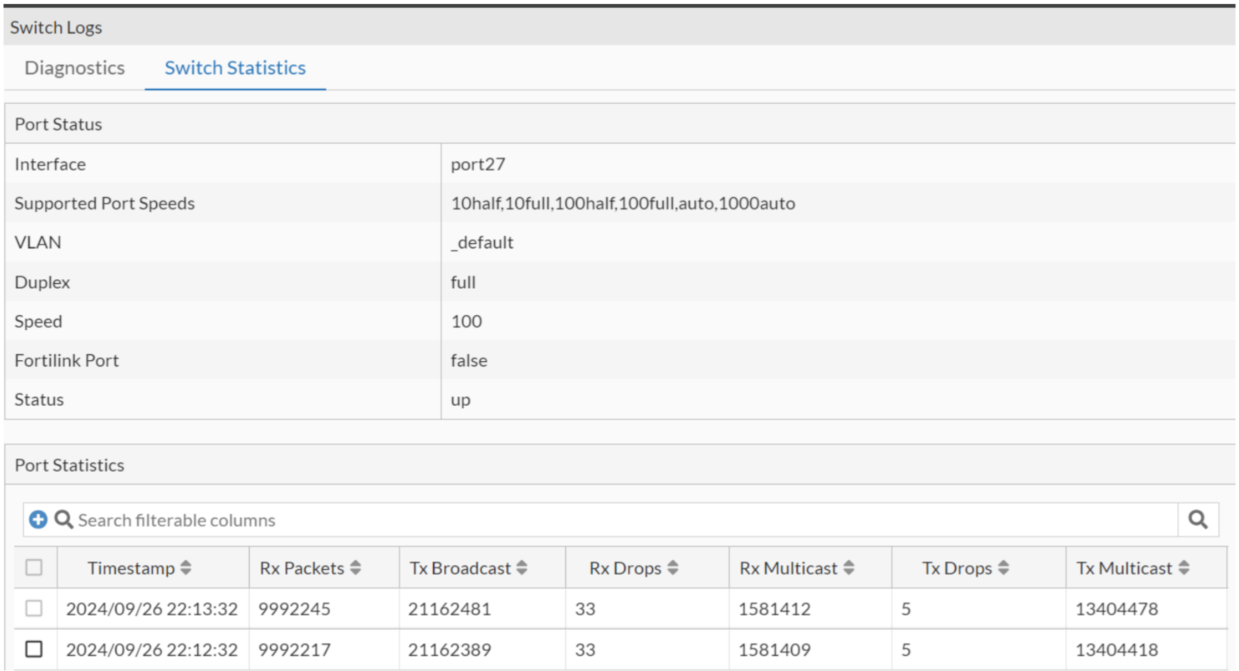
Attribute	Description
Issue Cause List	Detailed cause of the SLA breach that impacted the client/switch.
Remedies	The suggested remedy to resolve the issue.
Classifier	The classifier of the issue reported for the SLA.
Sub Classifier	The sub-classifier of the issue for the reported classifier.
FortiGate Hostname	The hostname of the FortiGate associated with the impacted client.
FortiGate Serial Number	The serial number of the FortiGate associated with the impacted client.
FortiSwitch Serial Number	The serial number of the impacted switch.
Port Name	The FortiSwitch port details.

To view the Switch logs, select a specific row of **Network** SLA event and click **View Logs**. You can view Switch details and diagnostics with the issue description and the suggested remediation, along with the FortiSwitch port statistics.



Switch Info	
FortiGate Hostname	FortiGate-300E-[redacted]
FortiGate Serial No	FG3H0E5[redacted]
IP Address	10.34.[redacted]
Switch Name	S524DF4K[redacted]
Switch Serial	S524DF4K[redacted]
Status	Connected
State	Authorized
Version	S524DF-v7.4.3-build830,240422 (GA)
Connecting From	169.[redacted]

Issue Diagnostics	
Issue Cause	• Mulitcast Storm detected on port4. Received Multicast traffic exceeds storm rate 500.00 [pps]. • Multicast pps: 600. • Drop pps: 0. • Redundant links in the network or some devices could be flooding switch with broadcast/multicast traffic
Remedy	• Segment the network into VLANs to limit the scope of multicast traffic • Configure QoS policies to prioritize multicast traffic over less critical traffic • Enable IGMP snooping on switch ports to prevent flooding of traffic • Configure PIM for efficient multicast routing



Port Status

Interface	port27
Supported Port Speeds	10half,10full,100half,100full,auto,1000auto
VLAN	_default
Duplex	full
Speed	100
Fortilink Port	false
Status	up

Port Statistics

□	Timestamp	Rx Packets	Tx Broadcast	Rx Drops	Rx Multicast	Tx Drops	Tx Multicast
□	2024/09/26 22:13:32	9992245	21162481	33	1581412	5	13404478
□	2024/09/26 22:12:32	9992217	21162389	33	1581409	5	13404418

Switch Health and Uptime

The Switch Health and Uptime SLA determines the health of the switches based on the configured thresholds (CPU, memory, temperature) and events such as uplink and power budget issues, port flapping, port down, switch down, and so on. FortiAIOps displays relevant SLAs under different sections on the **AI Insight** dashboard and the **Impacted SLA** and **Impacted Devices** pages.

Switch Connection Failure

The Switch Connection Failure determines the failed/unsuccessful client connections based on authentication events such as MAC authentication and 802.1x authentication, MAC learning limit, and blocked DHCP clients.

Wireless Enhancements

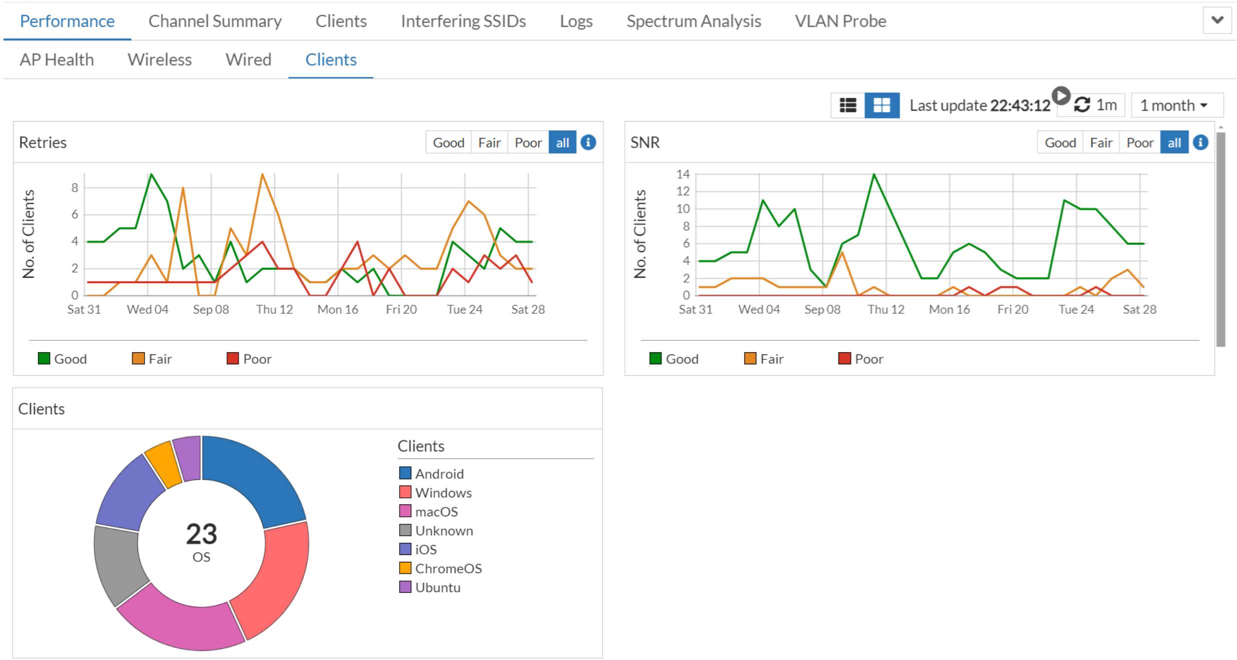
This release provides additional statistics for better assessment of network issues, navigate to **Wireless > Access Points** in the FortiAIOps GUI and click **View Details** .

• Clients - The **Clients** tab is added in the **Performance** page with the panels **Retries**, **SNR**, and **Clients**.

• Wireless - The **Transmission** and **Noise** panels are added in the **Performance > Wireless** page.

Clients

The **Clients** tab helps you monitor your network, based on the retries percentage, SNR, and client distribution. This data is displayed per OS for the selected time interval.



- Retries
- SNR
- Clients

Retries

The statistics for retries are categorized as good, fair, and poor based on the following criteria.

