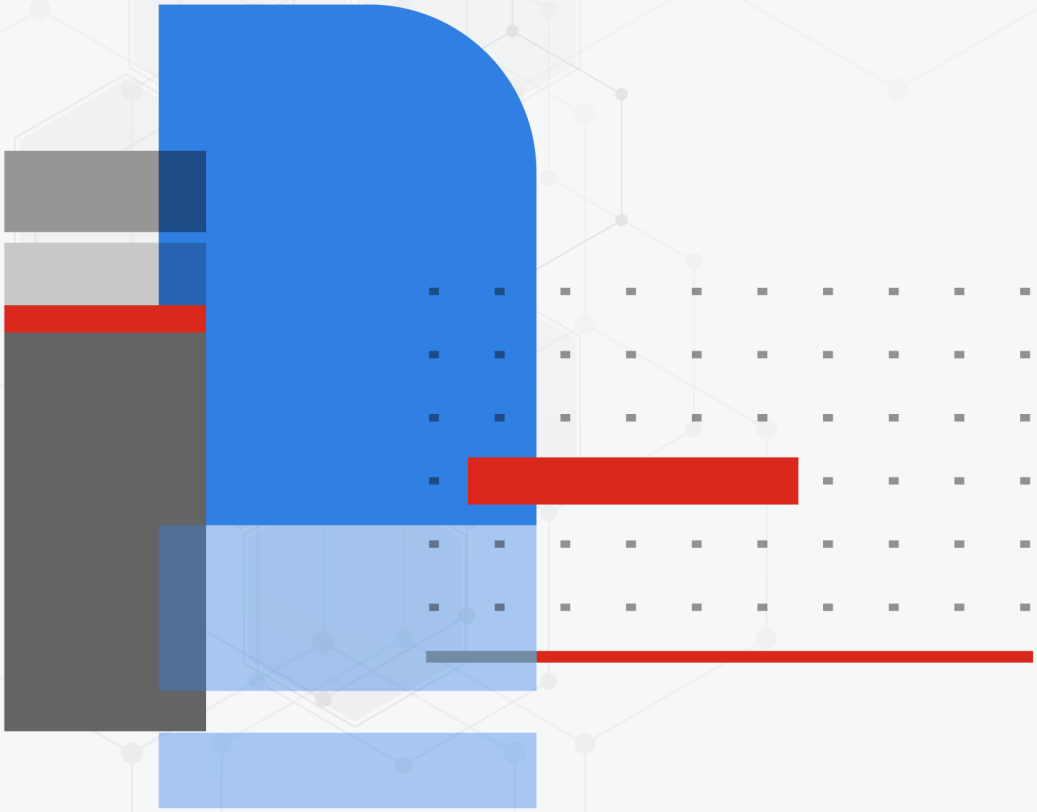
User Guide

FortiAIOps 3.0.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
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/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

Jan 19, 2026
FortiAIOps 3.0.0 User Guide
83-300-1157851-20260119

TABLE OF CONTENTS

Change log ... **6**
Overview ... **7**
Getting Started ... **12**
Installing FortiAIOps ... 13
Initial FortiAIOps Configuration ... 13
Licensing ... 14
Adding FortiGate ... 15
Enable Log Forwarding ... 15
Monitoring ... 17
System Diagnostics ... 18
API Reference ... 19
Deploying FortiAIOps on VM Platforms ... **20**
Pre-installation Requirements ... 20
Installing FortiAIOps on VMware ESXi ... 20
Installing FortiAIOps on Hyper-V ... 22
Installing FortiAIOps on KVM ... 30
Installing FortiAIOps on Nutanix ... 32
Installing FortiAIOps on Proxmox ... 36
Post-installation Tasks ... 37
Increasing VM Disk Space ... 37
Accessing FortiAIOps ... 39
Upgrading FortiAIOps ... 39
Deploying FortiAIOps on Public Cloud Platforms ... **40**
Microsoft Azure ... 40
Post-installation Tasks ... 48
Google Cloud Platform ... 48
Amazon Web Services (AWS) ... 55
Oracle Cloud Infrastructure (OCI) ... 60
Deploying FortiAIOps on Hardware Platforms ... **64**
Deploying FortiAIOps 500G (FAO-500G) ... 64
Initial Configuration ... 64
Accessing the GUI ... 64
Command Line Interface (CLI) Reference ... **65**
Dashboard ... **72**
Summary ... 72
Wireless ... 78
Switch ... 104
SD-WAN ... 116
Custom Dashboard ... 128
Managing Dashboard Widgets ... 132

AI Insights 136
Impacted SLA 136
Impacted Devices 137
SLA Config 140
Device Health 141
Time To Connect 143
Roaming 144
FortiAI 147
Using FortiAI 148
FortiAI Data Privacy 150
FortiAI Tokens 150
FortiAI Example Tasks 151
Inventory 158
Adding and Managing FortiGates 158
Adding a FortiGate 158
Importing and Exporting FortiGates 160
Managing FortiGates 160
Device Groups 171
VDOM Support 172
Wireless 174
Access Points 174
AP 174
Radio 176
Access Points Diagnostics and Tools 177
Wireless Clients 185
Wireless Clients Diagnostics and Tools 186
Channel Summary 189
Summary 189
Events 191
Insights 191
Applications 194
Location Services Monitor 196
Heat Maps 198
Rogue APs 203
Map Management 204
Switch 210
FortiSwitch 210
Wired Clients 216
SD-WAN 218
Insights 219
Forecast 223
Security Fabric 230
Physical Topology 230
Logical Topology 231

Logs and Reports **232**
Event Logs 232
Local Logs 238
Reports 238
Creating Reports 238
Viewing Reports 246
Scheduled Reports 246
PCI Reports 246
System **248**
User Management 248
Users 248
User Groups 250
User Sessions 251
Backup and Restore 251
Settings 253
Upgrade 264
Licensing 265
FortiGuard 265
Location Services 266
Network Interface 267
Certificates 268
SAM **270**
Trends 270
Completed Tests 272
Baseline Tests 273
Schedule Tests 276

Change log

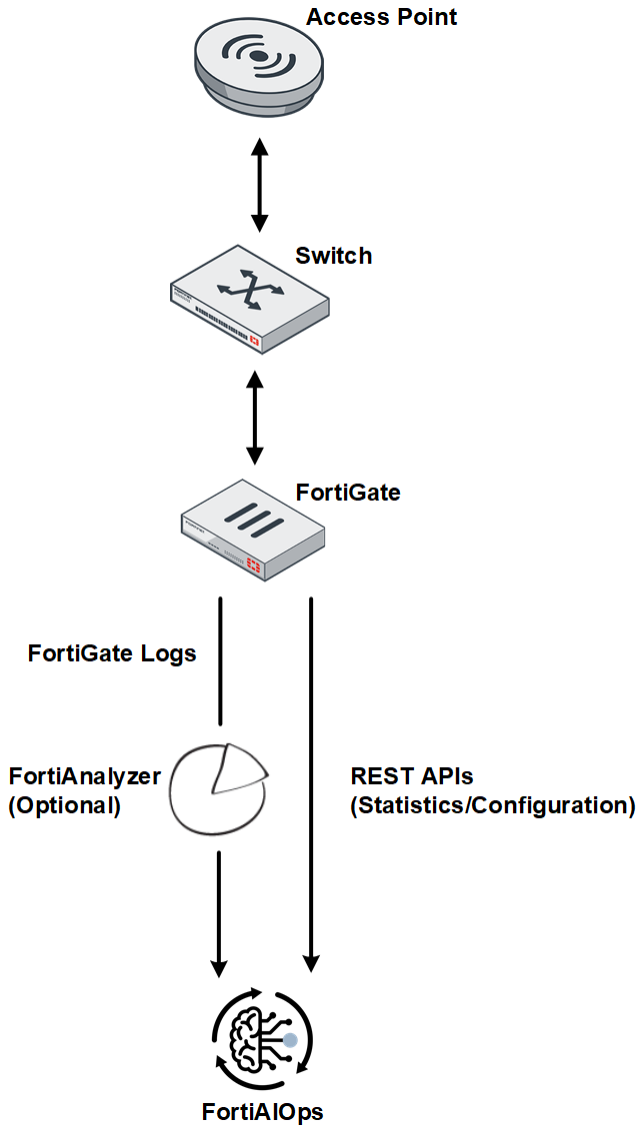
Date	Change description
2025-07-01	FortiAIOps 3.0.0 release document.
2025-07-22	Updated Enable Log Forwarding.
2025-09-05	Updated Licensing.
2025-09-25	Added Increasing VM Disk Space section.
2025-11-12	Editorial fix.
2026-01-19	Updated Backup and Restore.

Overview

FortiAIOps enables you to proactively monitor the health of your entire wireless, wired, and SD-WAN network, and provides insights into key health statistics, based on the Artificial Intelligence (AI) and Machine Learning (ML) architecture that it is built upon. FortiAIOps ingests data for analysis and automated event correlation to precisely detect anomalies that impact the clients' network experience. It learns from numerous sources such as FortiGates, FortiAPs, FortiSwitches, and FortiExtenders to report statistics on a series of comprehensive and simple dashboards, providing visibility and deep insight into your network. This predictable network infrastructure enables you to swiftly identify the root cause with the highest probability of association to actual issues, and its resolution.

FortiAIOps is 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.

FortiAIOps monitors integrated wireless, wired, and SD-WAN networks by supporting the monitoring of FortiGate controllers. You can monitor and manage FortiGate controllers concurrently associated with FortiAPs and stations in a large deployments. The centralized real-time data and event logs offered by FortiAIOps, aim at diagnosing and troubleshooting network issues by analyzing potential problems and suggesting remedial steps.



The FortiAIOps application provides the following advantages.

- Maximizes the uptime of your organization's network infrastructure.
- Reduces the time taken to diagnose network issues, thereby the mean response time.
- Increases the productivity of network users and that of your organization.

FortiAIOps calculates the SLA thresholds/baselines *dynamically* using the AI-ML architecture, to enable you to diagnose network issues based on accurate and latest data trends. The algorithms identify the values for each environment by clustering clients based on the connection quality using specific parameters. The thresholds are then derived based on the calculated average of the client connection data, to report variations in your network. These AI driven algorithms are designed to learn new data regularly for changes in client activity, calculate thresholds, and report statistics. You can also provide *static* threshold values for some SLAs, to report network issues. You can view the impacted SLA data in the dashboards.

- Wireless
- Switching
- WAN

Wireless

The following SLAs are monitored for wireless clients.

- Throughput
- Coverage
- Roaming
- Time to Connect
- Connection Failure
- AP Health and Uptime
- WIDS

Throughput

This SLA monitors your wireless network at the system and client level, to identify potential low throughput conditions and categorize them based on the underlying issue type, into different classifiers and sub-classifiers. Low throughput is determined based on specific network health parameters, such as, noise, retries, discards, channel utilization etc. and client health parameters, such as, MCS index, data rate.

Coverage

Network coverage issues are monitored by detecting the coverage holes and overlapping FortiAPs (crowded FortiAPs). These conditions in a network are determined by evaluating client's RSSI (low signal strength) and presence of multiple neighbouring FortiAPs.

Roaming

Wireless clients roam from one AP to another in a multi-AP deployment area swiftly and frequently. Associating with different AP requires a process of re-authentication that can take some time to complete, impeding data connectivity especially for time sensitive applications. The *Roaming* SLA identifies such slow roaming connections, determines the causes for it and suggests suitable remedy for facilitating faster client roaming.

Time to Connect

This SLA computes the time taken by clients to connect to the network. FortiAIOps reports those clients that take longer than certain thresholds to connect to the network. These thresholds are statically configured or FortiAIOps computes them dynamically using machine learning algorithms. The algorithms compute specific thresholds for the AP-client environment and for different connectivity phases such as association, authentication (4-way handshake) and DHCP.

Connection Failure

This SLA determines the failed/unsuccessful client connections based on different stages of connection to a network. For example, association failures due to low RSSI, authentication failures due to unreachable RADIUS server, DHCP failure due to a DHCP server process crash, or DNS failure due to an invalid DNS domain.

AP Health and Uptime

This SLA determines the health of the FortiAPs based on the configured CPU, memory, temperature thresholds, and events such as FortiAP reboot, FortiSwitch port down, FortiGate, and so on. FortiAIOps

displays relevant SLAs under different sections on the monitor dashboard.

WIDS

The WIDS SLA monitors and reports on potential Wireless Intrusion Detection System (WIDS) attempts on your network. It detects security threats and recommends corrective actions to maintain network integrity, boosting security with real-time alerts and actionable insights for faster threat resolution.

Switching

The switching SLAs monitor the switch health and connection status.

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

Throughput

The **Throughput** 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.

Network

The **Network** 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.

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** SLA 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.

WAN

WAN is a software-defined approach for managing Wide-Area Networks (WAN). It allows you to offload internet bound traffic, that is, private WAN services remain available for real-time and mission critical applications. This

added flexibility improves traffic flow and reduces pressure on the network. WAN has member interfaces and ports that are used to run traffic.

- Performance
- FortiExtender Health
- Interface Health

Performance

FortiAIOps continuously monitors network performance using Performance SLA, tracking key metrics like latency, jitter, and packet loss. This helps assess link quality, detect configuration issues, and identify SD-WAN failures, reporting SLA breaches when forecast thresholds are exceeded. By leveraging real-time and historical data from FortiGate health checks, FortiAIOps forecasts future network performance for proactive optimization. It also monitors tunnel status to pinpoint overlay network misconfiguration that could impact performance and connectivity.

FortiExtender Health

FortiExtender integrates with FortiGate and SD-WAN to extend the network reach and resilience within the Fortinet Security Fabric. It provides continuous connectivity by acting as SD-WAN extension for FortiGate, ensuring failover if the primary link fails. FortiExtender also enables network access for remote sites beyond fixed broadband and facilitates load balancing with the primary SD-WAN link.

The FortiExtender Health SLA monitors and reports the FortiExtender's health metrics, including CPU, Memory, Temperature, and Carrier Failure.

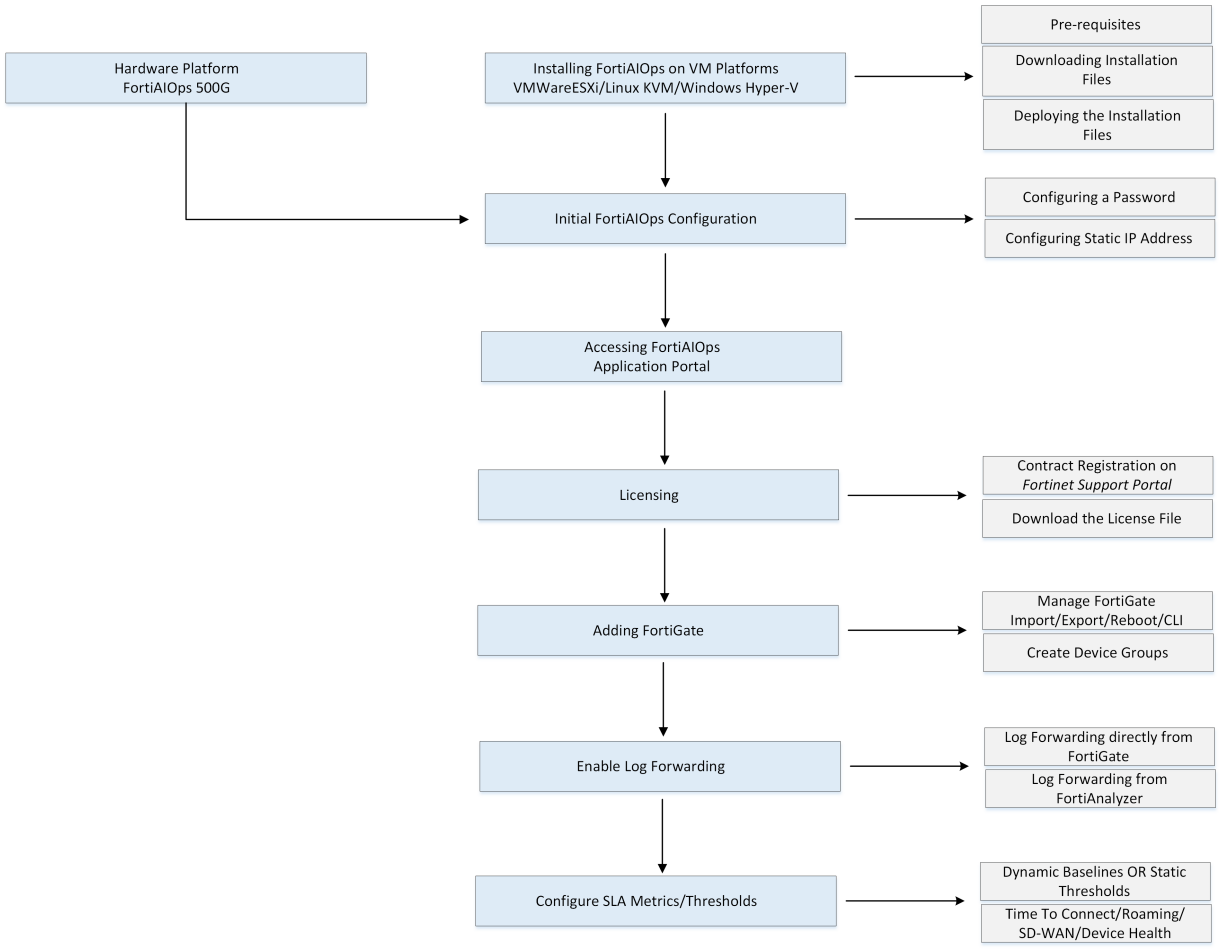
Note: FortiAIOps monitors only the FortiExtender devices managed by FortiGate.

Interface Health

Interface Health SLA in FortiAIOps monitors the stability of both underlay and overlay network links, detecting status changes and interface flaps to ensure consistent performance. It also evaluates SD-WAN interface selection strategies to identify the most efficient traffic paths, ensuring seamless connectivity and optimizing SD-WAN configurations for maximum performance and reliability.

Getting Started

This section is a tutorial to get you started with installing, setting up, and using the FortiAIOps application to monitor your networks.



The steps depicted in this graphic are described in the following sections.

- Installing FortiAIOps
- Initial FortiAIOps Configuration
- Accessing FortiAIOps
- Licensing
- Adding FortiGate
- Enable Log Forwarding
- SLA Config
- Monitoring
- API Reference
- System Diagnostics

Installing FortiAIOps

You can deploy FortiAIOps on supported VM, public cloud, and hardware platforms. Refer to the following sections for detailed instructions on deployment procedures.

- **VM Platforms** - Deploying FortiAIOps on VM Platforms
- **Public Cloud Platforms** - Deploying FortiAIOps on Public Cloud Platforms
- **Hardware Platforms** - Deploying FortiAIOps on Hardware Platforms

Note: The FortiAIOps CLI and GUI users are different.

Initial FortiAIOps Configuration

After FortiAIOps is successfully installed, login as an administrator with the default username (**admin**). A password is not required. For more information on the commands, see Command Line Interface (CLI) Reference.

- Configuring a Password
- Configuring the IP Address
- NTP/Timezone and DNS Configurations
- Viewing the Configuration

Configuring a Password

Login into the CLI with the username `admin`, a password is not required. However, after you login, you are prompted to change the password.

Configuring the IP Address

The DHCP IP address is assigned by default. Run the `get system interface` command to view the IP address. Run the `config system interface` command to configure a static IP address.

```
fortiaiops # config system interface
fortiaiops (interface) # edit port1
fortiaiops (port1) # set mode static
fortiaiops (port1) # set ip 10.34.159.xxx/xx
fortiaiops (port1) # end
```

You are required to configure the gateway IP address when using a static IP address. Run the `config router static` command.

```
fortiaiops # config router static
fortiaiops (static) # edit 1
fortiaiops (1) # set gateway 10.34.159.xx
fortiaiops (1) # set device port1
fortiaiops (1) # end
```

NTP/Timezone and DNS Configurations

Fortinet recommends that you configure the NTP settings and DNS server. Run the following commands.

- `config system ntp`
- `config system global [set timezone]`
- `config system dns`

You can also configure the IP address , DNS, NTP, and the timezone via the GUI. See Settings.

Viewing the Configuration

Run the `show full-configuration` command to view all changes.

For detailed information on these configurations, see Post-installation Tasks

Licensing

FortiAIOps offers Monitoring, AI Insights, and SD-WAN subscriptions, with licensing based on the type of devices you use. For more information, see FortiAIOps Data Sheet.

Perform the following steps to obtain the license for FortiAIOps on VM platforms or public cloud platforms.

1. **Copy System ID information**: Navigate to **Dashboard > Summary** and copy the System ID.
2. **Contract Registration**: Login to https://support.fortinet.com using your account credentials to register the contract received over email for the product SKU purchased. Paste the copied system id during the registration process to generate the license file.
3. **Download License file**: Once the registration is complete, validate the entitlement details and download the license file if generated successfully. Upload this file in **System > FortiGuard > Upload License File**.

For FortiAIOps 500G, 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**.

Note:

- Fortinet recommends that all network elements are fully licensed.
- To enable monitoring and management of SD-WAN network, an SD-WAN license must be applied separately.

If the network elements are partially licensed, related statistics are not reported in FortiAIOps. For example, a FortiAP is licensed and the connected FortiSwitch is not licensed; a FortiAP down event is triggered due to FortiSwitch port down/FortiSwitch reboot. In this case, the FortiAP down event is reported in FortiAIOps but the

FortiSwitch port issues or reboot is not reported in FortiAIOps (as the FortiSwitch is not licensed). For more information, see Licensing.

Ensure that the FortiAIOps NTP settings and your time zone are synchronized.

Adding FortiGate

In the FortiAIOps application portal, manually add the FortiGate controller. Navigate to **Inventory > Managed FortiGates > Add** and provide the required configuration details. Standalone and HA FortiGate controllers can be added. Optionally, you can add FortiGates in bulk using the import operation. For detailed information on adding and managing FortiGate controllers, see Adding and Managing FortiGates.

You can group FortiGate controllers into **Device Groups** for ease of management. Each controller can belong to only one group; if a controller is added to a second group, it is automatically removed from the previous group. For detailed information on creating device groups, see Device Groups.

Enable Log Forwarding

FortiGate logs must be forwarded to FortiAIOps for seamless identification of issues and populating proper data.

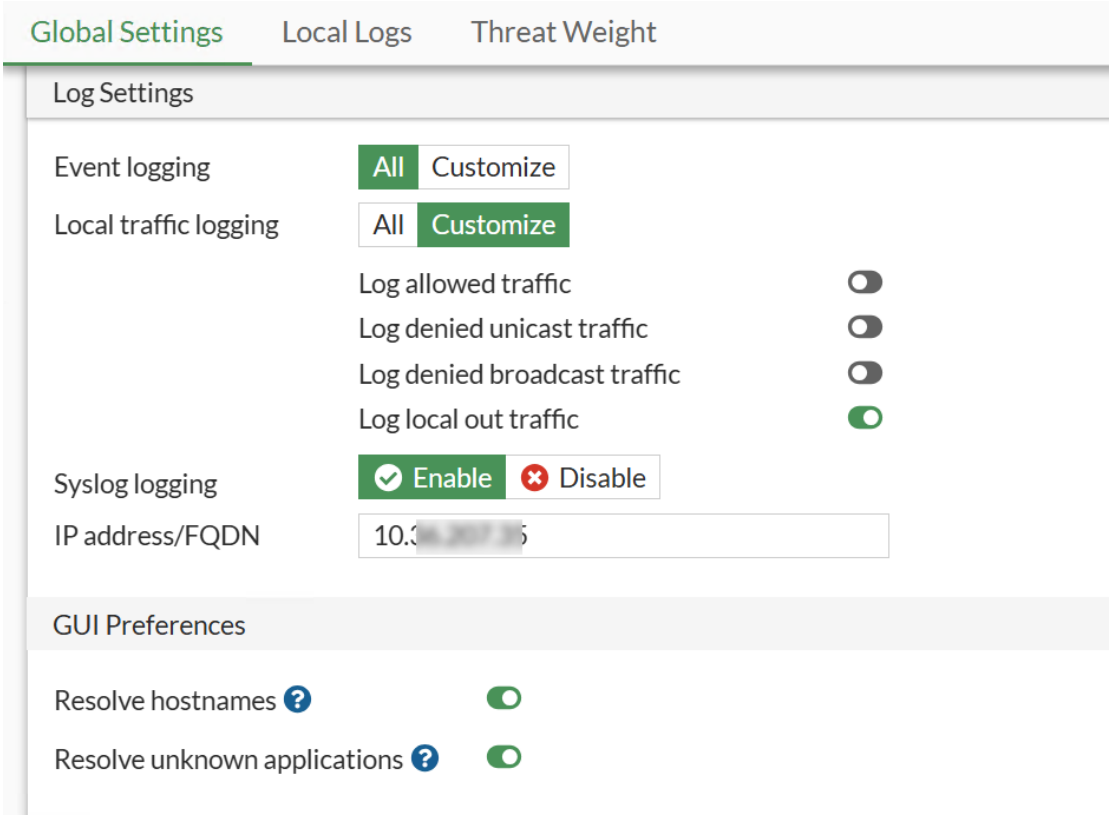
FortiAIOps supports direct FortiGate log forwarding and FortiAnalyzer log forwarding. You can enable log forwarding from FortiGate or FortiAnalyser based on the log storage used.

- Forwarding Logs from FortiGate
- Forwarding Logs from FortiAnalyzer

Forwarding Logs from FortiGate

To configure direct FortiGate log forwarding to FortiAIOps on the FortiGate GUI:

1. Navigate **Log & Report** > **Log Settings** and select the **Global Settings**.



2. Enter the IP address/FQDN with the FortiAIOps IP address.
3. Click **Apply**.

To configure direct FortiGate log forwarding to FortiAIOps from FortiGate CLI, use the following commands:

```
config log syslogd setting
set status enable
set server 10.34.xxx.xxx
end
```

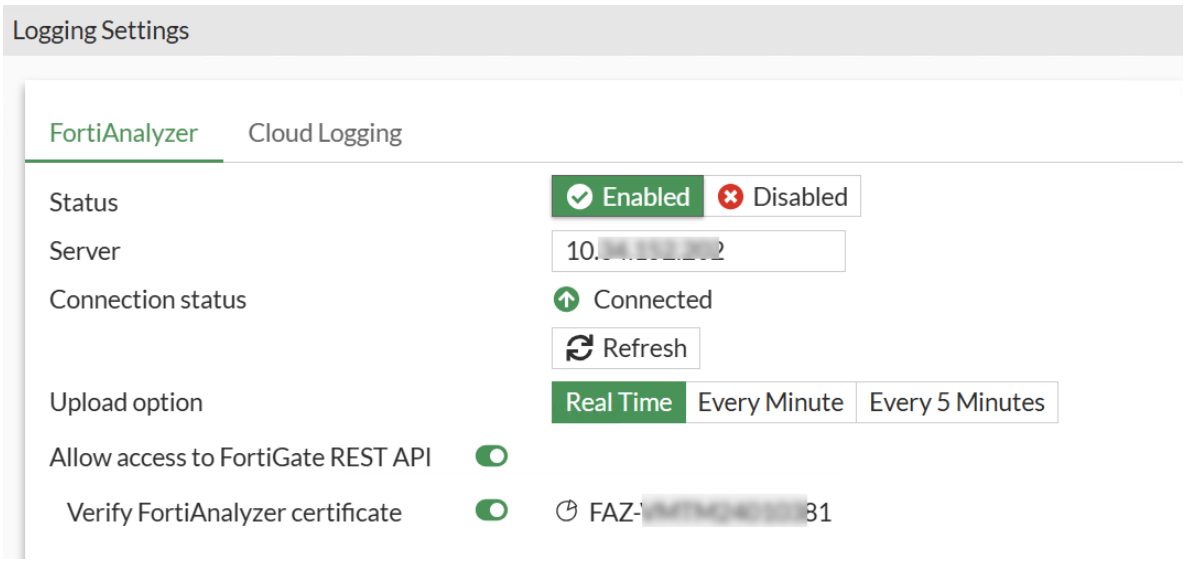
For more information, see FortiGate Administration Guide.

Forwarding Logs from FortiAnalyzer

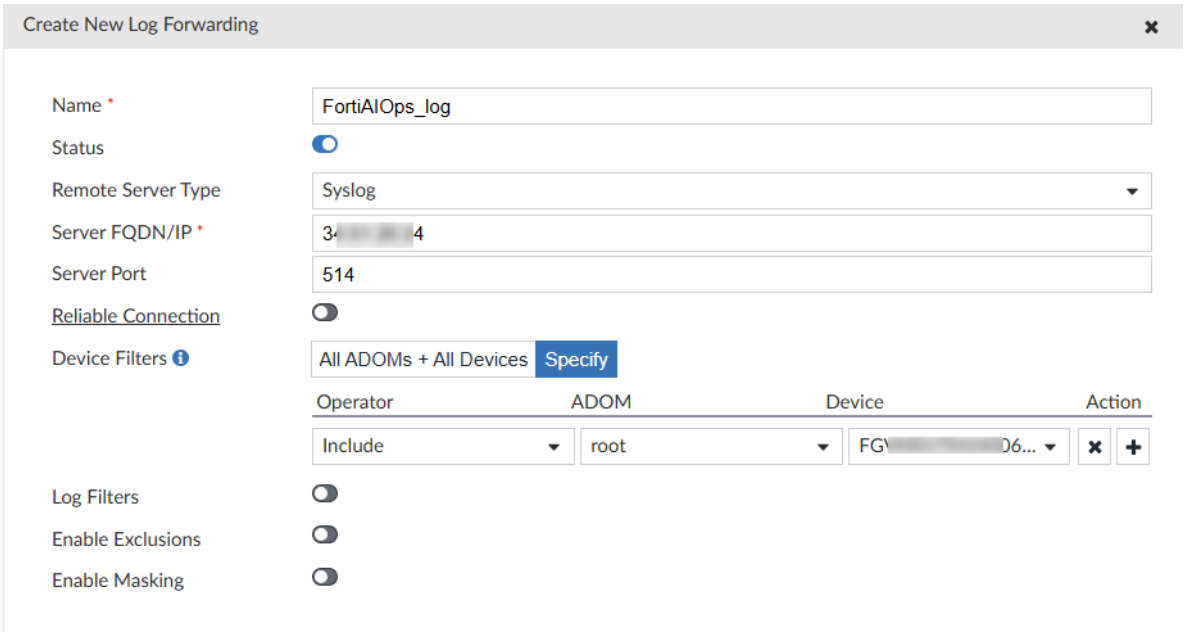
For FortiGates using FortiAnalyzer as the log storage, log forwarding to FortiAIOps can be enabled directly from the FortiAnalyzer.

To configure FortiAnalyzer to forward FortiGate logs to FortiAIOps, you must first configure FortiGate remote logging to FortiAnalyzer and then forward logs from FortiAnalyzer to FortiAIOps.

1. On the FortiGate GUI, navigate to **Fabric Connectors** > **Logging & Analytics** > **Logging Settings** > **FortiAnalyer** and specify the FortiAnalyzer IP address.



2. On the FortiAnalyzer GUI, navigate to **System Settings** >**Advanced** > **Log Forwarding** > **Settings**.
3. Click **Create New** to create new log forwarding.
4. Specify the FortiAIOps IP address and select the FortiGate controller in **Device Filters**.



Note:

- The syslog port is the default UDP port 514.
- Enable **Log Filters** to choose either **Traffic** or **Event**; the remaining options are not used.

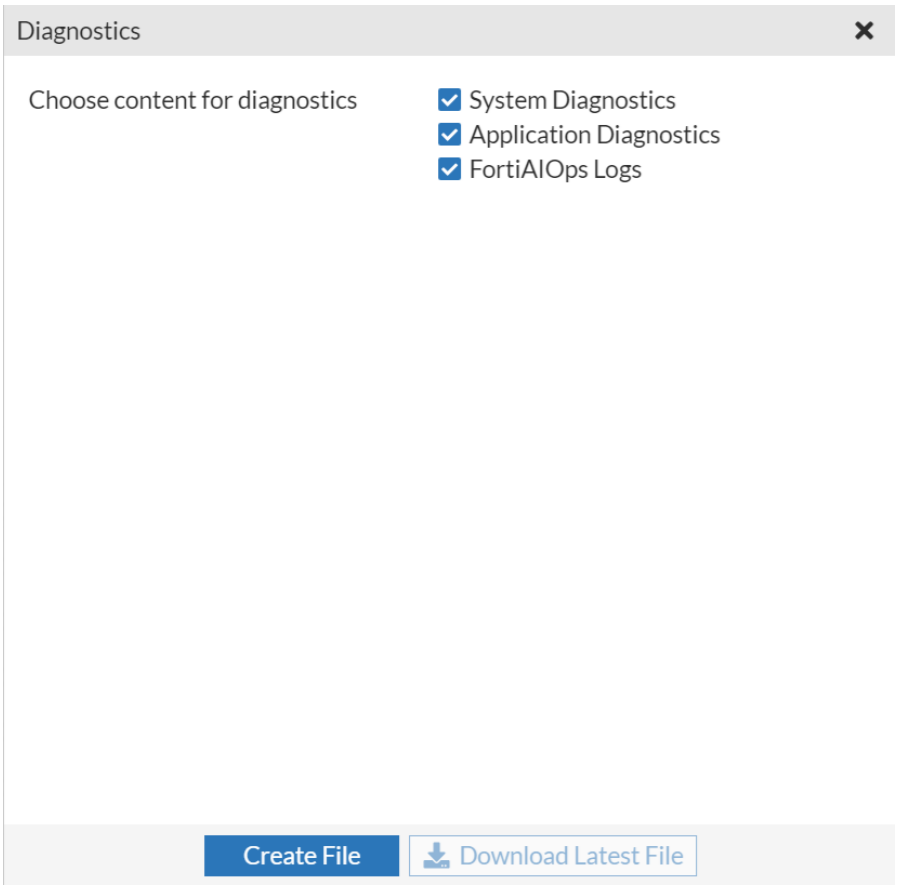
Monitoring

After the FortiAIOps setup and configurations are complete, you can view different aspects of your network in the following panels of the FortiAIOps application portal.

GUI Panels	Description
Dashboard	The dashboard provides a graphical overview of network elements, resource usage, and AI insights.
AI Insights	You can configure SLA metrics and the required thresholds, and monitor the AI enabled data insights of your network and the impacted SLAs and devices.
Inventory	You can add FortiGate controllers and configure management operations.
Wireless	The wireless section provides comprehensive data and statistics to monitor wireless networks.
Switch	The switch section provides comprehensive data and statistics to monitor FortiSwitches and FortiSwitch clients.
SD-WAN	The SD-WAN section provides comprehensive insights and forecasts on monitored SD-WAN interfaces and their associated health checks.
Security Fabric	The security fabric page represents the topology, that illustrates the logical placement of the wireless service and the physical placement of hardware devices.
Logs and Reports	The Logs section offers both detailed event logs and local logs. Logs for specific event types like WiFi Events, FortiSwitch Events, and SD-WAN Events are available. You can also generate comprehensive FortiAIOps reports here.
System	The system section includes several pages that offer valuable insights into various aspects of system management, such as users, user groups, backup and restore, settings, licensing, location services, and certificates.
SAM	The service assurance section provides an overview of the diagnostic and trouble-prevention capability of FortiAIOps.

System Diagnostics

Access the FortiAIOps GUI and in top-right, click to download the diagnostics to aid in troubleshooting, comprising of system, application, and FortiAIOps related logs. You can create the diagnostics file and download it as required.



API Reference

FortiAIOps is Swagger compliant providing well documented APIs and improving their accessibility. You can access API documentation using the URL, *https://<FortiAIOps IP address>/swagger*.

Deploying FortiAIOps on VM Platforms

Deploying FortiAIOps is a simple process that involves downloading the installation files, performing the installation, and completing post-installation steps. Here is an overview of the deployment process:

1. Ensure that the prerequisites are met before performing the installation.
2. Download installation files from the *Fortinet Support* portal.
3. Perform the installation.
   - Installing FortiAIOps on VMware ESXi
   - Installing FortiAIOps on Hyper-V
   - Installing FortiAIOps on KVM
   - Installing FortiAIOps on Nutanix
   - Installing FortiAIOps on Proxmox on page 36
4. Complete the post-installation tasks.

Pre-installation Requirements

Ensure that the following requirements are met before proceeding with the installation.

Supported Environments

Supported environments include:

- *VMware ESXi* - 7.0.3 and above
- *Microsoft Hyper-V*
- *KVM* - Ubuntu 20.04 and above, CentOS 9.0 and above

Hardware Requirements

The following table lists the minimum hardware requirements for deploying FortiAIOps.

CPU	Memory	Storage	
		Disk 1	Disk 2
8	32 GB	8 GB	500 GB

Note: Disk 1 is used for OS and Disk 2 is used for data. You can extend or modify Disk 2 size based on your requirements.

Installing FortiAIOps on VMware ESXi

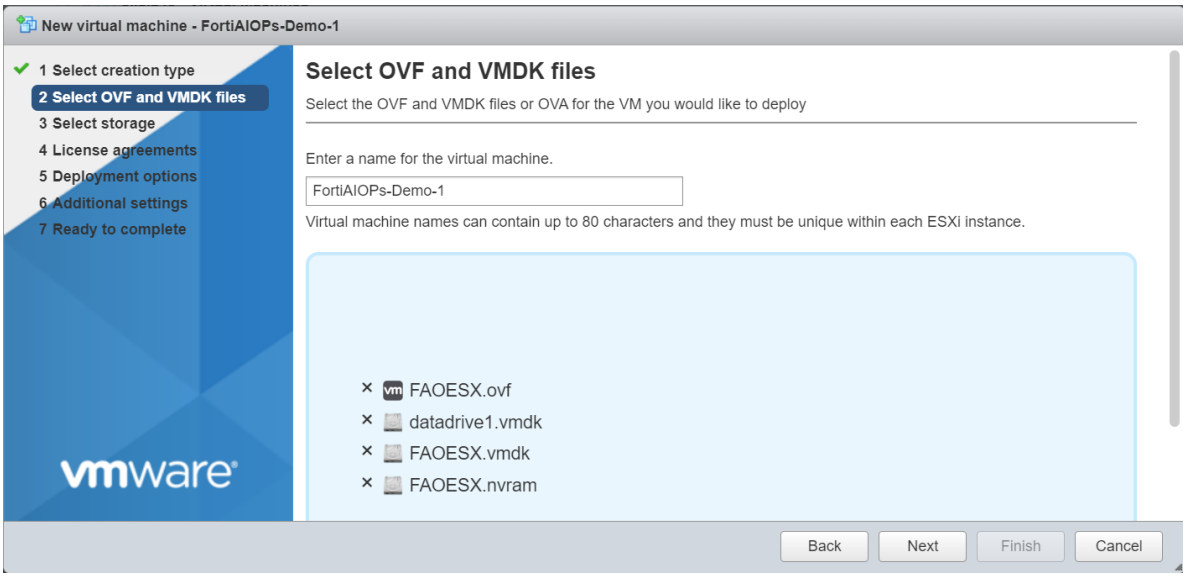
Perform the following steps to deploy FortiAIOps.

1. Download the installation file from *Fortinet Support* portal and unzip the file (*FAO_VM64-vx.x.x-devbuildxxxx-FORTINET.out.ovf.zip*). This folder contains 4 installation files.

datadrive1.vmdk	13-10-2023 06:42	VMDK File	131 KB
FAOESX.ovf	13-10-2023 06:42	OVF File	25 KB
FAOESX.vmdk	13-10-2023 06:42	VMDK File	13,19,844 KB
FAOESX.nvram	13-10-2023 06:41	NVRAM File	265 KB

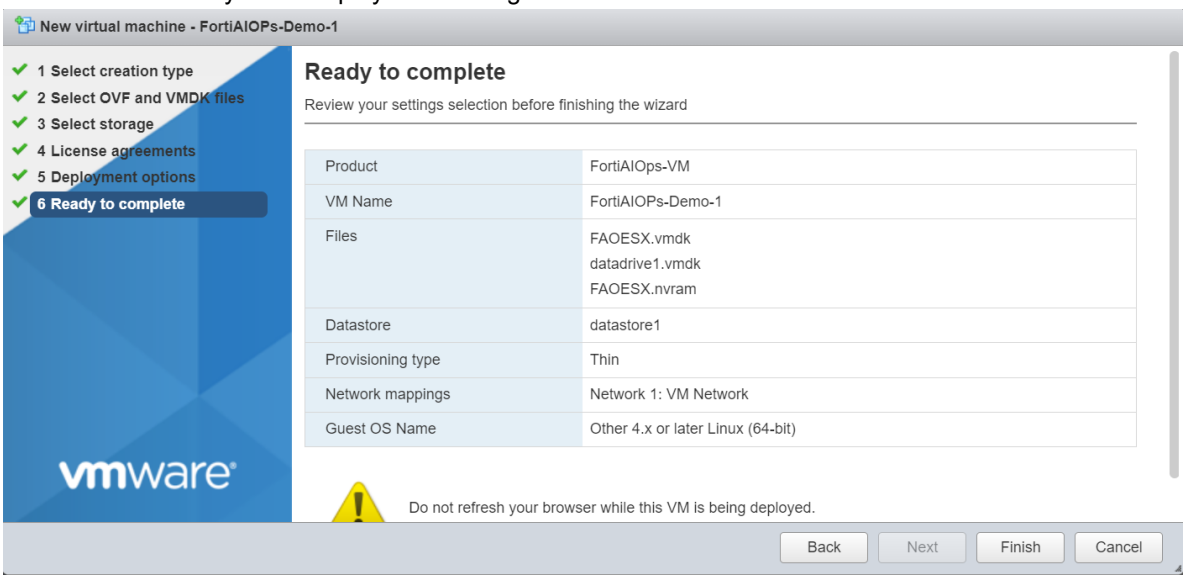
2. Connect and log in to the VMware ESXi host client with administrative rights.
3. Select **Create/Register VM** in the **Host** tab.

4. Select **Deploy a virtual machine from an OVF or OVA** file as the creation type.
5. Browse and select the downloaded installation files and enter a suitable hostname.



6. Select your preferred datastore to store the virtual machine files in the **Select storage** page.
7. Accept the end user license agreement.
8. In the **Deployment options** page:
   a. Select you preferred VM network
   b. Select your preferred disk provisioning method. Thin disk provisioning method is recommended.
   c. Ensure **Power on automatically** option is selected
   Note: To modify configurations, it is necessary to edit the VM configuration while the VM is in a powered off state, and then start the VM.

9. Review the summary of the deployment settings and click **Finish.**



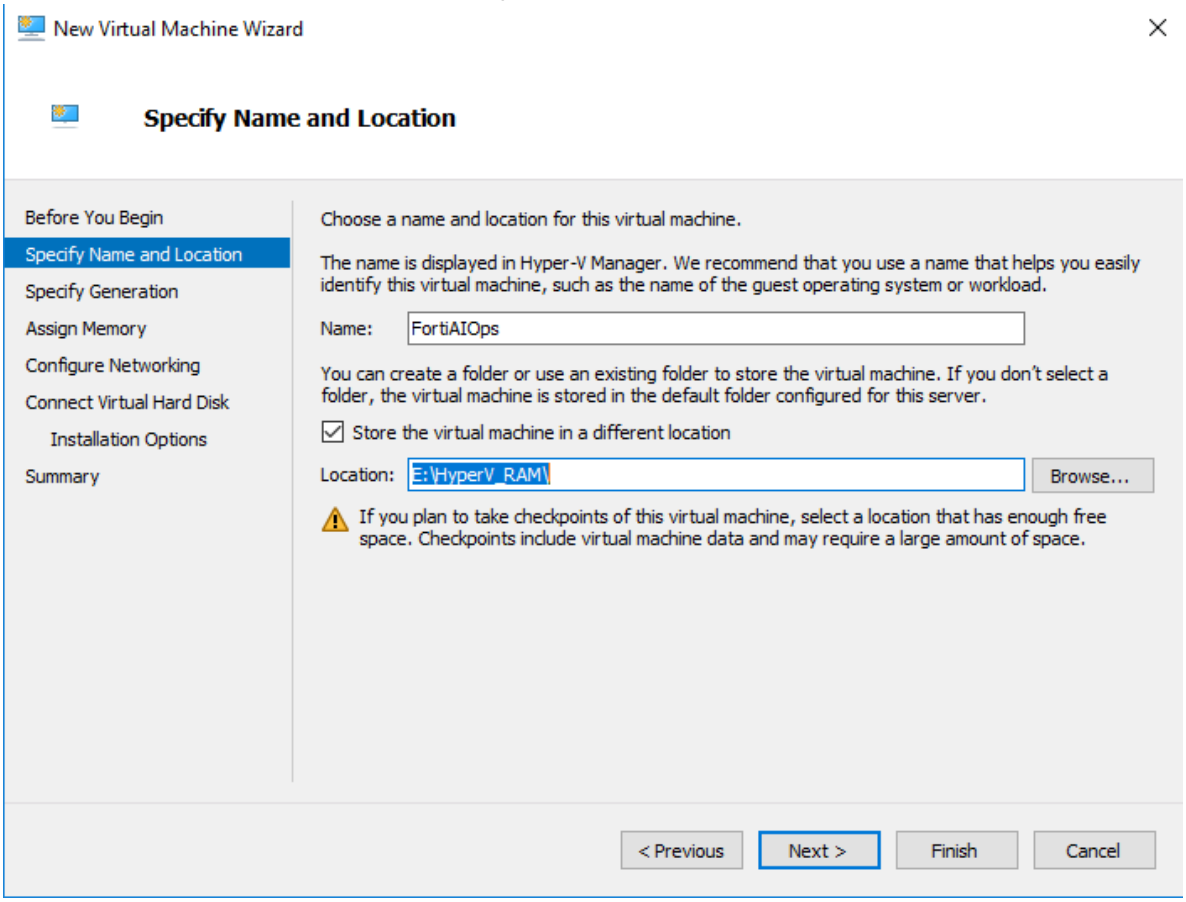
10. You can monitor the progress of the deployment in the **Recent Tasks** pane. When the installation is complete, the virtual machine will be listed in the **Inventory** pane.
11. Perform post-installation tasks.

Installing FortiAIOps on Hyper-V

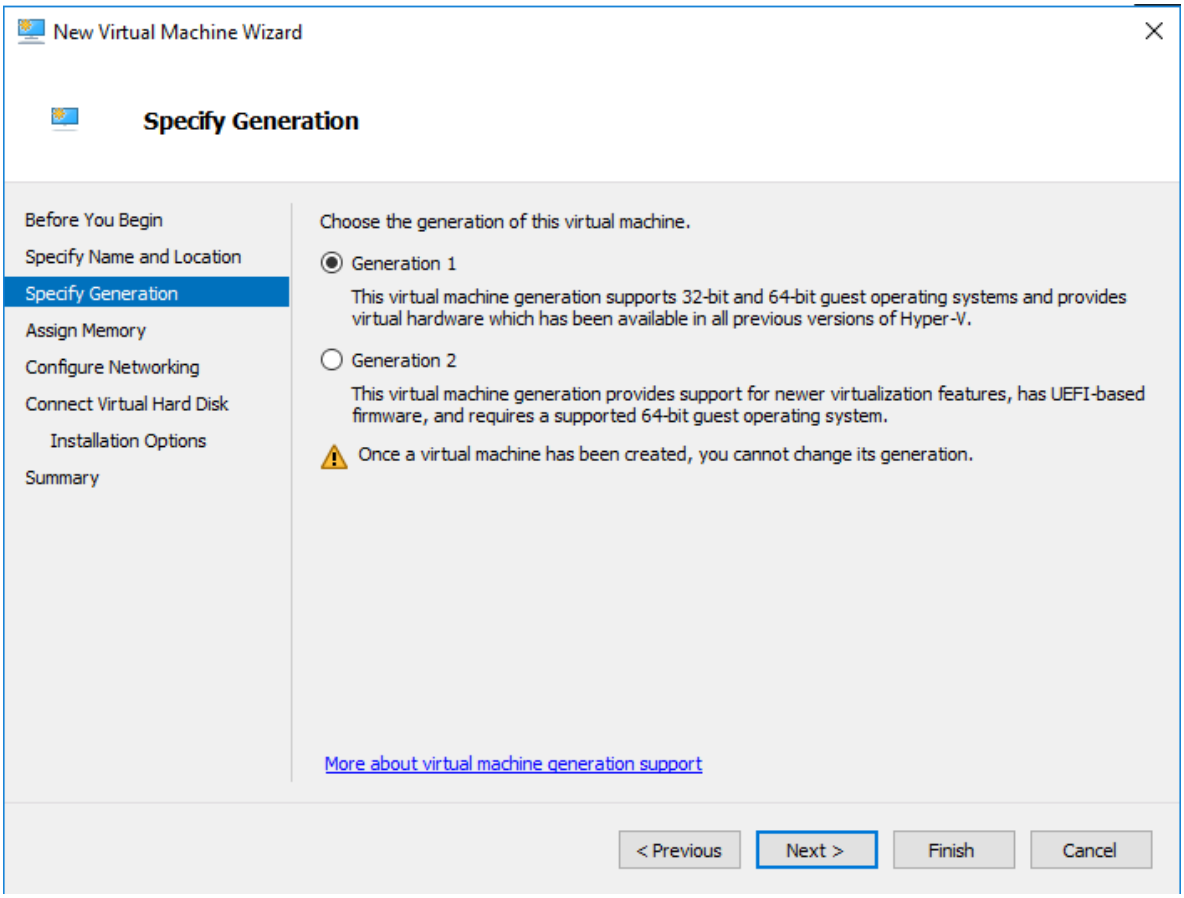
Perform the following steps to deploy FortiAIOps.

1. Download the installation file from *Fortinet Support* portal and unzip the file *FAO_VM64_HV-vx.x.xdevbuildxxxx-FORTINET.out.hyperv.zip*. This folder contains 2 installation files.
2. Open the Start menu, search for **Hyper-V Manager**, and click on the application to launch it.
3. Click **New** in the Actions pane and select **Virtual Machine** to start the New Virtual Machine Wizard. Click **Next.**

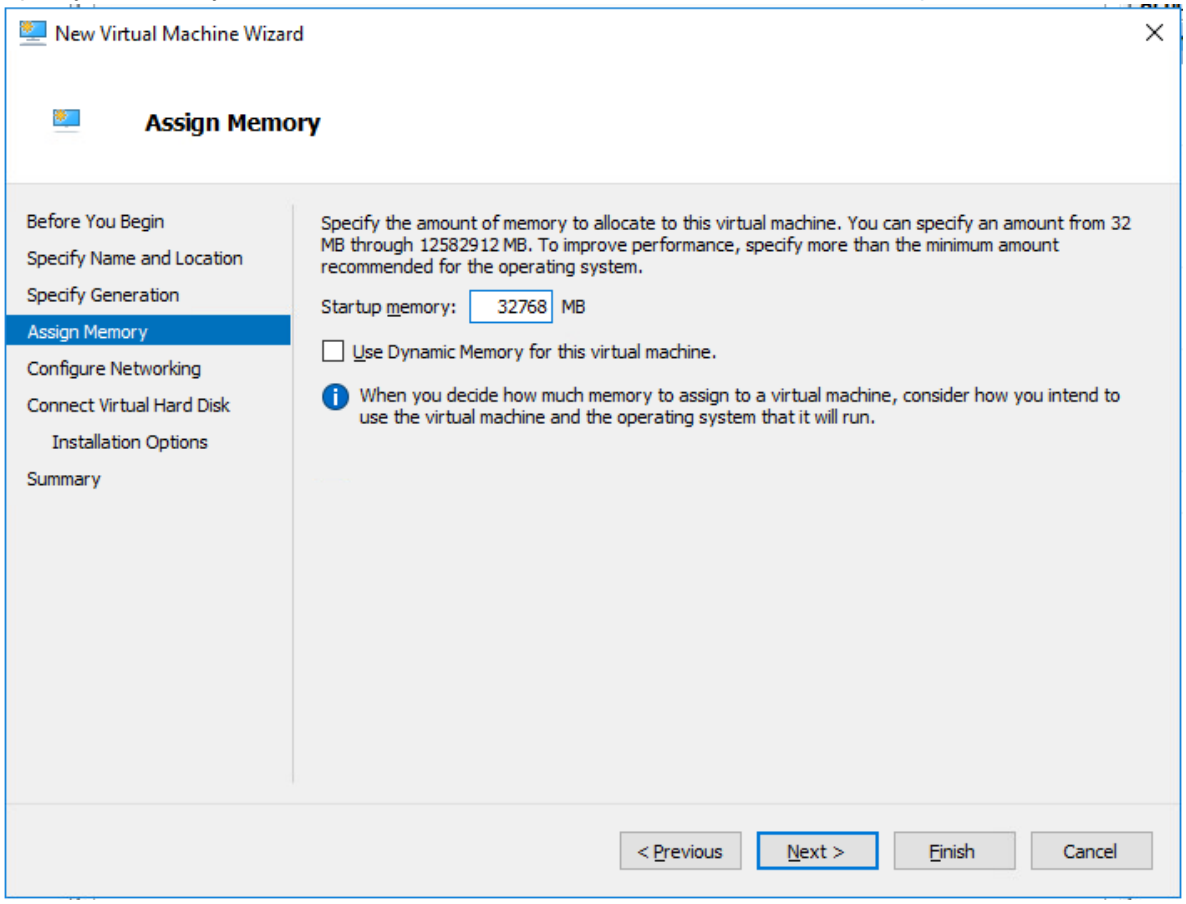
4. Enter a name and select location for FortiAIOps. Click **Next**.



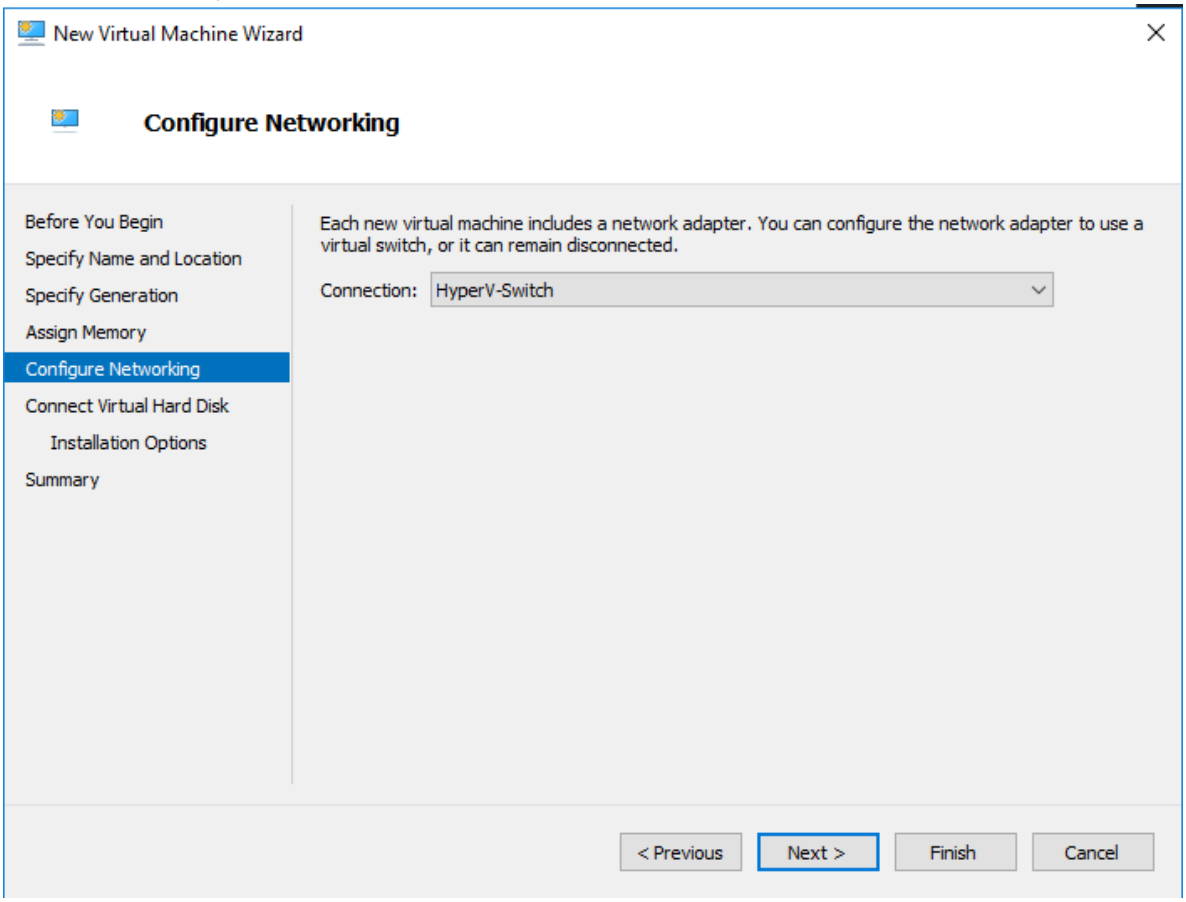
5. Select **Generation 1** and click **Next**.



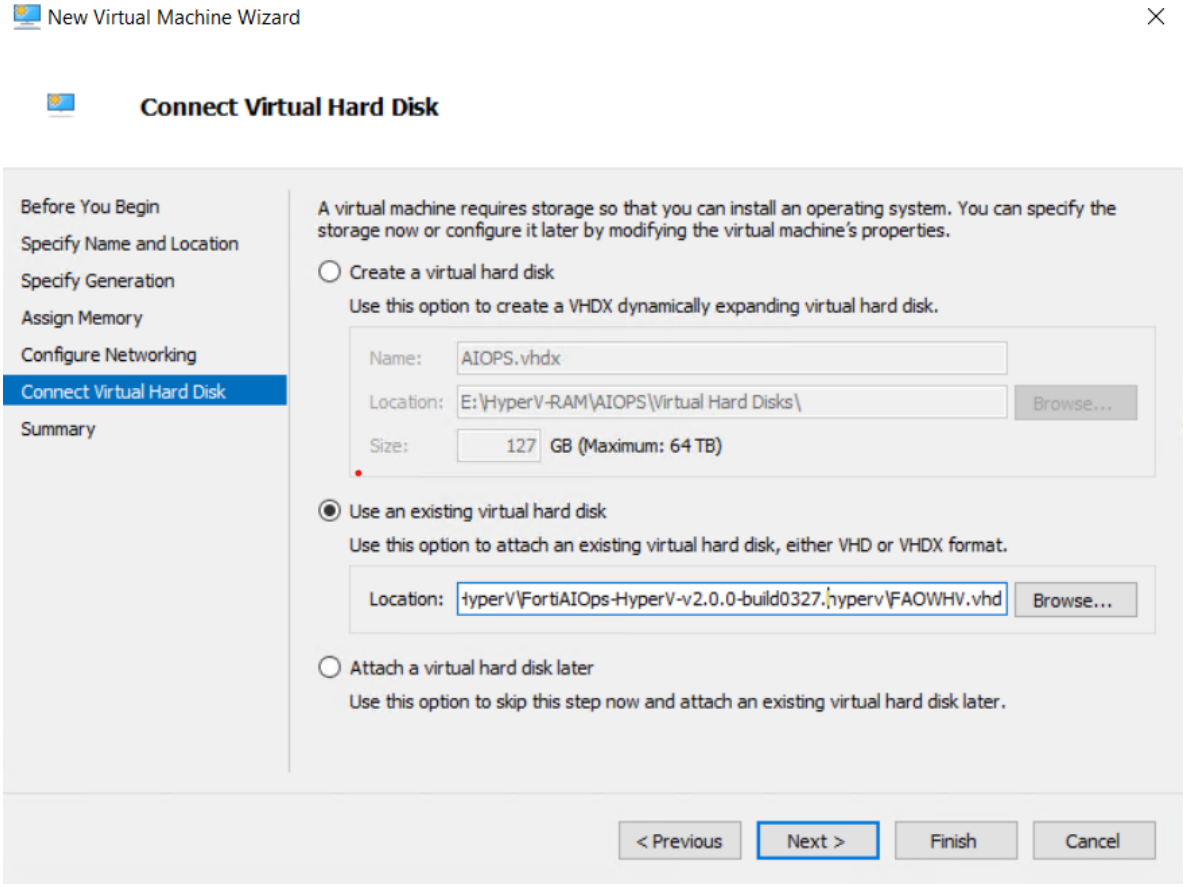
6. Specify the memory that needs to be allocated. Click **Next**. See Pre-installation Requirements.



7. Select network adapter and click **Next**.

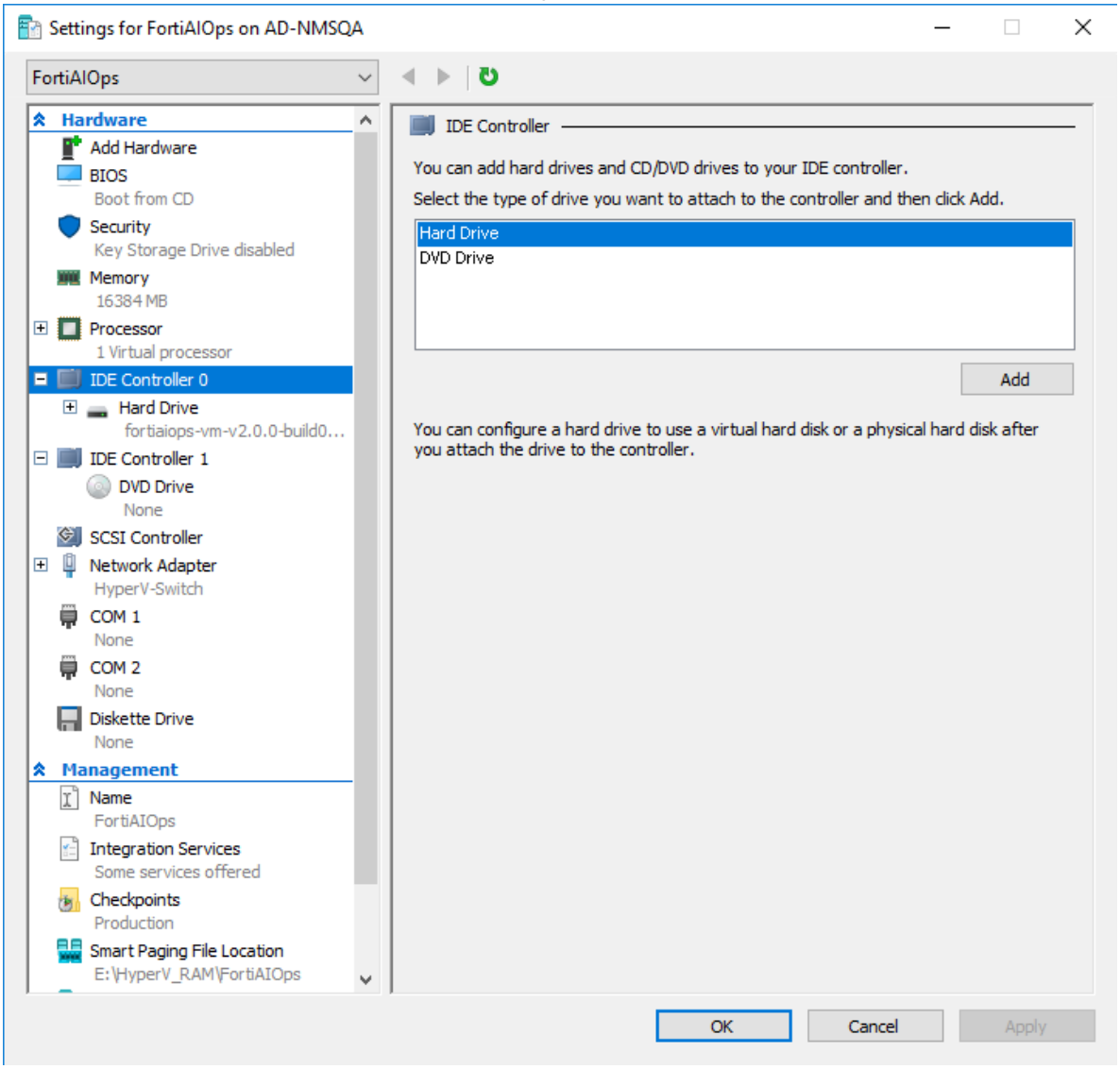


8. Select **Use an existing virtual hard disk**. Browse and select **FAOWHV.vhd** image locally stored. Click **Next**.

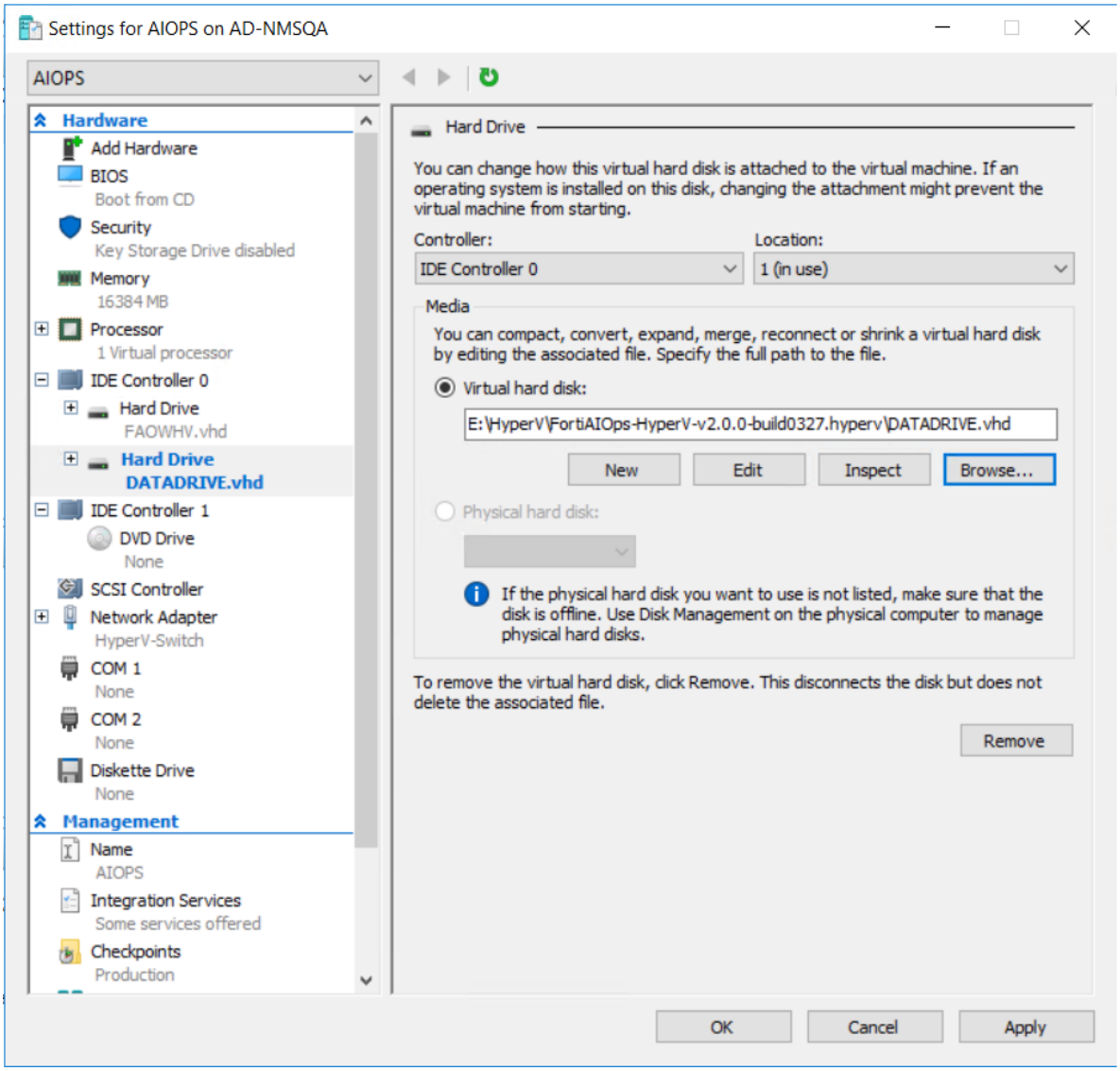


9. Review the settings and click **Finish**.
10. Right click on the new virtual machine created and select **Settings**.

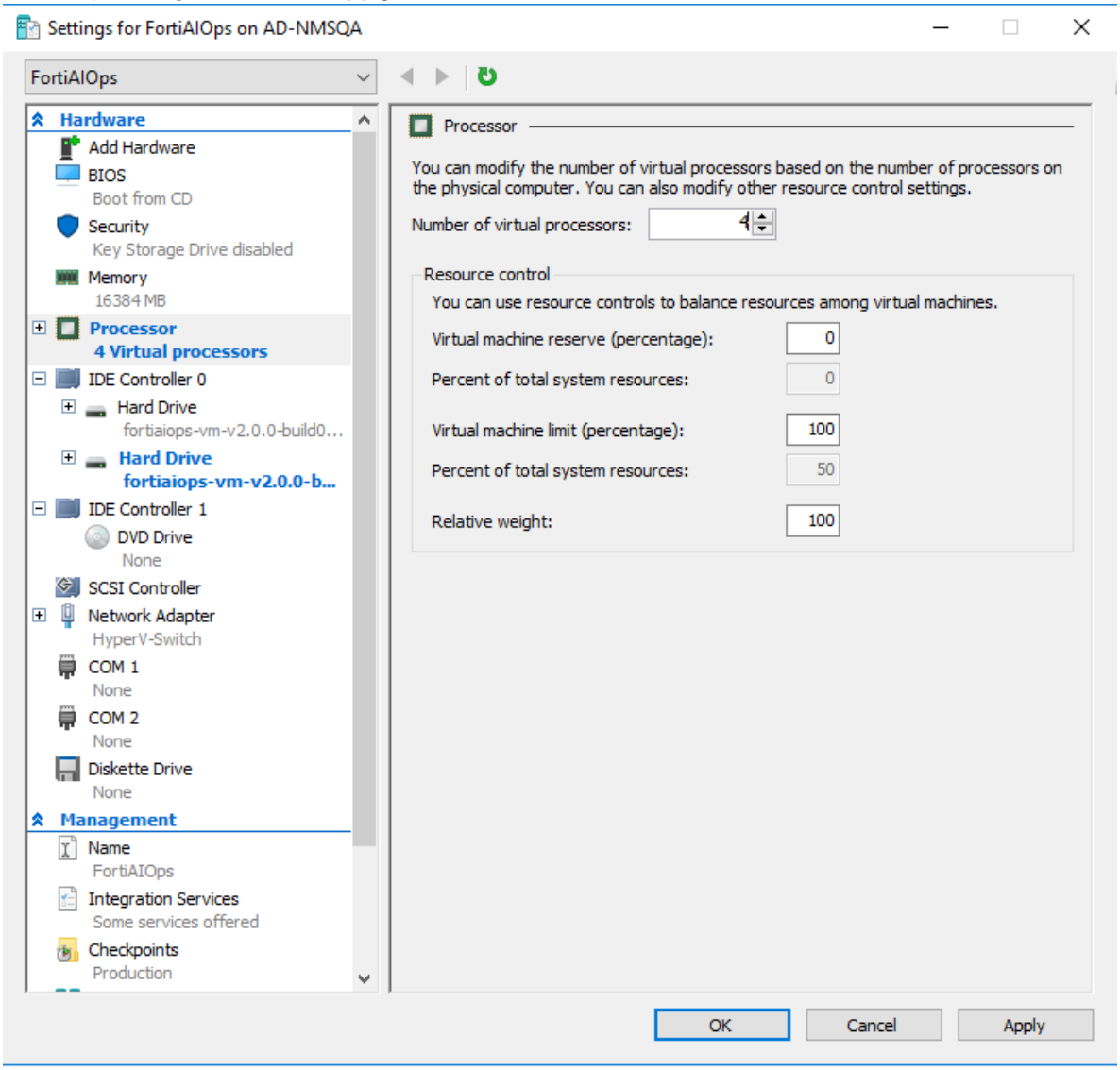
11. Select **IDE Controller 0** under **Hardware** in the left pane. Select **Hard Drive** and click **Add**.



12. Select the newly created hard drive. Select **Virtual hard disk** option. Browse and select the **DATADRIVE.vhd** image. Click **Ok**.



13. Select **Processor** under **Hardware** in the left pane. Enter the number of virtual processors based on your FortiAIOps configuration. Click **Apply**. Click **Ok**.



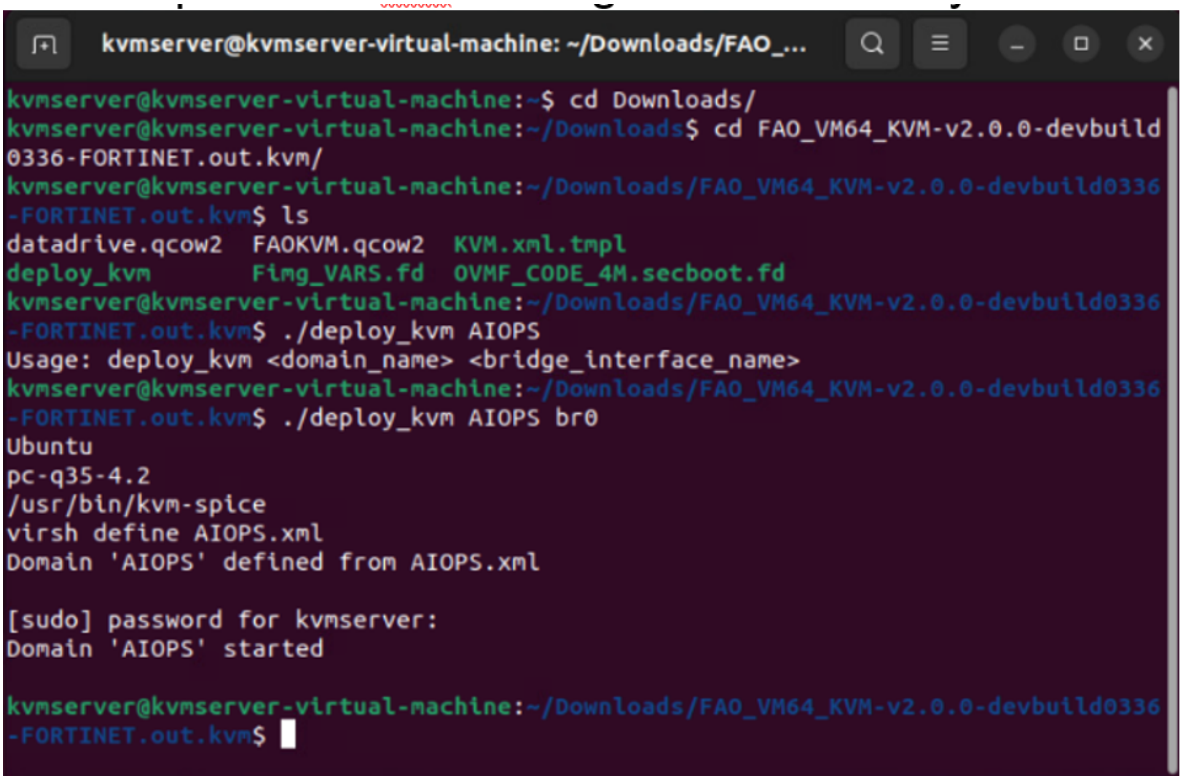
14. Right click on the virtual machine and click **Start**. Once the virtual machine is up and running, launch the console.
15. Perform post-installation tasks.

Installing FortiAIOps on KVM

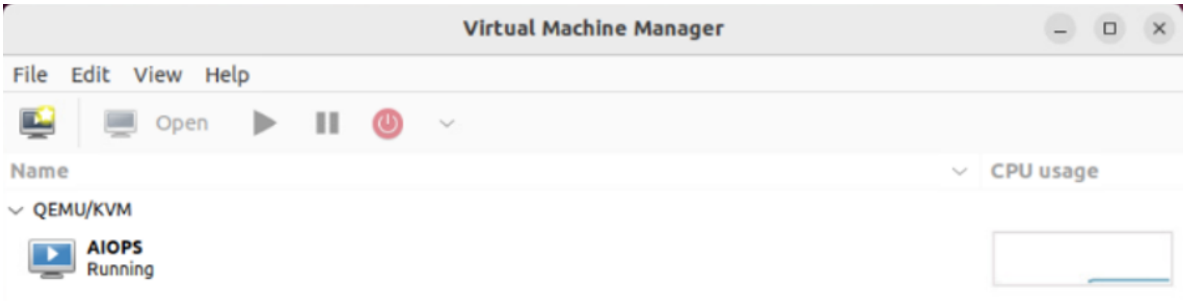
Perform the following steps to deploy FortiAIOps on KVM using virt-manager.

1. Download the installation file from *Fortinet Support* portal and unzip the file *FAO_VM64_KVM-vx.x.xdevbuildxxxx-FORTINET.out.kvm.zip*.
2. Open terminal and navigate to the path of the downloaded and unzipped installation files.

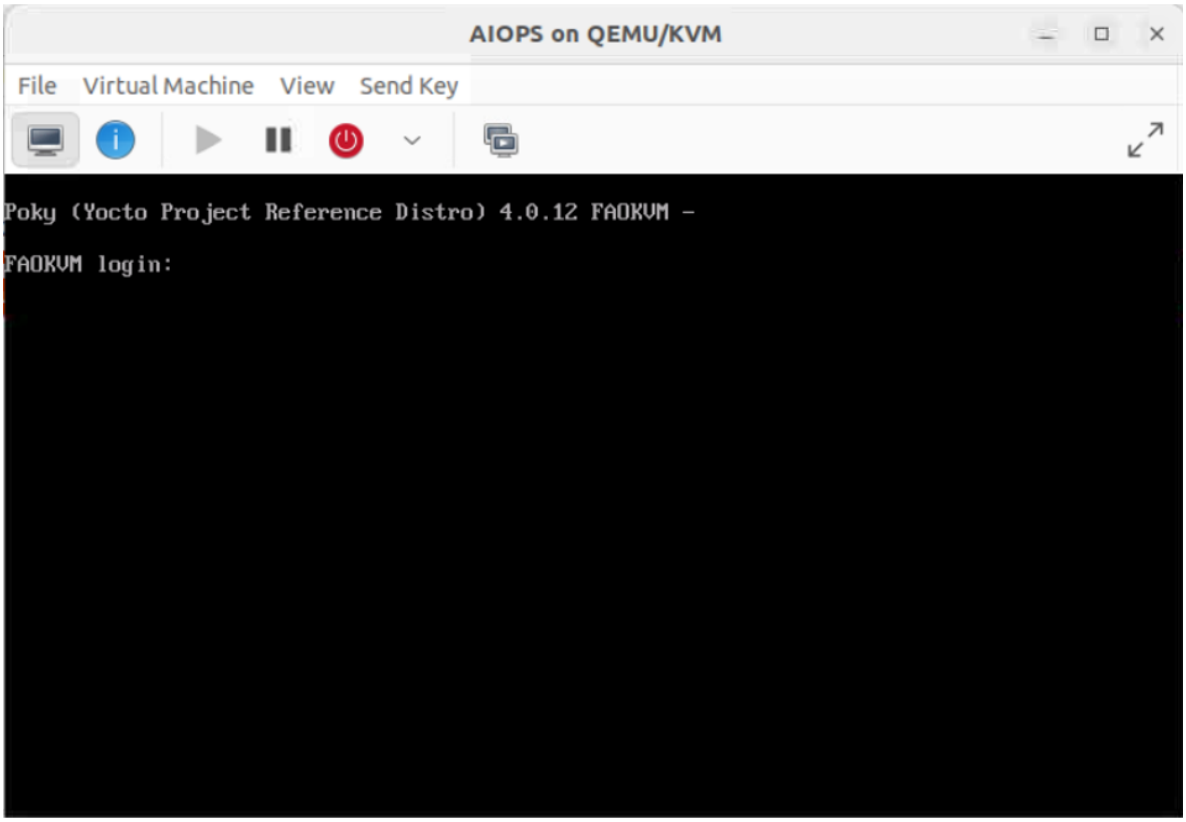
3. Run the `./deploy_kvm {name of machine} {interface to run the machine}` command to deploy FortiAIOps in the virt-manager automatically.



4. Open the virt-manager window.



5. Click **Open** to launch the console after the virtual machine is in a running state.

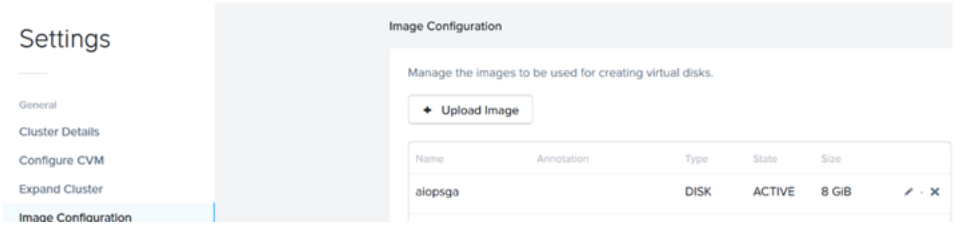


6. Perform post-installation tasks.

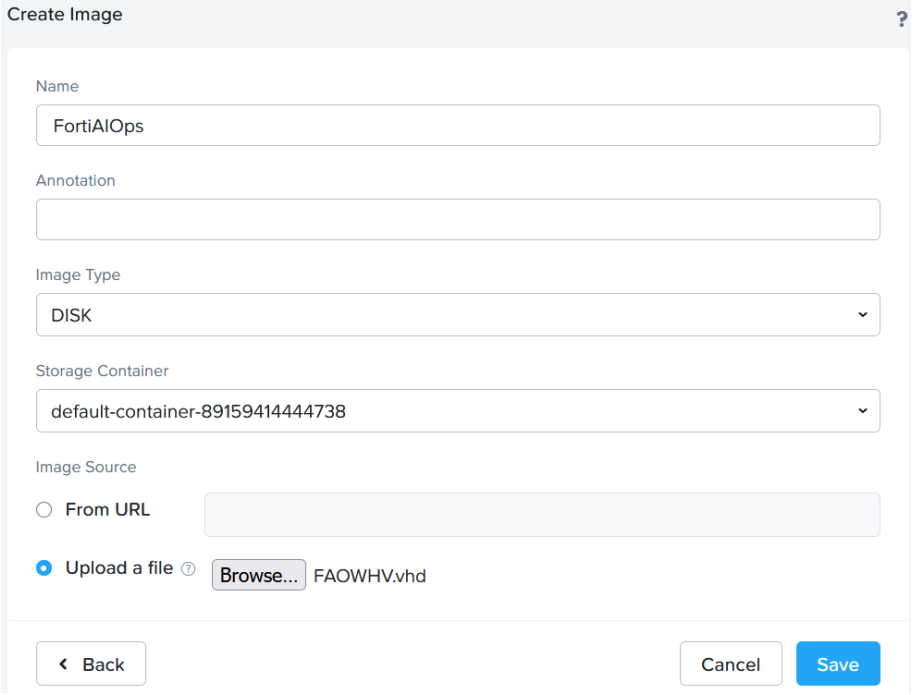
Installing FortiAIOps on Nutanix

Perform the following steps to deploy FortiAIOps on Nutanix.

1. Obtain *FAO_VM64_HV-v2.0.1-[build0xxx]-FORTINET.out.hyperv.zip* from Fortinet and extract it to obtain the files *FAOWHV.vhd* and *DATADRIVE.vhd*.
2. Log in into the Nutanix Prism user interface and click the icon. Select **Image Configuration**.

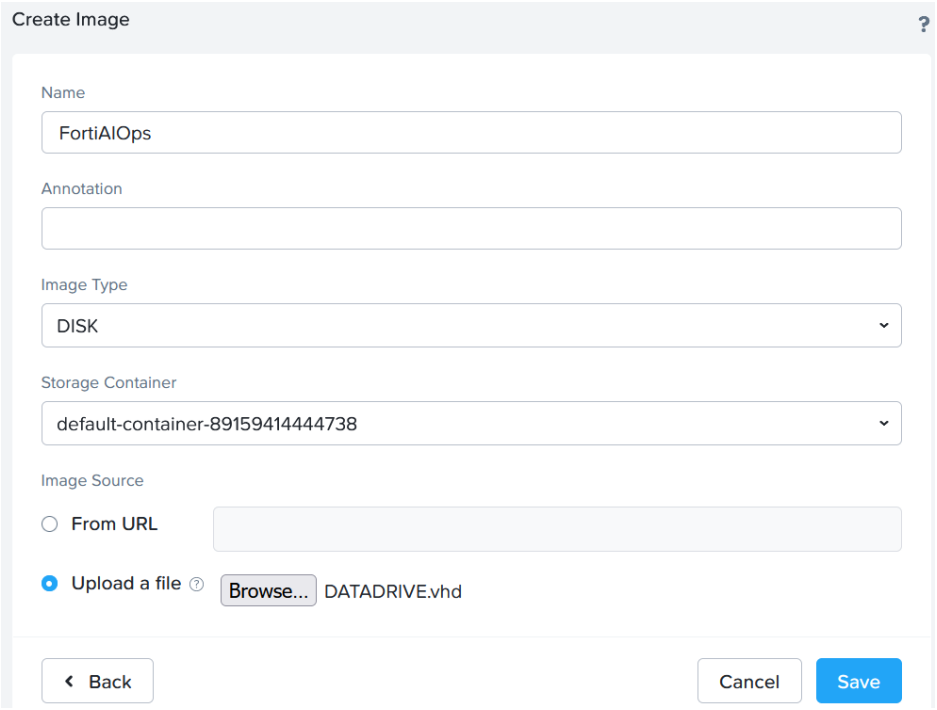


3. Upload both the *FAOWHV.vhd* and *DATADRIVE.vhd* files in the order as mentioned here. To upload *FAOWHV.vhd*, click **Upload Image** and update the following fields.



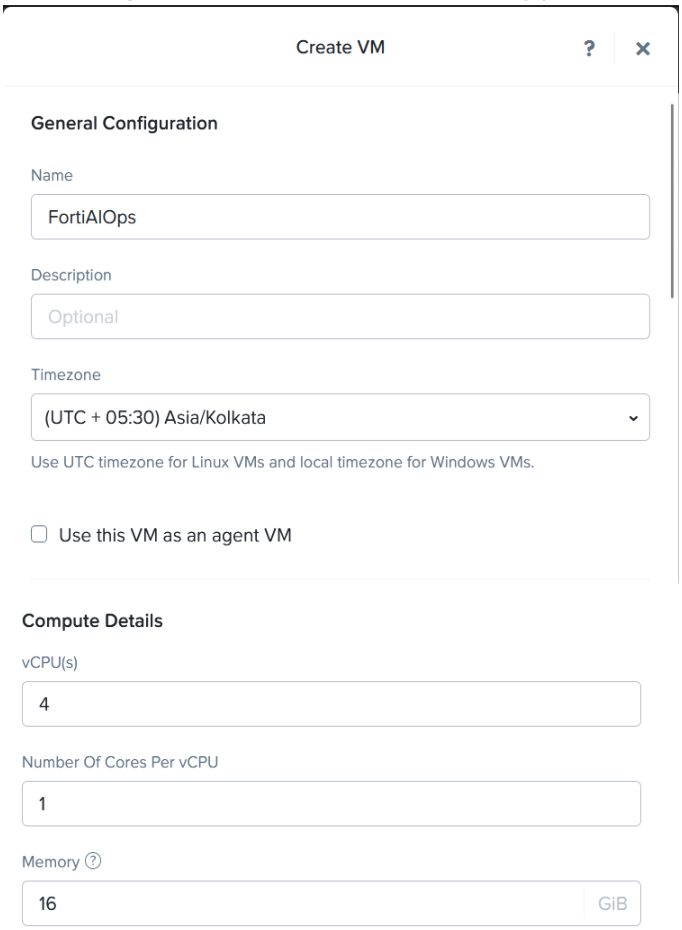
- Enter a **Name** for the FortiAIOps image file.
- Select **Disk** in as the **Image Type**.
- Select the **Storage Container**.
- In the **Image Source** section, click **Upload a file** and browse to the FortiAIOps image file *FAOWHV.vhd*.

4. Click **Save**.
5. Repeat steps 3 and 4 to upload *DATADRIVE.vhd*.

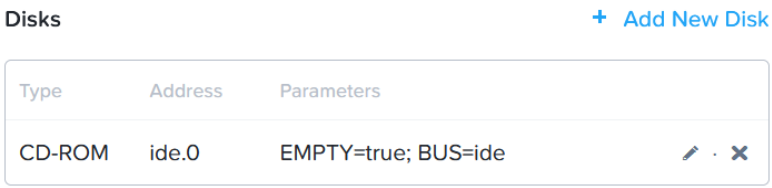


6. Refresh the browser after a few seconds and the newly created images are listed in the **Image Configuration** page.
7. To create a VM, navigate to the VM dashboard and click **Create VM** and enter the following configuration.

- Enter a **Name** for the FortiAIOps VM.
- Select your **Timezone**.
- In the **Compute Details** section, enter 4 **vCPU(s)** and 8 GB of **Memory**.

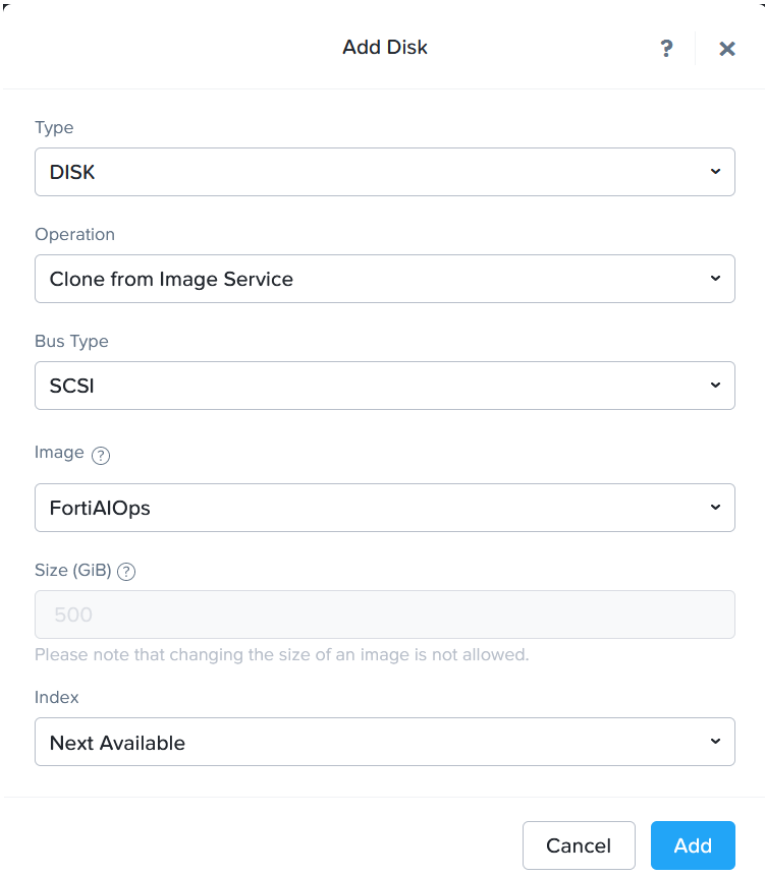


Note: By default, a CD-ROM is listed under **Disks**, delete this CD-ROM.

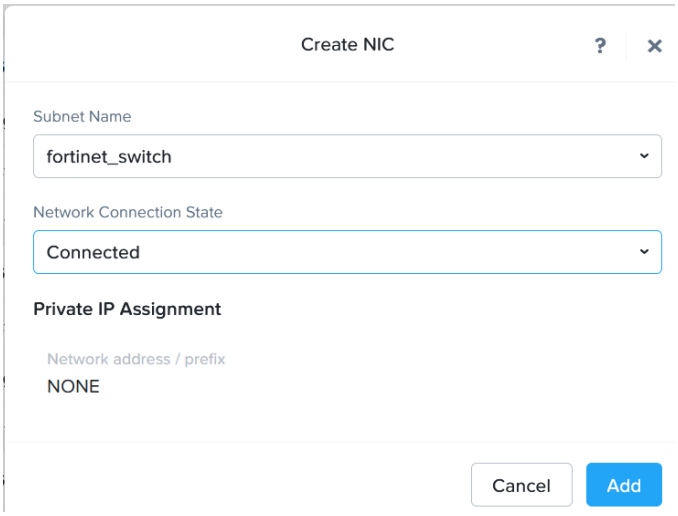


8. To create a new Boot disk, click **Add New Disk** and enter the following configuration.
   - Select **Clone from Image Service** as the **Operation** and the disk is cloned from the FortiAIOps image files uploaded earlier in this procedure.
   - Select **SCSI** as the **Bus Type**.

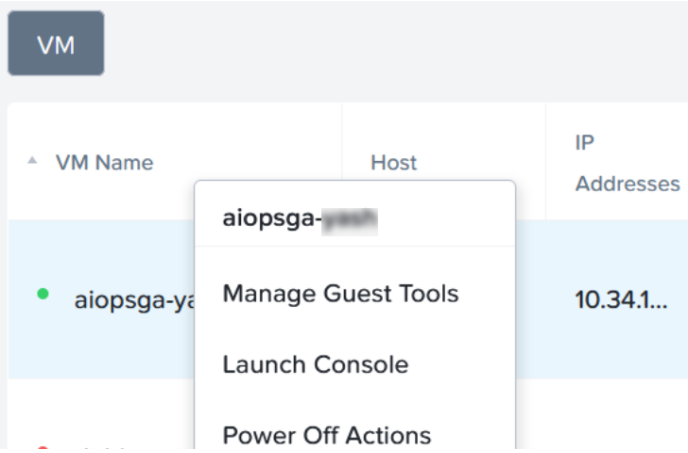
- Select the uploaded FortiAIOps disk **Image** - *FAOWHV.vhd*.



9. Click **Add**.
10. Add another disk for *DATADRIVE.vhd* following the previous step.
    Note: Ensure to create a new disk for *FAOWHV.vhd* first and then for *DATADRIVE.vhd*.
11. Add 4 Network Adapters, click **Add New NIC**.



12. Power on the VM and launch the console.



13. Configure the FortiAIOps static IP address on starting the VM. See Post-installation Tasks.

Installing FortiAIOps on Proxmox

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
```

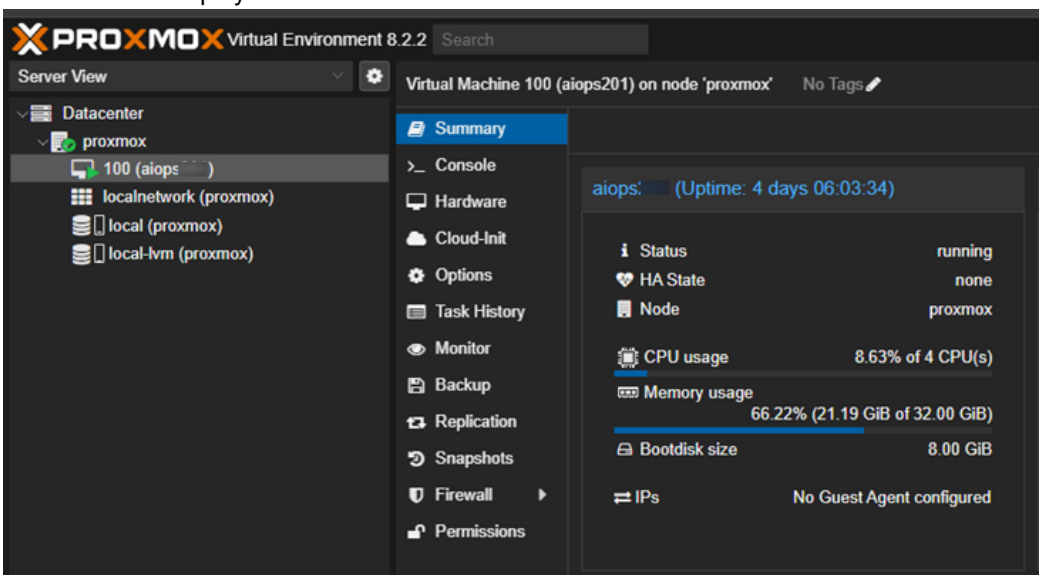
3. Import the FortiAIOps disk image manually in the Proxmox shell to create the VM.

```
./deploy_pmx -n <name> -v <volume> -b <bridge> [-i <vmid>] [-c <cores>] [-m
<memory>]
```

where

`<name>`is the name of the VM, for example, fortiaiops.
`<volume>` is the target storage ID, for example, local-lvm.
`<bridge>` is the network bridge to use, for example, vmbr0.
`<vmid>` is the ID assigned to the new VM; the default is to use the next available free ID.
`<cores>` is the number of CPU cores to allocate; the default is 8.
`<memory>` is the amount of RAM to allocate (in MB); the default is 32768 MB.

4. The VM is now deployed.



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

Post-installation Tasks

Perform the following steps to access FortiAIOps after successful installation.

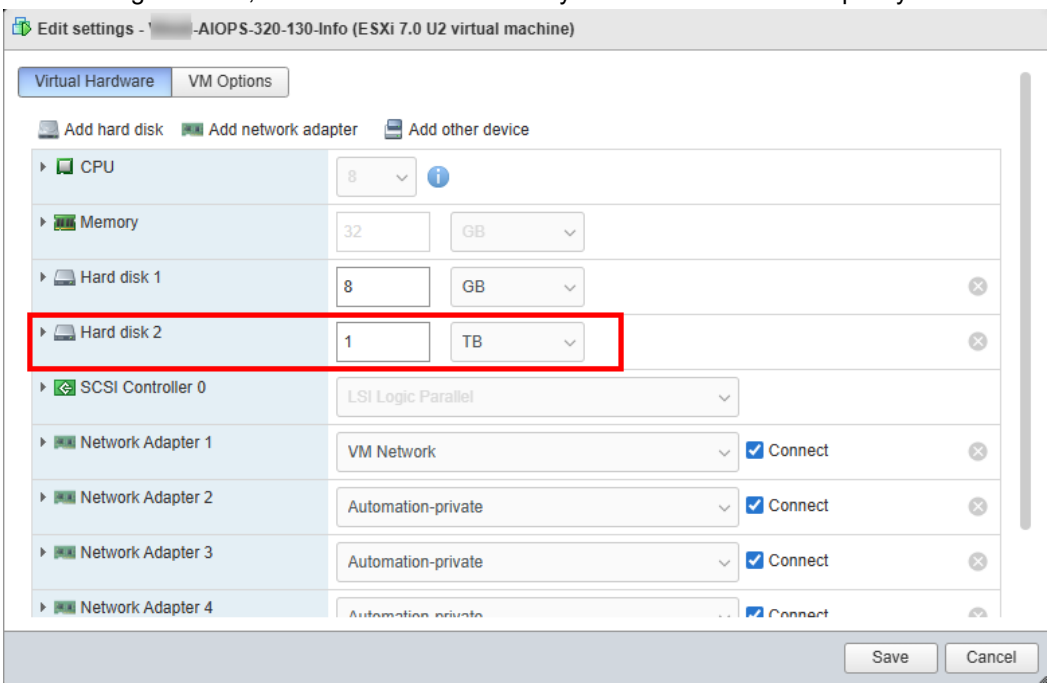
1. Turn on the newly created VM, if it is not already ON. In the virtual machine console, log in as an admin user with the username **admin**. A password is not required
2. Login as FortiAIOps administrator with username **admin**. Configure the password after the first login.
   Note:
   - By default, there is no password for logging into the CLI mode for the first time. However, you are prompted to change the password after logging in.
   - By default, the username for logging into GUI is admin and there is no password.
   - Configuring the CLI password will sync with GUI password
3. Ensure that the IP address is configured properly. Run the `get system interface` command to view the dynamically assigned IP address. Run `config router static` command to assign a static IP address.

Increasing VM Disk Space

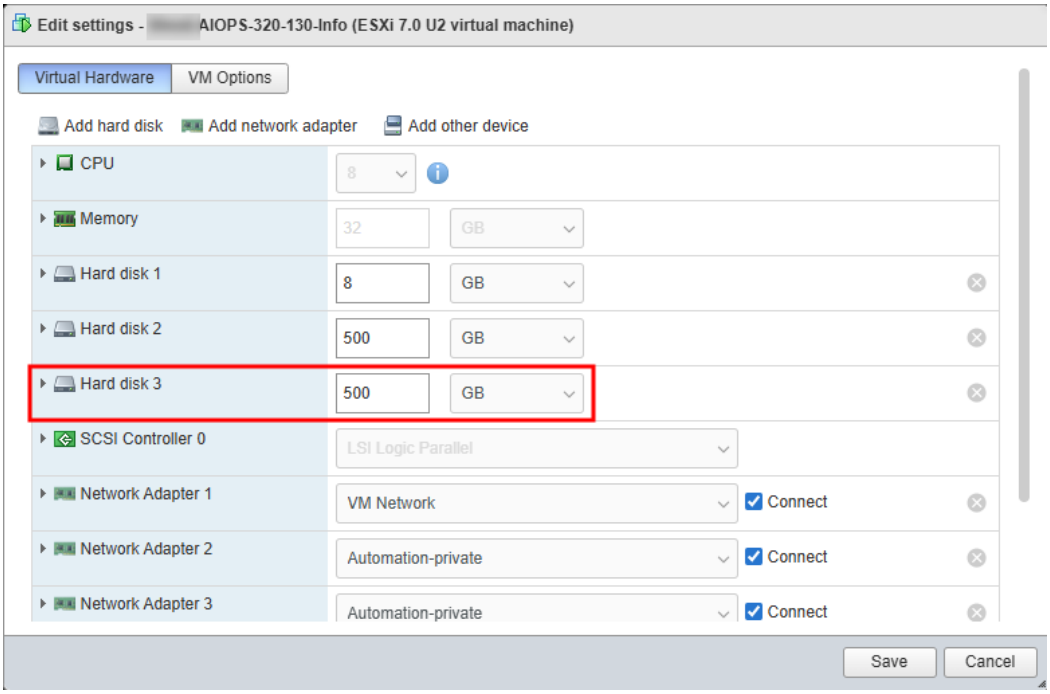
Use the following procedure to increase the disk space on your virtual machine. This procedure uses VMware ESXi as an example, but the steps are similar for other virtual machine platforms.

1. Log in to your virtual machine management GUI (For example, VMware ESXi).
2. Navigate to the list of virtual machines and select the instance you want to modify.
3. Before making any hardware changes, you must **Shut down** the virtual machine instance to prevent data corruption.

4. Once the VM is off, select the option to **Edit** its settings.
5. In the settings window, find **Hard disk 2** and modify its size to the desired capacity.

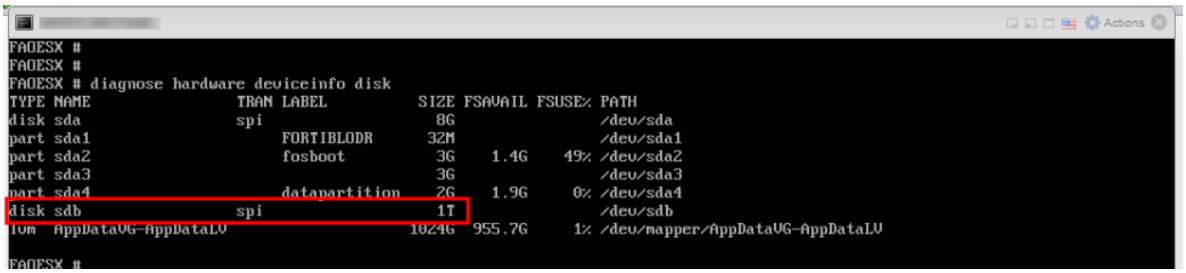


6. To add another hard disk, click **Add hard disk**. Modify the size as required.

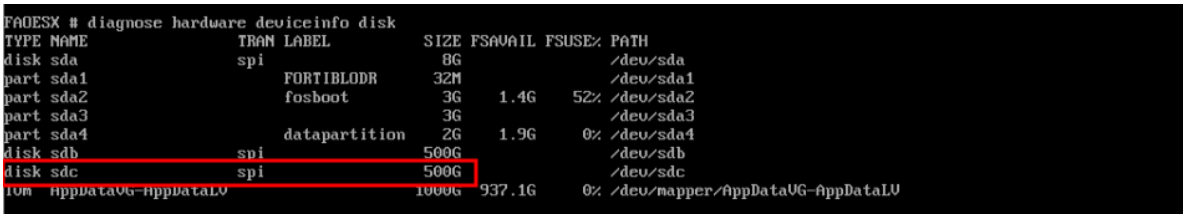


7. Click **Save** to apply the changes.
8. **Power on** the virtual machine instance.
9. After the VM reboots, log in to the virtual machine using the console.
10. Run the following command to view the updated disk and partition information:

```
diagnose hardware deviceinfo disk
```



The output shows that the disk sdb is increased to 1 TB in size.
If you have added another hard disk, you will see an output similar to the following:



Accessing FortiAIOps

After successfully generating a new password and configuring a static IP address for the FortiAIOps server, you can access the FortiAIOps application portal for management operations and to monitor your network. Open a compatible web browser and enter the *https://<fortiaiops_server_IP>* URL, where *<fortiaiops_server_IP>* is the configured static IP address. The default username is admin and there is no password. You are prompted to change the password after the first login.

Upgrading FortiAIOps

You can upgrade FortiAIOps via the GUI and the CLI.

- **Upgrade via GUI** - Navigate to **System > Upgrade** to upgrade FortiAIOps. See Upgrade.
- **Upgrade via CLI** - Run the following command to upgrade FortiAIOps.