- **Good** - Retries are less than 30%
- **Fair** - Retries are between 31% - 70%
- **Poor** - Retries are more than 70%

SNR

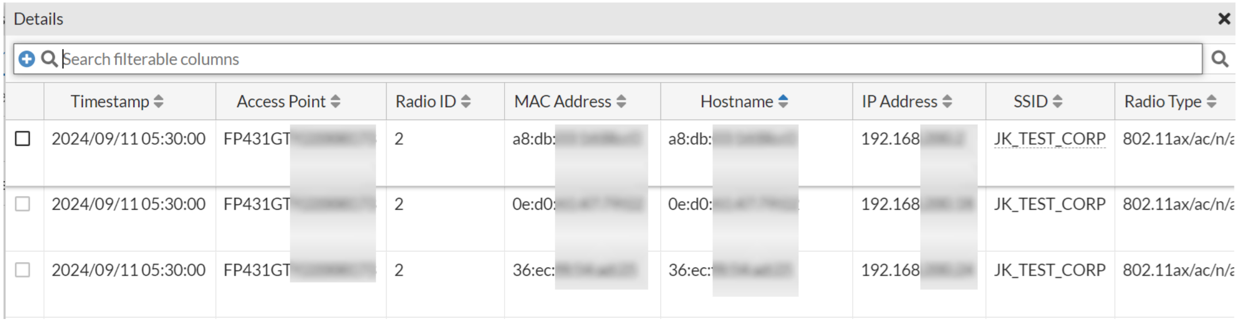
The statistics for SNR are categorized as good, fair, and poor based on the following criteria.

- **Good** – SNR is equal to or greater than 25 dB
- **Fair** – SNR between 15 and 24 dB
- **Poor** – SNR is less than 15 dB

Clients

This panel provides the total number of clients and also the number of clients associated with each OS type. Hover over the graph or the OS name to view details.

To view details for each of the 3 panels, click on the retries and SNR graphs, or on the OS name to view details. The **Details** page displays data such as, the host name, access point and radio details, associated SSID, OS type, throughput, noise, retries, and so on.



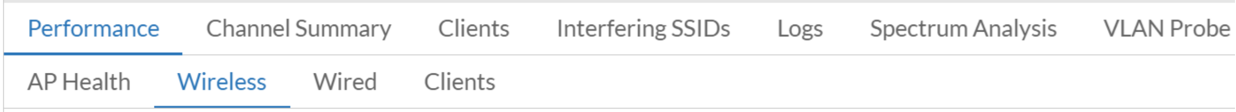
Details

Search filterable columns

	Timestamp	Access Point	Radio ID	MAC Address	Hostname	IP Address	SSID	Radio Type
□	2024/09/11 05:30:00	FP431GT[redacted]	2	a8:db:[redacted]	a8:db:[redacted]	192.168[redacted]	JK_TEST_CORP	802.11ax/ac/n/a
□	2024/09/11 05:30:00	FP431GT[redacted]	2	0e:d0:[redacted]	0e:d0:[redacted]	192.168[redacted]	JK_TEST_CORP	802.11ax/ac/n/a
□	2024/09/11 05:30:00	FP431GT[redacted]	2	36:ec:[redacted]	36:ec:[redacted]	192.168[redacted]	JK_TEST_CORP	802.11ax/ac/n/a

Wireless

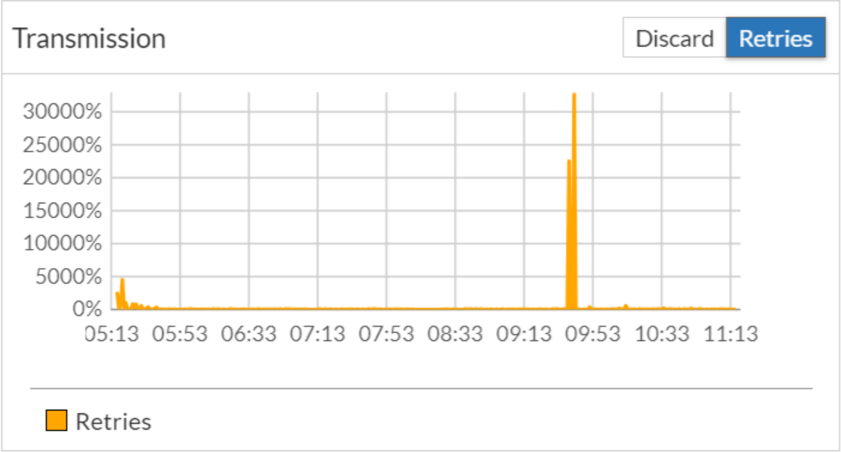
In **Wireless**, additional panels giving details of transmission discard, retries, and noise levels are added.



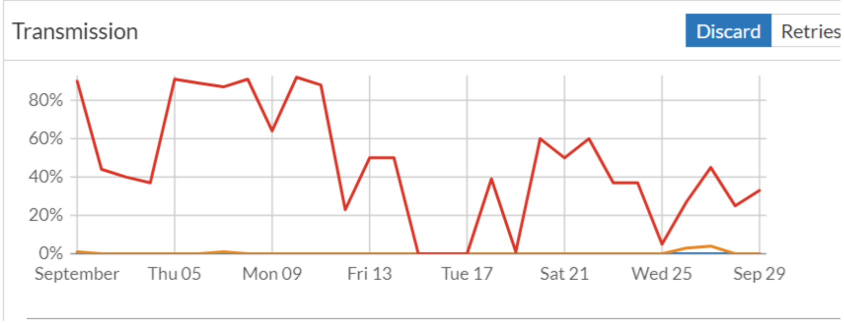
- Transmission
- Noise

Transmission

This panel provides information about transmit discard and retries percentage for the selected time interval, on the respective radio interface.

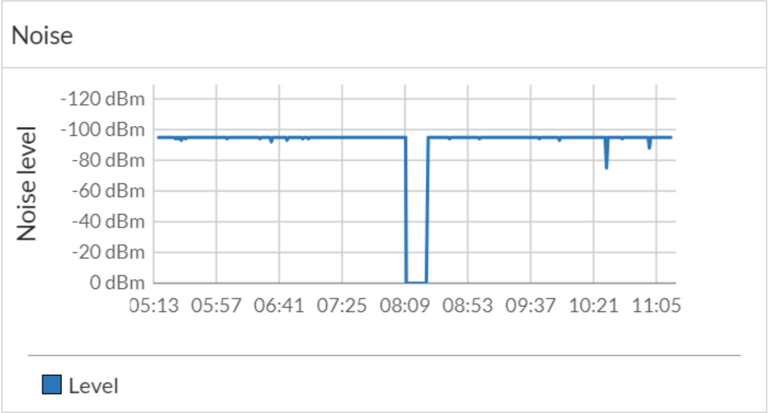


It also provides the minimum, maximum, and average values, when the time interval selected is more than 6 hours as depicted in the following image.

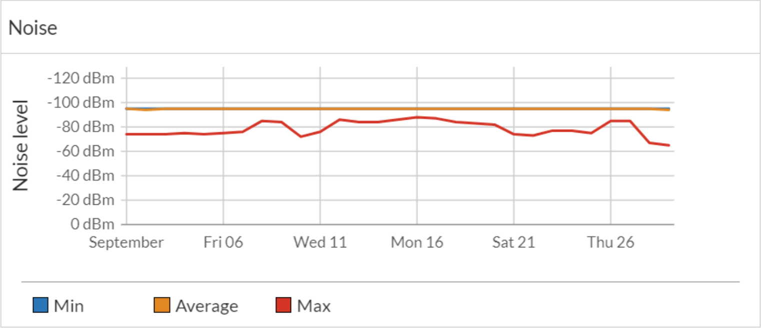


Noise

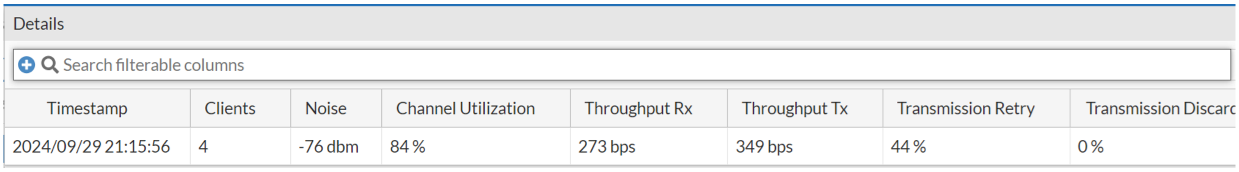
This panel displays the noise values in dBm for the selected time interval on the respective radio interface.



It also provides the minimum, maximum, and average noise values when the time interval selected is more than 6 hours.



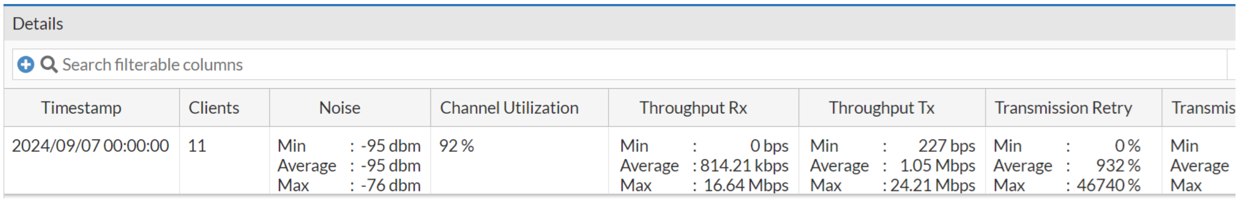
Click on the **Noise** or **Transmission** graphs for a specific time to view details. The following image depicts the noise and transmission details displayed for an interval of less than 6 hours.


Details

Search filterable columns

Timestamp	Clients	Noise	Channel Utilization	Throughput Rx	Throughput Tx	Transmission Retry	Transmission Discard
2024/09/29 21:15:56	4	-76 dbm	84 %	273 bps	349 bps	44 %	0 %

The following image depicts the noise and transmission details displayed for an interval of more than 6 hours.


Details

Search filterable columns

Timestamp	Clients	Noise	Channel Utilization	Throughput Rx	Throughput Tx	Transmission Retry	Transmis
2024/09/07 00:00:00	11	Min : -95 dbm Average : -95 dbm Max : -76 dbm	92 %	Min : 0 bps Average : 814.21 kbps Max : 16.64 Mbps	Min : 227 bps Average : 1.05 Mbps Max : 24.21 Mbps	Min : 0 % Average : 932 % Max : 46740 %	Min Average Max

VDOM Support

VDOMs are used to divide a FortiGate into two or more virtual units that function independently. VDOMs can provide separate security policies and, in NAT mode, completely separate configurations for routing and VPN services for each connected network. When a FortiGate is in multi-VDOM mode, a VDOM can be configured as an *Admin*, *Traffic*, or LAN extension type VDOM. For more information to add a VDOM, see Virtual Domains.

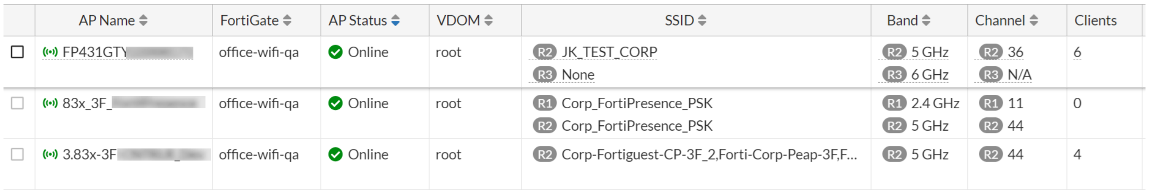
Adding/Managing VDOMs in FortiAIOps

To add and manage FortiGate VDOMs in FortiAIOps, note the following.

- Add the FortiGates using the root VDOM IP address/hostname.
- The FortiAPs, FortiSwitches, and client information displayed in FortiAIOps dashboards is retrieved from all the VDOMs.

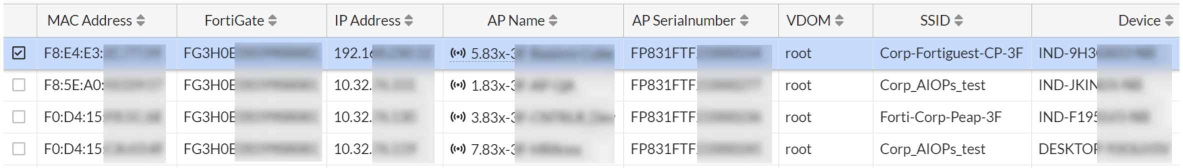
The VDOM information is displayed in the following pages of the FortiAIOps GUI. You can view VDOM information in the **VDOM** column.

- *Wireless > Access Points*



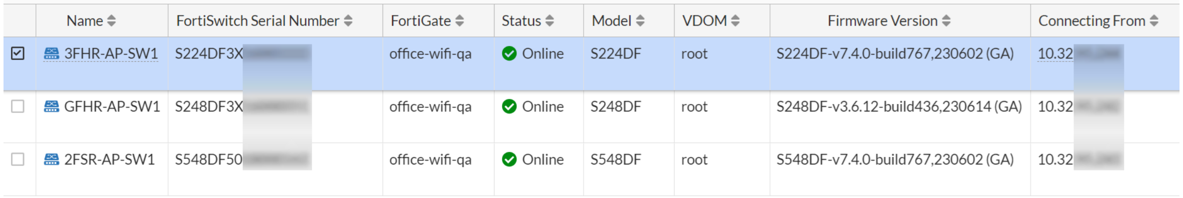
	AP Name ⬍	FortiGate ⬍	AP Status ⬍	VDOM ⬍	SSID ⬍	Band ⬍	Channel ⬍	Clients
□	FP431GTY[redacted]	office-wifi-qa	✓ Online	root	R2 JK_TEST_CORP R3 None	R2 5 GHz R3 6 GHz	R2 36 R3 N/A	6
□	83x_3F_[redacted]	office-wifi-qa	✓ Online	root	R1 Corp_FortiPresence_PSK R2 Corp_FortiPresence_PSK	R1 2.4 GHz R2 5 GHz	R1 11 R2 44	0
□	3.83x-3F[redacted]	office-wifi-qa	✓ Online	root	R2 Corp-Fortiguest-CP-3F_2,Forti-Corp-Peap-3F,F...	R2 5 GHz	R2 44	4

- *Wireless > Clients*



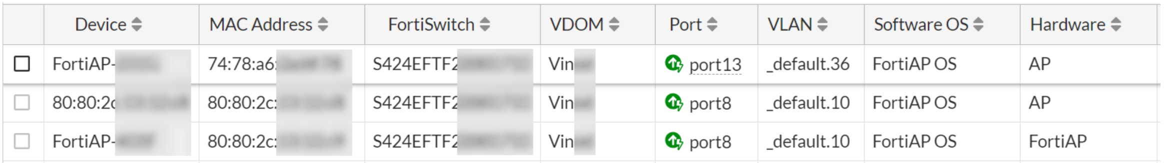
	MAC Address ⬍	FortiGate ⬍	IP Address ⬍	AP Name ⬍	AP Serialnumber ⬍	VDOM ⬍	SSID ⬍	Device ⬍
☑	F8:E4:E3:[redacted]	FG3H0E[redacted]	192.1[redacted]	5.83x-3[redacted]	FP831FTF[redacted]	root	Corp-Fortiguest-CP-3F	IND-9H3[redacted]
□	F8:5E:A0:[redacted]	FG3H0E[redacted]	10.32.[redacted]	1.83x-3[redacted]	FP831FTF[redacted]	root	Corp_AIOPs_test	IND-JKIN[redacted]
□	F0:D4:15[redacted]	FG3H0E[redacted]	10.32.[redacted]	3.83x-3[redacted]	FP831FTF[redacted]	root	Forti-Corp-Peap-3F	IND-F19[redacted]
□	F0:D4:15[redacted]	FG3H0E[redacted]	10.32.[redacted]	7.83x-3[redacted]	FP831FTF[redacted]	root	Corp_AIOPs_test	DESKTO[redacted]

- *Switch > FortiSwitch*



	Name ⬍	FortiSwitch Serial Number ⬍	FortiGate ⬍	Status ⬍	Model ⬍	VDOM ⬍	Firmware Version ⬍	Connecting From ⬍
☑	3FHR-AP-SW1	S224DF3X[redacted]	office-wifi-qa	✓ Online	S224DF	root	S224DF-v7.4.0-build767,230602 (GA)	10.32[redacted]
□	GFHR-AP-SW1	S248DF3X[redacted]	office-wifi-qa	✓ Online	S248DF	root	S248DF-v3.6.12-build436,230614 (GA)	10.32[redacted]
□	2FSR-AP-SW1	S548DF50[redacted]	office-wifi-qa	✓ Online	S548DF	root	S548DF-v7.4.0-build767,230602 (GA)	10.32[redacted]

- *Switch > FortiSwitch Clients*



	Device ⬍	MAC Address ⬍	FortiSwitch ⬍	VDOM ⬍	Port ⬍	VLAN ⬍	Software OS ⬍	Hardware ⬍
□	FortiAP-[redacted]	74:78:a6:[redacted]	S424EFTF2[redacted]	Vin[redacted]	port13	_default.36	FortiAP OS	AP
□	80:80:2c[redacted]	80:80:2c:[redacted]	S424EFTF2[redacted]	Vin[redacted]	port8	_default.10	FortiAP OS	AP
□	FortiAP-[redacted]	80:80:2c:[redacted]	S424EFTF2[redacted]	Vin[redacted]	port8	_default.10	FortiAP OS	FortiAP

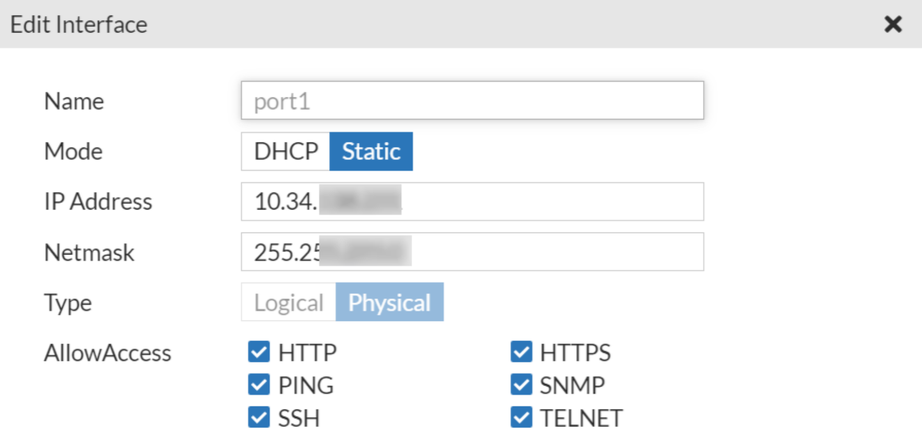
The following limitations apply on VDOM usage in this release of FortiAIOps.

- Monitoring and managing individual VDOMs is not supported currently; hence, data from all VDOMs is displayed in FortiAIOps.

- Moving a FortiGate between device groups moves all the VDOMs.
- The AI Insights dashboards do not display VDOM separation.