  ```
  execute restore image ftp <path to upgrade file><upgrade file name> <IP address> <username> <password>
  ```

Deploying FortiAIOps on Public Cloud Platforms

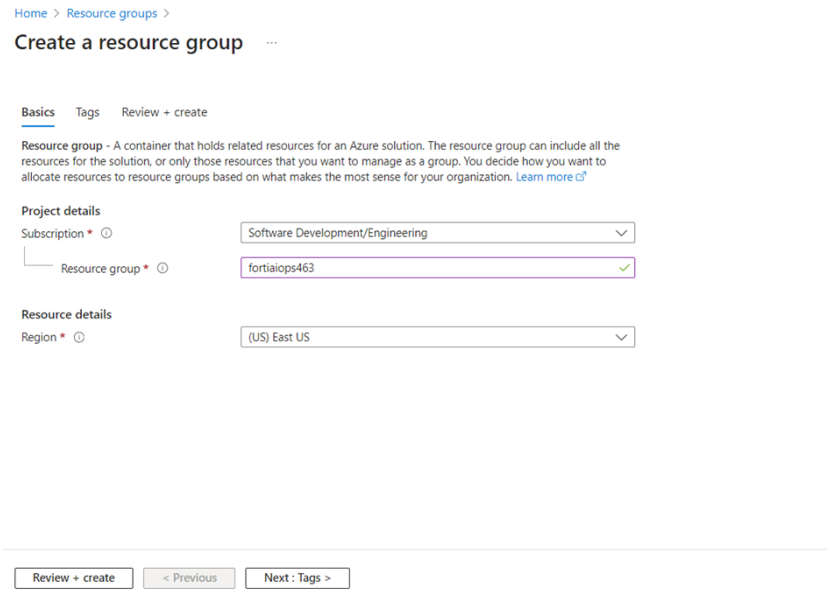
FortiAIOps can now be deployed on the following public Cloud platforms.

- Microsoft Azure
- Google Cloud Platform
- Amazon Web Services (AWS)
- Oracle Cloud Infrastructure (OCI)

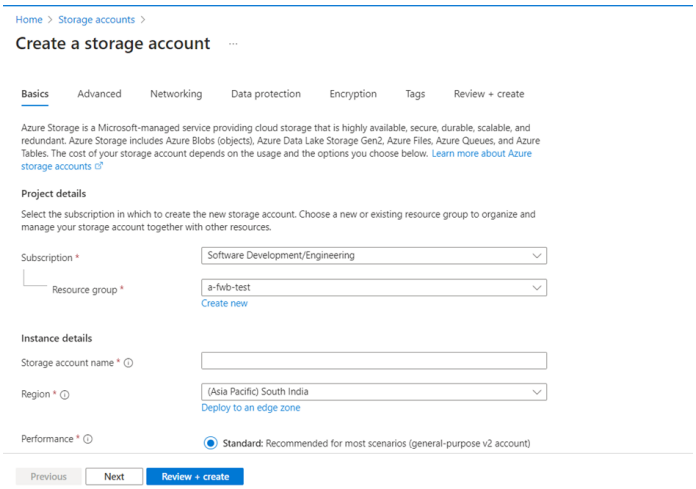
Microsoft Azure

Perform the following steps to deploy FortiAIOps on Microsoft Azure. For more information on the Azure portal configurations, see the Azure documentation.

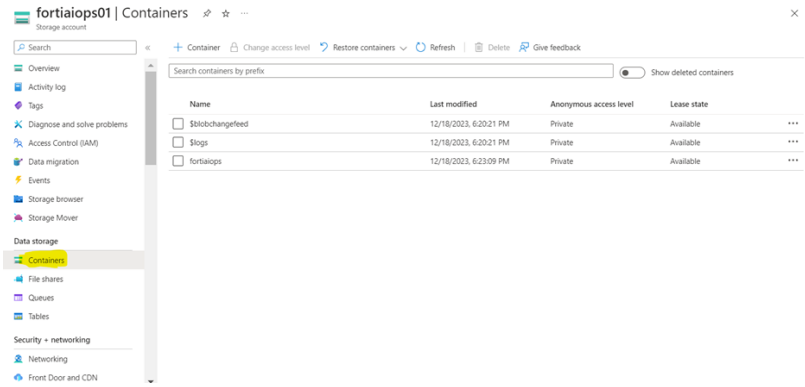
1. Download the file *FAO_VM64_AZURE-v2.0.1-[build0xxx]-FORTINET.out.azure.zip* from Fortinet and extract it to obtain the file *FAO_VM64_AZURE-v2.0.1-[build0xxx]-FORTINETout.vhd*.
2. Upload the extracted VHD file on to the Azure portal using the following procedure.
   - Create a new **Resource Group** or use an existing one from the portal. See Manage Azure Resource Group.



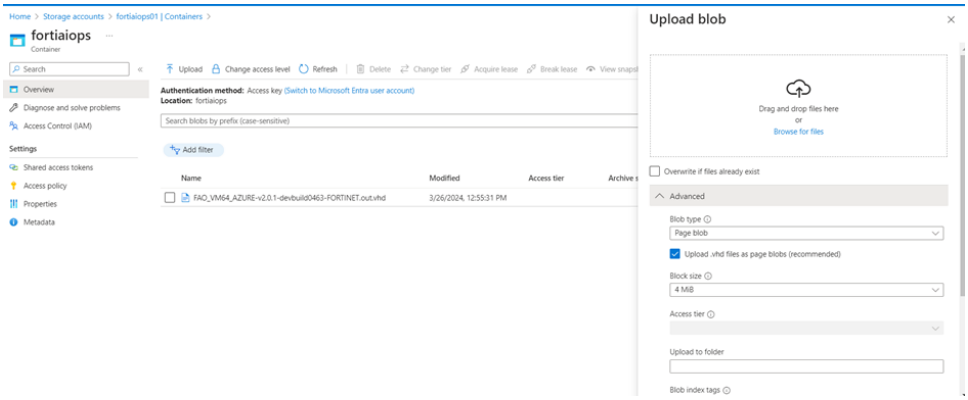
   - Create a new **Storage account** or use an existing one from the portal. See Create a storage account.



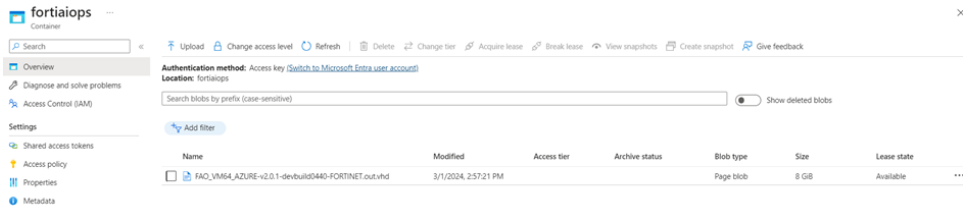
- In the Storage account, select a **Container** or create a new one to upload the VHD file. See Create a container.



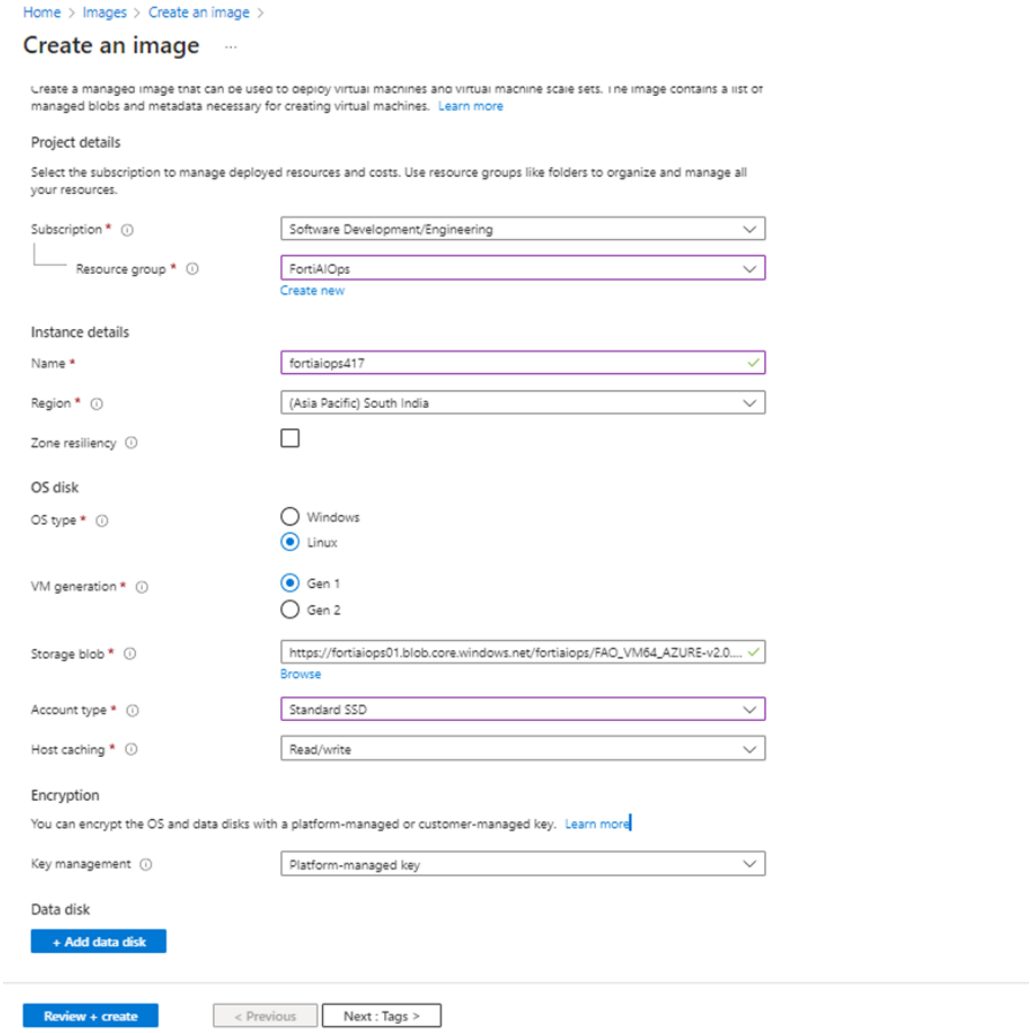
- When uploading the VHD file, select the **Blob type** as **Page blob**.



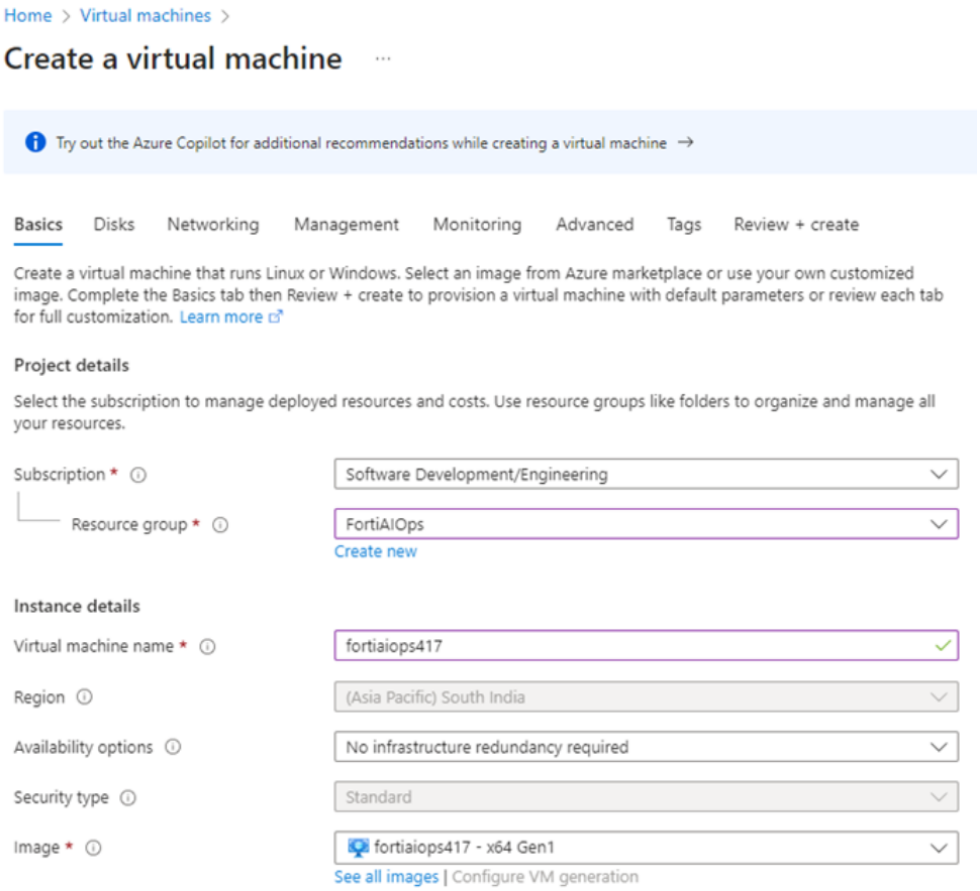
- After the upload, verify that the file is listed in the **Containers** page.



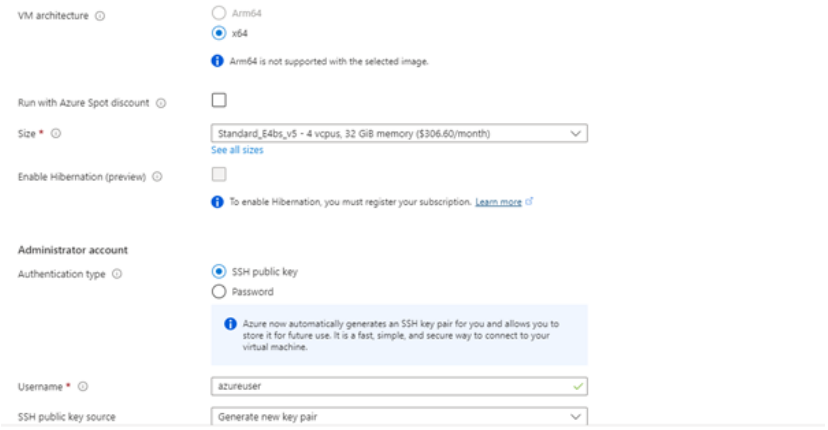
3. Create a managed image from the uploaded VHD file. Navigate to **Images > Create** an image in the Azure portal and configure the following settings.
   - Select a **Resource group**.
   - Enter a **Name** for the image.
   - Select the applicable **Region** from the list.
   - Set the **OS type** to **Linux**.
   - Set the **VM generation** to **Gen 1**.



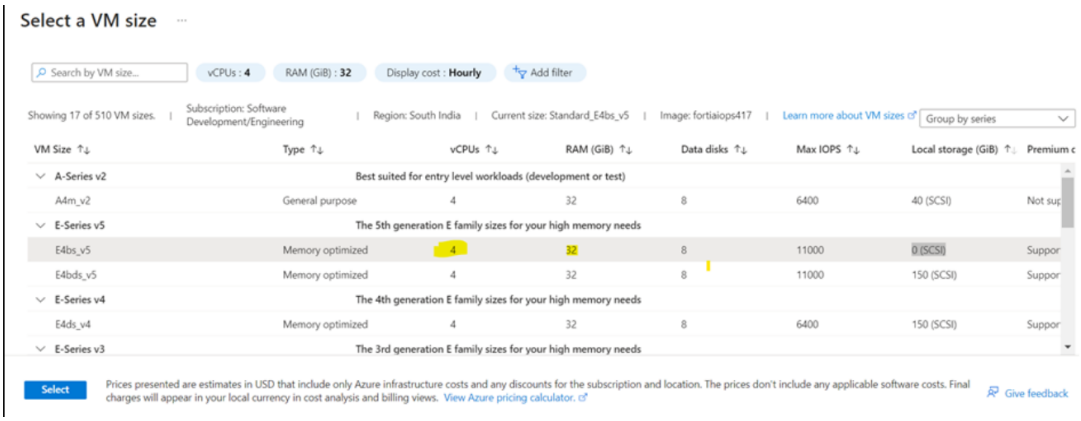
4. Browse and select the uploaded VHD file in the **Storage blob**.
   Note: It is not required to add data disk in this step, the data disk addition is required when the virtual machine is created.
5. Click **Review + create** to create an image.
6. Create a virtual machine from the managed image that you just created. Select **Virtual machines > Create Azure virtual machine** on portal.



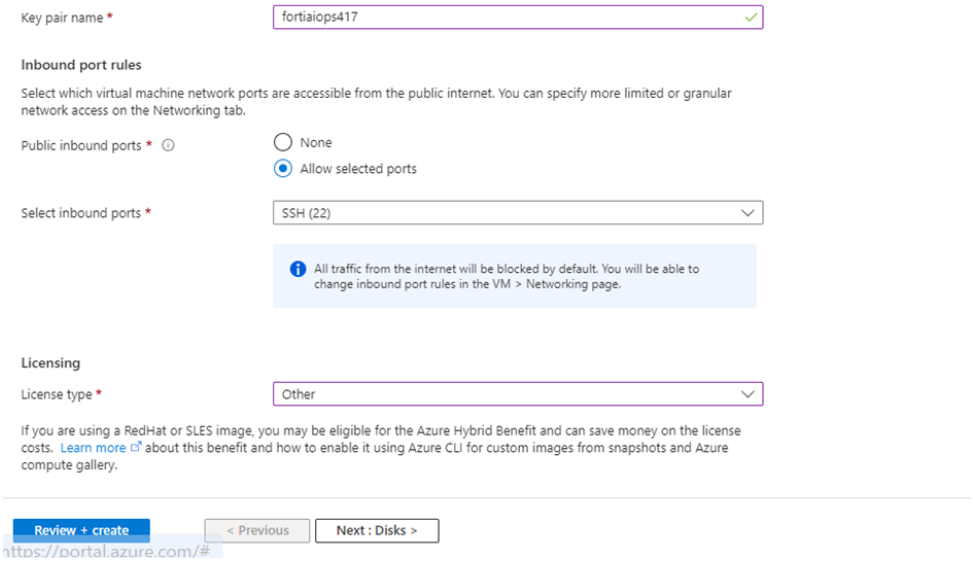
- Select a **Resource group**.
- Enter a **Name** for the virtual machine.
- Select the applicable **Region** from the list.



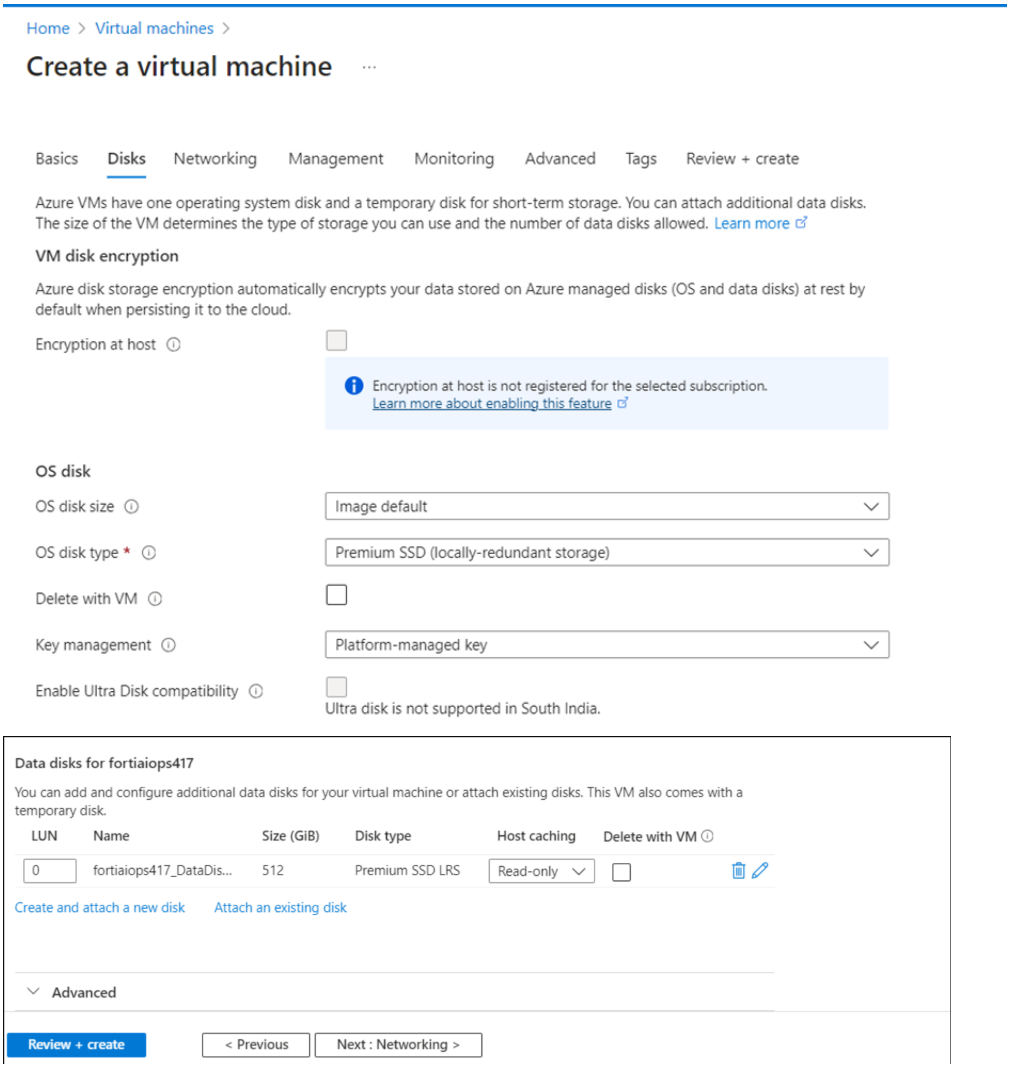
7. Click **See all images** to browse and select the image that was generated in the previous step.
8. Click **See all sizes** to select a virtual machine size.
   Note: It is recommended to select VM size as 4 vCPU and 32 GB RAM, and the **Local storage** as 0.



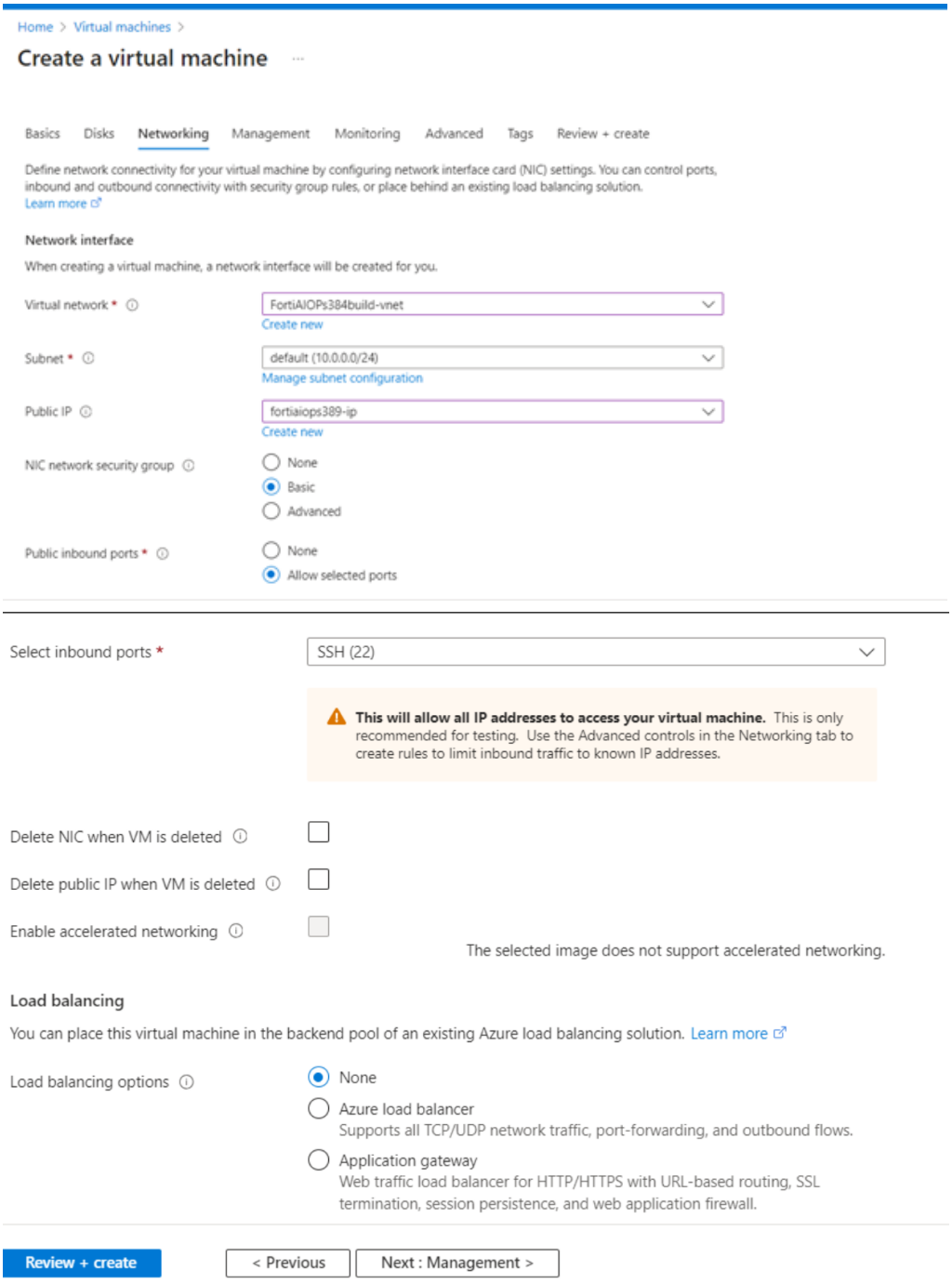
9. Configure network inbound port rules to allow SSH access in the field **Select inbound ports**.



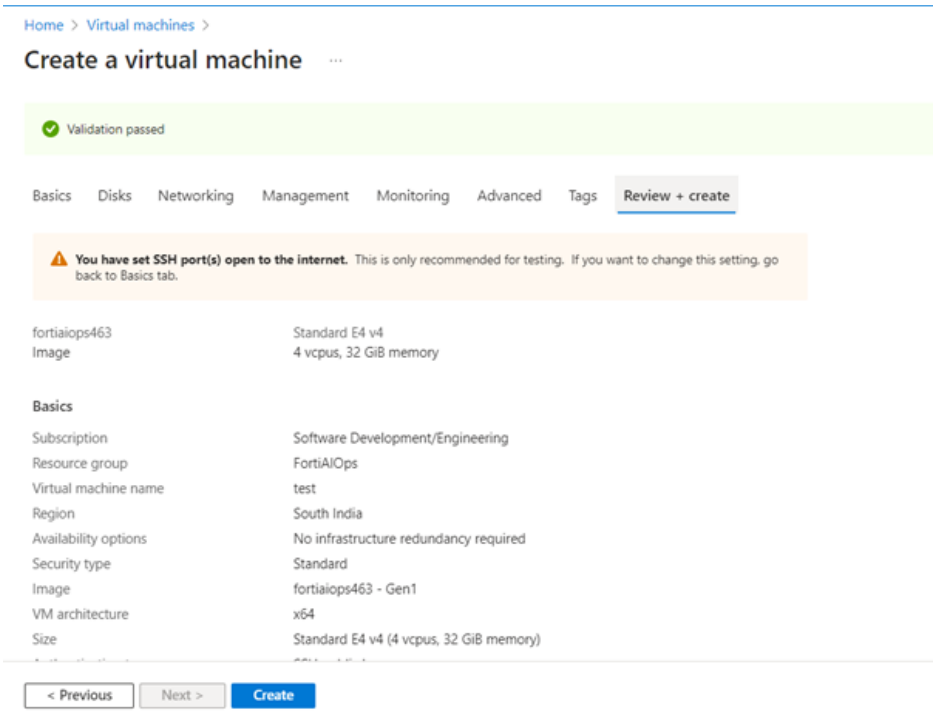
10. Click **Next: Disks** and configure disk data as is depicted in the following image.
Note: The recommended minimum data disk size is 128GB.


Home > Virtual machines >
Create a virtual machine
Basics
Disks
Networking
Management
Monitoring
Advanced
Tags
Review + create
Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. Learn more
VM disk encryption
Azure disk storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.
Encryption at host
Encryption at host is not registered for the selected subscription.
Learn more about enabling this feature
OS disk
OS disk size
Image default
OS disk type *
Premium SSD (locally-redundant storage)
Delete with VM
Key management
Platform-managed key
Enable Ultra Disk compatibility
Ultra disk is not supported in South India.
Data disks for fortiaiops417
You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.
LUN
Name
Size (GiB)
Disk type
Host caching
Delete with VM
0
fortiaiops417_DataDis...
512
Premium SSD LRS
Read-only
Create and attach a new disk
Attach an existing disk
Advanced
Review + create
< Previous
Next : Networking >

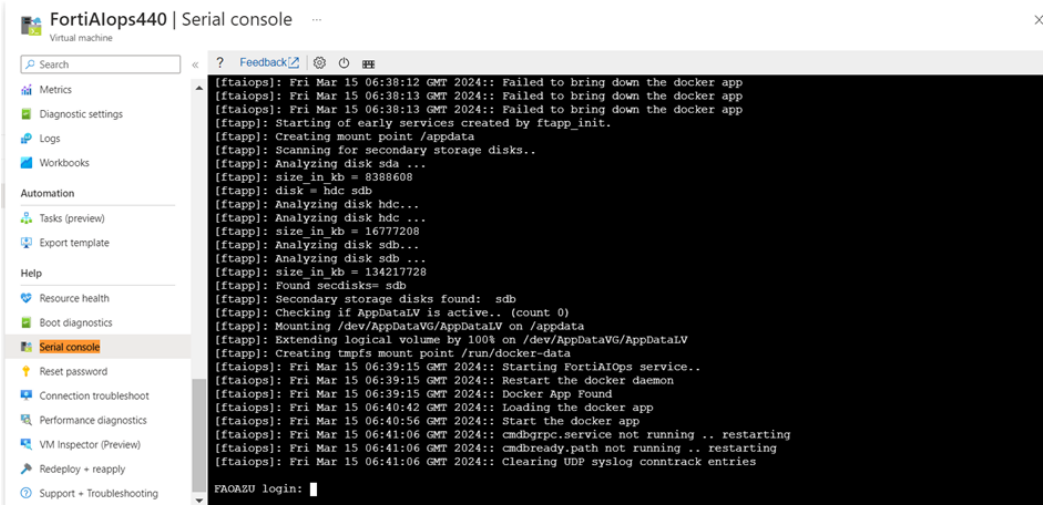
11. Click **Next: Networking** to configure the network settings.



12. Select the available **Virtual network** and the **Public IP** of the deploying machine.
13. Review the configurations under the tabs, **Management**, **Monitoring**, and **Advanced**.
14. Click **Next: Tags** and add the required tags.
15. Click **Next: Review + create** and click **Create** only if the virtual machine validation is passed, as depicted in the following image.



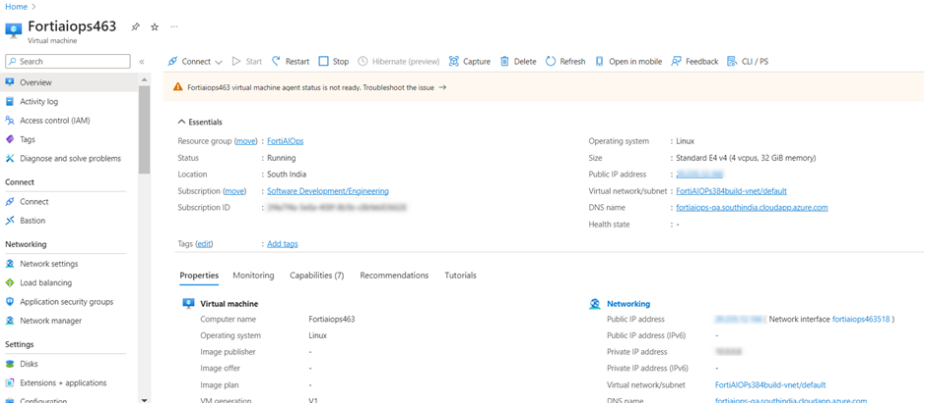
16. Connect the virtual machine in one for the following methods.
    - **Connect via Serial Console** - Select the running virtual machine and then select Serial console in the menu.



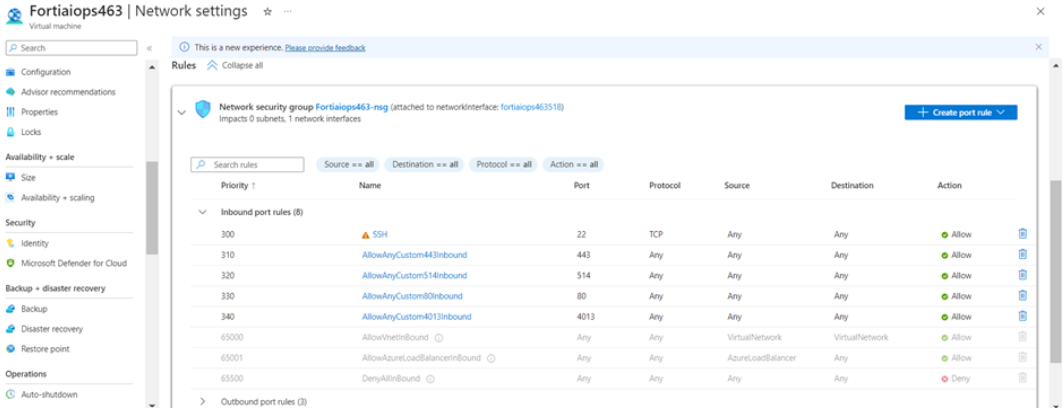
    - **Connect via SSH** - Obtain the public IP address of the virtual machine and use SSH to connect to the virtual machine.
      `ssh admin@<public_IP>`

Post-installation Tasks

- The public IP address of the virtual machine is available in the **Overview** page of the virtual machine.



- Create the inbound port rules as depicted in the following image, in the **Network settings** of the virtual machine, to enable all FortiAIOps functionality.



Note: Do not change the corresponding IP mode setting from the FortiAIOps GUI or CLI; modify all network from the Azure portal only.

Google Cloud Platform

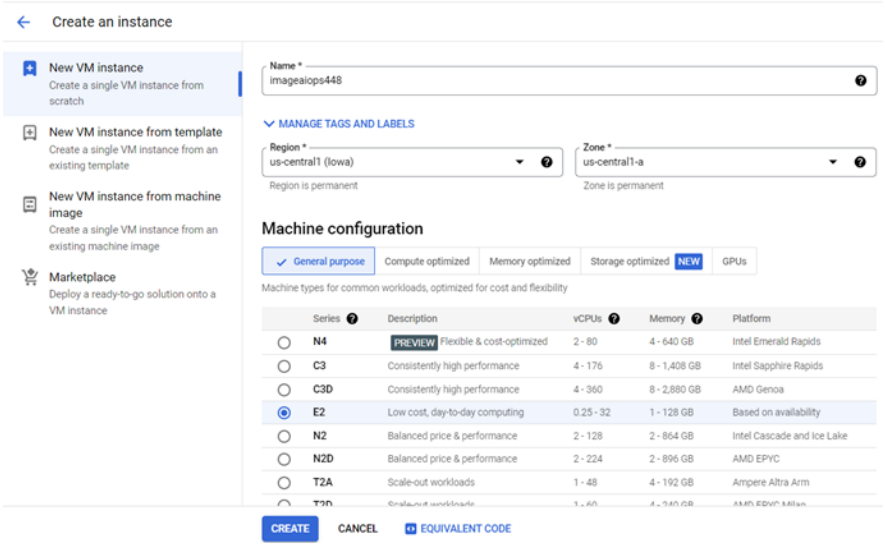
Perform the following steps to deploy FortiAIOps on Google Cloud.

1. Download the file *FAO_VM64_GCP-v2.0.1-[build0xxx]-FORTINET.out.gcp.zip* from Fortinet and extract it to obtain *FAO_VM64_GCP-v2.0.1-[build0xxx]-FORTINET.out.gcp.tar.gz*.
2. Install and setup **gsutil** to access Cloud storage from the CLI using HTTPS. To install **gsutil**, see Install gsutil.
3. Alternatively, run the following command to download the Linux 64-bit archive file.
   `curl -O https://dl.google.com/dl/cloudsdk/channels/rapid/downloads/google-cloud-cli-389.0.0-linux-x86_64.tar.gz`
4. Extract the contents of the file to any location on your file system (preferably your Home directory). To replace an existing installation, remove the existing *google-cloud-sdk* directory and then extract the archive to the same location - *tar -xf google-cloud-cli-389.0.0-linux-x86.tar.gz*.

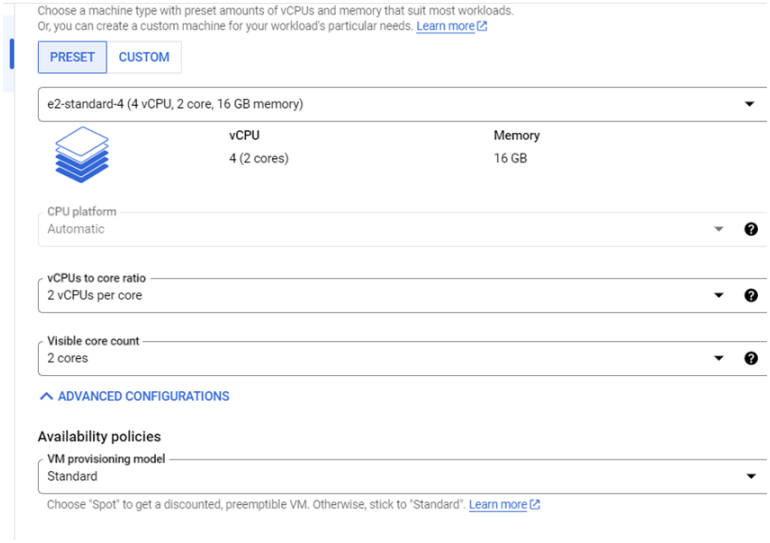
5. Run the *./google-cloud-sdk/install.sh* script (from the root of the folder you extracted the file to).
6. Run `./google-cloud-sdk/bin/gcloud init` to initialize GCP CLI.
7. Upload the file *FAO_VM64_GCP-v2.0.1-[build0xxx]-FORTINET.out.gcp.tar.gz* to the Cloud storage bucket in the GCP CLI.
   `./google-cloud-sdk/bin/gsutil FAO_VM64_GCP-v2.0.1-[build0xxx]-FORTINET.out.gcp.tar.gz gs://my-some-bucket`
8. Run the following script to create a secure boot image.
   `# bash -x import2gcpimg.sh AIOPSBuild FAO_VM64_GCP-v2.0.1-devbuild0448-FORTINET.out.gcp.tar.gz aiops-gcp`.
   where, *IMAGE_NAME =[FortiAIOps build]*, *SOURCE_FILE= [FortiAIOps image file name*, and *BUCKET_NAME =aiops-gcp*.
   Note: Make sure to create a storage bucket in the GCP GUI where the FortiAIOps image files are uploaded.

9. In the GCP portal, navigate to **Compute Engine > Images** and select the uploaded FortiAIOps image file.
10. Click **Create instance** and update the following configurations. For more information, see Create a VM.
    - Enter a **Name** for the instance.
    - Select the applicable **Region** from the list.

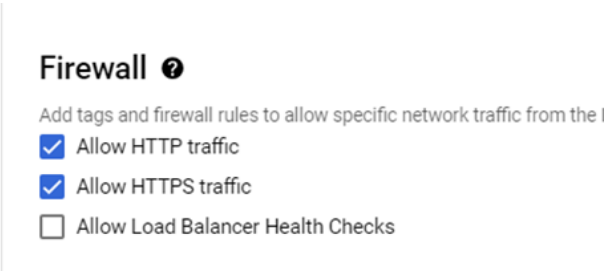
- In the Machine configuration, configure the E2 Standard with 4 VCPUs and 16 GB memory.



Note: It is recommended to use a minimum of 4 CPUs and a memory of 16 GB with the Intel Broadwell CPU platform.

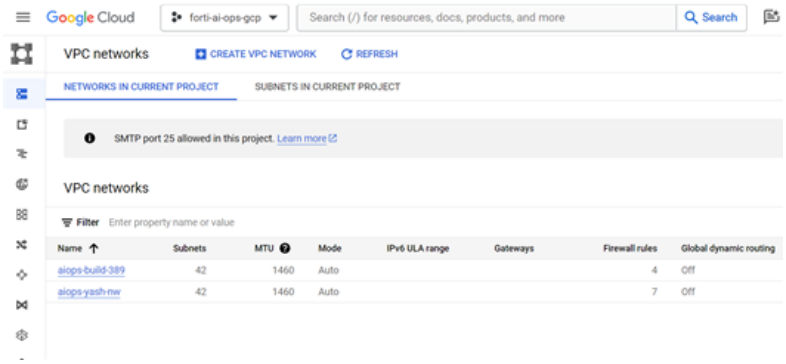


11. Enable **Allow HTTPS traffic** for web access in Firewall.

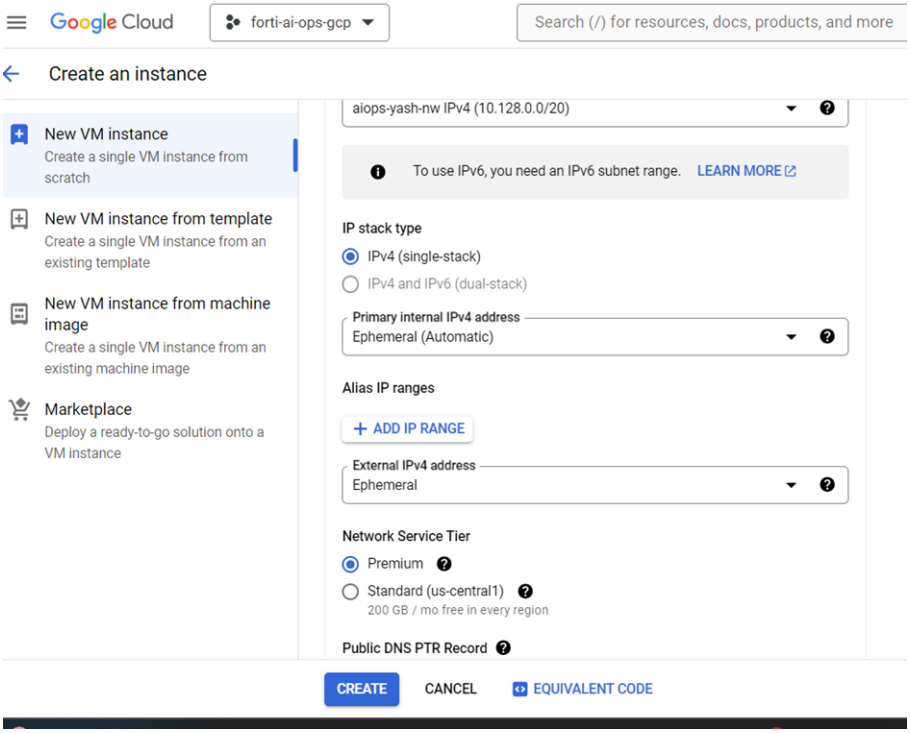


12. Click **Advanced options** to configure networking, disk and security parameters for the instance.
    - Set the **Network interface card** to **VirtIO** .
    - Select the Virtual Private Cloud (VPC) in the **Network interfaces**.
      Note:Ensure that you create VPC networks to use as network interfaces for your instance, and provide

the IP address from specified subnets. To create and use a VPC network, see Create and manage VPC networks.

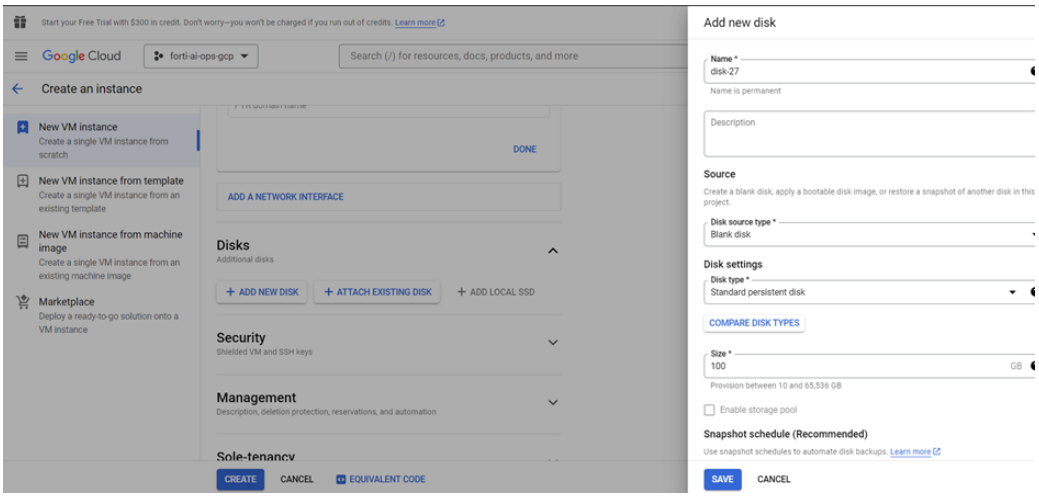


- Select other network parameters such as IP stack, primary Internal IPv4 address, and external IPv4 address as depicted in this image.
  Note: You can select the external IPv4 address as Ephermal (automatic /dynamic or static IP address.). To create external IPv4 addresses for GCP, see Reserve a static external IP address.

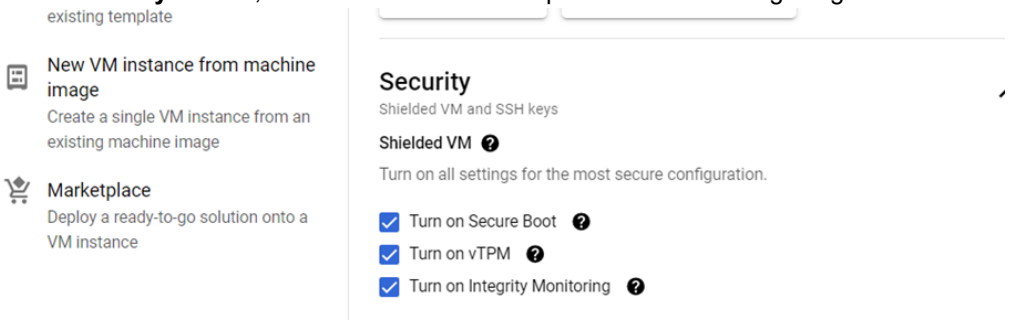


13. Add another hard disk. In the **Create an instance** page, select **Add New Disk** and configure the following.
    - Enter a disk **Name**.
    - Set the **Disk source type** to **Blank disk**.
    - Set the **Disk type** to **Standard persistent disk**.
    - Set the disk **Size** to 100 GB

Note: The minimum recommended disk size is 100 GB.

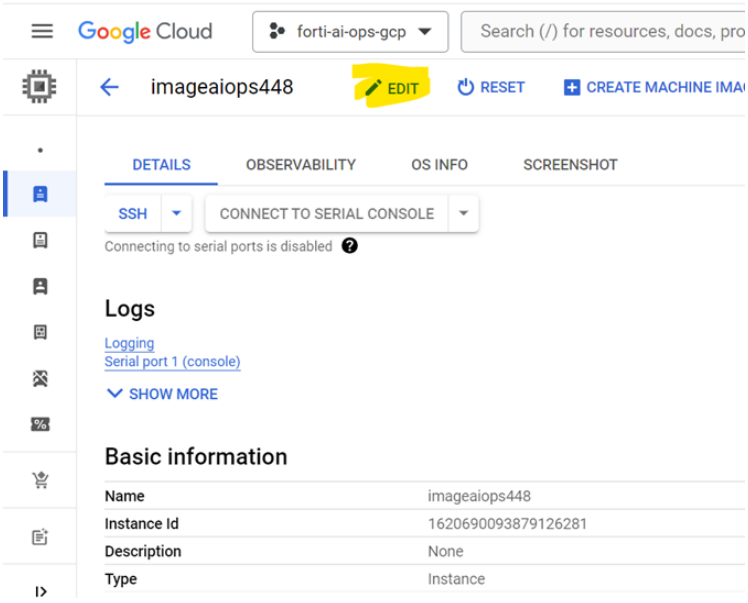


14. Click **Save**.
15. In the **Security** section, enable secure boot as depicted in the following image.

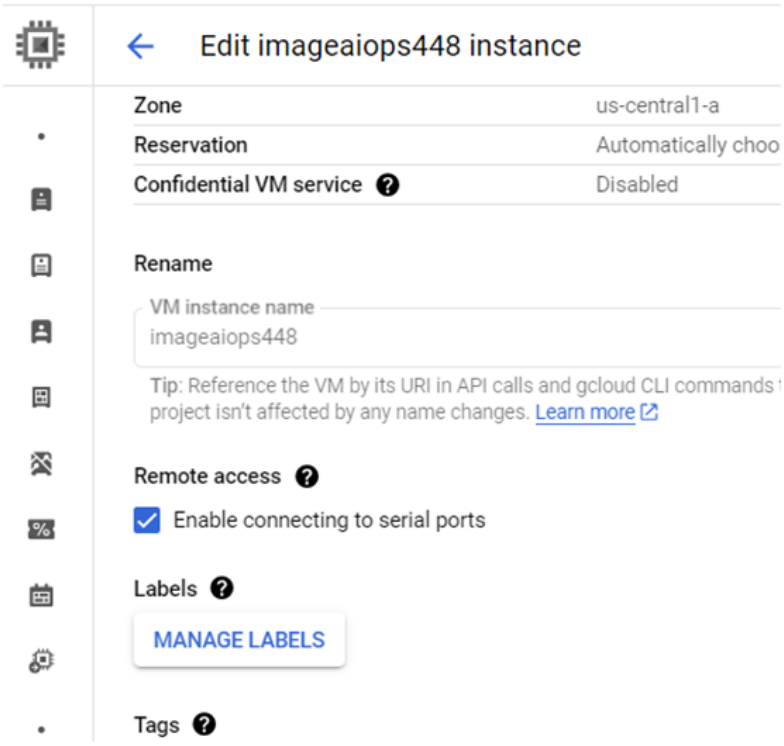


16. Click **Create** to complete installation. The newly created instance is listed in the **VM instances** page. Select the instance and verify that the instance is running with the recommended CPU and machine configurations.

17. After successful installation, enable the serial console.
    - Select the instance in the **VM instances** page.

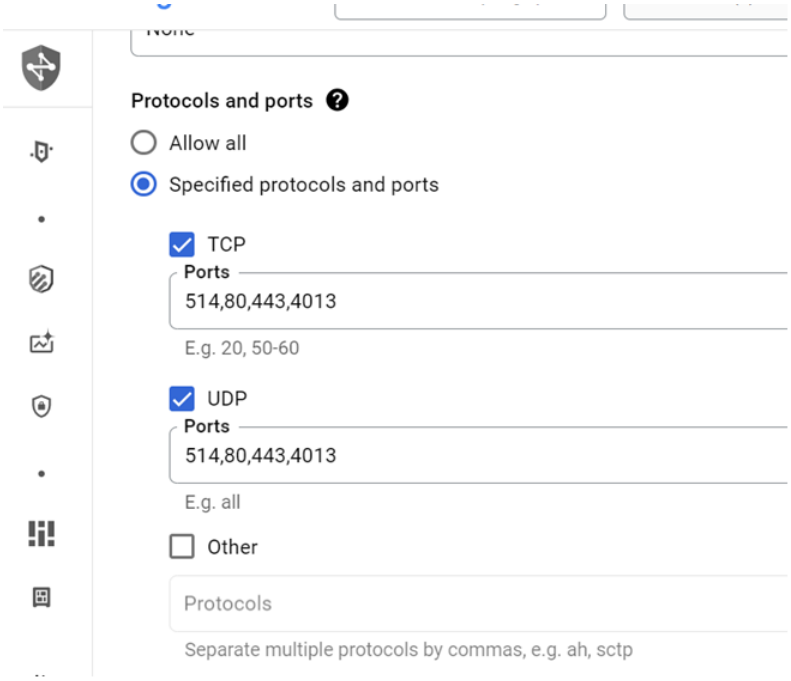


    - Click **Edit** to enable the following TCP and UDP ports.



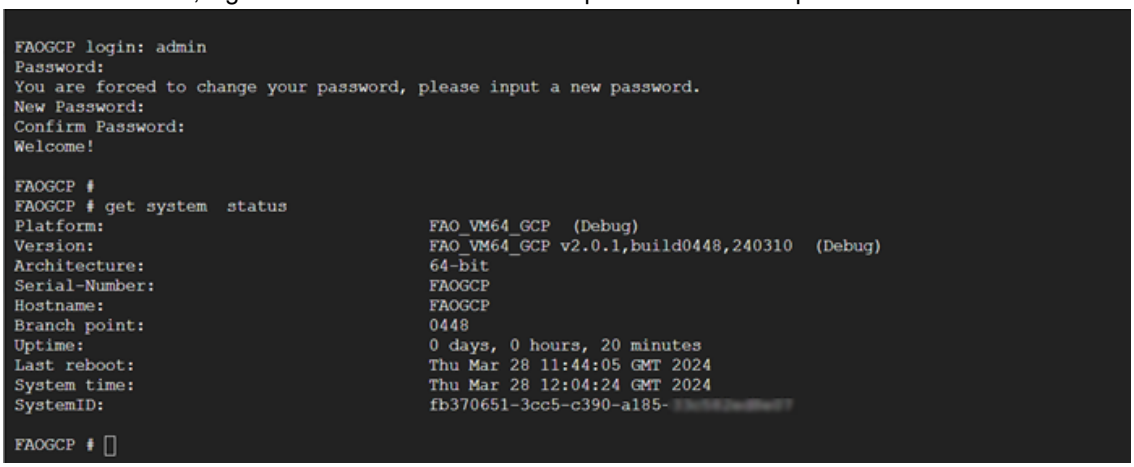
      - 514:514/udp
      - 514:514/tcp
      - 4013:4013/udp
      - 4013:4013/tcp
      - 443:443/tcp

- 80:80/tcp



Note: Ensure that all required TCP and UDP ports are enabled.

18. Connect the VM instance and login.
    - To connect via the Compute Engine console, click **VM Instances** and select the VM instance that you want to connect to. Click **Connect to Serial Console**. See Connect to the Serial Console. In the console interface, login with the user name admin. A password in not required.



    - To connect via the SSH, obtain the public IP address from the VM Instances interface and connect via SSH. The `get system interface` command displays the internal IP address assigned to the

instance.

You can use the external IP address to access the FortiAIOps GUI, *https: <external_IP_address>*.

Amazon Web Services (AWS)

Perform the following steps to deploy FortiAIOps on AWS.

1. Download the file *FAO_VM64_AWS-v2.0.1-[build01xx]-FORTINET.out.aws.zip* from Fortinet
2. Install or gain access to the AWS CLI. See Get started with the AWS CLI.
3. Configure the AWS CLI as per your access requirements. These are some sample values that you must replace with the relevant ones.

```
$ aws configure
   AWS Access Key ID [None]: AKIAIOSFODNN7EXAMPLE
   AWS Secret Access Key [None]: YEXAMPLEKEY
   Default region name [None]: us-west-2
   Default output format [None]: json
```

4. Create *vmimport* role and attach the policy to the IAM user. This operation requires IAM permissions.

```
cat <<EOF > trust-policy.json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": { "Service": "vmie.amazonaws.com" },
         "Action": "sts:AssumeRole",
         "Condition": {
            "StringEquals":{
               "sts:Externalid": "vmimport"
             }
         }
      }
    ]
}
EOF

aws iam create-role --role-name vmimport --assume-role-policy-document
```

```
file://trust-policy.json
```

a. Create a policy for the Amazon S3 bucket and attach it to the AWS IAM user.

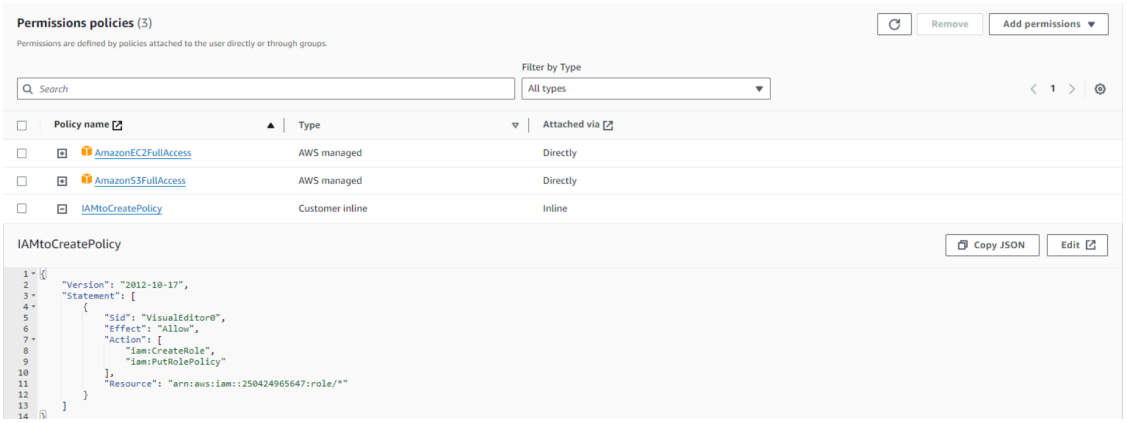
```
cat <<EOF > role-policy.json
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetBucketLocation",
            "s3:GetObject",
            "s3:ListBucket"
         ],
         "Resource":[
            "arn:aws:s3:::$s3BacketName",
            "arn:aws:s3:::$s3BacketName/*"
         ]
      },
      {
        "Effect":"Allow",
        "Action":[
            "ec2:ModifySnapshotAttribute",
            "ec2:CopySnapshot",
            "ec2:RegisterImage",
            "ec2:Describe*"
        ],
        "Resource":"*"
      }
   ]
}
EOF

aws iam put-role-policy --role-name vmimport --policy-name vmimport --
policy-document file://role-policy.json
```

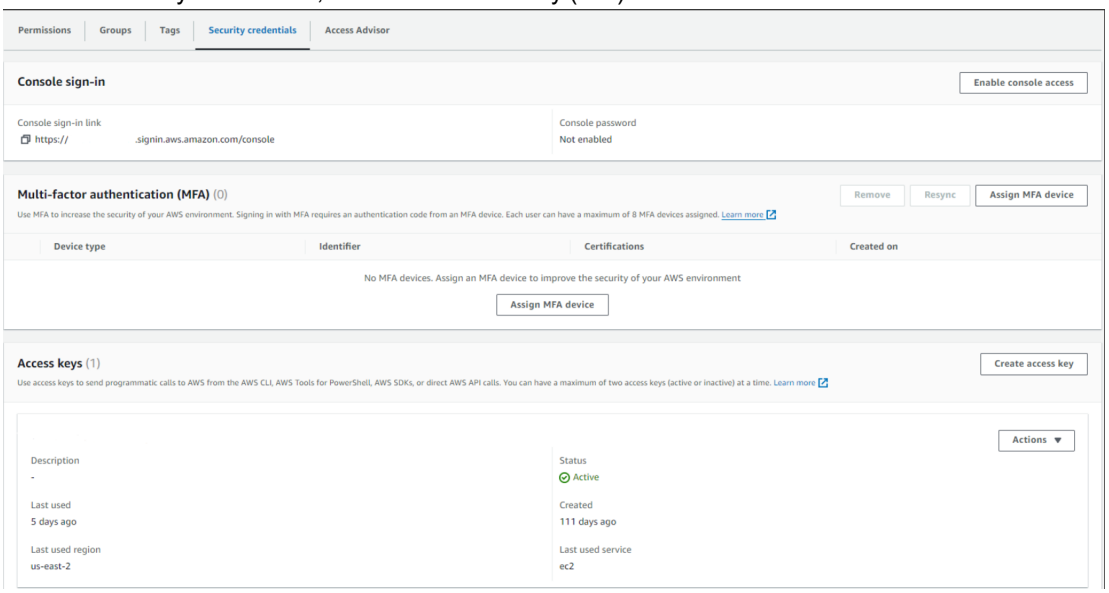
For more information, see Importing a VM as an Image.

5. Enable *Amazon EC2 Full Access* and *Amazon S3 Full Access* permissions.

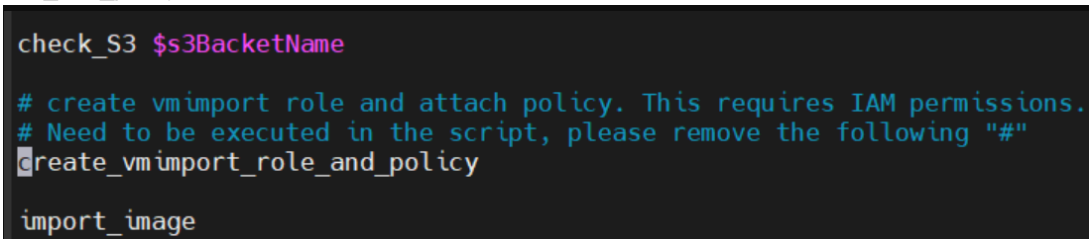
a. Add permission for *create inline policy* in **Permission policies**. Enable write access (*CreateRole*) and user permission management (*PutRolePolicy*). Select **Any** as the policy name in resource selection.



b. For user security credentials, create an access key (CLI) and download the CSV.



c. If you run the `import2awsimg.sh` manually, then un-comment the line 209 in *Creare_vmimport_role_and_policy*.



6. Extract the file *FAO_VM64_AWS-v2.0.1-[build01xx]-FORTINET.out.aws.zip*. Post extraction, you have the VHD file and the import script.

a. VHD - *FAO_VM64_AWS-v2.0.1-[build01xx]-FORTINET.out.vhd*

b. Import script - *import2awsimg.sh*

7. Run the *import2awsimg.sh* script to import the VM.

```
bash -x import2awsimg.sh <imported_image_file> <s3_bucket_name>
```

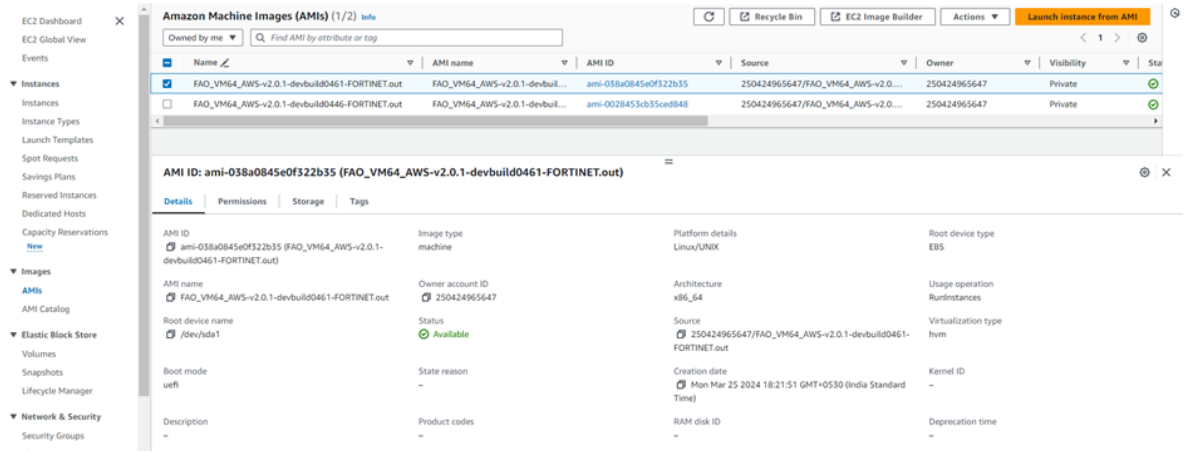
```
-virtual-machine:~/Downloads/test$ bash -x import2awsimg.sh FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out.vhd aiopsqa
+ '[' 2 -gt 1 ']'
+ imageFile=FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out.vhd
+ s3BacketName=aiopsqa
+ '[' '!' -f FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out.vhd ']'
+ check_S3 aiopsqa
+ type aws
+ aws s3 ls s3://aiopsqa
+ '[' 0 -ne 0 ']'
+ import_image
++ basename FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out.vhd
+ imageName=FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out.vhd
+ amiName=FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out
+ echo 'Upload image file to S3..'
Upload image file to S3..
+ aws s3 cp FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out.vhd s3://aiopsqa/FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out.vhd
upload: ./FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out.vhd to s3://aiopsqa/FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out.vhd
+ cat
+ echo 'Start import image file as snapshot..'
Start import image file as snapshot..
++ aws ec2 import-snapshot --description 'Fimg aws' --disk-container file://container.json
++ awk -F '"' '{if($2=="ImportTaskId")print $4}'
+ import_task_id=import-snap-05a78f80bdd0517b1
+ '[' -z import-snap-05a78f80bdd0517b1 ']'
+ echo import-snap-05a78f80bdd0517b1
import-snap-05a78f80bdd0517b1
+ true
++ aws ec2 describe-import-snapshot-tasks --import-task-ids import-snap-05a78f80bdd0517b1
```

```
+ amiId=ami-038a0845e0f322b35
+ '[' -z ami-038a0845e0f322b35 ']'
+ aws ec2 create-tags --resources ami-038a0845e0f322b35 --tags Key=Name,Value=FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out
+ echo 'Register AMI done..'
Register AMI done..
+ echo 'AMI ID: ami-038a0845e0f322b35'
AMI ID: ami-038a0845e0f322b35
+ echo 'AMI NAME: FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out'
AMI NAME: FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out
+ rm -f block_device_mappings.json container.json
```

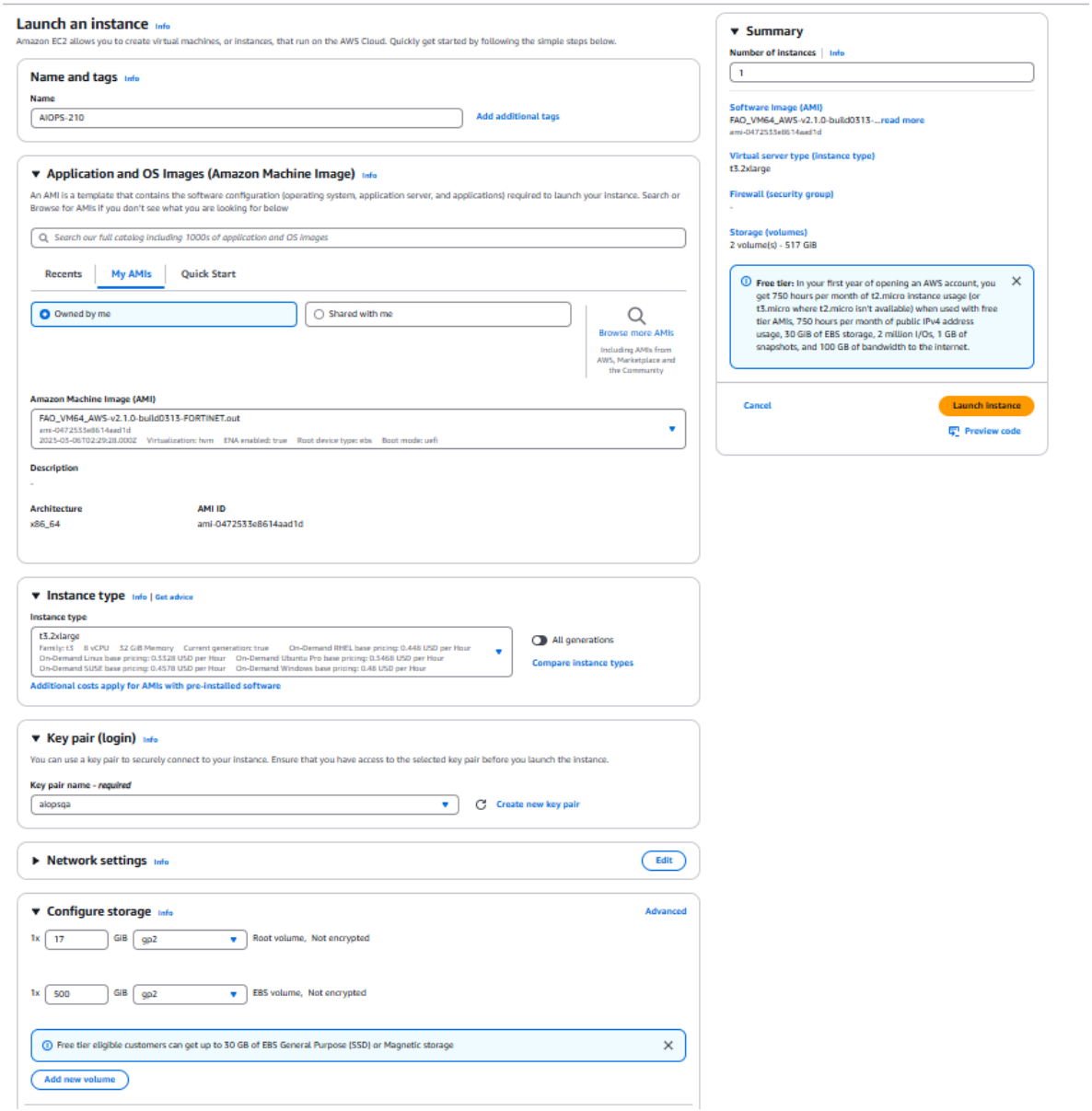
Note:

- To import the VM, you must have read & write permissions to the Amazon bucket, EC2 Snapshot, and image creation, and import permissions.
- Some AWS regions use `/dev/xvda` as the root device name instead of `/dev/sda1`. If you are importing an image into a region that uses `/dev/xvda`, update the script by replacing all instances of `/dev/sda1` with `/dev/xvda`. For example, modify the `block_device_mappings.json` section of the `import2awsimg.sh` by replacing `/dev/sda1` with `/dev/xvda`.

8. Launch an instance from the Amazon Machine Images (AMI). Select **Images > AMI** in the EC2 service interface and select the image that you just imported. Click **Launch instance** from AMI.



9. Add **Name and tags** for the instance, select the **Instance type**, set the **Key pair**, and configure the **Network settings** based on your requirement. Select the required hard disk size in **Configure storage**. The default size of disk storage 2 is10 GB, modify the size as per your requirement. Click **Launch instance**.



10. Obtain the public IP address of the instance from the EC2 service interface and connect via a private key using SSH.

```
FAOAWS [redacted] #
 config                Configure object.
 get                   Get dynamic and system information.
 show                  Show configuration.
 diagnose              Diagnose facility.
 execute               Execute static commands.
 exit                  Exit the CLI.
 full-configuration    Show full configuration.

FAOAWS-AWS-Vinod # show
config system global
    set hostname FAOAWS-AWS-Vinod
end
config system interface
    edit port1
        set type physical
        set mode dhcp
        set allowaccess https ping ssh http
        config ipv6
        end
    next
end
config router static
end
config router static6
end
config system dns
end
config system ntp
end
config system admin
    edit admin
```

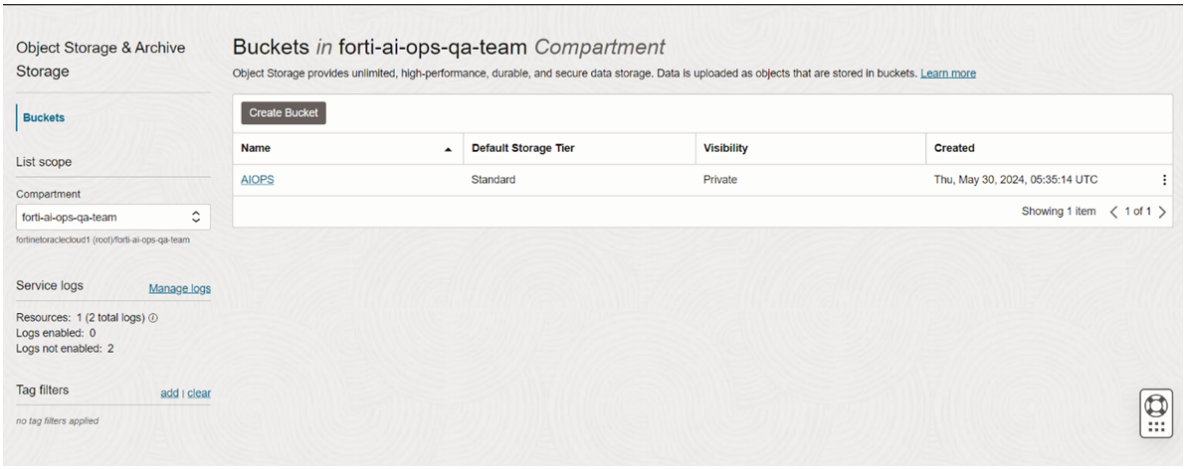
11. From release 3.0.0, by default AWS AIOPS `instance-id` will be the password for the AIOps CLI/GUI. After login through CLI/GUI you will prompt to change the password.

Oracle Cloud Infrastructure (OCI)

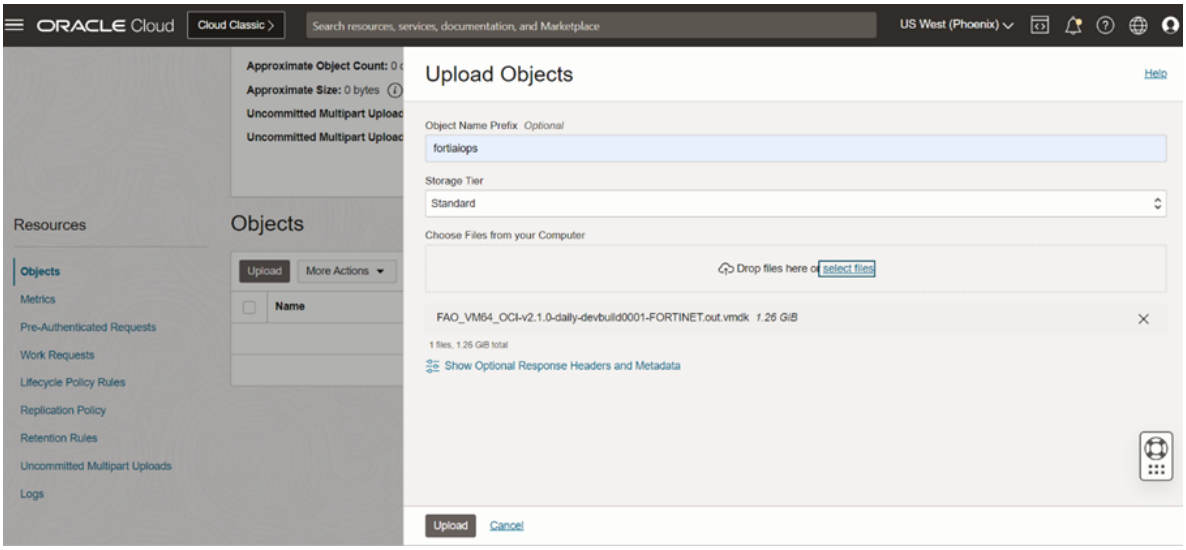
Perform the following steps to deploy FortiAIOps on OCI, for more information, see OCI Documentation.

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*.

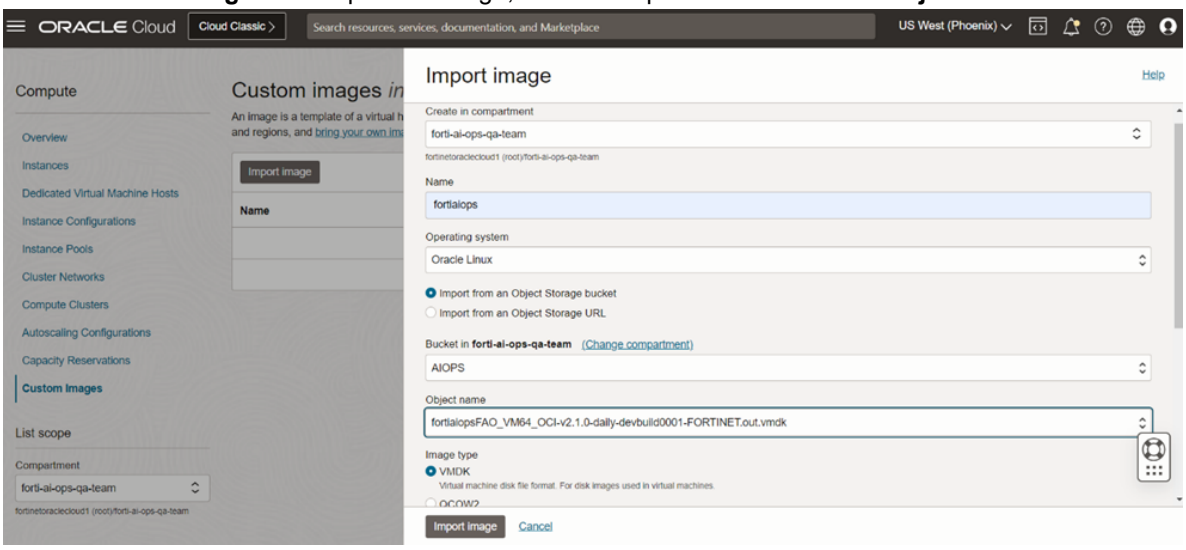
4. Click **Create** or **Confirm**.



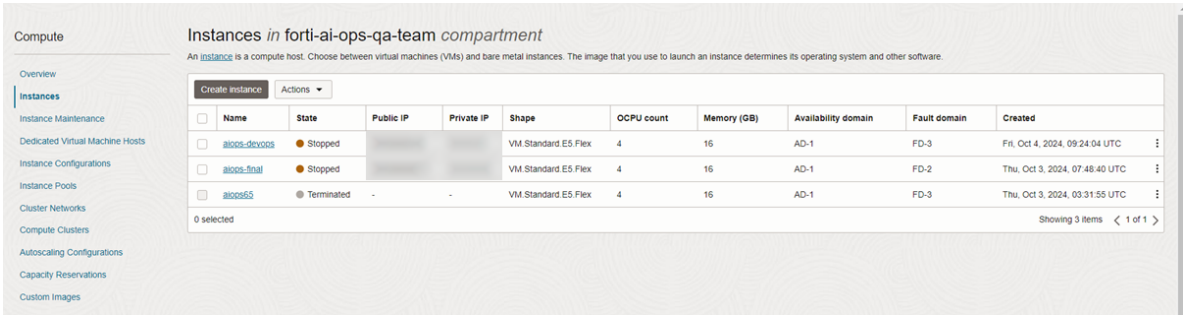
5. Extract the file *FAO_VM64_OCI-v2.1.0-[build0xxx].out.oci.zip* to obtain *FAO_VM64_OCI-v2.1.0-[build0xxx].vmdk*. Upload the *.vmdk* file in the bucket.



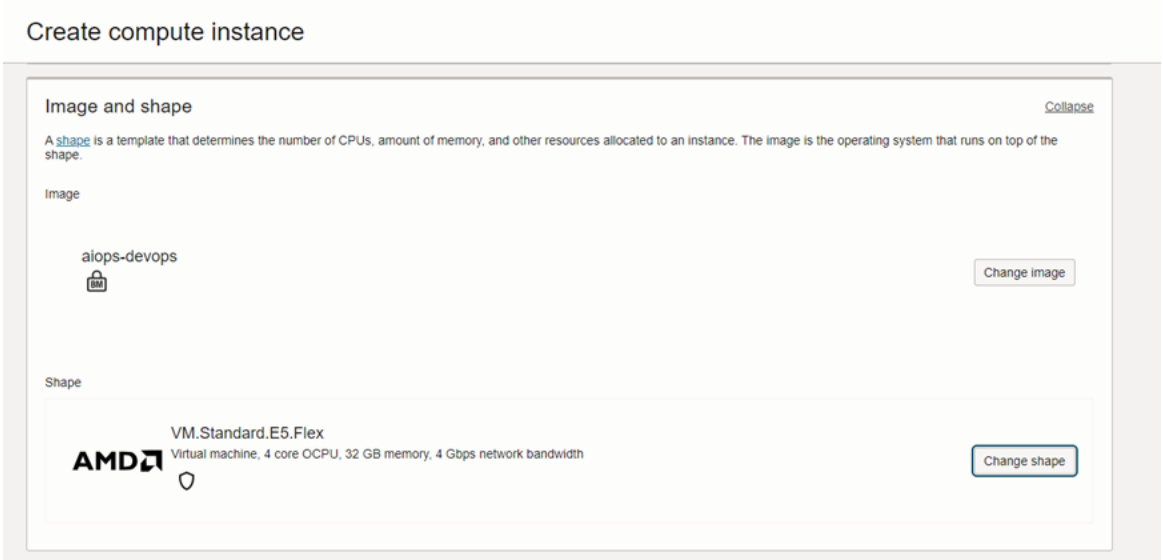
6. Select **Custom Images** and import the image; select the uploaded VMDK file in **Object Name**.



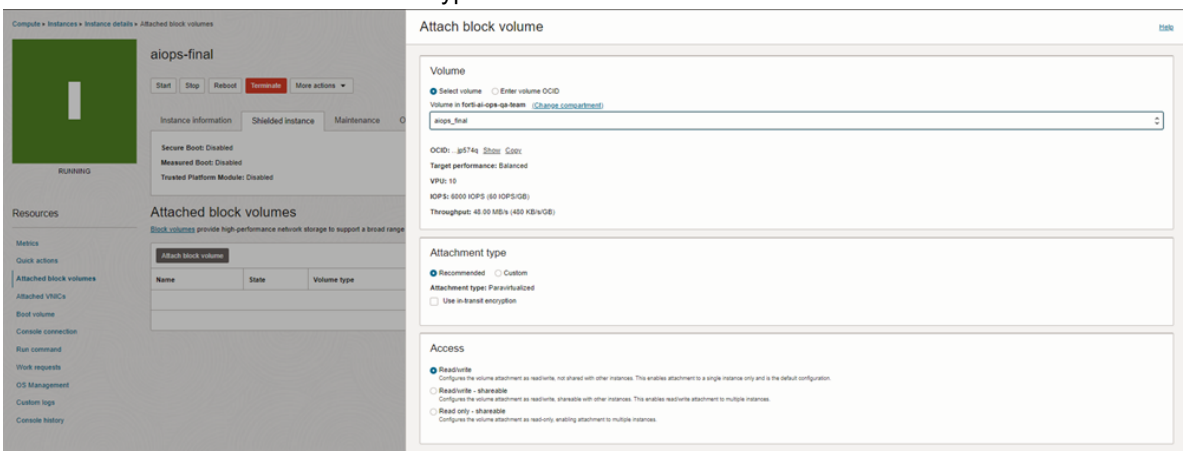
7. Search for the **Block Volume Service** and create block volume with 500 GB using the **Custom** option.
8. Navigate to **Compute Service** in the OCI portal and create an instance with the uploaded custom image.



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).
   Wait for the import process to complete. This may take 6-10 minutes (approximately).



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**.



12. Reboot the instance after attaching the volume.

Deploying FortiAIOps on Hardware Platforms

FortiAIOps can be deployed on the following hardware platform:

- FortiAIOps 500G (FAO-500G)

Deploying FortiAIOps 500G (FAO-500G)

The FAO-500G hardware platform comes with FortiAIOps pre-installed. Perform the following steps to deploy and configure the device.

- Initial Configuration
- Accessing the GUI

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 same as the GUI password. The default username for logging into GUI is admin and there is no password.

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`

For a complete list of supported CLI commands, see Command Line Interface (CLI) Reference.

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. Enter the username as admin. There is no password for the initial login.

Command Line Interface (CLI) Reference

The following commands are supported for FortiAIOps.

- Configuration Commands
- Show Commands
- Diagnostic Commands
- Management Commands
- System Information
- Diagnostic Tool Commands

Configuration Commands

The following commands are available to configure FortiAIOps.

Command	Parameters	Description
config system interface	edit <interface port>	Edit the interface port and enter the port setting mode in the CLI.
	?	Displays the various parameters available for this command.
	abort	Aborts the port setting mode and exits.
	next	Returns to the interface configuration mode.
	set mode <static|DHCP>	Configure the port IP address mode; static or DHCP.
	set ip <IP/netmask>	Configure the port IP address (static).
	set allowaccess <ssh|https|http|ping>	Configure the admin access type; SSH, THHP, HTTPS, Ping, or SNMP.
	get	Obtain the system information.
	show	Displays the current interface configuration details.

Command	Parameters	Description
	`end`	Exit the port configuration mode; the configuration changes then take effect.
`config system`	`admin`	Configures admin users. `edit admin` - Edit admin user details. `set password` - Set the admin user password.
	`dns`	Configures DNS and enters the DNS configuration mode. `set primary` - Configures the primary DNS server.
	`global`	Configures global settings and enters the global configuration mode.
	`interface`	Configures the system interface.
	`ntp`	Configures system NTP information. • `set ntpsync` - Enable/disable the system time by synchronizing with the NTP server. • `set ntpserver` - Configure the IP address or hostname of the NTP servers (up to 10).

Command	Parameters	Description

	`lldp-transmission`	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>`

Show Commands

The following commands can be used for viewing configuration information.

Command	Parameters	Description
`show`		Displays bootstrap configuration.
`show full-configuration`		Displays all configuration (includes defaults).

Diagnostic Commands

The following commands are used to diagnose and troubleshoot issues.

Command	Parameters	Description
`diagnose`	`?`	Displays the various parameters available for this command.
	`hardware ?`	Displays the various parameters available for this command.
	`hardware deviceinfo disk`	Displays information of all disks.
	`hardware deviceinfo nic`	Display the available list of NICs.

Command	Parameters	Description
	`hardware deviceinfo <nic name>`	Displays information of a specific NIC.
	`hardware deviceinfo tpm`	Displays Trusted Platform Module (TPM) module information.
	`hardware lspci`	Displays the PCI parameters.
	`hardware lspci tree`	Displays PCI bus tree.
	`hardware lspci verbose`	Displays detailed information about all devices.
	`hardware sysinfo ?`	Displays the various parameters available for this command.
	`hardware sysinfo cpu`	Displays detailed information for all installed CPU(s).
	`hardware sysinfo interrupts`	Displays details of system interruptions.
	`hardware sysinfo iomem`	Displays the memory map of I/O ports.
	`hardware sysinfo ioports`	Display the address list of I/O ports.
	`hardware sysinfo memory`	Displays the system memory details.
	`hardware sysinfo mtrr`	Displays the memory type range register.
	`hardware sysinfo slab`	Displays the memory allocation information.
`diagnose system`	`top all`	Displays the top threads information.
	`top cpu`	Displays processes with the highest CPU usage at the top of the list.
	`load`	Displays system uptime and load information.
	`process <cpu | mem> <num>`	Displays the processes sorted by specified criteria (default 10 processes).

Command	Parameters	Description
	`fsck harddisk`	Check and repair the file system, then reboot the system.
	`raid hwinfo`	Displays raid controller information.
	`raid hwinfodetail`	Displays detailed raid controller information.
	`raid migrate`	Migrate to a new disk.
	`raid rebuild`	Rebuild the existing disk.
	`disk attributes`	Displays vendor specific Self-Monitoring, Analysis, and Reporting Technology (SMART) attributes.
	`disk errors`	Displays SMART error logs.
	`disk health`	Displays SMART health status.
	`disk info`	Displays SMART information.

Management Commands

The following enable some management and other operations in FortiAIOps.

Command	Parameters	Description
`execute`	`?`	Displays the various parameters available for this command.
	`date <YYYY-MM-DD>`	Set the date in the *YYYY-MM-DD* format.
	`time <HH:MM:SS>`	Set the time in the *HH:MM:SS* format.
	`factoryreset reboot`	Reset to the factory default settings and reboot the system.
	`factoryreset shutdown`	Reset to the factory default settings and shutdown the system.
	`formatlogdisk`	Format the log disk.
	`ping <destination>`	Ping the host name or IPv4 address.

Command	Parameters	Description
	`traceroute <destination>`	Traceroute of the host name or IPV4 address.
	`reboot`	Reboot the system.
	`shutdown`	Shut down the device.
	`backup config ftp <path> <server fqdn|ipaddr>[:port] [ftp_user] [ftp_passwd]`	Creates a remote backup of the configuration file from an FTP server.
	`backup config tftp <filename> <server fqdn|ipaddr>`	Creates a remote backup of the configuration file from a TFTP server.
	`restore image ftp <filename string> <ftp server>[:port] [ftp_user] [ftp_passwd]`	Restores the firmware image from an FTP server using specific details.
	`restore image tftp <filename string> <tftp server>`	Restores the firmware image from a TFTP server.
	`dns-no-domain`	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>`
	`sensor list`	Displays sensor list and status from IPMI.
	`format disk 0`	Create RAID 0 and format disk.
	`format disk 1`	Create RAID 1 and format disk.
	`format disk 5`	Create RAID 5 and format disk.
	`format disk 10`	Create RAID 10 and format disk.

System Information

The following commands information related to the system configurations.

Command	Parameters	Description
get system	?	Displays the various parameters available for this command.
	status	Displays system status, such as, version, serial number, BIOS details, time stamp, hostname, and so on.
	admin	Displays the configuration details of the admin users.
	admin <username>	Displays the configuration details of a specific admin user.
	dns	Displays the DNS configuration.
	global	Displays the configuration details of global attributes.
	interface	Displays the interface details, status, and IP address.
	interface <port>	Displays the port details, status, and IP address.
	ntp	Displays the configuration details and status of NTP server.

Diagnostic Tool Commands

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.

Dashboard

The FortiAIOps dashboard provides a graphical overview of network elements, resource usage, AI insights, and Service Assurance.

The interactive graphs and charts allow you to navigate into detailed views of network statistics for analytical and monitoring purpose.

The data on this dashboard is automatically refreshed every 60 seconds; the following options are available to manage the auto-refresh feature for this page.

- Click to manually refresh data.
- Click to pause the auto-refresh.
- Click to resume the auto-refresh.
- Select the time range from the drop-down. Choose from 10 minutes, 1 hour, 4 hours, 6 hours, 1 day, 1 week.

Adding a Widget to the Dashboard

You can add widgets based on your requirements to the dashboards.

To add a widget to the dashboard:

1. Select the dashboard you want to modify.
2. Click **Add Widget** to add required widgets from the widget library.
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 Managing 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.

Summary

This dashboard provides visual summary of key system information, network elements, and resource usage.

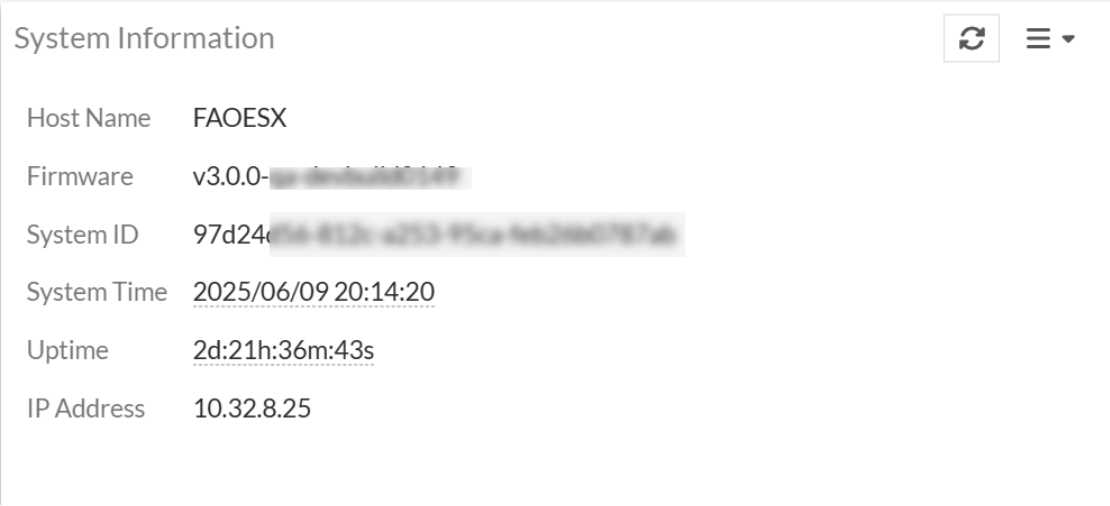
The following charts are available:

- System Information
- System Resource Summary
- Summary
- Overall Network Health
- Top 5 Problematic Devices
- Impacted Clients Trend
- FortiGates
- FortiGate Events

- FortiGates CPU Usage and FortiGates Memory Usage
- High Latency FortiGates

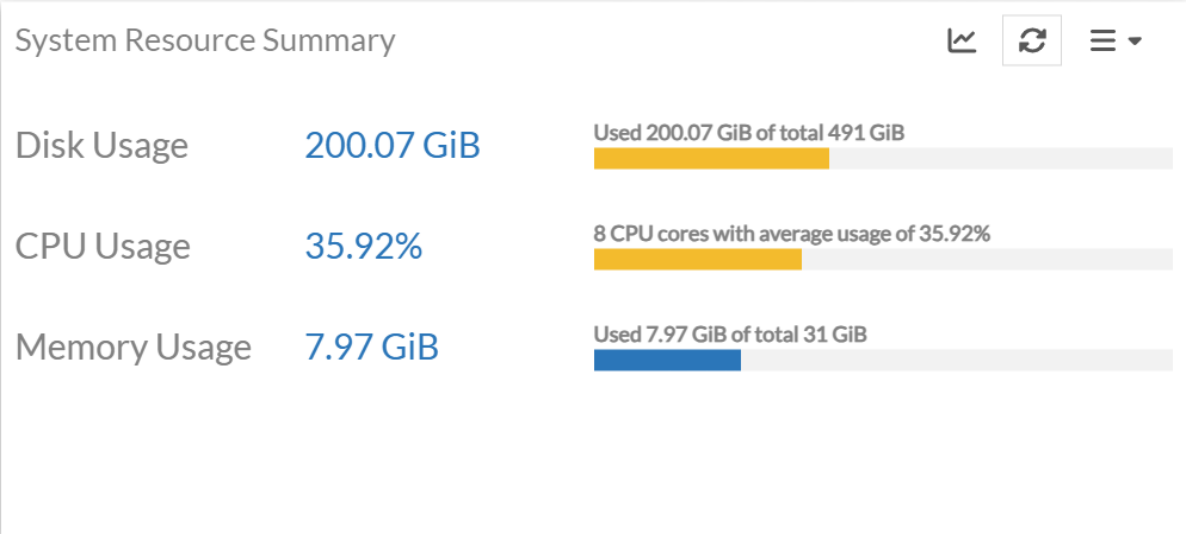
System Information

This widget provides generic information about the FortiAIOps such as the host name, firmware version, system ID, current system time, uptime, and the IP address.



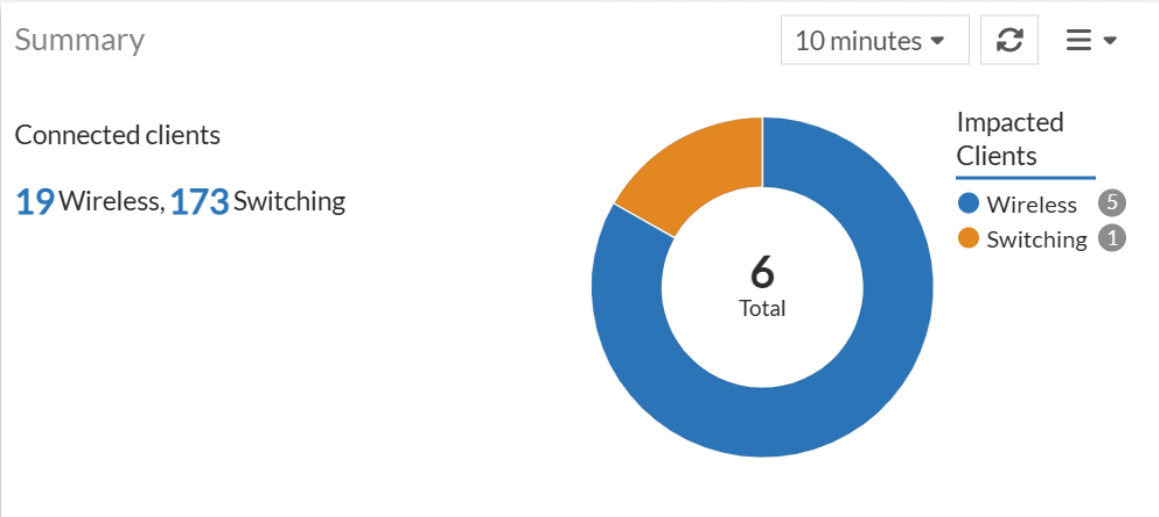
System Resource Summary

This widget provides an overview of the current system resource usage for FortiAIOps. The statistics include the total available and used disk space (HDD and SSD), the number of CPU cores used and the average usage, and total available and used memory. Click on the trends icon to view the resource usage summary; filter 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**.The minimum, maximum, and average values are displayed when a time interval of more than 6 hours is selected.



Summary

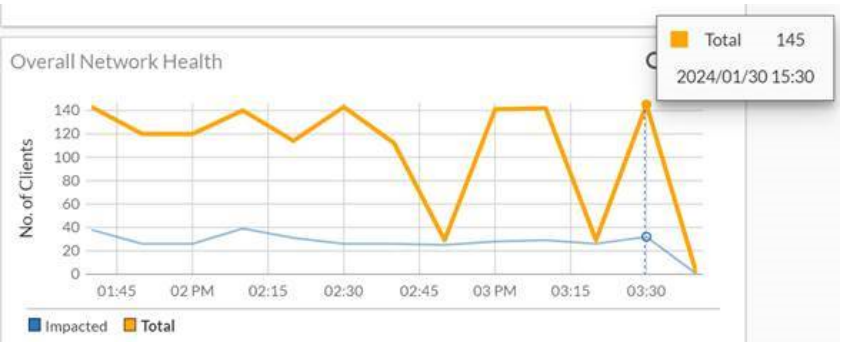
This chart displays details of the various devices in your network that are associated with impacted clients, that include the wireless, switching, and WAN clients. For more information, see Impacted Devices.

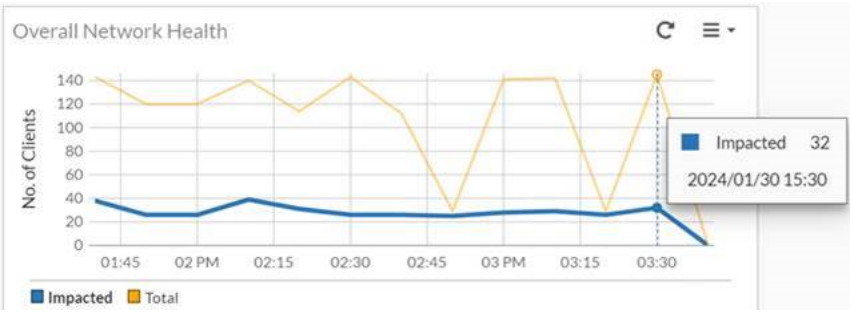


Overall Network Health

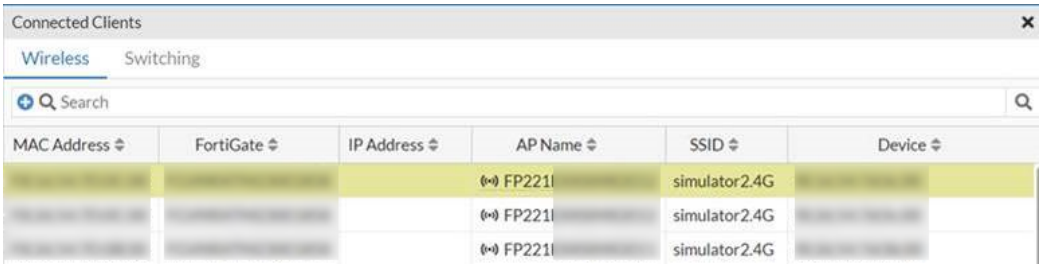
This panel displays the overall client count trends and health status of all wireless, switching, and WAN clients connected to your network, at specific intervals of 10 minutes. You can view the total number of clients in your network and the number of impacted clients at a given point in time.

Hover over the line to view the total number of clients and the line to view the number of impacted clients. In this example, at 03.30 hours, a total of 145 clients were present in the network of which 32 clients are impacted.



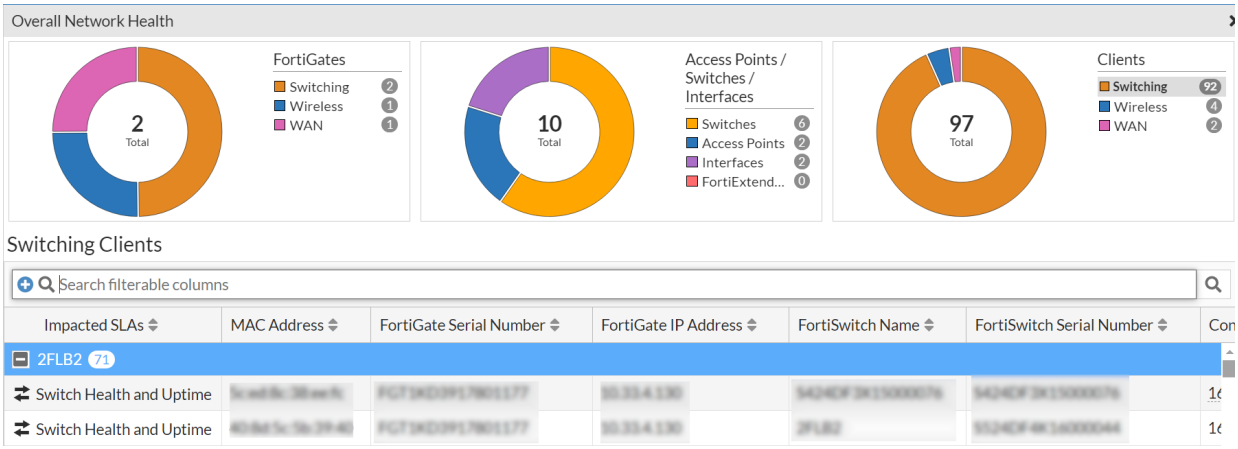


Click on any given time interval for total clients to view the **Connected Clients** panel. The data displayed in tabular format in all the monitor dashboard pages is filterable based on columns, you can group data by a specific column or filter data for specific values.



Click the **AP Name** to view the FortiAP details and the operational status of the radios.

Click on any given time interval for total clients to view the **Overall Network Health** panel. This page displays details of the various devices in your network that are associated with impacted clients. The number of devices are listed for each category, you can click on any of these or click on the respective section in the donut chart to view details. The data is displayed in the following three panels. Refer to Impacted Devices for more descriptions.



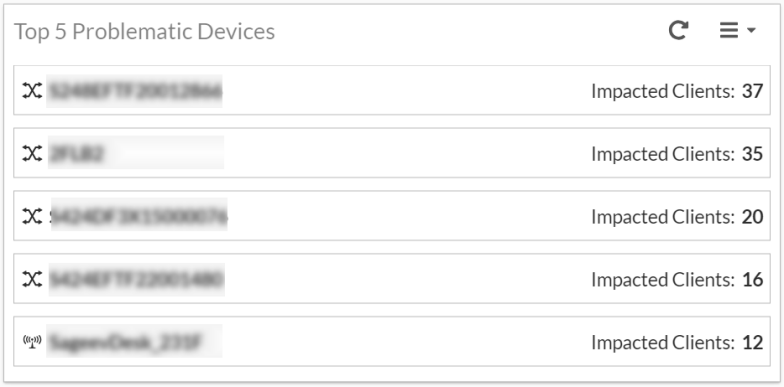
FortiGates - Displays the number of deployed FortiGate controllers with impacted wireless, switching, and WAN clients.

- **Access Points/ Switches/ Interfaces/FortiExtenders** - Displays the number of devices, that is, APs, interfaces, FortiExtenders, and switches with impacted clients.
- **Clients** - Displays the number of impacted clients for the wireless, switching, and WAN.

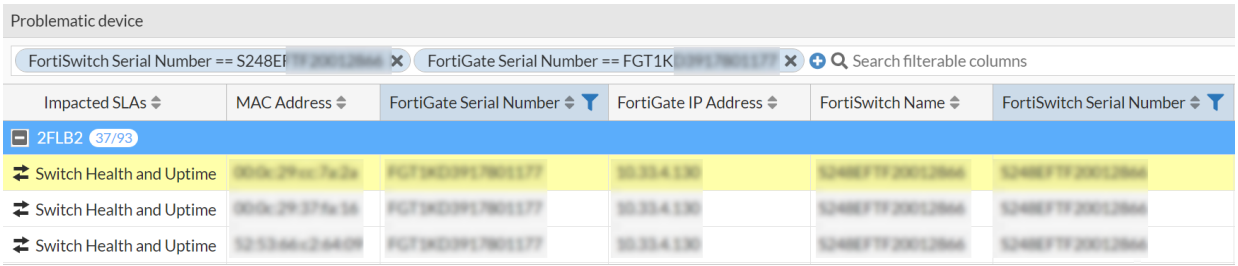
Click on the impacted SLA to view the device topology.

Top 5 Problematic Devices

This panel displays the 5 devices with the highest number of impacted clients. The devices displayed here can be FortiAPs, FortiSwitches, FortiExtenders, and/or interfaces. The device name and the number of associated clients that are impacted are displayed in descending order.

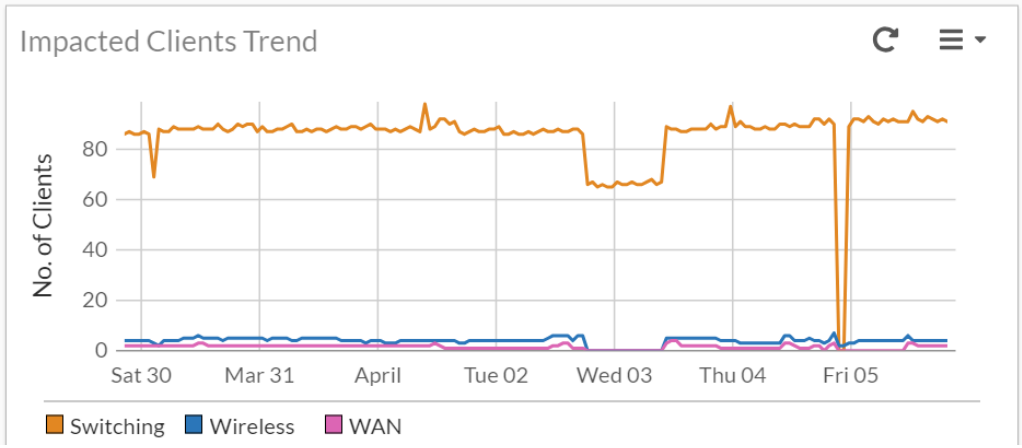


Click on the device name to view details.

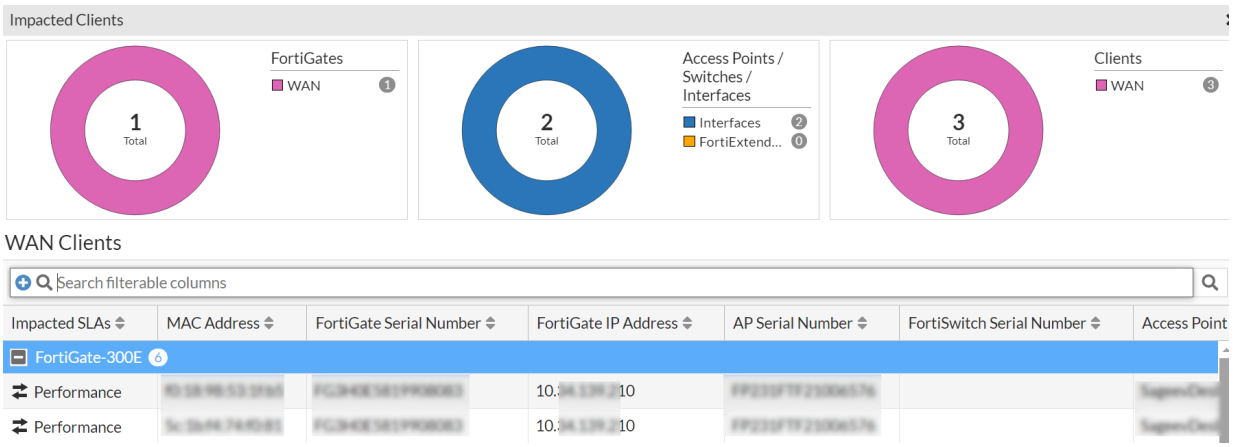


Impacted Clients Trend

The **Impacted Clients Trend** panel displays data trends for the total number of impacted clients for switching, wireless, and WAN, over a period of time.



Click on any given time interval for the impacted clients to view the **Impacted Clients** page. This page displays details of the various devices in your network that are associated with impacted clients. The following image depicts an example of the impacted WAN clients.



The data is displayed in the following three panels. For more information on the data and fields displayed on this page, see Impacted Devices.

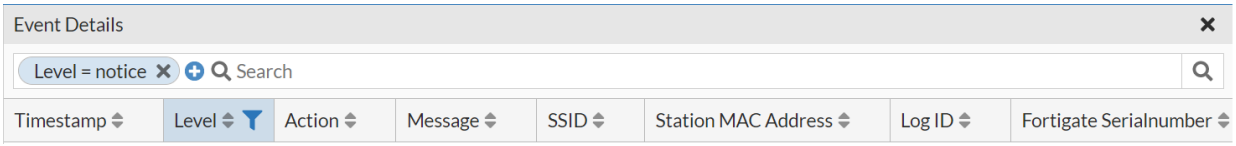
- **FortiGates** - Displays the number of deployed FortiGate controllers with impacted wireless, switching, and WAN clients.
- **Access Points/ Switches/ Interfaces/FortiExtenders** - Displays the number of devices, that is, APs, interfaces, FortiExtenders, and switches with impacted clients.
- **Clients** - Displays the number of impacted clients for the wireless, switching, and WAN.

FortiGates

Displays the total number of FortiGate controllers in your network and their status (*Online*/*Offline*). Click on the chart to view more details of the controllers. For more information, see Managing FortiGates.

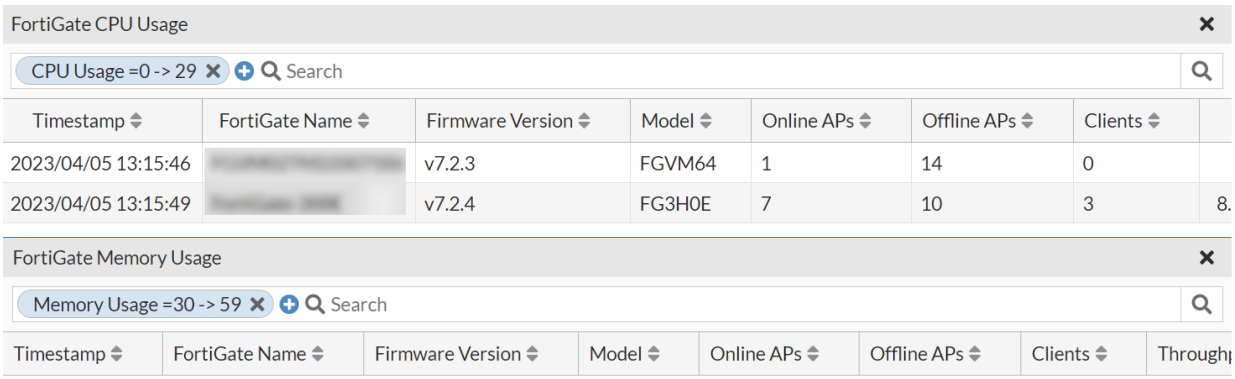
FortiGate Events

Displays the FortiGate events at a given time 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).



FortiGates CPU Usage and FortiGates Memory Usage

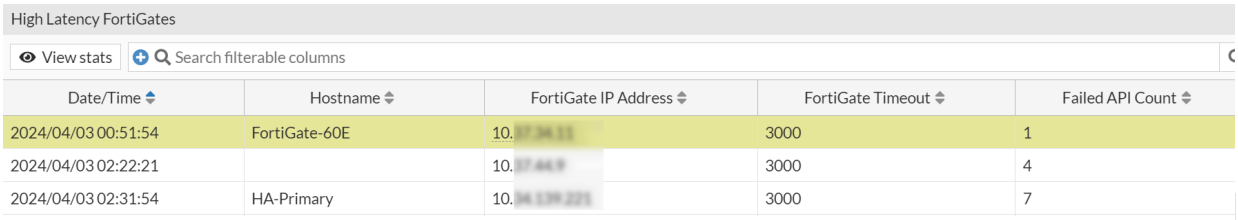
Displays the real-time FotiGate CPU and memory usage at a given time and categorizes it as *Low*, *Medium*, *High*, and *Critical*. You can select the period to view the resource usage (10 or 30 minutes, 1 or 12 hours, or 1 day). Click on the graph to view the details.



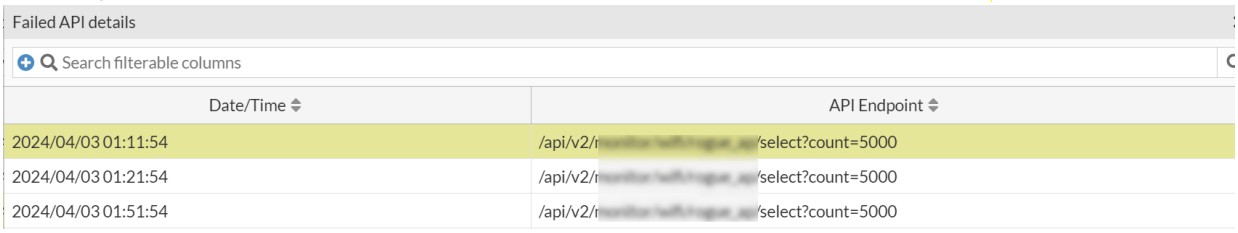
High Latency FortiGates

This widget displays the FortiGates with high latency determined based on the timed out API request. Hover over the graph to view the number of FortiGates with high latency at a given period of time and click on the graph to view the details of the FortiGates. You can select the period to view the FortiGates (10 or 30 minutes, 1 or 12 hours, or 1 day).

Note: This is not a default widget. To add it to your dashboard, click **Add Widget** and select it from the **Manage Dashboard Widgets** pane.



Select a particular FortiGate and click **View stats** to view the details of the timed out APIs.



Wireless

The **Wireless** page gives you a complete picture of your wireless network. It displays key metrics such as the status, CPU usage, and memory usage of your Access Points, along with WIDS events for a selected time period. It also provides wireless client insights, a summary of rogue APs, and details of the top impacted applications and a full list of applications by usage.

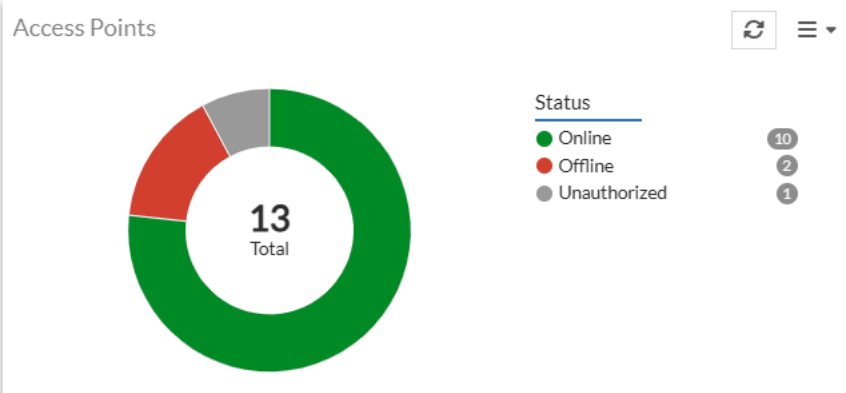
The following charts are available in the **Wireless** page:

- Access Points
- WIDS Events

- Access Points CPU Usage
- Access Points Memory Usage
- Wireless
- Top 3 Impacted Apps
- Wireless Insights
- Rogue APs
- Applications by Usage

Access Points

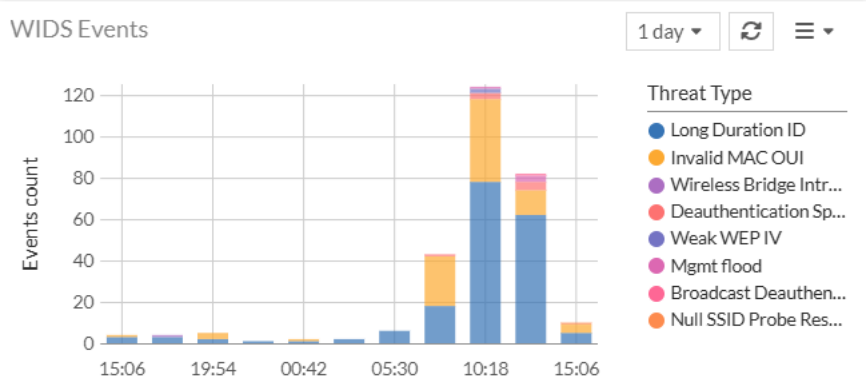
This chart displays the total number of access points in your network and their status (Online, Offine, Waiting for Authorization, or Unknown).



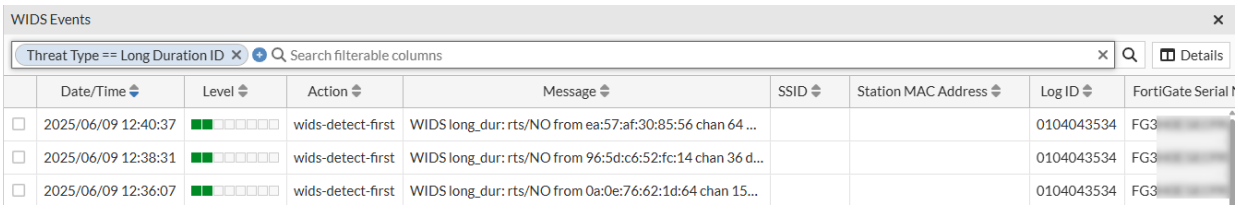
Click the chart for detailed information about the Access Points in use. For more information, see Access Points.

WIDS Events

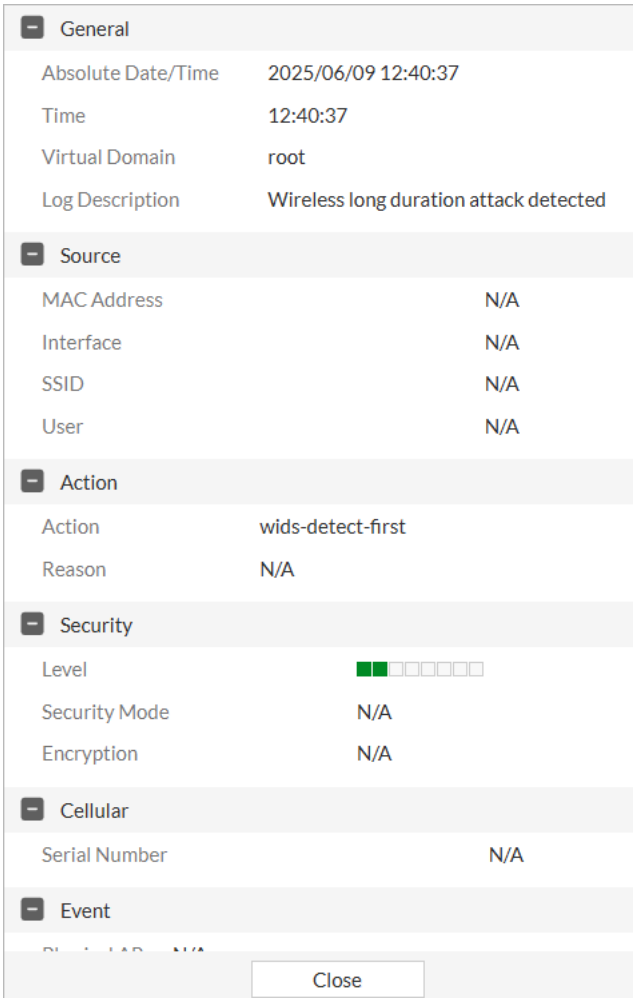
This chart displays the threat type and the number of events for each type of threat.



Click on a Threat Type to open WIDS Events pane with details for the filtered threat type.

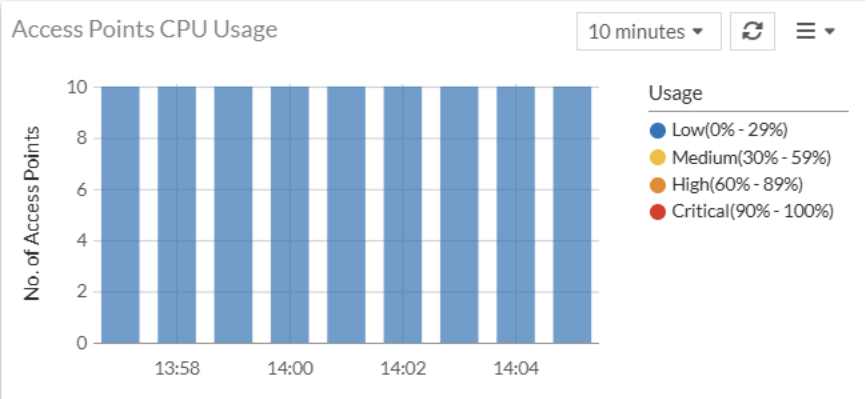


Double-click on an event to view more details

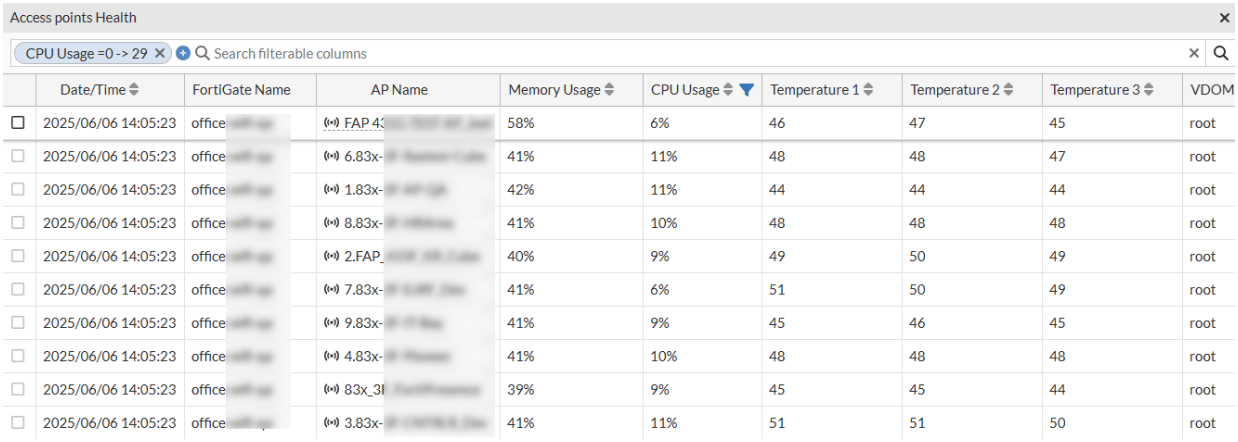


Access Points CPU Usage

This chart displays the real-time FortiAP CPU 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).

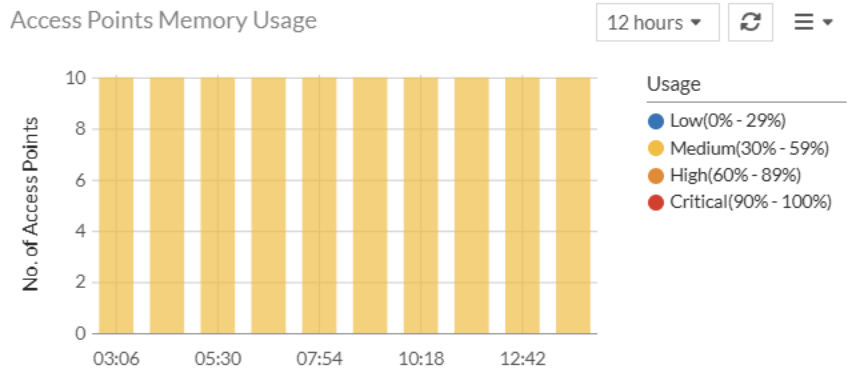


Click on the CPU usage chart to view more details.

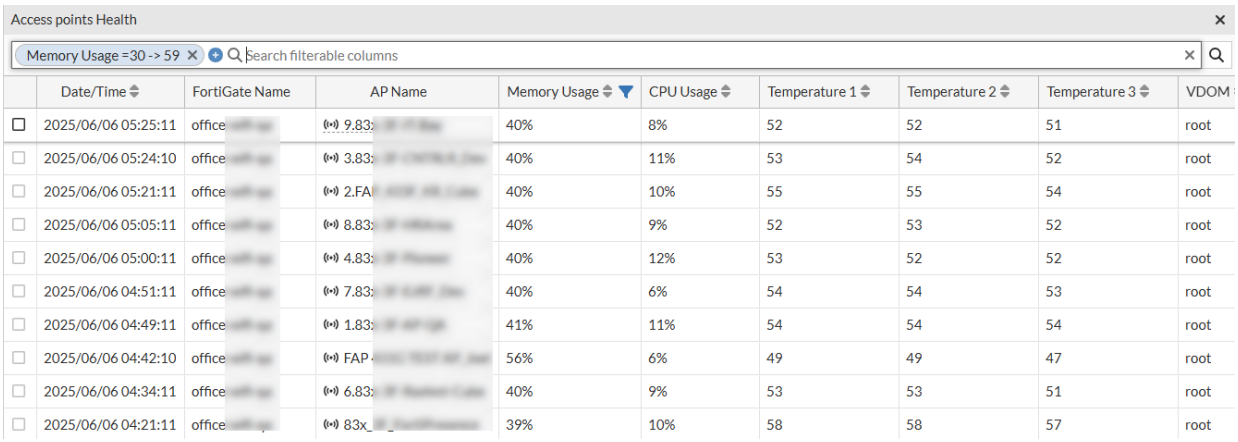


Access Points Memory Usage

This chart shows real-time FortiAP memory usage, categorized into Low, Medium, High, and Critical levels. You can select the viewing period to see resource usage over 10 or 30 minutes, 1 or 12 hours, or 1 day.

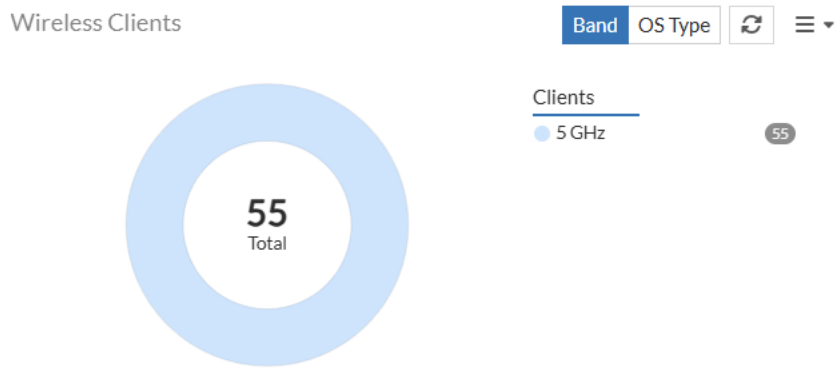


Click on the memory chart to view more details.



Wireless Clients

This chart displays the total number of connected clients with their Band categorization of 2.4GHz, 5GHz, and 6GHz. This panel also provides representation for clients based on the OS Type.

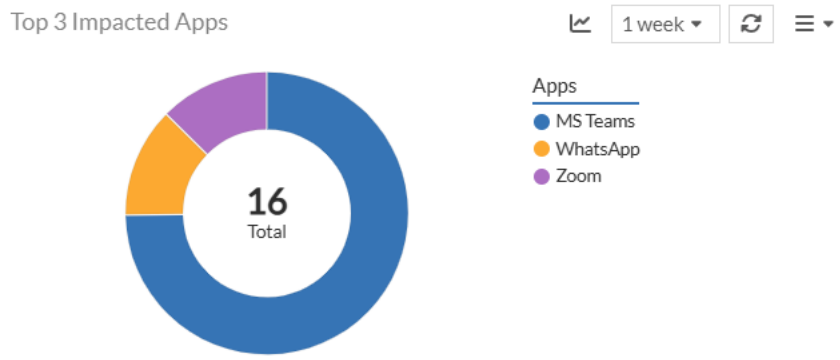


Click on the chart to view more details. For more information, see Wireless Clients.

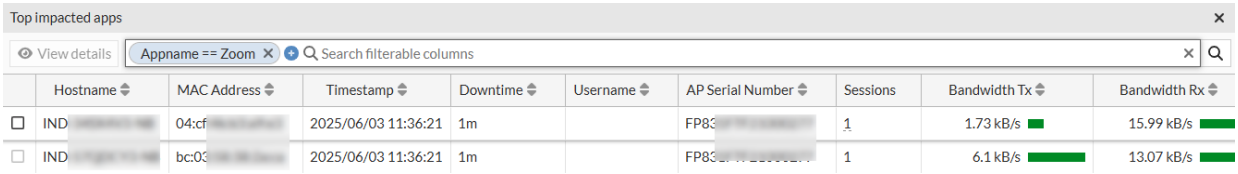
Top 3 Impacted Apps

This panel displays the 3 conference applications running on client devices that are most impacted. These applications are Microsoft Teams calls, Google Meet, Zoom, WhatsApp audio and video call, and Apple FaceTime.

Note: This is not a default widget. To add it to your dashboard, click **Add Widget** and select it from the **Manage Dashboard Widgets** pane.



To view details, click on the name of the application on the chart or the panel.

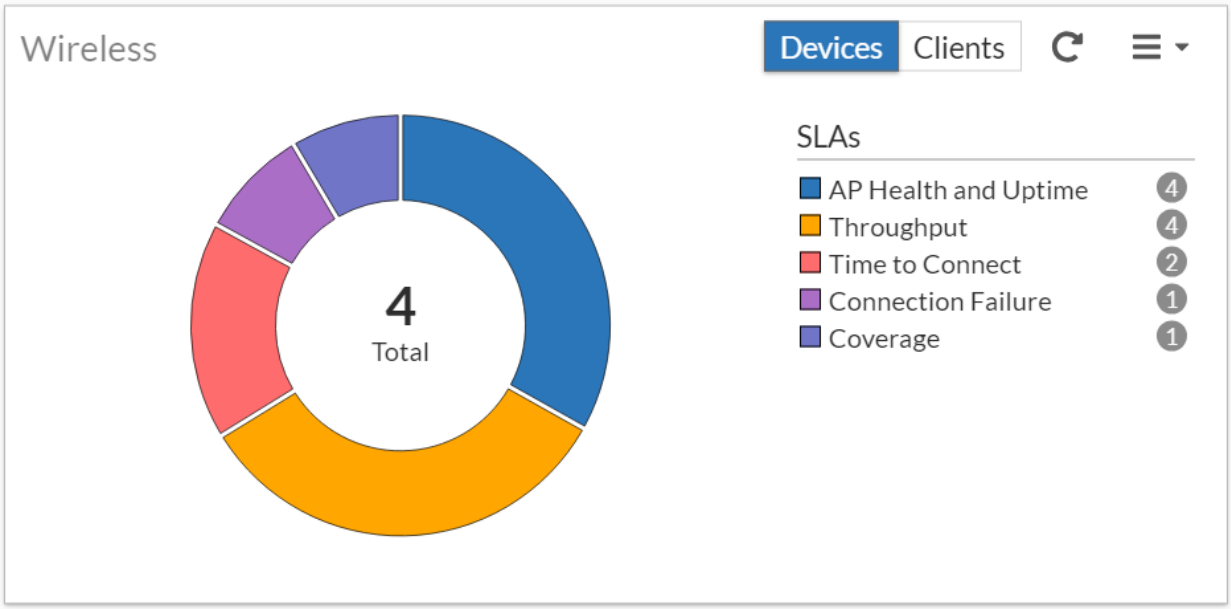


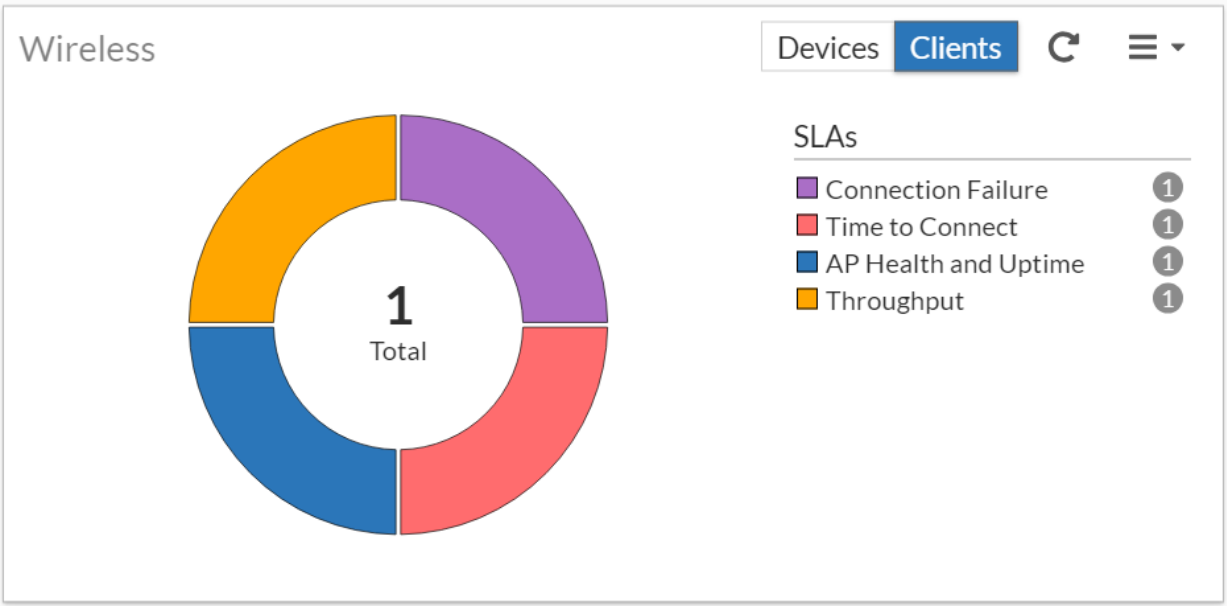
The applications are classified as impacted based on the downtime it experiences during various sessions in the selected time period. You can view the downtime for the latest session and the number of sessions. Furthermore, click on the number of sessions to view the downtime and other details for each session.

Note: For accurate applications related data in this panel, renew the FortiGuard license for general updates, including application control signatures for application detection.

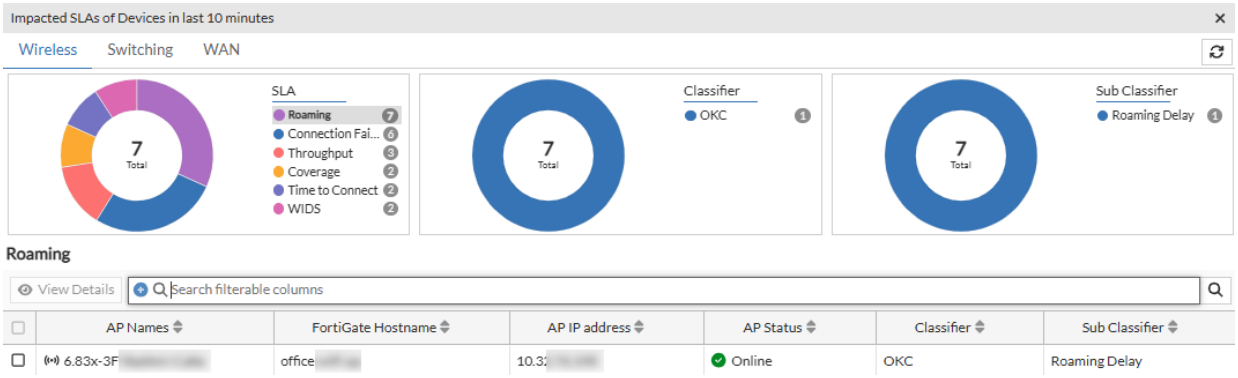
Wireless Insights

The **Wireless** panel displays the details of impacted SLAs with the associated device and client details. The **Clients** view displays the impacted client count and the **Devices** view displays the impacted AP count.

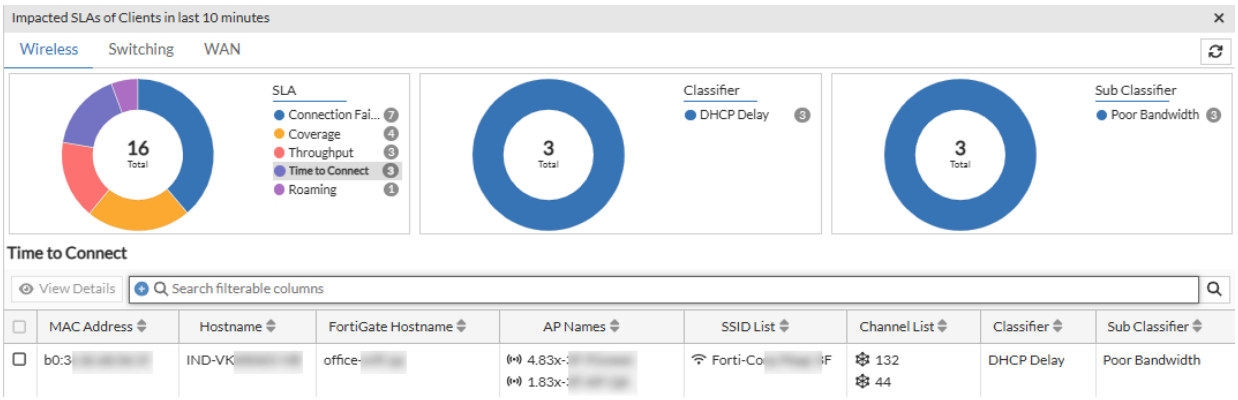




The impacted SLAs are detected and reported by FortiAIOps with device and client details. The issues reported are categorized based on classifiers and sub-classifiers, with suggested remedial measures to curtail the SLA breaches and enhance network performance. The data displayed in this panel is for the time period set in the dashboard. If you select the **Devices** view in the Wireless panel and click on any SLA in the impacted SLAs list or click on the bar in the chart, the impacted devices details such as, AP name, AP serial number, AP IP address, AP status (online/offline) and state, FortiGate host name and serial number, and classifier and sub-classifier are displayed.



If you select the **Clients** view in the Wireless panel and click on any SLA in the impacted SLAs list or click on the bar in the chart, the impacted client details, such as, MAC address, hostname, associated SSID and channels, the AP name, IP address, and serial numbers, the associated FortiGate hostname and serial number, and the classifier and sub-classifers are displayed.

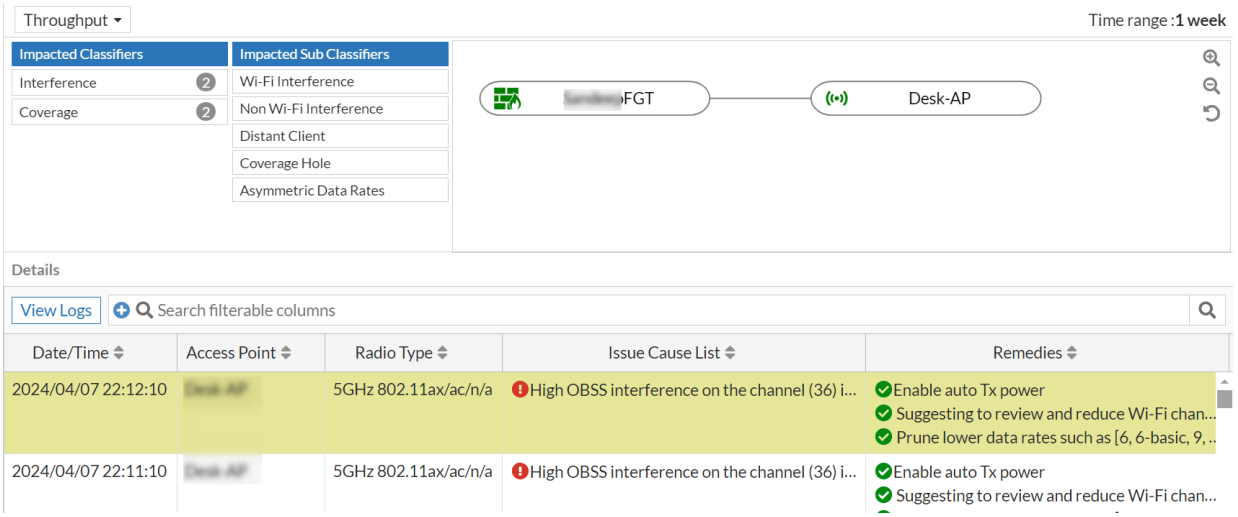


Select any row and click **View Details** to view a simplified topology with a visualization/illustration of the physical placement of devices, such as, FortiGates, FortiSwitches, and FortiAPs connected to each other in your network. This hierarchical pattern is representational; you cannot modify the placement of devices on this page. The topology displays the impacted devices, categorized based on their SLAs, classifiers, and sub-classifiers. The details of the topologies are described for each SLA in the following sections. You can toggle between different impacted SLAs on this page and filter data based on the impacted classifier and sub-classifier.

- Throughput
- Connection Failure
- Time to Connect
- Coverage
- Roaming
- AP Health and Uptime
- WIDS

Throughput

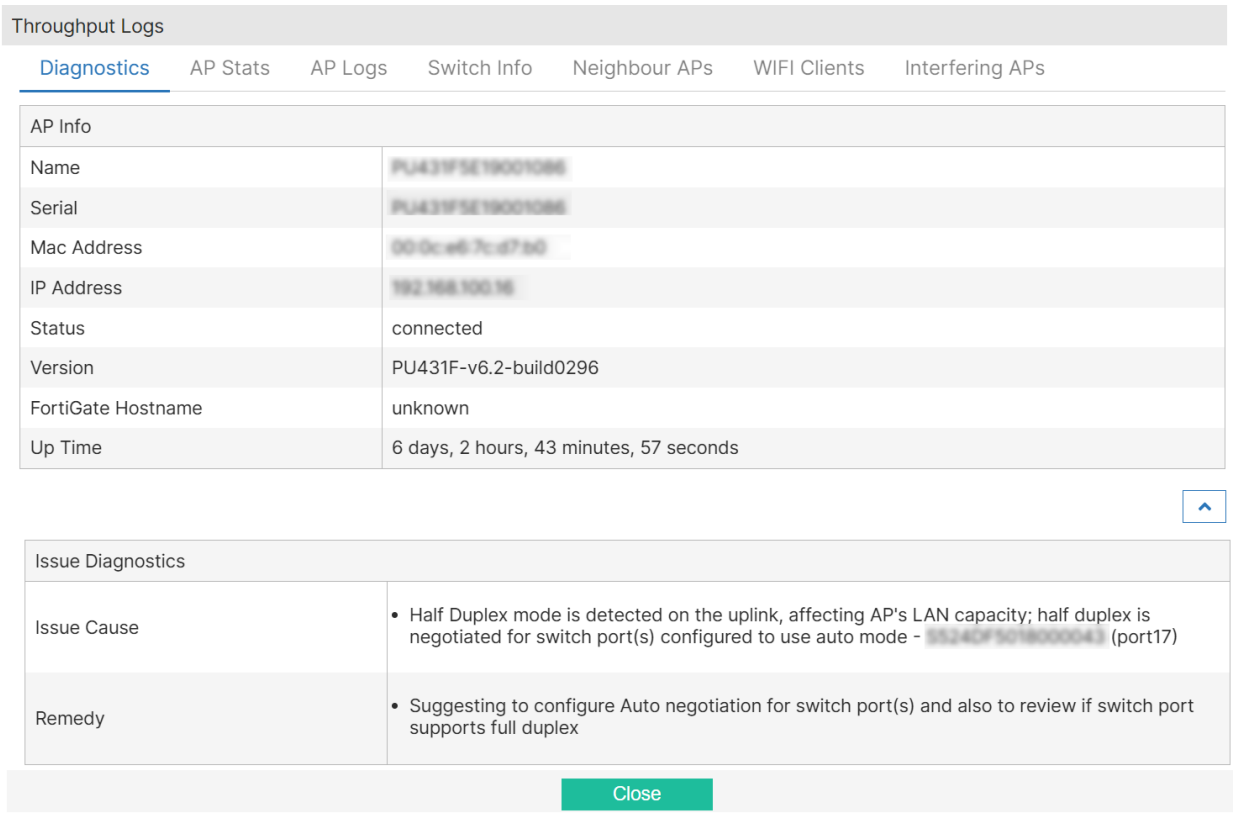
This SLA monitors your network for low throughput conditions and reports clients/devices based on dynamically configured threshold breaches.

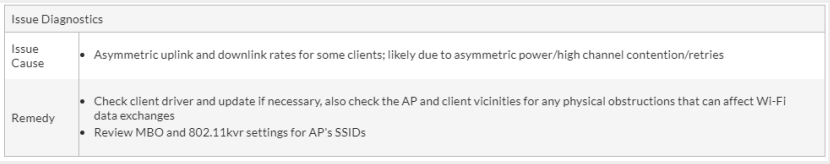
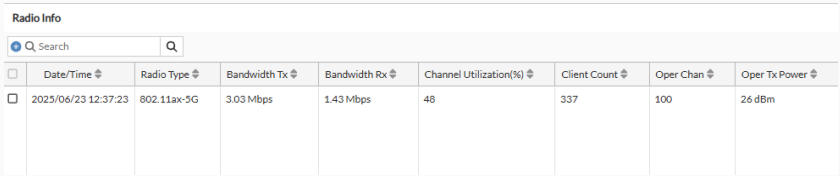


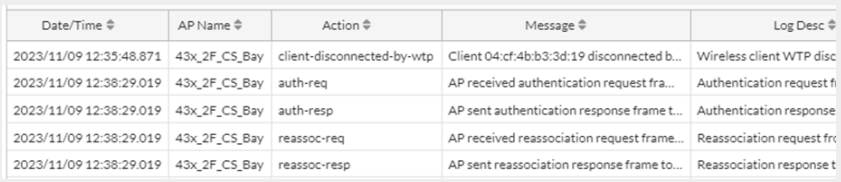
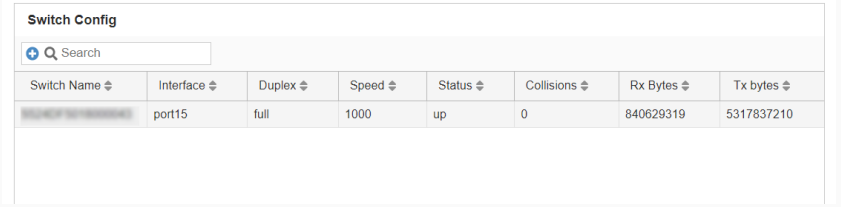
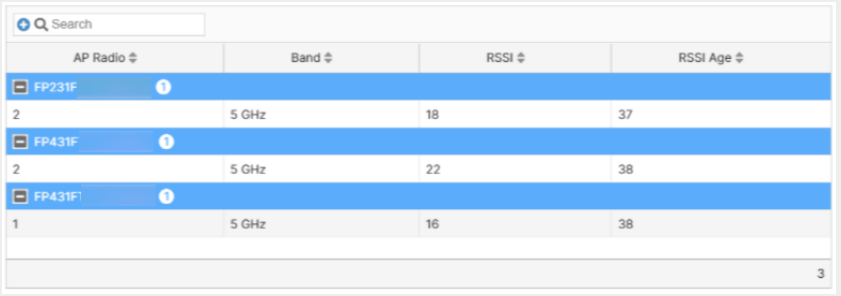
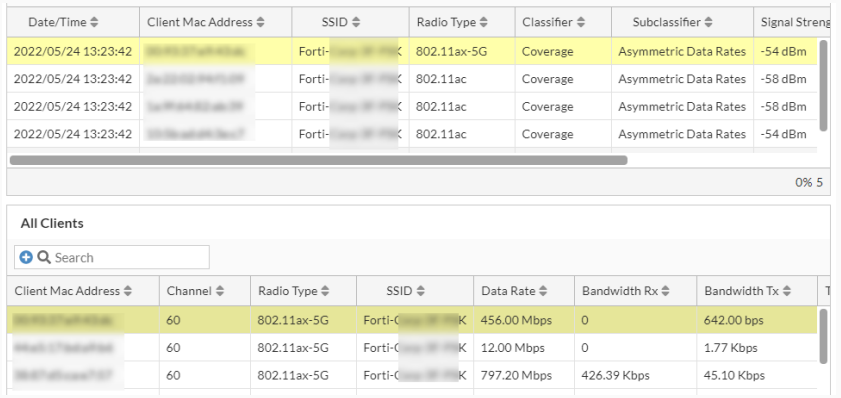
The **Details** table displays information such as the impacted radios for the reported classifiers and sub-classifiers, issue description and the suggested remediation measure, and so on are displayed. Right-click on the header of the table to select the columns that you wish to view.

Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
Classifiers	The classifier of the issue reported for the SLA.
Sub Classifiers	The sub-classifier of the issue for the reported classifier.
Impacted Client Count	The number of impacted clients.
Issue Cause List	Detailed cause of the SLA breach that impacted the client/AP/FortiGate.
Remedies	The suggested remedies to resolve the issue.
Radio	The AP radio that the client associated with.
Access Point	The AP name that the client associated with.
AP Serial Number	The AP serial number that the client associated with.
Bandwidth Rx	The Rx data throughput of the impacted AP.
Bandwidth Tx	The Tx data throughput of the impacted AP.
FortiGate Hostname	The hostname of the FortiGate associated with the AP/impacted client.
FortiGate Serial	The serial number of the associated FortiGate.
Radio Type	The impacted radio and band information.
Radio Impacted Minutes	The duration (in minutes) that the radio was impacted for.

In the impacted details displayed, select a specific row of throughput failure and click **View Details**. You can view details of the impacted AP and issue diagnostics. You can view throughput logs related to **Diagnostics** with the issue description and the suggested remediation, **AP Stats** with the associated AP radio details, **AP Logs** with the time of the throughput failure event and the associated AP details, **Switch Info** with the switch port details connected to the AP, **WIFI Clients** with details of the impacted clients and a list of all WiFi clients, **Interfering APs** with the BSSID and the signal strength of the interfering APs.



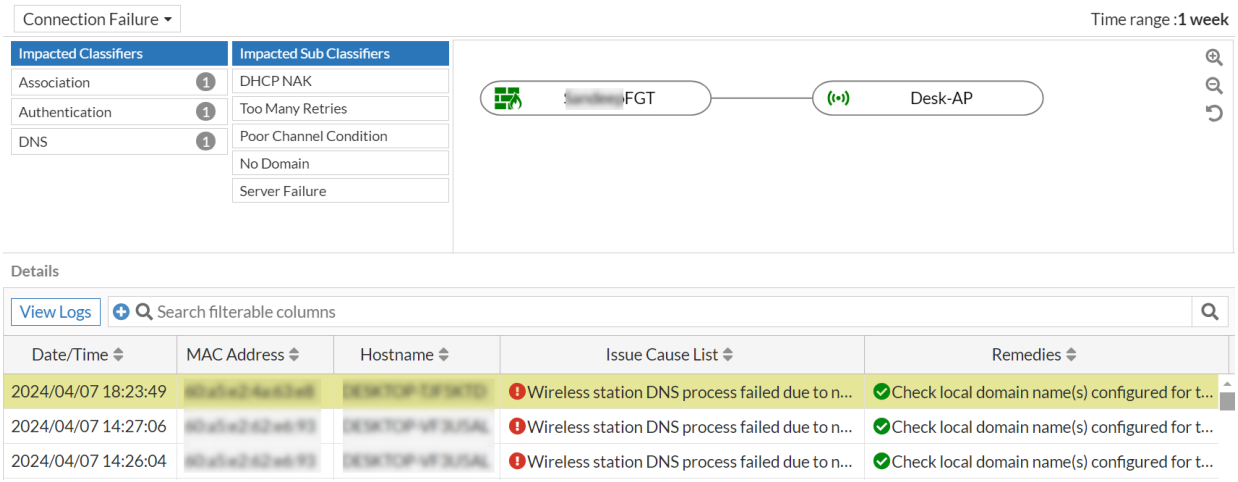
Logs	Description
Diagnostics	This tab provides detailed cause of the SLA breach that impacted the client/AP/FortiGate. FortiAIOps also suggests the remedy to resolve the issue. 
AP Stats	This tab displays the details of the AP radio that the client associated with and the WAN status details of the AP. 
AP Logs	This tab provides the AP event logs generated from FortiGate.

Logs	Description
	
Switch Info	This tab displays the configuration details of the switch port connected to the AP. 
Neighbour APs	This tab displays details of the detected neighbour APs by the client, for distant client & coverage hole issues. 
WIFI Clients	This tab provides details of the impacted clients and also lists all the clients associated with the AP. 
Interfering APs	This tab displays details of the interfering APs in your network.

Logs	Description

Connection Failure

Displays the failed/unsuccessful client connections based on different stages of connection to a network. For example, association failures due to low RSSI, authentication failures due to unreachable RADIUS server, DHCP failure due to a DHCP server process crash, or DNS failure due to an invalid DNS domain.

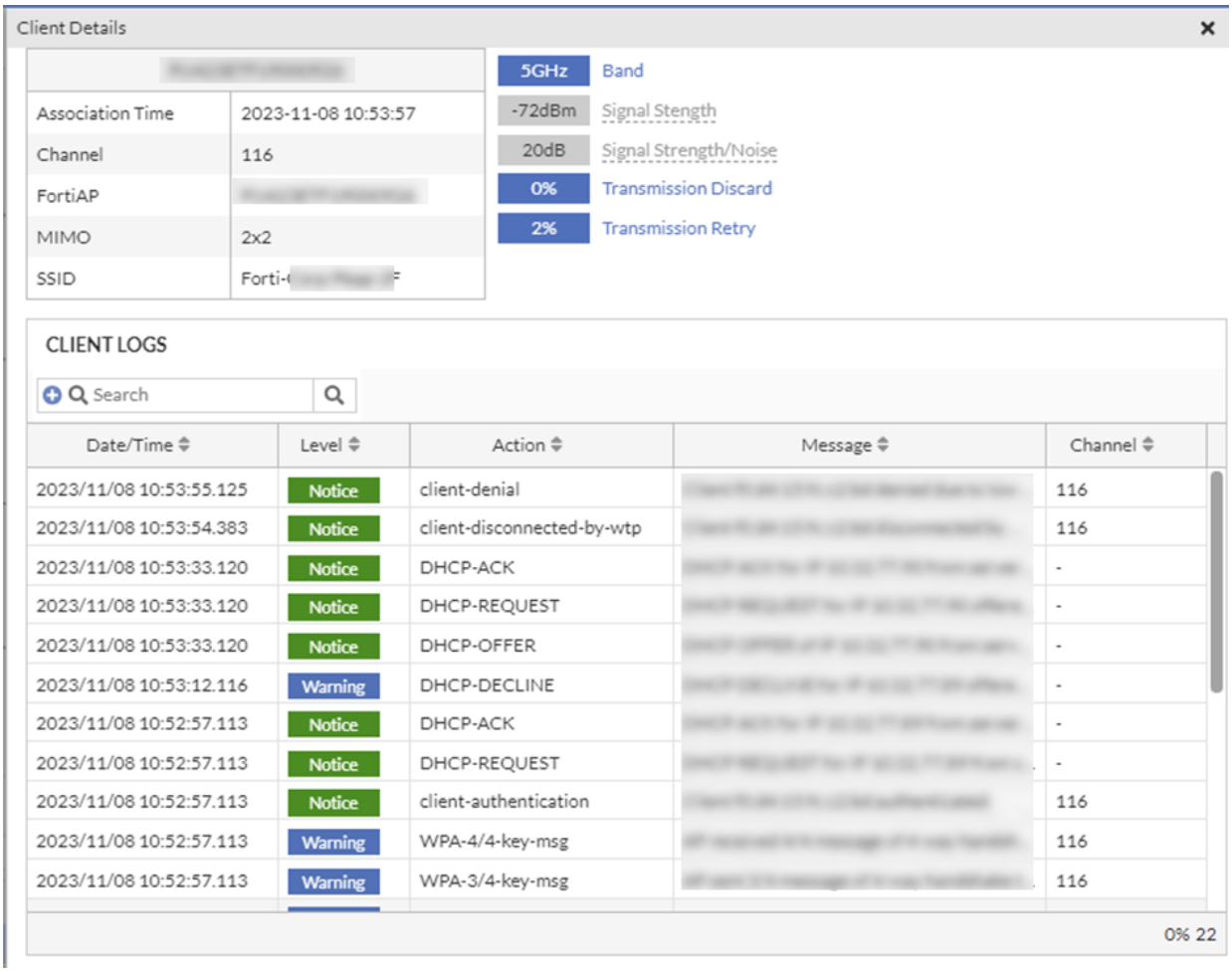


The **Details** table displays details such as the client MAC address, the associated AP serial number and the SSID, the issue classifier/category and the sub-classifier, the issue description and the suggested remediation measure, and so on are displayed. Right-click on the header of the table to select the columns that you wish to view.

Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
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.
Access Point	The name of the AP that the impacted client associated with.
SSID	The SSID that the impacted client is associated with.
Classifier	The classifier of the issue reported for the SLA.
Sub Classifier	The sub-classifier of the issue for the reported classifier.
Issue Cause List	The detailed causes of the SLA breach that impacted the client/AP/FortiGate.

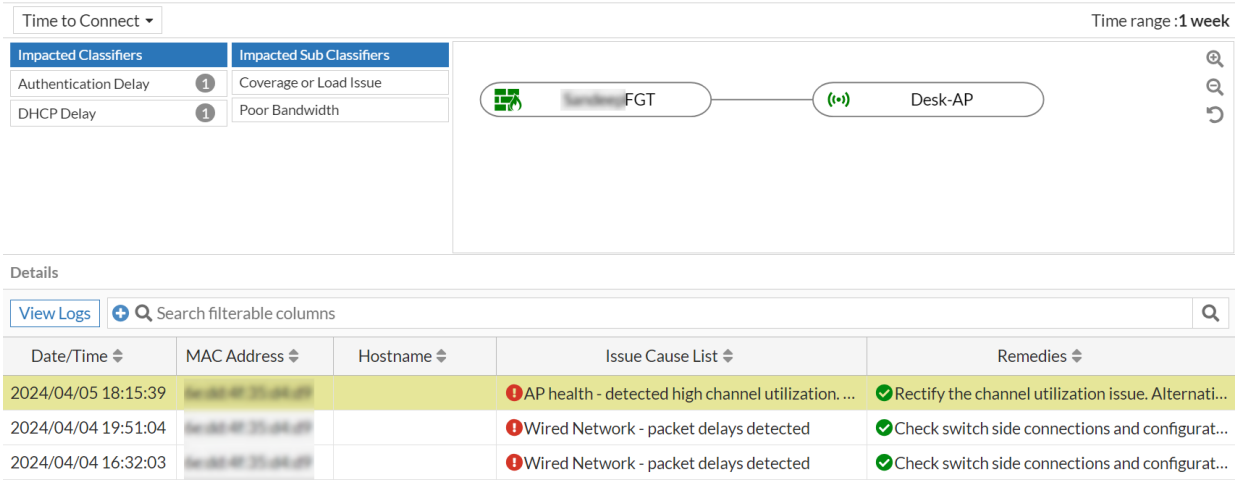
Attribute	Description
Remedies	The suggested remedies to resolve the issue.
AP Serial Number	The AP serial number that the client associated with.
FortiGate Hostname	The hostname of the FortiGate associated with the AP/impacted client.
FortiGate Serial	The serial number of the associated FortiGate.
User Name	The impacted client user name.

Select a specific client and click **View Logs**. You can view **Client Details** such as the client device name, the name of the AP it is associated with and the time of association, associated SSID, and operational details such as the channel and the MIMO mode. The client **Status** such as the associated bandwidth (2.5GHZ/5GHZ), signal strength (RSSI), signal noise, rate of transmission discard and rate of transmission retry between the client and the AP. The **Client Logs** display the time stamp of each action and action classification as notice, warning, etc., and the action details and the associated channel.



Time to Connect

Displays the details of clients that breach the SLA threshold values for these stages of connection, **Association**, **Authentication**, **DHCP**, and **DNS**. The actual value of time taken and the configured **Time to Connect** threshold values (static/dynamic) are compared. For SLA configurations, see Time To Connect

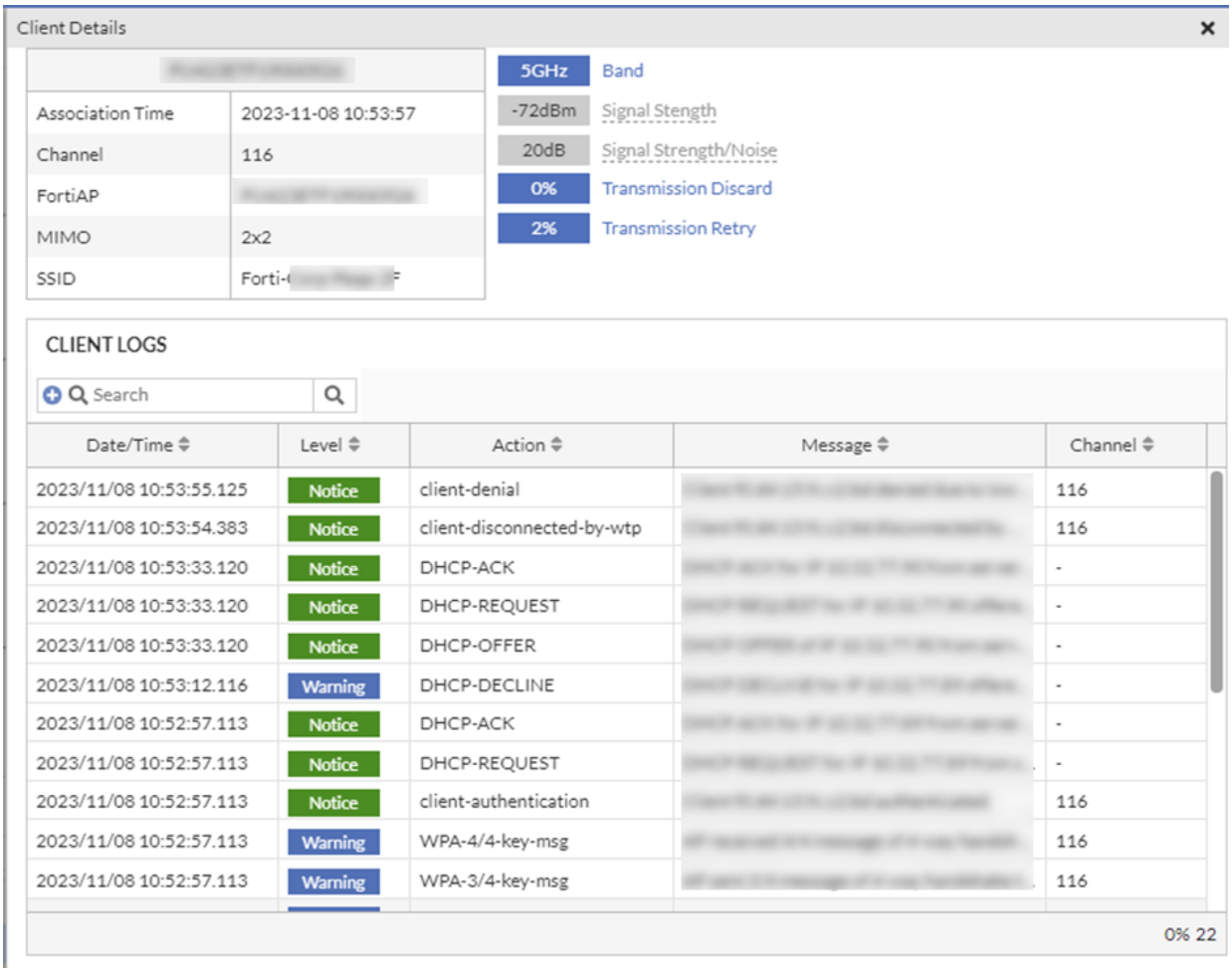


The **Details** table displays details such as the client MAC address, the associated AP serial number and the SSID, the issue classifier/category and the sub-classifier, the issue description and the suggested remediation measure, and so on are displayed. Right-click on the header of the table to select the columns that you wish to view.

Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
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.
SSID	The SSID that the impacted client is associated with.
Classifier	The classifier of the issue reported for the SLA.
Sub Classifier	The sub-classifier of the issue for the reported classifier.
Signal Strength	The signal strength of the client at the time of impact.
Issue Cause List	The detailed causes of the SLA breach that impacted the client/AP/FortiGate.
Remedies	The suggested remedies to resolve the issue.
Access Point	The name of the access point that the client associated with.
AP Serial Number	The AP serial number that the client associated with.
FortiGate Hostname	The hostname of the FortiGate associated with the AP/impacted client.
FortiGate Serial	The serial number of the associated FortiGate.
User Name	The impacted client user name.
Association Delay	The association delay measured in milliseconds.
Association Time	The total time taken by the client for association.
Authentication Delay	The authentication delay measured in milliseconds.

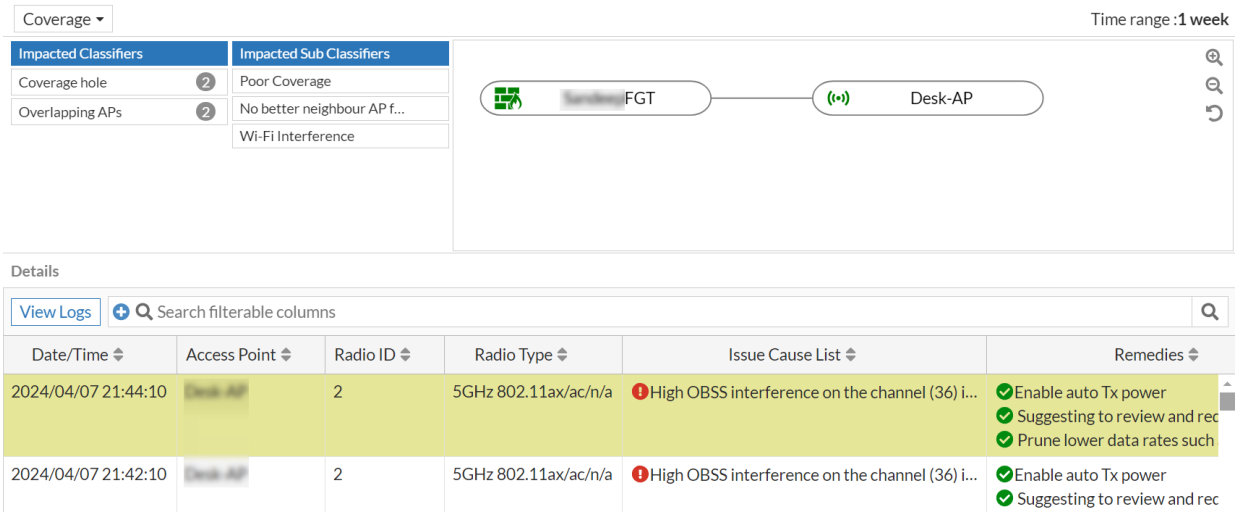
Attribute	Description
Authentication Time	The total time taken by the client for authentication.
DNS Delay	The DNS delay measured in milliseconds.
DNS Time	The total time taken by the client to resolve the DNS request.
DHCP Delay	The DHCP delay measured in milliseconds.
DHCP Time	The total time taken by a client to receive a DHCP address.

Select a specific row and click **View Logs** to view the raw logs associated with the impacted client. You can view **Client Details** such as the client device name, the name of the AP it is associated with and the time of association, associated SSID, and operational details such as the channel and the MIMO mode. The client **Status** such as the associated bandwidth (2.5GHZ/5GHZ), signal strength (RSSI), signal noise, rate of transmission discard and rate of transmission retry between the client and the AP. The **Client Logs** display the time stamp of each action and action classification as notice, warning, etc., and the action details and the associated channel.



Coverage

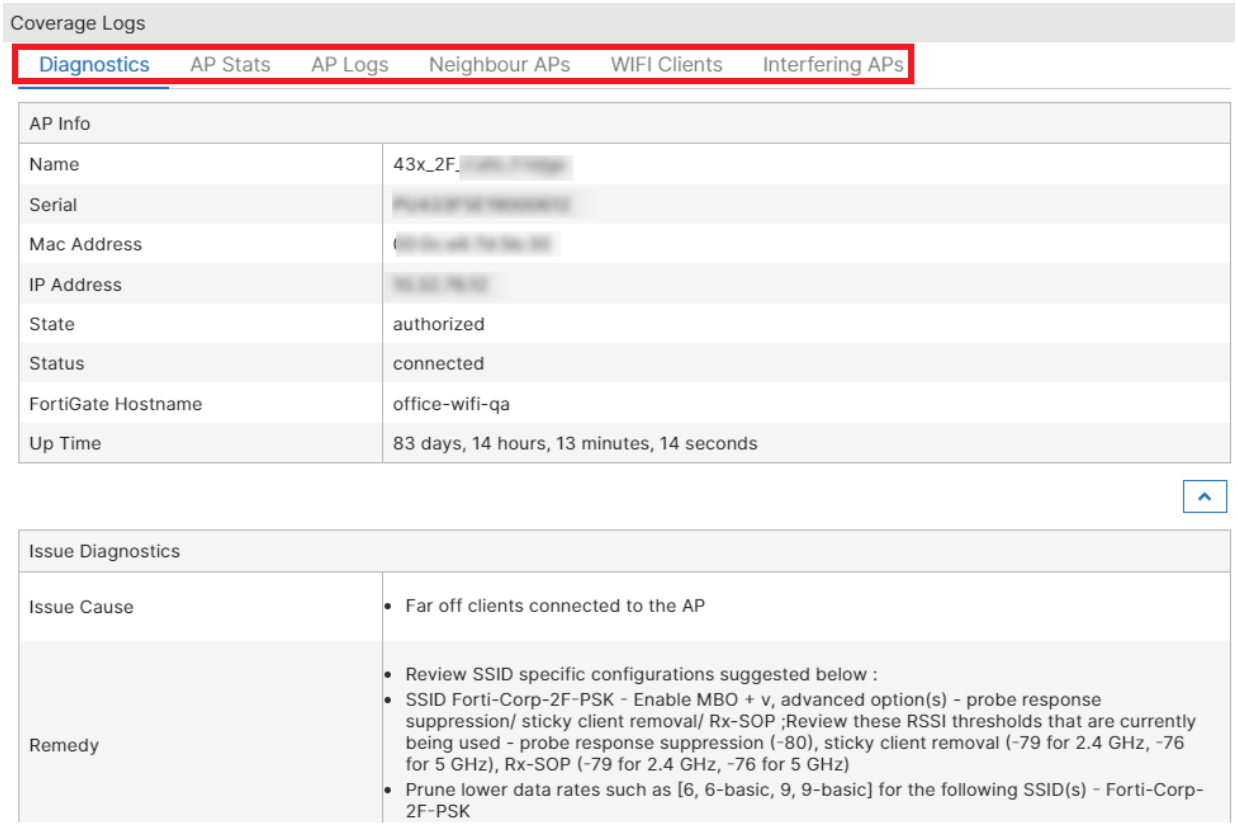
This SLA monitors your network for coverage issues and reports clients/devices based on dynamically configured threshold breaches.

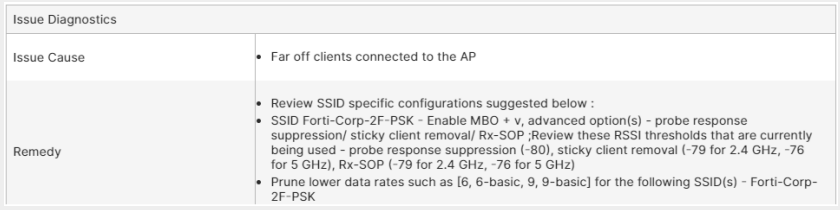
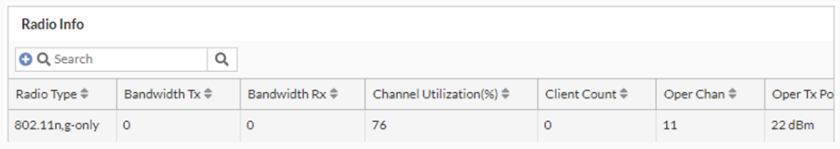


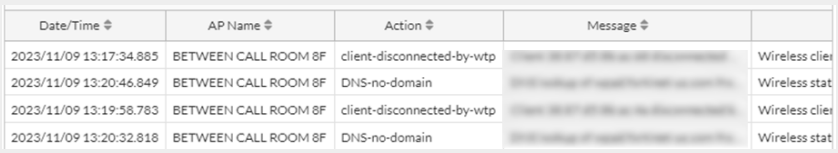
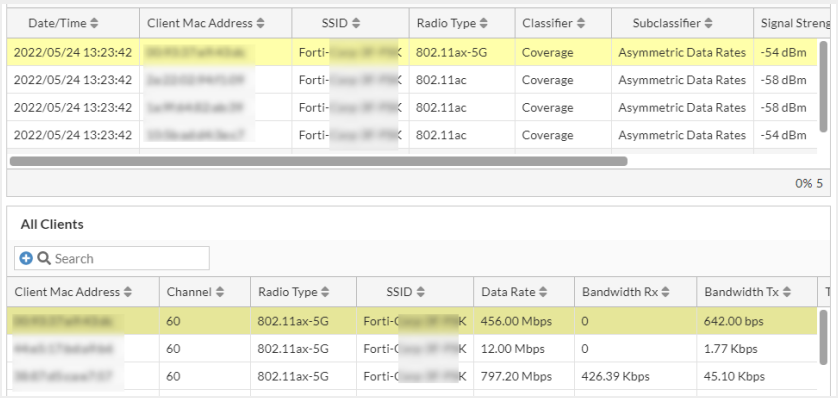
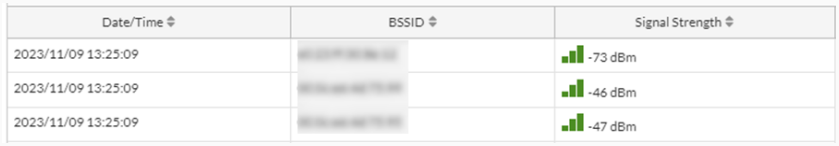
The **Details** table displays issue details such as the radio type, Tx power, neighbour AP count, the issue classifier/category and the sub-classifier, the issue description and the suggested remediation measure, and so on are displayed. Right-click on the header of the table to select the columns that you wish to view.

Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
Access Point	The name of the FortiAP.
Classifiers	The classifiers of the issue reported for the SLA.
Sub Classifiers	The sub-classifiers of the issue for the reported classifier.
Issue Cause List	The detailed causes of the SLA breach that impacted the client/AP/FortiGate.
Remedies	The suggested remedies to resolve the issue.
Radio ID	The AP radio that the client associated with.
Radio Type	The impacted radio and band information associated with the client.
Radio Impacted Minutes	The duration of time (in minutes) that the Radio was impacted.
AP Serial Number	The AP serial number that the client associated with.
TX Power	The Tx power of the AP at the time of impact.
FortiGate Hostname	The hostname of the FortiGate associated with the AP/impacted client.
FortiGate Serial	The serial number of the associated FortiGate.
Radio Type	The impacted radio and band associated with the client.
Channel	The channel at which the client connected.
Impacted Client Count	The number of impacted clients.
Interfering AP	The list of interfering APs in the network.

To view the logs, select a specific row of an AP event and click **View Logs**. You can view coverage logs related to **Diagnostics** with the issue description and the suggested remediation, **AP Stats** with the associated AP radio details, **AP Logs** with the time of the throughput failure event and the associated AP details, **Switch Info** with the switch port details connected to the AP, **WIFI Clients** with details of the impacted clients and a list of all WiFi clients, **Interfering APs** with the BSSID and the signal strength of the interfering APs.



Logs	Description
Diagnostics	This tab provides detailed cause of the SLA breach that impacted the client/AP/FortiGate. FortiAIOps also suggests the remedy to resolve the issue. 
AP Stats	This tab displays the details of the AP radio that the client associated with and the WAN status details of the AP. 

Logs	Description
AP Logs	This tab provides the AP event logs generated from FortiGate.  Date/Time | AP Name | Action | Message 2023/11/09 13:17:34.885 | BETWEEN CALL ROOM 8F | client-disconnected-by-wtp 2023/11/09 13:20:46.849 | BETWEEN CALL ROOM 8F | DNS-no-domain 2023/11/09 13:19:58.783 | BETWEEN CALL ROOM 8F | client-disconnected-by-wtp 2023/11/09 13:20:32.818 | BETWEEN CALL ROOM 8F | DNS-no-domain