Network Interfaces

You can configure FortiAIOps with 4 active physical interfaces for VM deployments. The administrators can configure access protocols like HTTP, HTTPS, and so on, on a per interface basis. Navigate to **System > Network**.



Edit Interface ✕

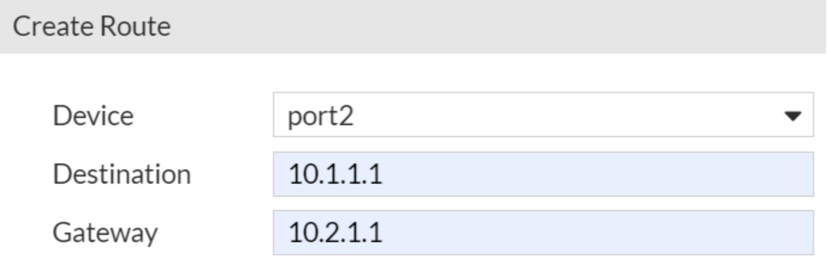
Name	port1	
Mode	DHCP [✓ Static]	
IP Address	10.34.[redacted]	
Netmask	255.25[redacted]	
Type	Logical [✓ Physical]	
AllowAccess	☑ HTTP	☑ HTTPS
	☑ PING	☑ SNMP
	☑ SSH	☑ TELNET

Select a port and click **Edit** to modify the following settings as required.

- **Mode** - Configure the port IP address mode; **Static** or **DHCP**.
- **IP Address & Netmask** - Enter the IPv4 address and netmask associated with this interface.
- **AllowAccess** - Select the allowed administrative access protocols from the following.
  - SSH
  - HTTP
  - HTTPS
  - Ping
  - SNMP
  - Telnet

Click **Update**.

In the **Static Routes** tab, you can create a default route to your network gateway on the interface that connects to the gateway. You can create, edit, or delete routes as required.

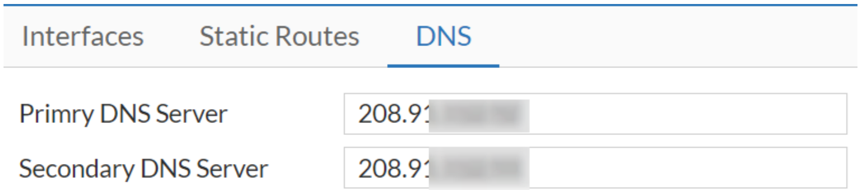


Create Route

Device	port2 ▾
Destination	10.1.1.1
Gateway	10.2.1.1

- **Device** - Select the network interface that connects to the gateway.
- **Destination** - The destination IP address and netmask for this route.
- **Gateway** - Enter the IP address of the next hop router to which this route directs traffic

You can configure the DNS server settings. Enter the IP addresses for the **Primary DNS Server** and **Secondary DNS Server**.

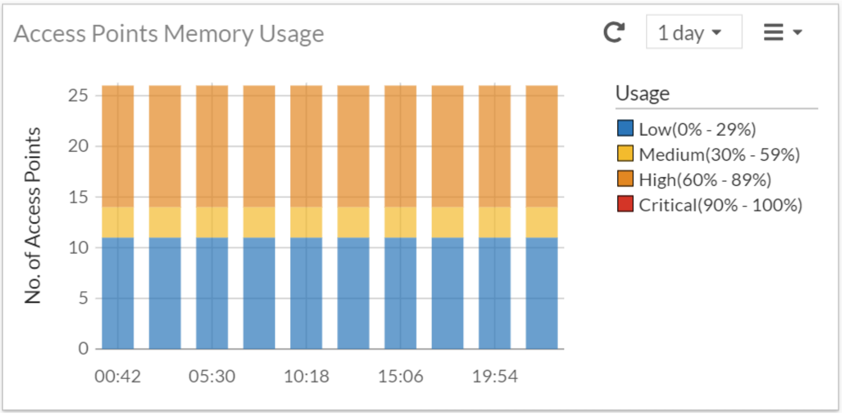


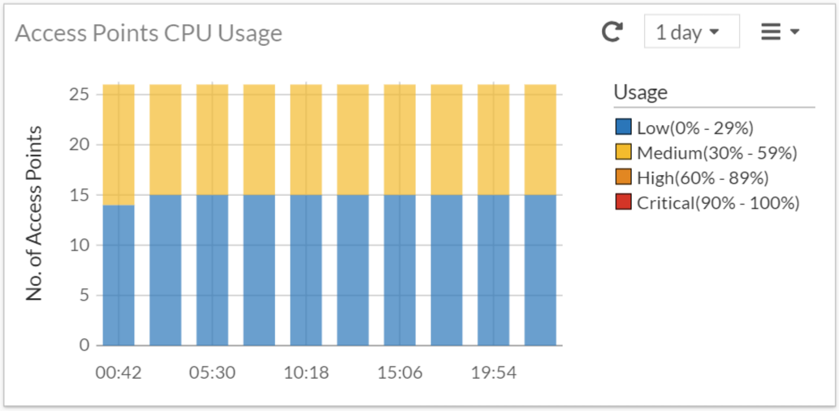
Primry DNS Server	208.91[redacted]
Secondary DNS Server	208.91[redacted]

Summary Dashboard Enhancements

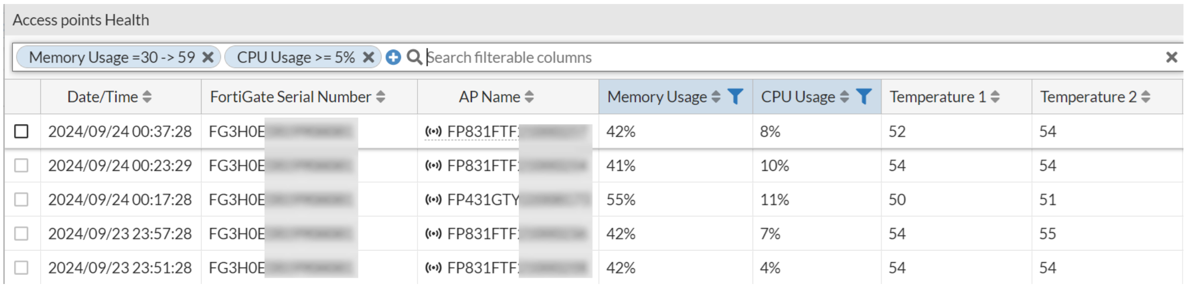
The following enhancements are delivered in the summary dashboard.

- **Access Points CPU** and **Memory Usage** – Displays the real-time FortiAP CPU and memory usage at a given time and categorizes it as *Low, Medium, High*, and *Critical*. You can select the period to view the resource usage (10 or 30 minutes, 1 or 12 hours, or 1 day).





Click on the memory and CPU graphs to view the details, as depicted in the following image.

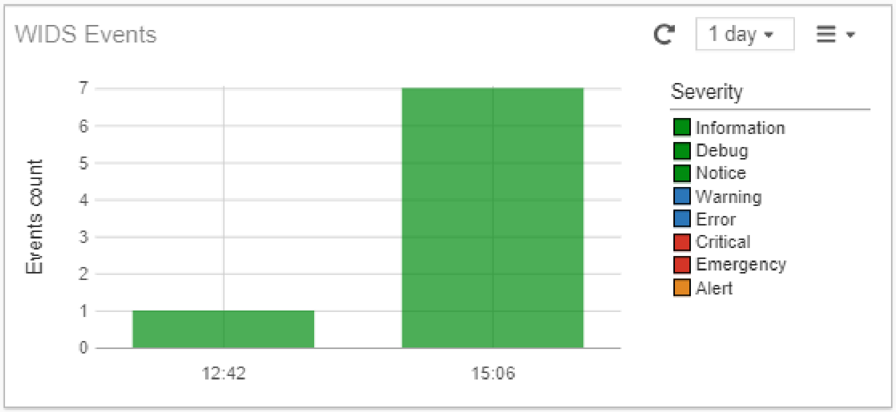


Access points Health

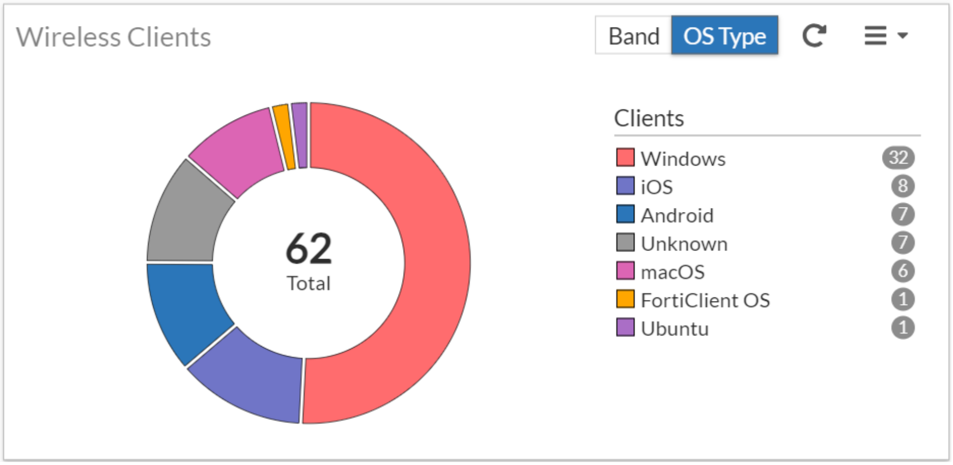
Memory Usage =30 -> 59 ✕ CPU Usage >= 5% ✕ Search filterable columns ✕