WIFI Clients	This tab provides details of the impacted clients and also lists all the clients associated with the AP.  Date/Time | Client Mac Address | SSID | Radio Type | Classifier | Subclassifier | Signal Streng 2022/05/24 13:23:42 | Forti- | 802.11ax-5G | Coverage | Asymmetric Data Rates | -54 dBm 2022/05/24 13:23:42 | Forti- | 802.11ac | Coverage | Asymmetric Data Rates | -58 dBm 2022/05/24 13:23:42 | Forti- | 802.11ac | Coverage | Asymmetric Data Rates | -58 dBm 2022/05/24 13:23:42 | Forti- | 802.11ac | Coverage | Asymmetric Data Rates | -54 dBm 0% 5 All Clients Search Client Mac Address | Channel | Radio Type | SSID | Data Rate | Bandwidth Rx | Bandwidth Tx 60 | 802.11ax-5G | Forti- | 456.00 Mbps | 0 | 642.00 bps 60 | 802.11ax-5G | Forti- | 12.00 Mbps | 0 | 1.77 Kbps 60 | 802.11ax-5G | Forti- | 797.20 Mbps | 426.39 Kbps | 45.10 Kbps
Interfering APs	This tab displays details of the interfering APs in your network.  Date/Time | BSSID | Signal Strength 2023/11/09 13:25:09 | -73 dBm 2023/11/09 13:25:09 | -46 dBm 2023/11/09 13:25:09 | -47 dBm

Roaming

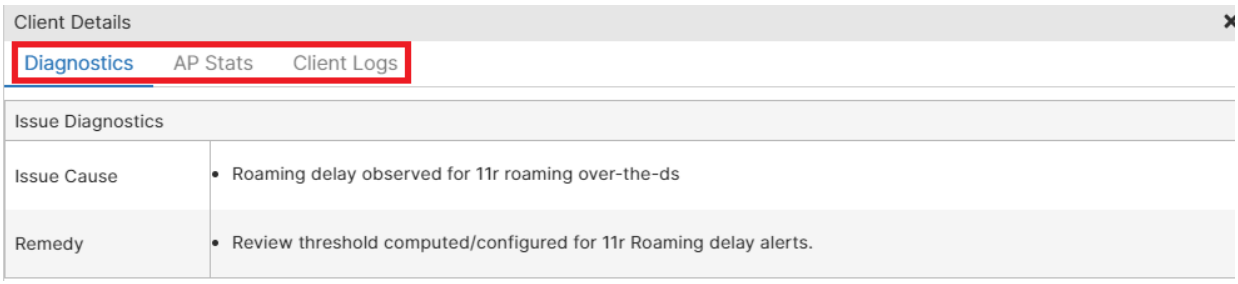
Slow roaming clients are detected based on the variation of the classifier threshold values set by the users or calculated dynamically by FortiAIOps. The parameters to identify slow roaming clients are **Fast BSS Transition Roams**, **PMK Cache**, and **Opportunistic Key Caching Roams**. Any breach in the threshold values are detected and reported. For SLA configurations, see Roaming.

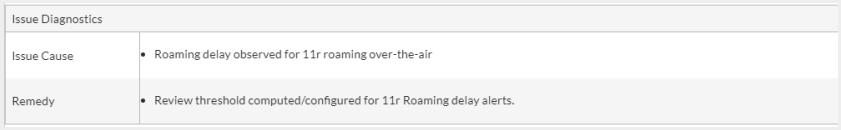
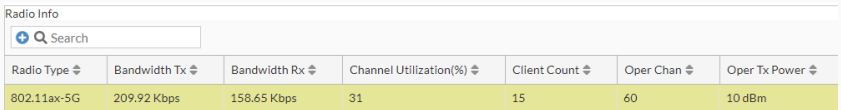
The **Details** table displays details such as the client MAC address, the associated AP serial number and the SSID, the issue classifier/category and the sub-classifier, the issue description and the suggested remediation measure, and so on. Right-click on the header of the table to select the columns that you wish to view.

Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
MAC Address	The MAC address of the impacted client device.
Device	The name of the device as configured by the user. If the name is not configured or available, then MAC address is displayed.
SSID	The SSID that the impacted client is associated with.
Classifier	The classifier of the issue reported for the SLA.

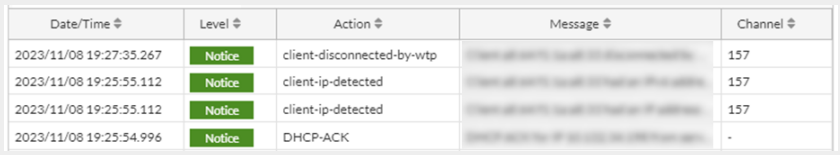
Attribute	Description
Sub Classifier	The sub-classifier of the issue for the reported classifier.
Roaming Delay	The delay (latency) in client roaming (milliseconds) in case of threshold breach.
Roaming Time	The duration of time the client was roaming the network.
Radio ID	The AP radio that the client associated with.
Radio Type	The impacted radio and band information.
AP Serial Number	The AP serial number that the client associated with.
Channel	The channel at which the AP/client were operating.
Issue Cause List	detailed cause of the SLA breach that impacted the client/AP/FortiGate.
Remedies	The suggested remedies to resolve the issue.
Access Point	The name of the access point.

To view the logs, select a specific row of an AP event and click **View Logs**. You can view client details such as **Diagnostics** with the issue description and the suggested remediation, **AP Stats** with the associated AP radio details, and **Client Logs** with details of the impacted clients.



Logs	Description
Diagnostics	This tab provides detailed cause of the SLA breach that impacted the client. FortiAIOps also suggests the remedy to resolve the issue. 
AP Stats	This tab displays the details of the AP radio that the client associated with. 
Client Logs	This tab provides client event logs.

Logs	Description

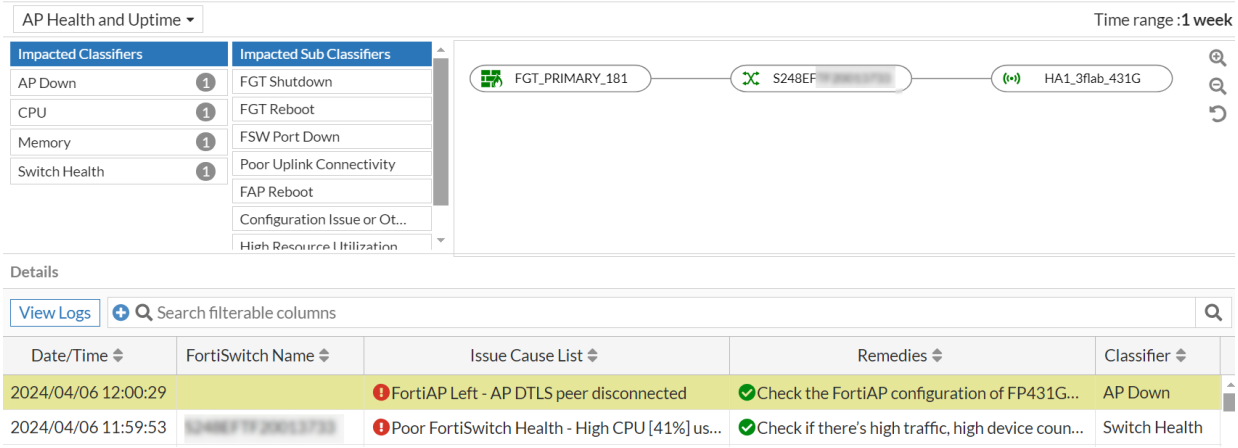


Date/Time	Level	Action	Message	Channel
2023/11/08 19:27:35.267	Notice	client-disconnected-by-wtp		157
2023/11/08 19:25:55.112	Notice	client-ip-detected		157
2023/11/08 19:25:55.112	Notice	client-ip-detected		157
2023/11/08 19:25:54.996	Notice	DHCP-ACK		-

In the various throughput logs displayed, you can right-click on the table header to select the details you want to view.

AP Health and Uptime

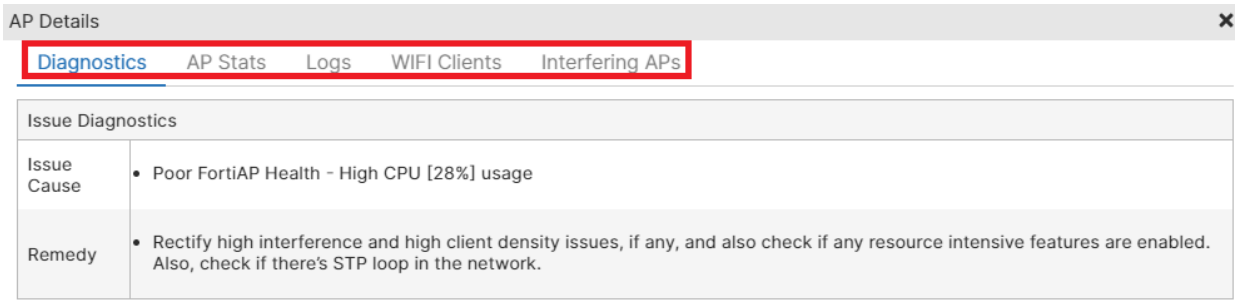
Displays the AP health based on the configured AP health threshold values and the AP down status due to AP/FortiGate reboot, disabled switch port etc. For SLA configurations, see Device Health

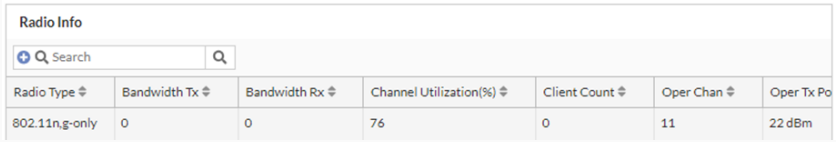
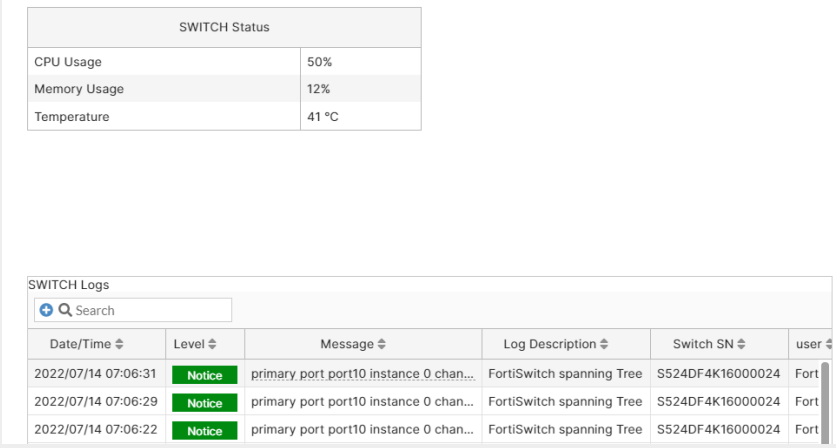


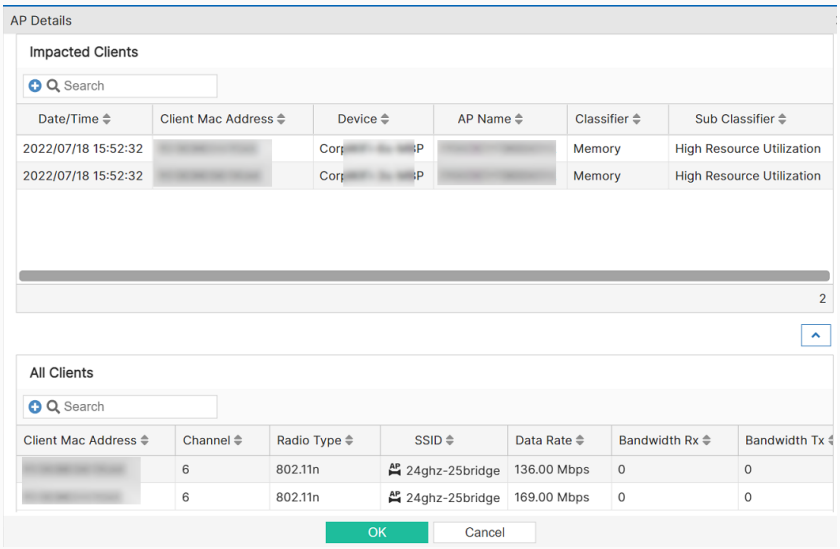
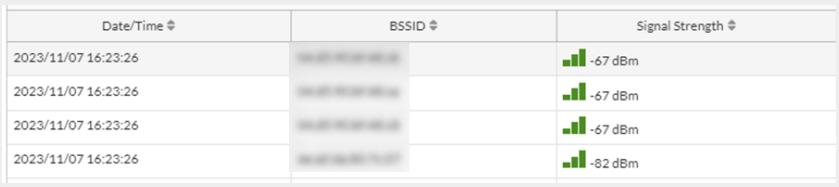
The **Details** table displays issue details such as the issue classifier/category and the sub-classifier, the issue description and the suggested remediation measure, and so on. Right-click on the header of the table to select the columns that you wish to view.

Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
FortiSwitch Name	The name of the switch associated with the impacted AP/client.
Issue Cause List	The detailed causes of the SLA breach that impacted the client/AP/FortiGate.
Remedies	The suggested remedies 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.
AP Serial Number	The AP serial number that the client associated with.
FortiGate Hostname	The hostname of the FortiGate associated with the AP/impacted client.
FortiGate Serial Number	The serial number of the associated FortiGate.
FortiSwitch Serial Number	The serial number of the switch associated with the impacted AP/client.

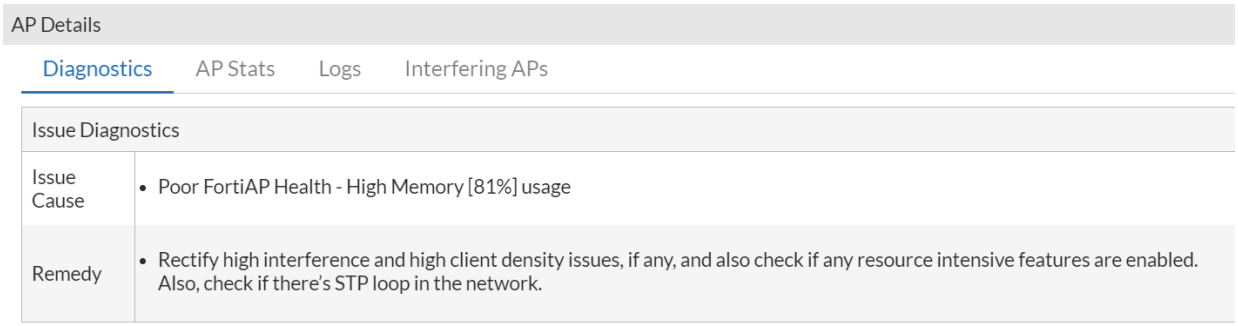
In the AP events displayed, select an event and click **View Logs**.



Logs	Description
Diagnostics	This tab provides detailed cause of the SLA breach that impacted the client/AP/FortiGate. FortiAIOps also suggests the remedy to resolve the issue.
AP Stats	This tab displays the details of the AP radio that the client associated with and the WAN status details of the AP. 
Logs	• For the AP *down*/FortiSwitch health events, triggered due to FortiSwitch related failure, the FortiSwitch status and logs are displayed. • For AP health related events like poor CPU and memory, the AP status and logs are displayed. • For AP down events triggered due to FortiAP/FortiGate failure, the AP status and logs, and FortiGate logs are displayed. 

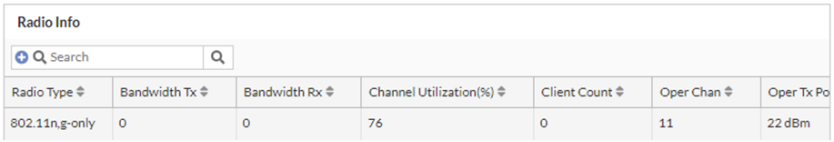
Logs	Description
WIFI Clients	This tab provides details of the impacted clients and also lists all the clients associated with the AP. 
Interfering APs	This tab displays details of the interfering APs in your network. 

Select any impacted client and click **Show AP details** to view the detailed AP logs.



Select any of the tabs to view the data described in this table.

Logs	Description
Diagnostics	This tab provides detailed cause of the SLA breach that impacted the client/AP/FortiGate. FortiAIOps also suggests the remedy to resolve the issue.

Logs	Description
AP Stats	This tab displays the details of the AP radio that the client associated with and the WAN status details of the AP. 
Interfering APs	This tab displays details of the interfering APs in your network.
Logs	This tab provides the AP event logs generated from FortiGate.

WIDS

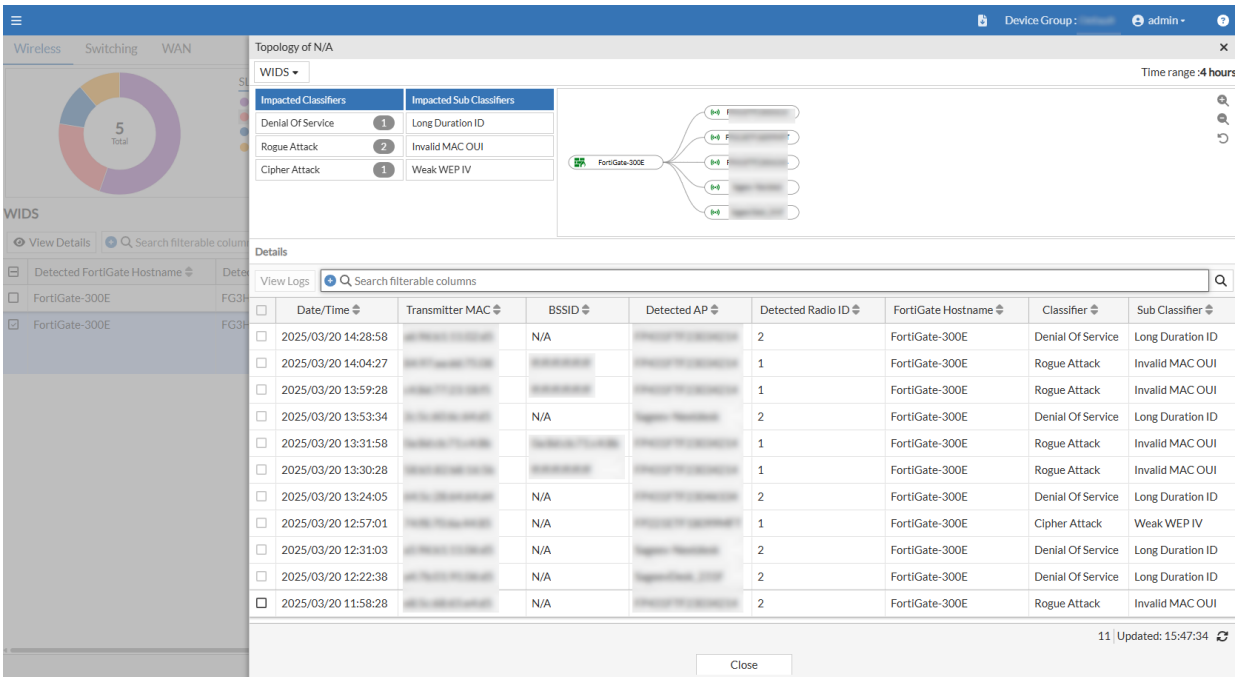
The WIDS SLA monitors and reports on potential events detected within the network by the WIDS (Wireless Intrusion Detection System) system. It detects security threats and recommends corrective actions to maintain network integrity, enhancing security with real-time alerts and actionable insights for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

Intrusion Type	Description
	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.

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



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

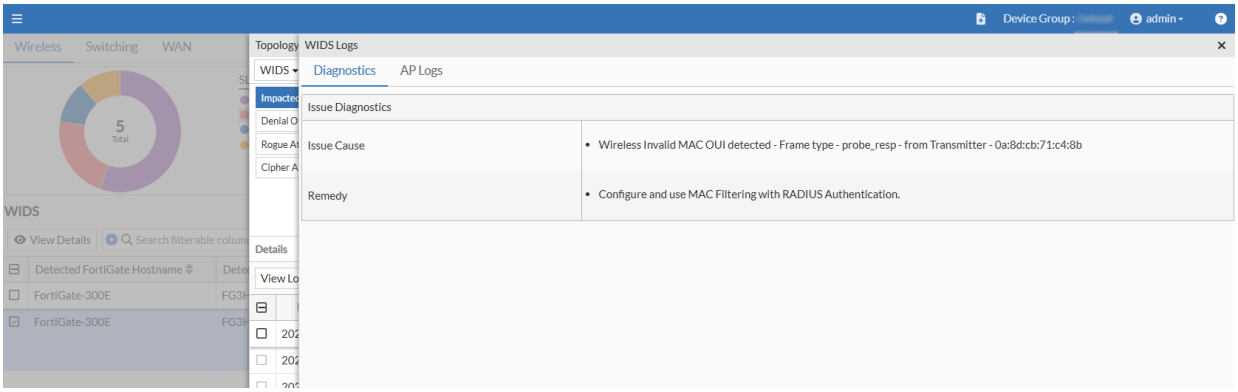
The **Details** table displays information such as the Detected FortiGate Hostname, Detected FortiGate, Affected AP Serial Number, Detected FortiGate IP Address, Classifier, Sub Classifier, Affected AP IP Address, Affected AP Name, Affected AP State, and Affected AP Status. Right-click on the header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

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

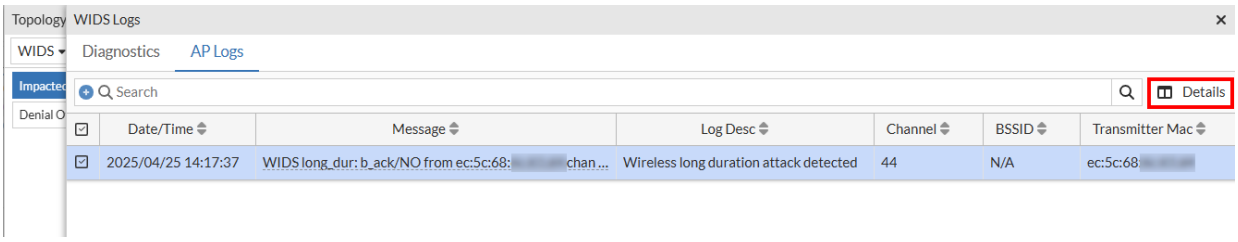
Attribute	Description
Detected FortiGate Hostname	The hostname of the FortiGate associated with AP detecting WIDS events.
Detected FortiGate	Name of the FortiGate in which AP detecting WIDS is connected.
Affected AP Serial Number	Serial number of Access Point detecting WIDS event.
Detected FortiGate 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.

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

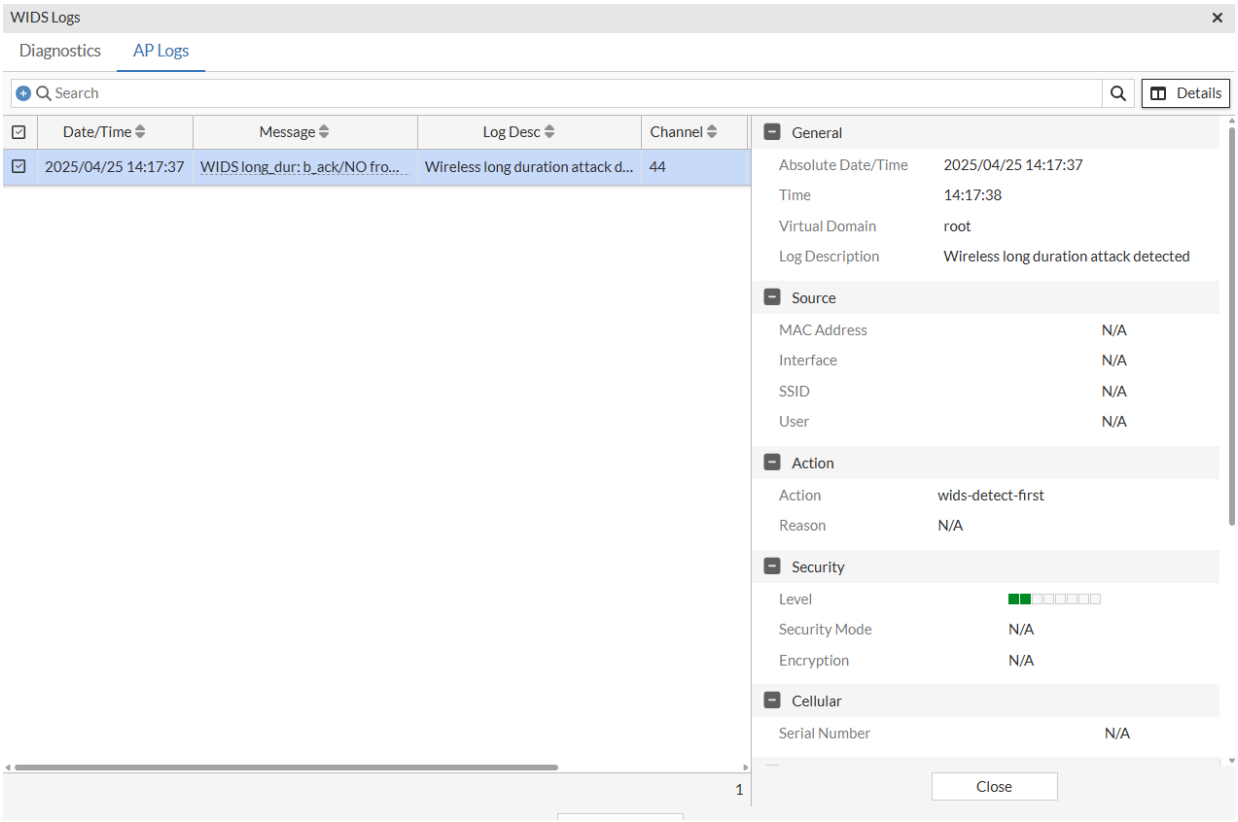
The **Diagnostics** tab displays diagnostics details such as Issue Cause and Remedy suggested to resolve the issue.



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.



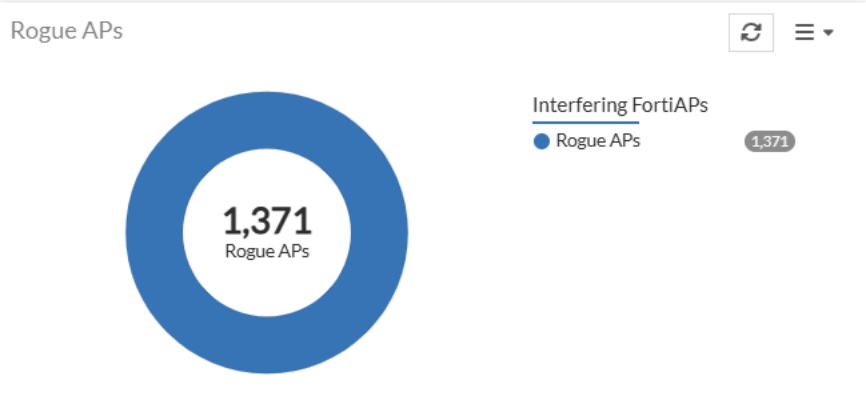
Select the log and click **Details** to view a more detailed log.



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.

Rogue APs

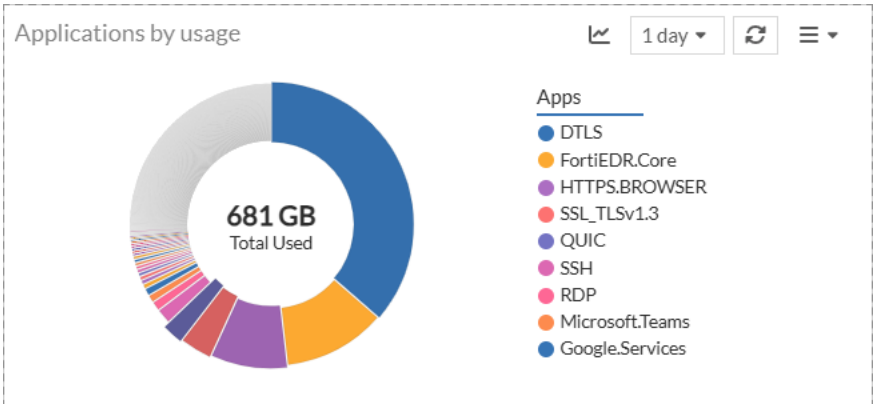
This chart provides details of the rogue APs detected on the network.



Click on the chart to view more details. For more information, see Rogue APs.

Applications by Usage

This chart provides details of the applications being used in the network along with the data being used by each application.



Click on an application name to view more details. For more information, see Applications.

Switch

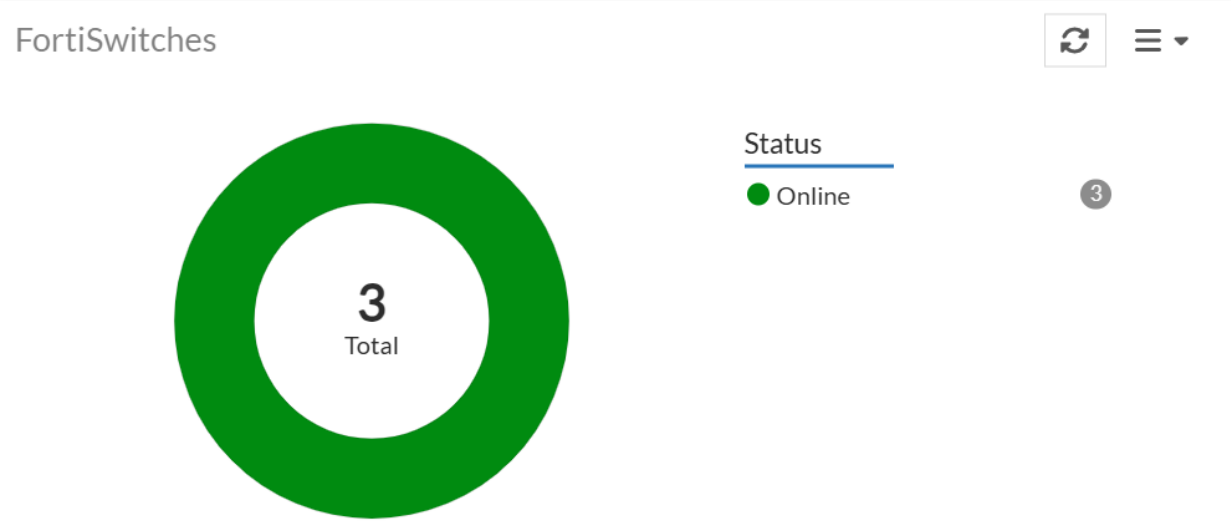
The Switch page displays all the important details about the switches within your network. Details of all the FortiSwitches and their status, the types of even in a specific time period, details of the wired clients, and different SLAs displayed.

The following charts are available:

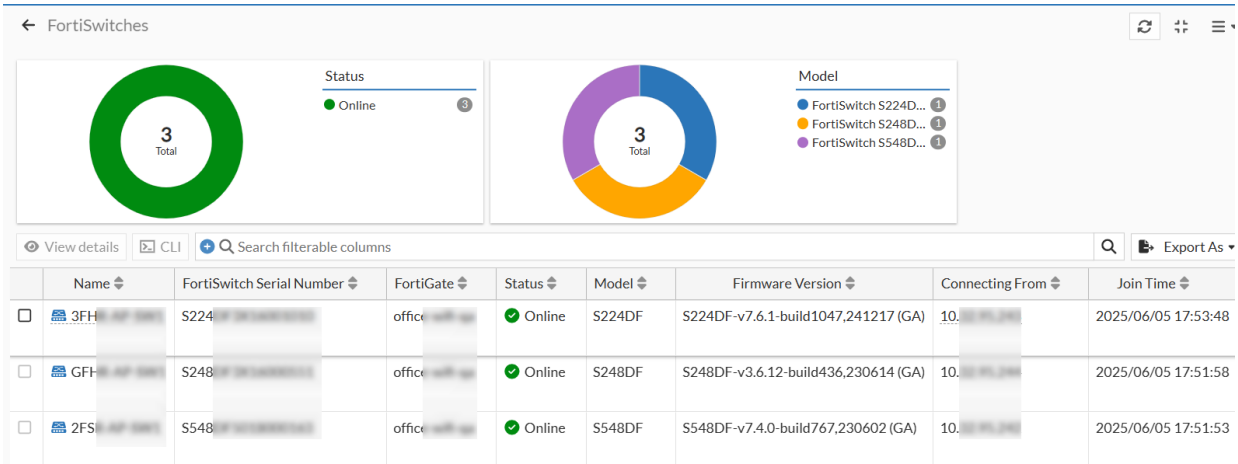
- FortiSwitches
- FortiSwitches Events
- Wired Clients
- Switching Insights

FortiSwitches

This chart displays the total number of FortiSwitches in your network and their status (Online, Offine, Waiting for Authorization, or Unknown).



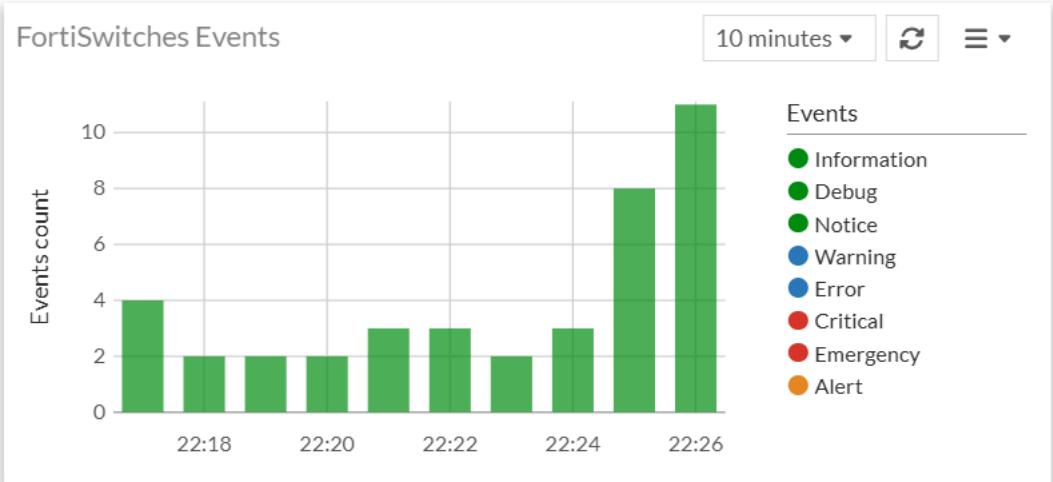
Click the chart for detailed information about the FortiSwitches.



For more information, see FortiSwitch.

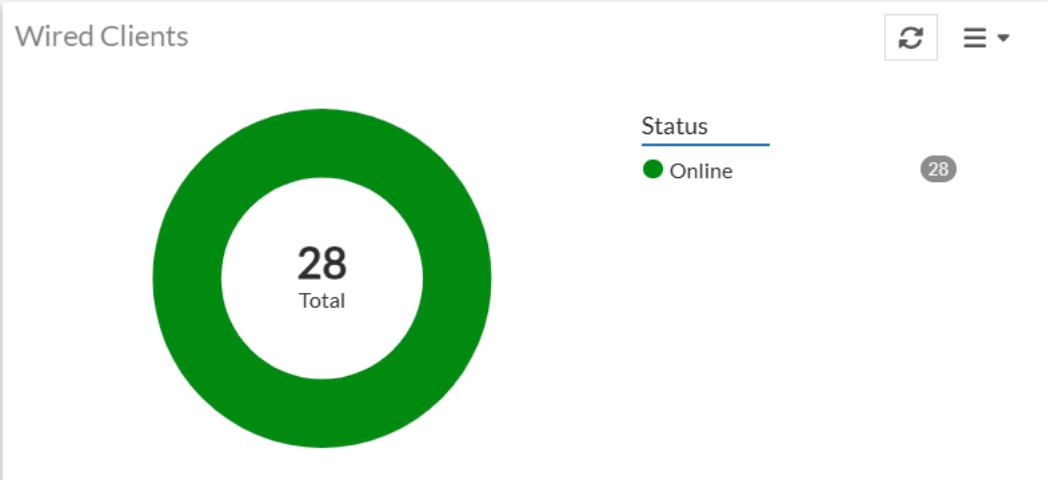
FortiSwitches Events

This chart displays the FortiSwitch events at a given time and categorizes them based on the type of event 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).



Wired Clients

This chart helps you to monitor the wired clients on your network.



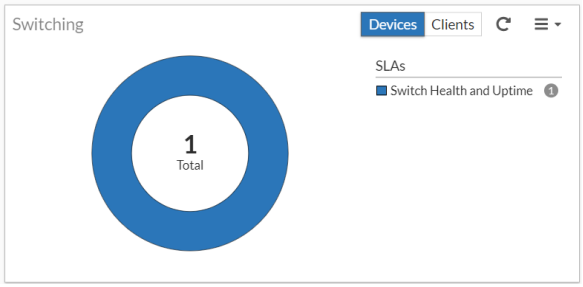
Click on the chart to view more details. For more information, see Wired Clients.

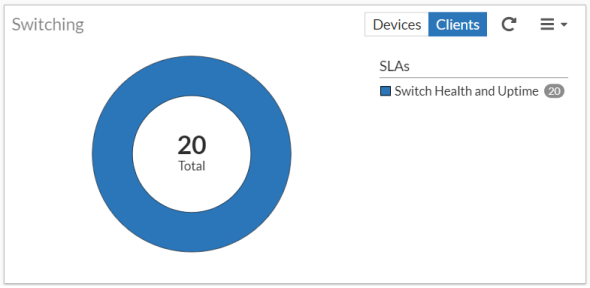
Switching Insights

The **Switching Insights** panel displays the total number of impacted clients and SLA data. Select **Devices** to view the impacted switch count or click **Clients** to view the impacted client count.

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.





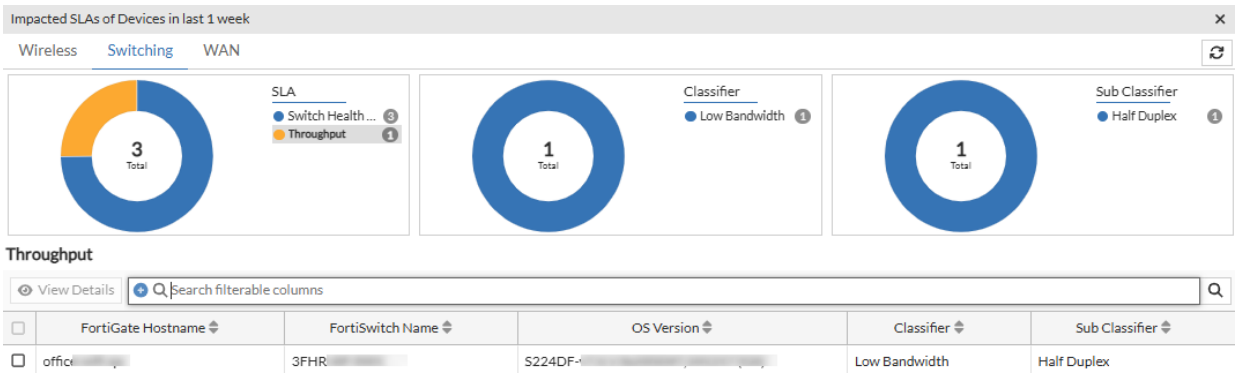
SLAs, Topology and Logs

The following SLAs are detected and reported by FortiAIOps for switching. The issues reported are categorized based on classifiers and sub-classifiers, with suggested remedial measures to curtail the SLA breaches and enhance network performance.

- Throughput
- Network
- Switch Health and Uptime
- Switch

Throughput

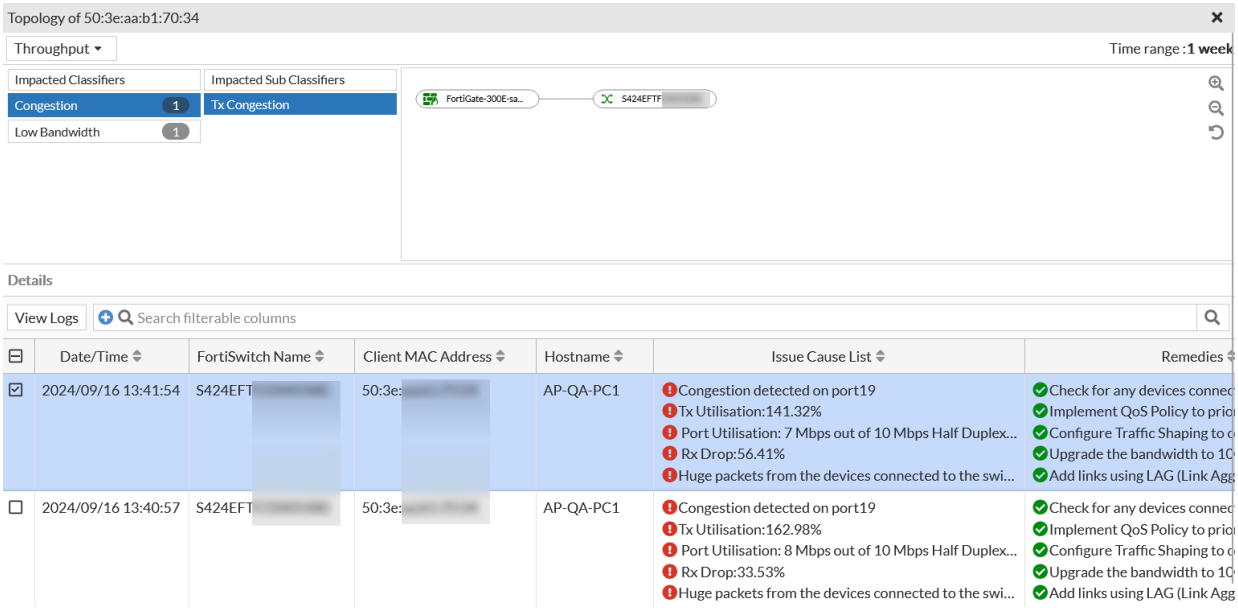
Displays potential low throughput conditions. The system uses intelligent machine learning to analyze recent switch port statistics by dynamically learning from recent data. Unusual patterns and potential breaches are identified with significantly improved accuracy.



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 Details**. The **Details** table displays the following information.

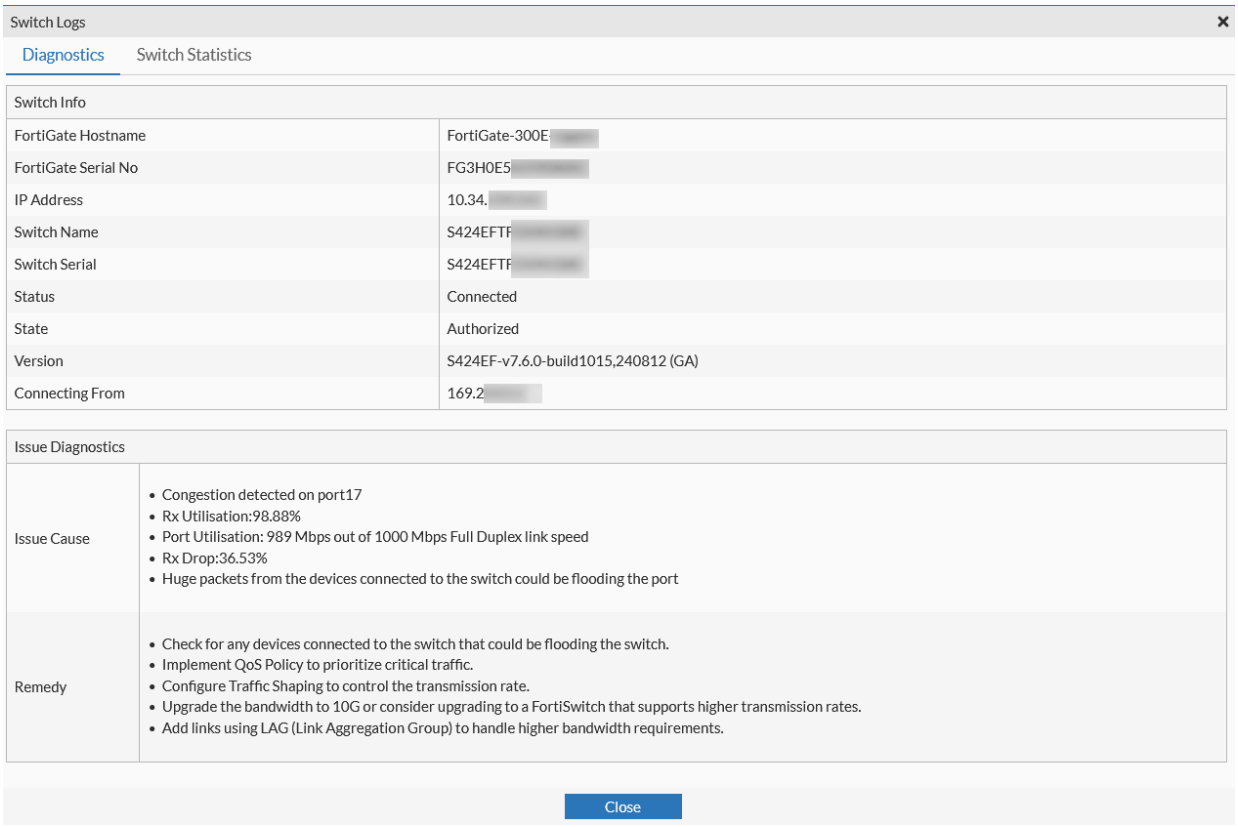


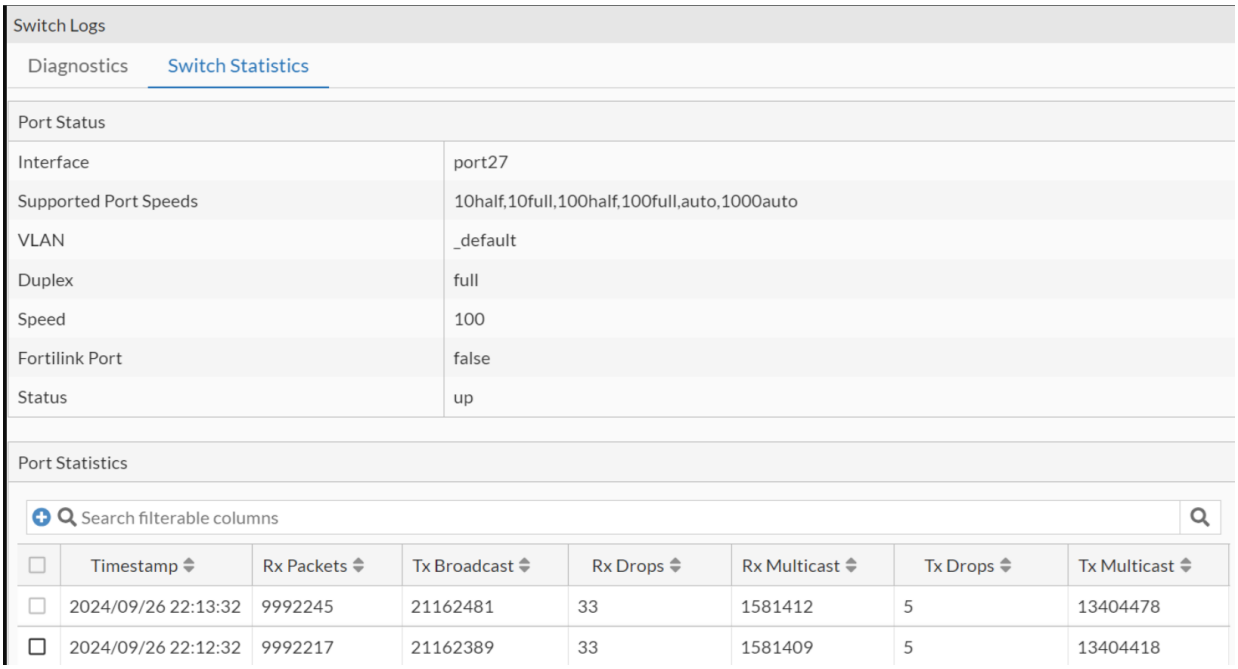
Right-click on the header of the table to select the columns that you wish to view.

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.

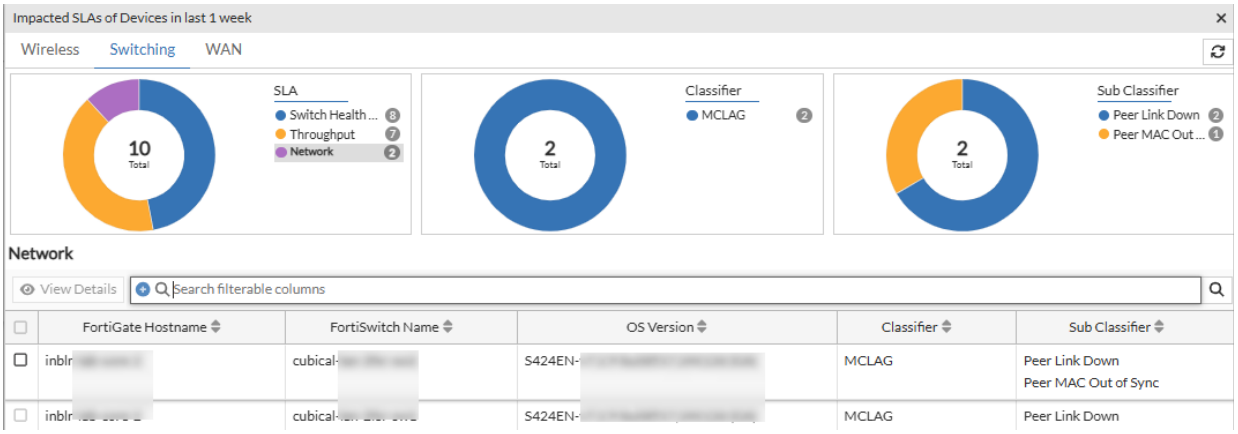
To view the Switch logs, select a specific row of a **Throughput** event and click **View Logs**. You can view Switch details and diagnostics with the issue description and the suggested remediation, along with the FortiSwitch port statistics.





Network

Displays potential network disruptions that may lead to poor connectivity. Intelligent machine learning is used to analyze recent switch port statistics and learn from recent data, thus identifying unusual patterns and potentials threats.

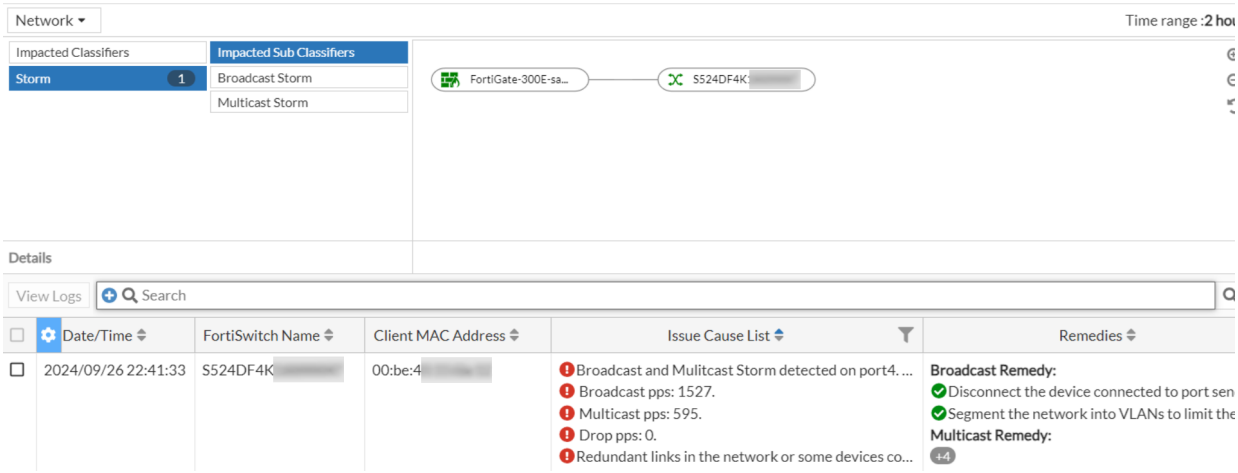


The **Network** table displays information such as the client MAC address and the associated FortiSwitch details for the reported classifiers and sub classifiers, issue description and the suggested remediation measure, and so on are displayed. Right-click on the header of the table to select the columns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

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

Attribute	Description
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 Details**. The **Details** table displays the following information.

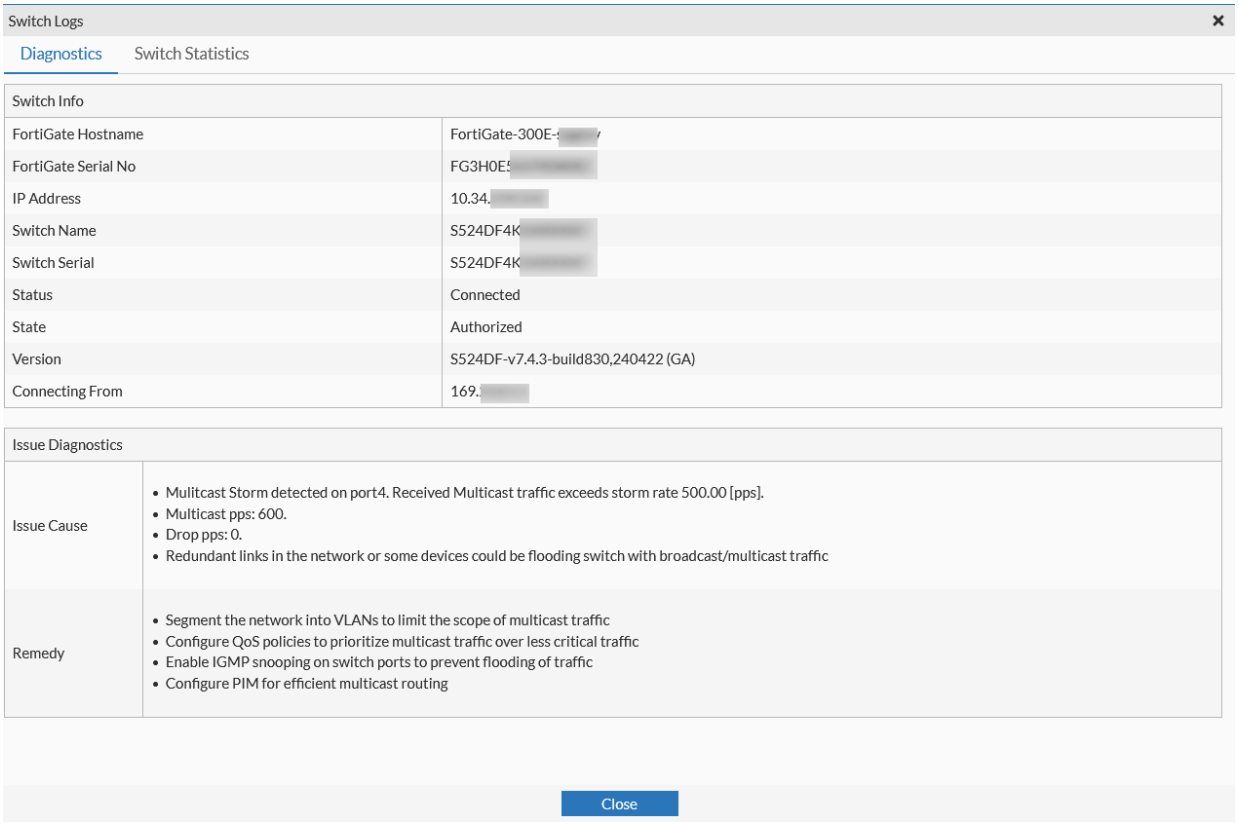


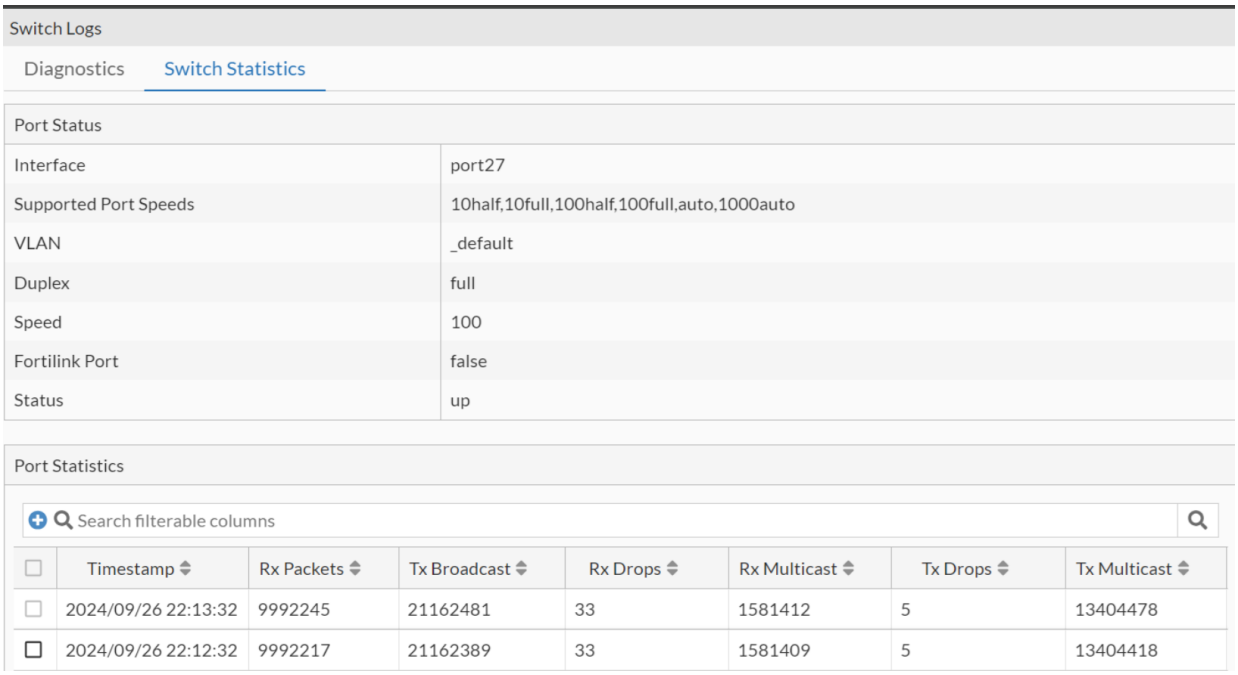
Right-click on the header of the table to select the columns that you wish to view.

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.
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.

Attribute	Description
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.

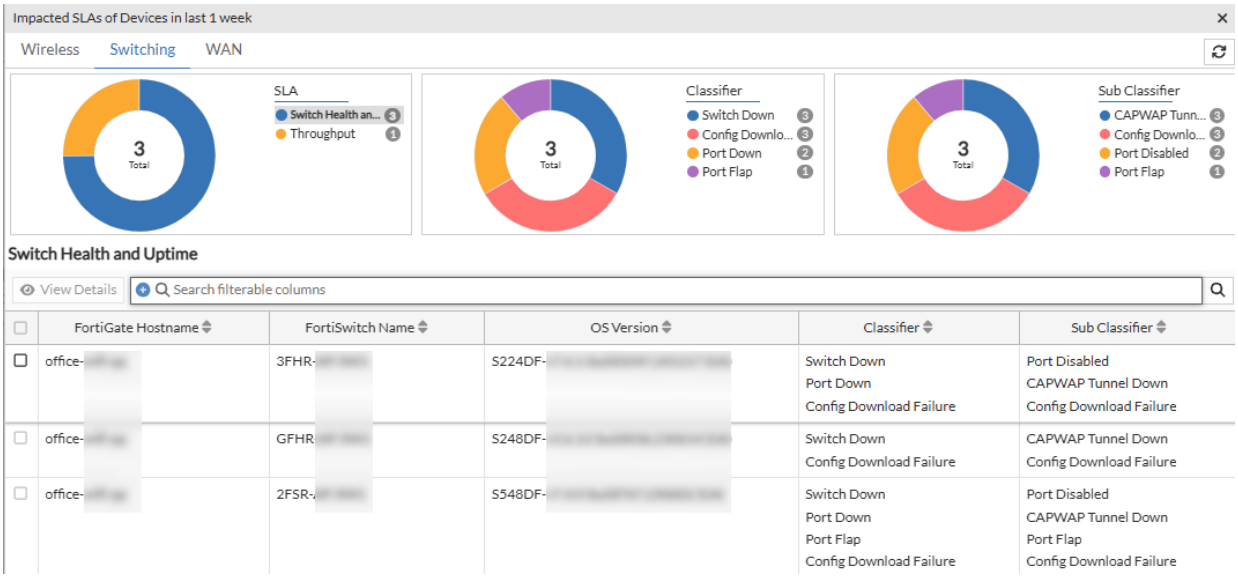
To view the Switch logs, select a specific row of **Network** SLA event and click **View Logs**. You can view Switch details and diagnostics with the issue description and the suggested remediation, along with the FortiSwitch port statistics.



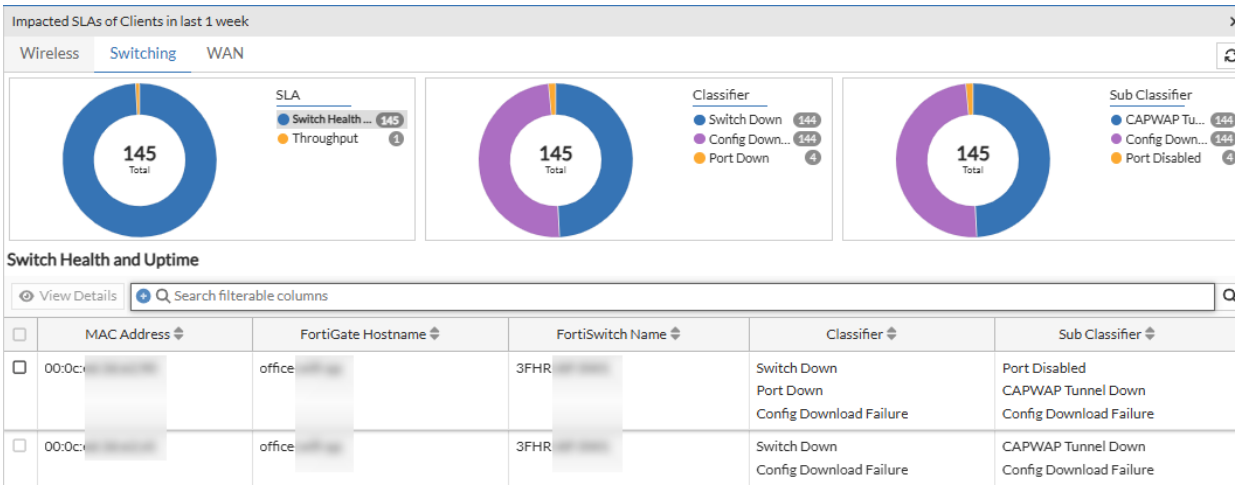


Switch Health and Uptime

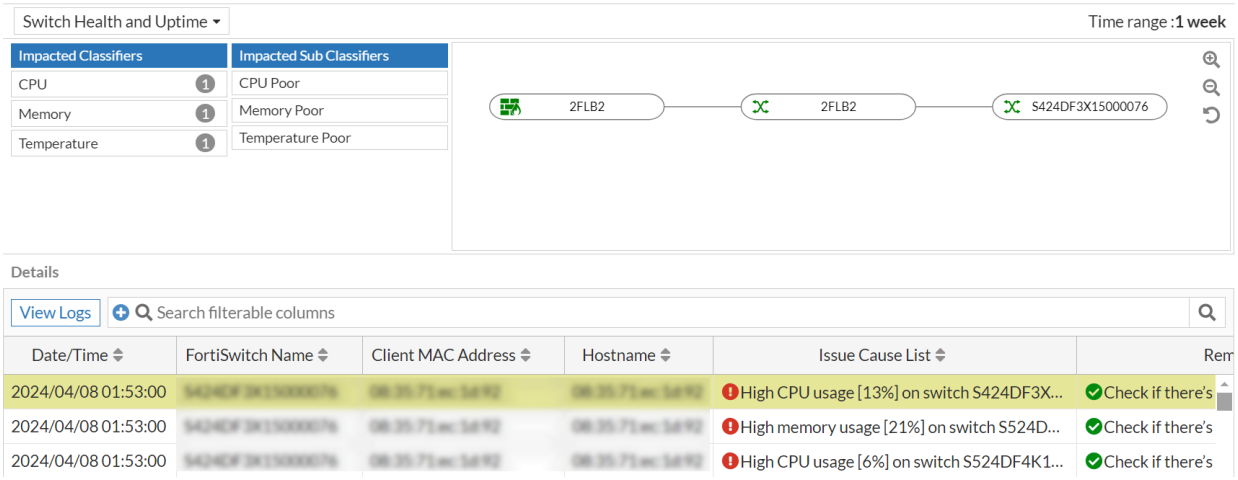
Displays the switch health based on the configured switch health threshold values and the status of the switch (Up/Down). The associated impacted FortiGate controller, switch, and client count are displayed in a collapsible topology. If you select the **Devices** view in the Switching panel and click on the SLA in the impacted SLAs list or click on the bar in the chart, the impacted switches' details such as, OS version, the associated FortiGate host name and serial number, FortiSwitch name and serial number, FortiSwitch state and status, and classifier and sub-classifier are displayed.



If you select the **Clients** view in the Switching panel and click on the SLA in the impacted SLAs list or click on the bar in the chart, the impacted client details, such as, MAC address, OS version, the associated FortiGate host name and serial number, FortiSwitch name and serial number, FortiSwitch state and status, and classifier and sub-classifier are displayed.



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

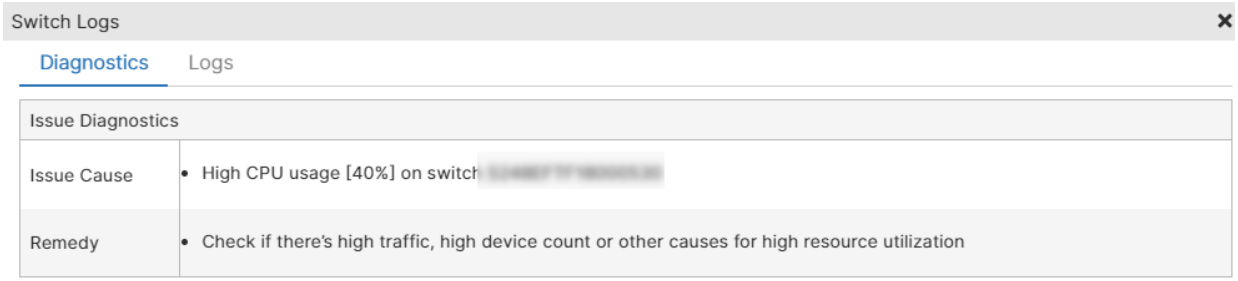


Right-click on the header of the table to select the following columns that you wish to view.

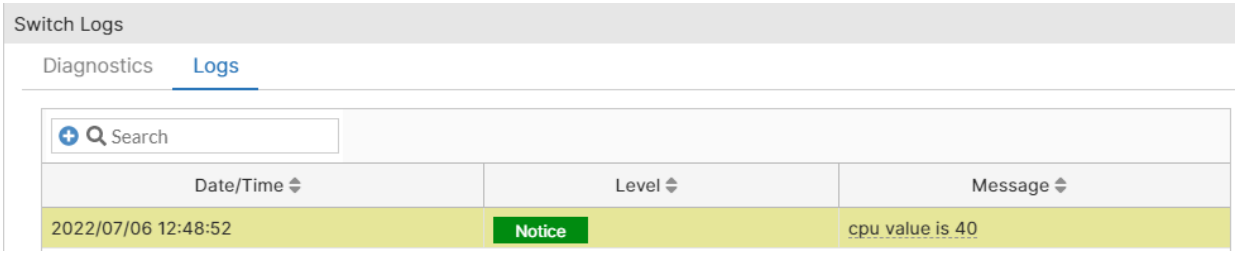
Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
FortiSwitch Name	The name of the impacted switch.
Client MAC Address	The MAC address of the impacted client device.
Hostname	The name of the device as configured by the user. If the name is not configured or available,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

Attribute	Description
FortiGate Serial Number	The serial number of the FortiGate associated with the impacted client.
FortiSwitch Serial Number	The serial number of the impacted switch.

Select a particular switch and click **View Logs**, the issue diagnostics and the suggested remedy are displayed.



The **Logs** tab displays the time stamp of each action, the type of action such as notice, warning, etc., and the impact details are displayed. Different data tabs are displayed based on the selected issue/failure.



Note: The default value for the CPU and memory parameters is 80% and the default value for the temperature is 65 degree Celsius.

Switch Connection Failure

Displays the failed/unsuccessful client connections based on authentication events such as MAC authentication and 801x authentication and MAC learning limit.

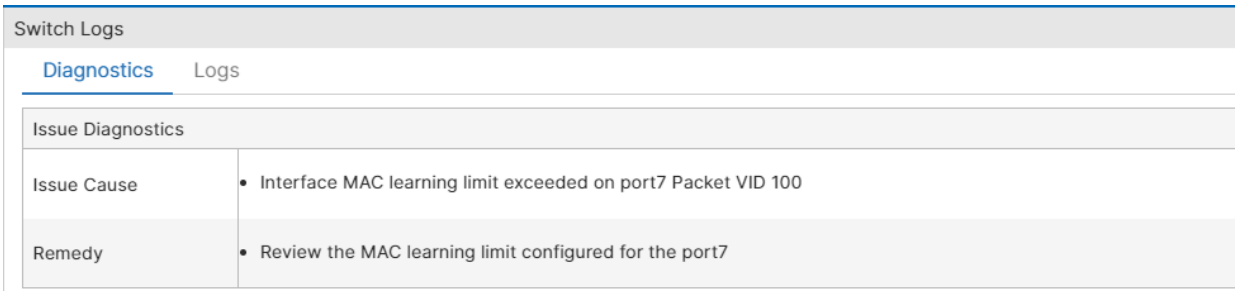
Select a row and click **View Details**. The **Details** table displays the following information.

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

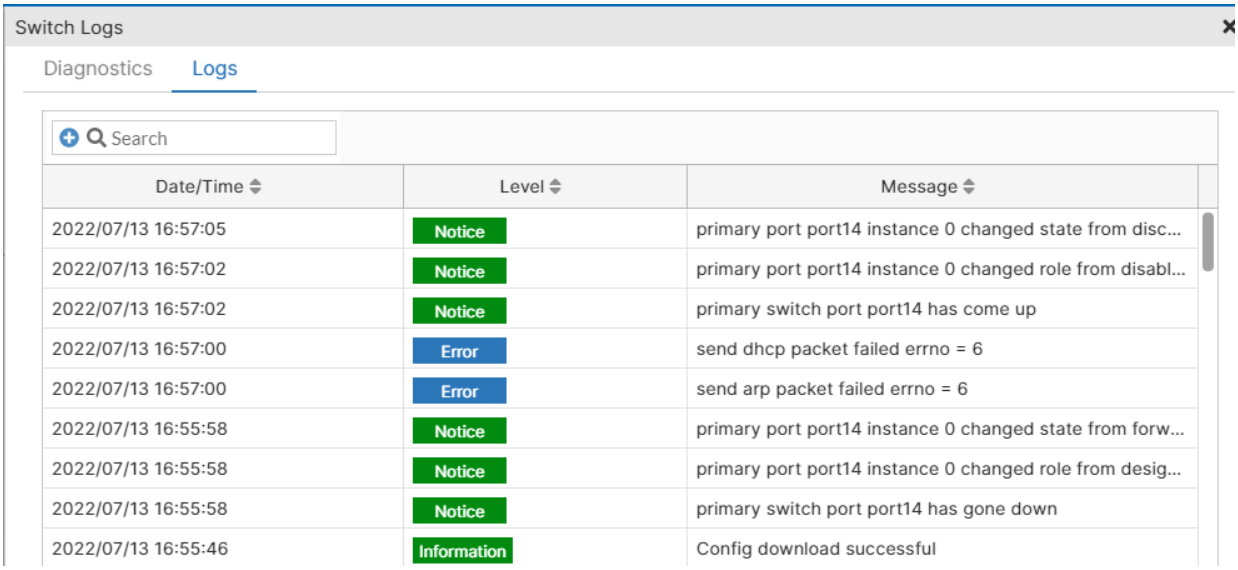
Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
FortiSwitch Name	The name of the impacted switch.
Client MAC Address	The MAC address of the impacted client device.
Hostname	The name of the device as configured by the user. If the name is not configured or available,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

Attribute	Description
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.

Select a particular switch and click **View Logs**, the issue diagnostics and the suggested remedy are displayed.



The **Logs** tab displays the time stamp of each action, the type of action such as notice, warning, etc., and the impact details are displayed. Different data tabs are displayed based on the selected issue/failure.



Note: In the **Switch Logs** > **Diagnostics** tab, if the remedy contains the phrase `cable test`, a **Run Cable Test** button is displayed, to initiate a cable test on the affected port. For more information, see Cable Testing section in FortiSwitch.

SD-WAN

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.

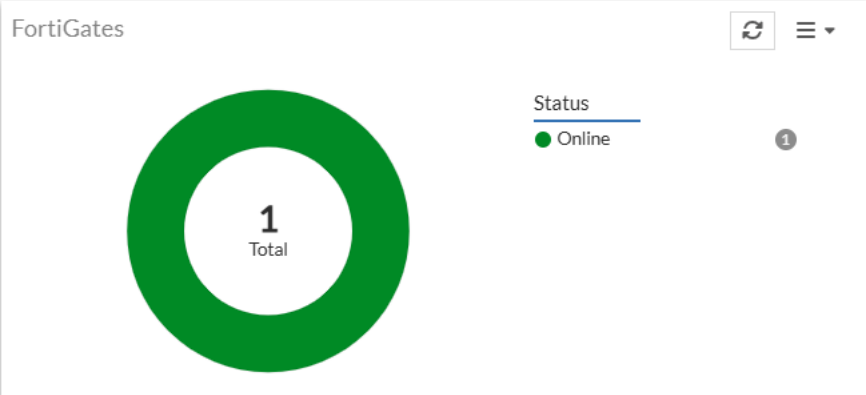
To ensure the charts display accurate values, configure the necessary prerequisites and consider the recommendations provided. If the prerequisites are not configured, both the SD-WAN dashboard and Forecast will appear empty. For more information, see SD-WAN.

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

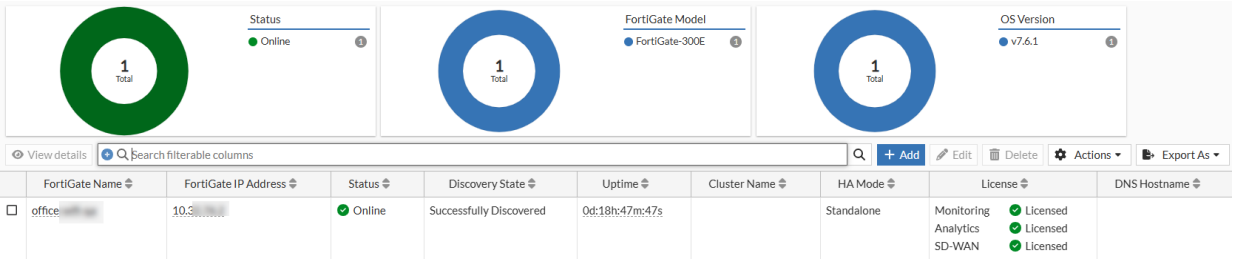
- FortiGates
- SD-WAN Health Overview
- SD-WAN Events
- SD-WAN
- Top SLA Issues
- Top Talkers
- Top Applications

FortiGates

This chart displays the total number of FortiGate controllers in your network and their status (Online/Offline).

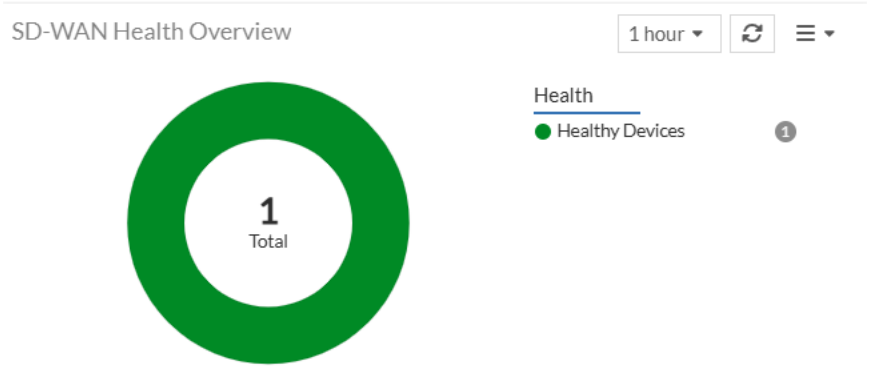


Click the widget to view more details of the FortiGate controllers.



For more information, see Managing FortiGates.

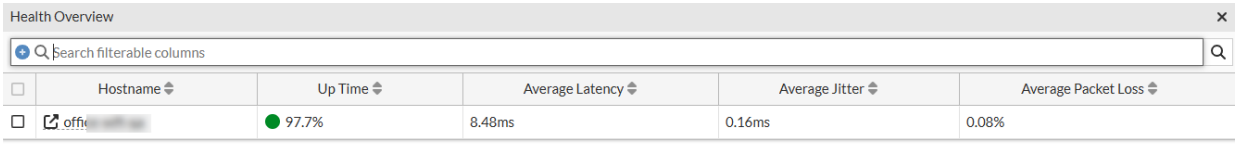
SD-WAN Health Overview



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).

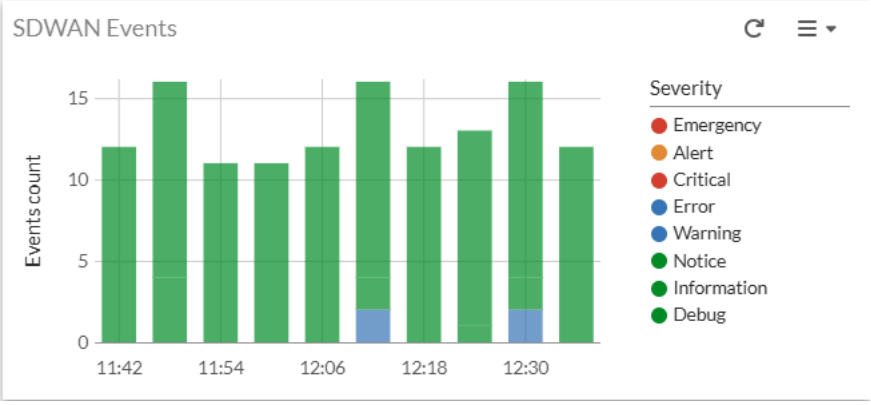
Clicking on each value displays a detailed table with information such as the hostname, up time, average latency, average jitter, and average packet loss.



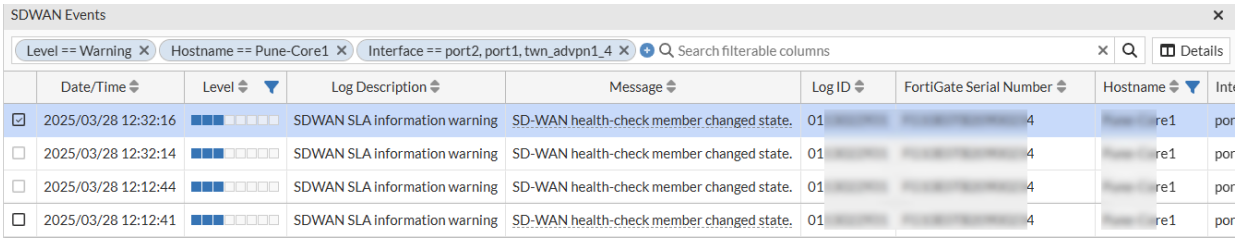
Clicking on a FortiGate name redirects to the **Insights** page, which displays various SD-WAN Insights for the associated interfaces. These insights are derived from the performance of configured health checks and include metrics such as bandwidth usage, SD-WAN rule utilization, application usage, and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

SD-WAN Events

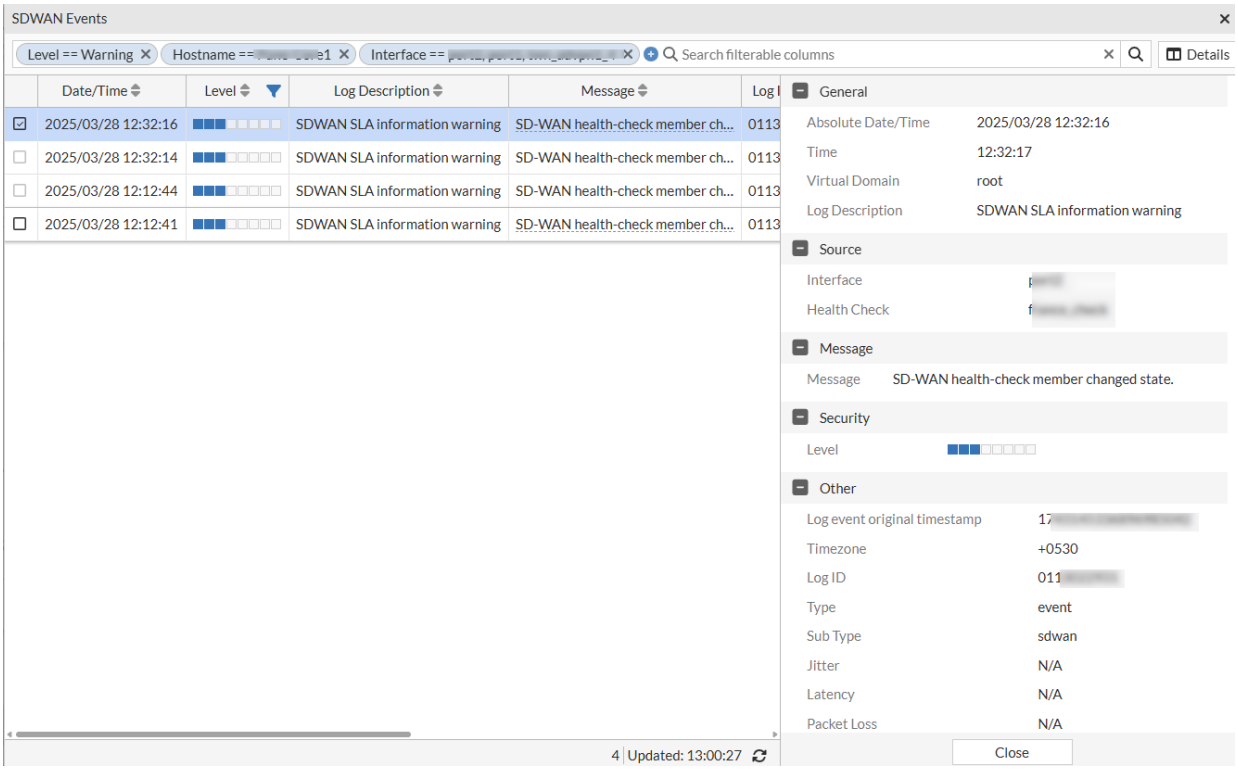
This chart displays the number of SD-WAN events across various severity levels within a specified time frame.



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.

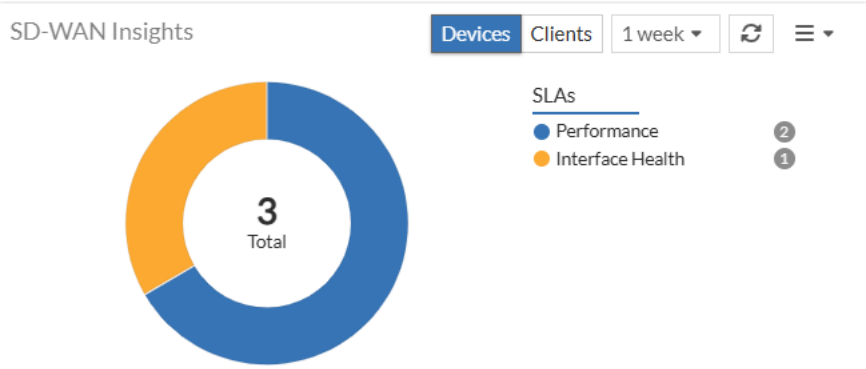


Double-click a row in the detailed table to view further details.



SD-WAN Insights

The SD-WAN panel presents Performance SLA and Interface Health failures for monitored SD-WAN members, including detected issues related to FortiExtender health. It also highlights the affected clients on impacted SD-WAN interfaces. Within each SLA panel, you can select **Clients** to view the number of impacted clients or choose **Devices** to see the count of affected interfaces.



Note: **Devices** option is selected by default.

Topology and Logs

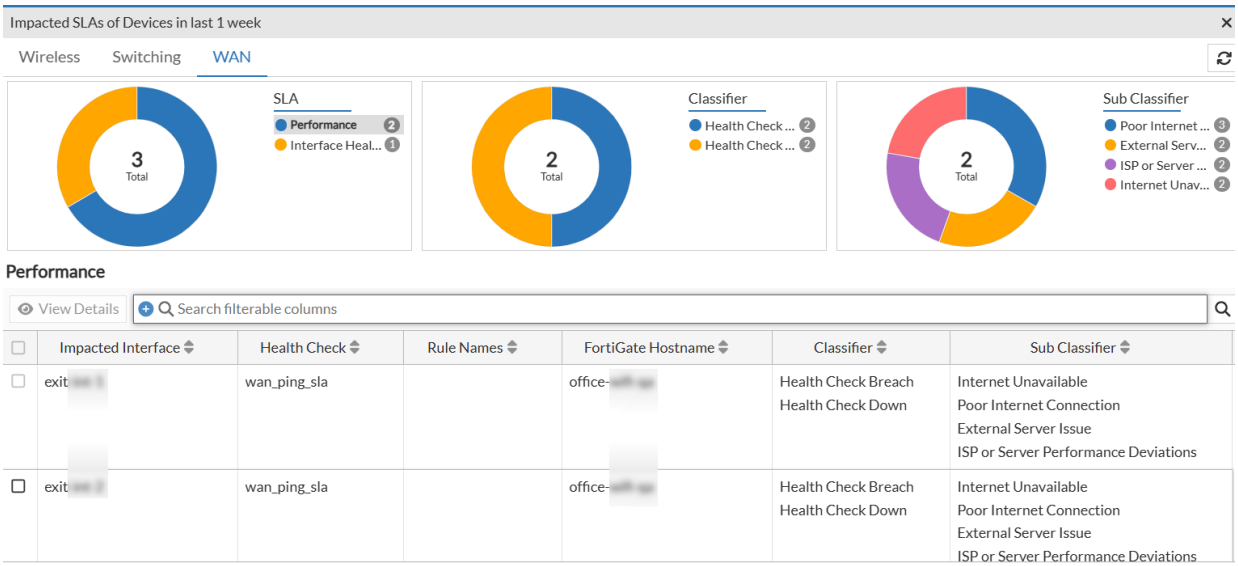
You can click on the impacted SLA listed in the panel to view the **Performance**, **Interface Health** or **FortiExtender Health** impacted interface and client details. The issues reported are categorized based on classifiers and sub-classifiers, with suggested remedial measures. The data displayed in this panel is for the time period set in the dashboard.

Performance SLA

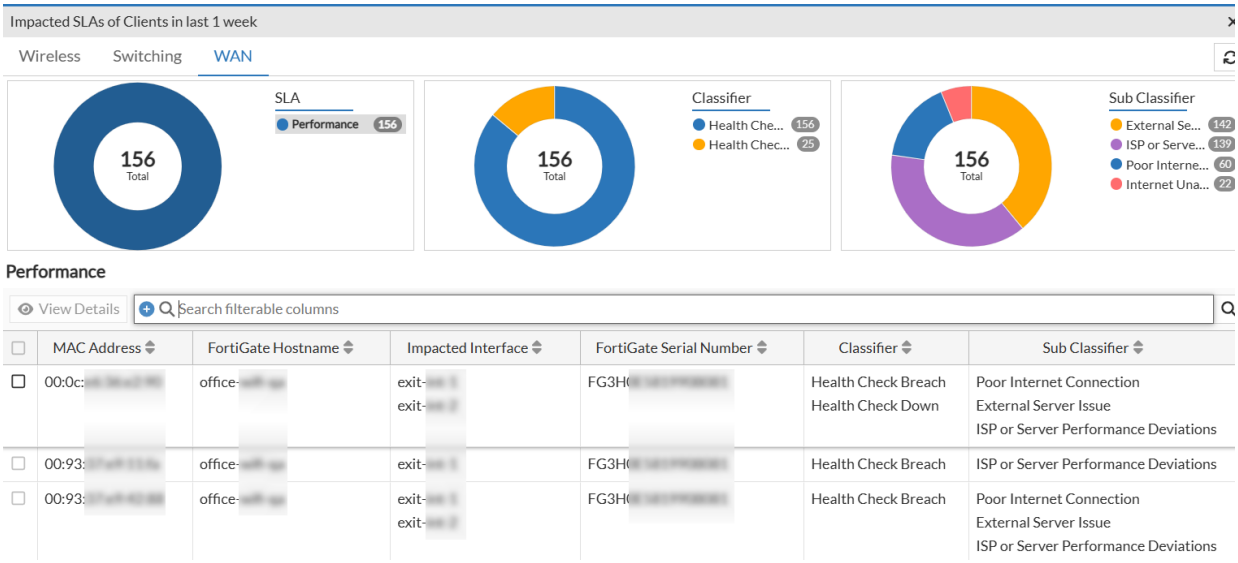
FortiAIOps continuously monitors network performance using Performance SLA to measure key metrics such as latency, jitter, and packet loss. This helps assess the quality of network links, detect Performance SLA configuration issues, and track SD-WAN rule-based failures, reporting SLA breaches when forecasted thresholds are exceeded. By monitoring all health checks on FortiGate devices, FortiAIOps leverages real-time and historical trends to forecast future network performance, enabling proactive optimization.

It is recommended to retain the default configurations for Link Status configuration in FortiGate monitored Performance SLAs. Aggressively configured values may lead to the generation of excessive failure alerts.

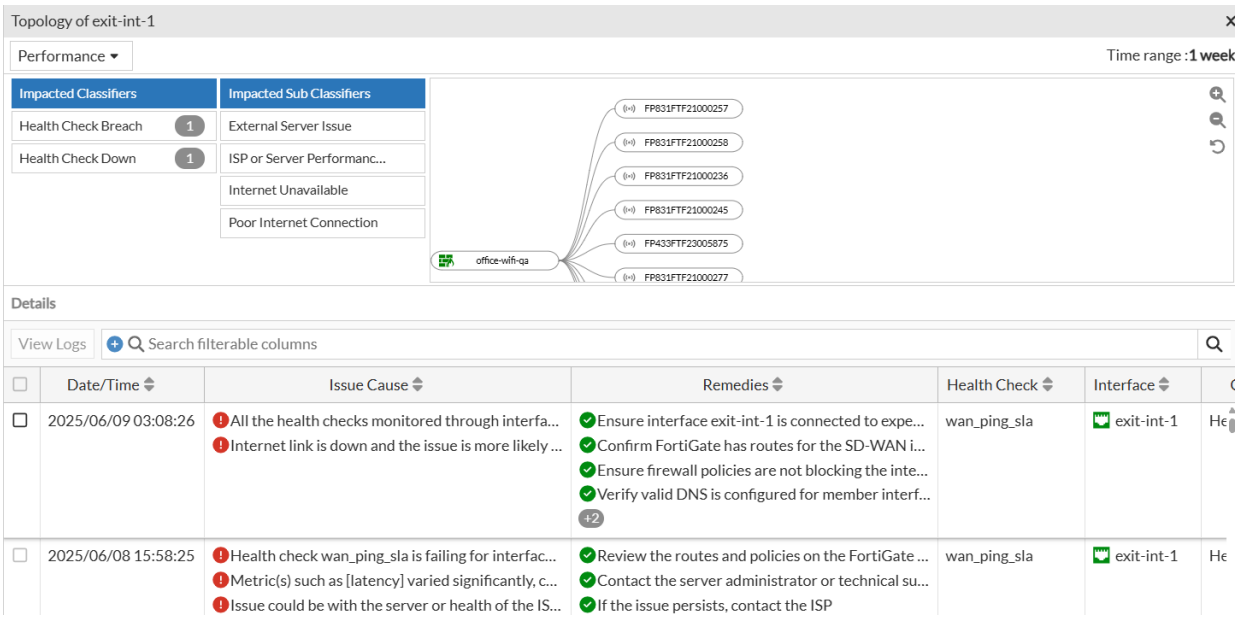
If you select the **Devices** view in the SD-WAN panel and click on the Performance SLA in the impacted SLAs list or click on the bar in the chart, the impacted interfaces' details such as, destination interface, the associated FortiGate host name, IP address, and serial number, FortiSwitch serial number, and classifier and sub-classifier are displayed.



If you select the **Clients** view in the SD-WAN panel and click on the Performance SLA in the impacted SLAs list or click on the bar in the chart, the impacted client details, such as, MAC address, the AP name and serial numbers, the associated FortiGate hostname and serial number, FortiSwitch name and serial number, destination interface, and the classifier and sub-classifers are displayed.



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

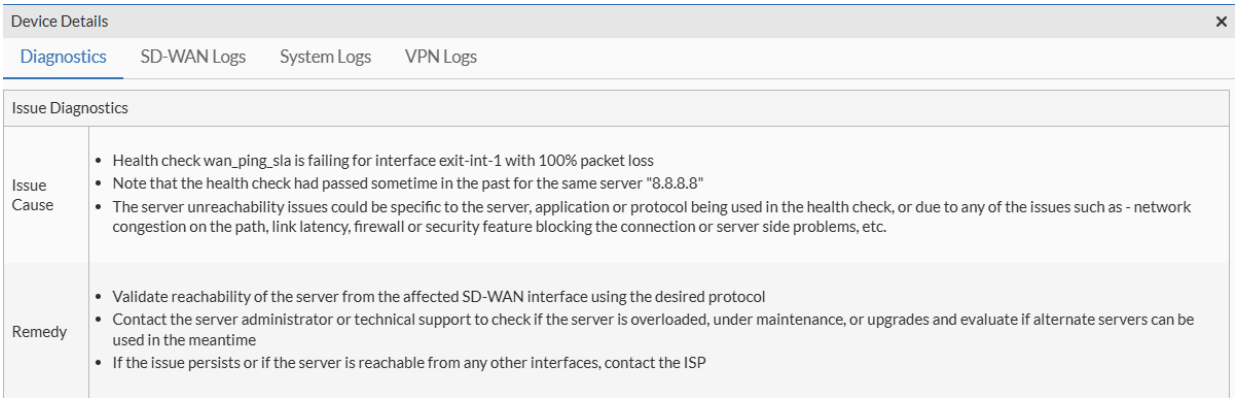


Right-click on the header of the table to select the columns that you wish to view.

Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
Issue Cause List	The detailed causes of the SLA breach that impacted the client/AP/FortiGate.
Remedies	The suggested remedies to resolve the issue.
Health Check	The performance SLA check configured in FortiGate.
Interface	The interface name for the reported issue.
Classifier	The classifier of the issue reported for the SLA.
Sub Classifier	The sub-classifier of the issue for the reported classifier.
Jitter	The amount of jitter (milliseconds) reported for the client.
Packet Loss	The percentage of packet loss reported for the client.
Latency	The amount of latency (milliseconds) reported for the client.
End Timestamp	End time of the impact based on your timezone.
FortiGate Hostname	The hostname of the FortiGate associated with the AP/impacted client.
FortiGate Serial Number	The serial number of the associated FortiGate.
Jitter Dynamic Threshold	Dynamically calculated jitter value based on historical values.
Jitter Max Threshold	Dynamically calculated maximum variation observed in Jitter for the Health check.
Jitter Static Threshold	Jitter SLA target configured in Performance SLA or FortiAIOps Default target.

Attribute	Description
Latency Dynamic Threshold	Dynamically calculated Latency value based on historical values.
Latency Max Threshold	Dynamically calculated maximum variation observed in Latency for the Health check.
Latency Static Threshold	Latency SLA target configured in Performance SLA or FortiAIOps Default target.
Packet Dynamic Threshold	Dynamically calculated Packet loss value based on historical values.
Packet Max Threshold	Dynamically calculated maximum variation observed in Packet loss for the Health check.
Packet Static Threshold	Packet loss SLA target configured in Performance SLA or FortiAIOps Default target.
Rule Name	The name of the rule to track the interface failure.
Status	Status of the interface.

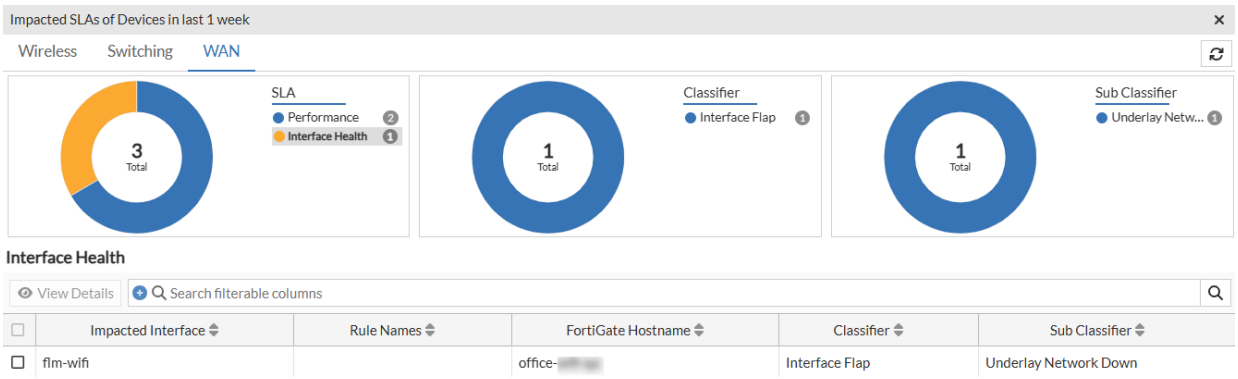
Select a row from the table and click **View Logs** to view further details.



The **Diagnostics** tab details identified issues and provides steps for rectification. For more in-depth logs, navigate to the **SD-WAN Logs**, **System Logs**, or **VPN Logs** tabs.

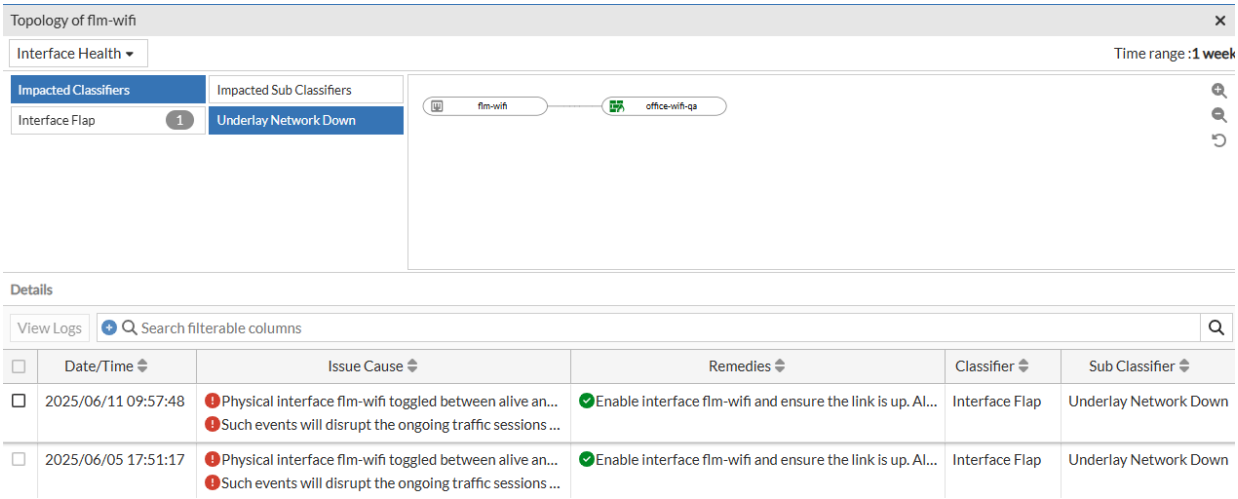
Interface Health SLA

Interface Health SLA in FortiAIOps focuses on monitoring the stability and reliability of both underlay and overlay network links. It detects link status changes and interface flaps to ensure consistent network performance. Additionally, FortiAIOps evaluates the interface selection strategies defined in SD-WAN rules, helping to identify the most efficient path for traffic. This ensures seamless connectivity and aids in optimizing SD-WAN configurations for maximum performance and reliability.



The Interface Health table displays information such as Impacted Interface, Rule Names, FortiGate Hostname, Classifier, Sub Classifier, AP List, FortiExtender Name, FortiExtender Serial, FortiGate IP Address, FortiGate Serial Number, FortiSwitch Serial Number, and Health Check.

To get detailed information, select the impacted interface and click **View Details**.

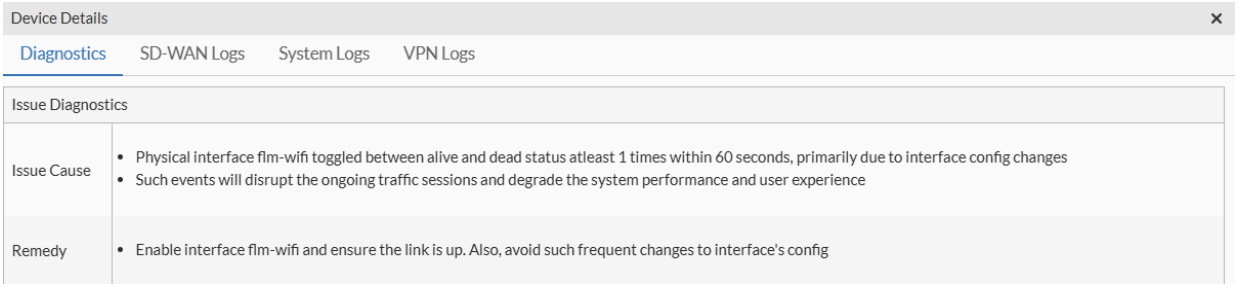


Right-click on the header of the table to select the columns that you wish to view.

Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
Issue Cause	The detailed causes of the SLA breach that impacted the client/AP/FortiGate.
Remedies	The suggested remedies 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.
End Timestamp	End time of the impact based on your timezone.
In Bandwidth	Bandwidth of the incoming data.
Interface	The interface name for the reported issue.
Out Bandwidth	Bandwidth of the outgoing data.

Attribute	Description
Rule Name	The name of the rule to track the interface failure.
Tunnel Interface	Name of the tunnel interface.

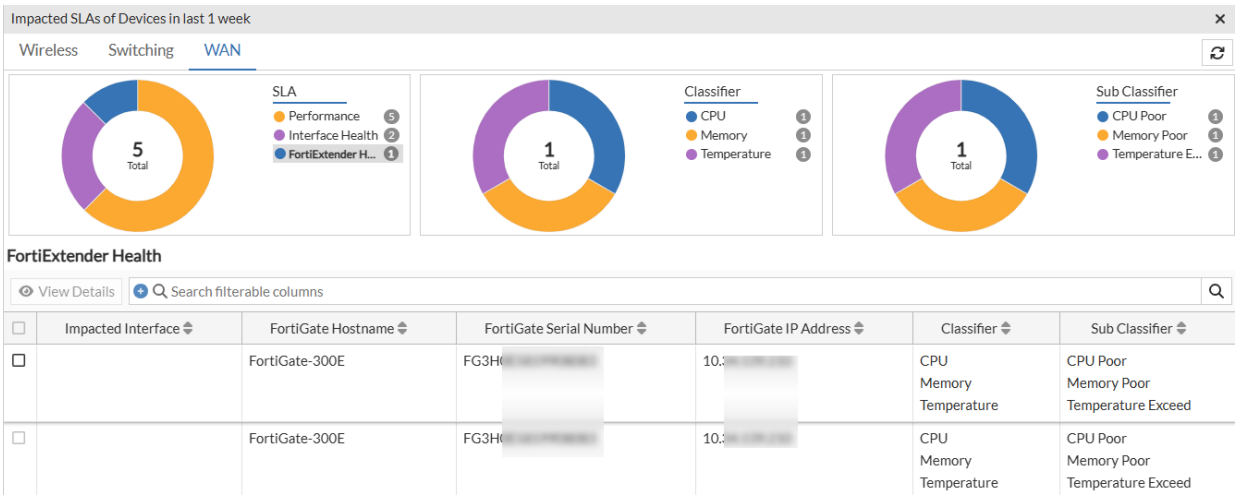
Select a row and click **View Logs** to view detailed logs for the issue.



The **Diagnostics** tab details identified issues and provides steps for rectification. For more in-depth logs, navigate to the **SD-WAN Logs**, **System Logs**, or **VPN Logs** tabs.

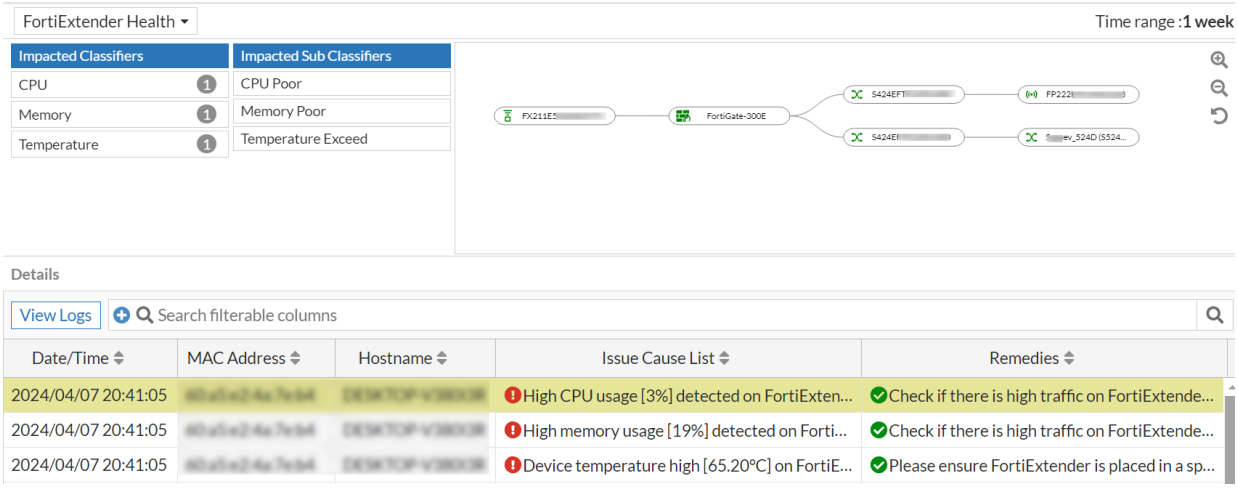
FortiExtender Health SLA

If you select the **Devices** view in the SD-WAN panel and click on the FortiExtender Health SLA in the impacted SLAs list or click on the bar in the chart, the impacted interfaces' details such as, destination interface, AP serial number, the associated FortiGate host name, IP address, and serial number, FortiSwitch serial number, FortiExtender name and serial number, and classifier and sub-classifier are displayed.



If you select the **Clients** view in the SD-WAN panel and click on the FortiExtender Health SLA in the impacted SLAs list or click on the bar in the chart, the impacted client details, such as, MAC address, the AP name and serial number, the associated FortiGate hostname and serial number, FortiSwitch name and serial number, FortiExtender name and serial number, destination interface, and the classifier and sub-classifers are displayed.

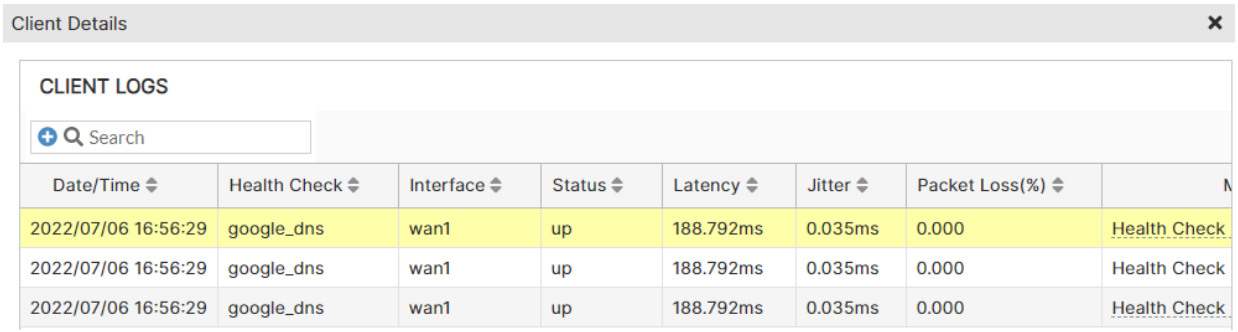
Select a row and click **View Details**. The **Details** table displays the following information.



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

Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
FortiGate Serial Number	The serial number of the associated FortiGate.
AP Serial	The serial number of the associated AP.
Access Point	The name of the associated AP.
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	The detailed cause of the SLA breach that impacted the client/AP/FortiGate/FortiExtender.
Remedies	The suggested remedies 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.
Source and Destination Interface	The SD-WAN interface name.
FortiSwitch Serial Number	The serial number of the impacted switch.
FortiSwitch Name	The name of the impacted switch.
FortiExtender Serial Number	The serial number of the impacted FortiExtender.
FortiExtender Name	The name of the impacted FortiExtender.
FortiGate Hostname	The hostname of the FortiGate with which the impacted FortiExtender is associated.
Client Type	The client type that is impacted, wireless or wired.

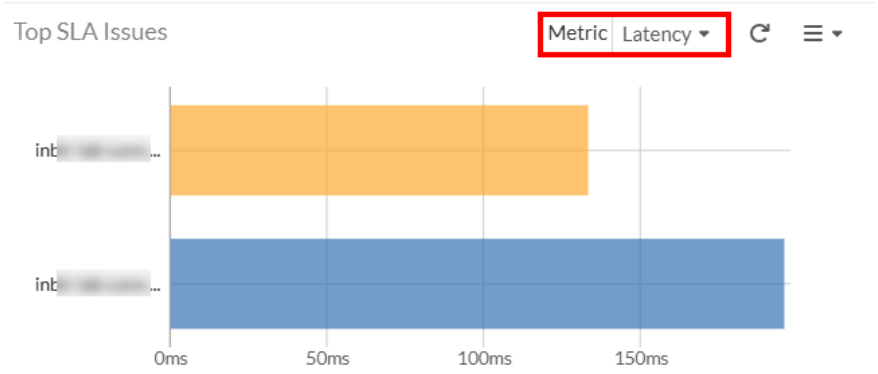
Select a particular client and click **View Logs**, to view the impacted client logs.



Top SLA Issues

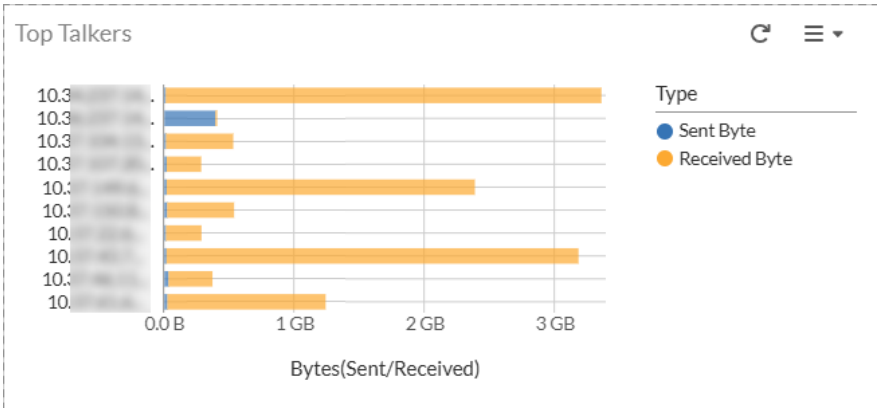
This chart displays the top 10 worst SD-WAN performance values for each metrics for Interfaces—Latency, Jitter, and Packet Loss for the selected time period.

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



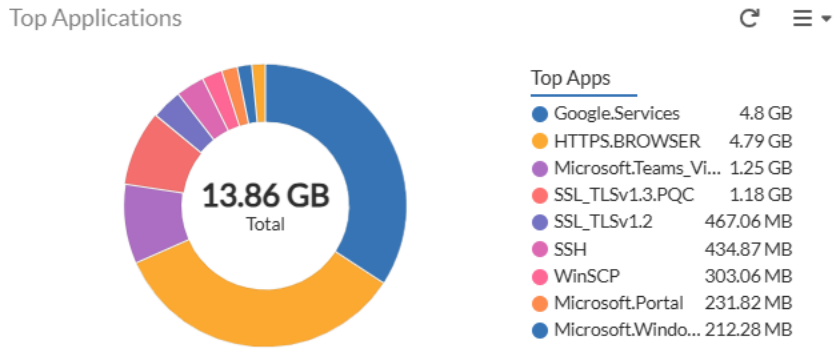
Top Talkers

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.



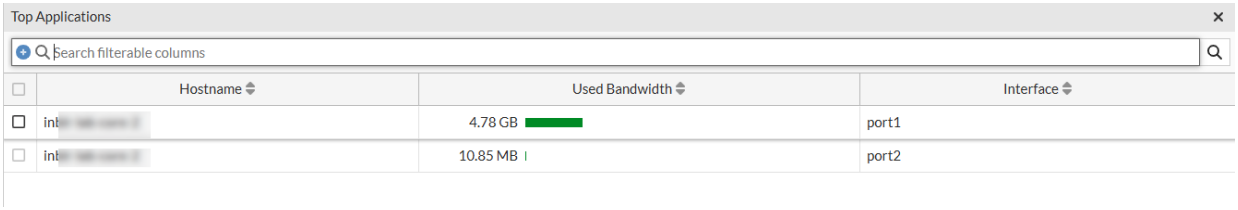
Top Applications

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.



Custom Dashboard

You can customize your dashboard experience—modify existing layouts by adding or deleting widgets, or create entirely new dashboards with your preferred widgets.

The following customizations are available:

- Creating a New Dashboard
- Modifying an Existing Dashboard
- Deleting a Dashboard
- Rearranging the Dashboards
- Resetting the Dashboard Section

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

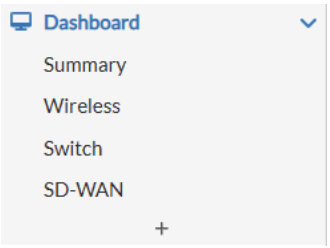
The widget library has also been improved for a more seamless user experience. For more information, see Managing Dashboard Widgets.

Creating a New Dashboard

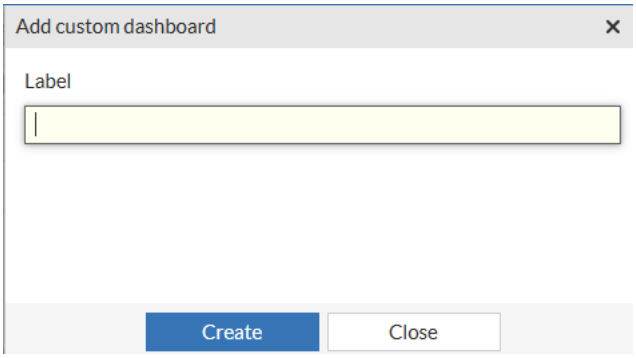
You can now create new custom dashboards and add widgets from the widget library.

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 Modifying an Existing Dashboard.

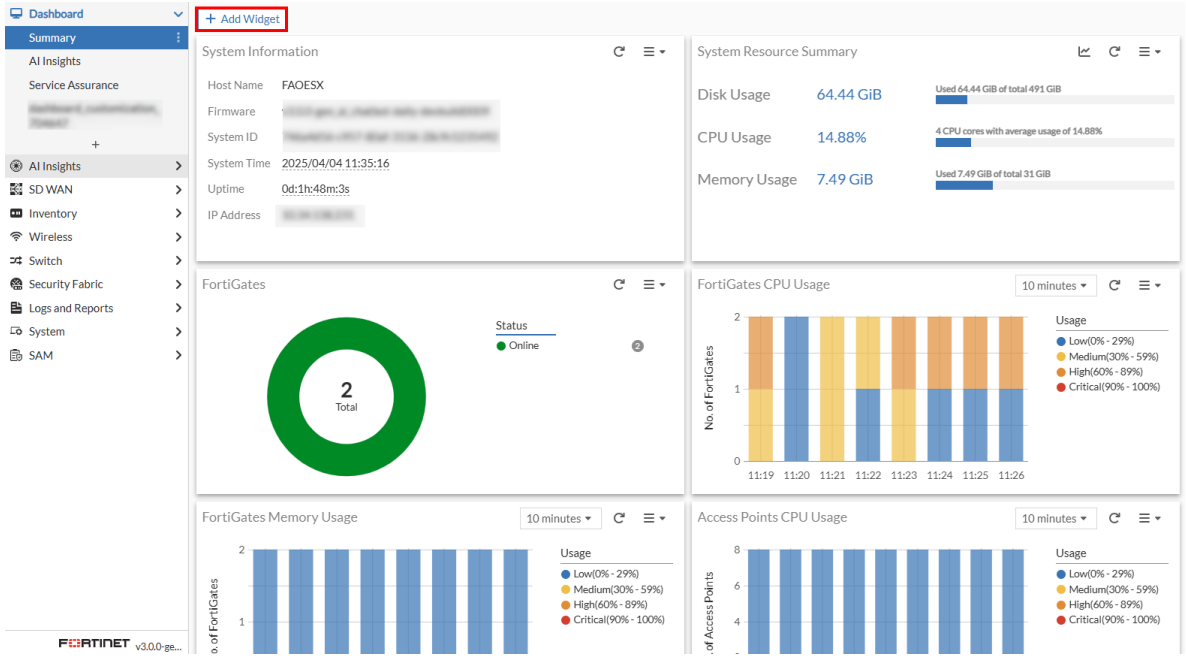
Modifying an Existing Dashboard

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:

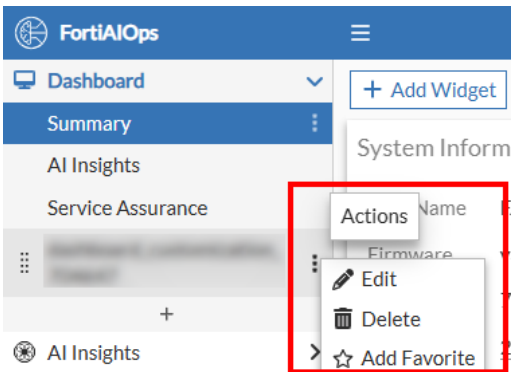
1. Select the dashboard you want to modify.
2. Click **Add Widget** to add required widgets from the widget library.



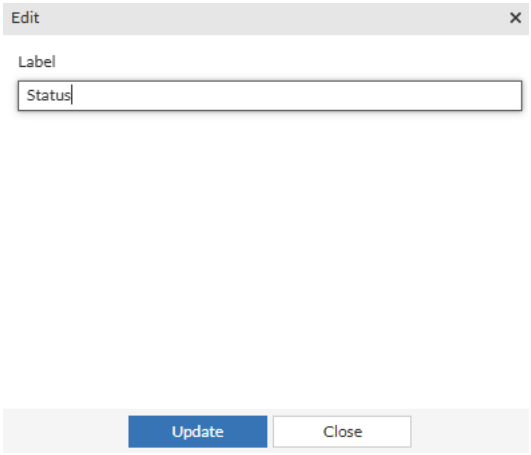
3. In the the **Manage Dashboard Widgets** pane, hover on the widget name to select the required widget and click +.
   For more information on widget library, see Managing Dashboard Widgets
4. Click **Close** to close the pane once the widgets are selected.
5. Click **Reset dashboard layout** to clear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



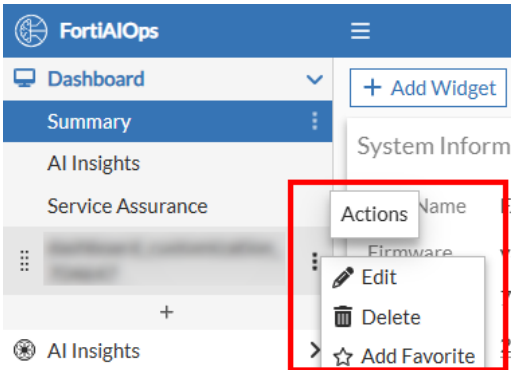
2. Change the name of the dashboard in the **Label** field and click **Update**.



Deleting 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.

Rearranging the Dashboards

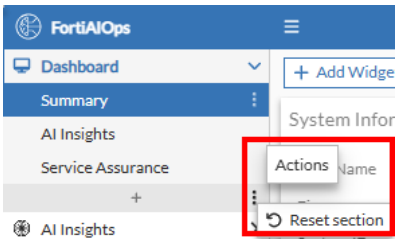
You can move a dashboard up or down to rearrange the dashboard list.

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

Resetting the Dashboard Section

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

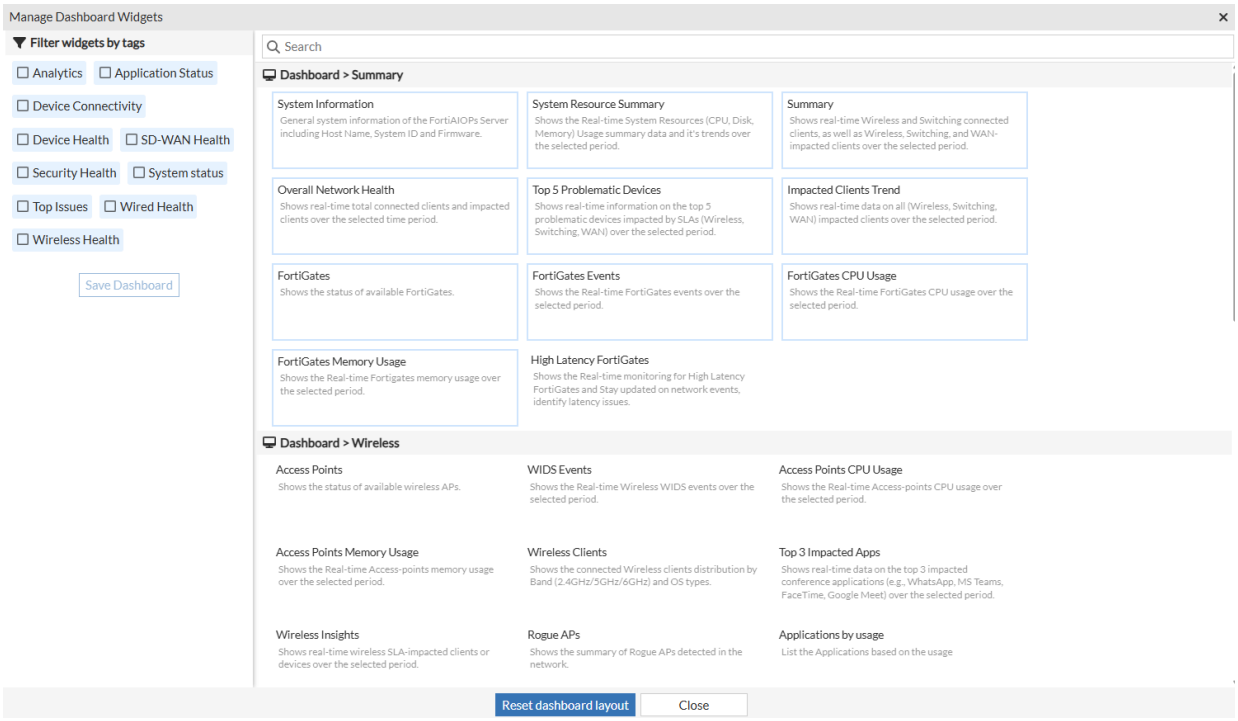
Hover over **+** and from the **Actions** menu, click **Reset section**.



Managing Dashboard Widgets

The Manage Dashboard Widgets window 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.

Use the filters on the left pane to quickly locate the widgets you are looking for.



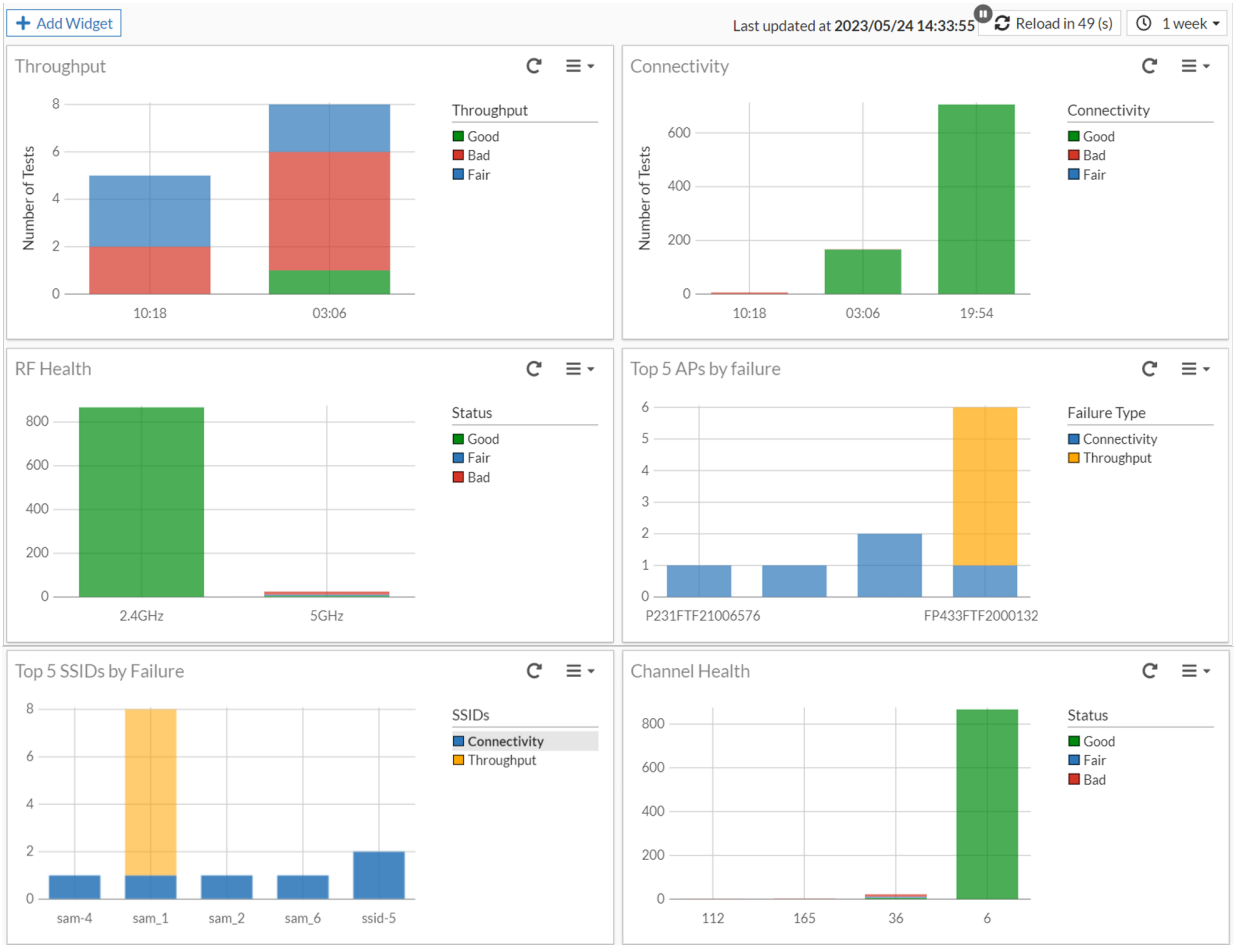
To clear all the widgets added to the dashboard, click **Reset dashboard layout**.

The widgets are categorized into the following sections:

- Summary
- Wireless
- Switch
- SD-WAN
- Applications
- Licensing
- Service Assurance

Service Assurance

The Service Assurance dashboard for FortiAIOps is designed to provide comprehensive insights and monitoring of network performance. It consists of various widgets that offer visual representations and classifications of different metrics.

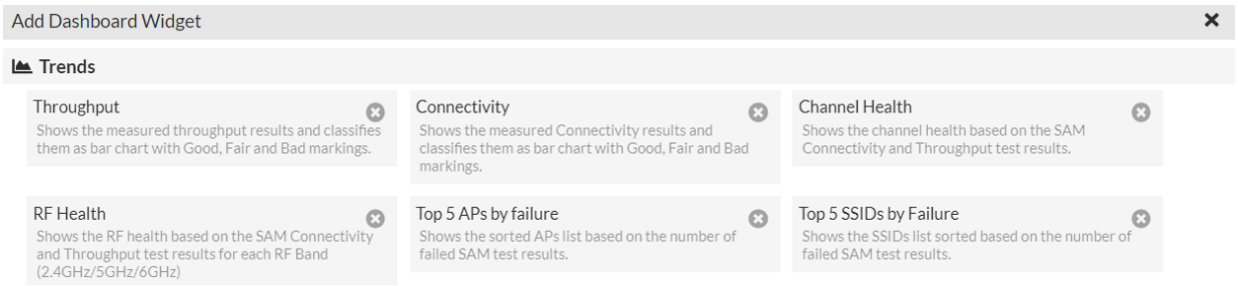


The data on this dashboard is based on scheduled test results and is automatically refreshed every 60 seconds; the following options are available to manage the auto-refresh feature for this page.

- Click to manually refresh data.
- Click to pause the auto-refresh.
- Click to resume the auto-refresh.
- Select the time range from the drop-down. Choose from 10 minutes, 1 hour, 4 hours, 6 hours, 1 day, 1 week.

The dashboard provides an option to select the duration of the data displayed. You can choose between 1 day, 1 week, 1 hour, and 10 minutes.

Use the **Add Widget** option to manage the widgets displayed on the dashboard; you can choose to add or remove the widgets.



The following widgets provide network data on this dashboard.

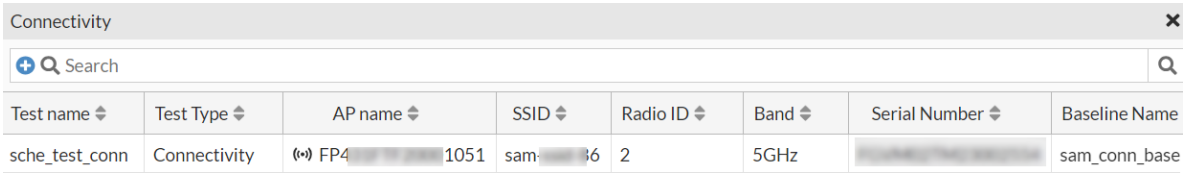
- **Throughput** - This widget displays the measured throughput results of your network. Throughput refers to the amount of data transferred through the network over a given time period. It presents the data in the form of a bar chart, indicating the performance levels as *Good, Fair*, or *Bad*. Click on the charts to view additional information.

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

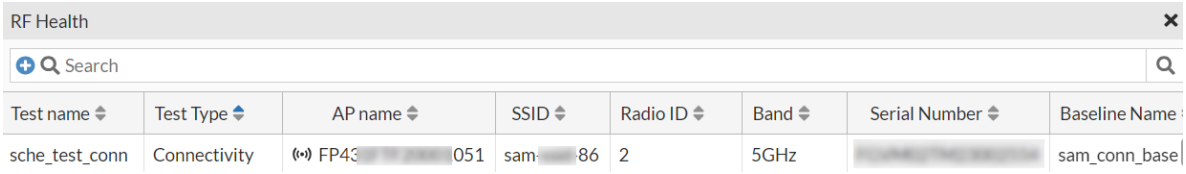
Attribute	Description
Test Name	The name of the associated test.
Test Type	The type of test, *throughput* or *connectivity*.
AP Name	The name of the access point used during the test.
SSID	The SSID associated with the network.
Radio ID	The associated radio ID .
Band	The frequency band utilized, *2.5 GHz* or *5 GHz*.
Serial Number	The serial number of the associated FortiGate.
Baseline Name	The name of associated baseline.
Channel	The channel number utilized.
Status	The status of the test, *Good, Fair*, or *Bad*.
Start Time	The timestamp indicating when the test was initiated.

Attribute	Description
Packet Loss	The amount of data lost during transmission, expressed as a percentage.
Throughput	The measured network throughput, indicating the amount of data transferred.

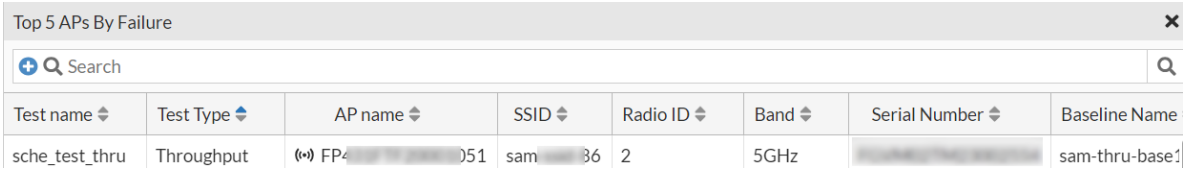
- **Connectivity** - This widget displays the measured Connectivity results using a bar chart and classifies the results as *Good, Fair,* or *Bad*. Connectivity refers to the ability of devices to establish and maintain a connection to the network.Click on the charts to view additional information.



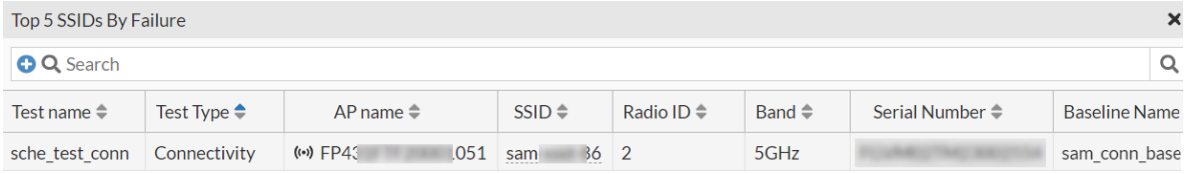
- **RF Health** - This widget displays the radio frequency (RF) health based on the Service Assurance Manager (SAM) Connectivity and Throughput test results for each RF Band(2.4GHz/ 5GHz). Click on the charts to view additional information.