□	Date/Time	FortiGate Serial Number	AP Name	Memory Usage	CPU Usage	Temperature 1	Temperature 2
□	2024/09/24 00:37:28	FG3H0E[redacted]	FP831FTF[redacted]	42%	8%	52	54
□	2024/09/24 00:23:29	FG3H0E[redacted]	FP831FTF[redacted]	41%	10%	54	54
□	2024/09/24 00:17:28	FG3H0E[redacted]	FP431GTY[redacted]	55%	11%	50	51
□	2024/09/23 23:57:28	FG3H0E[redacted]	FP831FTF[redacted]	42%	7%	54	55
□	2024/09/23 23:51:28	FG3H0E[redacted]	FP831FTF[redacted]	42%	4%	54	54

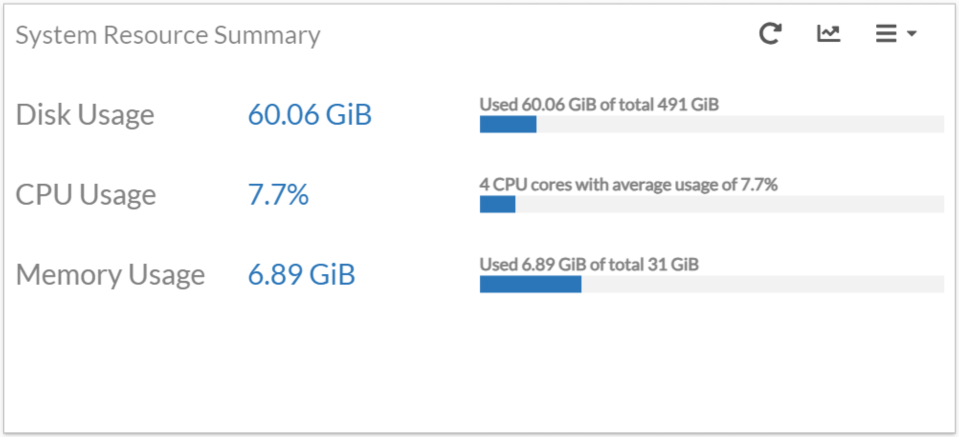
- **WIDS Events** – Displays the real-time wireless WIDS events and categorizes them based on the severity level as, *Information, Debug, Notice, Warning, Error, Critical, Emergency*, and *Alert*. You can select the period to view the data (10 or 30 minutes, 1 or 12 hours, or 1 day).



- The **Wireless Clients** panel now provides representation for clients based on the OS type.



- The **System Resource Summary** panel now displays usage for both HDD and SSD.


System Resource Summary

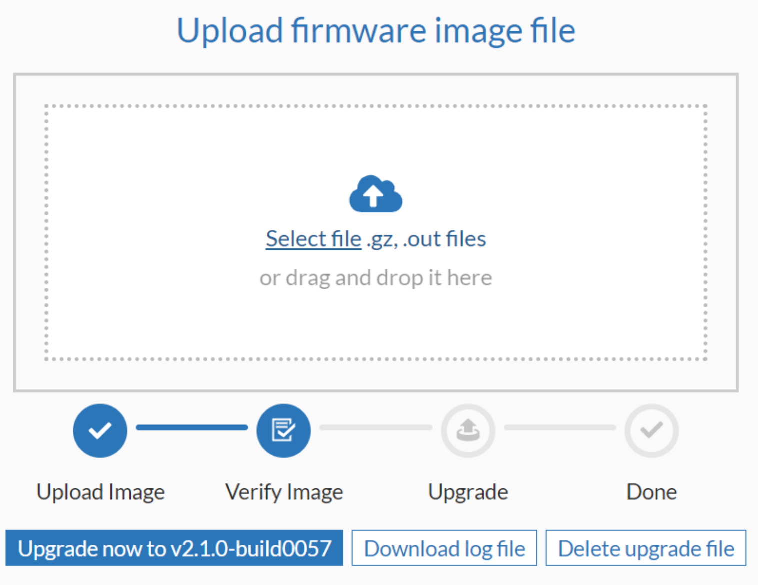
Disk Usage 60.06 GiB Used 60.06 GiB of total 491 GiB

CPU Usage 7.7% 4 CPU cores with average usage of 7.7%

Memory Usage 6.89 GiB Used 6.89 GiB of total 31 GiB

Upgrade via GUI

You can now upgrade FortiAIOps via the GUI. Navigate to **System > Upgrade** and upload the FortiAIOps image file.

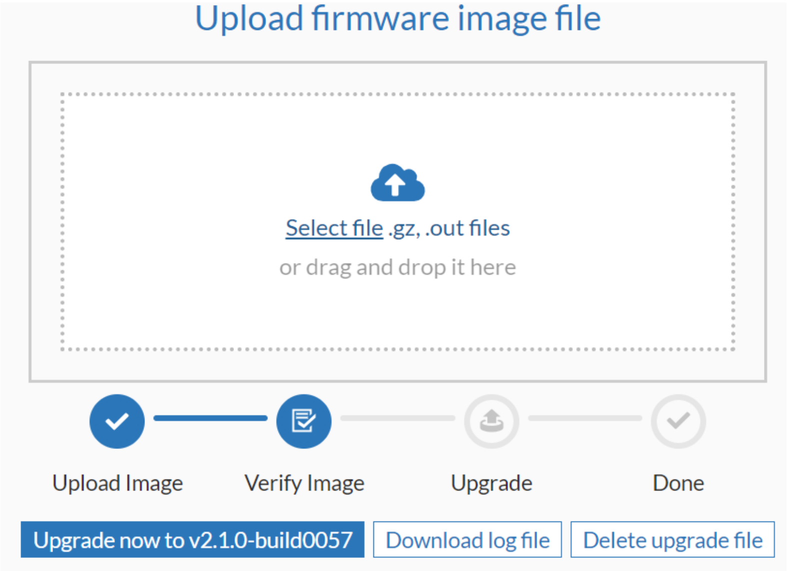


Upload firmware image file

Select file .gz, .out files

or drag and drop it here

1. Browse to the image file or drag and drop it in the upgrade window. Click **Upload**.
2. After successfully uploading the file, click **Upgrade Now** to upgrade FortiAIOps to the uploaded version.



Upload firmware image file

Select file .gz, .out files

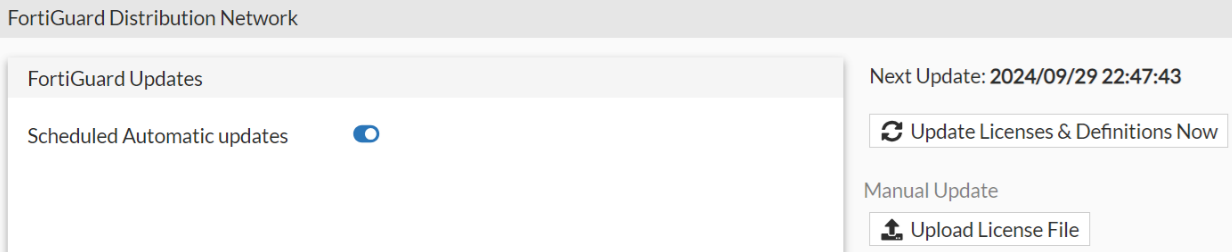
or drag and drop it here

You can also chose to cancel an ongoing upload or delete the uploaded file. To download the log file with the upgrade status, click **Download log file**.

FortiGuard Updates

You can now enable automatic updates for the FortiGuard Distribution Network (FDN) license, for accurate license data synchronization. Navigate to **System > FortiGuard** and enable **Scheduled Automatic updates**. FortiAIOps displays the time for the next scheduled update, if you require an immediate update, click **Update License and Definitions Now**.

After successfully obtaining the license file from Fortinet, you can upload it on this page. Click **Upload License File**.



FortiGuard Distribution Network

FortiGuard Updates

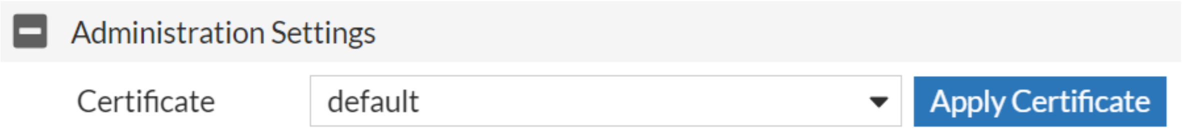
Scheduled Automatic updates ●

Next Update: **2024/09/29 22:47:43**

Additional Settings

The following additional settings are added in this release, navigate to **System > Settings**.

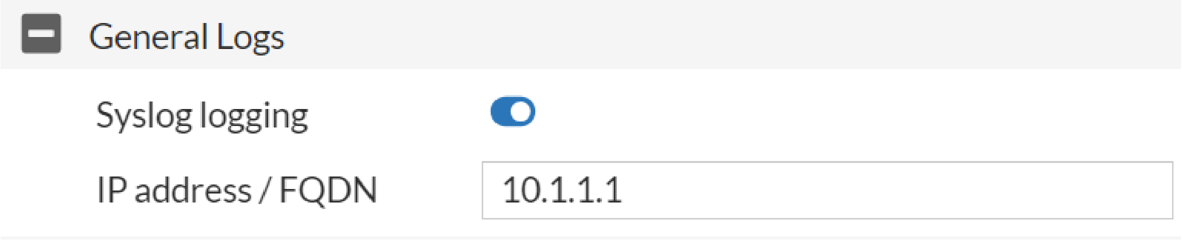
- **Administration Settings** – You can select and apply a certificate that is generated/imported in **System > Certificates** and click **Apply Certificate**.



Administration Settings

Certificate: default

- **Syslog** - You can now configure forwarding FortiAIOps local logs to a remote machine. Enable **Syslog logging** and enter the IP address/FQDN of remote machine where logs are to be stored.



General Logs

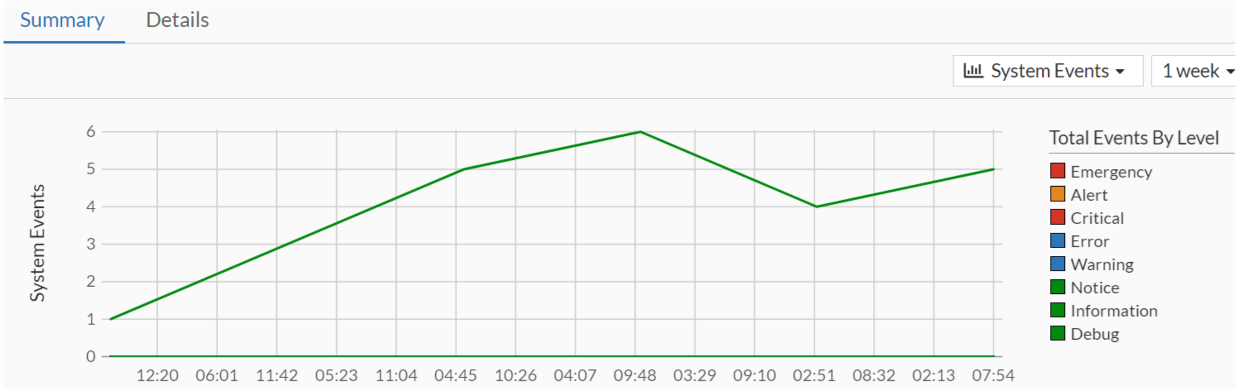
Syslog logging: ●

IP address / FQDN: 10.1.1.1

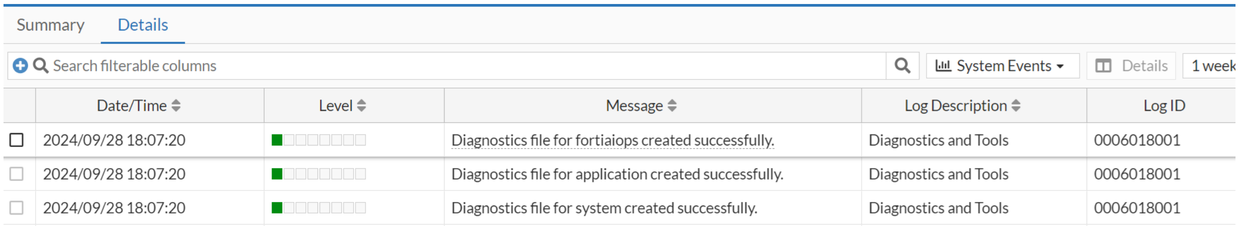
Note: If the configured syslog server IP address/FQDN is incorrect or not reachable, then the syslog messages are not logged.

Local Logs

This release of FortiAIOps introduces the local logs that provide key insights into the system, configuration, reports, license, SAM, and mail events. Navigate to **Logs & Reports > Local Logs** and select the time interval to access the logs for. The **Summary** tab displays the top five most frequent events in each type of event log along with the severity level and the total count. A line chart displays aggregated events by each severity level. Clicking on a peak in the line chart displays the specific event count for the selected severity level.



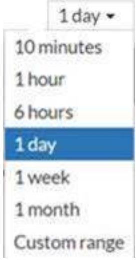
The **Details** page for that event type filtered by the selected time span. You can select the time frame to view the logs from the top-right corner of the GUI.



	Date/Time	Level	Message	Log Description	Log ID
□	2024/09/28 18:07:20	🟩□□□□□□□	Diagnostics file for fortiaiops created successfully.	Diagnostics and Tools	0006018001
□	2024/09/28 18:07:20	🟩□□□□□□□	Diagnostics file for application created successfully.	Diagnostics and Tools	0006018001
□	2024/09/28 18:07:20	🟩□□□□□□□	Diagnostics file for system created successfully.	Diagnostics and Tools	0006018001

Time Range Selection

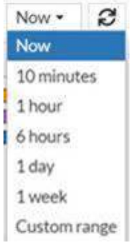
This feature allows you to view data based on the selected duration or customized time slot. You can select a time window or define a **Custom range**. The custom range allows the selection of a minimum of 1 day and the maximum is the duration of log retention configured in **System > Settings**.



This feature is available for the following data and statistics.

- **Dashboard > Summary > System Resource Summary (Details)**
- **Inventory > Managed FortiGates > View Details**
  - Performance
  - Channel Summary > Trends
  - FortiAPs > View Details
  - Clients > View Details
  - FortiSwitches > View Details
- **Wireless > Access Points > View Details**
  - Performance
  - Channel Summary > Trends
  - Clients > View Details
- **Wireless > Channel Summary > Trends**
- **Wireless > Applications > Trends** (**Apps by Usage** and **Users by Usage**)
- **Switch > FortiSwitch > View Details > Statistics** (**Ports** and **Switches**)

The wireless and switching client data can be filtered based on the selected duration or customized time slot with the additional option of **Now**, which displays data for the last 1 minute. The **Custom range** allows the selection of a minimum of 1 hour and maximum of 1 week.



- **Wireless > Clients**
- **Switch > FortiSwitch Clients**

CLI Enhancements

The following new commands are added in this release of FortiAIOps.

- The *DNS No Domain* events are disabled in FortiAIOps, by default. Run the following commands to enable these events.

  ```
  execute dns-no-domain
     disable <disable the events>
     enable <enable the events>
     status <show the current setting>
  ```

- LLDP is enabled by default on all interfaces, global and per interface settings. Run the following commands to manage LLDP.

  ```
  config system global
       set lldp-transmission
       enable <enable LLDP>
       disable <disable LLDP>
  ```

Deploying FortiAIOps

This release provides additional FortiAIOps deployment support for Proxmox and Oracle.

- VM Platform - Proxmox Support
- Public Cloud Platform - Oracle Cloud Infrastructure (OCI)

VM Platform - Proxmox Support

Perform the following steps to deploy FortiAIOps on the Proxmox KVM platform.

1. Obtain *FAO_VM64_KVM-v2.0.1-[build0xxx]-FORTINET.out.kvm.zip* from Fortinet.
2. Use SCP to transfer this file to a Proxmox machine and extract it.

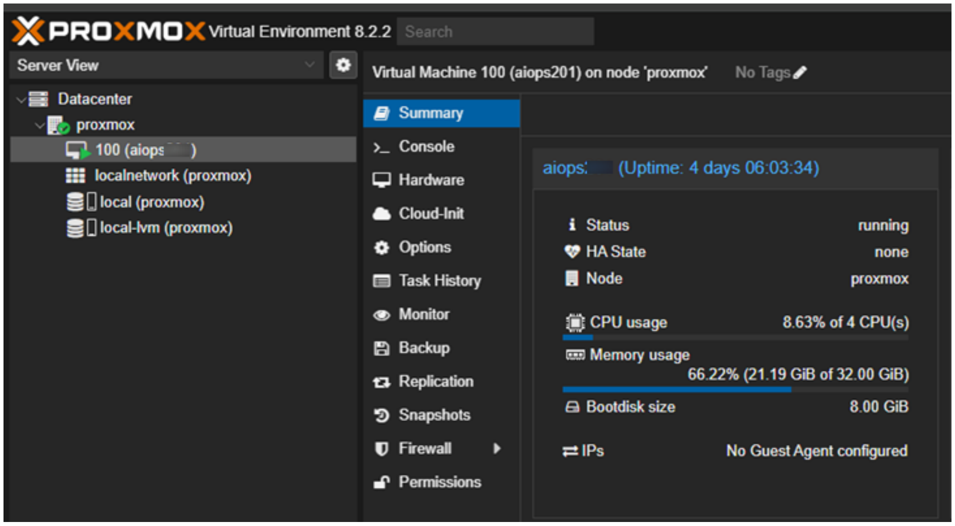
```
unzip FAO_VM64_KVM-v2.0.1-[build0xxx]-FORTINET.out.kvm.zip
-rwxrwxr-x 1 root root 3653632 May 9 12:06 OVMF_CODE_4M.secboot.fd
-rwxrwxr-x 1 root root 540672 May 9 12:06 Fimg_VARS.fd
-rw-r--r-- 1 root root 1394802688 May 9 12:20 FAOKVM.qcow2
-rwxr-xr-x 1 root root 1964 May 9 12:20 deploy_pmx
-rwxr-xr-x 1 root root 4112 May 9 12:20 deploy_kvm
-rw-r--r-- 1 root root 204608 May 9 12:20 datadrive.qcow2
-rw-r--r-- 1 root root 4521984 May 9 12:20 OVMF.qcow2
-rwxr-xr-x 1 root root 2749 May 9 12:20 KVM.xml.tmpl
-rw-r--r-- 1 root root 1358948555 May 9 16:48 FAO_VM64_KVM-v2.0.1-
[build0xxx]-FORTINET.out.kvm.zip
```

3. Import the FortiAIOps disk image manually in the Proxmox shell to create the VM.

```
./deploy_pmx <name> local-lvm vmbr0
```

   Where `<name>` is the name of the VM.