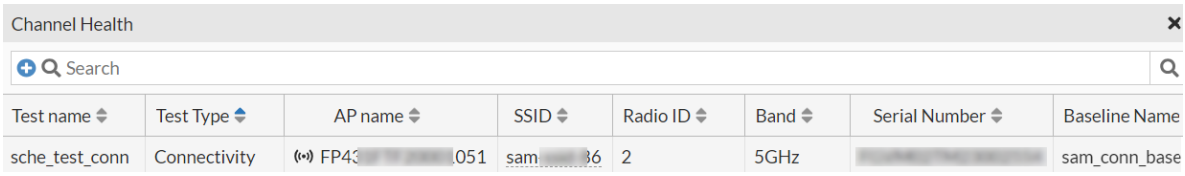
- **Top 5 APs by Failure** - This widget displays a sorted list of Access Points (APs) based on the highest number of bad results. Click on the charts to view additional information.



- **Top 5 SSIDs by Failure** - This widget displays a sorted list of SSIDs based on the highest number of bad results. Click on the charts to view additional information.



- **Channel Health** - This widget displays the overall health of the network channels based on the SAM Connectivity and Throughput test results. Click on the charts to view additional information.



AI Insights

This section describes the FortiAIOps AI enabled data insights of your network and SLA configurations.

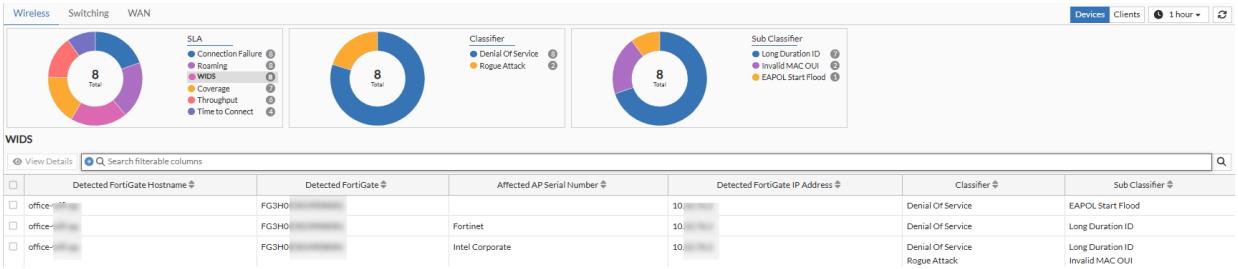
- Impacted SLA
- Impacted Devices
- SLA Config

Impacted SLA

This page displays the impacted wireless, switching, and WAN clients, categorized based on their SLAs, classifiers, and sub-classifiers. Select any SLA and the associated classifier and sub-classifier charts are displayed. You can filter and view the SLAs as per any of these categories. In each impacted SLA panel for wireless, switching, and WAN, you can select **Clients** to view the impacted client count or click **Devices** to view the impacted device count. Navigate to **AI Insights > Impacted SLA**.

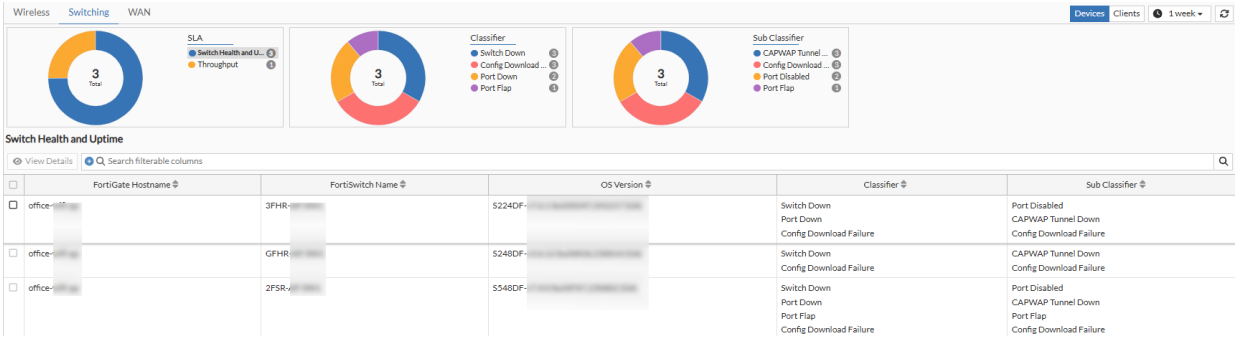
Wireless

The wireless SLA data is reported based on the classifiers and sub-classifiers displayed in this panel. The SLA data tables lists the client MAC address and hostname, FortiGate hostname and serial number, AP name, IP address, and serial number, classifier and sub-classifier, the associated SSID, and the operating channel. Select any row and click on **View Details** to view the impacted SLA details.



Switching

The switching SLA data is reported based on the classifiers and sub-classifiers listed displayed in this panel. The SLA data tables lists the client MAC address and hostname, FortiGate hostname and serial number, FortiSwitch name, serial number, and OS version, classifier and sub-classifier, FortiSwitch state and status (online/offline). Select any row and click on **View Details** to view the impacted SLA details.

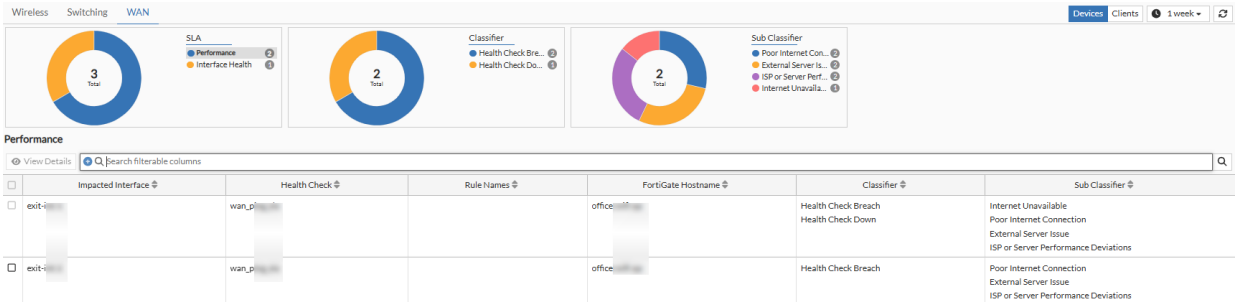


WAN

The SD-WAN SLA monitoring makes use of sub-classifiers for deep insight into critical performance issues. Using real-time logs and statistical data from FortiGate devices, these sub-classifiers allow for more precise identification and resolution of potential challenges, enhancing network reliability and efficiency. The monitoring incorporates use-case specific classifications for performance SLAs, interface health SLAs and SD-WAN rule [Service] based SLAs in the SD-WAN network. This enables to identify a wider range of performance and interface related problems within the SD-WAN network

The WAN SLA data is reported based on the classifiers and sub-classifiers displayed in this panel. The SLA data tables lists the Impacted Interface, Health Check, Rule Name, FortiGate Hostname, Classifier, and Subclassifier.

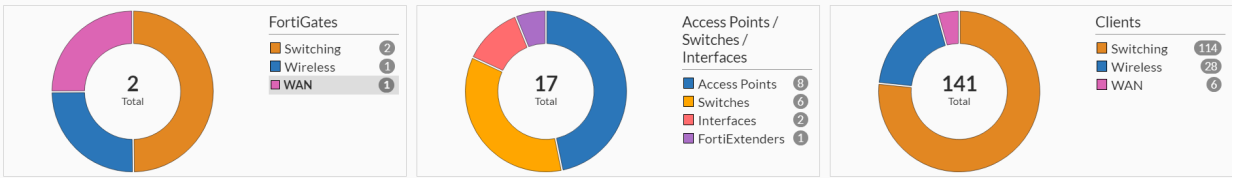
Note: To ensure the charts display accurate values, configure the necessary prerequisites and consider the recommendations provided. For more information, see SD-WAN.



Select any device listed in the tables and click on **View Details** for topology and other details. For details on the SLAs, topology, and logs, see SD-WAN.

Impacted Devices

This page displays details of the various devices in your network that are associated with impacted clients, that include the wireless, switching, and WAN clients. You can view and analyze the SLA data based on the device type. The data is displayed in the following three panels. The number of devices are listed for each category, you can click on any of these or click on the respective section in the donut chart to view details. Navigate to **AI Insights > Impacted Devices**.



FortiGates

Displays the number of deployed FortiGate controllers with impacted wireless, switching, and WAN clients.

The following example displays the *FortiGates-Wireless SLA* with information such as FortiGate host name, serial number, and IP address, and lists the impacted APs, clients, and SLAs. Select any row and click on the impacted SLA name to view the topology. Data is displayed for FortiGate wireless clients based on the selected SLA breaches only.

FortiGates Wireless SLA

Search filterable columns

Impacted SLAs	FortiGate Serial Number	IP Address	Impacted APs	Impacted Clients
FGVM04 6				
Connection Failure	FGVM04TM23010456	10.34.159.207	7	14
Time to Connect	FGVM04TM23010456	10.34.159.207	7	13
Throughput	FGVM04TM23010456	10.34.159.207	7	12

The following example displays the *FortiGates-WAN SLA* with information such as FortiGate host name, serial number, and IP address, and lists the impacted APs, clients, SLAs, switches, and interfaces. Select any row and click on the impacted SLA name to view the topology.

FortiGates WAN SLA

Search filterable columns

Impacted SLAs	FortiGate Serial Number	IP Address	Impacted APs	Impacted Switch	Impacted Interfaces	Impacted Clients	Extenders
FortiGate-300E 2							
Performance	FG340E5819908083	10.34.139.210	7	1	2	6	0
FortiExtender Health	FG340E5819908083	10.34.139.210	6	1	1	4	1

The following example displays the *FortiGates-Switching SLA* with information such as FortiGate host name, serial number, and IP address, and lists the impacted clients, SLAs, and switches. Select any row and click on the impacted SLA name to view the topology.

FortiGates Switching SLA

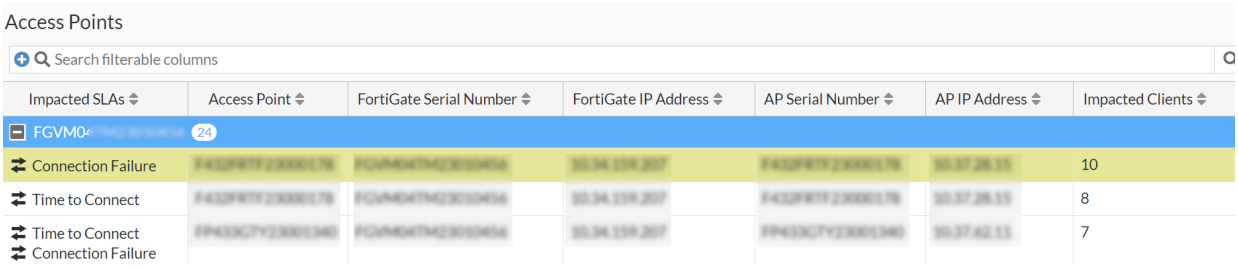
Search filterable columns

Impacted SLAs	FortiGate Serial Number	IP Address	Impacted Switch	Impacted Clients
1				
Switch Health and Uptime	FG200ETK18914993		1	5
FGT_BACKUP_182 1				
Switch Health and Uptime	FGVM04TM24002042	10.34.159.181	1	12
FGT_PRIMARY_181 1				

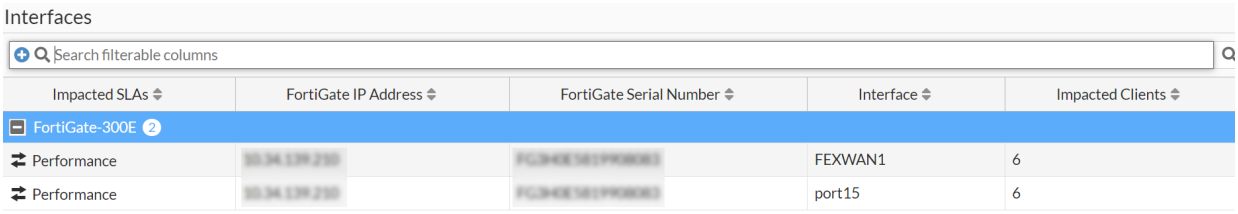
Access Points/ Switches/ Interfaces/FortiExtenders

Displays the number of devices, that is, APs, SD-WAN interfaces, FortiExtenders, and switches with impacted clients.

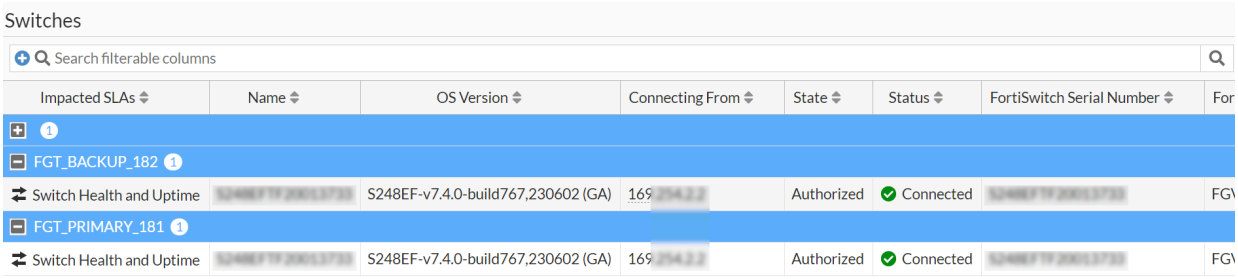
The following example displays the *Access Points* with information such as AP name, serial number, and IP address, FortiGate host name and IP address, and lists the impacted clients and SLAs. Select any row and click on the impacted SLA name to view the topology.



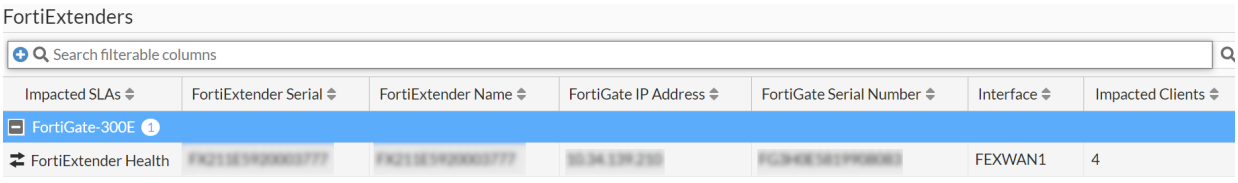
The following example displays the *Interfaces* with information such as the interface, FortiGate host name, serial number, and IP address, and lists the impacted clients and SLAs. Select any row and click on the impacted SLA name to view the topology.



The following example displays the *Switches* with information such as the switch host name, IP address, OS version, and serial number, FortiGate host name, serial number, and IP address, and lists the impacted clients and SLAs along with the status and state of the switch. Select any row and click on the impacted SLA name to view the topology.



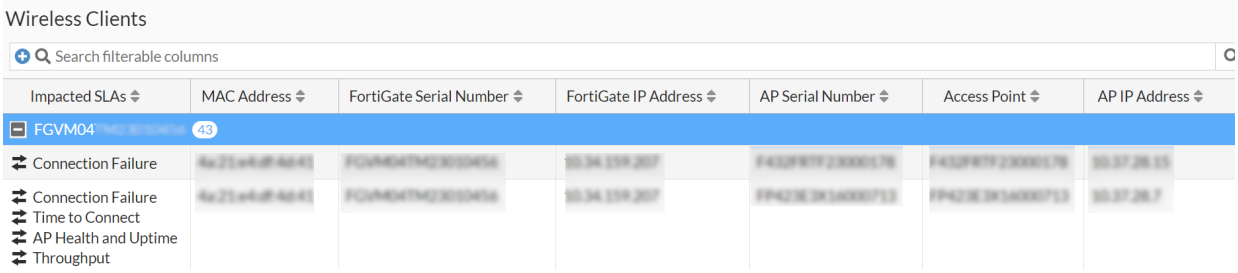
The following example displays the *FortiExtenders* with information such as the interface, FortiGate host name, and FortiExtender name, and lists the impacted clients and SLAs. Select any row and click on the impacted SLA name to view the topology.



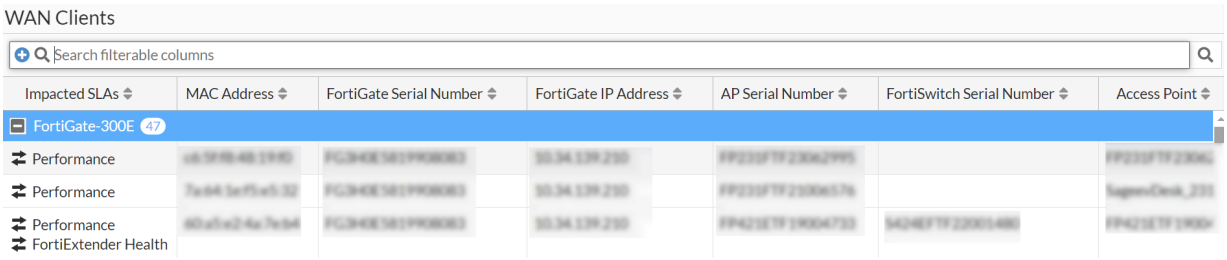
Clients

Displays the number of impacted clients for the wireless, switching, and WAN.

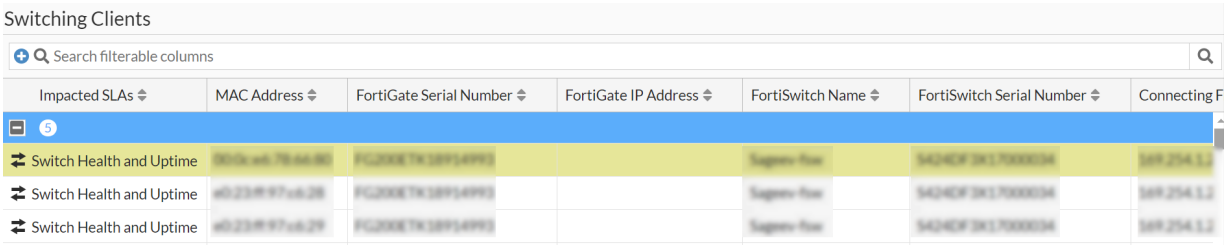
The following example displays the *Wireless Clients* with information such as the FortiGate host name, serial number, and IP address, AP name and IP address, client MAC address, and the impacted SLAs. Select any row and click on the impacted SLA name to view the topology.



The following example displays the *WAN Clients* with information such as the FortiGate host name, serial number, and IP address, AP name, IP address, and serial number, switch name, IP address, and serial number, client MAC address, interface details, and the impacted SLAs. Select any row and click on the impacted SLA name to view the topology.



The following example displays the *Switching Clients* with information such as the FortiGate host name, serial number, and IP address, switch name, IP address, OS version, state, and status, client MAC address, and the impacted SLAs. Select any row and click on the impacted SLA name to view the topology.



SLA Config

This section explains how to configure SLA metrics to define values to match network deployment and required thresholds. Navigate to **AI Insights > SLA Config**.

- Device Health
- Time To Connect
- Roaming

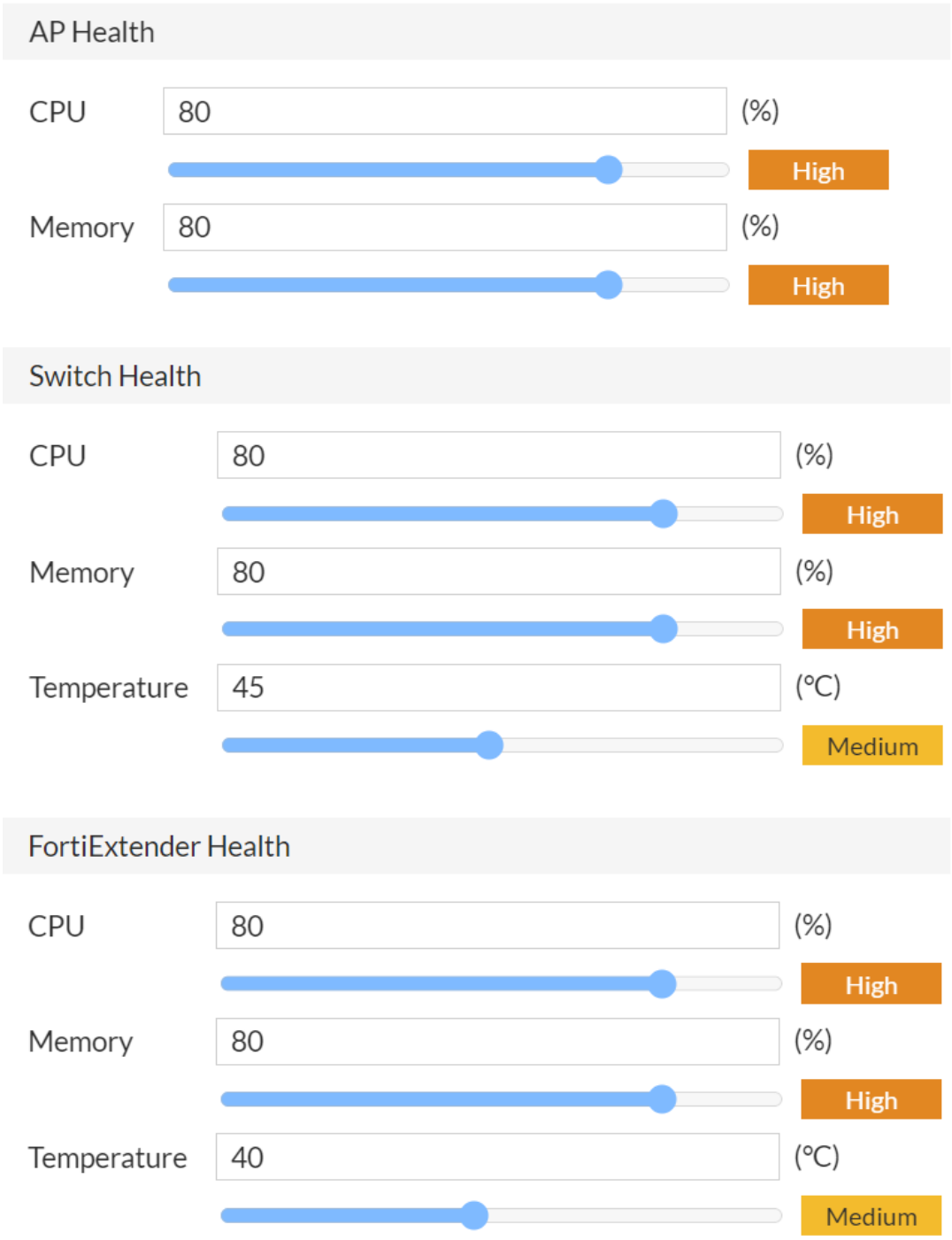
Device Health

Configure AP, switch, and FortiExtender health SLA threshold values. The AP health is displayed in the *AP Health and Uptime* SLA of the Wireless section, the switch health is displayed in the *Switch Health and Uptime* SLA of the Switching section, and the FortiExtender health is displayed in the *FortiExtender Health* SLA of the WAN section.

Navigate to **AI Insights > SLA config > Device Health** to configure the following parameters.

- **CPU** usage
- **Memory** usage

- **Temperature**



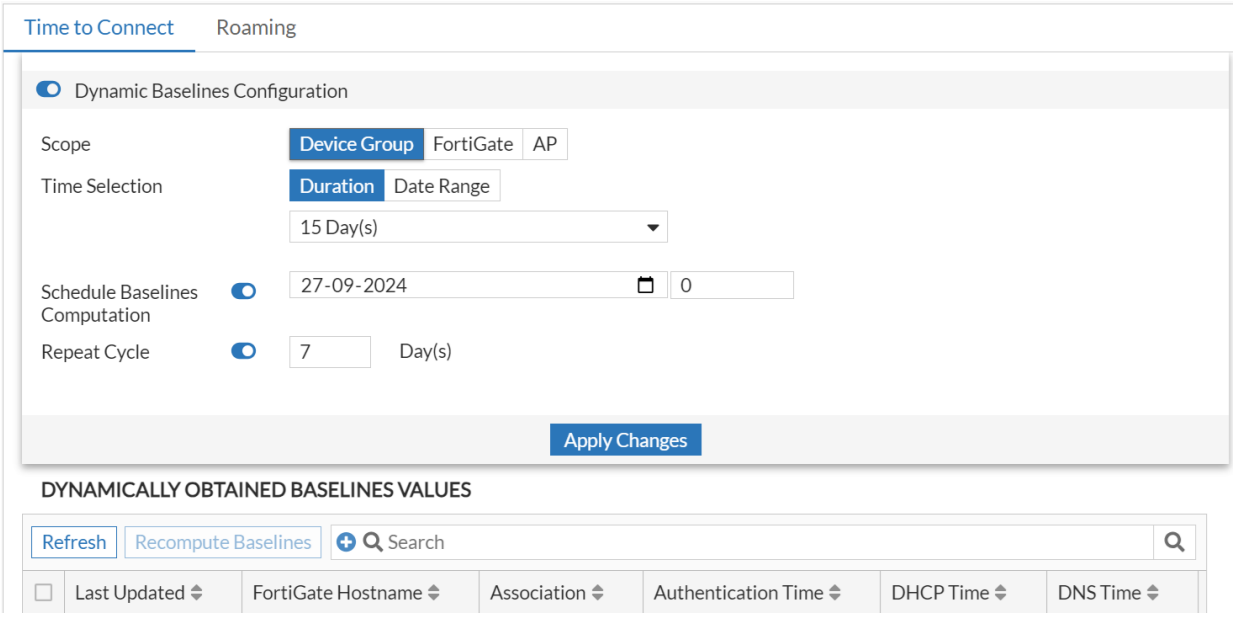
Note: The default value for the CPU and memory parameters is 80% and the default value for the temperature is 65 degree Celsius.

Time To Connect

You can configure static thresholds or enable FortiAIOps to compute them dynamically. Based on the configured thresholds, the variations in the time to connect are recorded for each phase, and the statistics are displayed in the AI Insights tab.

Dynamic Baselines

You are required to provide the following information for threshold/baseline configuration.

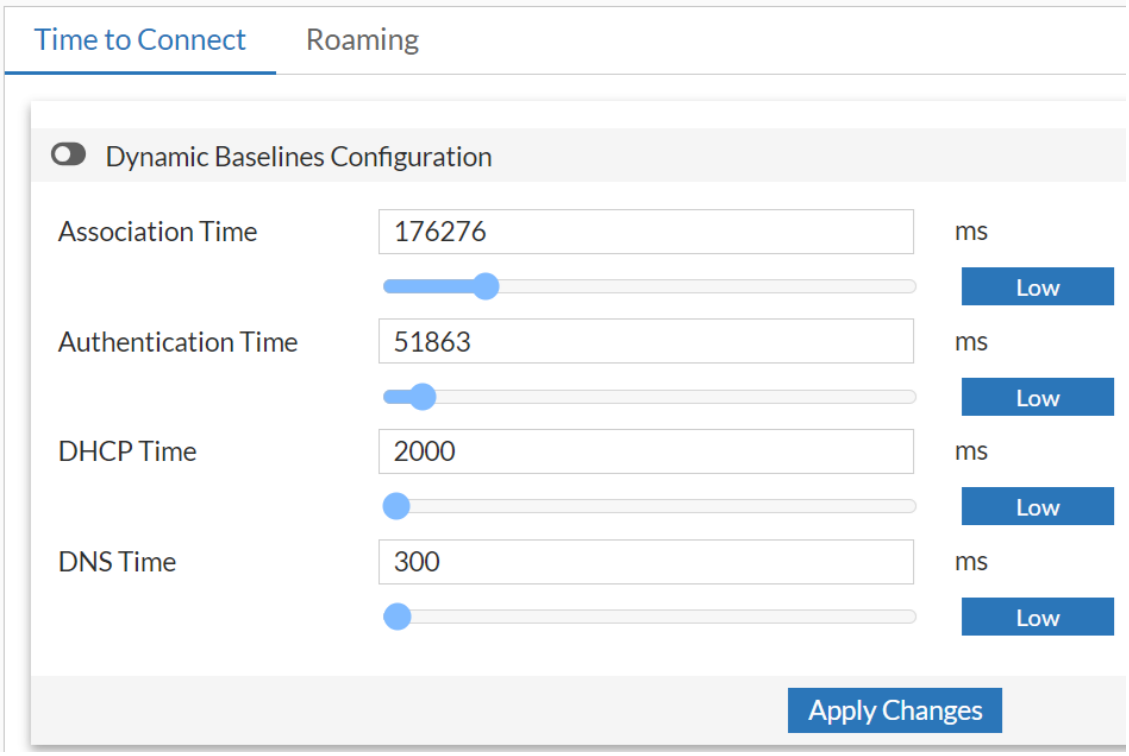


- **Scope** - Select the scope to calculate the thresholds which could either be per **Device Group**, per **FortiGate**, or per **AP**.
- **Time Selection** - Set the time range/duration for which FortiAIOps analysis client data to derive the thresholds.
- **Schedule Baselines Computation** - Set the time when FortiAIOps calculates the baselines and applies them to your network to obtain and report the relevant SLAs.
- **Repeat Cycle** - Configure the repetition of the above configurations, that is, the phase of analyzing client activity and the calculation/application of the algorithms.

The baseline values calculated by FortiAIOps are displayed in the table. You can re-compute specific baseline values.

Static Threshold

Configure the time (milliseconds) for the following stages of client connection to a network.



- **Association Time** - The time taken by a client to successfully associate.
- **Authentication Time** - The time taken by associated clients to authenticate.
- **DHCP Time** - The time taken by successfully associated and authenticated clients to receive a valid DHCP address.
- **DNS Time** - The time taken by successfully associated, authenticated, and received a DHCP address clients to resolve their first DNS request.

The default static threshold values for Time to Connect are as follows:

Attribute	Value
Association Time	1000 ms
Authentication Time	1000 ms
DHCP Time	300 ms
DNS Time	2000 ms

Notes:

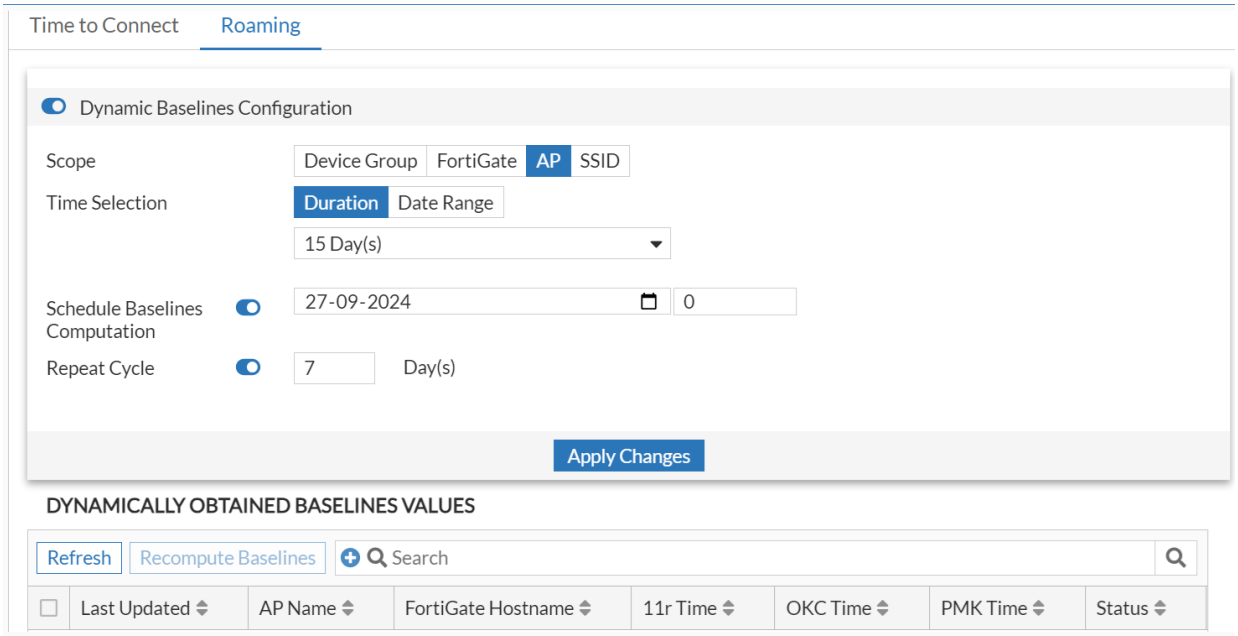
- The default value for these parameters is 300 milliseconds and the valid range is 1 - 1000000 milliseconds.

Roaming

You can configure static thresholds or enable FortiAIOps to compute them dynamically. Based on the configured thresholds, the variations in the time to connect are recorded for each phase, and the statistics are displayed in the AI Insights tab.

Dynamic Baselines

You are required to provide the following information for threshold/baseline configuration.

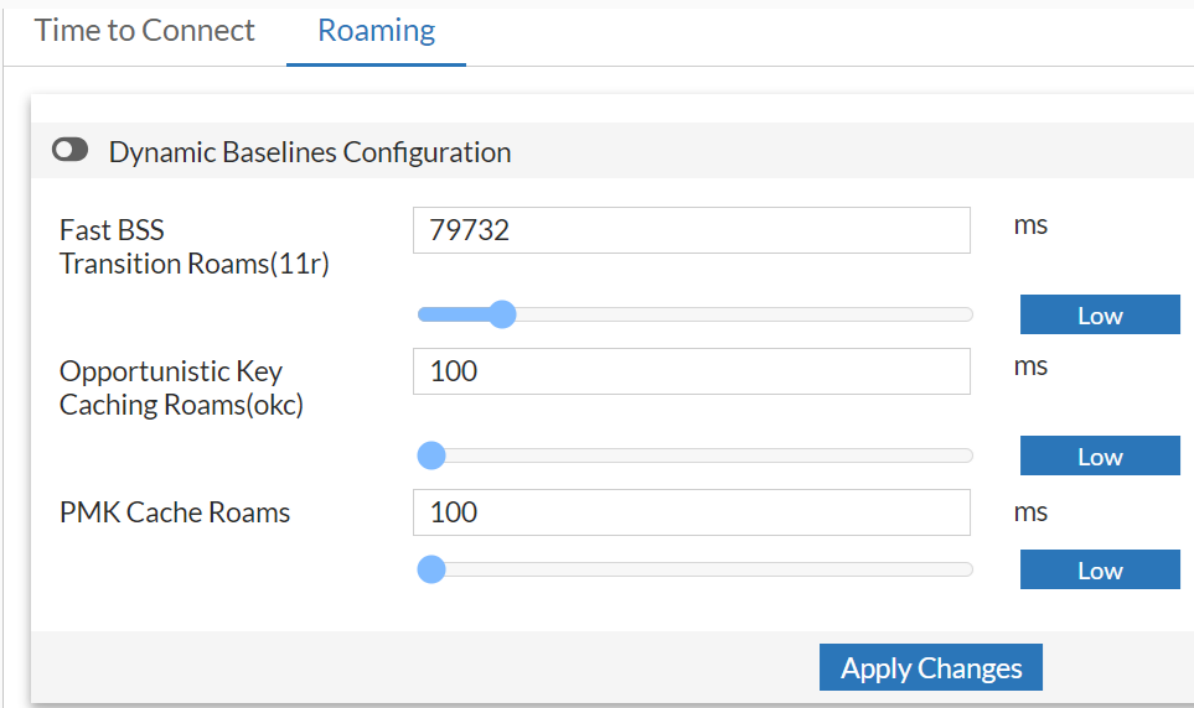


- **Scope** - Select the scope to calculate the thresholds which could either be per **Device Group**, per **FortiGate**, per **AP**, or per **SSID**.
- **Time Selection** - Set the time range/duration for which FortiAIOps analysis client data to derive the thresholds.
- **Schedule Baselines Computation** - Set the time when FortiAIOps calculates the baselines and applies them to your network to obtain and report the relevant SLAs.
- **Repeat Cycle** - Configure the repetition of the above configurations, that is, the phase of analyzing client activity and the calculation/application of the algorithms.

The baseline values calculated by FortiAIOps are displayed in the table. You can re-compute specific baseline values.

Static Threshold

For static threshold configuration to enable faster roaming, configure the following parameters.



- **Fast BSS Transition Roams(11r)** - This is implemented as part of the 802.11r standard and enables fast roaming of wireless clients by pre-authenticating them with several APs in the network; this pre-authentication is done prior to when the client begins roaming. This feature allows immediate BSS transitions between APs and curtails the latency caused by deferred data connectivity, often experienced when a client has to transition from one BSS to another while roaming in a multi-AP deployment. The default roaming time value is 55 ms and the valid range is 1 - 600000 ms.
  Note: To use this feature of FortiAIOps, ensure that the wireless client supports 802.11r standard enable 802.11r roaming on the SSID using the `set fast-bss-transition` CLI commands on FortiGate.
- **PMK Cache Roams** – The Pairwise Master Key (PMK) caching enables a wireless client to re-associate with an AP without re-authenticating. When a wireless client associates with an AP through the 802.1x authentication process, a master key negotiated with the AP is stored in a cache. When the client roams to different APs and then wants to re-associate with this AP again, then the already cached PMK is used for authentication. This significantly reduces the authentication time as the client-AP are not required to go through the entire 802.1x authentication process again, ensuring minimal latency in data connectivity during roaming. The default roaming time value is 100 ms and the valid range is 1 - 600000 ms.
- **Opportunistic Key Caching Roams (okc)** – This feature enables swift roaming of wireless clients to APs that it has never associated with earlier, without any requisite pre-authentication. When an AP successfully completes the 802.1x authentication and associates with a wireless client, it stores a unique PMK associated with that client. This per client PMK is advertised to and stored by all the APs in that particular network. When a client roams, it associates with a new AP based on this cached PMK, without any pre-authentication. This reduces the latency caused during roaming by eliminating the re-authentication process. The default roaming time value is 100 ms and the valid range is 1 - 600000 ms.

FortiAIOps dynamically determines the optimal roaming time for each type of roaming for a specific AP-Client environment using machine learning algorithms.

FortiAI

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:

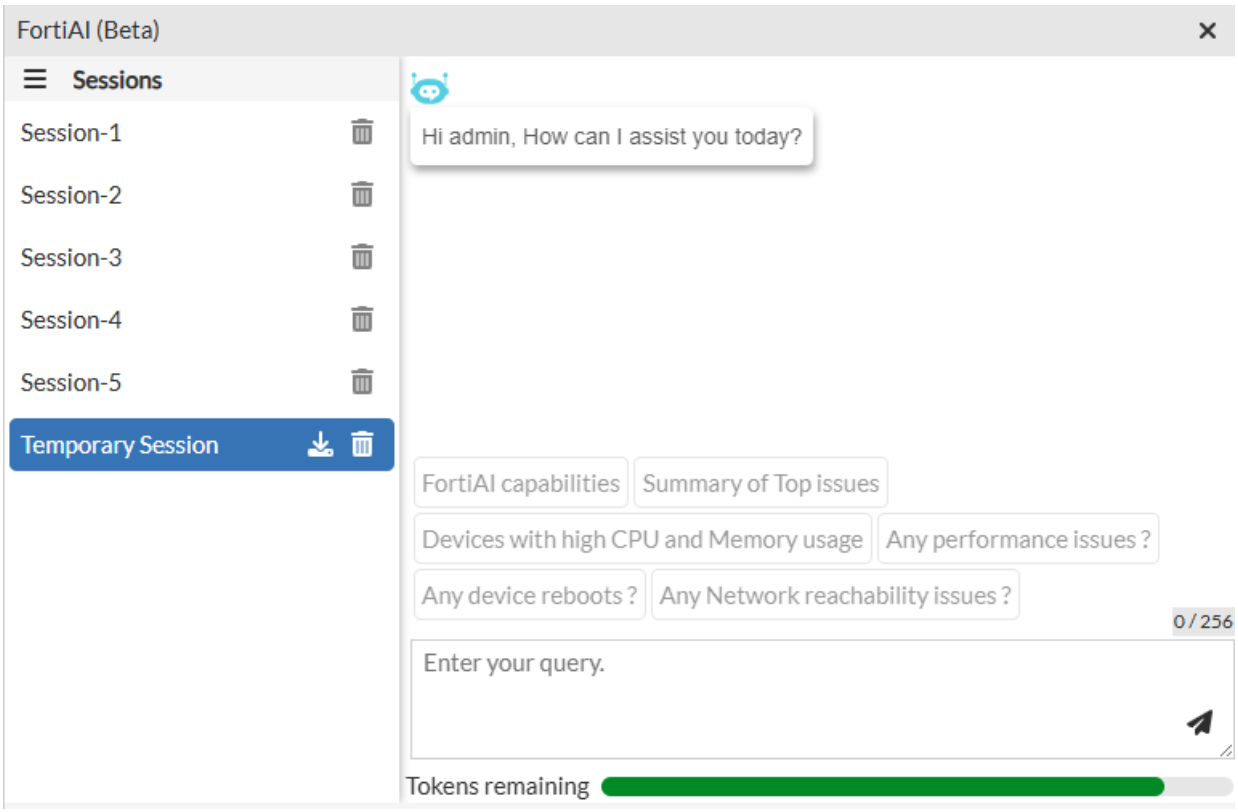
- Utilize natural language to monitor network health, identify stability issues like port flaps, troubleshoot specific client or device problems, and receive step-by-step configuration guidance using simple queries. Responses are delivered in multiple formats, including tabular data and plain text, with 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.

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.



A list of suggested queries is available in the main prompt area to help you get started.

Using FortiAI

FortiAI provides real-time performance monitoring and targeted troubleshooting for specific client and device issues.

You can interact with the assistant using simple, natural language prompts to request information or actions. If you enter a prompt that is not understood by the FortiAI assistant, it will ask for more details to clarify your request. Responses from the FortiAI assistant may also include suggestions and requests for you to consider.

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.

Category	Description
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 Prompts

For best results with FortiAI, ask clear, specific questions related to the network data it is designed to access. A good prompt is one that FortiAI can easily understand and translate into a precise data query, ensuring you get fast and accurate information.

Example of valid prompts:

- Is channel overlap causing coverage or interference problems?
- Are there any throughput issues in the network?
- Are any SD-WAN interfaces facing performance issues?
- How do I back up the configuration?

The above examples use full sentences. However, in general, using more text means using more tokens. To more efficiently use tokens, keep your prompts concise. For more information about tokens, see FortiAI Tokens.

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 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. For more information, see FortiAI Tokens.

FortiAI Data Privacy

FortiAIOps and FortiAI protects your data by masking private information such as IP addresses before it is sent to the FortiAI large language model (LLM) for processing.

Data such as MAC address, hostname, user name, IP address, VDOM names, and so on are considered as protected data and are masked before sending the information to FortiAI LLM.

How private data is protected

1. The FortiAI assistant identifies information in a query that matches the list of protected data.
2. FortiAIOps masks the private data, and the masked data is returned to the FortiAI assistant.
3. The FortiAI assistant creates a one-to-one mapping between the masked and unmasked data.
4. The FortiAI assistant sends the masked data to the LLM where the request is processed.
5. When the result is returned, FortiAI receives the masked data from the LLM, and a reverse mapping is performed.
6. The private data is returned to the user unmasked in the assistant's response.

FortiAI Tokens

As a FortiAIOps customer, you now have access to FortiAI as a **Beta** feature in this release. This includes an allocation of 5 million tokens for evaluation.

How token usage is calculated

Tokens are used in large language models (LLMs) to process text and quantify usage. Tokens usage is calculated using the following guidelines:

- When you use the FortiAI assistant, the text in both the prompt (input) and the response (output) is processed as tokens.
- While there is no one-to-one relationship between words or characters and tokens, in general, more text in the query and response means using more tokens.
- Because the FortiAI assistant uses session history for it's responses, queries that are a part of a long session will use more tokens than new conversations.

Best practices

To ensure you are using your allocation of tokens effectively, consider implementing the following best practices:

- Make your prompts concise and specific. Vague questions require more processing and can yield broad, less useful answers, consuming more tokens.
- Use filters in your prompts to receive concise and specific responses. Add details like time-frames, device names, or specific metrics to narrow the focus. For example, instead of "How is my network doing?", try asking "Show me the top 5 non-performing access points in the last hour."

- Use terms that directly relate to functions and metrics you see in the FortiAIOps dashboards. This helps the assistant translate your request into a precise query much more efficiently. For example, instead of "Are any connections bad?", try "Are there any throughput SLA issues in the network?"
- Reference details in the existing thread when possible. FortiAI remembers the context of your current conversation thread. Referencing previous responses is more efficient than starting a new query.

  For example, imagine the following exchange:

  You ask: "Is the <AP name> experiencing poor channel condition?"

  FortiAI responds with the information.

  Now, you can ask a related follow-up question: "Check for last 4 hours?"

Viewing token usage

The token usage is displayed at the bottom of the FortiAI pane in FortiAIOps. Mouse over the **Tokens remaining** bar to view the following in a tooltip:

- Total Tokens
- Consumed Tokens

FortiAI Example Tasks

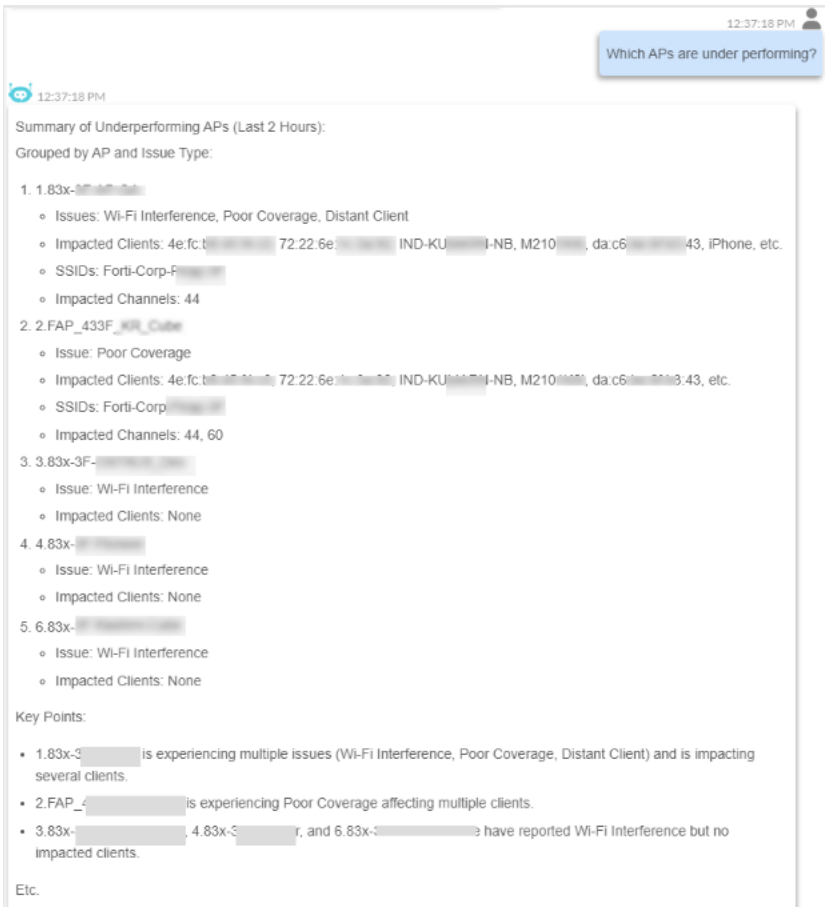
The following are some example tasks that can be performed using the FortiAI assistant:

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.

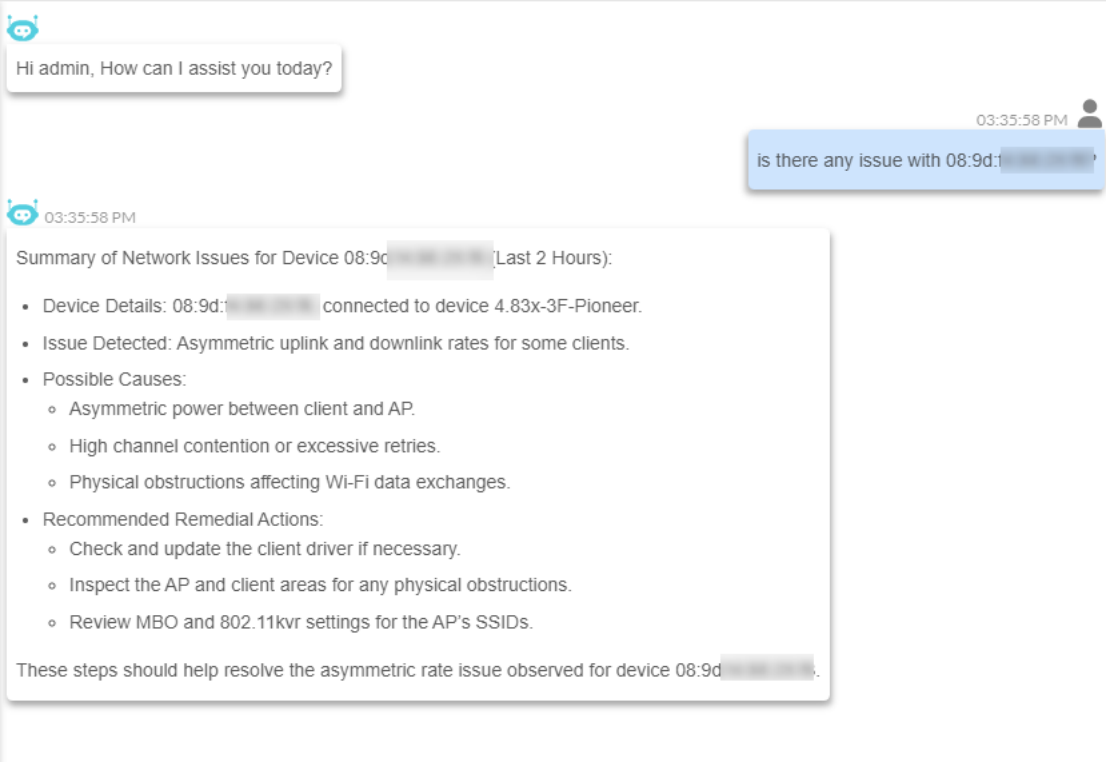
Prompt: Which APs are under performing?



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.

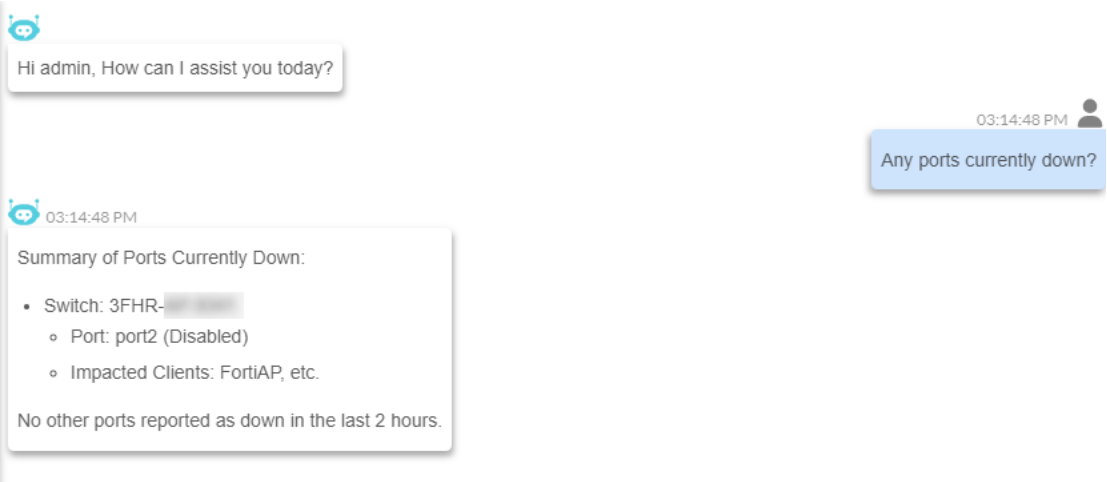
Prompt: Is there any issue with <MAC address>?



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?



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

2. Impacted SD-WAN Interfaces and Associated Issues:

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

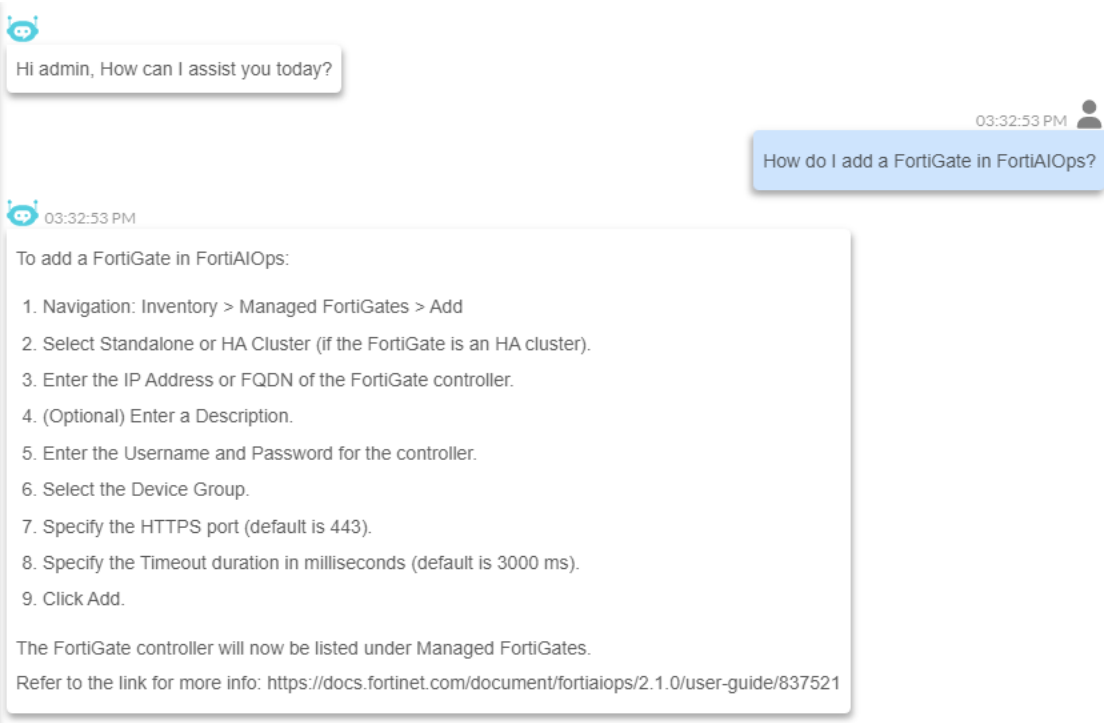
3. Clients Affected (Grouped and Deduplicated):

- IND-PRE
- IND-ARPI
- IND-34SX
- IND-C346
- IND-2QR
- IND-NAIR
- IND-MMU
- IND-4C9Z
- 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.

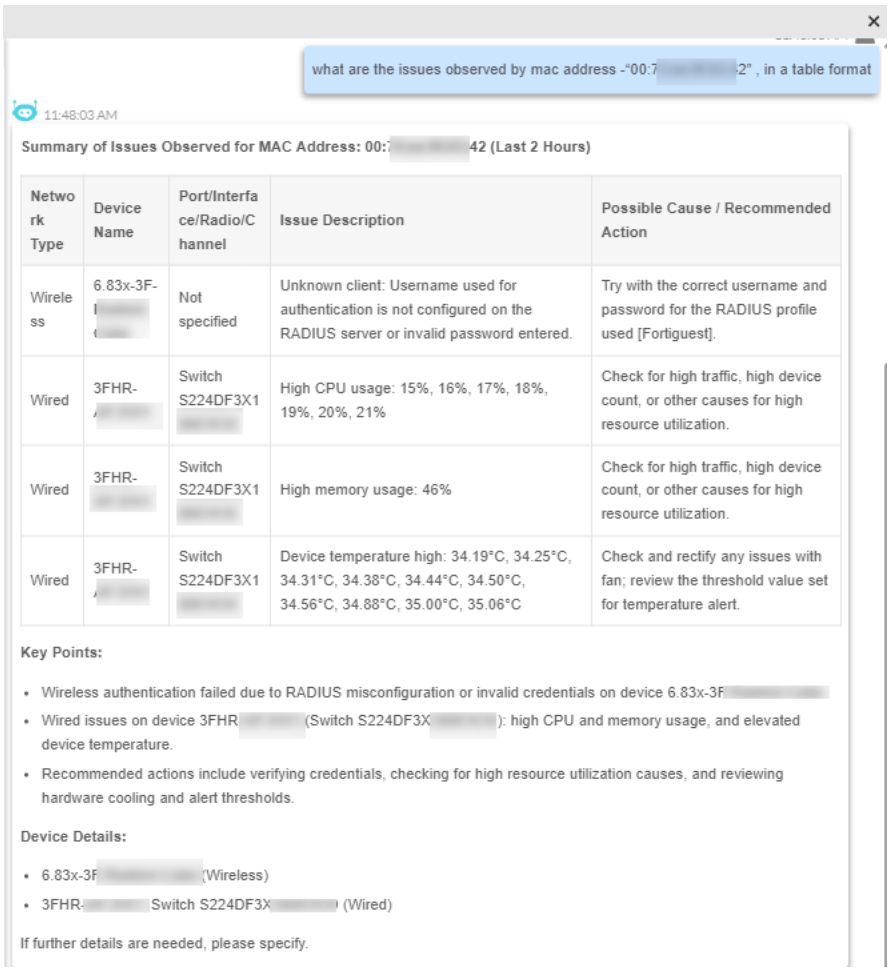
Prompt: How do I add a FortiGate in FortiAIOps?



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 :2" , in a table format

11:48:03 AM

Summary of Issues Observed for MAC Address: 00: 42 (Last 2 Hours)

Network Type	Device Name	Port/Interface/Radio/Channel	Issue Description	Possible Cause / Recommended Action
Wireless	6.83x-3F-	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-	Switch S224DF3X1	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-	Switch S224DF3X1	High memory usage: 46%	Check for high traffic, high device count, or other causes for high resource utilization.
Wired	3FHR-	Switch S224DF3X1	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
- Wired issues on device 3FHR (Switch S224DF3X): 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 (Wireless)
- 3FHR- Switch S224DF3X) (Wired)

If further details are needed, please specify.

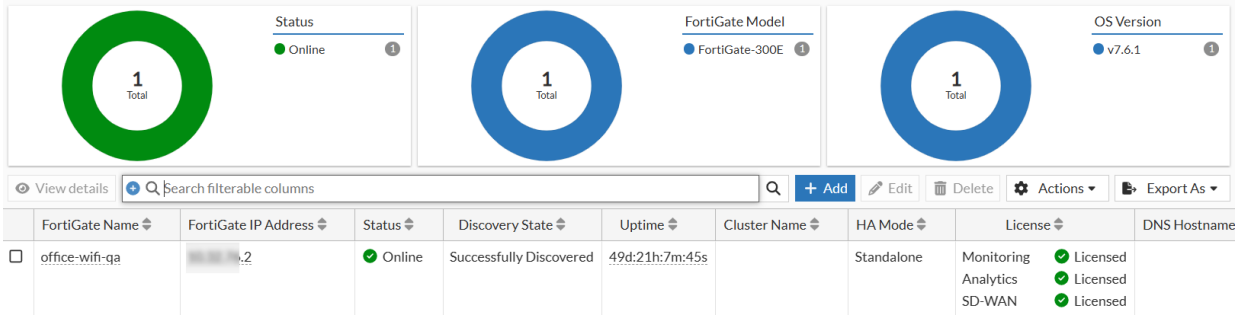
Inventory

This section describes adding the FortiGate controllers to FortiAIOps, grouping them, and the management operations on the added controllers.

- Adding and Managing FortiGates
- Device Groups
- VDOM Support

Adding and Managing FortiGates

This page provides a graphical representation of the FortiGate controllers deployed in your network. You can view and monitor the current status of the FortiGate controllers, the various FortiGate models in use, and the OS versions. The table beneath the charts provides the details of all FortiGate controllers; click on specific areas of the chart to filter data displayed in the table.



You can perform the following operations on this page.

- Adding a FortiGate
- Importing and Exporting FortiGates
- Managing FortiGates

Adding a FortiGate

The communication between the FortiAIOps application and FortiGate is secured by SSL/TLS encryption. Therefore, FortiAIOps can successfully discover a FortiGate only if a valid certificate is installed in FortiGate. However, FortiAIOps can also discover FortiGates with a default certificate over a trusted connection. If a 3rd party certificate is installed in FortiGate for HTTPS/web server then the corresponding CA certificate should be Installed in FortiAIOps for successful discovery. For more information see Certificates and FortiGate Certificates.

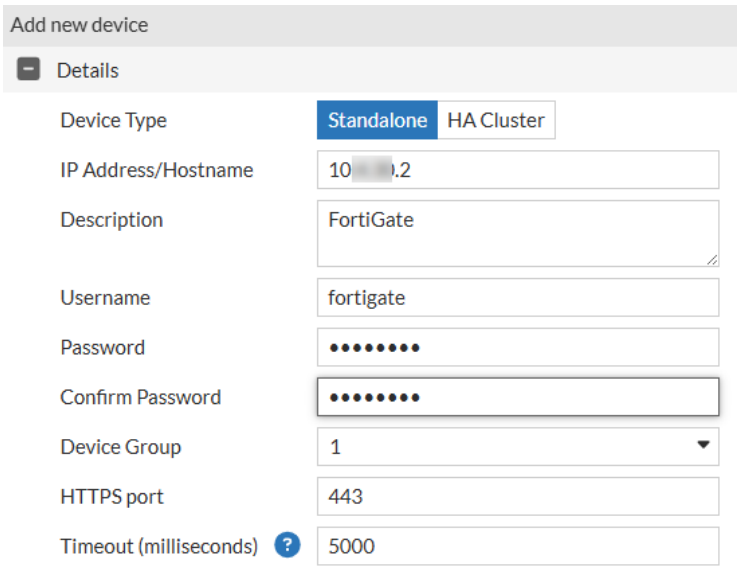
The managed FortiGate IP address/FQDN configured in FortiAIOps must match the Subject Alternative Name (SAN) in the FortiGate certificate, else, the FortiGate discovery fails.

- If the FortiGate IP address is configured in FortiAIOps then the SAN attribute in the certificate should be the FortiGate IP address.
- If the FortiGate FQDN is configured in FortiAIOps then the SAN attribute is the certificate should be the FortiGate FQDN.
- If the FortiGate IP address or FQDN are configured in FortiAIOps then the SAN attribute in the certificate should include both the FortiGate IP address and FQDN.

Notes:

- FortiGate discovery fails if a certificate is from an unknown authority. Ensure to install specific CA certificate of FortiGate in FortiAIOps.
- If a new certificate is installed in a managed FortiGate then Fortinet recommends to re-add the FortiGate in FortiAIOps.
- For self-signed CA certificates generated in FortiGate, valid CA certificate should be installed in FortiAIOps.
- To use a *Let's Encrypt* certificate, ensure to download and install the CA certificate of *Let's Encrypt* in FortiAIOps. For more information see Automated Certificate Management Environment (ACME).

To manually add a FortiGate controller, click **Add** and provide the following details.



1. Select **Standalone** or **HA Cluster** if the FortiGate is an HA cluster.
2. Enter the **IP Address** or FQDN of the controller and an optional **Description**.
   Note: If a 3rd party certificate is used by FortiGate then ensure to install a valid CA certificate in FortiAIOps.
3. Enter the **Username** and **Password** for the controller.
4. Select the **Device Group**. Controllers in the selected device group are added.
5. Specify the **HTTPS port**. The default is 443.
6. Specify the **Timeout** duration (milliseconds), that is, the maximum time allowed to establish a connection with FortiGate and obtain a response. The default value is 5000 milliseconds.

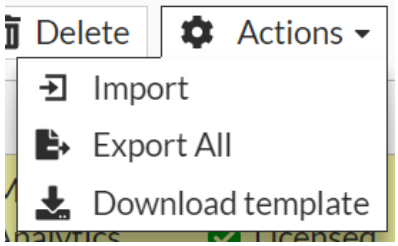
The added FortiGate controller is now listed.

Importing and Exporting FortiGates

You can import details of FortiGate controllers from a *.csv* file to add them. Enter the details in the format depicted in the image here.

	A	B	C	D	E	F	G	H
1	Device Type	IP address	Description	Username	Password	Device Group	HTTPS port	Timeout (milliseconds)
2	Standalone	[redacted]	fortigate1	admin	fortigate1	guestgroup	443	3000
3	Standalone	[redacted]	fortigate2	admin	fortigate2	test2	10443	3000
4	Standalone	[redacted]	fortigate3	admin	fortigate3	guestgroup	443	3000

You can download a sample template for populating the FortiGate details, from the **Actions** drop-down menu.



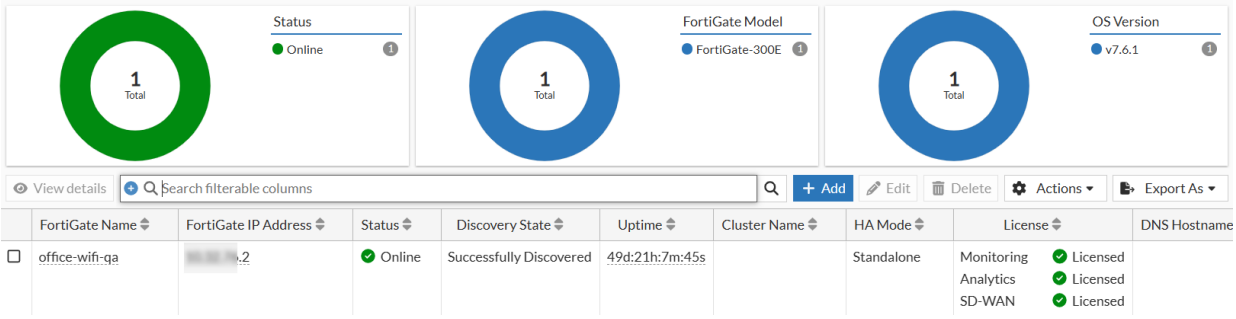
Select **Import** to upload the FortiGate configuration file.

You can export the configurations of all the existing FortiGate controllers added to FortiAIOps, in a *.csv* format. Click **Export All** and the file with details of the added FortiGate controllers is downloaded to your machine.

Note: The HA cluster addition does not work using the **Import** option.

Managing FortiGates

This page provides analytical information related to the performance of various elements and processes in your network. The data is visually represented with interactive options to drill-down and filter specific information. This enables monitoring, diagnostic, and troubleshooting operations for connectivity issues, data usage, and enhancing performance.



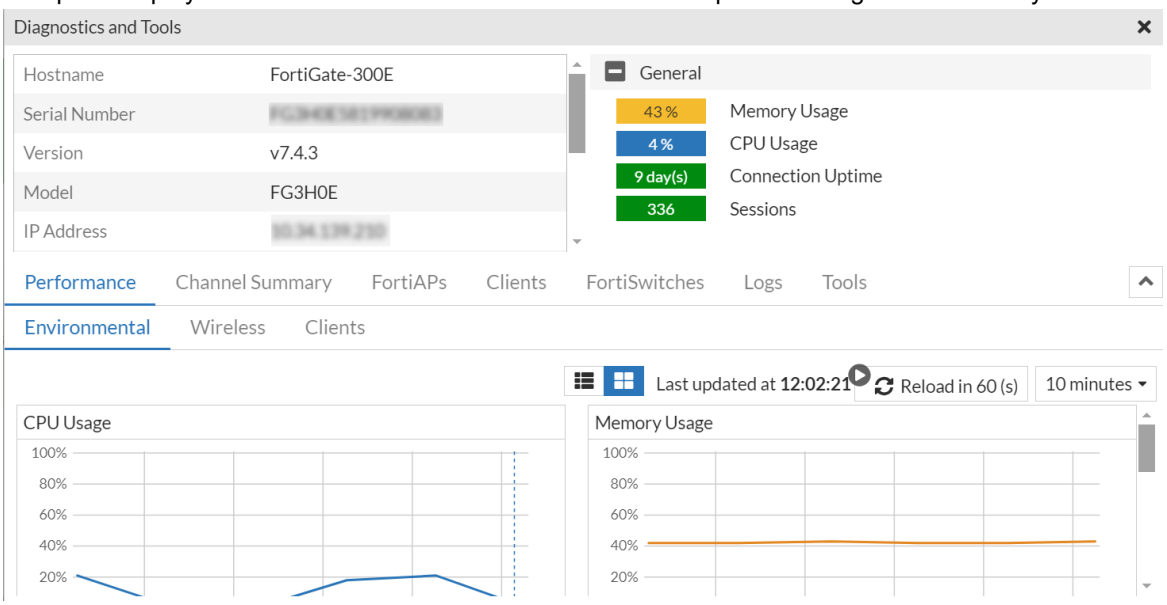
You can perform the following operations on a FortiGate controller listed on this page.

- **Add** - Select to add a FortiGate controller manually. For more information, see Adding a FortiGate.
- **Actions** - Click **Actions** to import and to download the template.
- **Export As** - Click 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.

- **View Details** - Select a FortiGate and click **View details** to open **Diagnostics and Tools** pane. You can also right-click the FortiGate and click **View details**.

  This pane displays details about the selected FortiGate and also provides diagnostic tools for your network.



- **CLI** - To open the CLI utility, right-click the FortiGate and select **CLI**.
- **Reboot** - Right-click the FortiGate and select **Reboot** to reboot the device.

Performance

This tab displays the performance data for your network based on various parameters. 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 data in this tab is automatically refreshed every 60 seconds; the following options are available to manage the auto-refresh feature for this page.

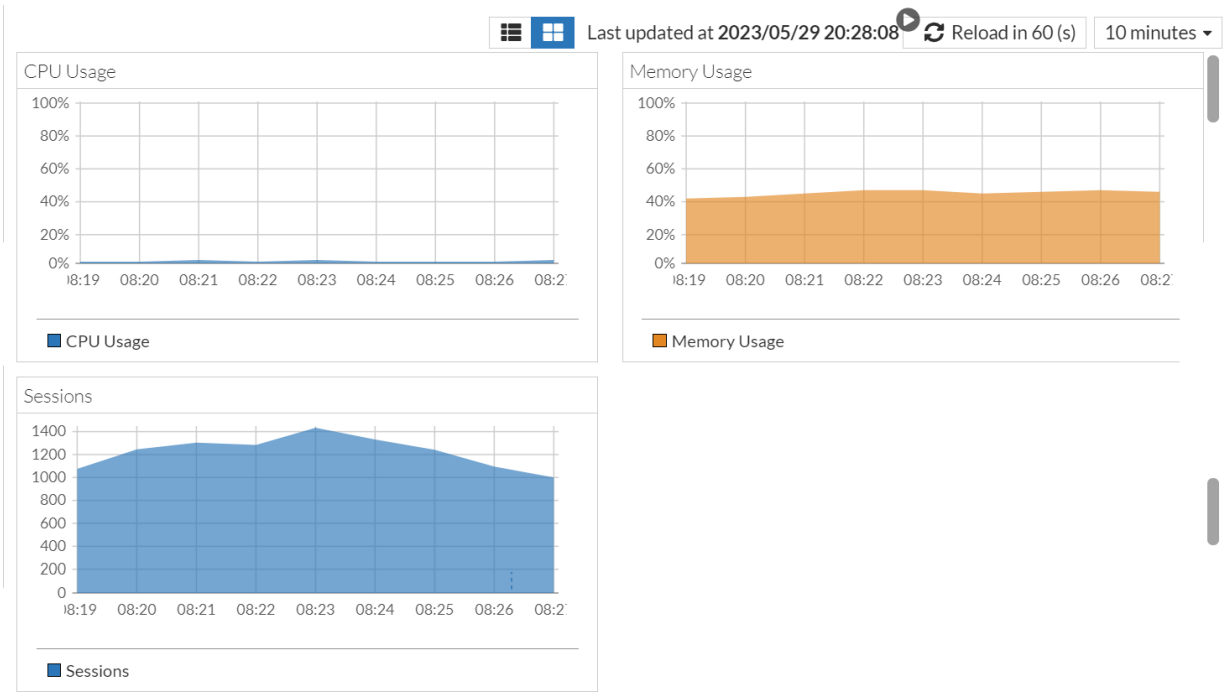
- Click to manually refresh data.
- Click to pause the auto-refresh.
- Click to resume the auto-refresh.

Performance is displayed for the following.

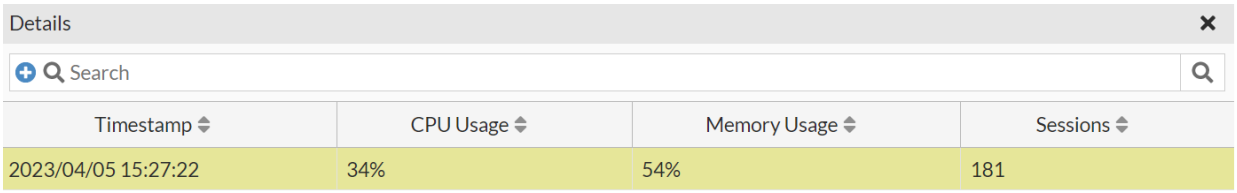
- Environmental
- Wireless
- Clients

Environmental

This tab displays resource usage such as, the maximum CPU and memory usage levels, and the maximum number of sessions at a given time.



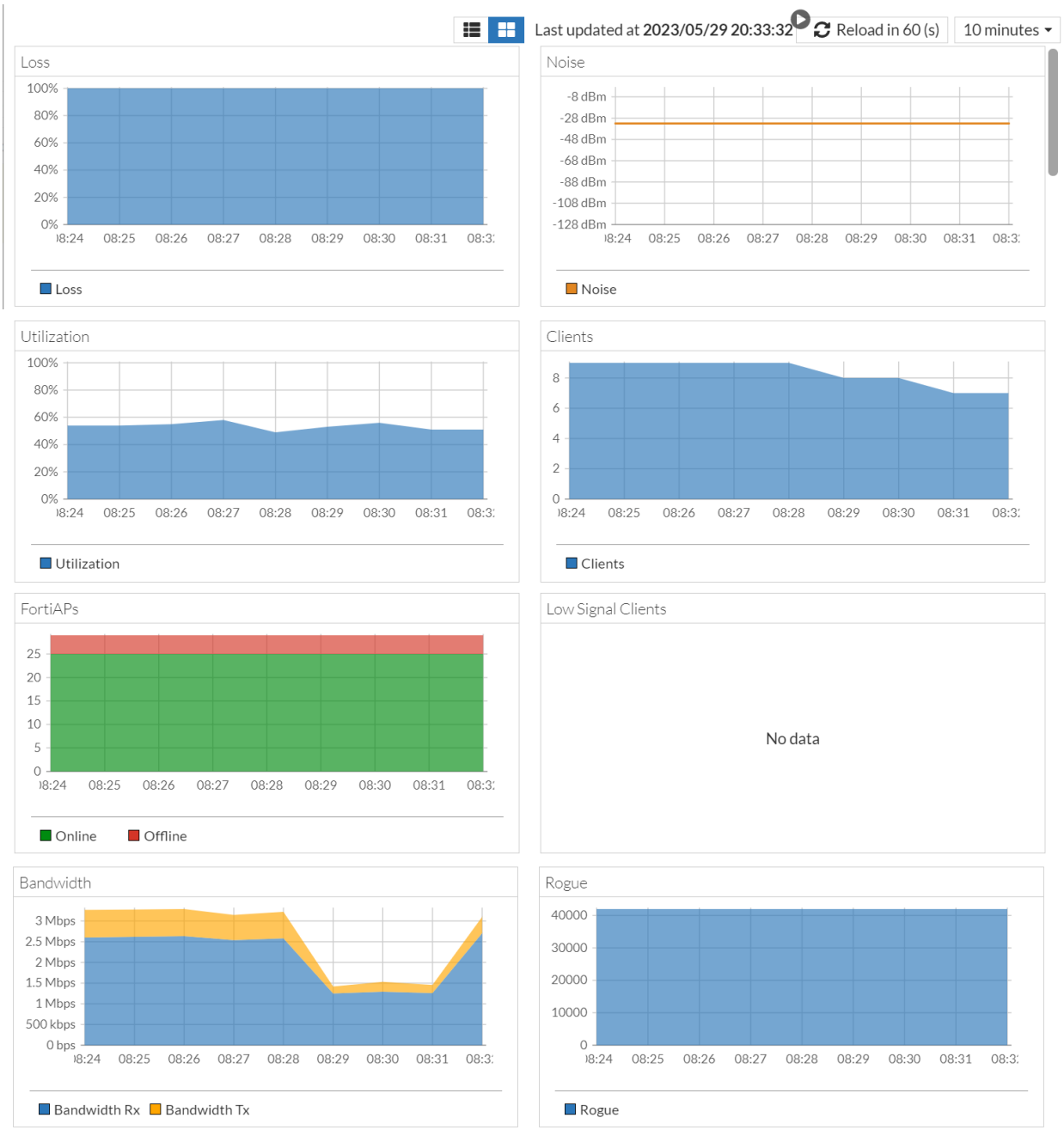
Hover over each of these graphs to view the current statistics and click on any of these graphs to view details.



Timestamp	CPU Usage	Memory Usage	Sessions
2023/04/05 15:27:22	34%	54%	181

Wireless

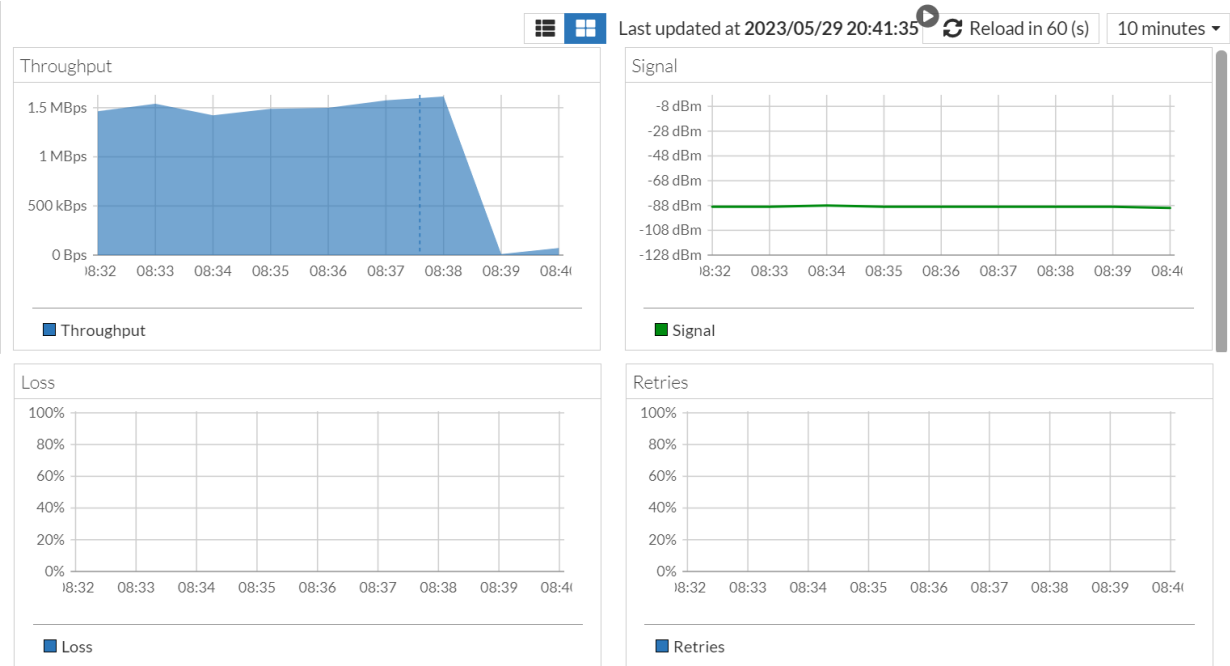
Displays detailed information about the health of the wireless connections in the network, such as, loss%, SNR, channel utilization %, number of stations, status of the FortiAPs, low signal stations, the average throughput at a given time, and the number of rogue APs at a given time.



Hover over each of these graphs to view the current statistics and click on any of these graphs to view details.

Clients

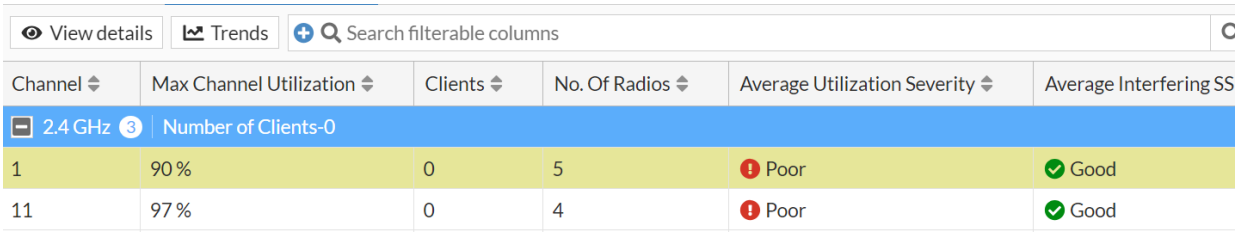
This tab displays information about the clients connected to the network, such as, throughput, Loss (%), Retries (%), and SNR (dB) and throughput.



Hover over each of these graphs to view the current statistics and click on any of these graphs to view details.

Channel Summary

This page provides granular insights into the performance of each channel with detailed statistics and trends. For more information, see Channel Summary.



FortiAPs

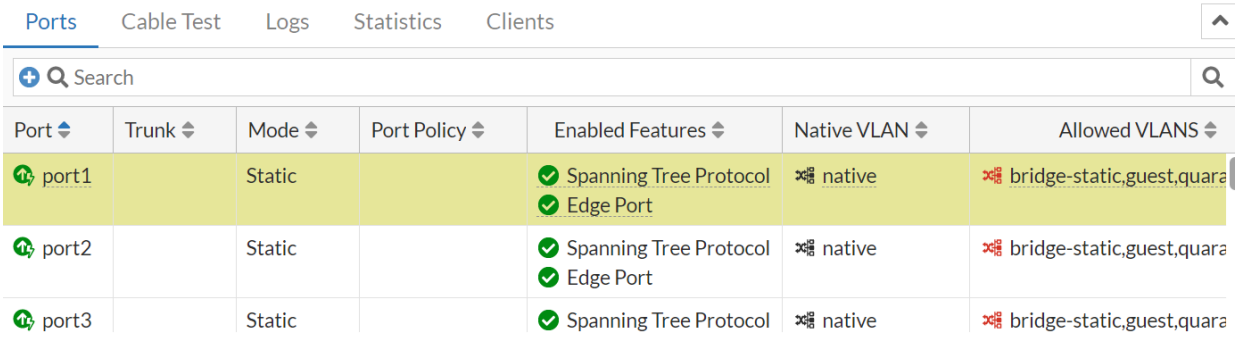
This tab displays details about the selected access point with their status and details. To view the details, select an access point and click **View Details**. For more information on the diagnostic options and details see Access Points.

Clients

This tab displays the clients currently connected to the selected access point along with their details. To view the details, select a client and click **View Details**. For more information on the diagnostic options and details see Wireless Clients on page 185.

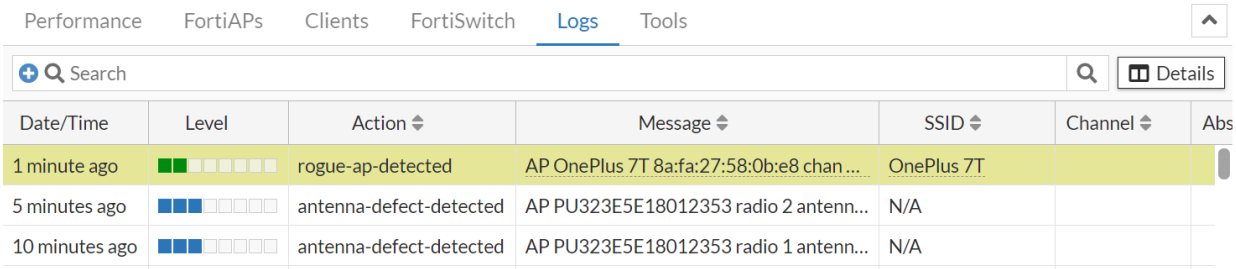
FortiSwitch

This tab displays a graphical snapshot of the FortiSwitch activity such as, the total number of FortiSwitches, their status (online/offline), and the deployed model details. To view the details, select a FortiSwitch and click **View Details**. For more information on the diagnostic options and details see FortiSwitch.



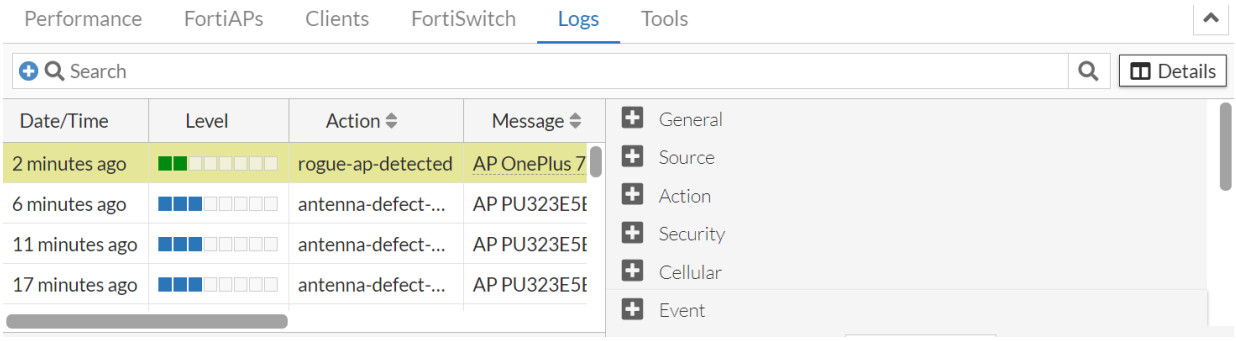
Logs

This tab displays the detailed FortiGate event logs and each event is assigned a severity, that is depicted with a color code. Hover over the color bar in the **Level** column to view the severity.



- Emergency, Critical (red)
- Alert (orange)
- Error, Warning (blue)
- Notice, Information, Debug (green)

Select an event row and click **Details** to view the detailed log information.



- **General** - Generic information about the log event such as, the date and time of event logging, the associated virtual domain, and the log description.
- **Source** - The details of the associated access point such as the MAC address, interface, and SSID.

- **Action** - The reason for the log event generation.
- **Security** - The severity of the log event, the configured security mode, and the encryption type.
- **Event** - The serial number of the access point and the generated log message.
- **Other** - Generic information such as the log event time stamp, the timezone, log type, and so on.

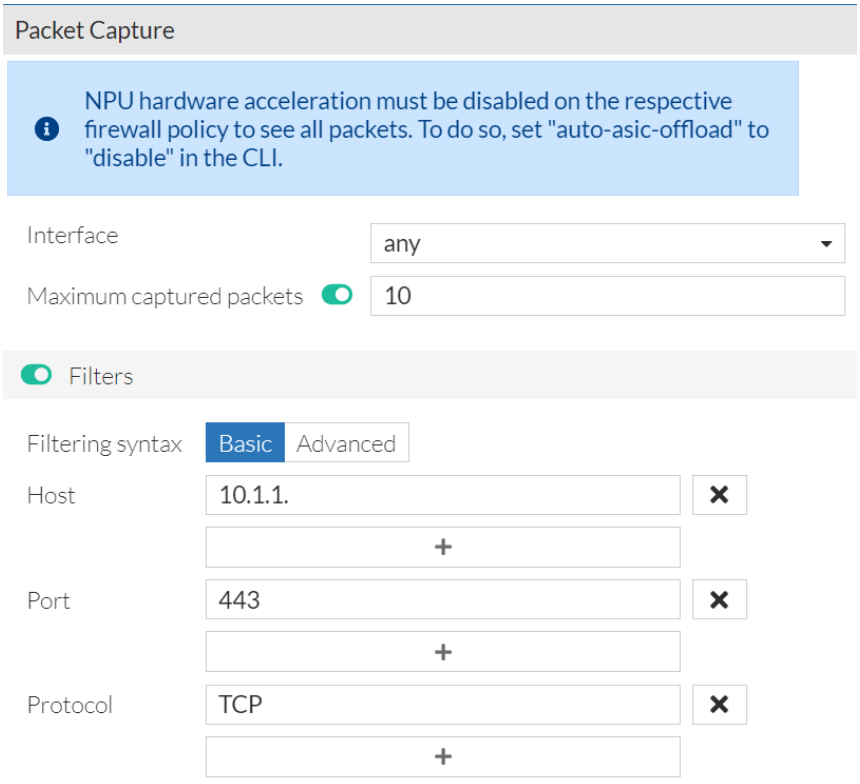
Tools

FortiAIOps provides various utilities that you can run on the FortiAP for **Connectivity Analysis**, **Network Analysis**, and **Enhanced Troubleshooting**.

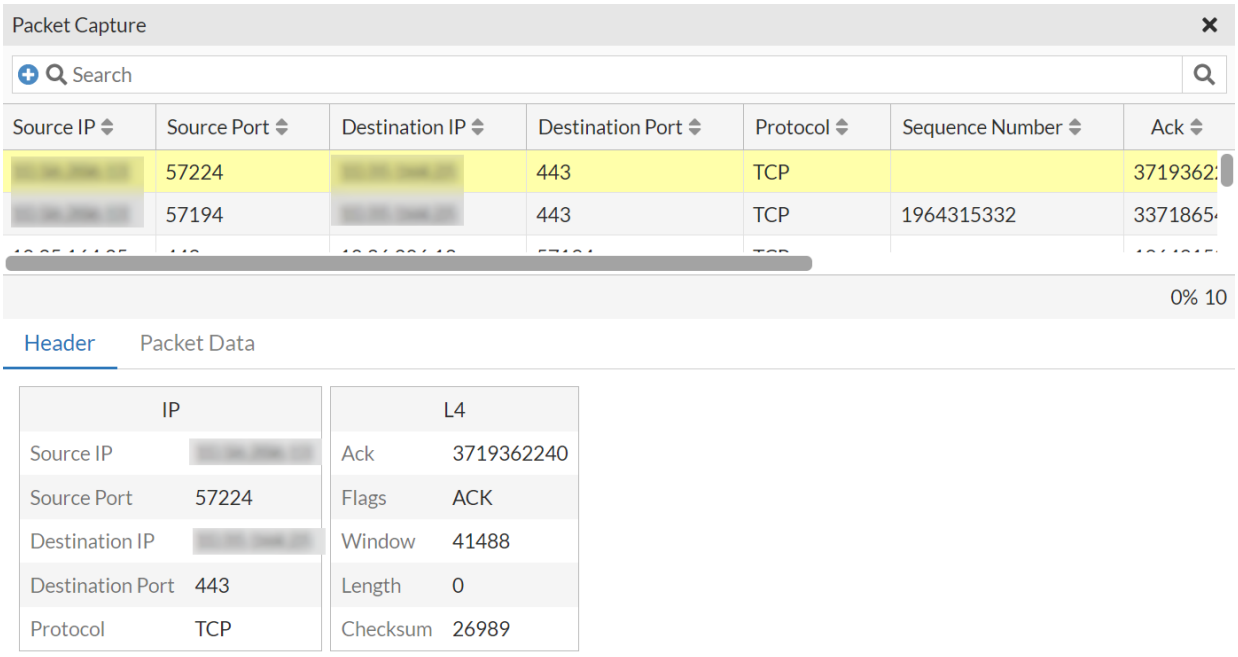
- Packet Capture
- ARP Table
- Routing Table
- DHCP
- DNS Lookup
- Reverse DNS Lookup
- Web CLI
- TAC Report
- Process Monitor

Packet Capture

You can use the packet capture tool to select a packet and view its header and payload information in real-time. Once completed, packets can be filtered by various fields or through the search bar. The capture can be saved as a PCAP file that you can use with a third-party application, such as Wireshark, for further analysis.

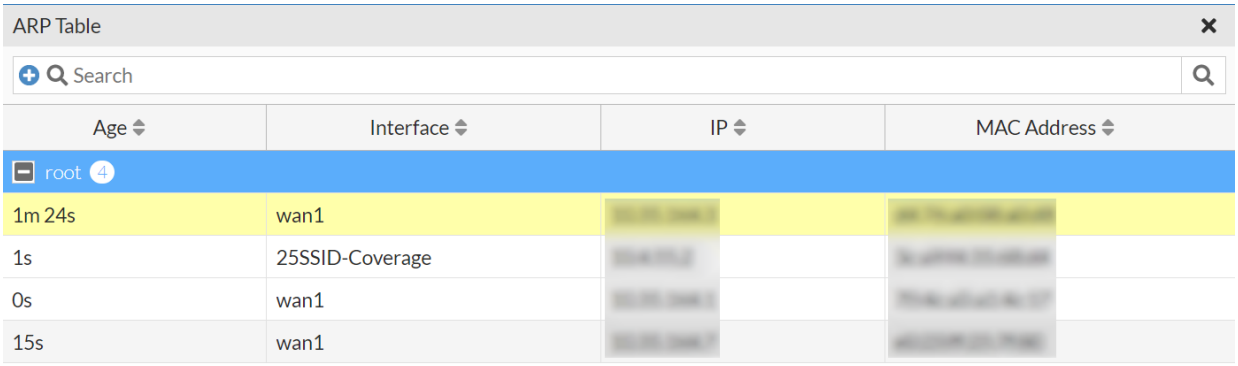


Click **Run** and select the **Interface** and the **Maximum captured packets** (default is 10). You can enable filters, for a **Basic** filter, provide the **Host**, **Port**, and **Protocol Number** and for an **Advanced** filter, enter a string, such as *src host 172.16.200.254 and dst host 172.16.200.1 and dst port 443*. Click **Start capture**.



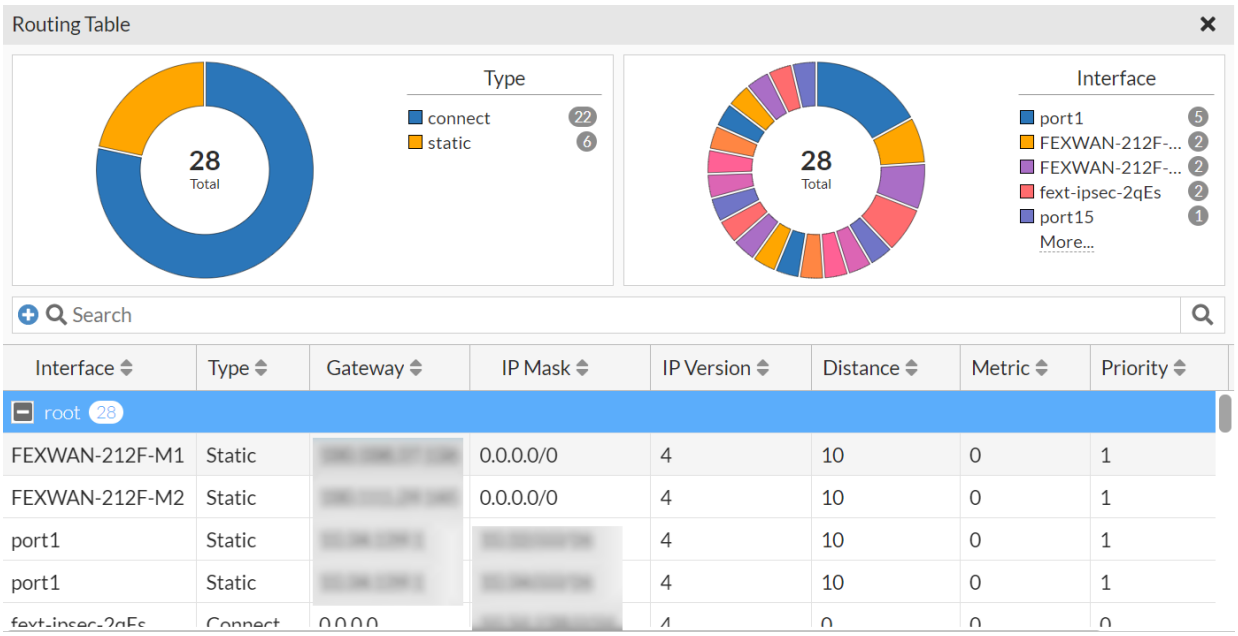
ARP Table

The ARP Table records the discovered MAC address - IP address pairs of devices connected to a network and the interface details. Each connected device has its own ARP table that stores the MAC-IP address pairs that the device has communicated with. Click **Run** to view the ARP table.



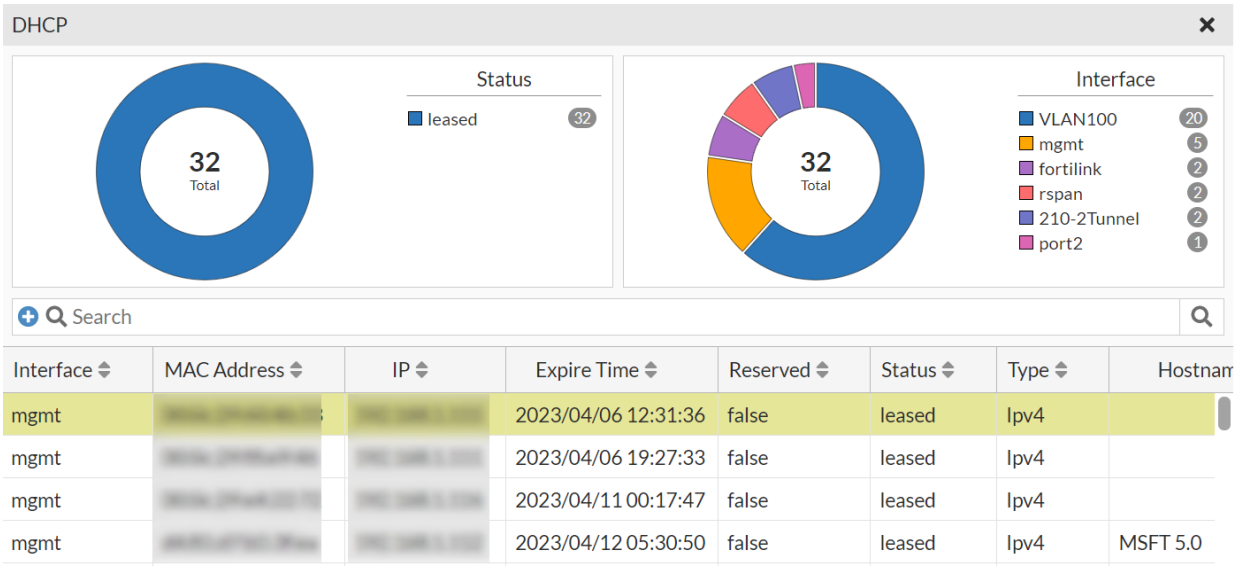
Routing Table

You can view the routing table on the FortiGate, including all static and dynamic routing protocols.



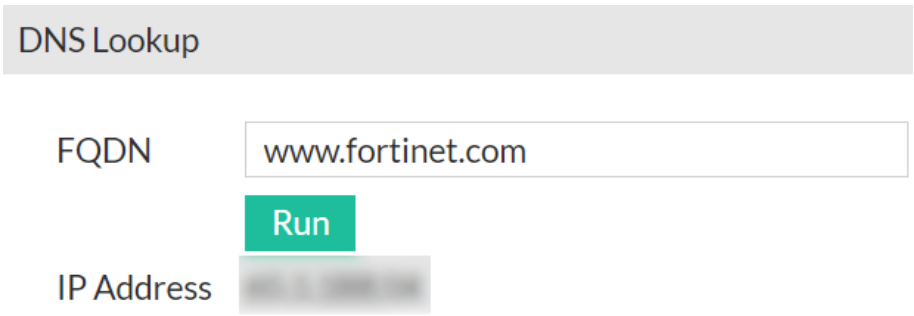
DHCP

The DHCP monitor shows all the addresses leased out by FortiGate's DHCP servers.



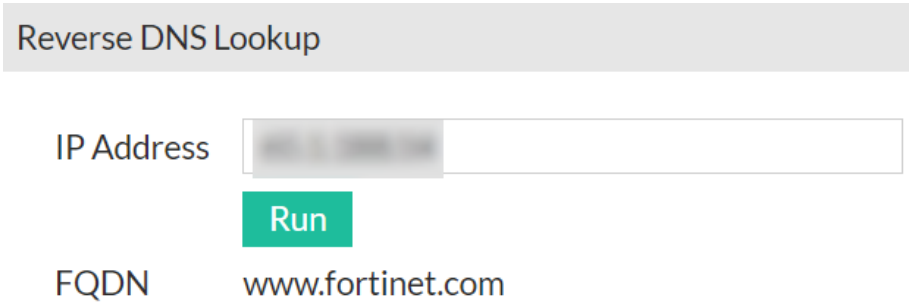
DNS Lookup

Enter the domain name (FQDN) to view the IP addresses associated with it.



Reverse DNS Lookup

Enter the IP address to view the domain name (FQDN) associated with it.



Web CLI

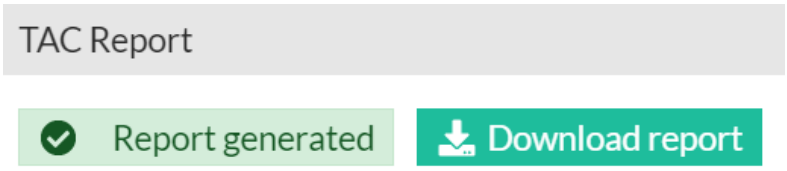
Access the FortiGate's command line interface.

Web CLI