4. The VM is now deployed.



Virtual Machine 100 (aiops201) on node 'proxmox'

aiops[redacted] (Uptime: 4 days 06:03:34)

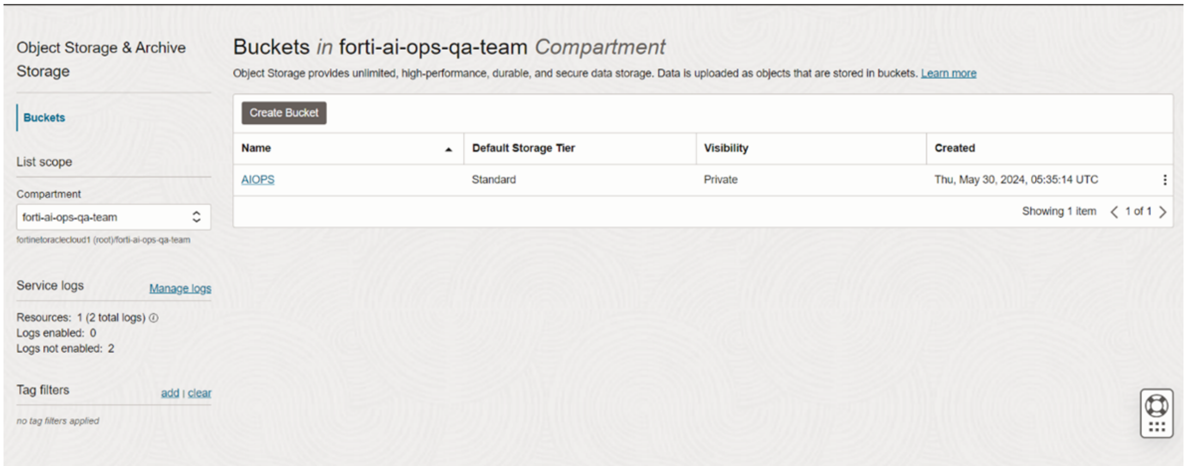
Status running
HA State none
Node proxmox
CPU usage 8.63% of 4 CPU(s)
Memory usage 66.22% (21.19 GiB of 32.00 GiB)
Bootdisk size 8.00 GiB
IPs No Guest Agent configured

5. Configure the FortiAIOps static IP address on starting the VM.

Public Cloud Platform - Oracle Cloud Infrastructure (OCI)

Perform the following steps to deploy FortiAIOps on OCI, for more information, see OCI Documentation.

1. Obtain the file *FAO_VM64_OCI-v2.1.0-[build0xxx].out.oci.zip* from Fortinet.
2. To create a Bucket in OCI, log in to your OCI account and navigate to the **Object Storage & Archive Storage > Buckets > Create Bucket** in the OCI portal.
3. Enter a unique name for your *Bucket* and select the relevant *Compartment*.
4. Click **Create** or **Confirm**.



Buckets *in* forti-ai-ops-qa-team *Compartment*

Object Storage provides unlimited, high-performance, durable, and secure data storage. Data is uploaded as objects that are stored in buckets. Learn more

Name	Default Storage Tier	Visibility	Created
AIOPS	Standard	Private	Thu, May 30, 2024, 05:35:14 UTC

Showing 1 item   1 of 1

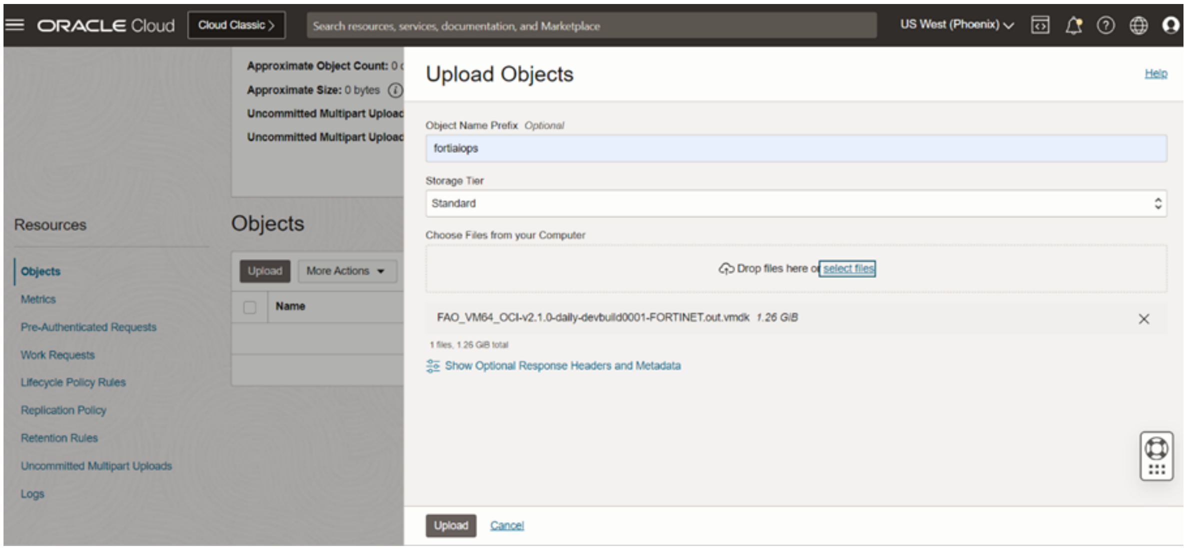
Compartment: forti-ai-ops-qa-team

fortinetoraclecloud1 (root)/forti-ai-ops-qa-team

Resources: 1 (2 total logs)
Logs enabled: 0
Logs not enabled: 2

no tag filters applied

5. Extract the file *FAO_VM64_OCI-v2.1.0-[build0xxx].out.oci.zip* to obtain *FAO_VM64_OCI-v2.1.0-[build0xxx].vmdk*. Upload the *.vmdk* file in the bucket.


ORACLE Cloud
Cloud Classic >
Search resources, services, documentation, and Marketplace
US West (Phoenix)
Resources
Objects
Metrics
Pre-Authenticated Requests
Work Requests
Lifecycle Policy Rules
Replication Policy
Retention Rules
Uncommitted Multipart Uploads
Logs
Objects
Upload
More Actions
Name
Help
Drop files here or select files
Show Optional Response Headers and Metadata
Upload
Cancel

Approximate Object Count: 0
Approximate Size: 0 bytes
Uncommitted Multipart Upload
Uncommitted Multipart Upload