```
FortiGate-300E # show
#config-version=FG3H0E-7.2.4-FW-build1396-230131:opmode=1:vdom=0:user=admin
#conf_file_ver=818427493209189
#buildno=1396
#global_vdom=1
config system global
    set admin-server-cert "self-sign"
    set admintimeout 480
    set alias "FortiGate-300E"
    set hostname "FortiGate-300E"
    set switch-controller enable
    set timezone 47
end
config system accprofile
    edit "prof_admin"
        set secfabgrp read-write
        set ftviewgrp read-write
        set authgrp read-write
        set sysgrp read-write
        set netgrp read-write
        set loggrp read-write
        set fwgrp read-write
--More--
```

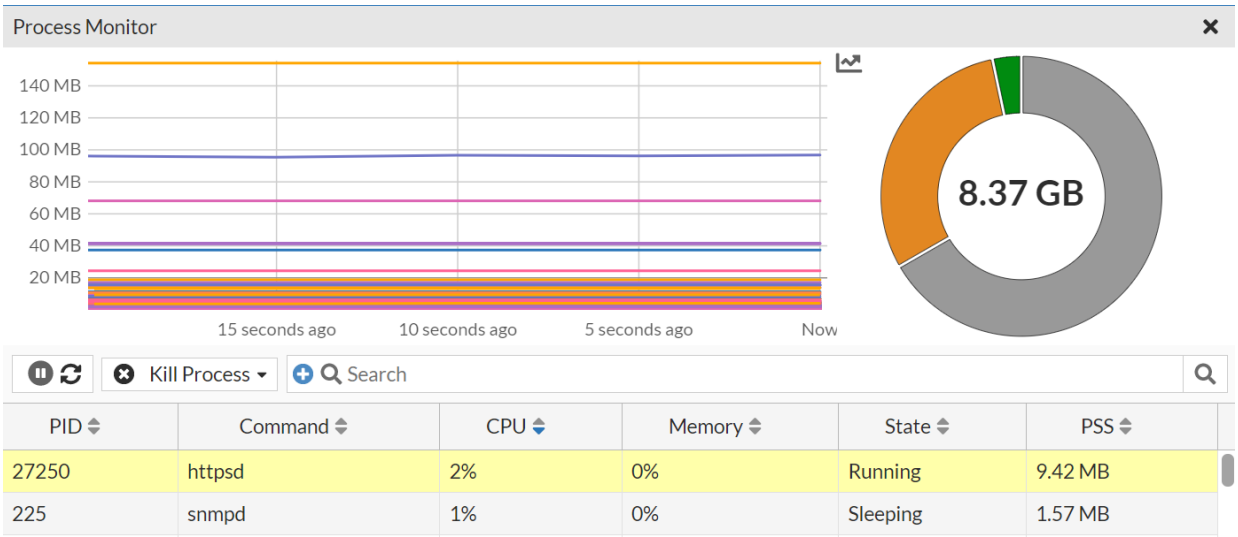
TAC Report

The Technical Assistance Center (TAC) report runs an exhaustive series of diagnostic commands for troubleshooting network issues. You are required to download the generated report (*.txt*) to view it; click **Download report**.



Process Monitor

The process monitor displays running processes with their CPU and memory usage levels. You can sort, filter, and terminate processes within the process monitor pane.



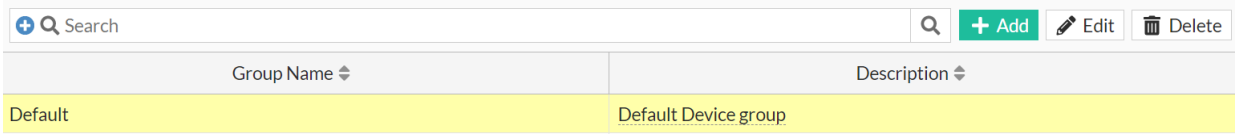
Select a process to perform any of the following operations.

- **Kill Process** - The standard kill option that produces one line in the crash log (diagnose debug crashlog read).
- **Force Kill** - The equivalent to *diagnose sys kill 9 <pid>*. This can be viewed in the crash log.
- **Kill & Trace** - The equivalent to *diagnose sys kill 11 <pid>*. This generates a longer crash log and backtrace. A crash log is displayed afterwards.

For more information on the FortiGate commands and related information, see FortiGate documentation.

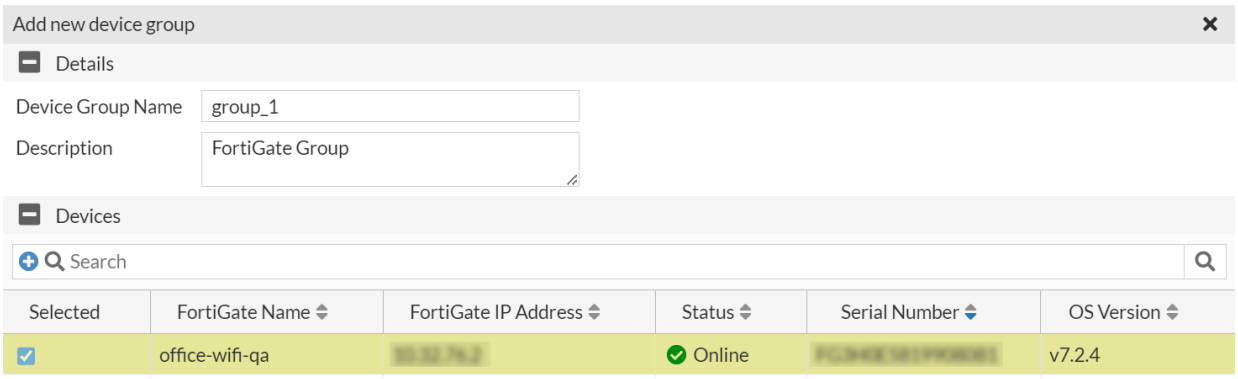
Device Groups

You can group FortiGate controllers for ease of management. Each controller can belong to only one group; if a controller is added to a second group, it is automatically removed from the previous group. Device groups allow administrators to manage devices in a certain way, such as, provide specific access to a set of devices. The *admin* user have access to all the device groups and devices within them. System administrators and users assigned the *super user* role can only create and configure device groups.



If you do not set up device groups, all controllers remain assigned to the *Default* device group.

1. Navigate to **Device Groups** and click **Add**.
2. Provide a unique **Device Group Name** and an optional **Description**.
3. A list of controllers managed by FortiAIOps is displayed. Select from the listed controllers and click **Create**. The controllers are added to the device group.



You can switch the device group from the bar on the top-right of the GUI; click **Device Group** and select the available group. To add a FortiGate controller to an existing device group or move a FortiGate to a different group, select the device group where you want to add/move the FortiGate to and click **Edit**. The FortiGate controllers are listed, select the FortiGate you want to add to this group and click **Update**.

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.

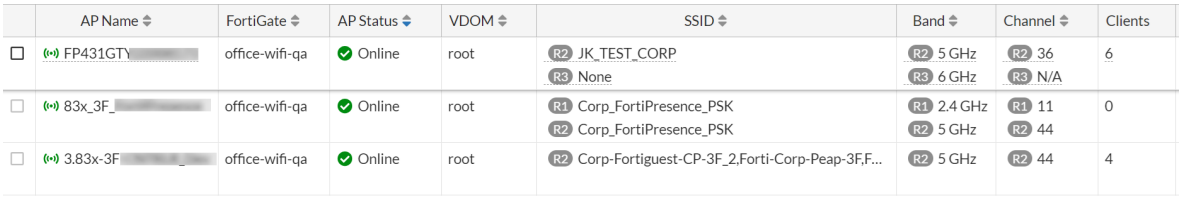
Adding/Managing VDOMs in FortiAIOps

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

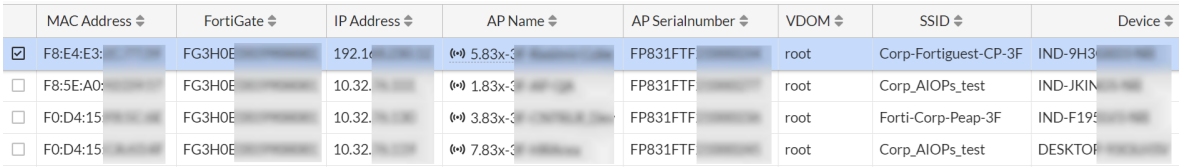
- Add the FortiGates using the root VDOM IP address/hostname.
- The FortiAPs, FortiSwitches, and client information displayed in FortiAIOps dashboards is retrieved from all the VDOMs.

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

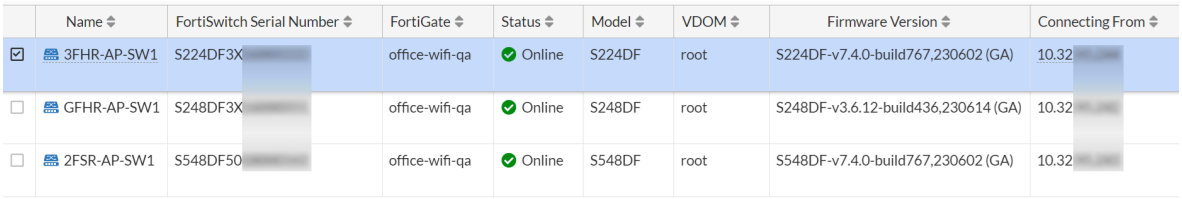
- *Wireless > Access Points*



- *Wireless > Clients*

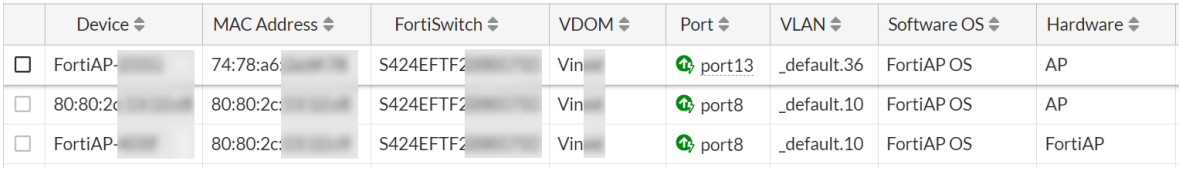


- *Switch > FortiSwitch*



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

- *Switch > FortiSwitch Clients*



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

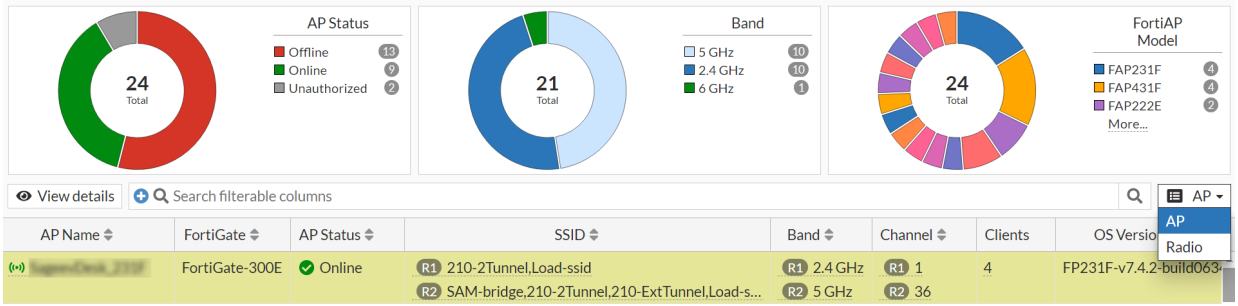
Wireless

The Wireless section of the FortiAIOps provides a comprehensive set of tools for managing and monitoring wireless networks.

- Access Points
- Clients
- Channel Summary
- Applications
- Location Services Monitor
- Heat Maps
- Rogue APs
- Map Management

Access Points

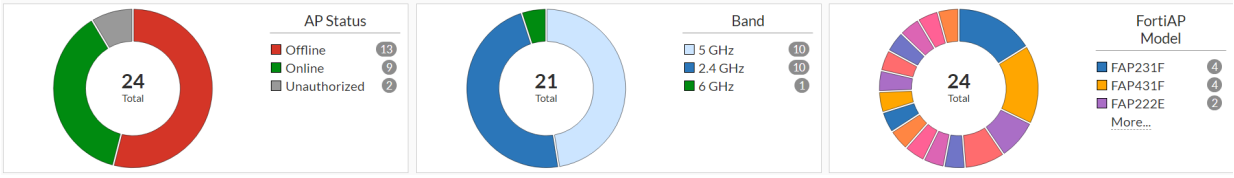
The Access Points page displays essential information about the APs in use and consists of two views - AP and Radio view. To switch between the AP and Radio views, select the desired view from the dropdown menu located at the middle of the Access Points page. By default, the AP is displayed when the page loads.



- AP
- Radio
- Diagnostics and Tools

AP

The AP view displays information related to the Access Point and consists of three widgets - FortiAP status, Channel Utilization, and FortiAP model.



FortiAP Status

The FortiAP Status widget provides information about the status of each AP listed on the page. It displays the current status of the AP, which can be either **Online**, **Offline** or **Unauthorized**.

Band

The band widget provides the number of channels for the 2.4GHz, 5GHz and 6GHz bands. Hovering over the chart displays the number of APs in that band and the percentage of the total channels that they comprise of.

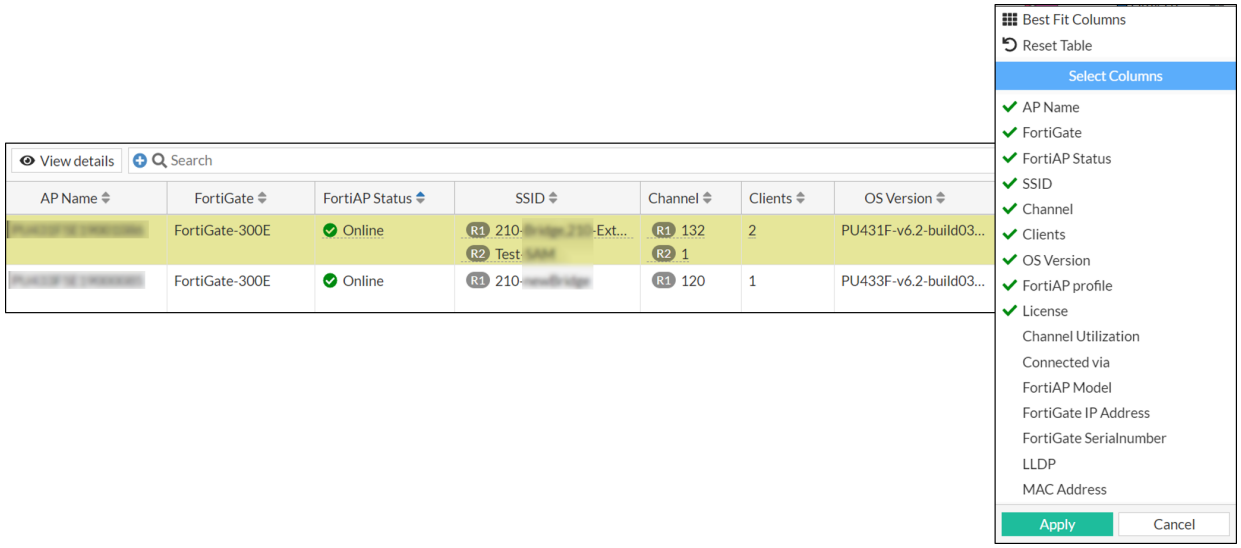
FortiAP Model

The FortiAP Model widget displays the model number of each AP listed on the page. It provides information about the hardware model of the AP and its associated count. This widget is useful for identifying the different models of APs being used in the network.

Note: Click the donut chart in the widgets, to filter the AP table. To reset the filter, click the widget name.

The APs are listed with their relevant details, including the AP name, FortiGate, FortiAP status, SSID , channel, clients, OS version, FortiAP profile and license. To view detailed information about an AP, select the desired AP from the list and click **View Details**. See, Diagnostics and Tools.

Right-click on the header of the table to select the desired columns to add to the table, and then click **Apply** to update the table with the selected columns.



To reset the table to its default state, click **Reset** button. Click **Best Fit Columns** to automatically adjust the column width to fit the data displayed in the table.

To filter the AP list based on the column data, click the filter icon in the column header next to the title, select the value to be filtered and click **Apply**.

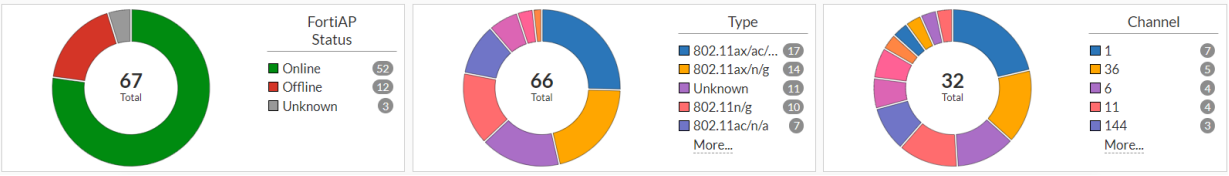
Type in the search term in the search bar located at the top of the AP list. The search term can be a specific AP name, client name, or any other relevant information.

Click the plus icon located to the left of the search bar to perform a more specific search based on a particular column. Select the desired column, and then enter the search term to narrow down the search results to specific criteria.

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.

Radio

The Radio view displays information related to the radios in the AP and consists of three widgets - Status, Type and Channel.



Status

The Status widget displays the current status of each radio, either Online or Offline.

Type

The Type widget displays the type of each radio, such as 802.11a/n/ac or 802.11b/g/n, 802.11ax, 802.11ax-6G, or unknown. This information is useful for identifying the capabilities and features of each radio within the AP.

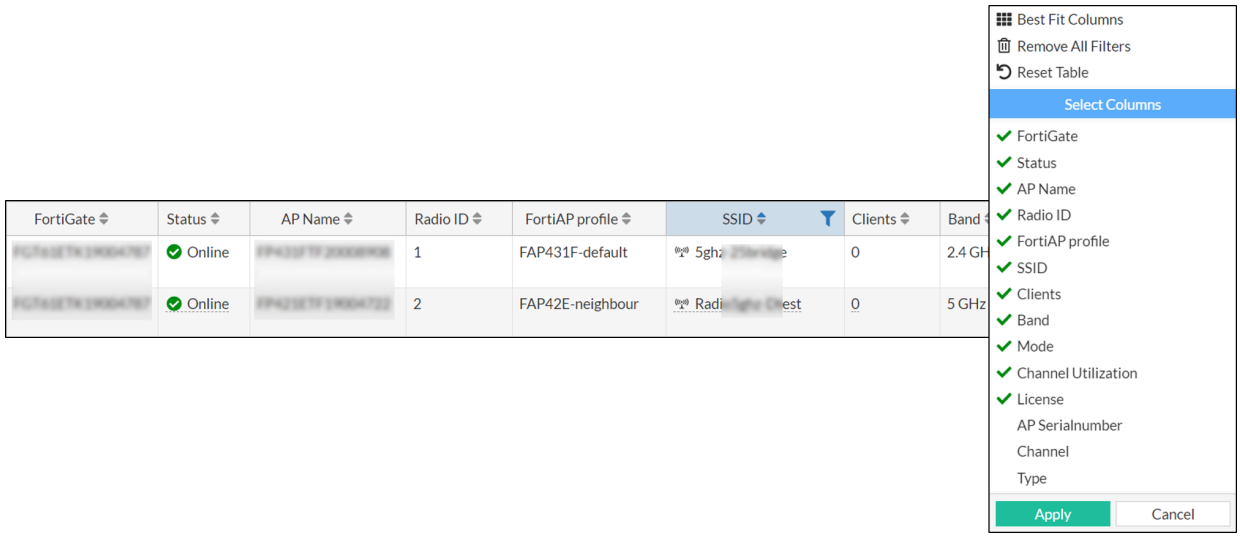
Channel

The Channel widget displays the channel being used by each radio. This information is important for optimizing the network's performance and minimizing interference between radios within the AP.

The radios are listed with their relevant details, including the AP name,AP serial number, FortiGate, FortiAP status, SSID , channel, No of clients, FortiAP profile, Band , Type, Radio ID, AP mode, Channel Utilization and license.

To view detailed information about an AP, select the desired AP from the list and click **View Details**. See, Diagnostics and Tools.

Right-click on the header of the table to select the desired columns to add to the table, and then click **Apply** to update the table with the selected columns.



To reset the table to its default state, click **Reset** button. Click **Best Fit Columns** to automatically adjust the column width to fit the data displayed in the table.

To filter the AP list based on the column data, click the filter icon in the column header next to the title, select the value to be filtered and click **Apply**.

Type in the search term in the search bar located at the top of the AP list. The search term can be a specific AP name, client name, or any other relevant information.

Click the plus icon located to the left of the search bar to perform a more specific search based on a particular column. Select the desired column, and then enter the search term to narrow down the search results to specific criteria.

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.

Access Points Diagnostics and Tools

The *Diagnostics and Tools* pane displays the details about the selected Access Point/Radio and allows you to run diagnostic tests.

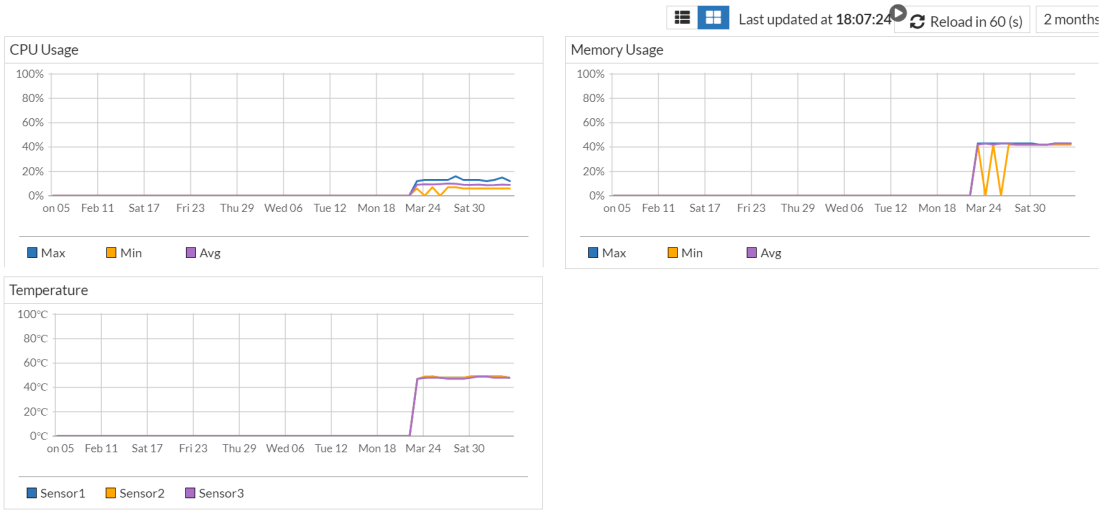
- Performance
- Channel Summary
- Clients
- Interfering SSIDs
- Logs
- Spectrum Analysis
- VLAN Probe

Performance

The performance tab displays trends for the FortiAP health, wireless, and wired clients for selected interval.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.

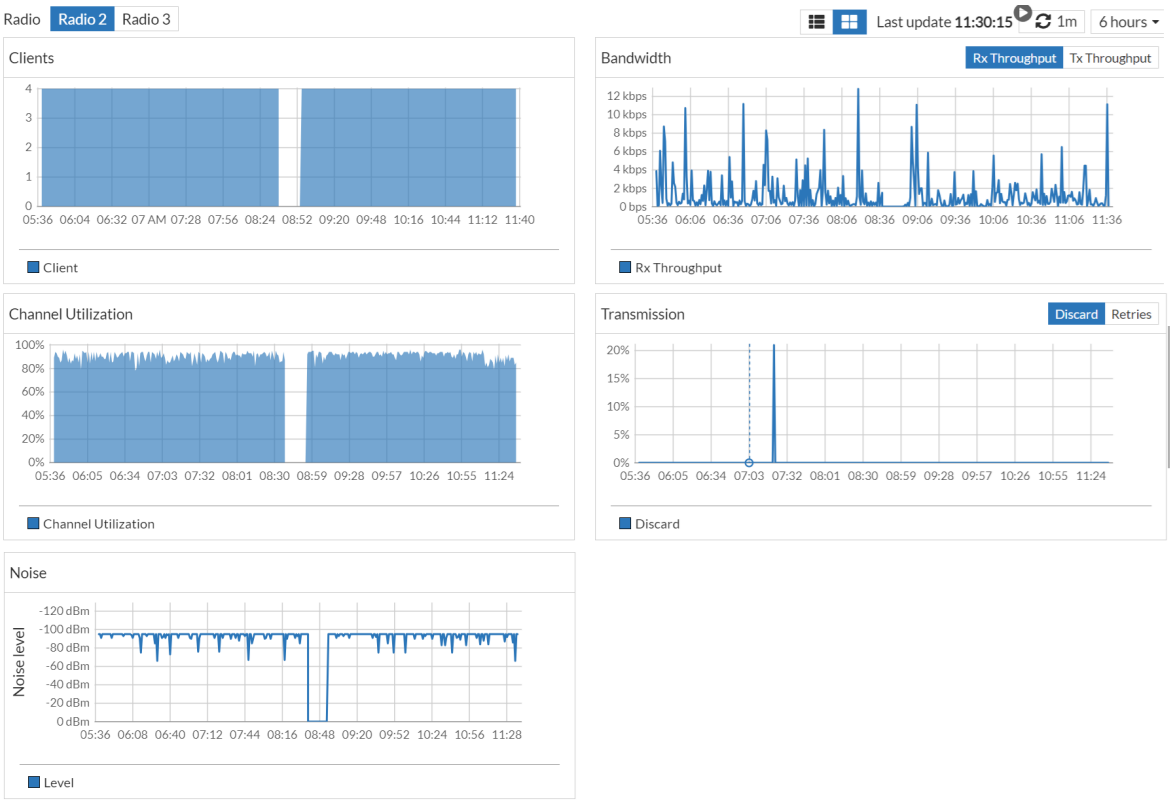
AP Health

This tab monitors and displays the CPU and memory usage by the FortiAP over the selected time interval. At any given point in time, you can view the maximum, minimum, and average CPU and memory usage. This tab also displays the operating temperature of the FortiAP collected by various sensors. The temperatures recorded by all sensors are displayed.

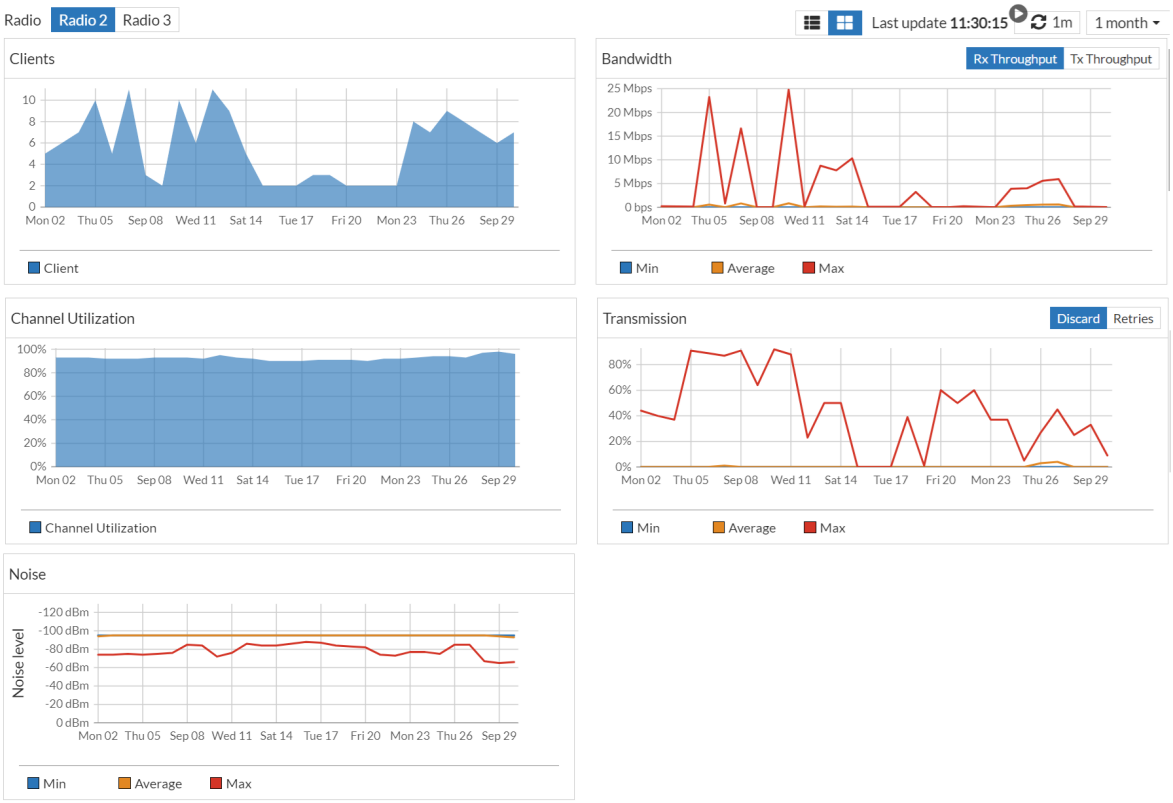


Wireless

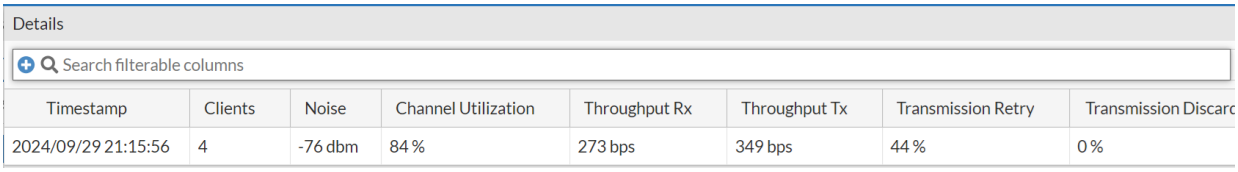
It includes charts for clients, bandwidth, channel utilization, transmission discard, retries, and noise levels on the respective radio interface. The default interval is 10 minutes and can it be changed according to your requirements.



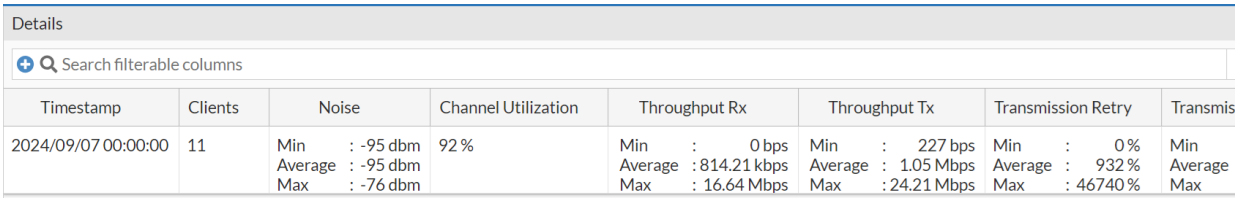
The minimum, maximum, and average values are displayed in the **Bandwidth**, **Transmission** and **Noise** panels when the selected time interval is more than 6 hours, as depicted in the following image.



Click on the graphs for a specific time to view details. The following image depicts the details displayed for an interval of less than 6 hours.



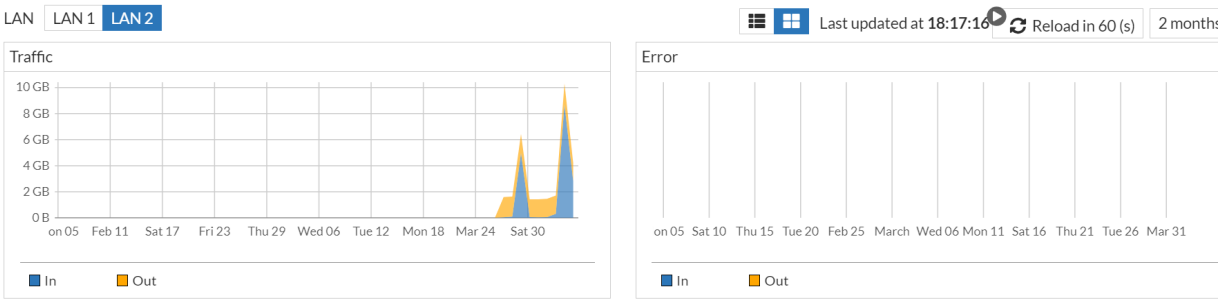
The following image depicts the details displayed for an interval of more than 6 hours.



Wired

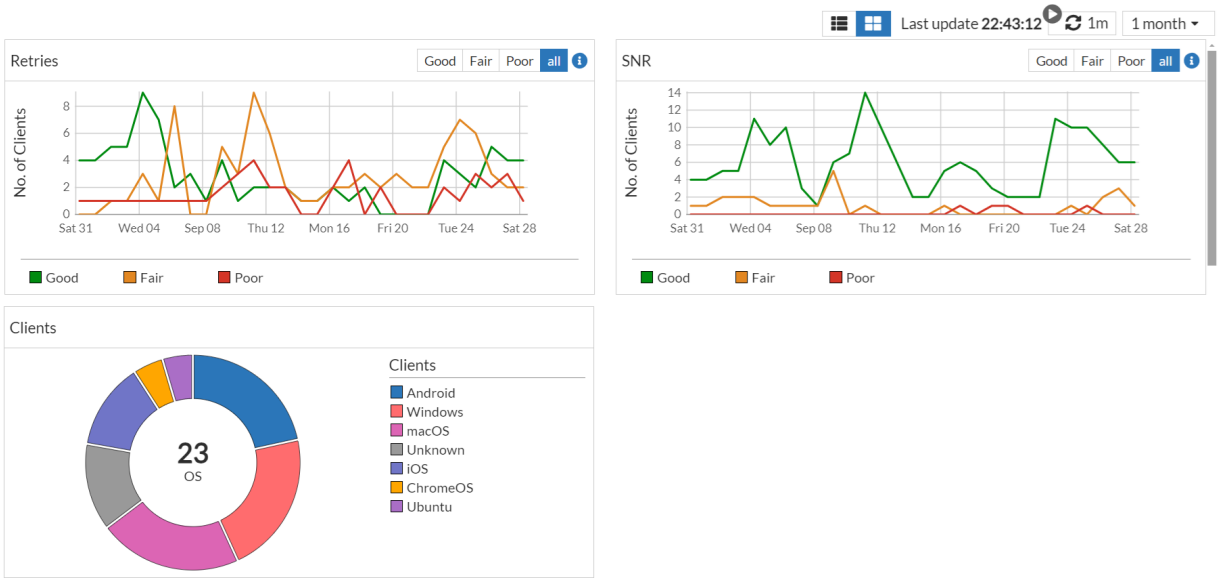
The LAN port statistics are now displayed for access points. You can view the traffic coming into a LAN port and the traffic leaving it at a given point in time. Also, the error statistics for both incoming and outgoing traffic is displayed.

Note: The LAN port status is not displayed for FAP-421E and FAP-423E.



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

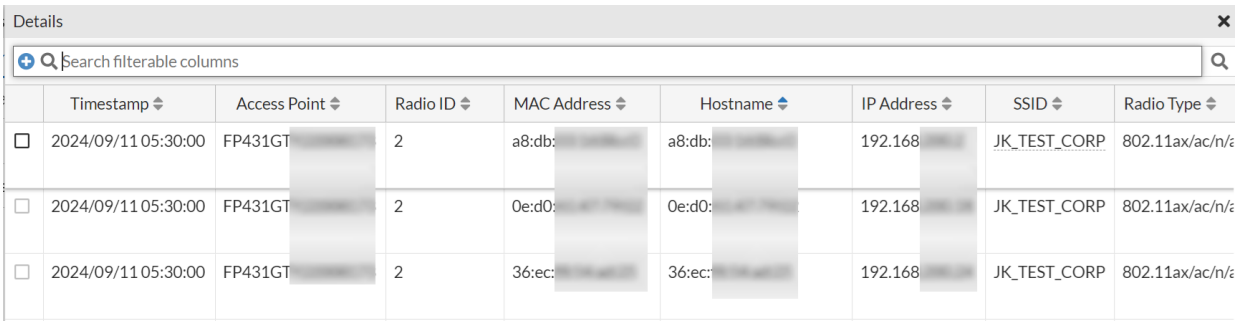
The statistics for SNR are categorized as good, fair, and poor based on the following criteria.

- **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

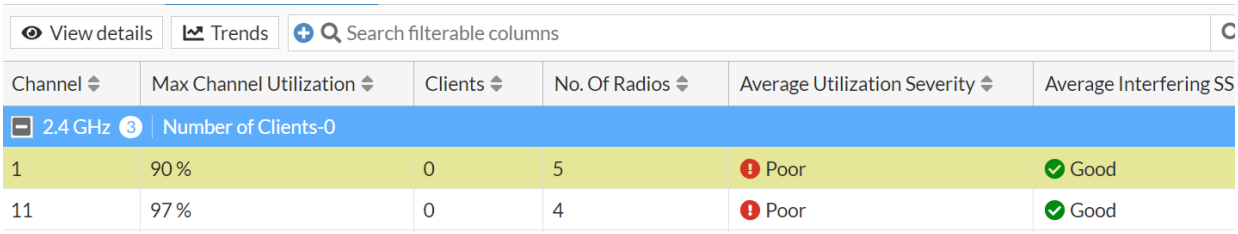
This panel provides the total number of clients and also the number of clients associated with each OS type. Hover over the graph or the OS name to view details.

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.



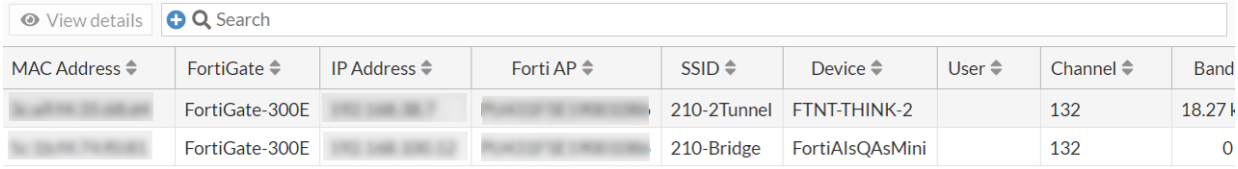
Channel Summary

This page provides granular insights into the performance of each channel with detailed statistics and trends. For more information, see Channel Summary.



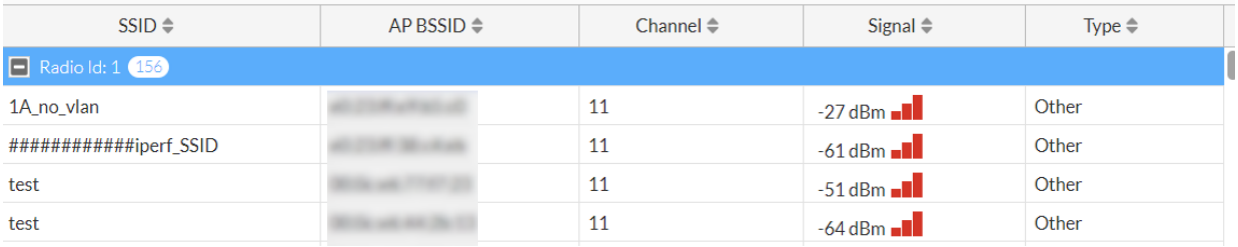
Clients

The Clients tab displays a list of clients currently connected to the selected AP, along with details such as the client MAC address, FortiGate and IP Address, FortiAP name , associated SSID, user name , operating channel and the radio details, Tx and Rx bandwidth, signal strength and noise, VLAN ID, RF band, the wireless standard, and the time of association. This information is useful for identifying any clients that may be experiencing connectivity issues or data usage problems. To view detailed information of a client, select the client and click **View details**.



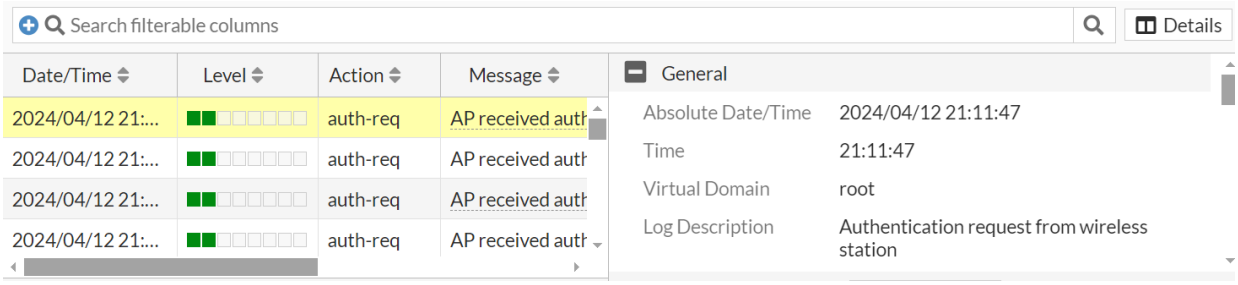
Interfering SSIDs

The Interfering SSIDs tab displays the details of interfering SSIDs associated with an AP; the interfering SSID page displays the associated SSID, related AP BSSID, operating channel, signal strength and the radio details are displayed in the AP dashboard. To view the interfering SSID details, ensure that the AP radio is using Radio Resource Provisioning or a WIDS profile in FortiGate (Managed FortiAP Profile).



Logs

The Logs tab provides detailed logs of events related to the selected AP/Radio. To view detailed information, select log and click **Details**.



Spectrum Analysis

Spectrum Analysis tab provides visual spectrum analysis capabilities that scan radios for RF channel conditions and sources of interference which can potentially impact WLAN efficiency. Based on the spectrum analysis data, corrective measures such as determining optimal channel planning, debugging client related connectivity issues and automatic transmit power settings are initiated. This facilitates quality wireless service levels by ensuring the optimal usage of the channels considering the information provided by the FortiAIOps spectrum analyser. Both 802.11 and non-802.11 sources of interference can be detected and analyzed by the spectrum analyzer.

Notes:

- Spectrum analysis is supported for all channels when the radio is in the dedicated monitor mode, and for selected channels when the radio is in the AP mode.
- FortiAP supports spectrum analysis and is online.

Select the channels to be scanned and configure the scan duration, the spectrum analysis is performed on 2.4 GHz, 5 GHz, and 6 GHZ frequency bands. The spectrum analyzer result displays widgets with the type of interference, signal strength, impacted channels, and wireless spectrum current utilization, start and end time and duration of the interference. It classifies wireless & non-wireless interferences to easy identification of the source.

- You can select the **AP**, **Radio**, and **Channels** to be scanned for interferences.
- The **Scan Duration** can be set to 1, 5, 30, or 60 minutes.
- The **Sampling Interval** and the number of **Spectrogram Samples** cannot be modified.

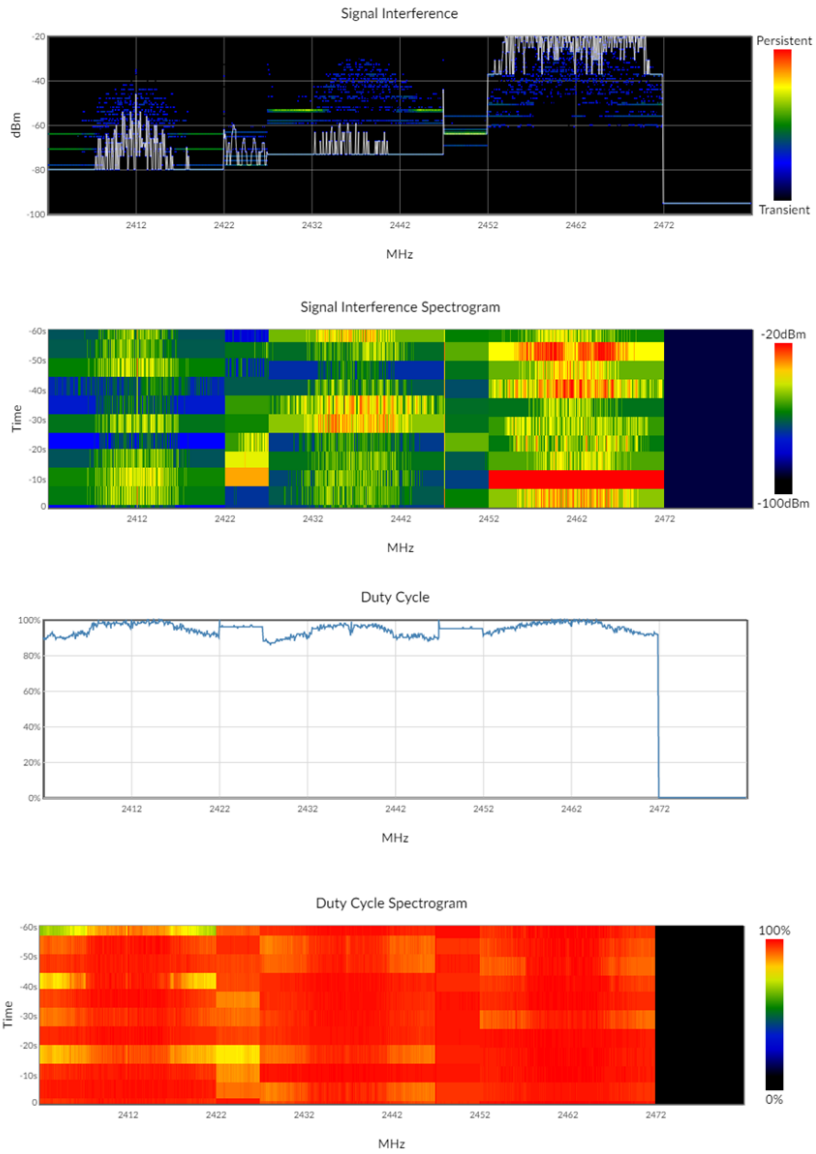
Select **Start** and the GUI periodically polls the spectrum analysis data based on the fixed sampling interval of 1000 milliseconds. Data is visualized as 4 charts representing signal interference marking the noise levels for each channel, signal interference spectrogram representing 60 samples for different channels at specific time

intervals, the duty cycle charts marking the extent to which a non-WiFi device/neighbouring AP is interfering, and the duty cycle spectrogram representing 60 such duty samples for each channel over a period of time.

The tabular data for non-WiFi interference displays the time and frequency of last detection and any of the following type of devices causing the interference.

- Microwave ovens
- Video bridges
- Wi-Fi, DSSS cordless phones
- Bluetooth, FHSS cordless phones

The tabular data for WiFi interference displays the online neighbouring AP's BSSID, SSID, maximum signal strength, and channel and time of last detection.

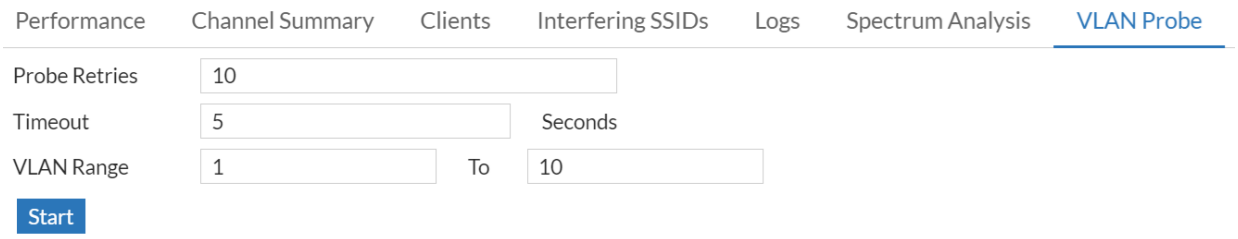


VLAN Probe

VLAN probe tab enables FortiAPs to probe connected VLANs and subnets. It sends DHCP probes from the FortiAP's Ethernet interface to specific VLANs on the wired interface and returns information on their availability and subnet details. This helps diagnose and troubleshoot WiFi deployment issues.

- **Probe Retries** – Configure the number of retries before timeout. The valid range is 1 to 10 with a default value of 6.
- **Timeout** – Configure the timeout for the VLAN probe. The valid range is 1 – 60 seconds with a default value of 10 seconds.
- **VLAN Range** – Select the range of VLANs to probe. The valid range is 1 - 4094.

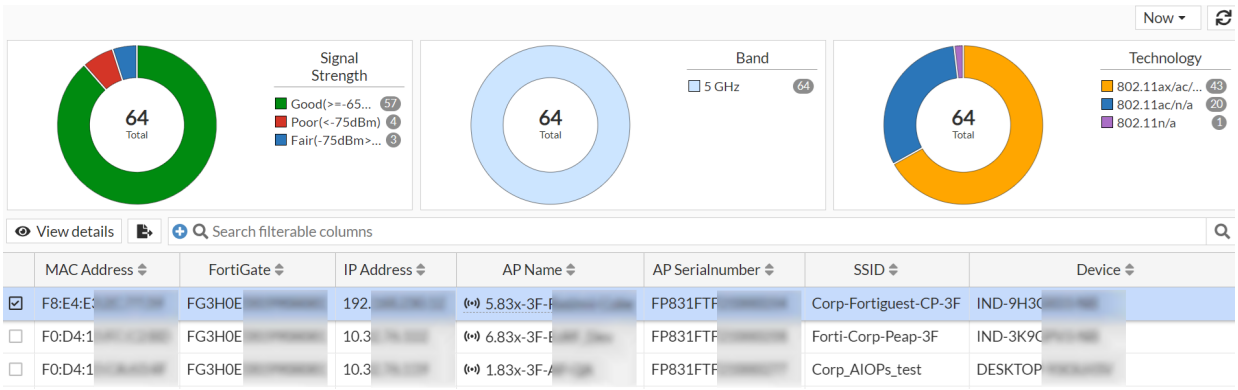
Select **Start** to initiate VLAN probe as per configurations.



Wireless Clients

The Clients page provides information about the clients connected to the wireless network and consists of three widgets - signal strength, band, and technology.

- You can filter the wireless client data for a selected duration or a customized time slot.The **Custom range** allows the selection of a minimum of 1 hour and maximum of 1 week, the option of **Now** displays data for the last 1 minute.



Signal Strength

The signal strength widget provides information about the strength of the signal between each client and the access point. It displays the signal strength in dBm, which is a measure of signal power. A higher dBm value indicates a stronger signal, while a lower dBm value indicates a weaker signal.

Band

The band widget displays the band that each client is connected to. It indicates whether the client is connected to the 2.4 GHz, 5 GHz or 6 GHz band.

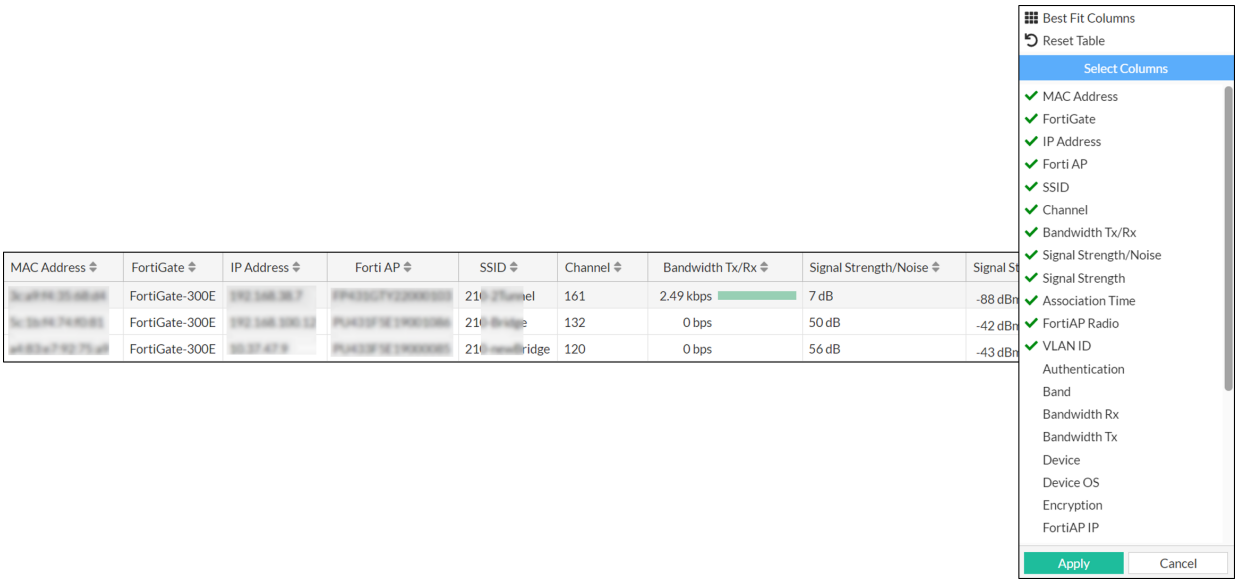
Technology

The technology widget displays the technology that each client is using to connect to the wireless network. It indicates whether the client is using 802.11a/b/g/n or 802.11ac technology.

The clients are listed with their relevant details, including the MAC address, FortiGate, IP address, FortiAP, SSID, channel, bandwidth, and signal strength. To view detailed information about a client, select the desired client from the list and click **View Details**. See, Clients Diagnostics and Tools.

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.

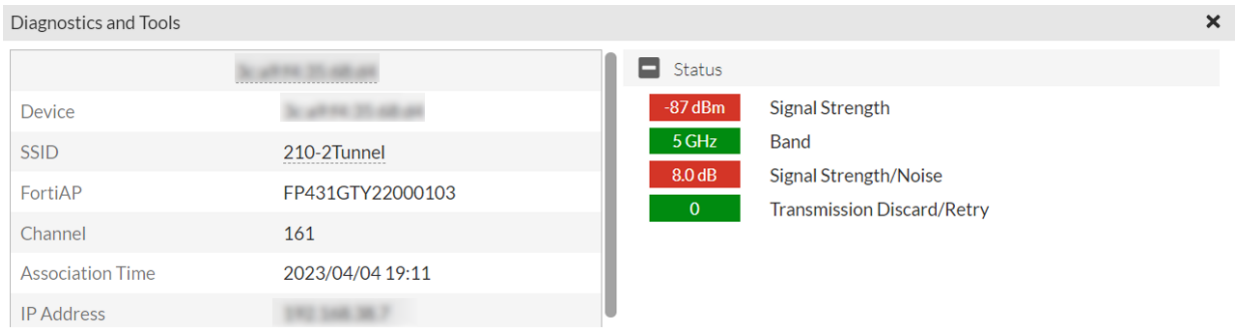
Right-click on the header of the table to select the desired columns to add to the table, and then click **Apply** to update the table with the selected columns.



Wireless Clients Diagnostics and Tools

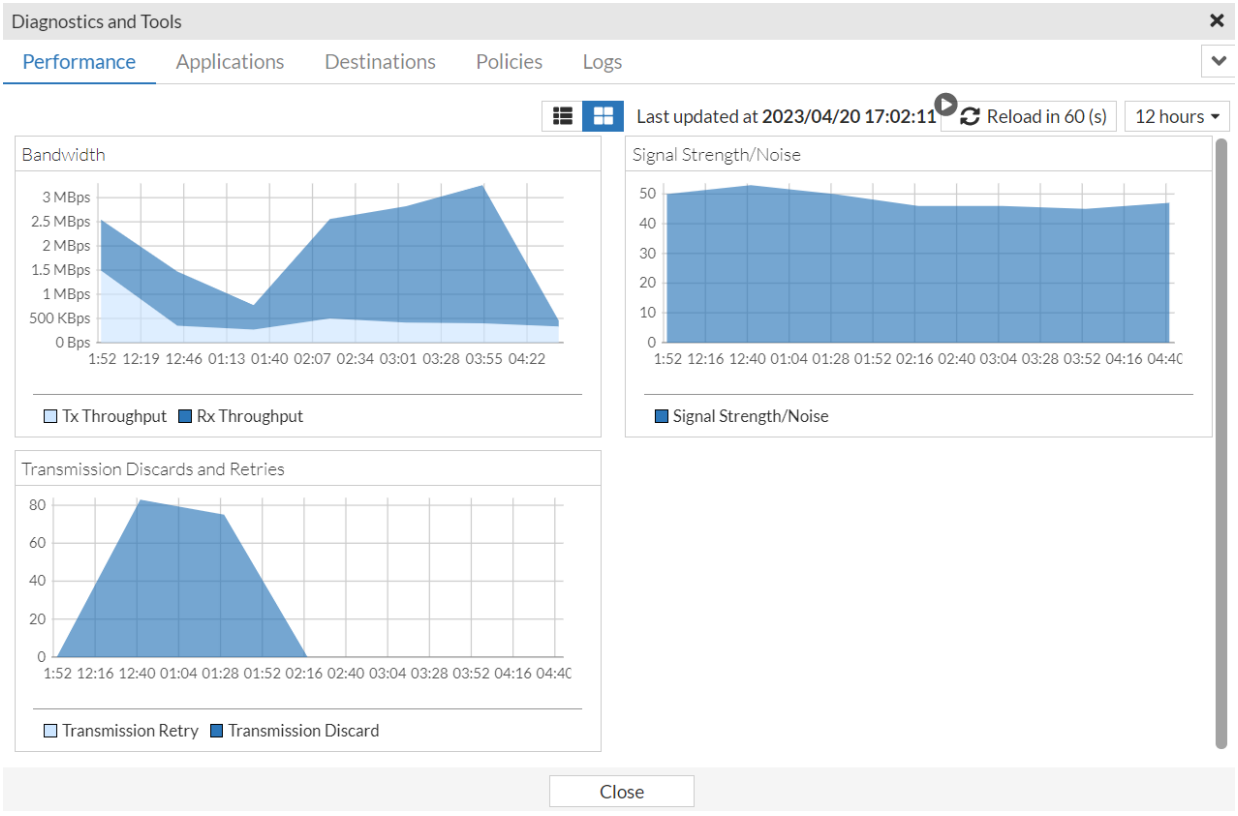
The *Diagnostics and Tools* pane displays the details about the selected Client and allows you to run diagnostic tests.

- Performance
- Applications
- Destinations
- Policies
- Logs



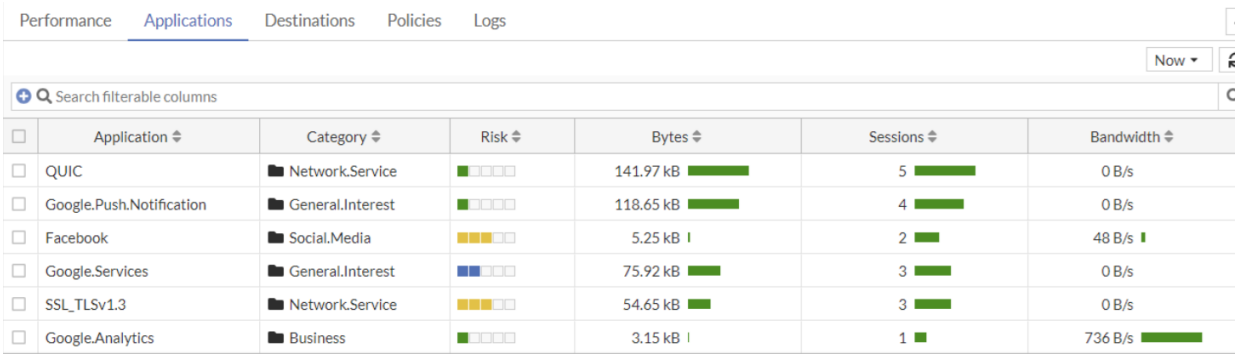
Performance

The **Performance** tab displays information about the client's performance, including data charts for bandwidth, signal strength, and transmission discards and retries. 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**.



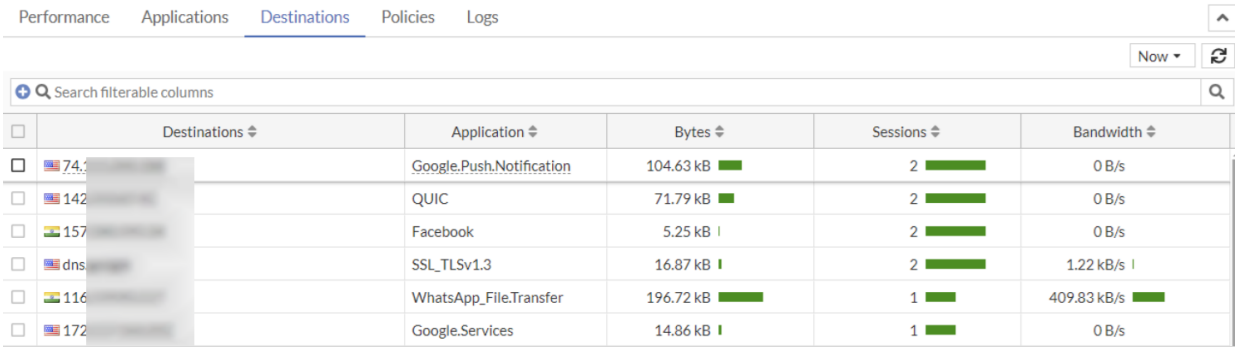
Applications

The Applications tab displays a list of applications in use by the selected client, along with details such as the application name, category, risk, data usage, session and bandwidth details.



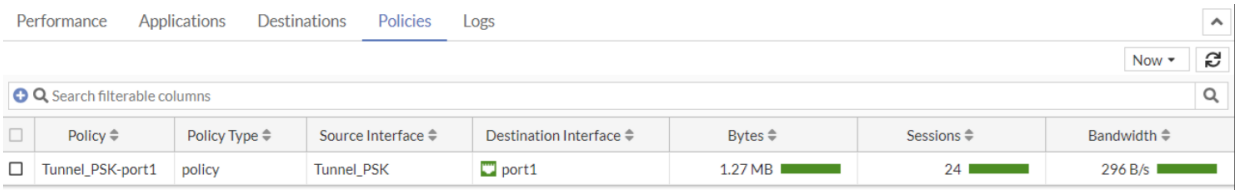
Destinations

The Destinations tab displays a list of network destinations accessed by the selected client, along with details such as the destination IP address, application name, data usage, session and bandwidth details.



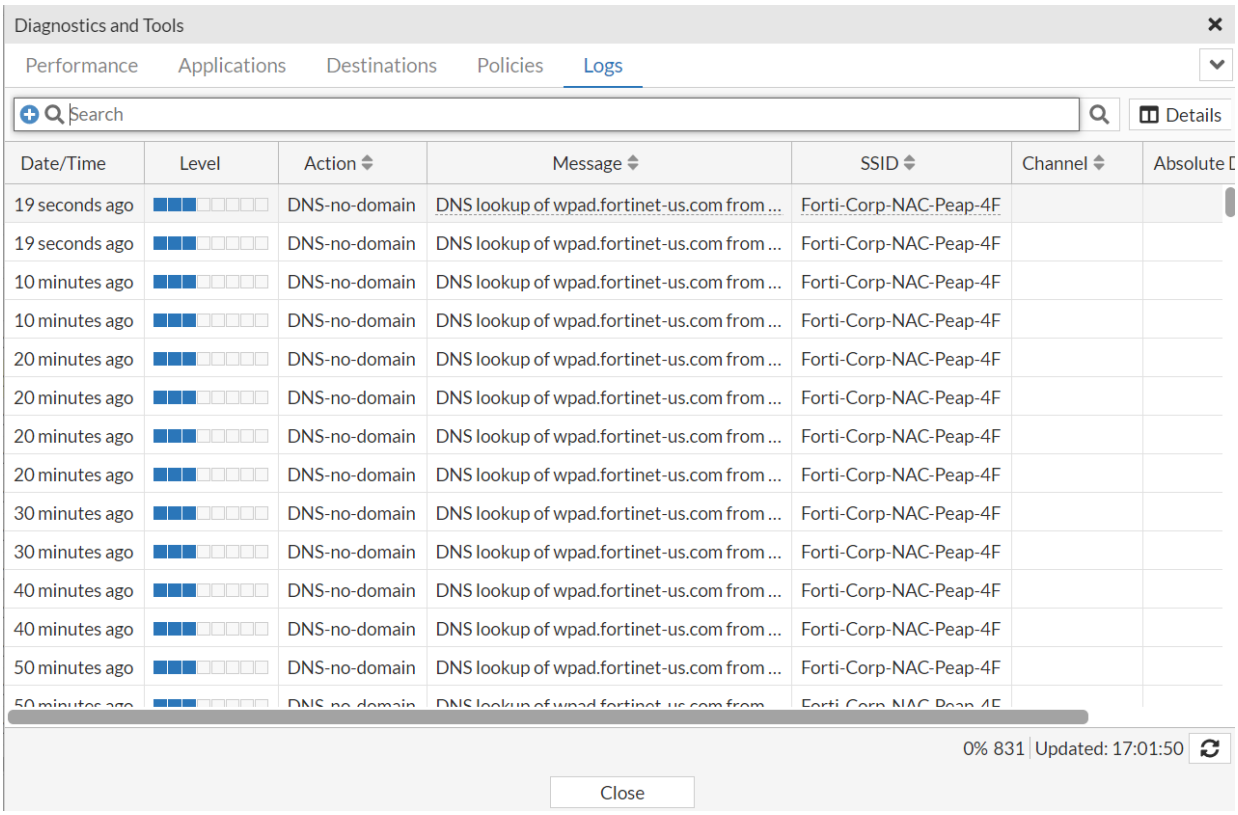
Policies

The Policies tab displays information about any policies applied to the selected client, such as policy name, policy type, source interface, destination interface, data usage, session and bandwidth details.



Logs

The Logs tab displays detailed logs of events related to the selected client, allowing you to troubleshoot any issues. To view detailed information, select log and click **Details**.



Channel Summary

The Channel Summary window provides information categorized within the following sub-tabs:

- Summary
- Events
- Insights

To access, navigate to **Wireless** > **Channel Summary**.

Summary

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

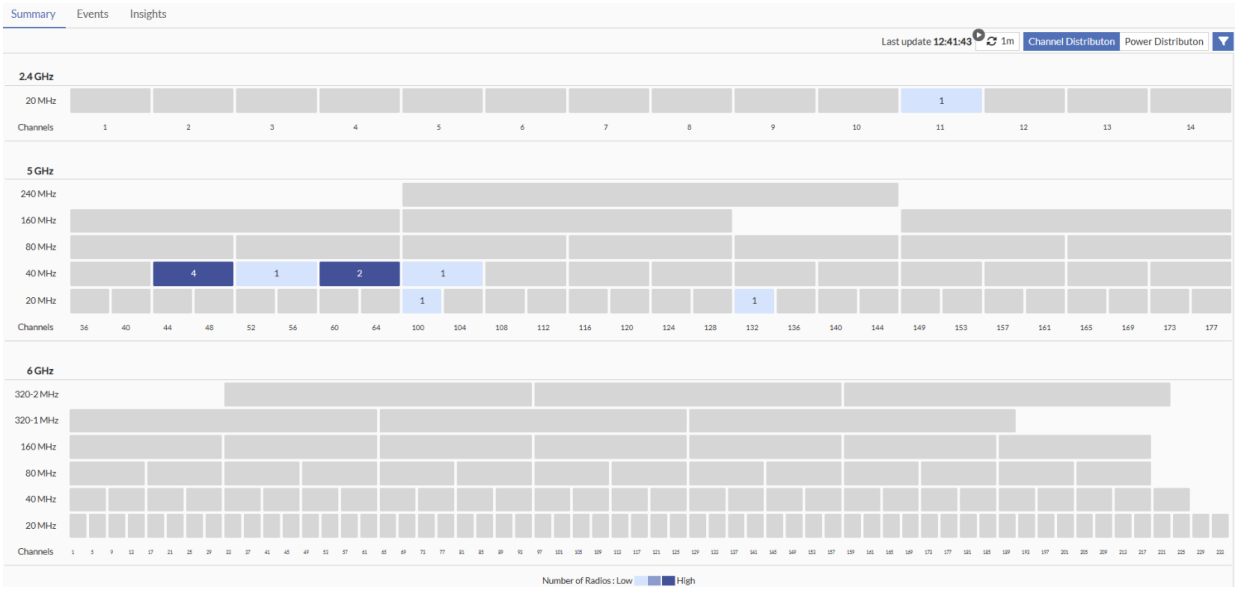
Toggle between the **Channel Distribution** and **Power Distribution** options for relevant information.

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.

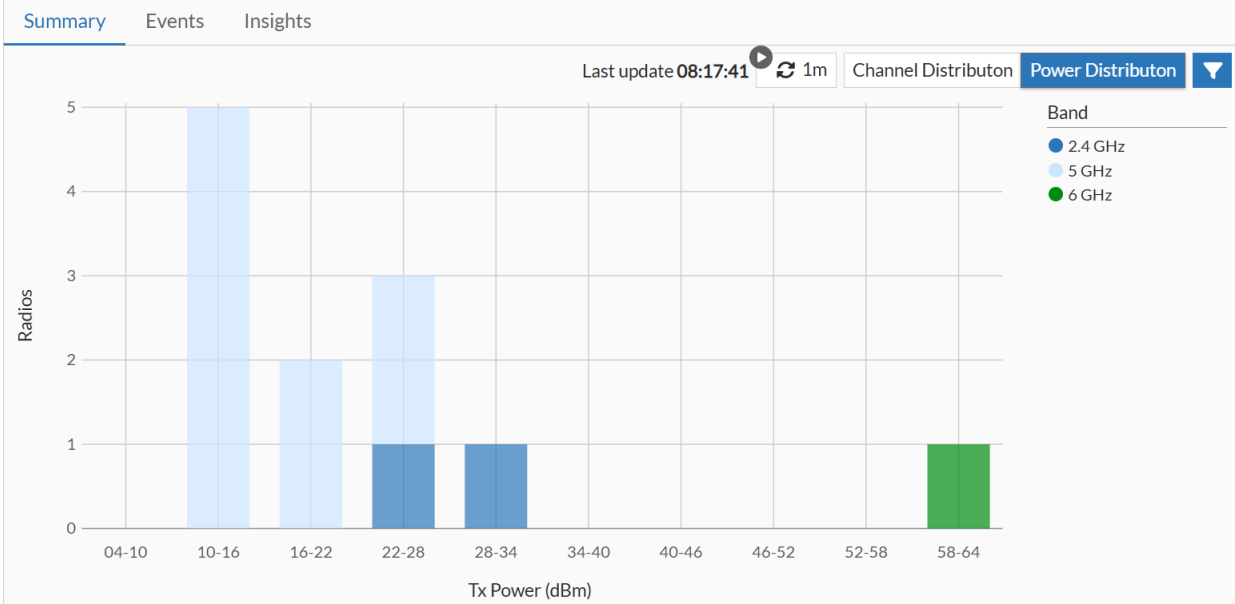
Power Distribution

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.

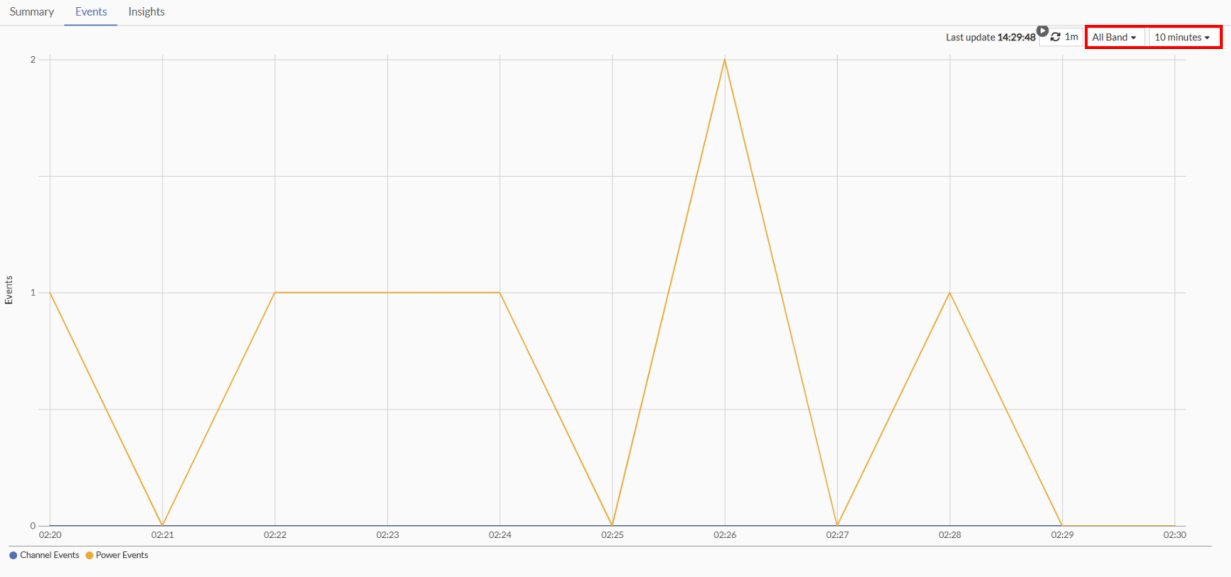
Use the **Filter** option to select FortiAPs and Radios at specific location such as Site, Building, and Floor.



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.



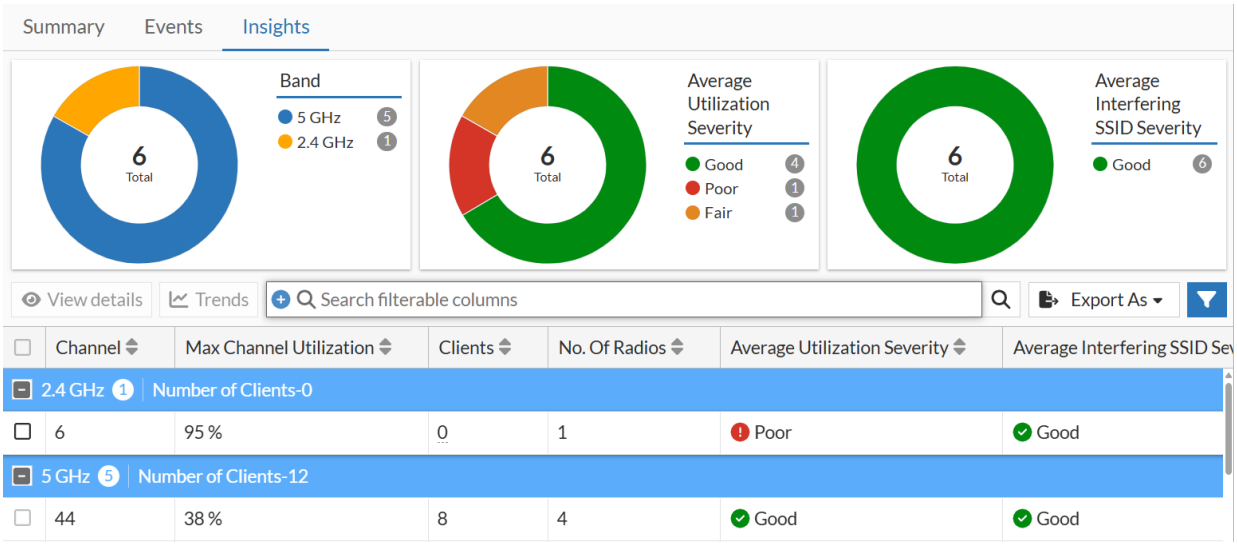
Select the desired bands and time period for the chart using the drop-down menus.

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.



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

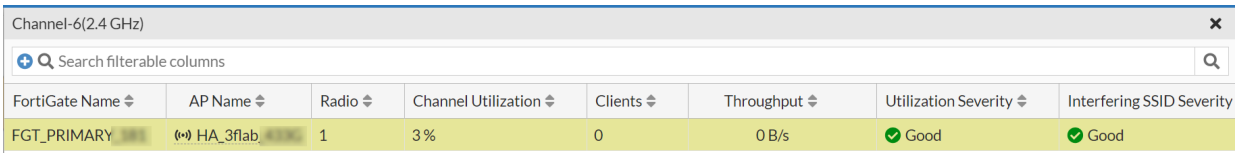
Average Utilization Severity

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**.



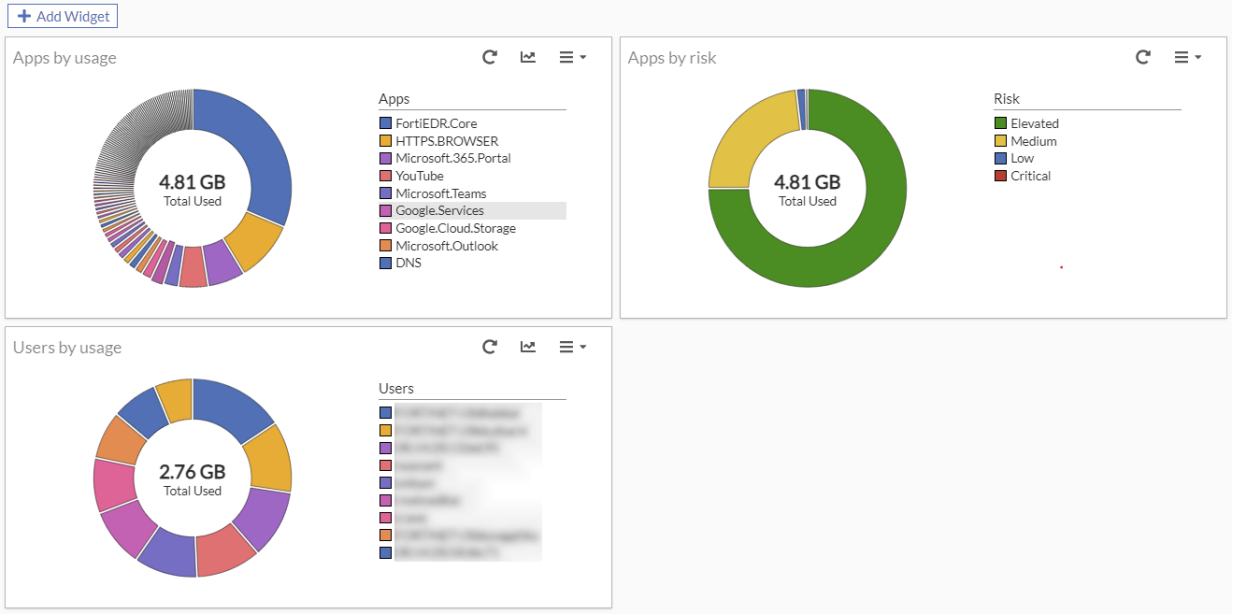
Field	Description
FortiGate Name and **AP Name**	The names of the FortiGate controller and FortiAP associated with the selected channel.
Radio	The radio operating on the selected channel.
Channel Utilization	Total channel utilization (in percentage) per radio.
Clients	The number of clients connected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

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.

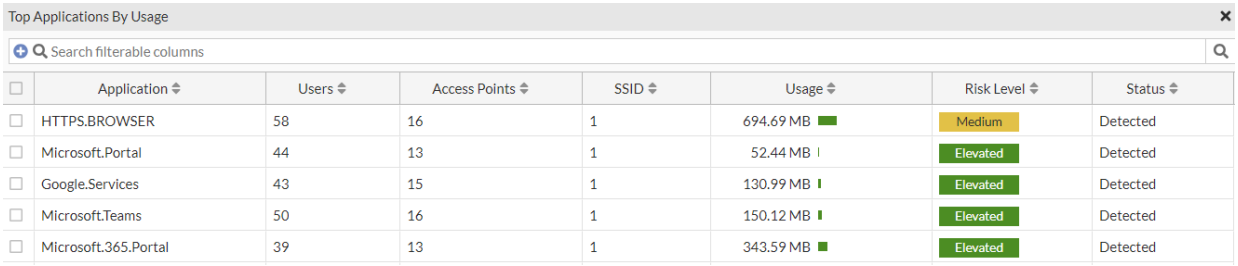
Applications

The Applications page provides information about the applications used by clients on the wireless network. This page consists of three widgets - Apps by usage, Apps by risk, and Users by usage.



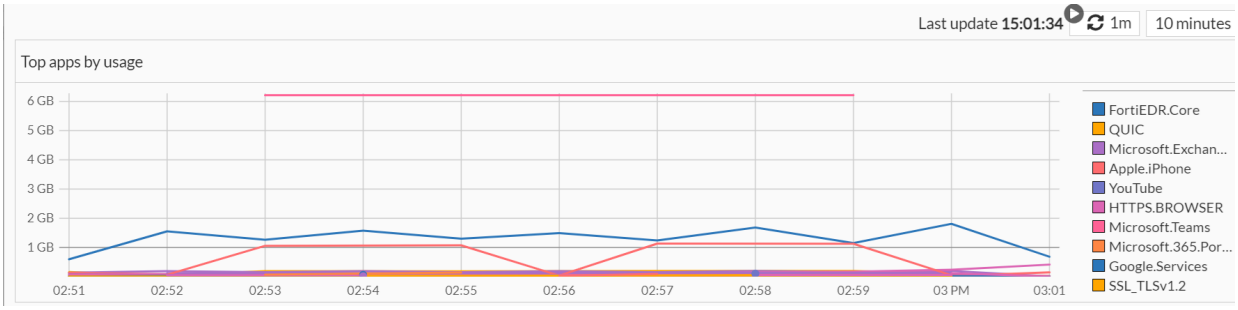
Apps by usage

The Apps by Usage widget displays a list of applications in use on the network, sorted by the amount of data each application is using.



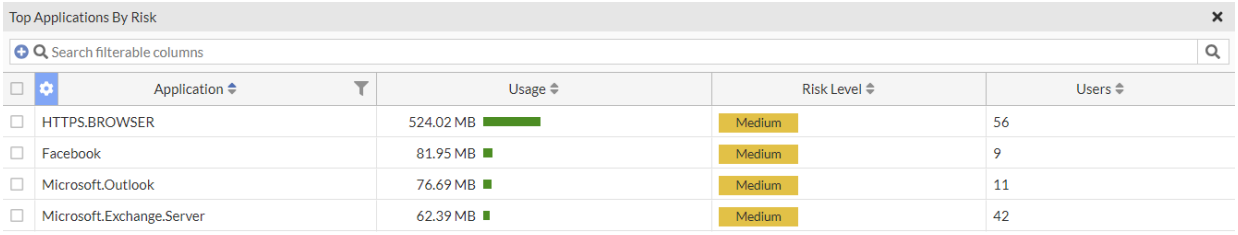
Application	Users	Access Points	SSID	Usage	Risk Level	Status
HTTPS.BROWSER	58	16	1	694.69 MB	Medium	Detected
Microsoft.Portal	44	13	1	52.44 MB	Elevated	Detected
Google.Services	43	15	1	130.99 MB	Elevated	Detected
Microsoft.Teams	50	16	1	150.12 MB	Elevated	Detected
Microsoft.365.Portal	39	13	1	343.59 MB	Elevated	Detected

Click on the trends icon to view the application usage trends. 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**.



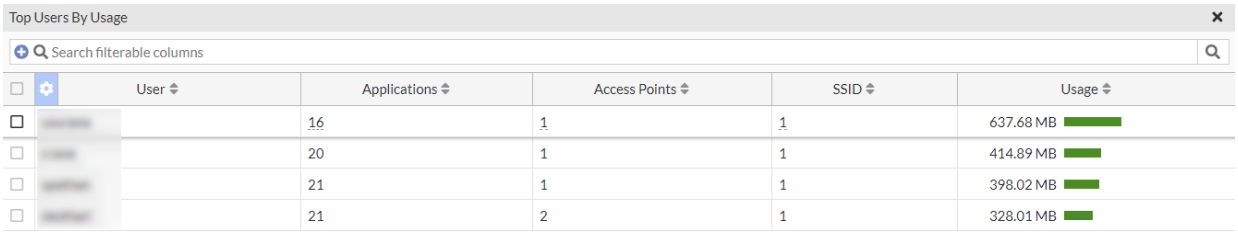
Apps by risk

The Apps by Risk widget displays a list of applications in use on the network, sorted by their risk level.

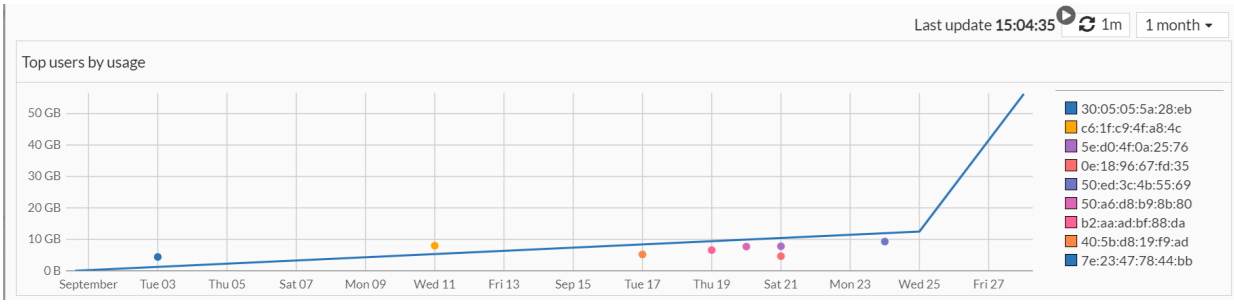


User by usage

The User by usage widget displays a list of clients on the network, sorted by the amount of data each client is using.



Click on the trends icon to view the application user trends. 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**.



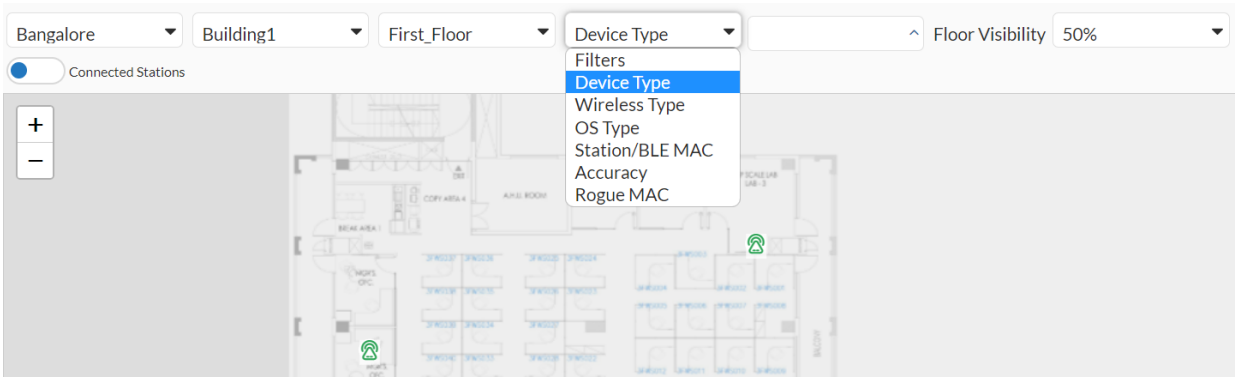
Location Services Monitor

The Location Services Monitor page plots the current location of all stations and rogue APs on the floor map imported into FortiAIOps. FortiAIOps plots the current location based on the location feed received from FortiGates (which are in turn connected to APs) and does not display the movement of the stations.

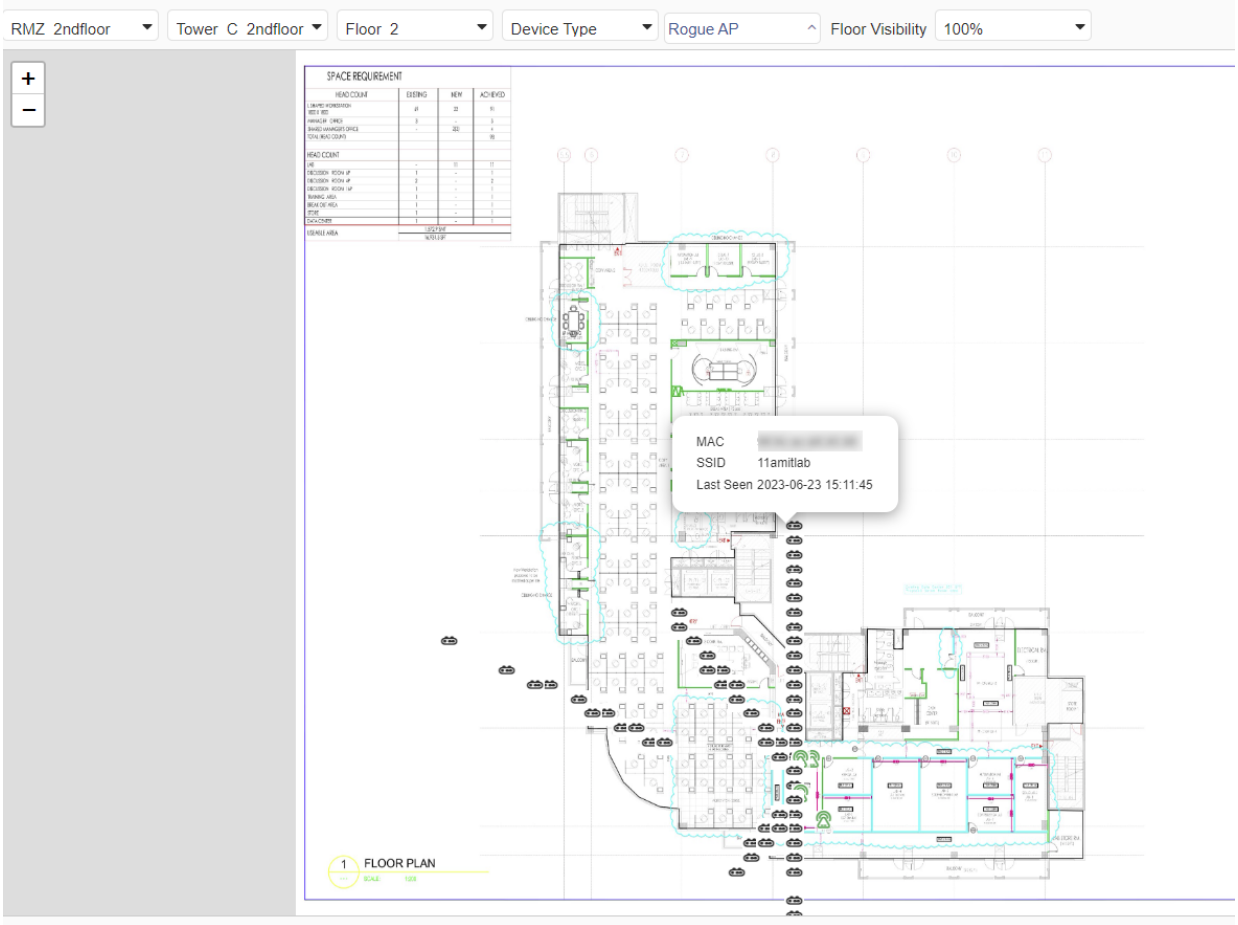
You can filter and view device locations based on the site, building, and floor. The following filters can be applied.

- Device Type
- Wireless Type
- OS Type
- Station/BLE MAC
- Accuracy
- Rogue MAC

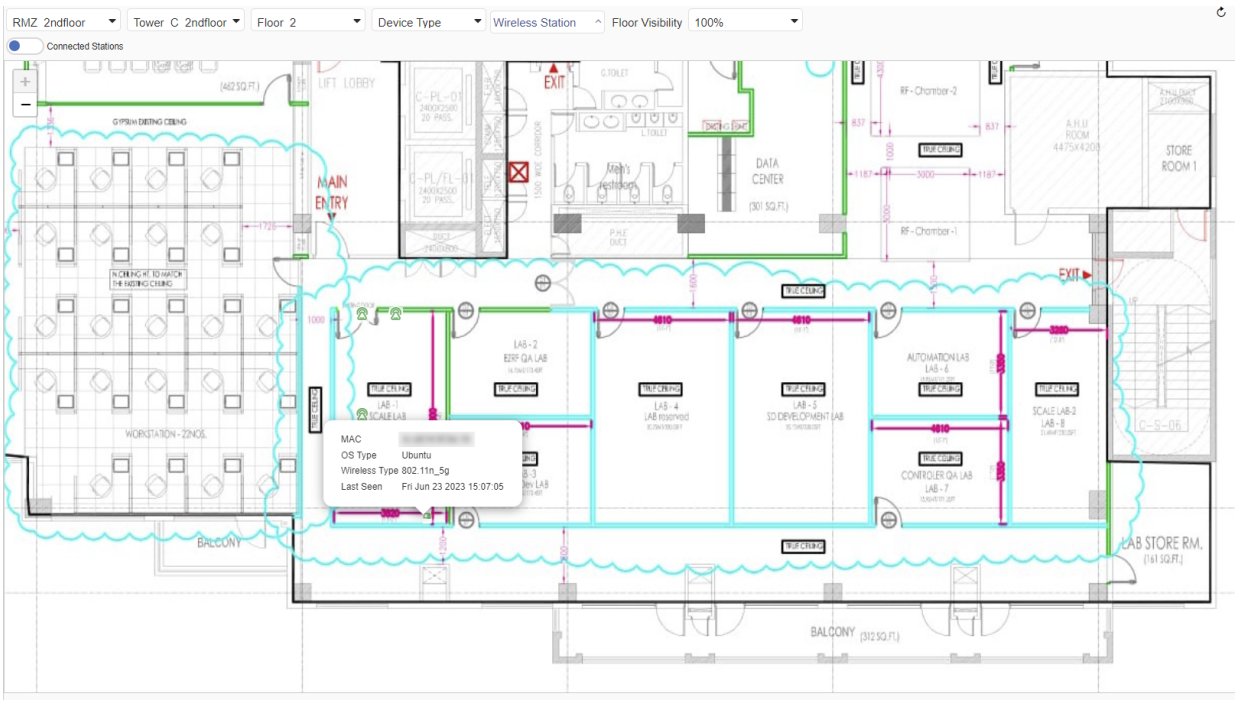
You can set the Floor Visibility and magnify the floor view.



Select **Rogue AP** as the **Device Type**, to view the rouge AP location.



Select **Wireless Station** as the **Device Type**, to view the stations location.



Click **Connected Stations** toggle to switch to **Connected & Discovered Stations** view.

Heat Maps

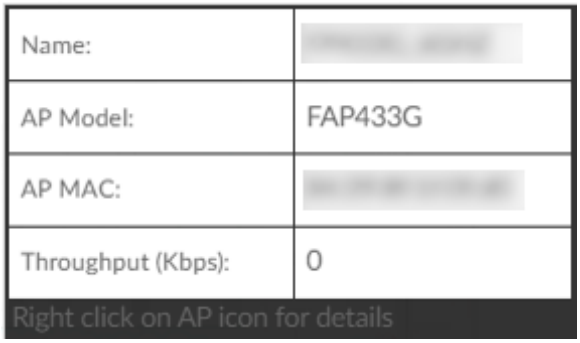
The heat map allows you to verify the coverage and performance of your WLAN APs. You can also use the maps to visually locate APs sending alarms. Use the map editor to set up your site maps.

- In the Network Heat Maps screen, select a Location from the menu on the left to see the corresponding map.
- Hover the mouse pointer over the objects on the screen to see details. For example, for this throughput map, by hovering the mouse pointer on an AP icon displays the Name, model, Mac Address, status of the AP and throughput value. If you change the Heat Map Type, be sure to click Refresh icon.
- In the Network Heat Maps screen select a floor. The following five types of heat maps can be viewed.

Throughput Heat Map

Throughput maps display the AP throughput over the represented area. The APs on the map are differentiated by using different colors to represent the corresponding AP throughput value.

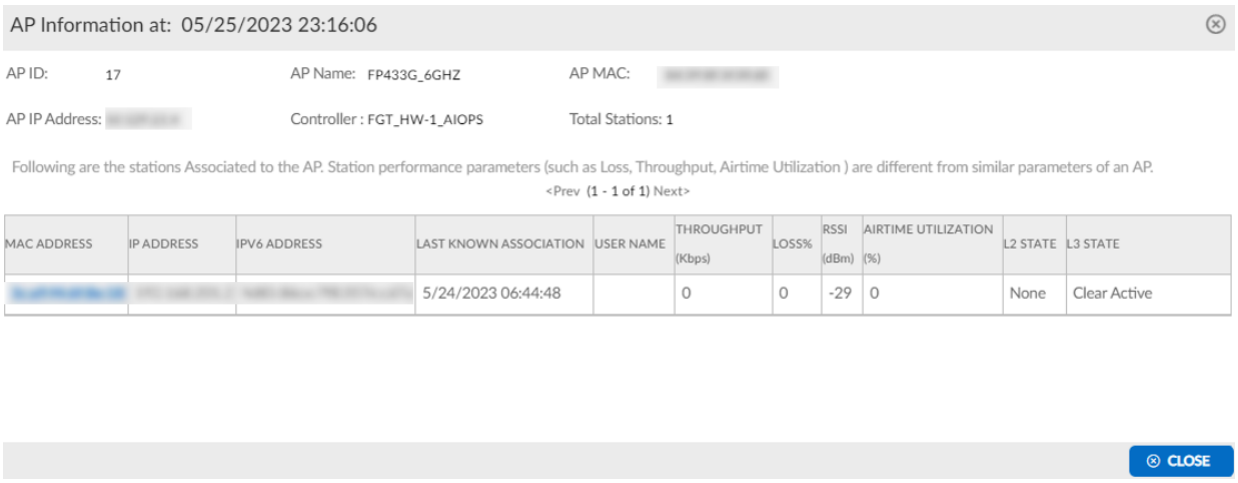
Hover over AP to view the AP information including name, AP model, MAC address, AP status, and throughput in Kbps.



To view AP and Station details in any of the heat maps, right-click an AP icon and click **Show Details**

- **AP Details**: AP ID, AP Name, AP MAC Address, AP IP Address, Controller, Total Stations.
- **Station Details**: MAC Address, IP Address, Last Known Association, User Name, Throughput, Loss%, RSSI, Airtime Utilization, L2 State, L3 State.
- To view Station Trend Dashboard, click MAC Address.

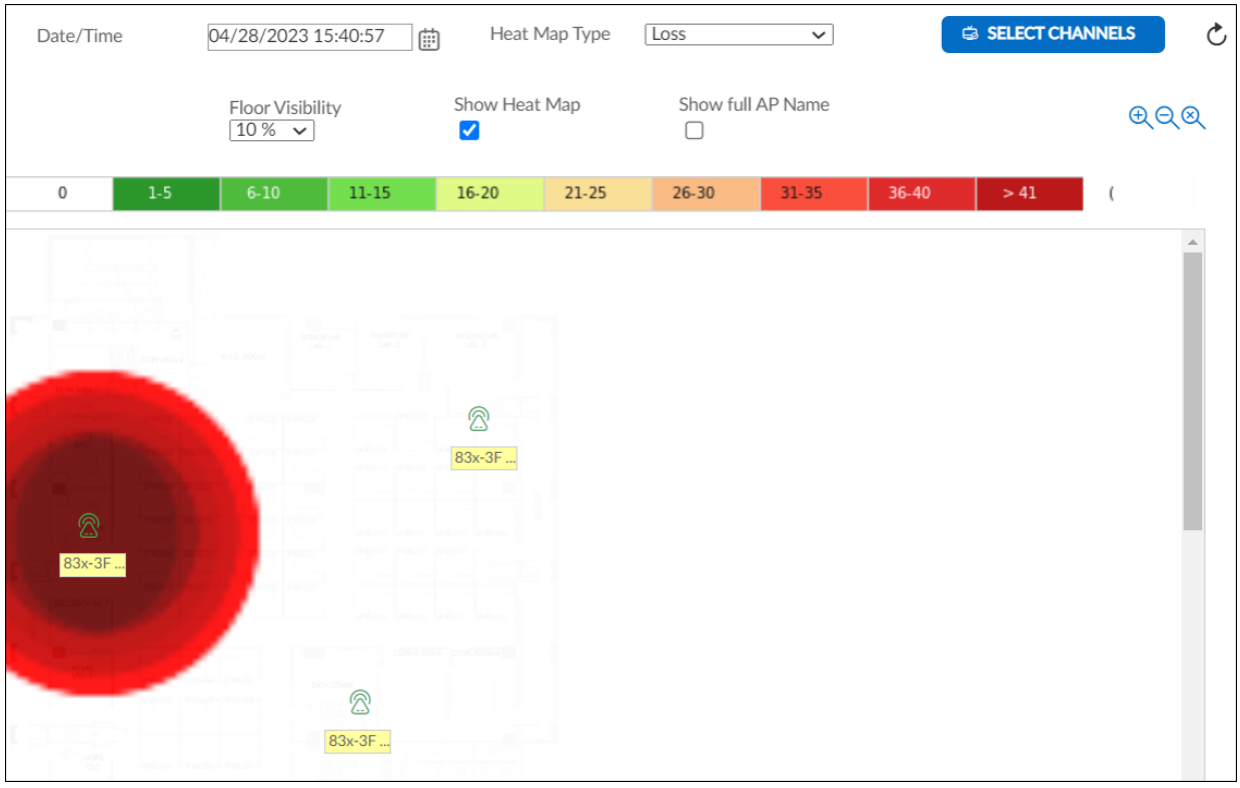
The filtering option comprises of All, 2.4 GHz [default], 5 GHz, 6 GHz and selected channels within the three bands.



Loss Heat Map

Loss maps show the AP loss over the represented area. The APs on the map are differentiated by using different colors to represent the corresponding AP Loss% value.

Hover over AP to view the AP information including name, AP model, MAC address, AP status, and loss %. Right click on AP icon and click **Show Details** to view detailed information.



Channel Utilization Heat Map

The Channel Utilization maps differentiate APs on the map by using different colors for the regions around APs corresponding to the AP channel utilization value.

Hover over AP to view the AP information including name, AP model, MAC address, AP status, and channel utilization (%). Right click on AP icon and click **Show Details** to view detailed information.

Number of Stations Heat Map

The Number of Stations Heat Map, represents the low signals over the area represented by the map. The Number of Stations maps differentiate APs on the map by using different colors for the regions around APs corresponding to the number of stations per AP.

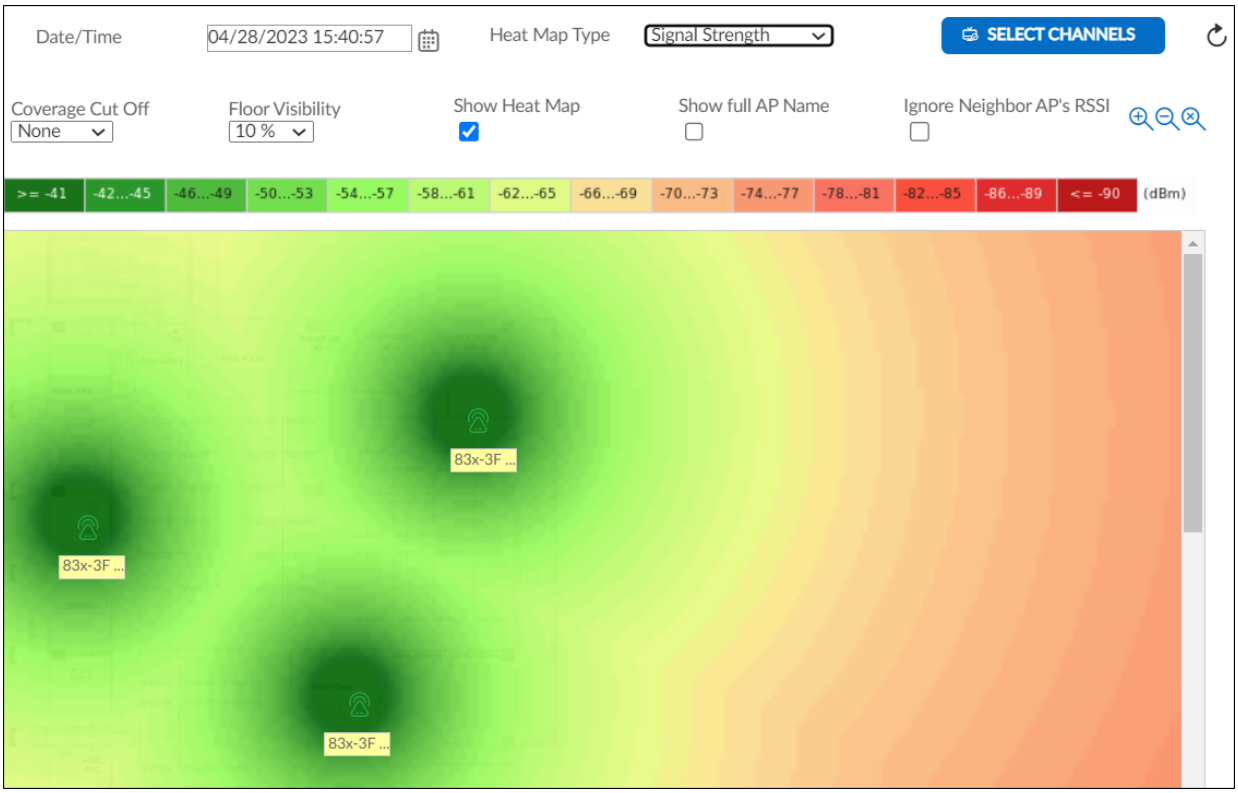
Hover over AP to view the AP information including name, AP model, MAC address, AP status, and number of stations.

Signal Strength Heat Map

Signal strength heat map provides a distribution of signal quality over the floor map. The signal strength is represented in dBm and is divided into color buckets. The Signal Strength maps display the availability of signal over the area represented by the map. Select different cut-off values to view the signal coverage.

Note: The signal strength heat map allows you to view the signals of all the APs on the floor. Due to this, the FortiAIOps displays heat map for all APs irrespective of whether the logged in user has scope for those APs or not. This enables you to capture accurate signal value for all APs located on the floor.

Hover over AP to view the AP information including name, AP model, MAC address, AP status, and signal strength.



With signal strength heat map having smooth transition in colors, the color at a given point may not exactly match with the bucket colors. For such cases, it should be interpreted as a value that is greater/lower than the nearest bucket color.

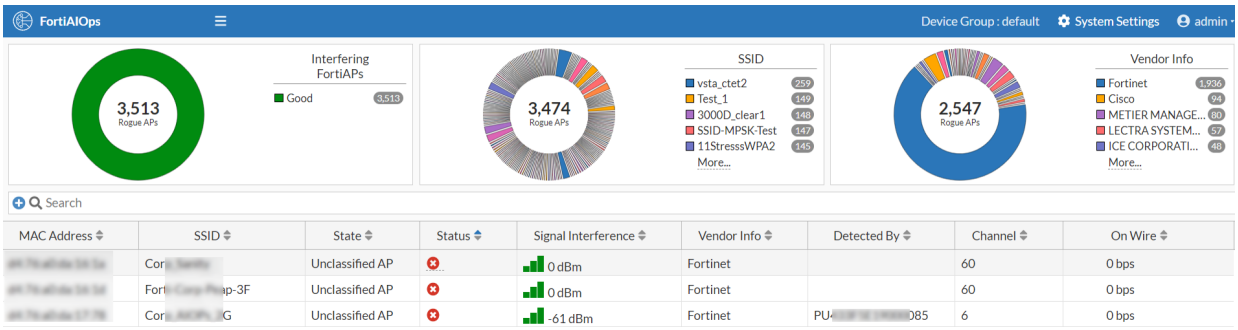
Coverage Cut Off: Coverage cutoff [default being none] can be used to see the signal coverage region within the cutoff value specified. The cutoff range is from -42dBM to -90dBM.

To view the signal strength heat map of a floor, follow these steps:

- Ensure that the APs are placed accurately through the map management feature.
- Click on **Heat maps** and select the desired floor.
- Select the RF band or relevant channel from the menu.
- Choose a cutoff of interest.
- Click on the **Refresh** icon.

Rogue APs

The Rogue APs page provides detailed information about rogue access points (APs) on the wireless network and consists of three widgets - Interfering APs, SSID, and Vendor Info.



Interfering APs

The Interfering APs widget displays the number of rogue APs detected by each managed FortiAP unit or FortiWiFi local radio.

SSID

The SSID widget displays the number of SSID names detected as rogue APs.

Vendor Info

The Vendor Info widget displays the vendor information for each rogue AP detected on the network.

The Rogue AP list provides detailed information about each rogue AP detected on the network, including the MAC address, SSID, state, signal interference, and vendor information.

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.

Map Management

Map management allows you to create visual representations of your access points (APs) to accurately represent the physical layout of a site. For best results, create separate maps for each floor in multi-level buildings, and use accurate architectural drawings as a basis for your images. Crop each floor map to remove extra space and save it as a PNG, JPEG, BMP, or GIF file no larger than 2MB before adding it to FortiAIOps.

Note: Provide a unique name to the site/building/floor plan. Do not use the same name across different device groups.

To set up a working map, you'll need to complete several tasks:

- Import a graphic map of the floor. See Importing a Map Image.
- Add a new site to FortiAIOps. See Add a Campus, Building, and Floor to the Map.
- Add a building.
- Add a floor.

- Place AP icons on the map to represent the WLAN network topology. See Add APs, Floor APs, and Landmarks to Maps.
- View the map. See Viewing Maps.

Importing a Map Image

Follow these steps to import a topology map:

1. Navigate to **Wireless > Map Management.**
2. Select a floor.
3. Click Change Image in the Floor Map section.
4. Select Image Type as Floor and Operation as Upload. Select the Image File by using the browse tab and click on Upload.

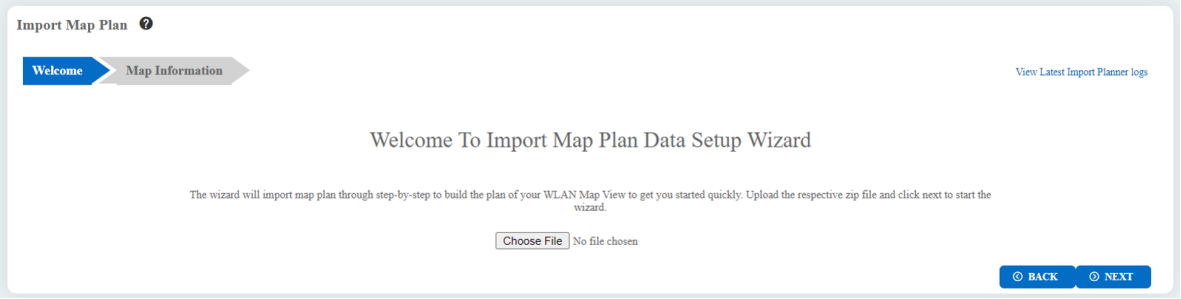
Next, add controllers and APs to the map.

Importing a Floor Map

FortiAIOps supports importing a floor map plan created on and exported from the FortiPlanner. Once the floor plan is created in the FortiPlanner, select Export in the project menu. The floor map to be imported is a .zip file.

Note: Only exported .zip files from the FortiPlanner can be imported. Contact the Customer Support to obtain the relevant version of the FortiPlanner. For more information on creating floor plans on the FortiPlanner, see the *FortiPlanner User Guide*.

1. Navigate to **Wireless>Map Management** page.
2. Click **Import**, the Import Map Plan screen is displayed.



3. Browse to the .zip file on your system and click **Next**. A summary of map information is displayed.
4. Map the unassigned APs and click **Finish.**
5. The planner for each site is displayed. On the **Map Management** screen, you can add and delete floors in the map and manage the APs on each floor of the site.

In case of errors importing the map, click View Latest Import Planner logs, to view the error logs.

You can perform the following operations on each floor:

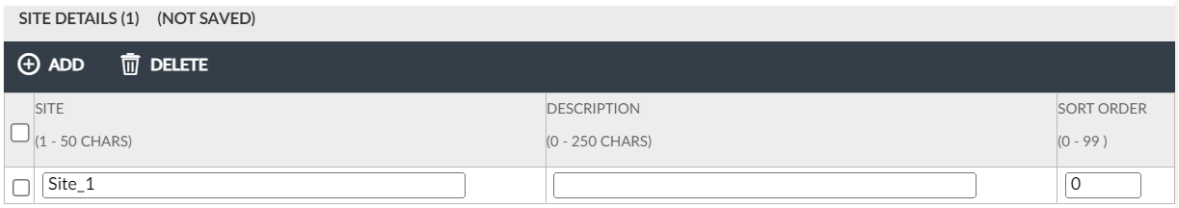
- **Add APs** - Select the APs to be added to the floor map.
- **Floor APs** - Select the APs to be deleted from the floor map.
- **Landmarks** - Add or delete landmarks on the floor map.
- **Change Image** - Upload a new image or delete an existing image from the floor map.

Click **Save** to save changes to the map

Adding a Site, Building, and Floor to the Map

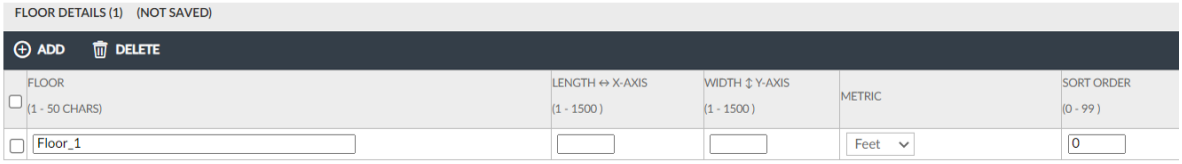
To create a new location (site, building, floor) in the enterprise, follow these steps:

1. Navigate to **Wireless > Map Management** page. All current maps are displayed on the Map Management page.
2. To add a new site, click on the **Site Details** section and then click on **Add**. A new site can only be added to the top level, Enterprise, which is the default.



3. Provide a name, description, and sort order for the site.
4. Click **Save Changes**.
5. In the left pane, double-click on the name of the new site you just created.
6. Click on the Buildings icon. In the Building Details pop-up, click **Add**.

7. Provide a name, description, and sort order for the building.
8. Click **Save Changes**.
9. In the left pane, double-click on the name of the new building you just created.
10. In the Floor Details section, click **Add**.



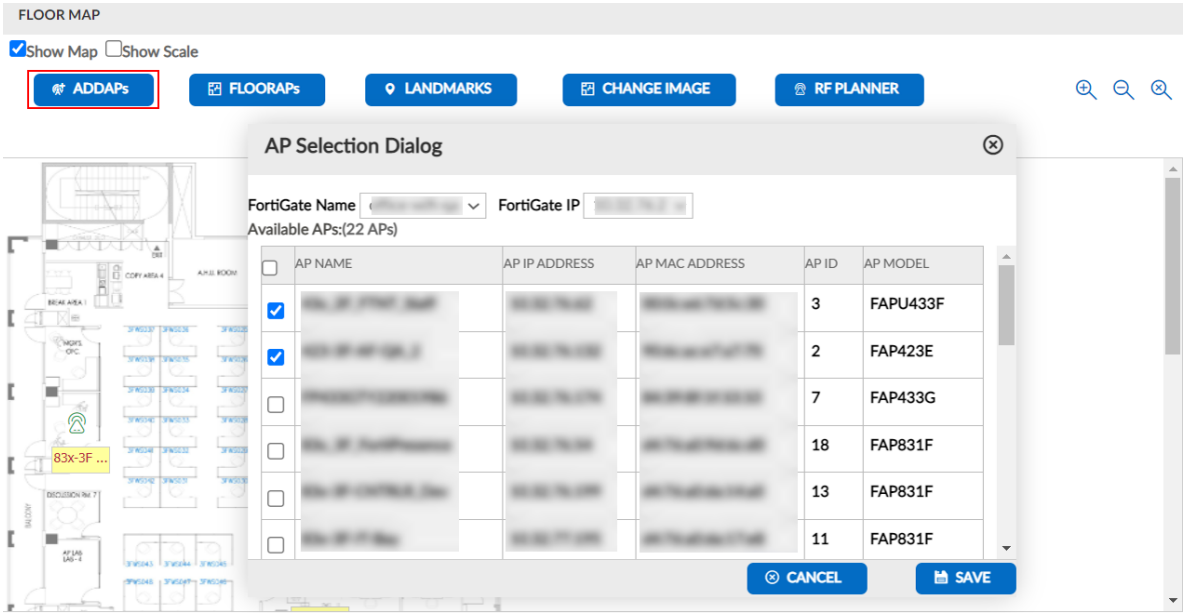
11. Provide a floor name, length, width, metric, and sort order for the floor.
12. Click **Save Changes**.

Adding APs, Floor APs, and Landmarks to Maps

To create the network map of your site, follow these steps:

1. Once a map image has been imported, add the APs to the map as close as possible to their actual physical location.
2. Select a floor by its heading in the left column to see a map of the floor. If the floor does not have a corresponding map, complete the steps to Import a Map Image.
3. Optionally, alter the map using the options Show Map and Show Scale in the Image Map section.

4. Click **Add APs** and select the APs to add from the drop-down list on the AP selection pop-up, then click **Save**. Drag the selected APs into position on the map.



5. To add landmarks to the map, click Landmarks > Add.
6. Once you have finished making changes, click **Save Changes**.

Editing AP Details

To edit the details of an access point (AP), follow these steps:

1. In the Map Management screen, click **APs** to display the AP list.
2. Select the AP you want to edit by clicking on its icon on the map or by selecting it from the AP list.
3. Click **Edit** to open the AP details window.
4. Edit the required fields, such as the AP name or its location coordinates.
5. Click **Save** to save the changes made to the AP details.
6. Click **Cancel** to discard any changes and close the AP details window.

Viewing Maps

You can view the placement of APs on a map or view Heat Maps that show the following five attributes of those APs:

- Throughput
- Loss
- Channel Utilization
- Number of Stations
- Signal Strength

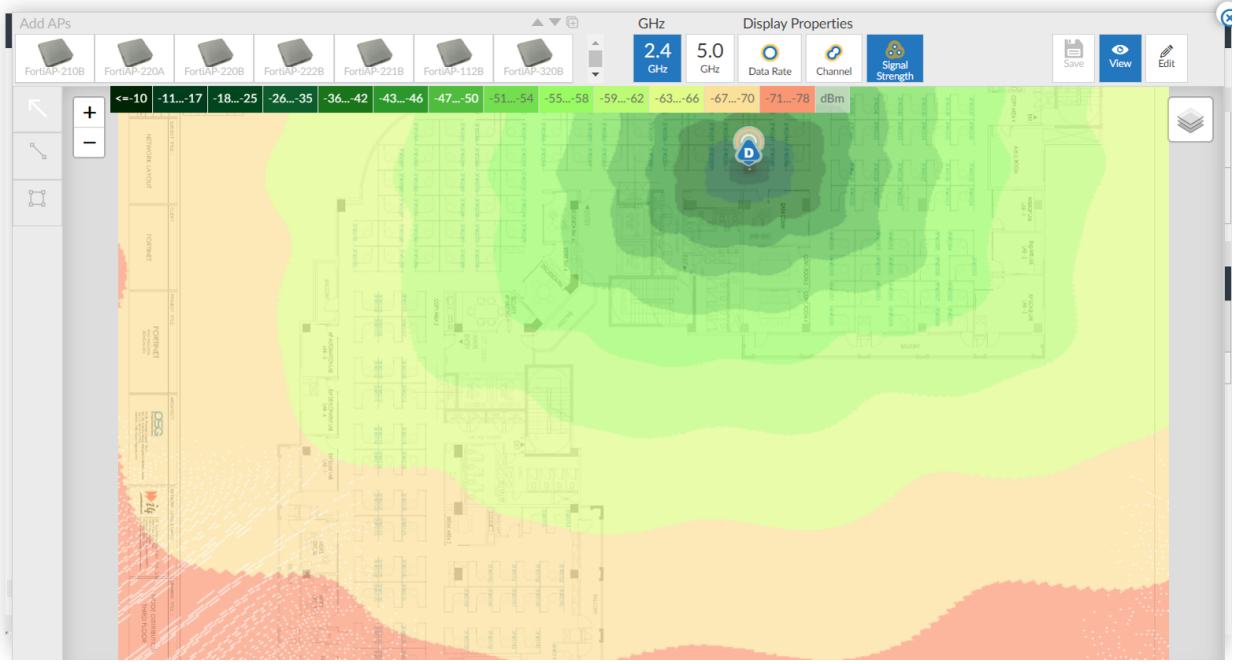
Heat map coloring depends on the distance between APs and selected attribute (throughput, loss, channel utilization, or stations) for all the APs on the floor. If there is only one AP on the floor, the entire floor will show the same coverage. See Heat Maps.

To view maps and heat maps, follow these steps:

1. Click on **Wireless > Heat Maps.**
2. Select a floor to display the map.
3. Optionally, alter the map using the options Floor Visibility or Show Heat Map.
4. To limit the map, click Select Channels, select channels, and then click **Save Changes.**
5. After any changes, click on the Refresh icon.

RF Planner

The RF planner is a tool that enables you to plan for new access points, areas, and obstacles (walls, shafts, etc.). It allows you to place APs and draw walls or columns in both View and Edit modes.



To use the RF planner, follow these steps:

1. Navigate to Map Management > RF Planner.
2. Add the required access points to the floor map and generate a heat map to predict the expected signal strength throughout the coverage area.
3. Adjust the placement of your APs based on the predicted signal strength and try out different placements for the APs before installing them.
4. Draw a floor plan of the coverage area and place the APs on your floor plan.
5. Run heat maps to predict the signal strength.

View Mode: In View mode, the floor map displays the coverage pattern, data rate, channel, and signal strength of the access points. You can select the 2.4GHz, 5GHz, or 6GHz frequency to view the access point details.

Edit Mode: In Edit mode, you can add or edit new access points. To do this, drag the required access point from the "Add APs" panel and place it on the floor map. Right-click on an access point and edit its configuration, such as the access point transmission power in dBm, channel, orientation, placement direction (in angles), ceiling, wall, and desk.

To draw walls and columns on the floor map, use the provided widgets. Select the required widget and draw the wall or column on the map. A column is a closed drawing with four walls, while a wall is demarcated as lines.

Right-click on the created walls and columns to specify the composition or material used to construct them. Each material has a different attenuation value.

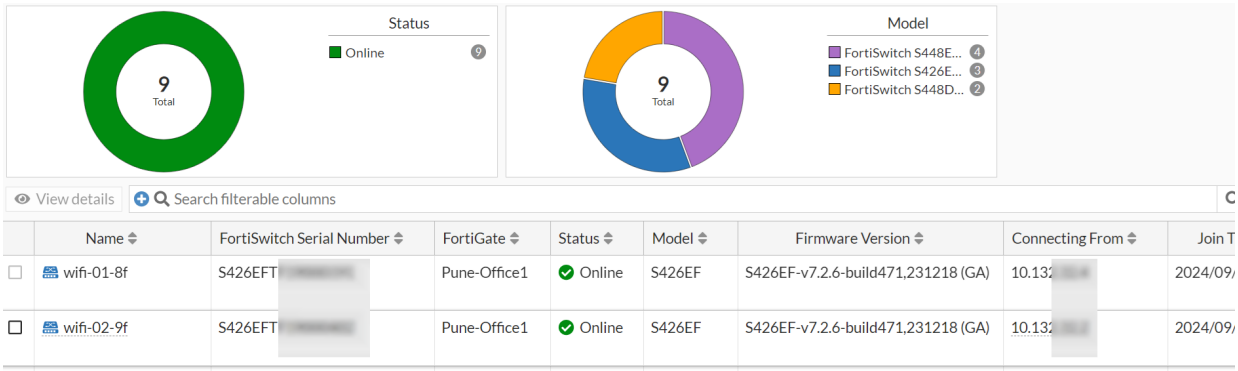
Switch

This section describes the FortiSwitch statistics and the FortiSwitch client details.

- FortiSwitch
- Wired Clients

FortiSwitch

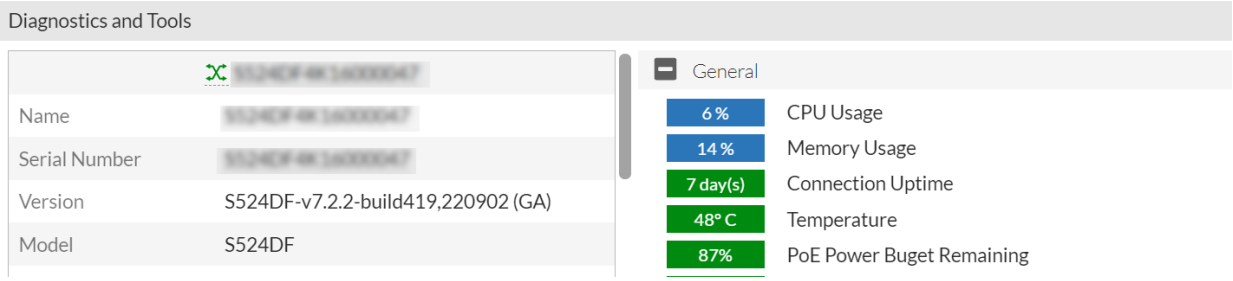
You can monitor the FortiSwitches in your network that are in the purview of FortiAIOps. This page displays a graphical snapshot of the FortiSwitch activity such as, the total number of FortiSwitches, their status (online/offline/unauthorized), and the deployed model details.



Click **Export As** to export a 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.

Diagnostics and Tools

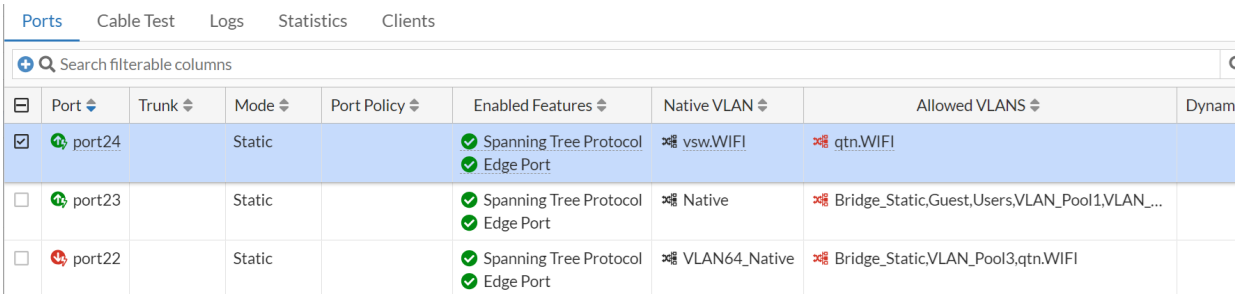
To view the FortiSwitch statistics and diagnostics in detail, select a row and click **View Details**. The **Status** including the FortiSwitch face plate, hardware summary, general status and statistics, and configuration details is displayed.



- Ports
- Cable Test
- Logs
- Statistics
- Clients

Ports

This tab displays each port details of the specific FortiSwitch unit.



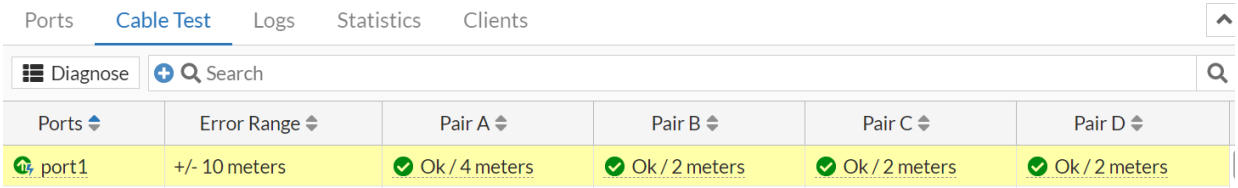
Each entry in the port list displays the following information.

Parameter	Description
Port	The name of the port (red for port down, green for port up)
Trunk	The associated trunk that the port is a member of.
Mode	The configured access mode of the port.
Port Policy	The configured port policy.
Enabled Features	The features enabled on the port.
Native VLAN	The native VLAN assigned to the port.
Allowed VLANs	The allowed VLANs set for the port.
Dynamic VLAN	The dynamic VLAN assigned to the port.
DHCP Snooping	The status of DHCP snooping status
Transceiver	The transceiver information.
Description	The port description
LLDP Profile	The associated LLDP profile.
Loop Guard	The status of the Loop Guard (enabled/disabled)
QoS Policy	The assigned QoS policy.
Security Policy	The assigned security policy.
STP	The status of STP (enabled/disabled).
STP BPDU	The status of STP BPDU Guard (enabled/disabled).
STP Root Guard	The status of STP Root Guard (enabled/disabled).

Cable Test

This is a diagnostic and troubleshooting tool to check the state of cables between the FortiSwitch and the devices connected to its physical ports. This tool does not work on fiber ports and on very short or very long cables (more than 100 meters).

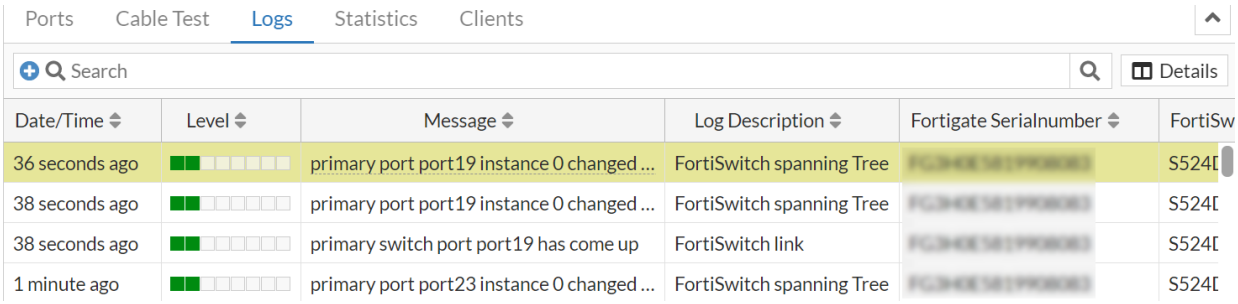
All available external physical ports of the FortiSwitch are displayed. Select one or more ports and click **Diagnose**.



Note: Running the cable diagnostic test on a port disables it briefly. The network traffic is affected for a few seconds.

Logs

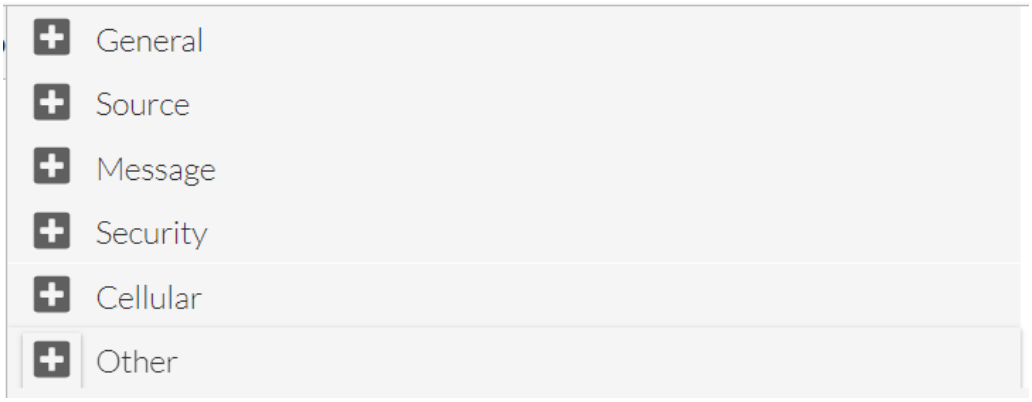
This tab displays the FortiSwitch log messages and the associated details.



Each log entry displays the following information.

Parameter	Description
Date/Time	The Date/time of log event generation.
Level	The log severity level. • Emergency, Critical (red) • Alert (orange) • Error, Warning (blue) • Notice, Information, Debug (green)
Message	The event log message that is generated.
Log Description	The description of the event log.
FortiGate Serial Number	The serial number of the associated FortiGate controller.
FortiSwitch Serial Number	The serial number of the associated FortiSwitch.
Relative Date/Time	The time lapsed since the event log was generated.
Source	The event source IP/MAC address.

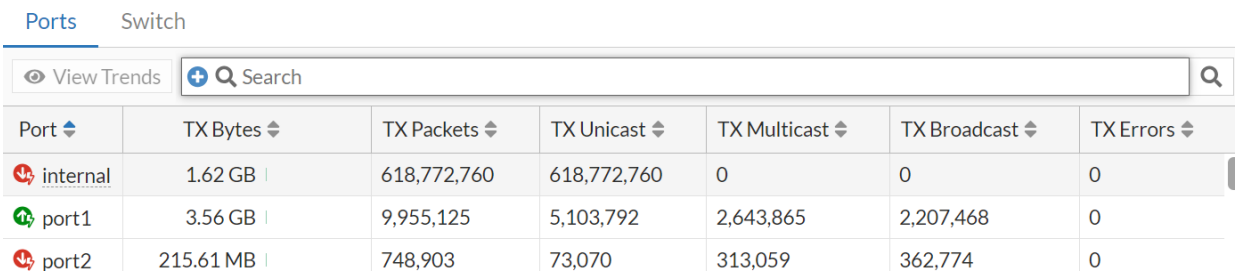
Select a log message and click **Details** to view specific related information. This view provides the following information.



- **General** - Generic information about the log event such as, the date and time of event logging, the associated virtual domain, and the log description.
- **Source** - The details of the user.
- **Message** - The generated log message.
- **Security** - The severity level of the log event.
- **Cellular** - The serial number of the FortiSwitch.
- **Other** - Generic information such as the log event time stamp, the timezone, log type, and so on.

Statistics

This tab displays the FortiSwitch and the associated port statistics.



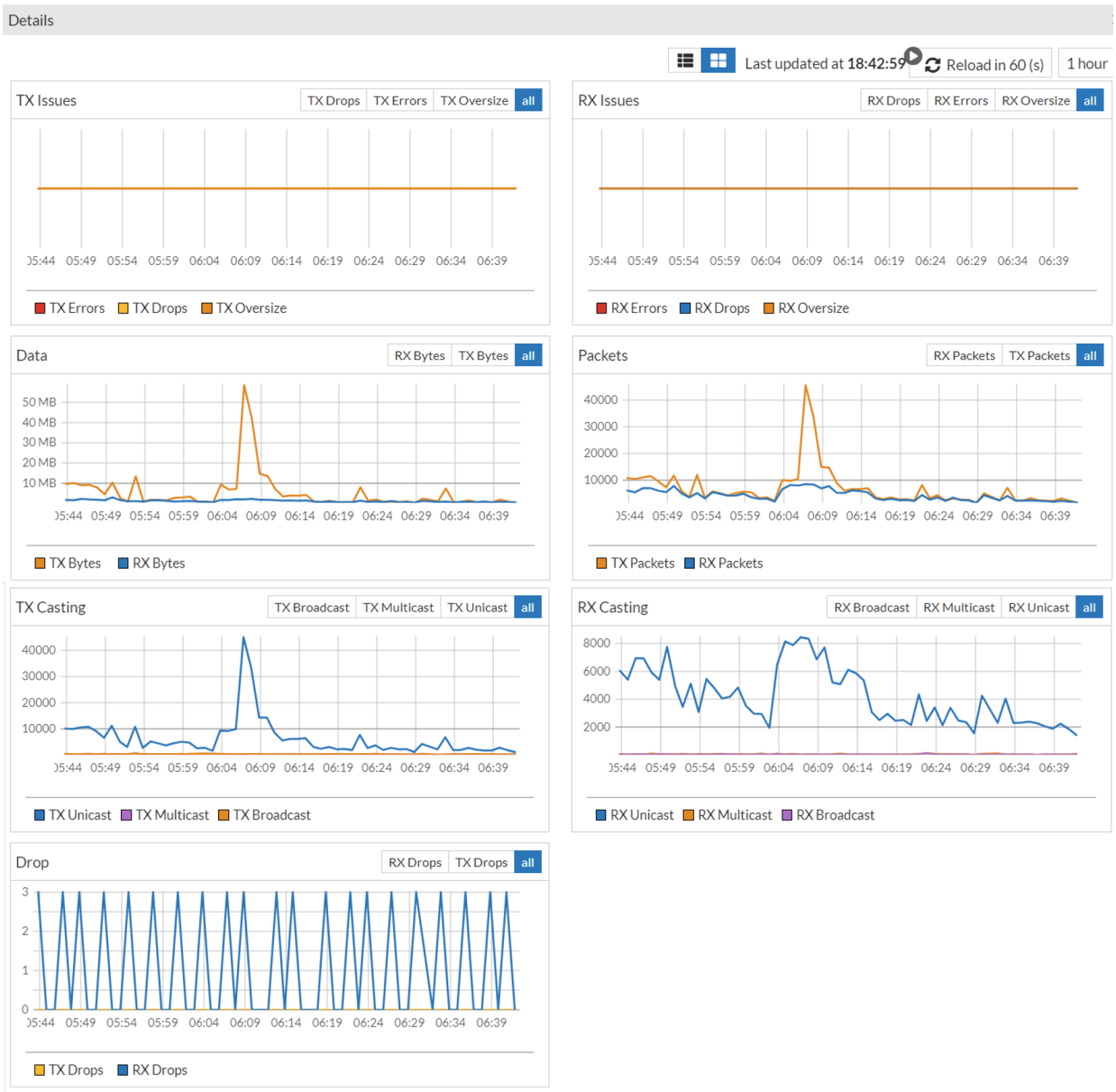
Port	TX Bytes	TX Packets	TX Unicast	TX Multicast	TX Broadcast	TX Errors
internal	1.62 GB	618,772,760	618,772,760	0	0	0
port1	3.56 GB	9,955,125	5,103,792	2,643,865	2,207,468	0
port2	215.61 MB	748,903	73,070	313,059	362,774	0

The **Ports** view provides the following information.

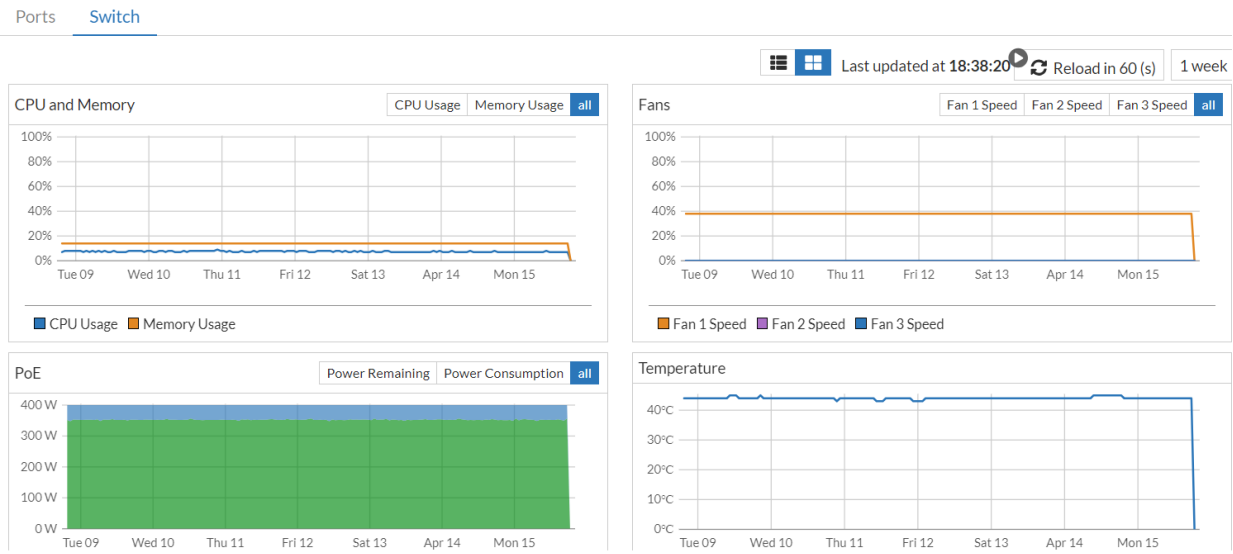
Parameter	Description
TX Bytes	The transmitted bytes.
TX Packets	The transmitted packets.
TX Unicast	The transmitted unicast packets.
TX Multicast	The transmitted multicast packets.
TX Broadcast	The transmitted broadcast packets.
TX Errors	The errors in transmitted packets.

Parameter	Description
TX Drops	The dropped packets in transmitted packets.
TX Oversize	The oversized packets in transmitted packets.
RX Bytes	The received bytes.
RX Packets	The received packets.
RX Unicast	The received unicast packets.
RX Broadcast	The received broadcast packets.
RX Errors	The errors in received packets.
RX Drops	The dropped packets in received packets.
RX Oversize	The oversized packets in received packets.
Undersize	The number of undersized packets.
Fragments	The number of fragments.
Jabbers	The number of jabbers.
Collisions	The number of packet collisions.
CRC Alignments	The number of CRC/alignment errors.
L3 Packets	The number of layer-3 packets.

Select a particular port and click **View Trends** to view a graphical representation of the trends in FortiSwitch statistics over a period of time. You can filter the trends based on the selected duration or customized time slot; select a time window or define a **Custom range** not exceeding 6 months. The minimum, maximum, and average values are displayed when a time interval of more than 6 hours is selected.



The **Switch** view provides a graphical representation of the trends in FortiSwitch statistics over a period of time. You can filter the trends based on the selected duration or customized time slot; select a time window or define a **Custom range** not exceeding 6 months. The minimum, maximum, and average values are displayed when a time interval of more than 6 hours is selected.



Clients

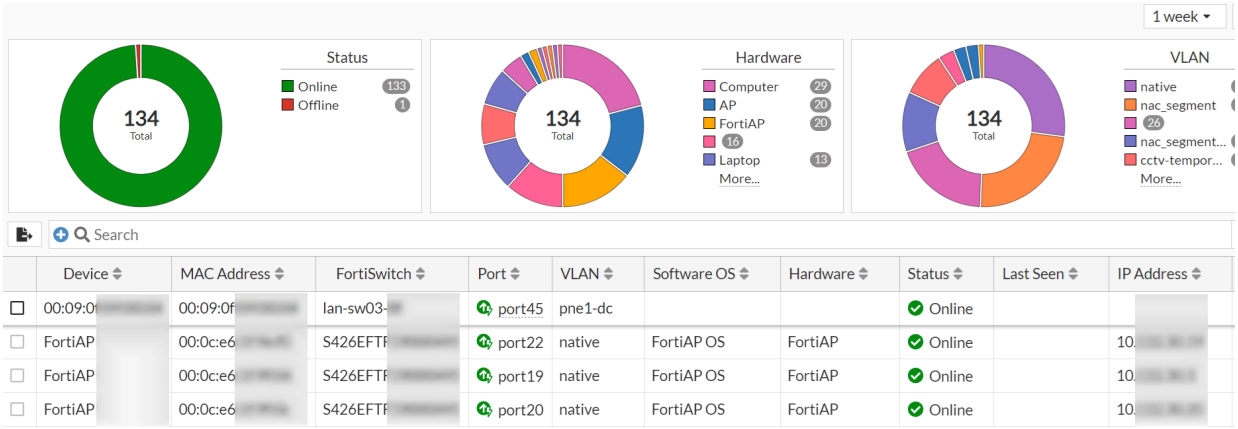
This tab displays the details of the FortiSwitch clients. The following information is displayed.

Parameter	Description
Device	The client device name.
Port	The associated port details.
VLAN	The associated VLAN details.
Software OS	The client device software OS.
Hardware	The client device hardware details.

Wired Clients

You can monitor the FortiSwitch clients associated with the FortiSwitches deployed in your network. This page displays a graphical snapshot of client activity such as, the total number of FortiSwitch clients, their status (online/offline), the client device details, and the associated VLANs. Hovering over the charts provides specific statistics and clicking on a specific area on the chart filters the data displayed on this page.

- You can filter the switching client data for a selected duration or a customized time slot. The **Custom range** allows the selection of a minimum of 1 hour and maximum of 1 week, the option of **Now** displays data for the last 1 minute.
- Click **Export As** to export a 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.



The table beneath the chart displays the client details.

Parameter	Description
Device	The name of the client device.
FortiSwitch	The host name or serial number of the FortiSwitch that the client is associated with.
Port	The associated port details of the FortiSwitch unit.
VLAN	The type of the VLAN.
Software OS	The software OS used by the client device.
Hardware	The hardware used by the client device.
Status	The status of the client (online/offline).
Last Seen	The time that the client was last seen online.
IP Address	The IP address of the client.
EMS Serial Number	The FortiClient EMS serial number.
EMS Tenant ID	The FortiClient EMS tenant ID.
Endpoint Tags	The endpoint (client) tags monitored by FortiGate.

SD-WAN

SD-WAN section enables interface monitoring for SD-WAN devices.

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.

- Prerequisites
- Recommendations

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.

The SD-WAN section enables you to configure baselines to monitor SD-WAN metrics and provides valuable insights about the network health:

- Insights
- Forecast

Insights

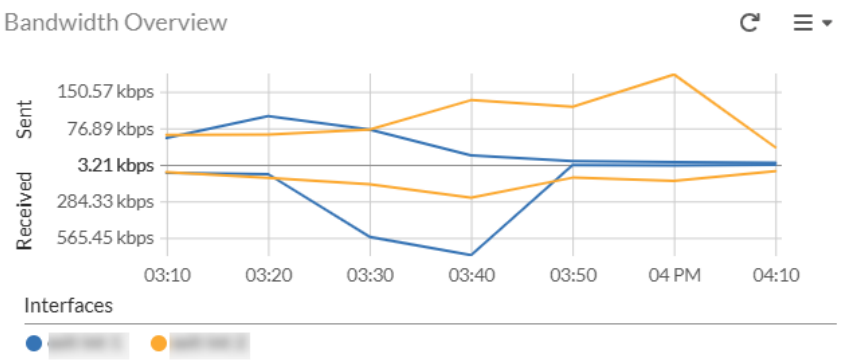
The Insights page provides valuable insights into your network's health and performance with the charts:

- 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.

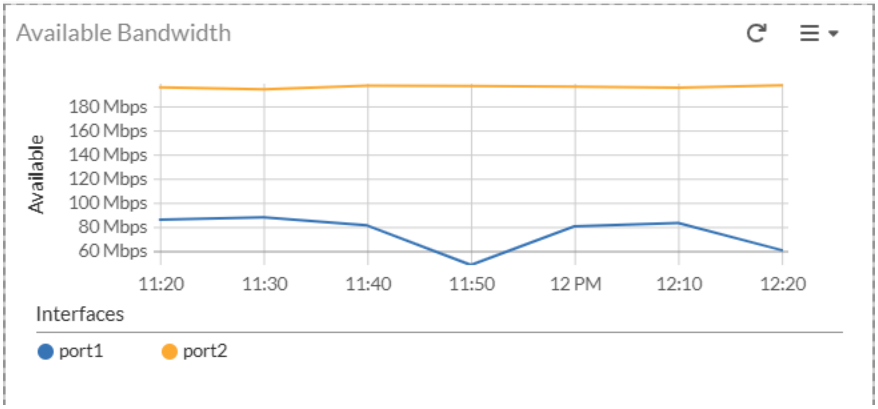
Hover over the points on graph to view sent/receive data.



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.

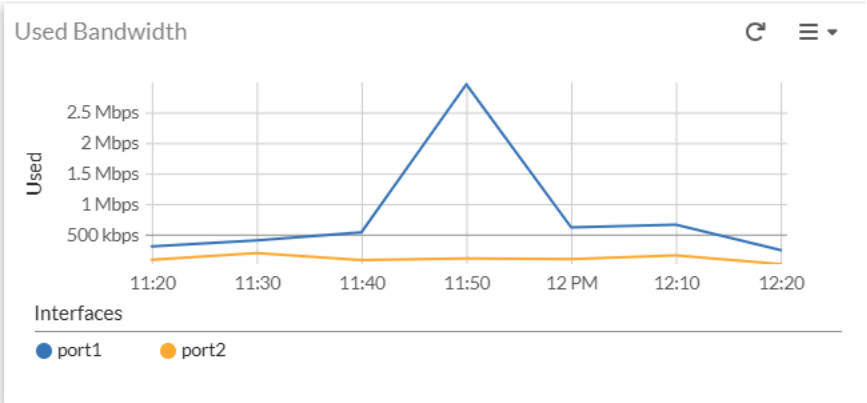


Note: Configure **Estimated Bandwidth** to estimate accurate WAN utilization. If not configured, the maximum capacity of the link is inserted as **Available Bandwidth**. For more information, see FortiGate Administration Guide.

Used Bandwidth

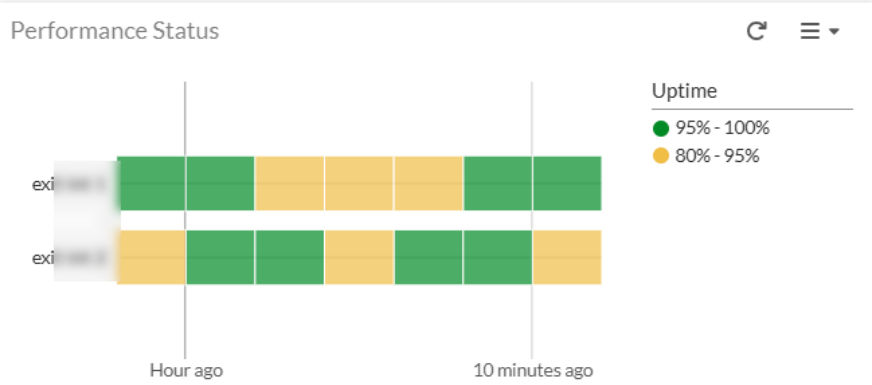
This chart displays the amount of bandwidth consumed by the SD-WAN interfaces over a period of time.

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.



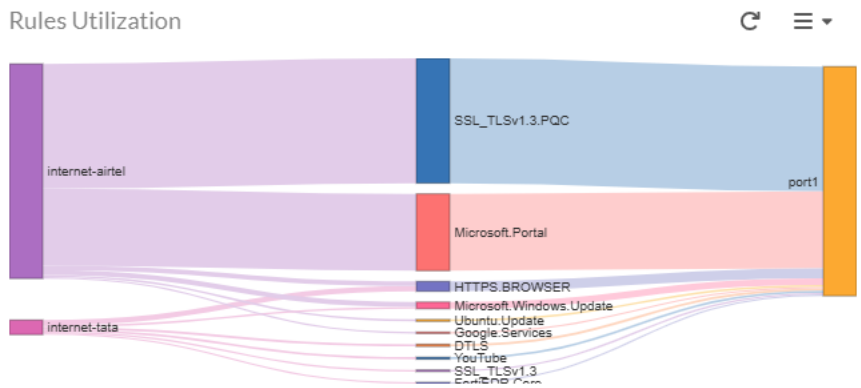
Color-coded indicators represent uptime percentages:

- 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.

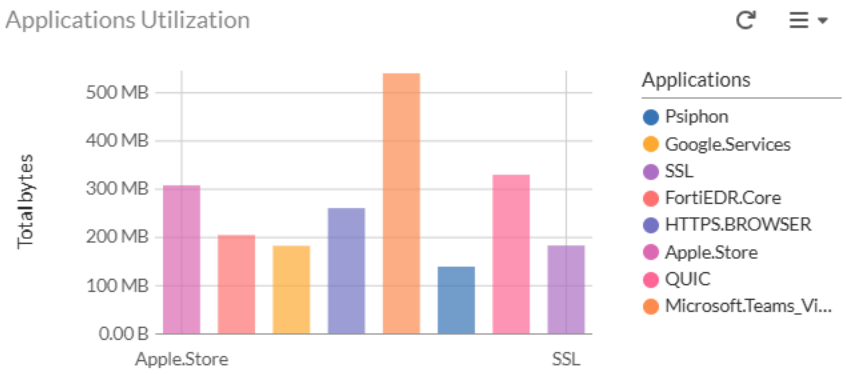
Rules Utilization

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.



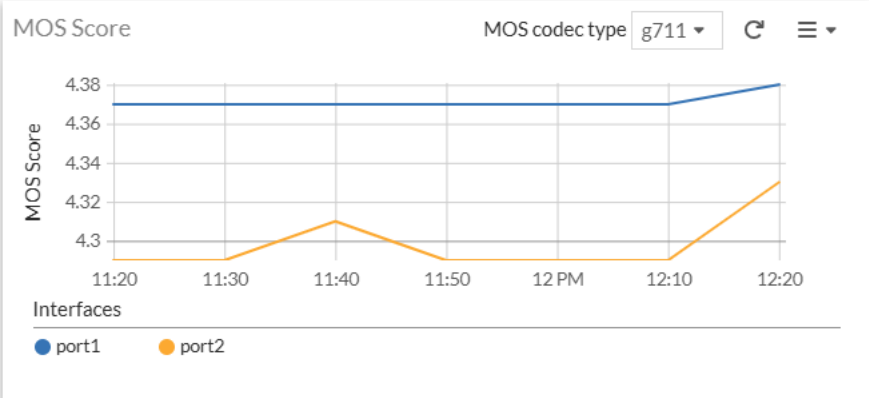
Applications Utilization

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:

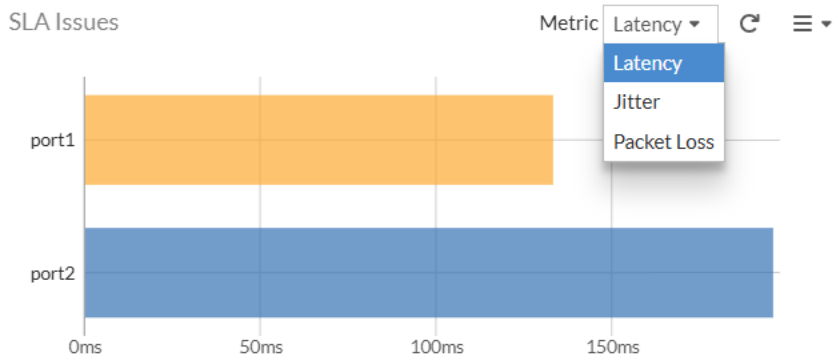
- MOS 4.3-5.0: Excellent
- MOS 4.0-4.3: Good
- MOS 3.6-4.0: Fair
- MOS 3.1-3.6: Poor
- MOS 2.6-1.0: Bad

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.

Forecast

The **Forecast** page helps to monitor and measure the health of links connected to your SD-WAN member interfaces by tracking latency, jitter, and packet loss. It provides a comprehensive summary of network health and performance in the form of statistics and trends for latency, jitter, and packet loss. The page offers detailed link quality measurements with insights to predict potential issues in your SD-WAN links. This crucial insight enables the selection of optimal links for traffic routing thus preventing data from being sent to broken connections and improving overall network performance and reliability.

FortiAIOps establishes a baseline for acceptable link performance based on historical data, detecting and reporting anomalies when SLA breaches occur. This forecasting capability enables you to proactively address performance issues that could impact network health.

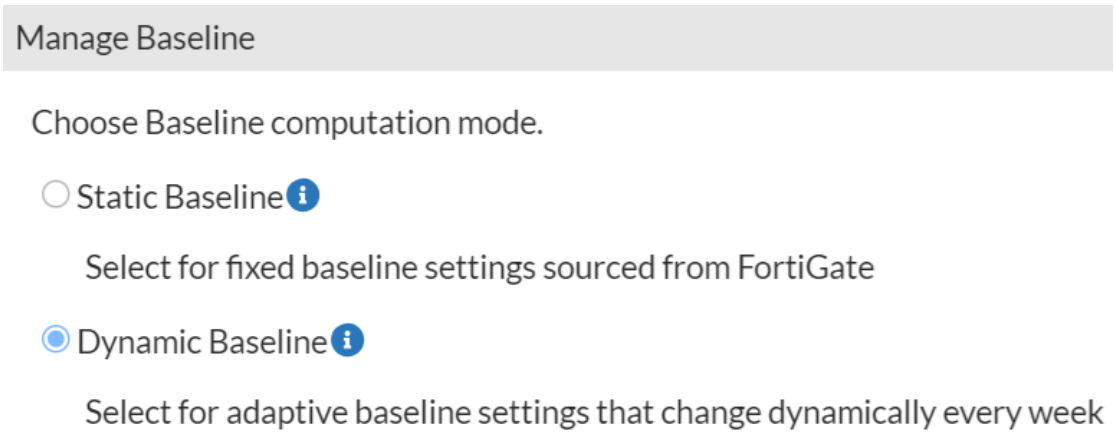
FortiAIOps monitors and forecasts latency, jitter, and packet loss for the upcoming week based on available SLAs, tracking real-time network performance to report any changes in SD-WAN link performance.

Navigate to **SD-WAN > Forecast** 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**.



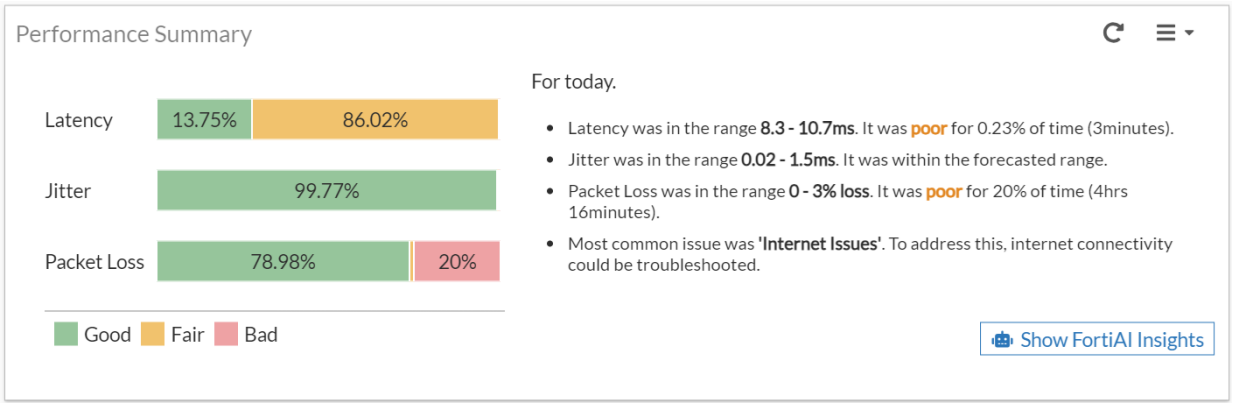
- **Static Baseline** - These baselines are SLA targets configured in FortiGate or FortiAIOps default thresholds, for jitter, packet loss, and latency. If the SLA targets are not specified in FortiGate, then the following default baselines are used for all the 3 metrics.
  - Latency - 100 ms
  - Jitter - 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.

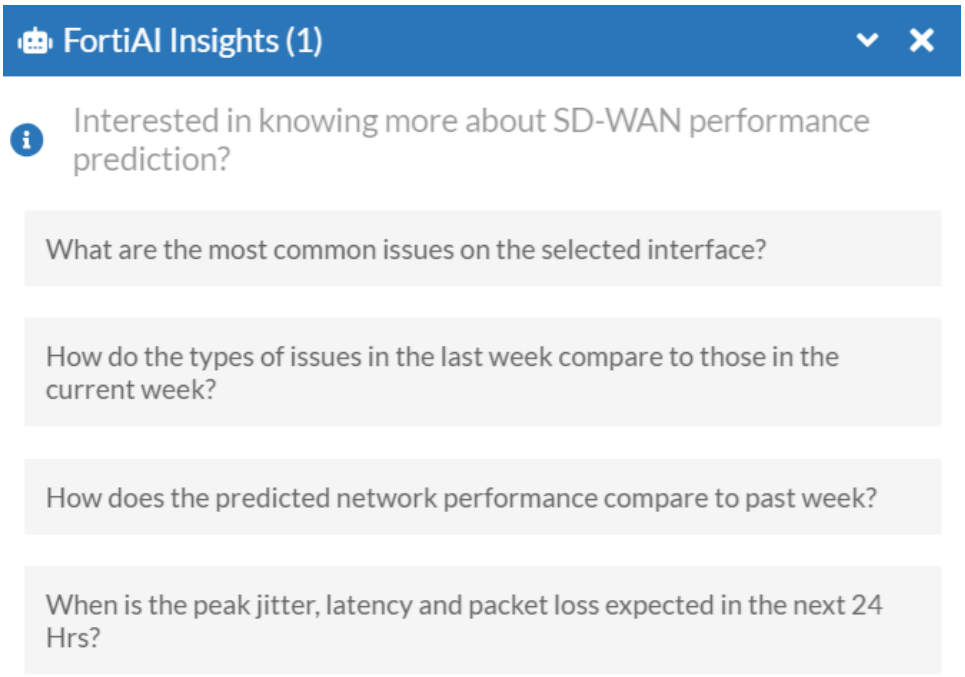
Note: Fortinet recommends to use SLA targets for the Performance SLA, when static mode is used. The SLA targets are a set of constraints that are used in SD-WAN rules to control the paths that traffic takes. The constraints are configured using the FortiGate GUI and CLI. For more information, see Link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



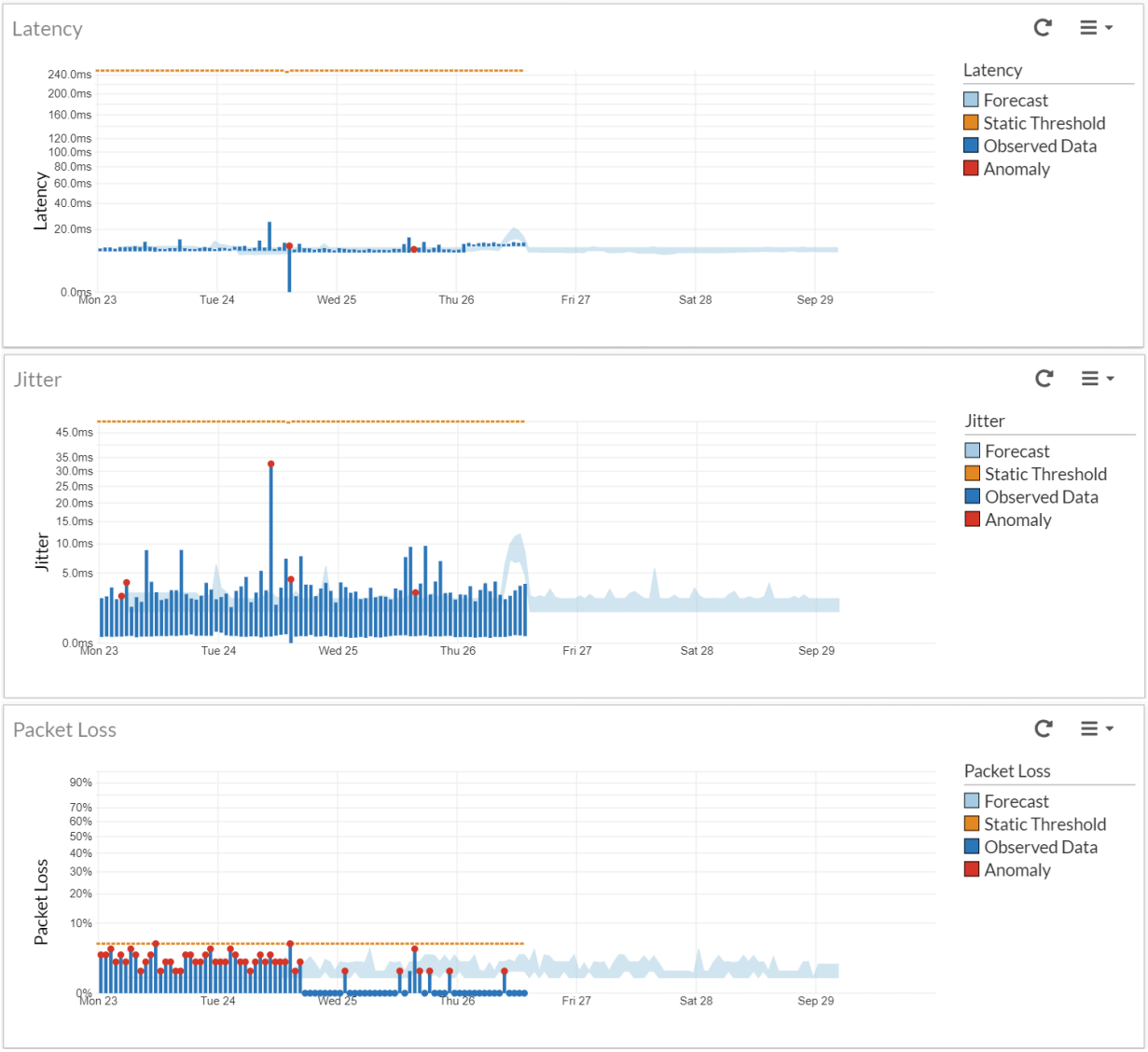
To learn more about the SD-WAN interface performance prediction based on the FortiAI insights, click **Show FortiAI Insights**.


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.

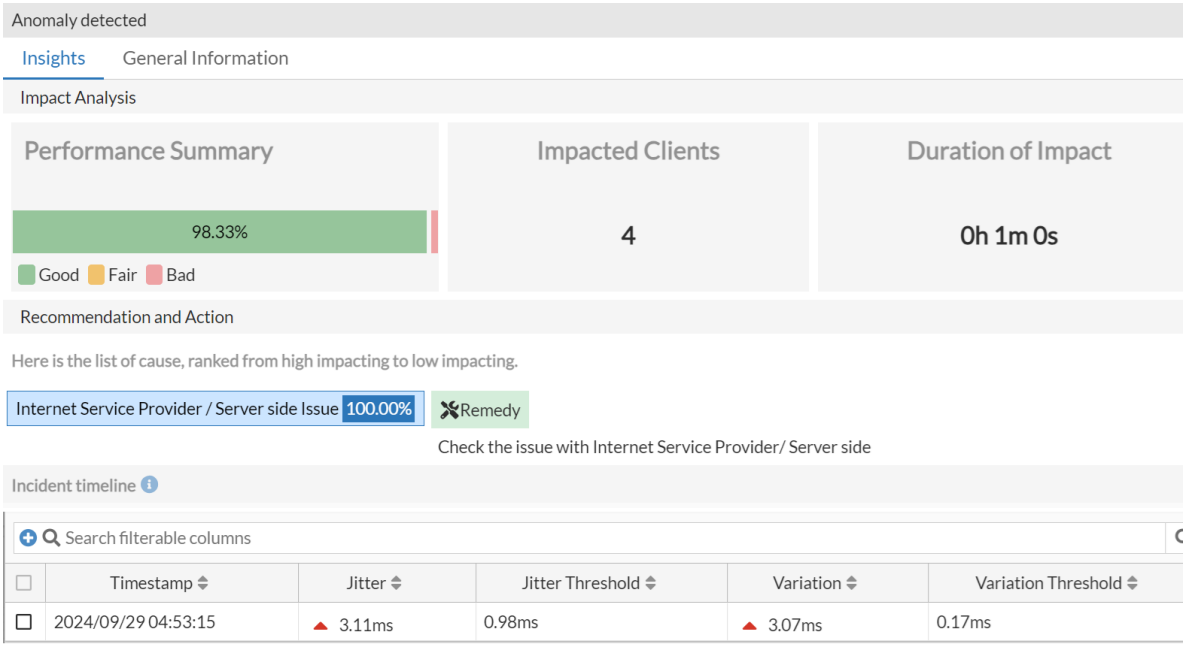
Note: The trends displayed are on an hourly basis.



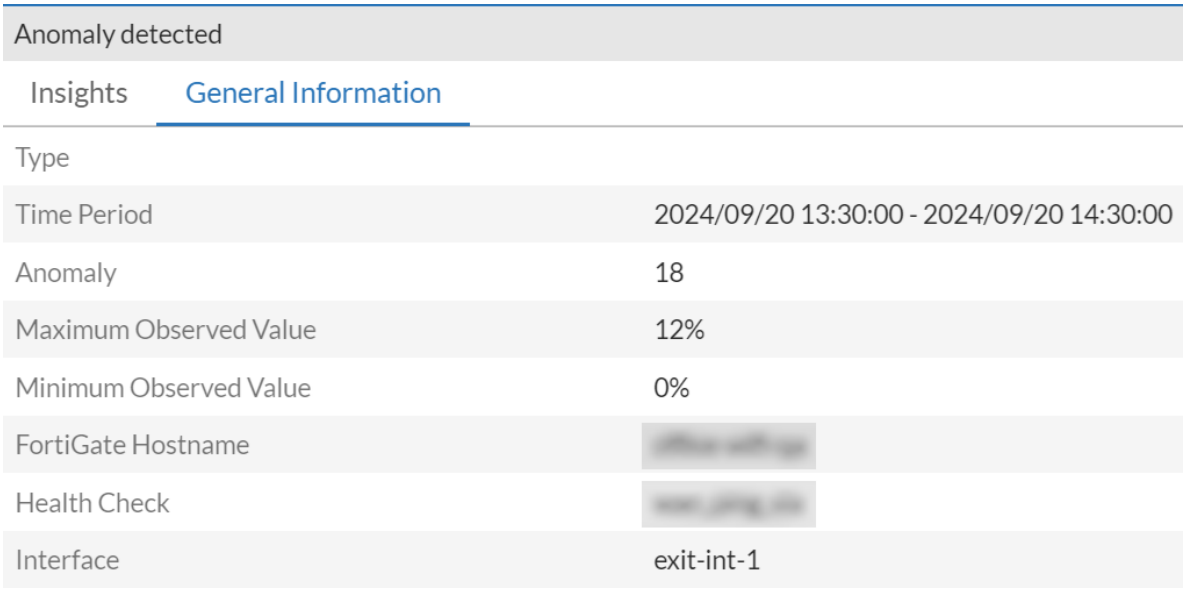
- **Forecast** - This is indicative of the range predicted by FortiAIOps based on historical statistics.
- **Observed Data** - This is the range of real time statistics observed in a given hour.
- **Anomaly** - Anomalies are reported when FortiAIOps observes a deviation in the data exceeding the usual 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.

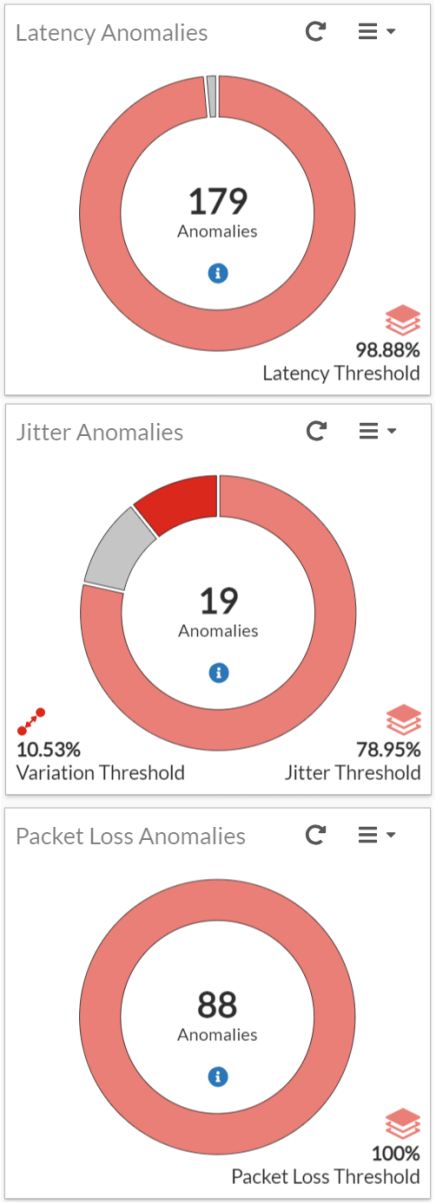


- **General Information** - This provides general information about the detected anomaly such as, the duration, the FortiGate host name, interface, configured health check, and so on.



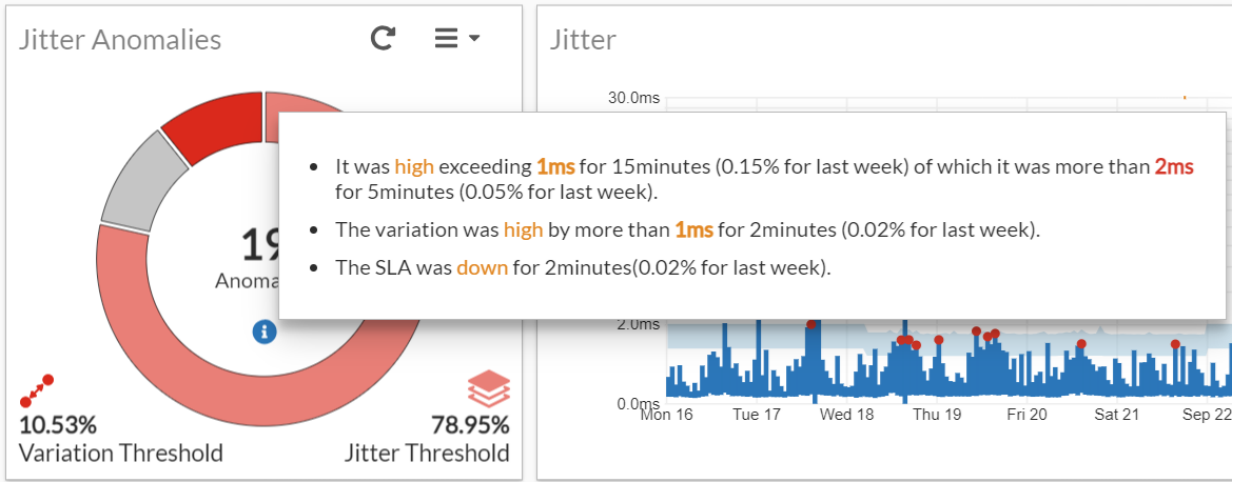
Anomalies

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.


Jitter Anomalies
19
Anoma
10.53%
Variation Threshold
78.95%
Jitter Threshold
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).
Jitter
30.0ms
2.0ms
0.0ms
Mon 16
Tue 17
Wed 18
Thu 19
Fri 20
Sat 21
Sep 22

Security Fabric

The Security Fabric page represents the topology, that illustrates the logical placement of the wireless service and the physical placement of hardware devices. The hardware devices include FortiGates, APs, and wireless clients in your network.

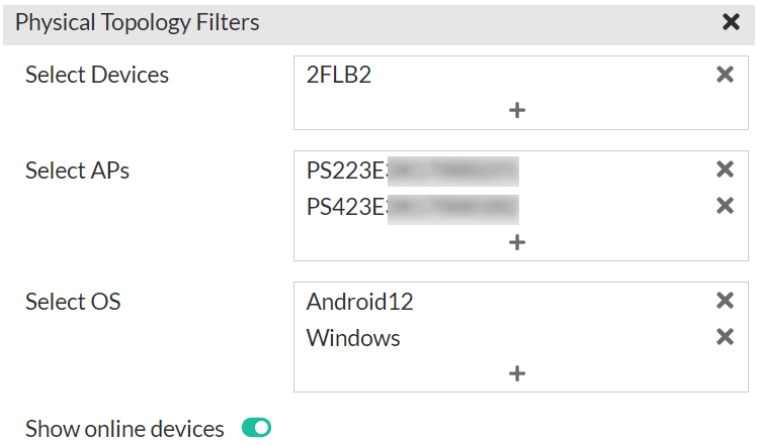
Note: The physical and logical topologies provide wireless client information.

- Physical Topology
- Logical Topology

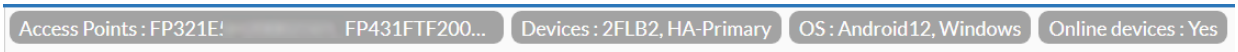
Physical Topology

The physical topology provides a visualization/illustration of the physical placement of devices, such as, FortiGate controllers, APs, and clients connected to each radio in your network, in an hierarchical pattern. The physical topology is representational; you cannot modify the placement of devices on this page.

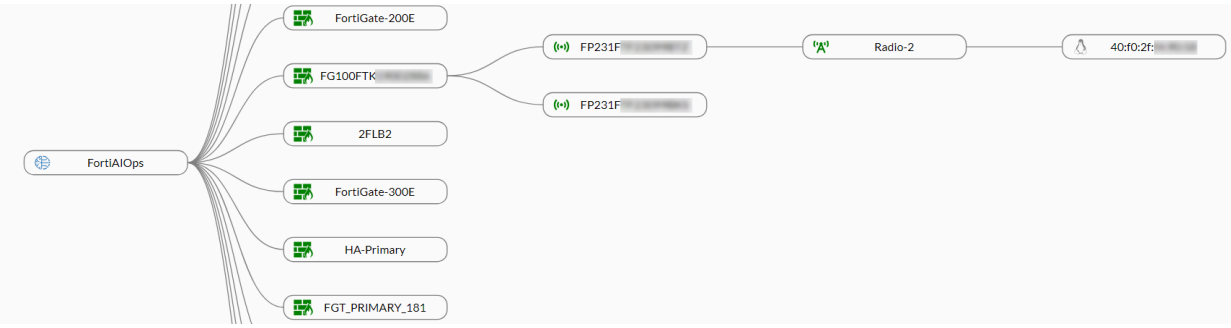
You can filter and view selective devices in the topology chart, the filter options available are FortiGate controllers (**Devices**), FortiAPs (**APs**), and device OS. You can also enable viewing of online devices only, in the topology (**Show online devices**). To apply the filter settings, click **Apply Filter**.



The devices/OS set in the applied filters are also displayed at the top of the topology page, hover over each of these to view the complete list.



The collapsible/expandable hierarchy of devices in the physical topology is ***FortiGate~ FortiAP ~ radio ~ client***; each of the devices displayed is click-able to display the next level of hierarchy.



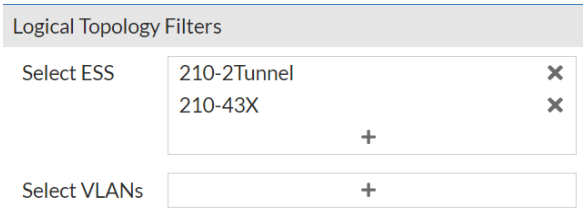
Hover over the device name to obtain additional information. The status of the FortiGate controllers and APs is marked using a color legend.

- *Green*: Online and active
- *Red*: Offline

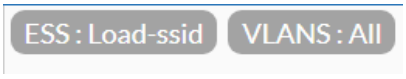
Logical Topology

The logical topology provides a visualization/illustration of the logical placement of the configured wireless service, the associated ESS pushed through the wireless service, VLAN (if applicable), and the stations connected to each ESS in a hierarchical pattern. The logical topology is representational; you cannot perform any operations on this page.

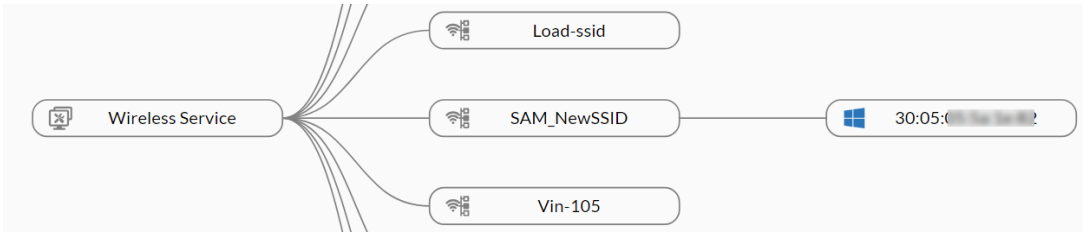
You can filter and view selective entities, the filter options available are ESS and VLANs. To apply the filter setttings, click **Apply Filter**.



The ESS and VLANs set in the applied filters are also displayed at the top of the topology page, hover over each of these to view the complete list.



The collapsible/expandable hierarchy of entities in the logical topology is wireless service ***~ ESS ~ VLAN ~ client***; each of the entities displayed is click-able to display the next level of hierarchy.



Note: The physical and logical network topology views differ based on the browser.

Logs and Reports

This section describes the WiFi and FortiSwitch event logs and the generation of the FortiAIOps reports.

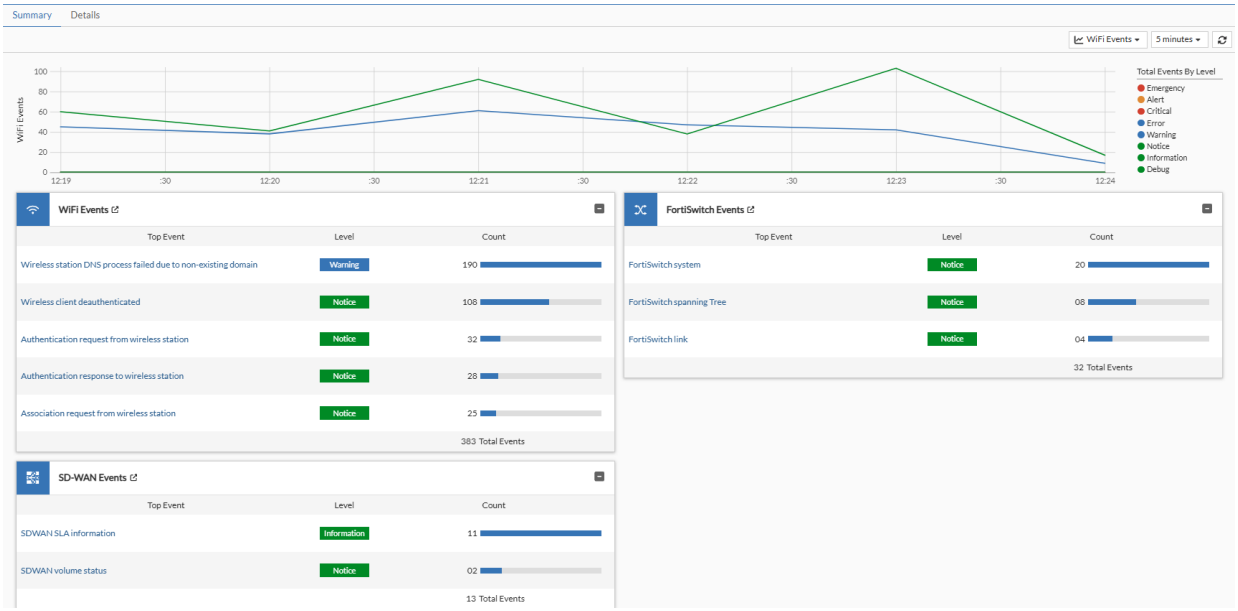
- Event Logs
- Local Logs
- Reports

Event Logs

The FortiAIOps provides a robust logging environment that enables you to monitor, store, and report WiFi events, FortiSwitch events, and SD-WAN events. 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 following event logs are available:

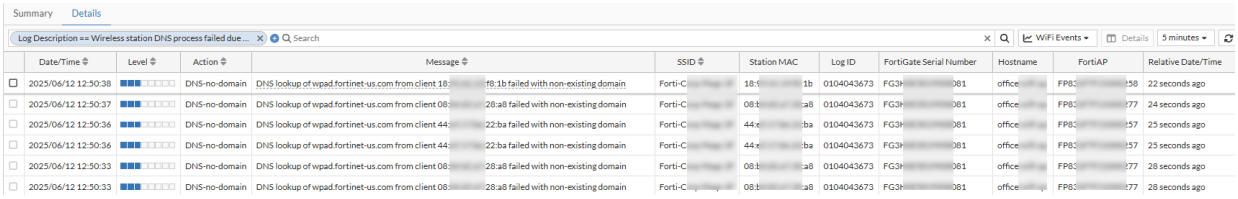
- WiFi Events
- FortiSwitch Events
- SD-WAN Events



Clicking on any event type title opens 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.

The **Details** tab displays individual, detailed log views for event type. By default, all event details are displayed on this page, you can filter the **WiFi Events** or **FortiSwitch Events** or **SD-WAN Events** data on this page.

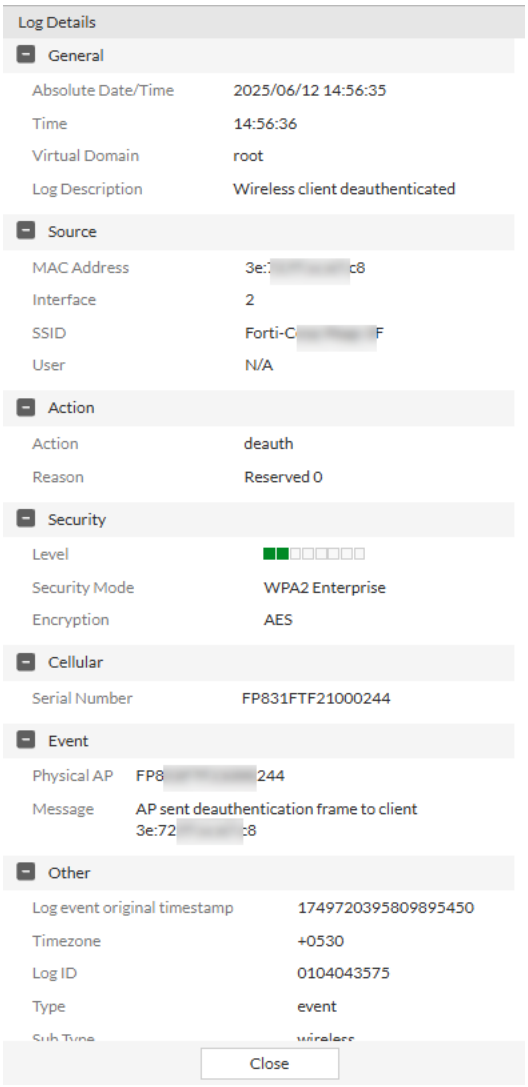
WiFi Events



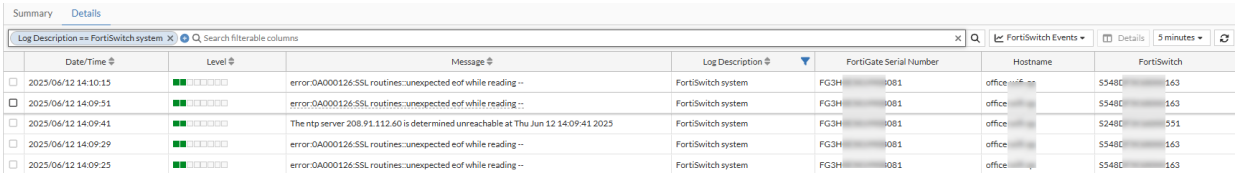
The following log details are displayed for each event.

Parameter	Description
Date/Time	The Date/time of log event generation.
Level	The log severity level. • Emergency, Critical (red) • Alert (orange) • Error, Warning (blue) • Notice, Information, Debug (green)
Action	The action leading to the event generation.
Message	The event log message that is generated.
SSID	The SSID that the client connected to.
Station MAC	The client MAC address.
Log ID	A unique identifier assigned to the event log.
FortiGate Serial Number	The serial number of the associated FortiGate controller.
Hostname	Name of the device.
FortiAP	The serial number of the access point that the client associated with.
Relative Date/Time	The time lapsed since the event log was generated.
Absolute Date/Time	The actual date/time the event log was generated.
Channel	The channel associated with the access point.
Log Description	The description of the event log.
Serial Number	The serial number of the access point.
Source	The event source IP/MAC address.
Status	Status of the access point.
User	The user name/details.
VDOM	Virtual domain name.

Select a log message and click **Details** to view specific related information.



FortiSwitch Events

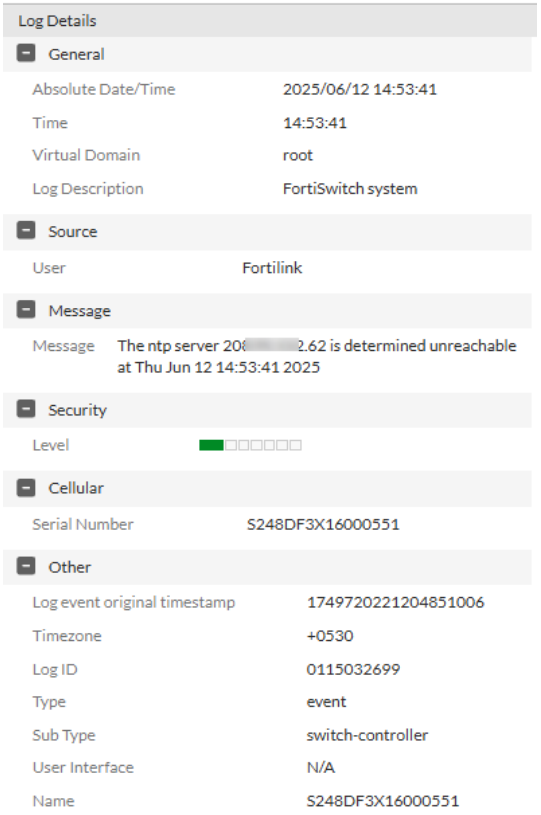


The following log details are displayed for each event.

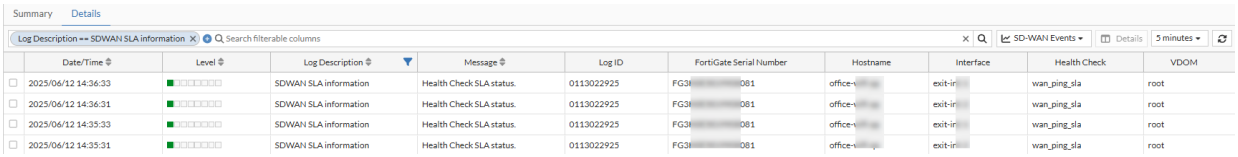
Parameter	Description
Date/Time	The Date/time of log event generation.
Level	The log severity level. • Emergency, Critical (red) • Alert (orange)

Parameter	Description
	• Error, Warning (blue) • Notice, Information, Debug (green)
Message	The event log message that is generated.
Log Description	The description of the event log.
FortiGate Serial Number	The serial number of the associated FortiGate controller.
Hostname	Name of the device.
FortiSwitch	The serial number of the associated FortiSwitch.
Absolute Date/Time	The actual date/time the event log was generated.
Action	The action leading to the event generation.
Channel	The channel associated with the access point.
Destination	The destination interface name.
FortiAP	The serial number of the access point that the client associated with.
Log ID	A unique identifier assigned to the event log.
Serial Number	The serial number of the access point.
Source	The event source IP/MAC address.
SSID	The SSID that the client connected to.
Station MAC	The client MAC address.
Status	Status of the access point.
User	The user name/details.
User Interface	User interface associated with the event.
VDOM	Virtual domain name.

Select a log message and click **Details** to view specific related information.



SD-WAN Events

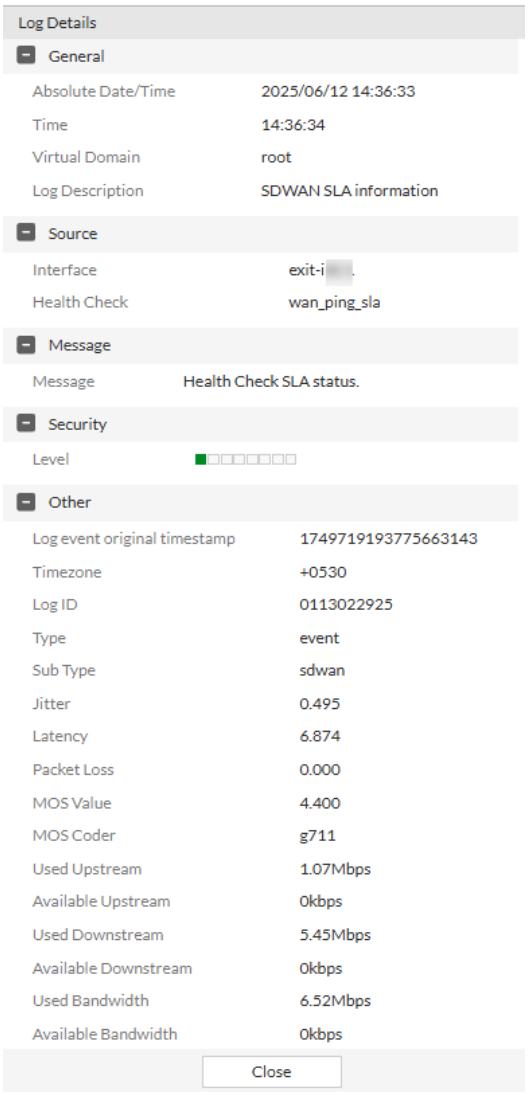


The following log details are displayed for each event.

Parameter	Description
Date/Time	The Date/time of log event generation.
Level	The log severity level. • Emergency, Critical (red) • Alert (orange) • Error, Warning (blue) • Notice, Information, Debug (green)
Log Description	The description of the event log.
Message	The event log message that is generated.
Log ID	A unique identifier assigned to the event log.

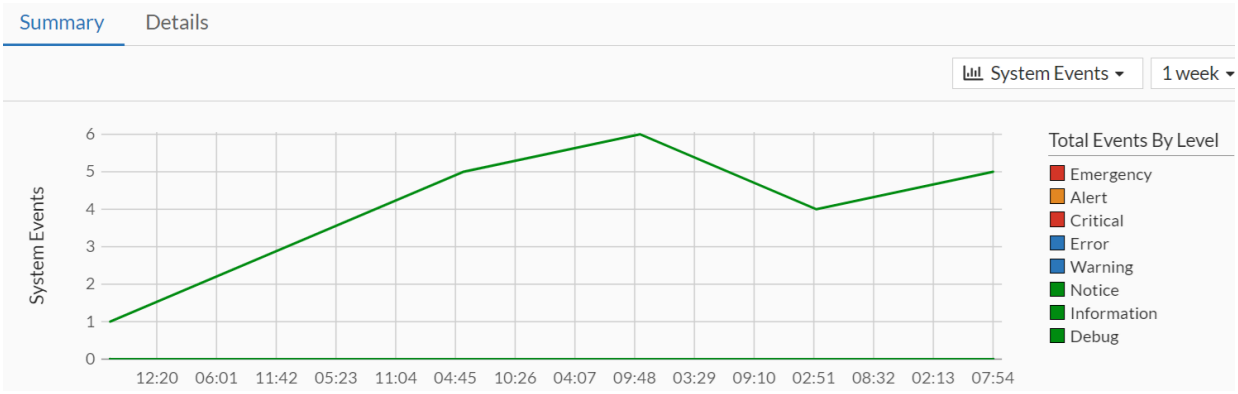
Parameter	Description
FortiGate Serial Number	The serial number of the associated FortiGate controller.
Hostname	Name of the device.
Interface	User interface associated with the event.
Health Check	Health check status of the SD-WAN.
VDOM	Virtual domain name.

Select a log message and click **Details** to view specific related information.

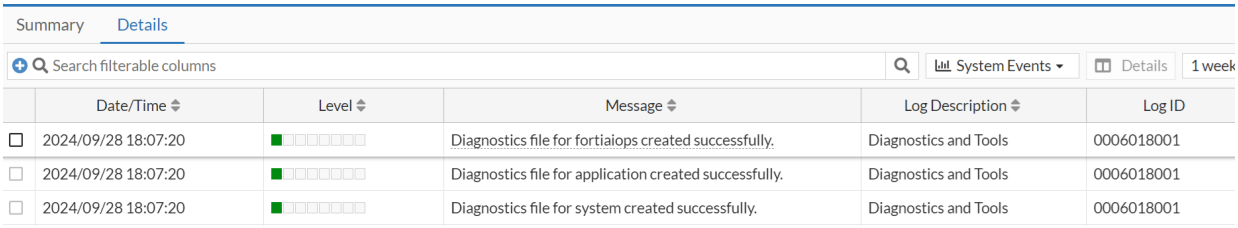


Local Logs

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.



Reports

You can create and view multiple report categories and types on FortiAIOps. Each report displays specific data based on the configurations and can be viewed or downloaded in multiple formats.

- Creating Reports
- Viewing Reports
- Scheduled Reports
- PCI Reports

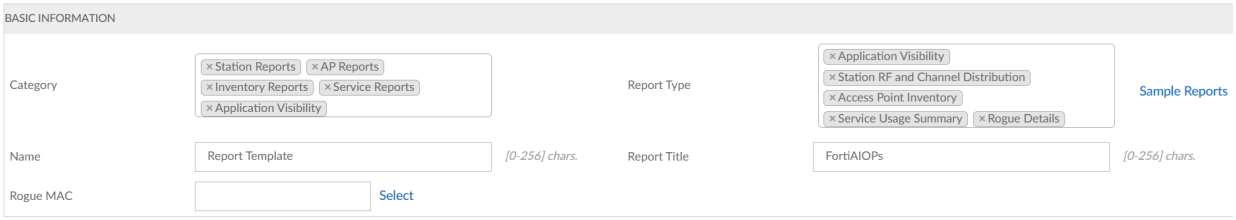
Creating Reports

FortiAIOps allows you to define new reports and generate one-time reports. You can select and combine multiple report categories and the subsequent report types (maximum 5) to generate a single report instead of

generating multiple reports for each category. These are saved as *Report Templates* and can be scheduled similar to other reports.

Basic Information

This section allows you to choose a **Category** of report, **Report Type**, provide a **Name** and **Report Title**.



The following categories of reports are supported.

- Station Reports
- AP Reports
- Inventory Reports
- Service Reports
- Application Visibility Reports

Station Reports

The following types of station reports are supported.

Category	Description

Station RF and Channel Distribution	Provides the station RF and channel distribution based on the OUI (Organizationally Unique Identifier). A graphical summary of the stations distributed by RF type, stations distributed across 2.4GHz and 5GHz bands and station density on each channel over time is displayed. The following details are displayed.
	• Graphs - The graphs are of the following types.
	  • *Station Density on each Channel Over Time* - This graph displays the station density on each of the channels over time plotted against the time in weeks.
	  • *Station Distribution Across 2.4 GHz, 5GHz, and 6GHz Bands* - This graph displays the station distribution based on the 2.4GHz, 5GHz, and 6GHz.
	  • *Station Distribution by RF Type* - This graph displays the station distribution based on the RF Type.
	• Station RF and Channel Distribution Details - This section provides each station's OUI, Date/Time (GMT), Station MAC, RF Type, AP Name, AP Radio, SSID and Channel.

Category	Description

Station Session Details	Provides the average station session trend details. A graphical summary of the station session trend details of throughput, loss, airtime utilization and noise for a connected station is displayed. The following details are displayed.
	• Graphs - The three types of *Station Session Details* graphs are displayed as follows.
	  • *Trend On Throughput* - This graph displays the trend of Throughput for the selected station.
	  • *Trend On Loss* - This graph displays the trend of Loss for the selected station.
	  • *Trend On Airtime Utilization* - This graph displays the trend of Airtime Utilization for the selected station.
	• Station Session Details - This section provides each station's Date/Time, IP4 Address, IP6 Address, Controller, AP ID, SSID, User, Throughput (Kbps), Loss%, Airtime Utilization% and AP Name.

Top Stations	The *Top Stations* report type generates reports for the busiest stations based on the *Throughput* and Airtime Utilization. This report type generates the top N stations based on the number of bytes transferred and received and total Rx/Tx. The information includes each station's Station Mac, Controller, AP Id, SSID, Throughput (Kbps) and Date/Time (GMT).

Unique Stations	Provides the unique station details based on all stations connected to a network within the reporting interval. A graphical summary of the stations distributed by RF type, stations distributed across 2.4GHz, 5GHz, and 6GHz bands, stations distributed by OUI, stations distributed by device type, and stations distributed by OS type is displayed. The *Unique Station* reports are available to all groups and list stations connected to network during last 24 hours. The following details are displayed.
	• Summary - This section provides the total number of Unique Stations.
	• Graphs - The graphs are of the following types.
	  • *Finger Print OS Distribution* - This graph displays the station distribution based on the OS Type.
	  • *Finger Print Device Distribution* - This graph displays the station distribution based on the Device Type.
	  • *OUI Distribution* - This graph displays the station distribution based on the OUI.
	  • *Station Distribution* - This graph displays the station distribution based on the RF Type.
	• Unique Station Details - This section provides the station's OUI, Date/Time (CST), Station MAC, User, IPv4 Address, IPv6 Address, RF Type, SSID, Device Type, OS Type and Floor.

EAP-AKA Error	The EAP-AKA Error type generates a report with details of EAP-AKA errors associated with specific ESSIDs and on specific stations connected to network within the reporting interval. The following details are displayed.

Category	Description
	• User selected Top 5 EAP-AKA Errors - The top 5 most common EAP-AKA errors with the number of stations the errors were reported on and the number of EAP authentication failures for each station. • User selected Top 5 Station by Errors - The top 5 stations (MAC addresses) with highest EAP-AKA errors reported and the number of EAP authentication failures for each station. • EAP-AKA Errors - The list of EAP-AKA errors within the reporting interval. The details displayed are, date and time of the error, associated controller, access point, station MAC address, and the ESSID, and the error description/reason.

AP Reports

The following types of AP reports are supported.

Category	Description
Rogue Details	The *Rogue Details* report type generates the report on the individual rogue. It displays the rogue mobility trend. The trend is plotted against time and APs detecting the rogue. The data displayed is a Max of hourly data sample. The following details are displayed. • Summary - This section provides the details of the selected rogue • Rogue Mobility Trend graph - Trend is plotted against AP which detects rogues with high strength and its time as samples. • Rogue Details - This section provides details about the APs detecting the rogue along with Date/Time, Controller, AP Detecting Rogue, AP Location, SSID, Channel and RSSI.

Rogue Summary	Summarizes the rogue device information on the trend of the number of rogues reported on a per controller basis, per hour. The rogue APs and rogue station count is displayed. A graphical summary of the trend on rogue AP, trend on rogue station, and trend on controllers is displayed. The following details are displayed.
	• Summary - This section provides the details of the total number of rogues.
	• Graph - The graphs are of the following types.
	  • *Rogue Trend By Type* - The two types of *Rogue Trend By Type* graphs are displayed as follows.
	  • *Trend on Rogue Station* - This graph displays the trend type based on the number of rogue Stations.
	  • *Trend On Rogue AP* - This graph displays the trend type based on the number of rogue APs.
	  • *Rogue Trend By Controllers* - This graph displays the top 10 controllers with the highest number of rogues.
	• New Rogues Detected During Reporting Interval - This section provides the details of the new rogues detected during reporting

Category	Description
	interval. The details are Date/Time, Controller, AP Detecting Rogue, AP Location, Rogue MAC, Rogue Type and Channel RSSI.
Top Radio	The Top Radio report type generates a report displaying all the Top N Radios based on Station Count, Throughput, and High Loss. The top radio report type displays the AP Name, Radio, Controller Name, AP Location, Station and Date/Time (GMT).

Inventory Reports

The following types of inventory reports are supported.

Category	Description
Access Points Inventory	This report type generates the AP inventory summary reports for any access points that are accessible. The following details are displayed. • Summary - This section provides the total number of Access Points. • AP Model Distribution graph - This provides the pictorial representation of the distribution of Access Points. • AP Inventory Summary - This section provides the details of Access Point Inventory. The details are Name, Mac address, Model, Software Version, IP Address, Controller, Availability State, Connectivity Preference and Floor.

Controller Inventory	Lists and tracks all the controllers, with its model and software versions on the network.
	• Summary - This section provides the total number of Controllers.
	• Graph - The graphs are of the following types.
	  • *Controller Software Version Distribution* - This graph displays the Controllers based on the controller software version distribution.
	  • *Controller Model Distribution* - This graph displays the Controllers based on the controller model distribution.
	• Controller Inventory Summary - This section provides the details of Controller Inventory. The details are Hostname, IP Address, Mac address, Node Name, Software Version, Model, Description, Availability State, Management State and Location.

Device Availability	Lists all the controllers and access points with its availability, uptime and down time of each of them. This report generates the report for each Controller and AP. It displays the Device Name, UP Duration, Down Duration time and Availability(%) for the AP and Controller.

Service Reports

The following types of service reports are supported.

Category	Description

Service Usage Summary	Provides the service usage summary based on the ESSIDs. A graphical summary of the top SSIDs based on throughput and number of stations is displayed.
	• Graph - The graphs are of the following types.
	  • *Top SSIDs Based on Throughput* - This graph displays the top SSIDs based on the throughput.
	  • *Top SSIDs Based on Number Stations* - This graph displays the top SSIDs based on number of stations.
	• Network Usage Summary - The Network Usage Summary displays the ESSID, Average Station Count, Max Station Count, Time When Max Station Occurred, Total Unique Stations and Maximum Throughput are displayed.

Service Usage Trend	Provides the service usage trends based on the ESSIDs. A graphical summary of the top SSIDs based on throughput and number of stations is displayed. • Server Usage Trend graphs - These are displayed with a trend of Max, Minimum and Average stations connected and stations throughput on hourly basis during reporting interval. This is a graphical report represented with a line chart having two lines, one for Max and second one for Average station count. • Service Usage Trend Details - The service usage trend report type displays Date/Time (GMT), Max Stations Connected, Min Stations Connected, Avg Stations Connected and Throughput (Kbps).

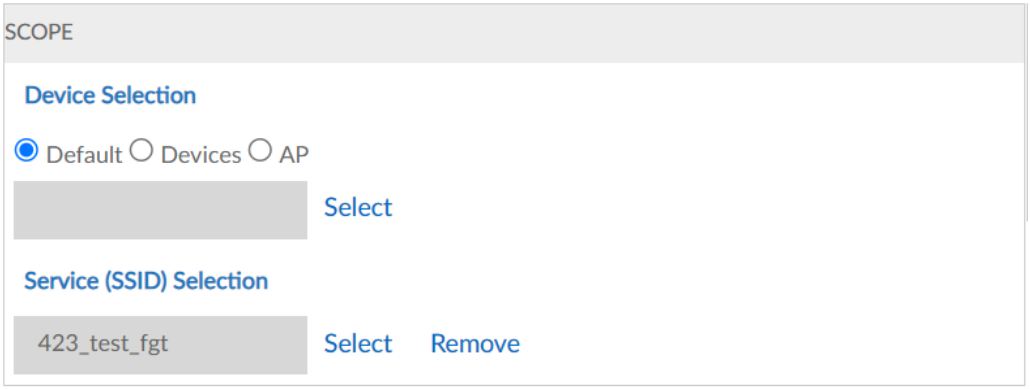
Application Visibility Reports

The application visibility reports provide the following information.

Category	Description
Application Visibility	This report provides the top 10 applications and the top 10 users in your network which allows you to monitor application usage. • Top 10 applications graph - For each application, it provides total number of connected users, ESSIDs and traffic utilization. • Top 10 users graph - For each of the user, it displays the client MAC address, applications connected by the client, ESSIDs and traffic utilization.

Scope

This section allows you to define the scope of a report by performing the device selection followed by the service (SSID) selection.

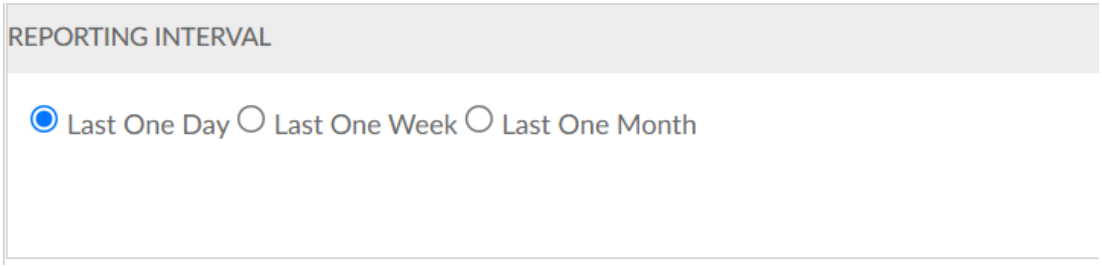


Update the following fields as per your requirement.

- **Default** - By choosing default, report is generated for all the controllers mapped to the FortiAIOps.
- **Devices** - Select one of multiple FortiGate controllers.
- **AP** - Select one or multiple access points.

Reporting Interval

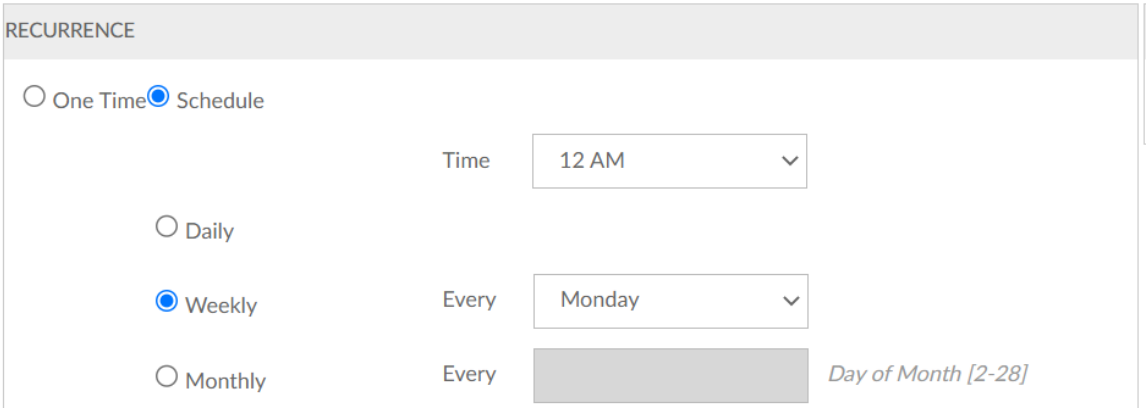
These fields depict the time period to be covered by the selected report. These fields are supported for most report types. When these fields do not appear, the report considers the current status. Select the **Schedule** option of the **Recurrence** section, the following options in the *Reporting Interval* section is enabled.