Upload Objects

Object Name Prefix *Optional*: fortiaiops

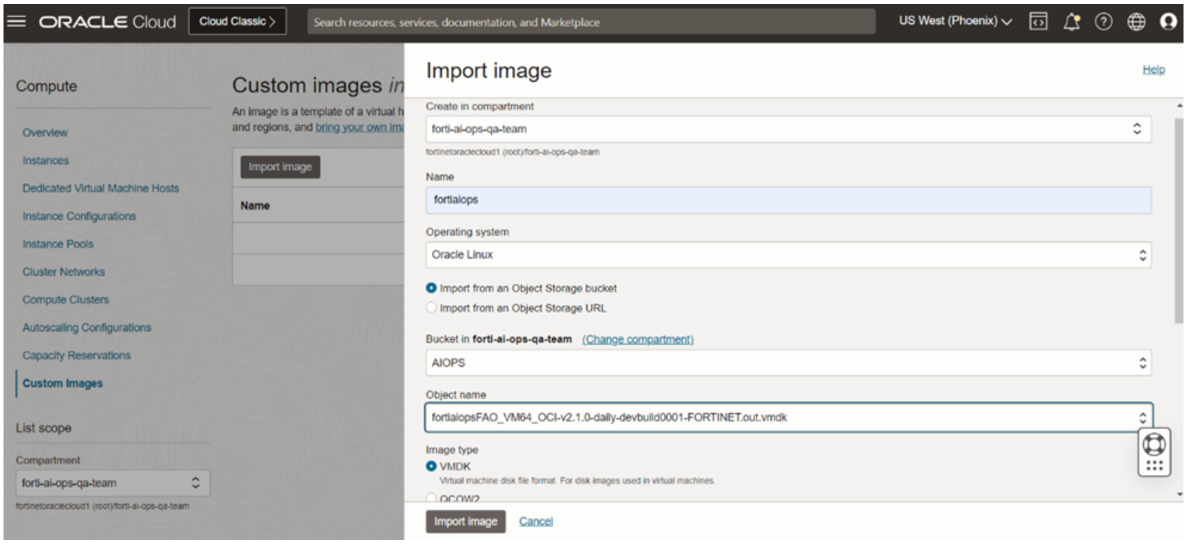
Storage Tier: Standard

Choose Files from your Computer

FAO_VM64_OCI-v2.1.0-daily-devbuild0001-FORTINET.out.vmdk *1.26 GiB*

1 files, 1.26 GiB total

6. Select **Custom Images** and import the image; select the uploaded VMDK file in **Object Name**.



Import image

Create in compartment: forti-ai-ops-qa-team

fortinetoraclecloud1 (root)/forti-ai-ops-qa-team

Name: fortiaiops

Operating system: Oracle Linux

● Import from an Object Storage bucket

○ Import from an Object Storage URL

Bucket in **forti-ai-ops-qa-team** (Change compartment): AIOPS

Object name: fortiaiopsFAO_VM64_OCI-v2.1.0-daily-devbuild0001-FORTINET.out.vmdk

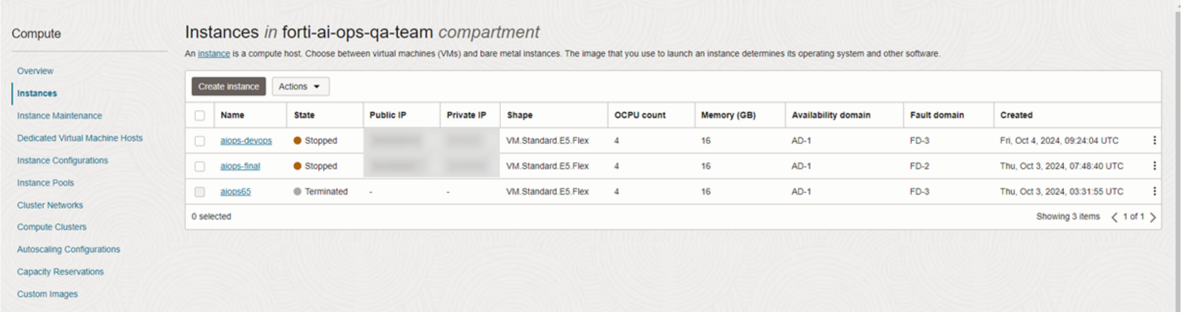
Image type

● VMDK

Virtual machine disk file format. For disk images used in virtual machines.

○ QCOW2

7. Search for the **Block Volume Service** and create block volume with 500 GB using the **Custom** option.
8. Navigate to **Compute Service** in the OCI portal and create an instance with the uploaded custom image.



Instances *in* forti-ai-ops-qa-team *compartment*

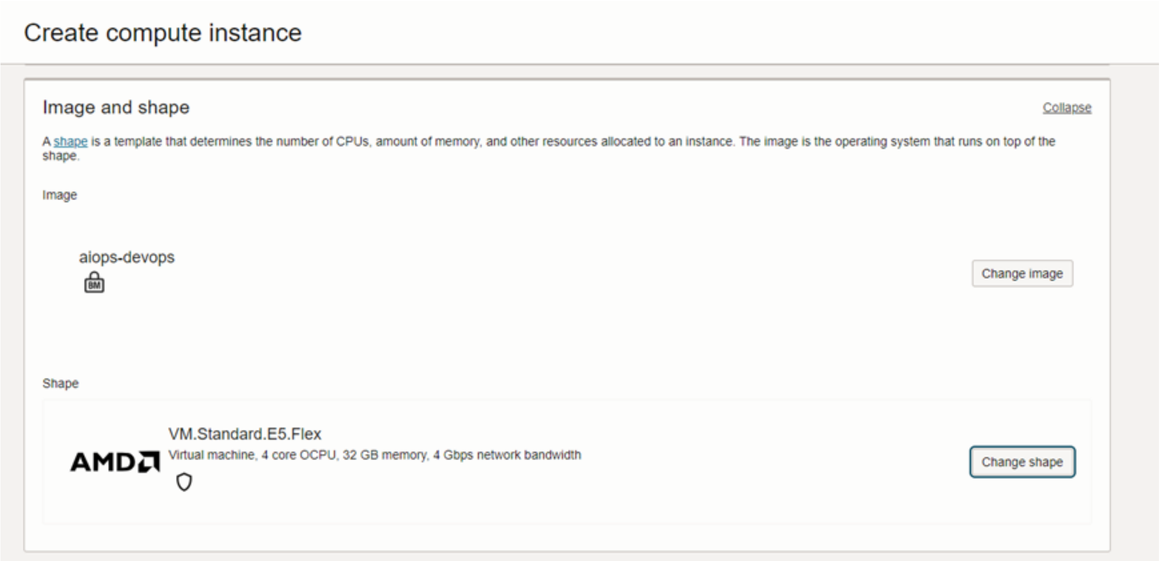
An instance is a compute host. Choose between virtual machines (VMs) and bare metal instances. The image that you use to launch an instance determines its operating system and other software.

Name	State	Public IP	Private IP	Shape	OCPU count	Memory (GB)	Availability domain	Fault domain	Created
aiops-devops	● Stopped	[redacted]	[redacted]	VM.Standard.E5.Flex	4	16	AD-1	FD-3	Fri, Oct 4, 2024, 09:24:04 UTC
aiops-final	● Stopped	[redacted]	[redacted]	VM.Standard.E5.Flex	4	16	AD-1	FD-2	Thu, Oct 3, 2024, 07:48:40 UTC
aiops65	● Terminated	-	-	VM.Standard.E5.Flex	4	16	AD-1	FD-3	Thu, Oct 3, 2024, 03:31:55 UTC

0 selected

Showing 3 items 1 of 1

9. Click **Create instance** and select the required **Image** and **Shape Series**. Set the number of CPUs to 4 and RAM to 32 GB, as per your requirements. Wait for the import process to complete. This may take 6-10 minutes (approximately). In the **Shape Series**, set the number of CPUs to 4 and RAM to 32 GB as per your requirements.
   Wait for the import process to complete. This may take 6-10 minutes (approximately).



Create compute instance

Image and shape

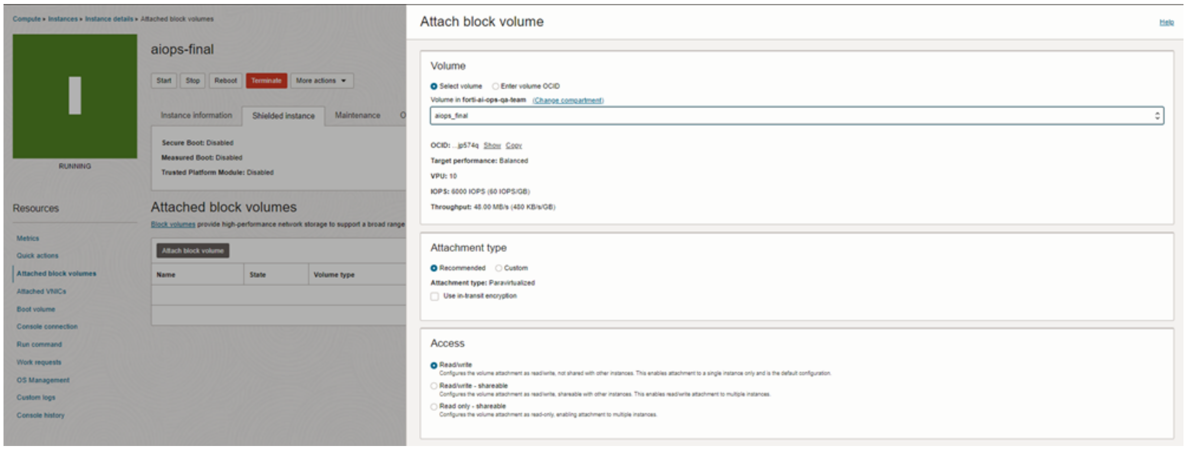
A shape is a template that determines the number of CPUs, amount of memory, and other resources allocated to an instance. The image is the operating system that runs on top of the shape.

Image: aiops-devops

Shape: VM.Standard.E5.Flex

Virtual machine, 4 core OCPU, 32 GB memory, 4 Gbps network bandwidth

10. Save any private keys or SSH keys that you may need to access the instance.
11. After creating an instance, navigate to **Attached block volumes** and select the block volume created earlier. The recommended attachment type is **Paravirtualized**.



Secure Boot: Disabled

Measured Boot: Disabled

Trusted Platform Module: Disabled

Attached block volumes

Block volumes provide high-performance network storage to support a broad range

Attach block volume

Volume

● Select volume ○ Enter volume OCID

Volume in forti-ai-ops-qa-team (Change compartment)

aiops_final

OCID: ...jp574q Show Copy

Target performance: Balanced

VPU: 10

IOPS: 6000 IOPS (60 IOPS/GB)

Throughput: 48.00 MB/s (480 KB/s/GB)

Attachment type

● Recommended ○ Custom

Attachment type: Paravirtualized

□ Use in-transit encryption

Access

● Read/write
Configures the volume attachment as read/write, not shared with other instances. This enables attachment to a single instance only and is the default configuration.

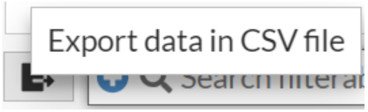
○ Read/write - shareable
Configures the volume attachment as read/write, shareable with other instances. This enables read/write attachment to multiple instances.

○ Read only - shareable
Configures the volume attachment as read-only, enabling attachment to multiple instances.

12. Reboot the instance after attaching the volume.

Others

The following are some additional enhancements delivered in this release.

- The FAP-241K and FAP-243K models are now supported.
- You can now export data in a *.csv* file from **Wireless > Clients** and **Switch > FortiSwitch Clients**. Click on the export icon on these pages - 

- FortiAIOps is now Swagger compliant that enhanced API accessibility. You can access API documentation using the URL, *https://<FortiAIOps IP address>/swagger*.

www.fortinet.com