- **Last one day** - The last one day's report is generated.
- **Last one week** - The last one week's report is generated.
- **Last one month** - The last one month's report is generated.

Recurrence

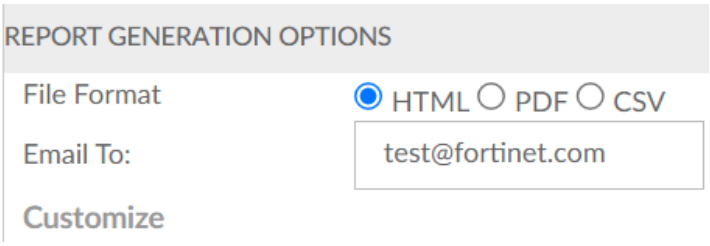
This section allows you to select the time of report recurrence. Select the **Schedule** option and the following get enabled.



- **One Time** - Instant report is generated for the selected reporting interval.
- **Schedule** - This option allows you to define a specific time for report creation. These schedule fields establish the time that a report runs, independent of the **Scope** and **Reporting** Interval.
- **Daily** - This option allows you to generate daily reports.
- **Weekly** - This option allows you to generate weekly reports, select this option followed by selecting the day of the report generation from the **Every** drop-down list.
- **Monthly** - This option allows you to generate monthly reports, select this option and enter the day of month; 1-31 is the valid range.

Report Generation Options

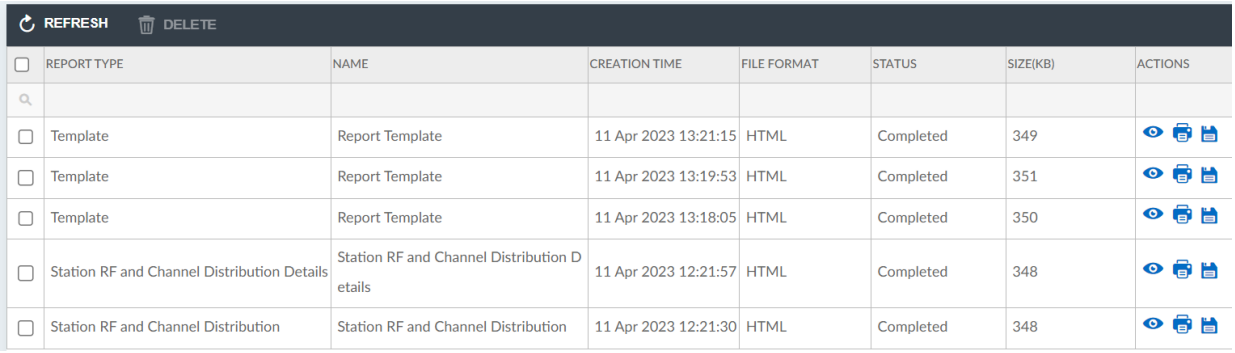
You can save the generated reports in any of the following formats and email the generated reports to the specified address.



- **File Format** - Choose one of the following formats.
  - **HTML** - Select the HTML option to export and save the report to HTML format. The generated report is saved with the naming convention, *<report type>_report_datetime.html*.
  - **PDF** - Select the PDF option to export and save the report to PDF format. The generated report is saved with the naming convention, *<report type>_report_datetime.pdf*.
  - **CSV** - Select the CSV option to export and save the report to CSV format. The generated report is saved with the naming convention, *<report type>_report_datetime.csv*.
- **Limit Report Size To** - This option is applicable only to the *Top Stations*, *Top Radio*, *Device Availability*, and *Application Visibility* reports. The maximum report size for the *Application Visibility* report is 100.

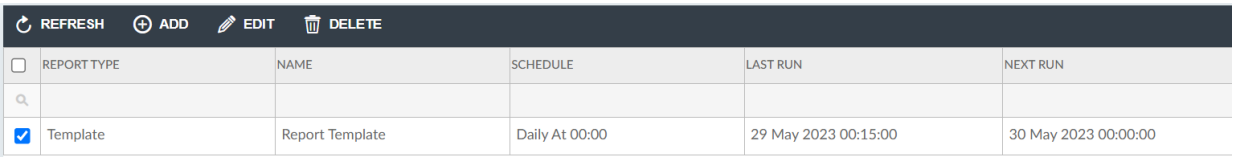
Viewing Reports

This screen displays a list of all the reports that are generated. These reports can be generated in HTML, CSV, or PDF format. They can be viewed, printed or saved locally.



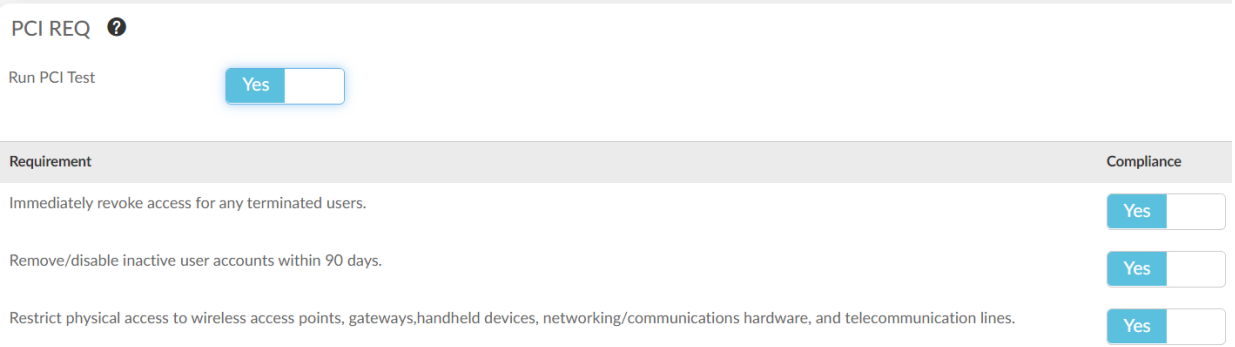
Scheduled Reports

This page displays a list of current running reports and reports scheduled to run in the future. In case of recurring reports, the next run time is displayed. To create a new report, click **Add**.

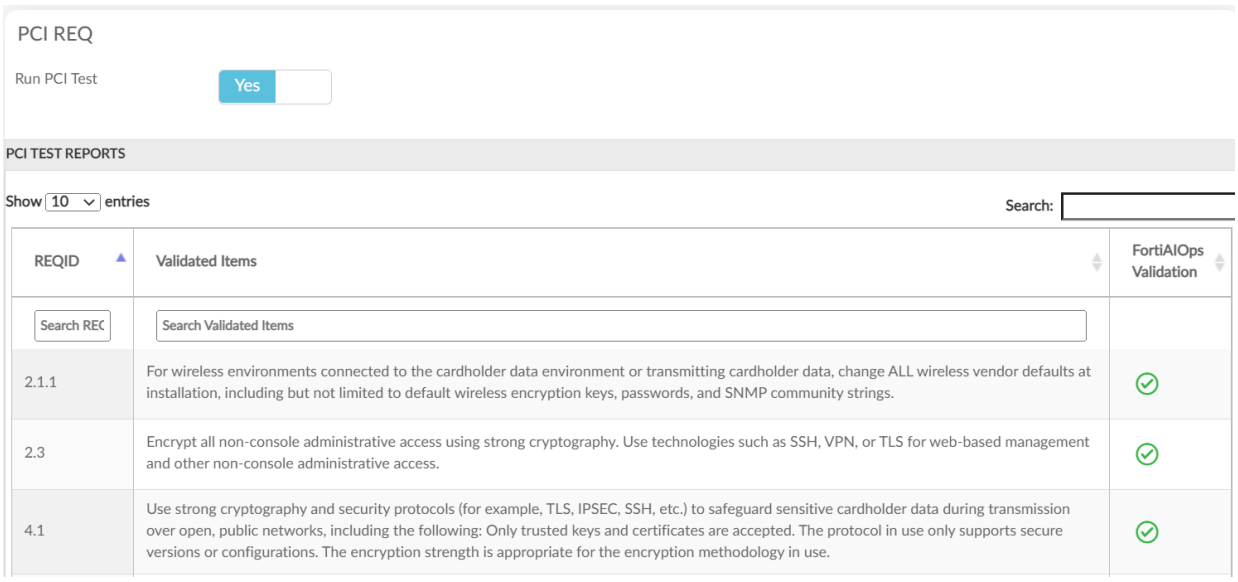


PCI Reports

You can validate FortiAIOps against specific PCI requirement compliance. To run a compliance test, enable **Run PCI Test**. Select the tests to validate FortiAIOps and click **Run Test**.



After the test is successfully completed, the page is refreshed to show the list of PCI requirements that are validated. The validation results are marked with green ticks if they are fully validated and in red if the compliance is not validated or fails. Click **Download PDF Report** to get a copy of the validation results in PDF format.


PCI REQ
Run PCI Test
Yes
PCI TEST REPORTS
Show 10 entries
Search:
REQID
Validated Items
FortiAIOps Validation
Search REC
Search Validated Items
2.1.1
For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.
2.3
Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or TLS for web-based management and other non-console administrative access.
4.1
Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following: Only trusted keys and certificates are accepted. The protocol in use only supports secure versions or configurations. The encryption strength is appropriate for the encryption methodology in use.

System

The System section includes several pages that offer valuable insights into various aspects of system management, such as users, user groups, backup and restore, maintenance, licensing, and location services.

- User Management
- Backup and Restore
- Settings
- Upgrade
- Licensing
- FortiGuard
- Location Services
- Network Interface
- Certificates

User Management

The User Management in the System allows you to view the users and configure user groups and provide the access permissions.

- Users
- User Groups

Users

The FortiAIOps allows administrators to create users, who will subsequently be available in the FortiAIOps application.

User profiles within FortiAIOps are 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.

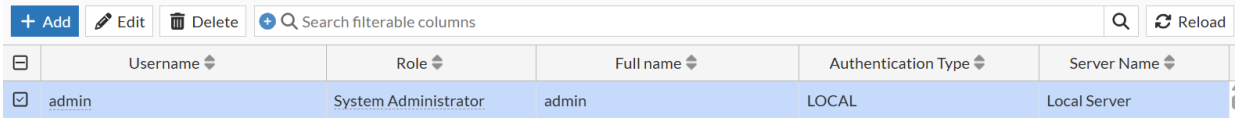
Note:

- 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.

User permissions are indirectly assigned through their membership in user groups. By default, all users are members of the *Default* user group. The *admin* user and all device groups are automatically members of the *Super User* user group, and cannot be moved to any other user group. All users must belong to at least one user

group. It is recommended to assign both the device group and users to the user group upon its creation to ensure that users have access to the assigned device group. If a user is removed from a user group, they will be moved to the *Default* user group.

Note: User Management configuration can only be performed by users with the *System Administrator* and *Super User* roles.



- Adding a New User
- Editing User Information
- Deleting User Information

Adding a New User

Perform the following steps to add a new user:

1. Click **+Add User**.
2. Enter the user information such as Full Name, and Username.
3. In the **Type** field, select the type of server. Choose between LOCAL, RADIUS, LDAP, Microsoft Active Directory, SAML SSO, or Microsoft ADFS SAML IDP.
4. Select the server from the **Server** drop-down menu.
   Note: If the **Type** selected is LOCAL, enter a password in the **Password** field and confirm the same in the **Confirm Password** field.
5. Enable **Match all users on remote server** to add all users from an remote server. All users specified in the remote server will be able to access FortiAIOps with the selected Admin Profile.
   Note: This option is not available for User Type **LOCAL**.
6. Specify the role. FortiAIOps supports **Guest**, **Standard_User** and **Super_User** roles.

User Role	Access Level
Guest	Read only access to all features in the system except system settings.
Standard_User	Read/Write privilege to all configurations and features except system settings .
Super_User/ System Administrator	Read/Write access across system. All super users will have access to all device groups, all devices, all system settings.

7. Click **Save**.

Notes:

- Once you have created users in FortiAIOps, it is necessary to refresh the FortiAIOps application portal in order for the users list to be updated and displayed in the **User Groups** page.
- The super user or system administrator can provide device group access to a user by choosing the device group and the users in the user group option in FortiAIOps application portal. See User Groups.
- Users created in GUI will be synced to CLI and vice versa.
- By default, user created in CLI will have super-user access, and can be changed from GUI.

Editing User Information

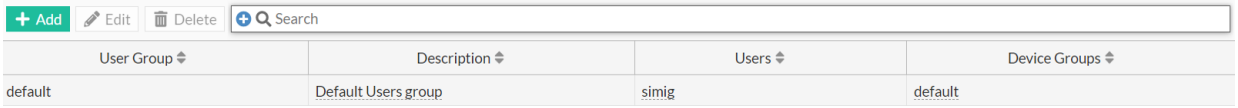
Select a user and click **Edit** to modify user information. This includes changing the user's full name, role or password.

Deleting User Information

To delete a user, select the user and click **Delete**. This action will remove the user from both the GUI and CLI.

User Groups

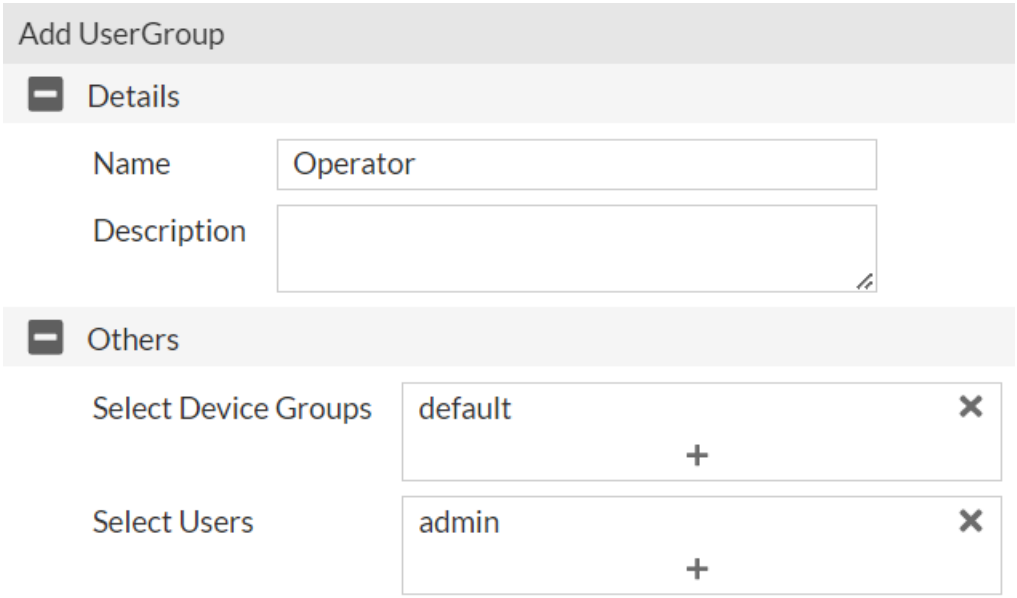
The FortiAIOps access assigned to a user group determines what users in that user group can do.



Adding a User Group

To add a user group, perform the following steps:

1. Navigate to User Groups.
2. Click **+ Add.**
3. Enter a name and description.
4. Select the Device Group that the users should be part of.
5. Select the Users from the list to be added.
6. Click **Create.**



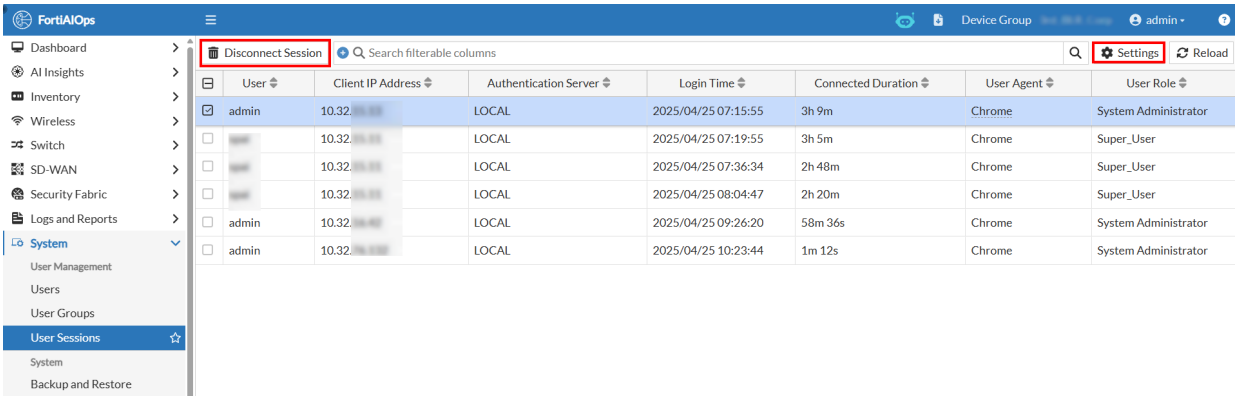
To edit an user group, select an existing user group from the list and click **Edit**.

To delete an user group, select the user group and click **Delete**.

User Sessions

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**.



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.

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

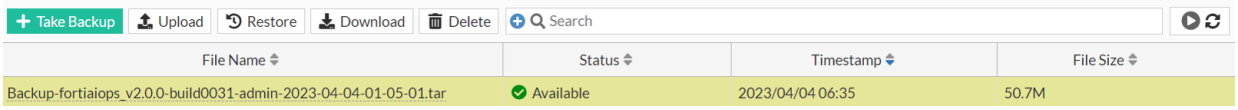
Note:

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

Backup and Restore

The **Backup and Restore** page provides valuable tools for managing and maintaining backups of the FortiAIOps configuration. This page includes options for taking, uploading, restoring, downloading, and deleting backups.

Note: This release supports the backup and restore function only for FortiAIOps configuration. CLI configurations are saved using the `execute backup config` command and it does not include any FortiAIOps specific configurations.

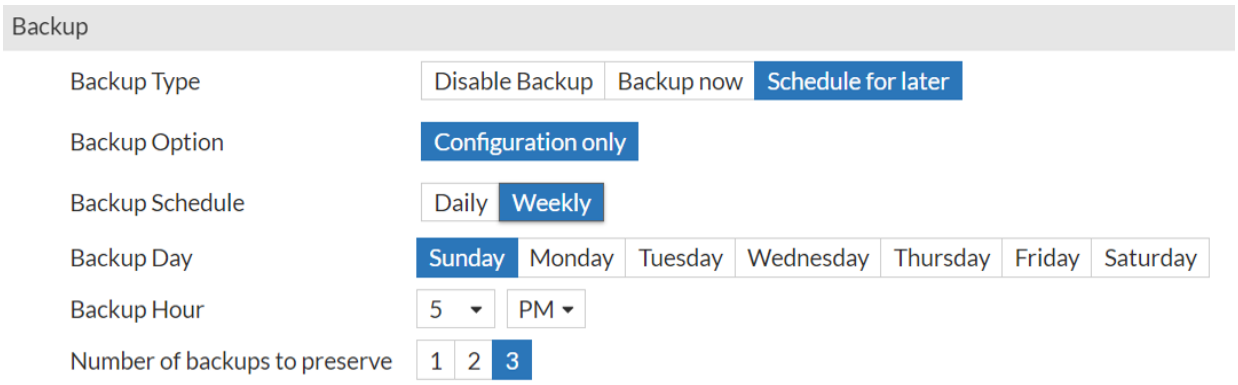


Take Backup

The **Take Backup** function allows you to take a backup of the FortiAIOps configuration. This information can be saved as a file (.tar) and used to restore the configuration and settings at a later time.

To perform the backup operation, perform the following steps:

1. Navigate to **System** > **Backup and Restore**.
2. Click **+ Take Backup.**
3. Select **Backup Option** as **Configuration only**. Backing up only the configuration includes information like maps, controller details, and AP details except statistics data.
4. Select the **Backup Type**. Choose between **Disable Backup**, **Backup now** or **Schedule for later.**
5. If schedule for later is selected, select backup schedule, day, hour and number of backups to preserve.
6. Click **Save.**



Upload

To upload an existing backup file, perform the following steps:

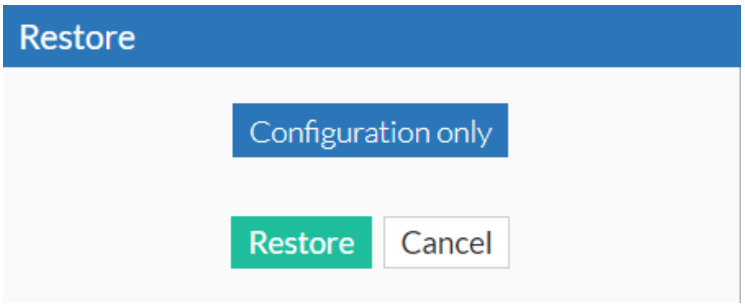
1. Navigate to **System** > **Backup and Restore**.
2. Click **Upload.**
3. Browse and select the backup file (.tar) file.
4. Click **Upload.**

Restore

To restore a backup, select the a backup from the list and click **Restore.**

Notes:

- When restoring a backup file on a different FortiAIOps machine, it is necessary to configure the latest FortiAIOps IP address in the FortiGate syslog settings.
- Admin credentials are retained after restoring the backup file.



Download

To download a backup file to your local machine, select the backup file from the list and click **Download.**

Delete

To delete a backup file, select the backup file from the list and click **Delete.**

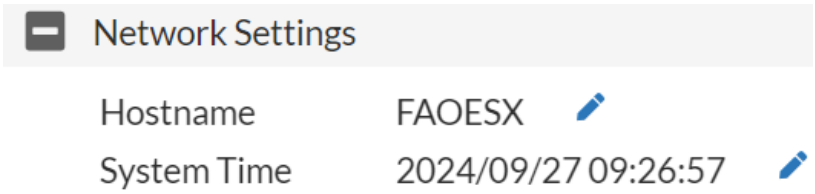
Settings

This page provides the following network and server maintenance parameters to be configured.

- Network Settings
- Statistics
- Administration Settings
- OUI Update
- General Logs
- Mail Server
- Authentication Servers

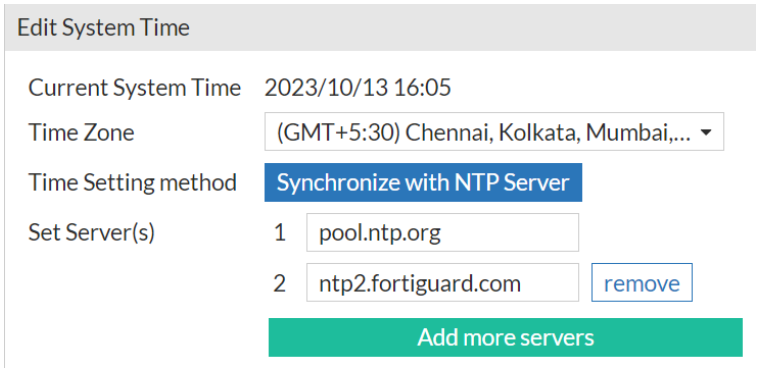
Network Settings

This section allows you to configure various system settings. Click icon to edit the system settings.



The **Hostname** displays the hostname of the system currently in use.

The **System Time** displays the current system time. This setting allows you to select timezone, set time and configure NTP server.



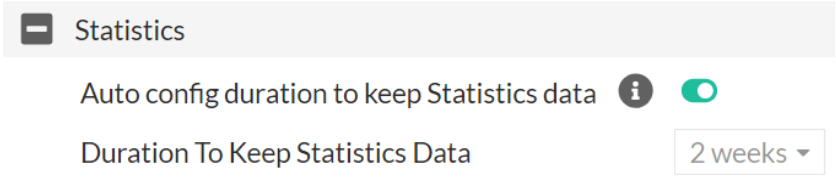
Notes:

- Both FortiAIOPs and FortiGate must be synchronized with an NTP server.
- Reboot the system (`execute reboot` command) after the NTP and timezone settings are configured.

Statistics

This section allows you to configure data retention period in FortiAIOps. All monitoring data is stored based on dynamically allocated or manually configured duration.

- **Auto config duration to keep Statistics data** - This feature allows FortiAIOps to dynamically configure the statistics retention period based on daily data accumulation and the available space for maximum data storage. This is enabled by default for a period of 3 weeks, but based on daily monitoring of the data accumulation and available space, FortiAIOps automatically adjusts the statistics retention period.
- **Duration to keep statistics data** - Manually configure the weeks or months to retain and preserve the statistics data. The permissible range is 1 to 3 weeks or 1 to 6 months. The statistics data older than the time period specified in this field from the current date, is automatically deleted from the FortiAIOps server. If the duration configured here requires more than the available space for statistics retention, then FortiAIOps throws an error.



Notes:

- You are allowed to configuring the statistics retention duration manually only based on the available disk space.
- The AI Insight statistics are stored for a maximum period of 1 week.
- Post-upgrade, the configured **Duration to Keep Statistics Data** is retained with **Auto config duration to keep Statistics data** enabled. Based on daily analysis, FortiAIOps configures the statistics retention period automatically.

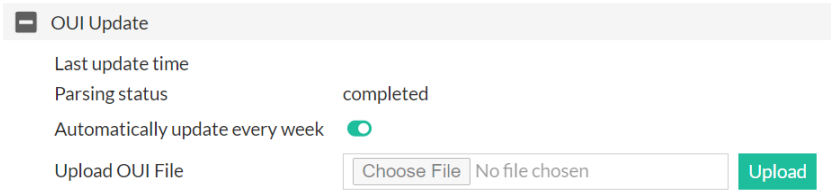
Administration Settings

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

OUI Update

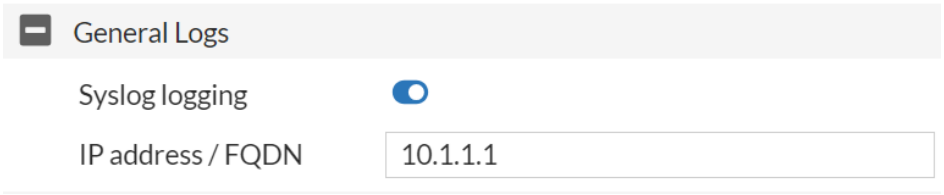
This section allows you to view and manage the OUI details.

- **Last update time** - Displays the date and time of the OUI details updated the last time.
- **Parsing status** - Displays the status of parsing.
- **Automatically update every week** - This option when enabled, will allow the system to automatically update the OUI details every week.
- **Upload OUI File** - To upload OUI file, click **Choose File**, browse and select the OUI file, and click **Upload**.



General Logs

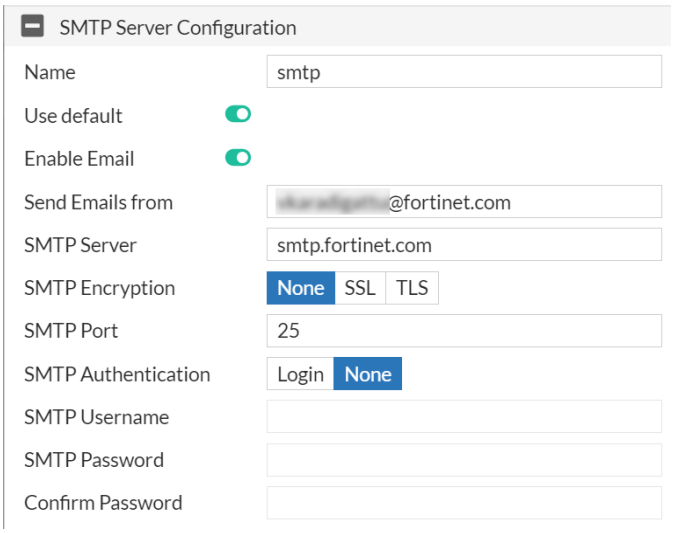
You can now configure forwarding FortiAIOps local logs to a remote machine. Enable **Syslog logging** and enter the IP address/FQDN of remote machine where logs are to be stored.



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

Mail Server

You can configure the SMTP server to receive email notifications for report generation.



Configure the following SMTP server settings.

- **Use default** - If enabled, the current configurations are used as the default for all SMTP server communication.
- **Send Emails from** - Enter the email address to trigger the email notifications from.
- **SMTP Server** - Enter the IP address or the hostname of the SMTP server.
- **SMTP Encryption** - Select the security mode as **SSL** or **TLS**. Select **None** to not use any encryption.
- **SMTP Port** - Enter the port number used to connect to the SMTP server.
- **SMTP Authentication** - Select the authentication via **Login** and enter the **SMTP Username** and **SMTP Password**. Select **None** to not use any authentication for the SMTP server.

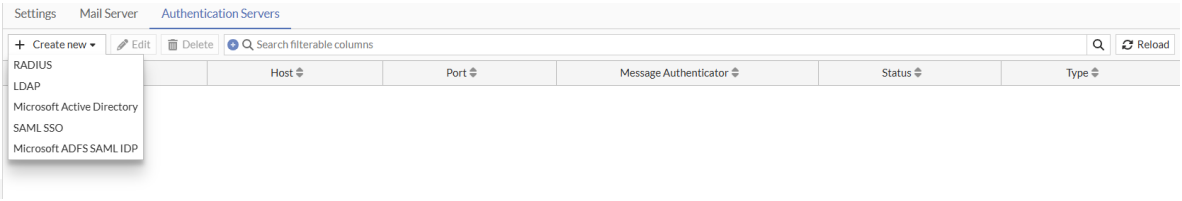
Authentication Servers

Remote users can be authenticated using remote servers.

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.

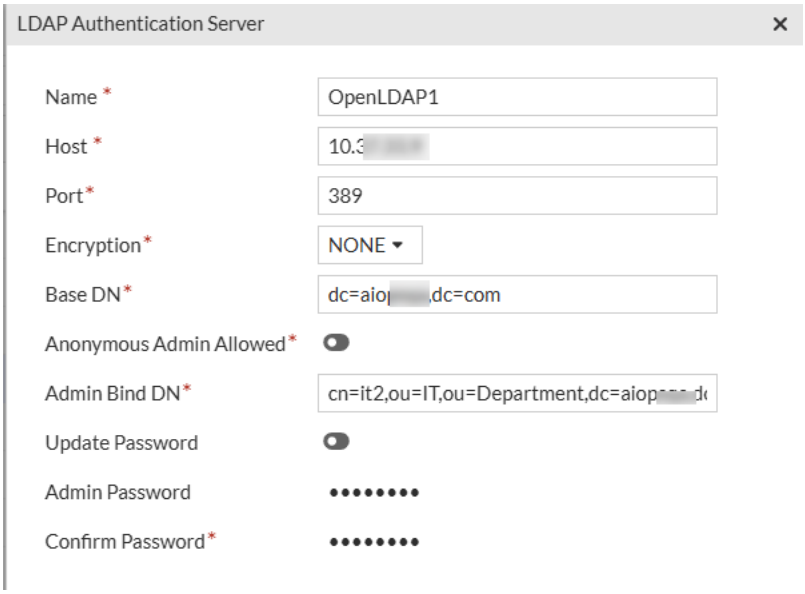
To add an Authentication Server:

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**.



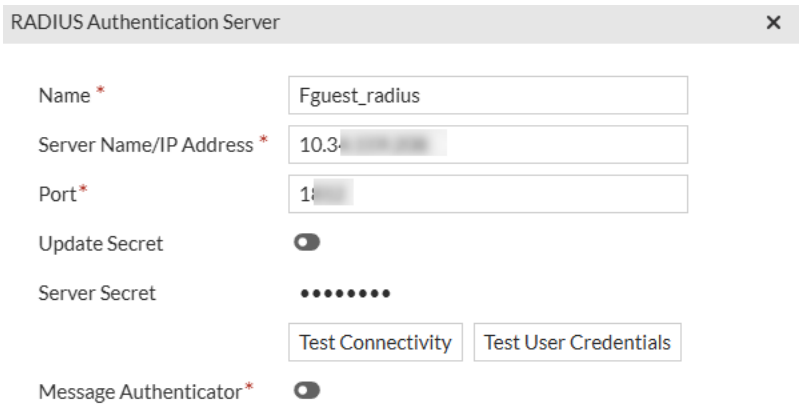
3. Configure the following settings for the server to be added:

- **LDAP Server**:



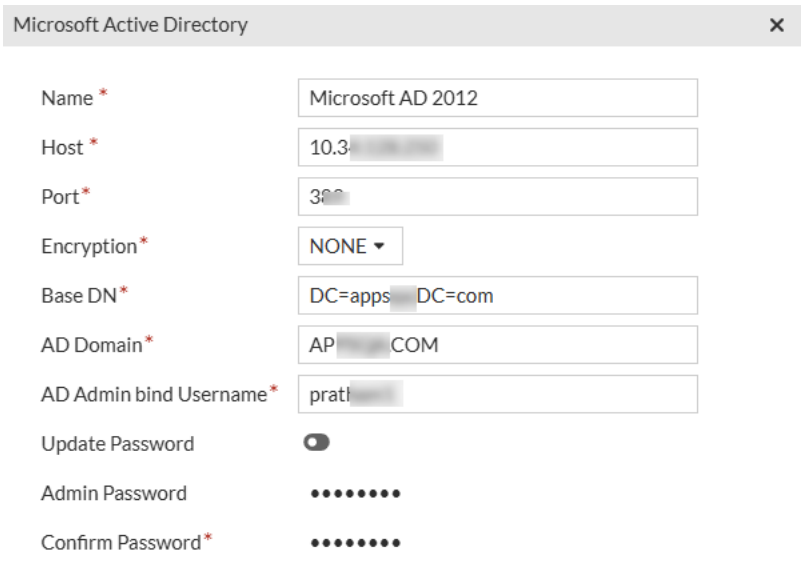
Name	Enter a name to identify the LDAP server.
Host	Enter the IP address of the LDAP server.
Port	Enter the port for LDAP traffic. The default port is 389.
Encryption	Select encryption from the drop-down. Choose between NONE and LDAPS.
Base DN	Enter the base Distinguished Name (DN) for the LDAP server. 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**:



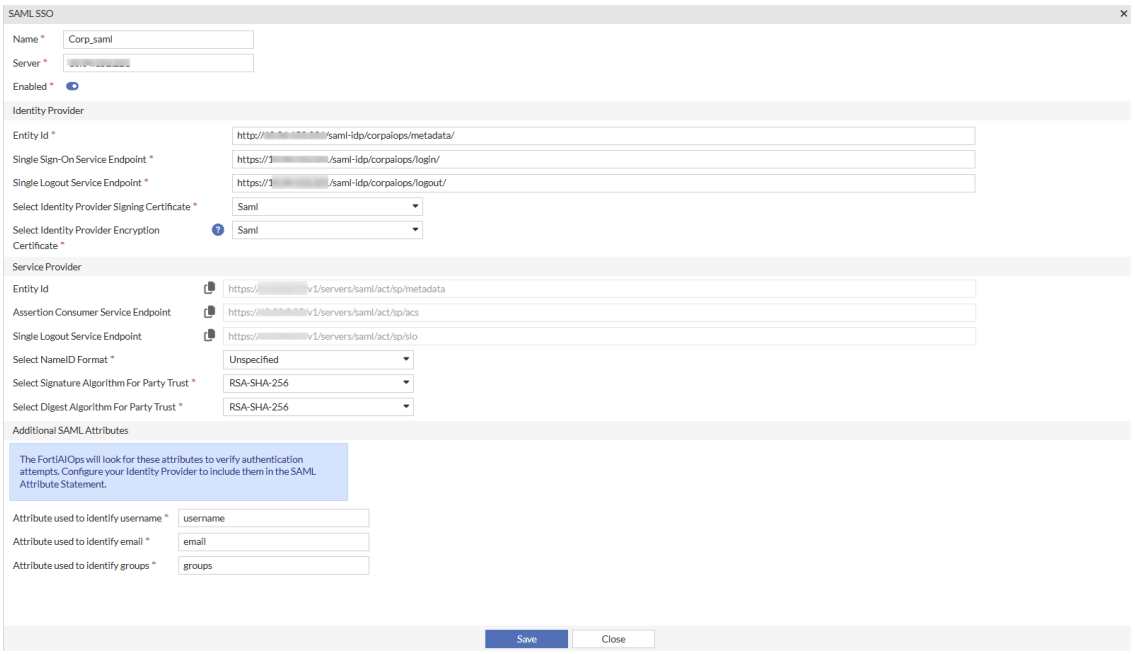
Name	Enter a name to identify the RADIUS server.
Server Name/IP Address	Enter the IP address or fully qualified domain name of the RADIUS server.
Port	Enter the port for RADIUS traffic. The default port is 1812. Some RADIUS servers use port 1645.
Update Secret	Enable to update Server Secret.
Server Secret	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	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.

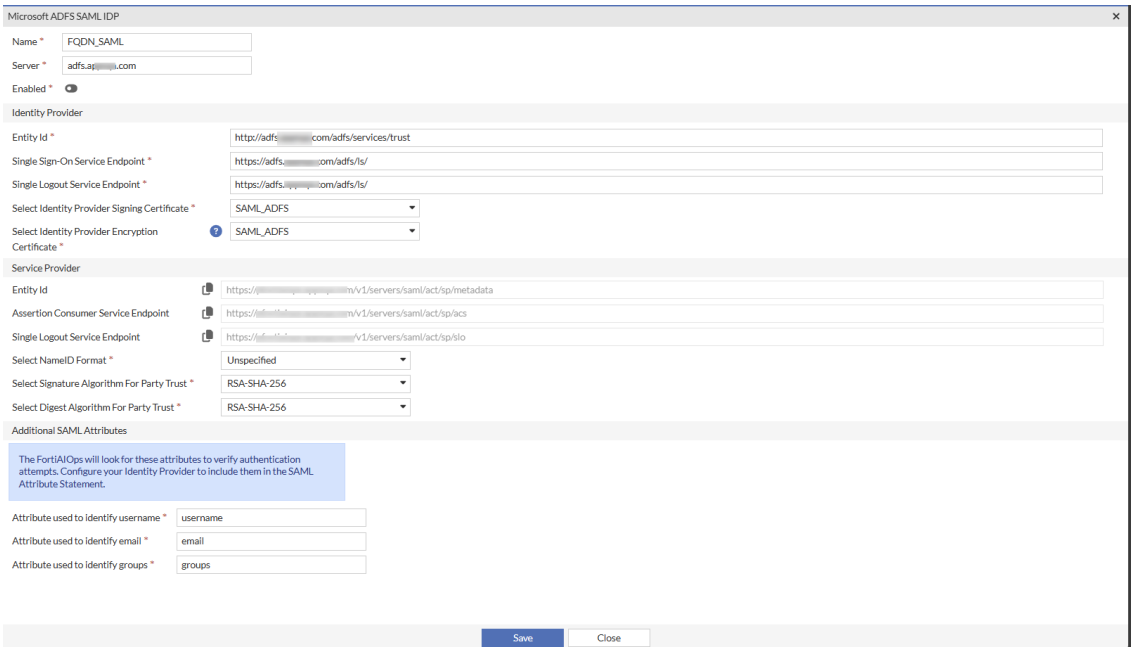
- **SAML SSO**:



Name	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	Select the IdP's encryption certificate. The certificate

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	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.	

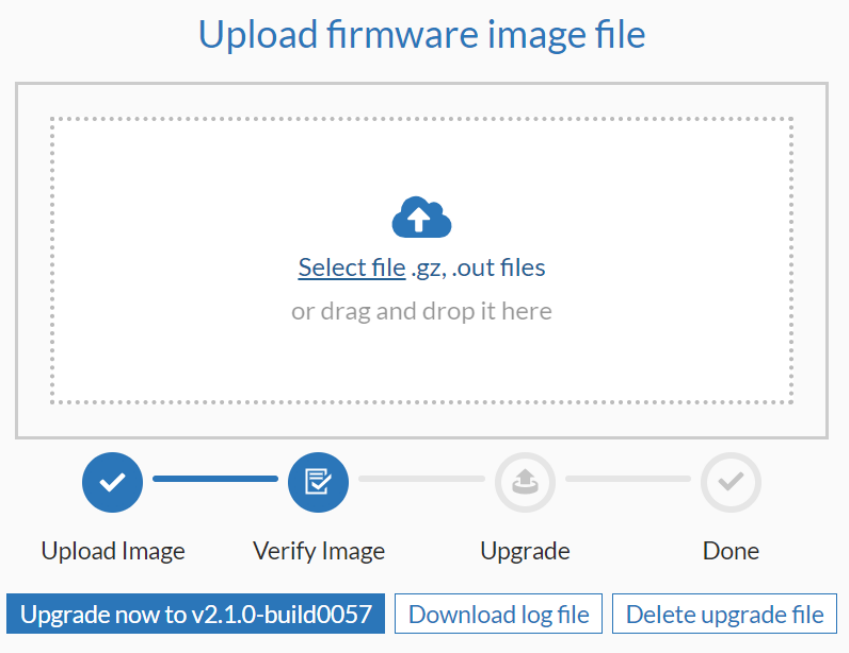
4. Click **Save**.

Note:

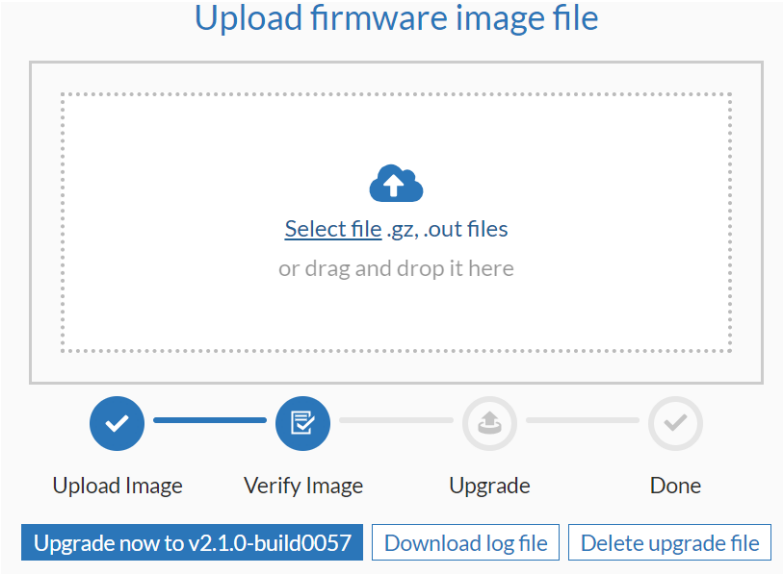
- To make changes to an Authentication Server, choose the desired server and then select the **Edit** option.
- To remove a server from the configuration, select it and then choose the **Delete** option.
- After adding the authentication server details, configure user accounts to utilize this server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

Upgrade

Navigate to **System > Upgrade** to upload the FortiAIOps image file and upgrade FortiAIOps.



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.



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**.

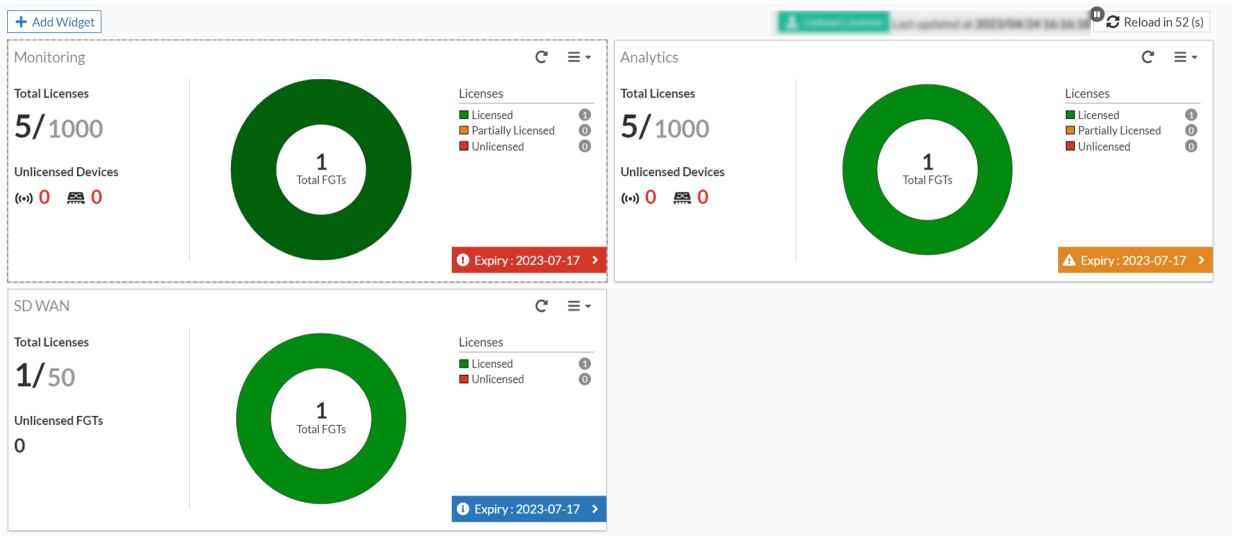
Licensing

The licensing page displays the license information including the current license status, expiration date, and the number of Monitoring, Analytics and SD-WAN licenses.

- **Monitoring** - displays the number of license consumed for monitoring and the number of switches or APs that are unlicensed. The doughnut chart shows the count of FortiGates that are licensed, partially licensed and unlicensed. Click on the filters to view license information in detail. For monitoring license, the consumption is based on the number of switches or APs added.
- **Analytics** - displays the number of license consumed for analytics and the number of switches or APs that are unlicensed. The doughnut chart shows the count of FortiGates that are licensed, partially licensed and unlicensed. Click on the filters to view license information in detail. For analytics license, the consumption is based on the number of switches or APs added.
- **SD-WAN** - displays the number of license consumed for SD-WAN and the number of FortiGates that are unlicensed. The doughnut chart shows the count of FortiGates that are licensed and unlicensed. Click on the filters to view license information in detail. For SD-WAN license, the consumption is based on the number of FortiGates added.

Notes:

- If you buy additional licenses or extend the existing ones through FortiCare, the expiration date displayed will show the nearest expiry and will not include the newly added license. To see the accurate license details, please check FortiCare portal.
- To purchase a co-term license or add any required extra devices to current licenses, please contact your distributor or Fortinet renewal team.

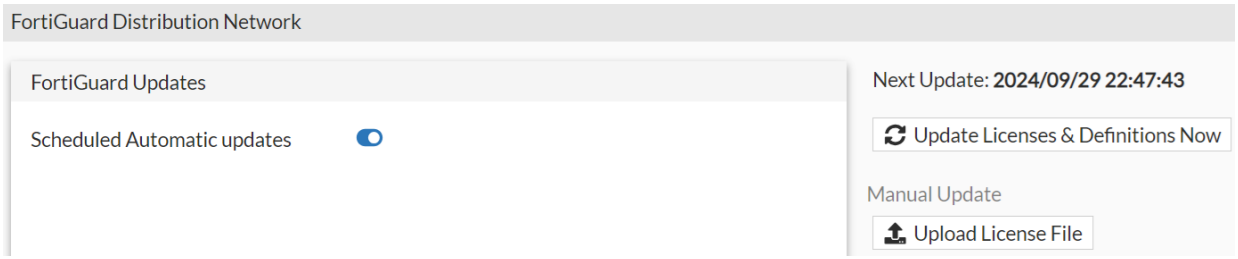


FortiGuard

You can 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**.



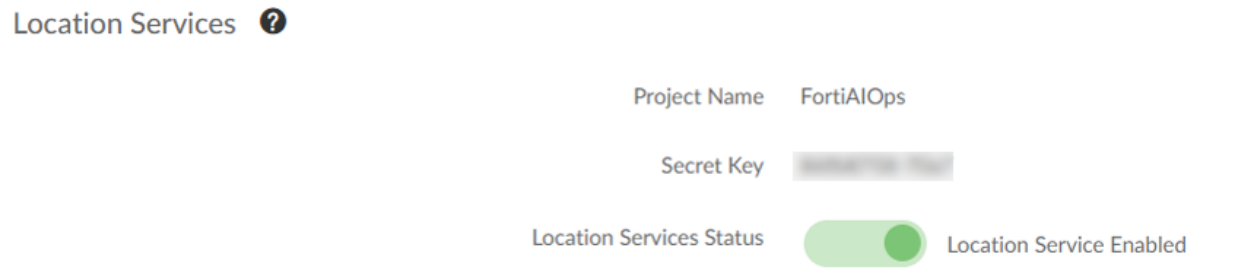
Location Services

Enable location service on this page and configure the following the FortiAP Profile in your FortiGate. To configure the location services, you should perform all necessary configurations within FortiGate. However, the location service status can be enabled or disabled within FortiAIOps.

To configure location based services:

1. Navigate to Location Based Services > FortiAIOps.
2. In the Project Name field, enter **FortiAIOps.**
3. In the Password field, enter the secret key displayed in System>Location Services.
4. In the FortiAIOps server IP field, enter the FortiAIOps IP address.
5. In the FortiAIOps server Port field, enter 4013.
6. Enable the Report Rogue APs option.
7. Configure the Report transmit frequency (seconds) as desired.

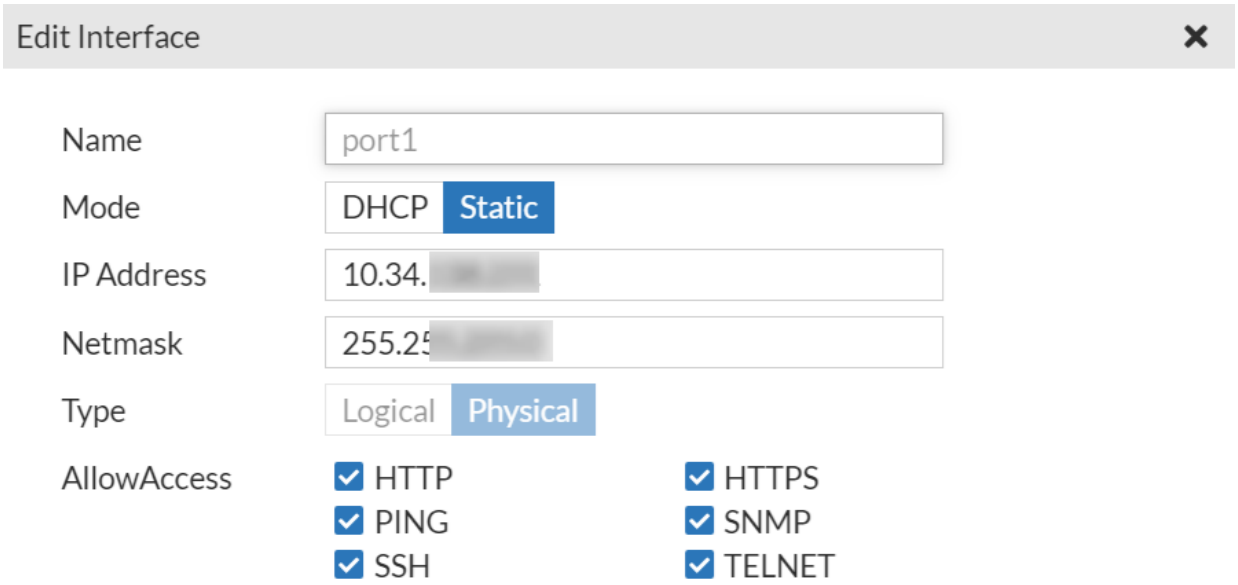
Note: that a minimum of 3 APs must be placed on the map for the locationing service to detect them.



For information on the FortiGate configuration, see the Configuration Guide.

Network Interface

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**.

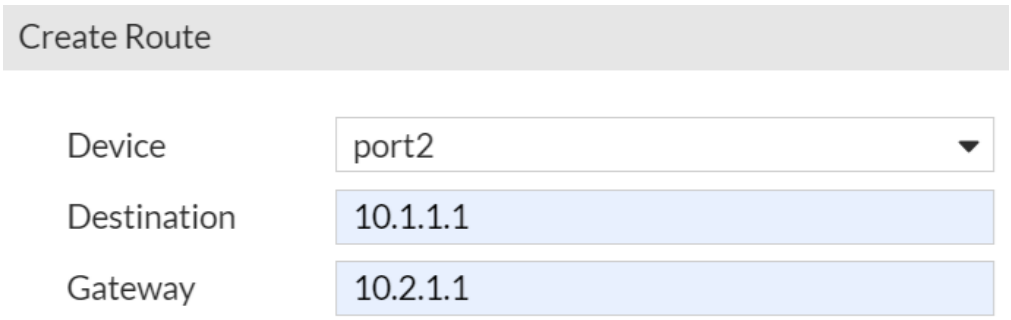


Select a port and click **Edit** to modify the following settings as required.

- **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

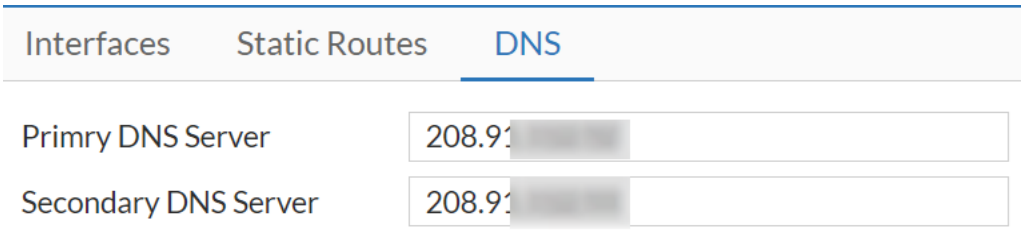
Click **Update**.

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.



- **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**.



Certificates

The Certificates page allows you to manage both local and CA certificates. Certificates provide security assurance validated by a Certificate Authority (CA).

- Local Certificates
- CA Certificates

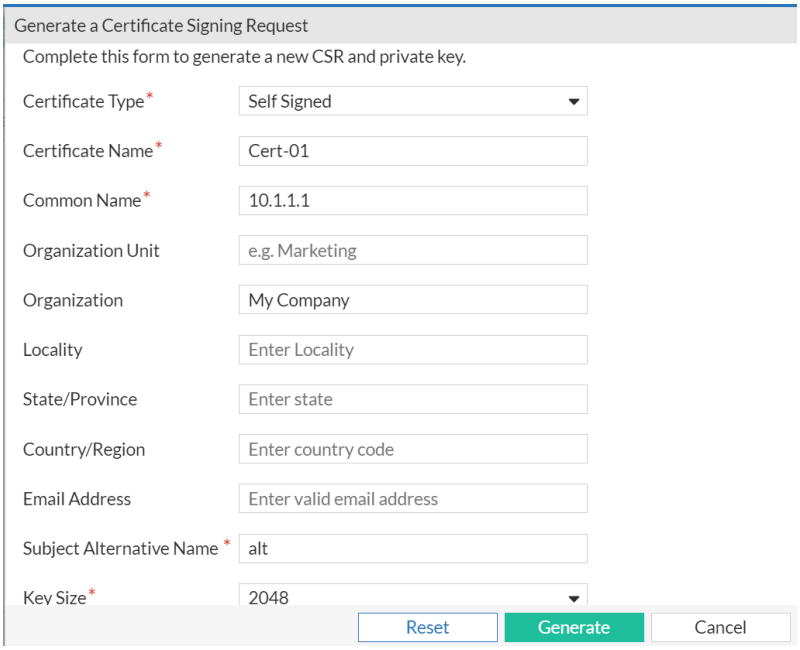
Local Certificates

The Local Certificates section allows you to install certificate key pair by uploading a zip file containing a certificate and a private key file. The supported zip file formats include *.tar, .tar.gz, tgz, zip, tar.xz,* and *.xz*. Also you can generate a Certificate Signing Request (CSR).

Server certificates are generated based on a specific CSR. The CSR is a request sent from an applicant to a CA in order to apply for a digital identity certificate. When a CSR is generated, the associated private key to sign and/or encrypt connections is also generated. Click on the **Generate CSR** button and fill in the required information to generate a CSR for your certificate. In the **Certificate Signing Request** window, enter the following.

- **Certificate Type** - The type of the certificate, either CA signed or self signed.
- **Certificate Name** - A name for the certificate.
- **Common Name** - The FQDN or IP address of the server.
- **Organization** - The name of your establishment or organization.

- **Locality** - The city or area where your organization is located.
- **State or Province** - The state or province of the above mentioned area.
- **Key Size** - Either 2048 or 4096.
- **Subject Alternative Name (SAN)** - It is mandatory to provide SAN.
- Optionally, you can enter the **Organization Unit** and the **Country**.
- Click **Generate**.



CA Certificates

The CA Certificates section allows you to install and manage your CA certificate. To install a CA certificate, click **Install CA Certificate** and upload your CA certificate (*.pem* or *.cer* file). You can view details, download, or delete selected CA certificate after installation.

Notes:

- To upload certificates, the Root CA, server certificate, and key file must be bundled together and uploaded in any of the supported formats.
- Certificates can only be uploaded in PEM or CER formats. Other formats are not supported. If the certificate is in any other format, such as P12 or PFX, it must be converted to a supported format before uploading.
- When using CA2, the intermediate and root CA content must be combined into a single text file (*.pem* file). This is necessary because only three files can be included in the bundle uploaded: Root CA, server certificate, and key file.
- To access FortiAIOps using a custom domain name, you must install the required CA and Server certificates for the domain configured on FortiAIOps.

SAM

Service Assurance Manager (SAM) is a predictive diagnostic software with trouble-prevention capability. It diagnosis the health of the wireless network and reports the issue before the users are impacted. The FortiAIOps infrastructure is used to perform on-demand end-to-end system tests. The SAM mode is activated in FortiAP during SAM tests. In this mode, FortiAP radios operate as a client and perform tests against another AP. Once baseline network performance is established, any schedule tests that deviate from the baseline/threshold are marked based on the SAM test values. Multiple tests can be configured with SAM.

- Connectivity tests to measure packet loss
- Throughput tests to measure performance

The tests can be configured to run on a WPA2 PSK SSIDs available in the FortiGate. SSIDs can only be configured in FortiGate.

Notes:

- The SAM is supported only for the following.
  - F-series, G-series, and K-series FortiAPs. Currently only radio 1 (2.4GHz) and radio 2 (5GHz) are supported for SAM operations.
  - Bridge mode SSIDs
  - WPA2 PSK security mode
  - Radios in AP mode.
- SAM tests are not supported on radio 3 of the K-series and G-series FortiAP models.
- While running SAM tests, FortiAIOps modifies the FortiAP Profile that is configured on the Access Point in FortiGate. As a result, the CAPWAP on the FortiAP is restarted.
- Creating a SAM test causes the following changes to your WLAN network, and these changes impact the clients connected to the FortiAP.
  - New FortiAP profiles are created to run the SAM tests.
  - Schedule and baseline tests are run immediately.
- Trends
- Completed Tests
- Baseline Tests
- Schedule Tests

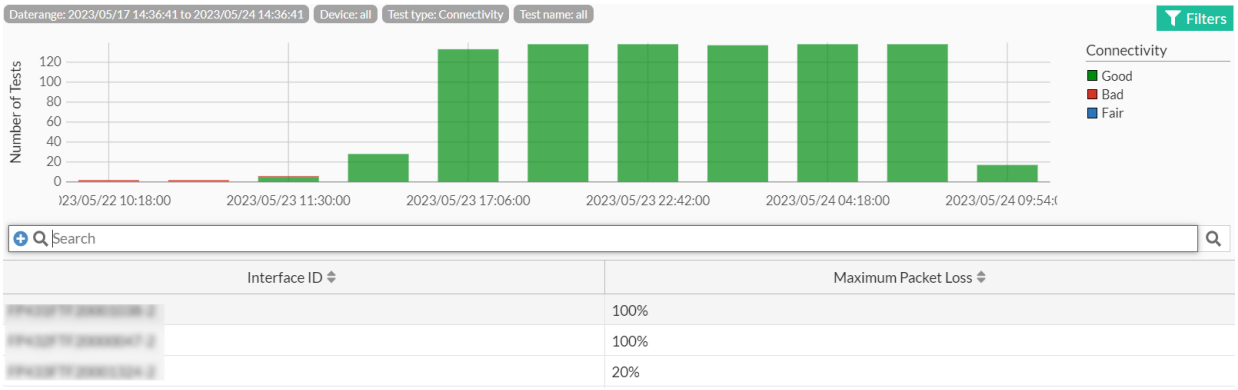
Trends

The Trends page in the Service Assurance section of FortiAIOps provides a comprehensive overview of network test performance. You can analyze the total number of tests performed, their categorization as Good, Fair, or Bad, and gain insights into interface-specific data such as Interface IDs and Maximum Packet Loss values.

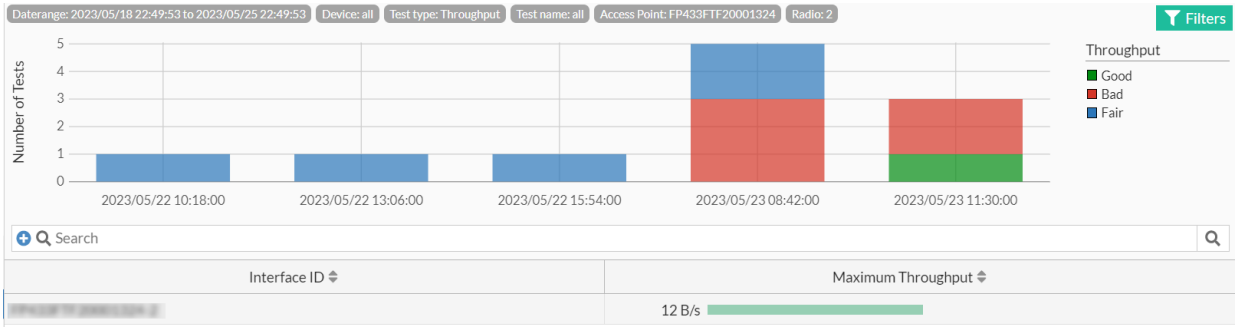
The bar chart classifies the total number of tests performed into three categories: *Good, Fair,* and *Bad*. This classification allows you to quickly assess the overall performance of the network based on the test results.

Each bar represents a specific time period, enabling you to identify trends and patterns in test performance over time.

If the **connectivity** test type is selected, the Trends page presents a table with the *Interface ID* and the *Maximum Packet Loss* for each interface.



If the **throughput** test type is selected, the Trends page displays a table with the *Interface ID* and the *Maximum Throughput* for each interface.

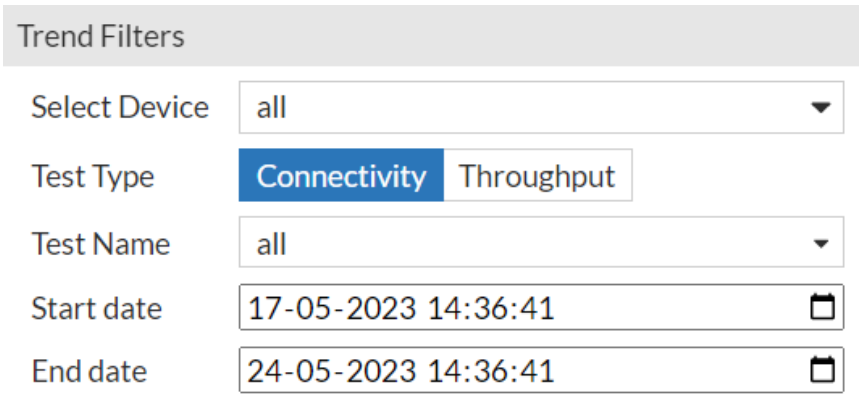


To filter the results in the bar chart, click the desired Interface ID.

Trend Filters

The Trends page offers various filters to refine the displayed data and narrow down the analysis. The available filters include:

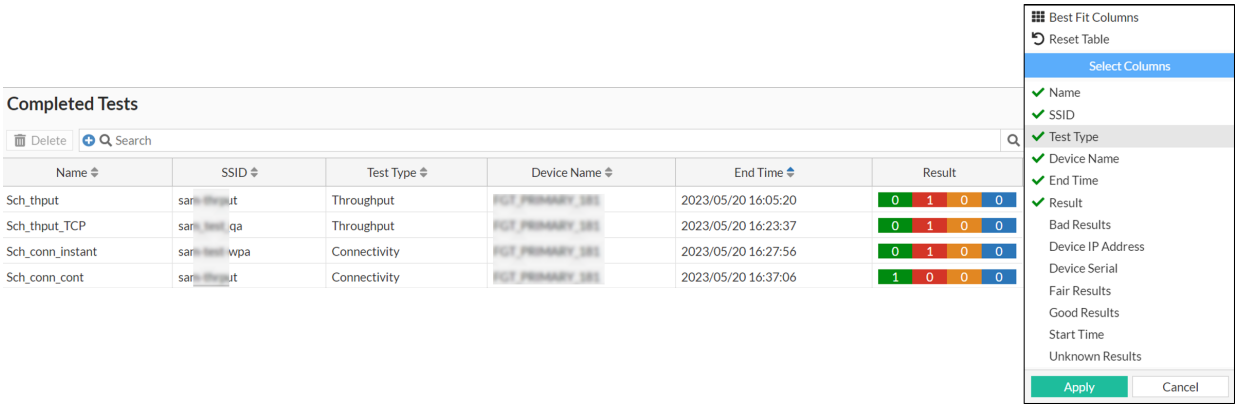
- **Select Device** - Select a specific device from the available options to filter the test results associated with that device.
- **Test Type** - Choose between the *Connectivity* or *Throughput* test types to filter the relevant test results.
- **Test Name** - Select a specific test name to filter the test results associated with that particular test.
- **Start Date and End Date** - Specify a start date and end date to filter the test results within a specific time range.



Completed Tests

Results page provides a comprehensive overview of the Connectivity/ Throughput test results, including completed tests and tests in progress.

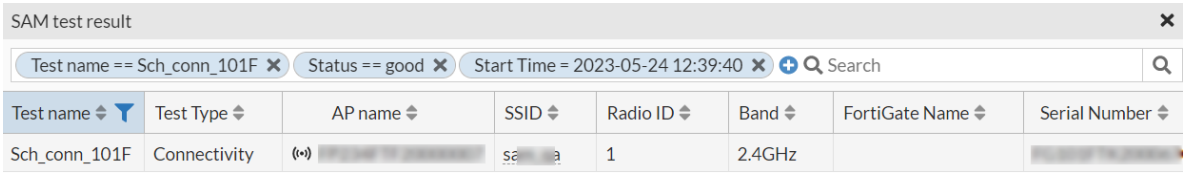
Completed Tests



The Completed Tests panel displays a list of tests that have been completed. It includes the following information for each test:

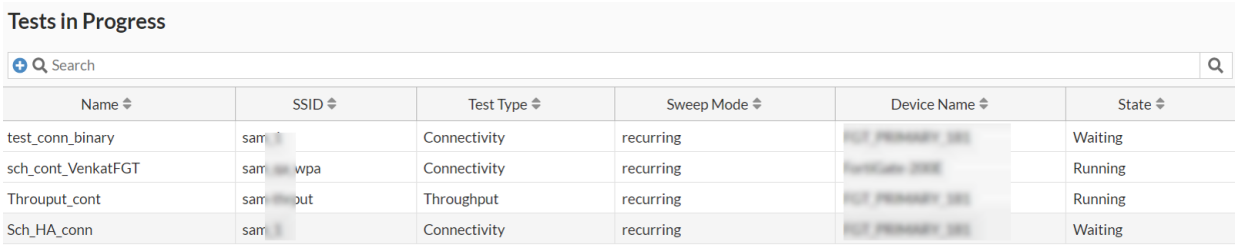
- **Test Name** - The name of the test performed.
- **SSID** - The SSID associated with the test, indicating the network or wireless access point being tested.
- **Test Type** - The type of test conducted, such as *Connectivity* or *Throughput.*
- **Device Name** - The name of the device used to perform the test, allowing users to track the source of the test data.
- **End Time** - The timestamp indicating when the test was completed.
- **Result** - The result field represents the outcome of the test. It is color-coded and displays the number of results categorized as *Good(Green), Bad(Red), Fair(Orange),* or *Unknown(Blue)*. Click on the test results

to view more detailed information.



- **Bad Results** - The number of bad results.
- **Device IP Address** - IP address of the device.
- **Device Serial** - The serial number of the device.
- **Fair Results** - The number of fair results.
- **Good Results** - The number of good results.
- **Start Time** - The timestamp indicating when the test was started.
- **Unknown Results** - The number of unknown results.

Tests in Progress

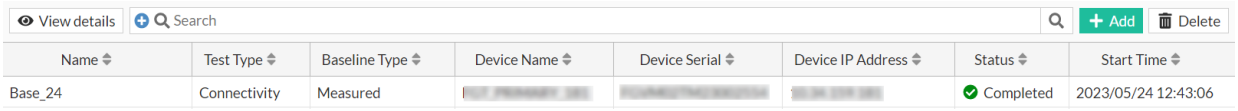


The Tests in Progress panel provides users with a list of tests that are currently in progress or scheduled. It includes the following information for each test:

- **Test Name** - The name of the test performed.
- **SSID** - The SSID associated with the test, indicating the network or wireless access point being tested.
- **Test Type** - The type of test conducted, such as *Connectivity* or *Throughput*.
- **Sweep Mode** - The sweep mode configured for the test, either recursive or baseline.
- **Device Name** - The name of the device designated to perform the test.
- **State** - The current state of the test.

Baseline Tests

Baselines serve as reference points for evaluating the health and performance of the wireless network. Baselines play an important role in detecting deviations from expected network behavior. SAM allows for the configuration of multiple tests, including connectivity tests to measure packet loss and throughput tests to assess overall performance.



Add a Baseline

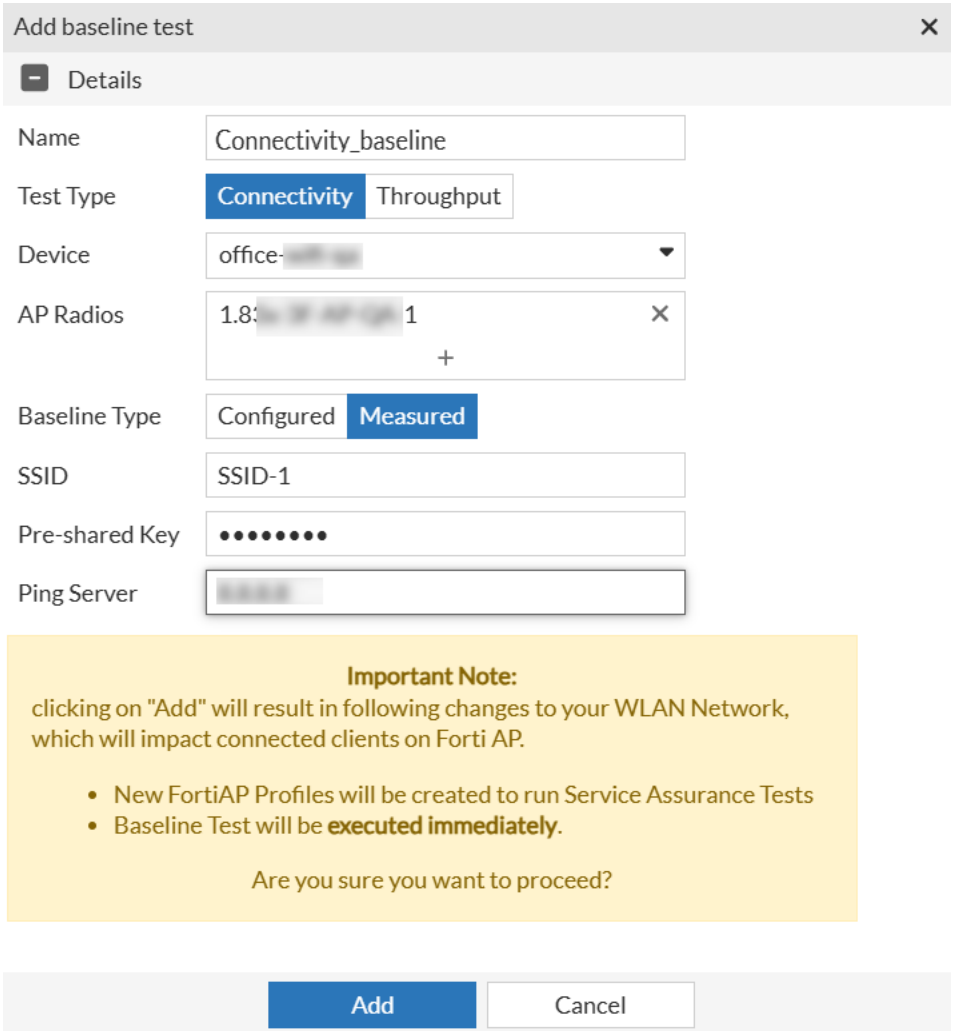
You have two options to execute the baseline tests.

- **Configured Test**: This option allows you to create a baseline test by providing theoretical values.
- **Measured Test**: This option allows you to create a baseline test by providing the actual baseline values. It is important to run a measured baseline when the wireless network is operating either normally or under optimal conditions, as it is used to evaluate subsequent tests.

Connectivity Baseline

To create a connectivity baseline, perform the following steps:

1. Navigate to **SAM** > **Baseline**.
2. Click **+ Add.**
3. Provide the following details:



- **Name**: Name for the baseline.
- **Test Type**: Select **Connectivity** as Test Type to measure packet loss.
- **Device**: Select the device.

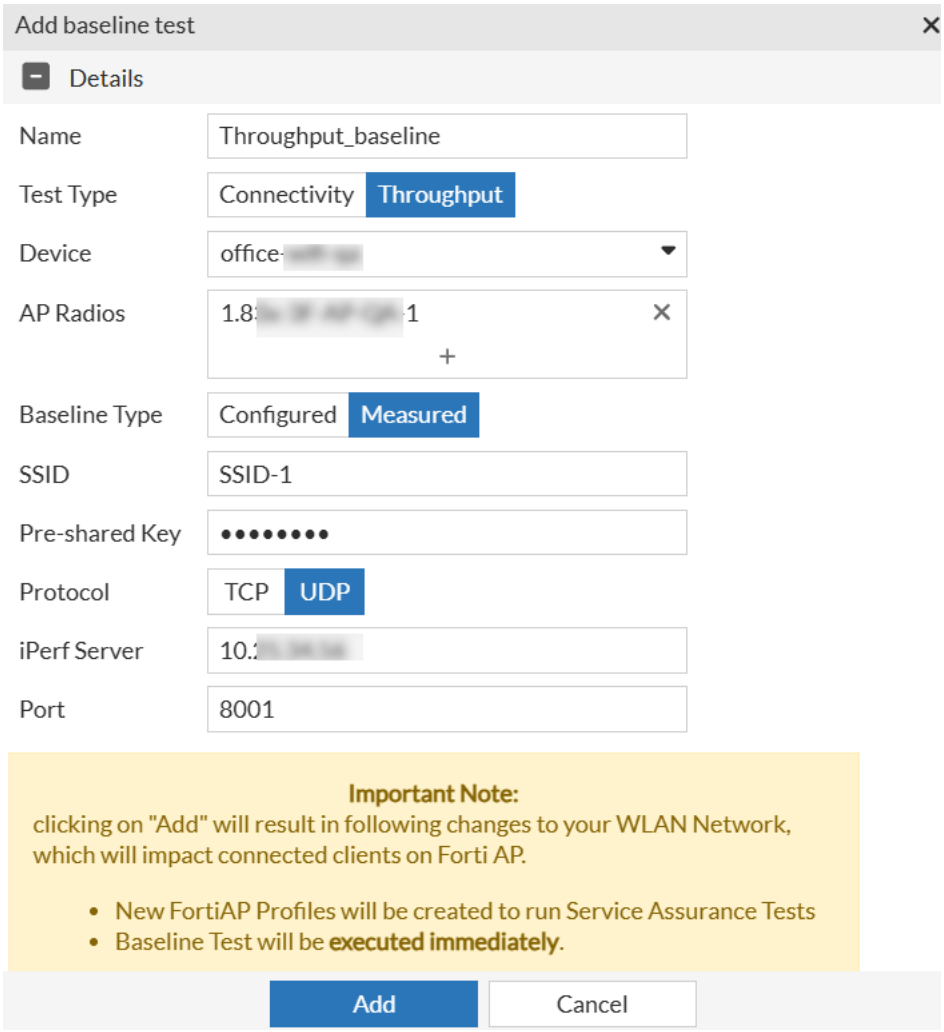
- **AP Radios**: Select AP radios.
- **Baseline Type**: Select baseline type, **Configured** or **Measured**
- **SSID**: Enter SSID name. SSID must be configured on a neighboring AP in FortiGate.
- **Pre-shared Key**: Enter the pre-shared key for the SSID.
- **Packet Loss(%)**: Enter packet loss value in %.
  Note: Packet Loss(%) field is displayed only when **Configured** is selected as baseline type.
- **Ping Server**: Enter **IP address** or **FQDN** of the ping server to perform connectivity tests.

4. Click **Add.**

Throughput Baseline

To create a throughput baseline, perform the following steps:

1. Navigate to **SAM** > **Baseline**.
2. Click **+ Add.**
3. Provide the following details:

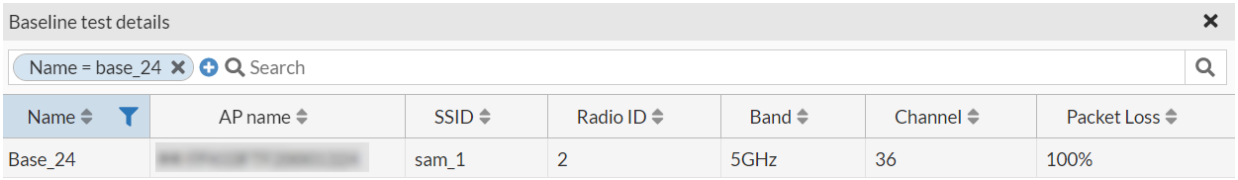


- Name: Name for the baseline.
- Test Type: Select **Throughput** as test type to measure performance.
  Note: Ensure that the network should have Iperf server running iperf3 traffic.

- Device: Select the device.
- AP Radios: Select AP radios.
- Baseline Type: Select baseline type, **Configured** or **Measured**.
- SSID: Enter SSID name. SSID must be configured on a neighboring AP in FortiGate.
- Pre-shared Key: Enter the pre-shared key for the SSID.
- Protocol: Select the protocol, **TCP** or **UDP**.
- iPerf Server: Enter iPerf server details. iPerf server generates TCP and UDP data streams which can be used to measure throughput.
- Port: Enter the port number.
- Throughput(MB/s): Enter throughput value in MB/s.
  Note: Throughput(MB/s) field is displayed only when **Configured** is selected as baseline type.

4. Click **Add.**

To view the detailed information of a baseline, navigate to *SAM* > *Baseline*, select the desired baseline from the list and click View Details.



To delete a baseline, navigate to *SAM* > *Baseline*, select the desired baseline from the list and click **Delete**.

Schedule Tests

The tests are the central activity of the SAM application that is dealt the most. A baseline test is performed occasionally, but the scheduled tests and their results are monitored constantly.

Scheduled tests are measured against a baseline test for Connectivity and Throughput using the configurations provided while creating the test. Only APs and SSIDs within the baseline test is measured in subsequent tests.

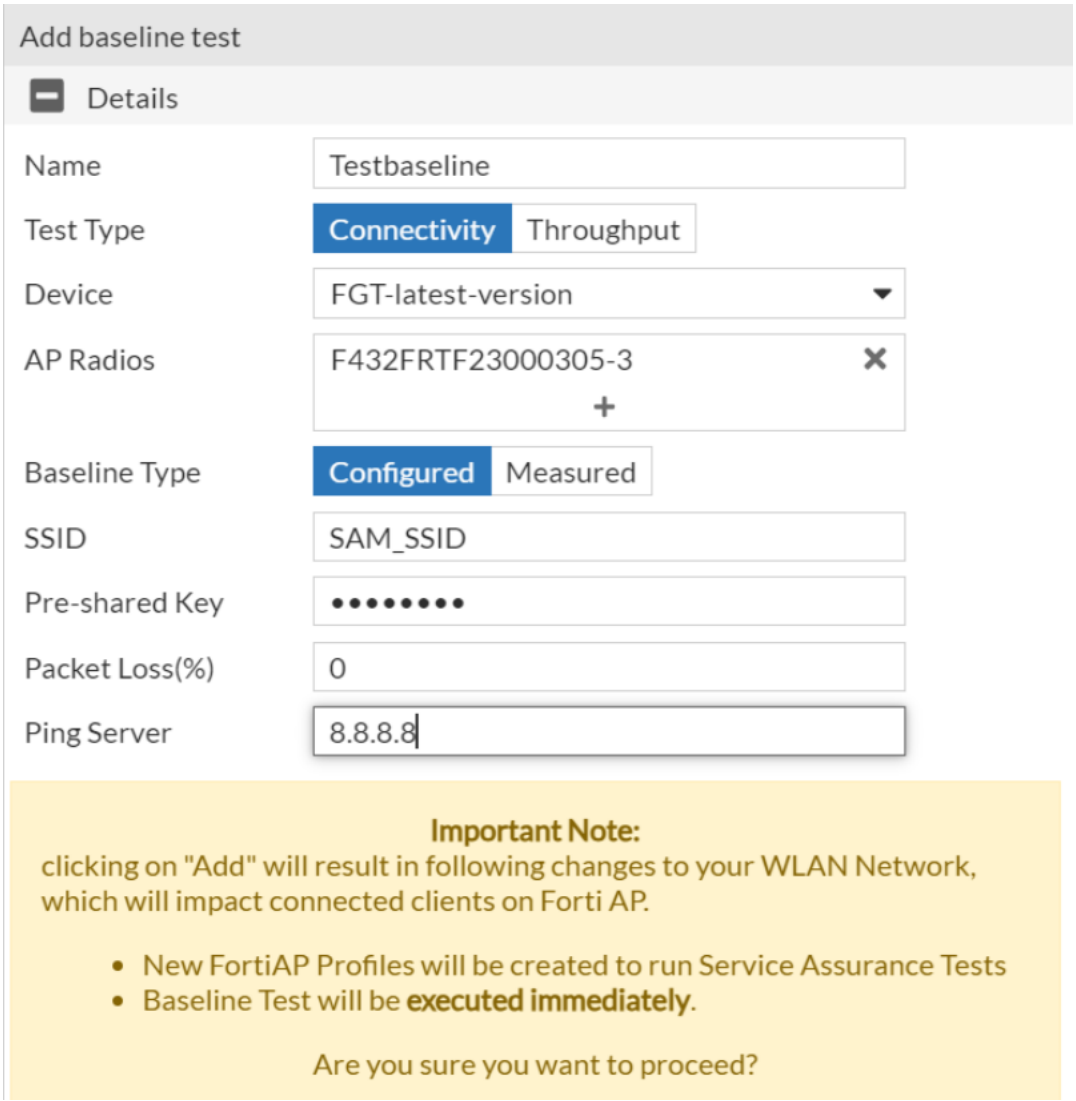
Add a Scheduled Test

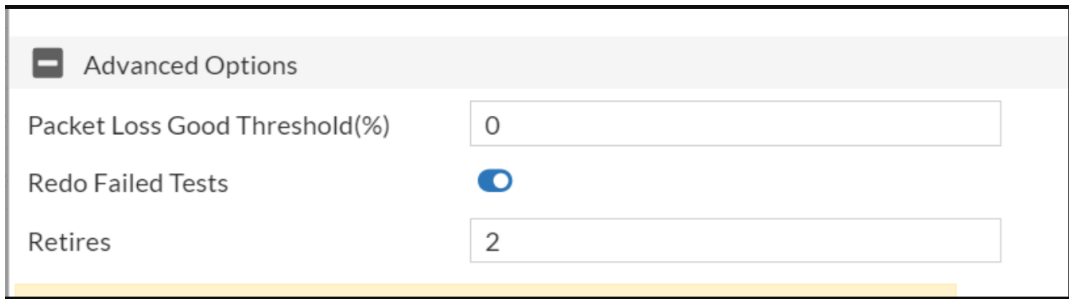
To add a Scheduled Test, follow these steps:

1. Navigate to **Service Assurance>Schedule.**
2. Click **+ Add.**
3. Provide the following details:
   a. Enter a name for the test.
   b. Select Test Type, either **Connectivity** or **Throughput.**
   Note: Based on the test type selection the advanced options filed changes.
   c. Select a device.
   d. Select a Baseline test.
   e. Select Interval. **Instant** option enables to run the scheduled test once, immediately after it is saved. **Continuous** option enables to execute the scheduled test continuously till you disable the test.

4. Configure Advance Options:
   - If Connectivity is selected as Test Type, you can configure the following fields:

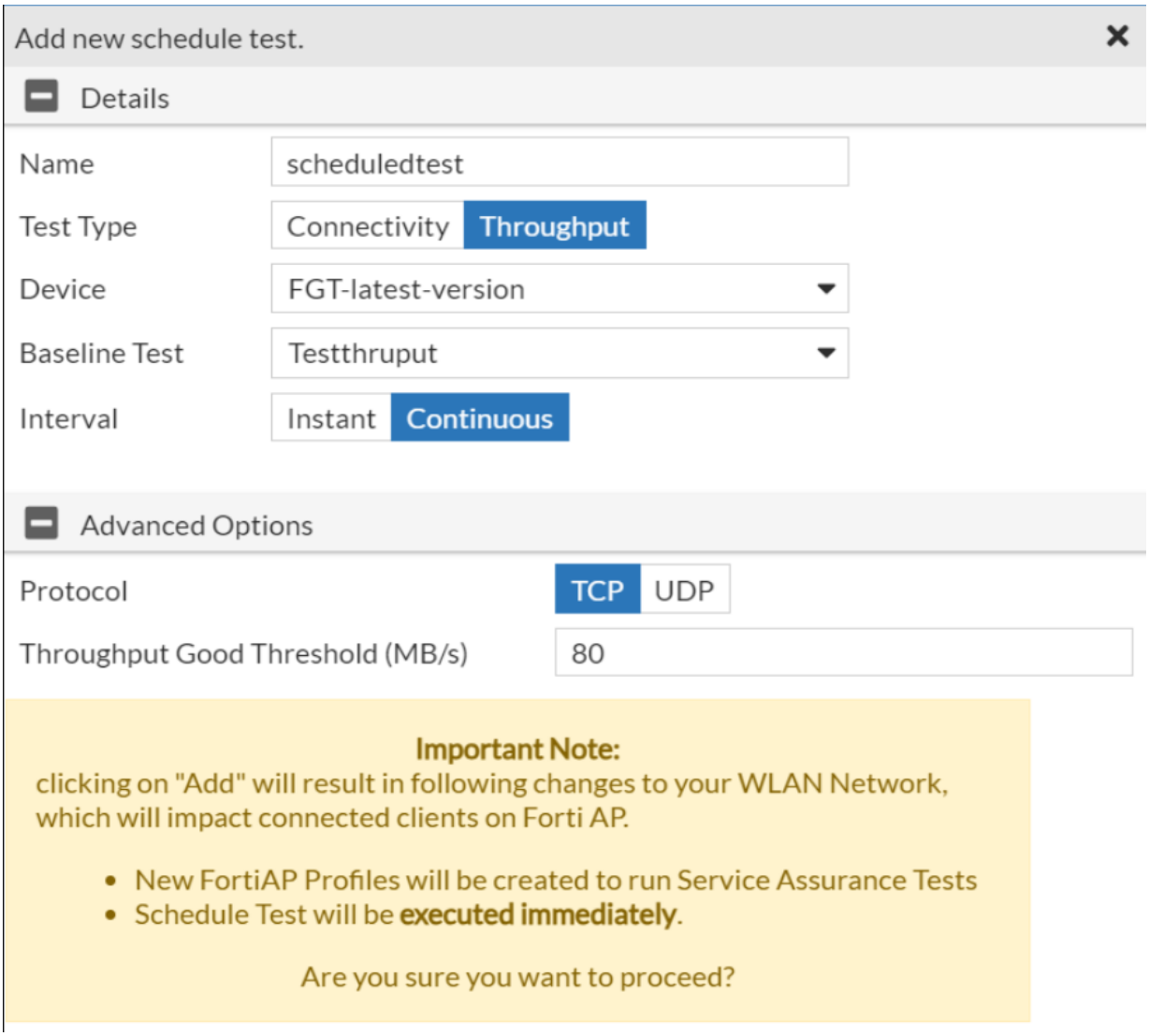
Field	Description
Packet Loss Good Threshold	Type a value for Packet Loss Good Threshold. If the measured packet loss is above this threshold and baseline, the test result is classified as *Bad*. If it falls between the threshold and the baseline, it is considered *Fair*, while values below the threshold and baseline are categorized as *Good*.





- If Throughput is selected as Test Type , you can configure the following fields:

Field	Description
Protocol	Select TCP or UDP.
Throughput Good Threshold (MB/s)	Type a value for the Throughput Good Threshold in MB/s. If the measured throughput is above this threshold, the test result is classified as *Good*. If it falls between the threshold and the baseline, it is considered *Fair*, while values below the threshold are categorized as *Bad*.



To delete a schedule, select a schedule from the list and click **Delete**.

To start a scheduled test, click start test icon under **Actions** field. To stop a running scheduled test, click stop test icon under **Actions** field.

Name	SSID	Test Type	Device Name	Baseline	Status	Interval	Action
Thput_UDP_2	sam_1	Throughput	[redacted]	Throughput_UDP_HA	Running	Continuous	
Thput_TCP_2	sam_1	Throughput	[redacted]	Thput_TCP_HA	Stopped	Continuous	

www.fortinet.com

Copyright© 2026 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 Chief Legal Officer, 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.