User Guide

FortiAIOps 2.1.0

Jan 20, 2026
FortiAIOps 2.1.0 User Guide
83-210-1017991-20260120

TABLE OF CONTENTS

Change log

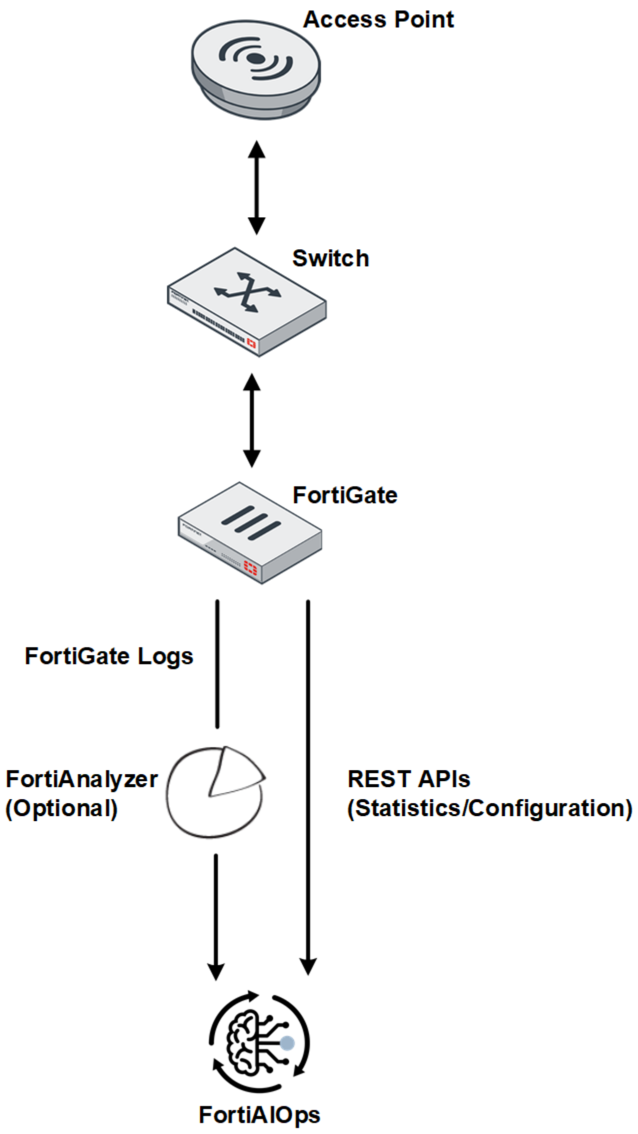
Date	Change description
2024-10-08	FortiAIOps 2.1.0 release document.
2025-02-07	Updated document to include FortiAIOps 500G hardware support.
2025-04-15	Updated Installing FortiAIOps on Proxmox section.
2025-05-21	Updated Pre-installation Requirements section.
2025-11-12	Editorial fix.
2026-01-20	Updated 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

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.

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

Performance

You can configure **Performance** SLAs to monitor member interface link quality and to detect link failures. The link quality is measured based on latency, jitter, and packet loss. FortiAIOps WAN SLA can follow the performance SLAs defined on FortiGate and report the SLA breaches.

FortiExtender

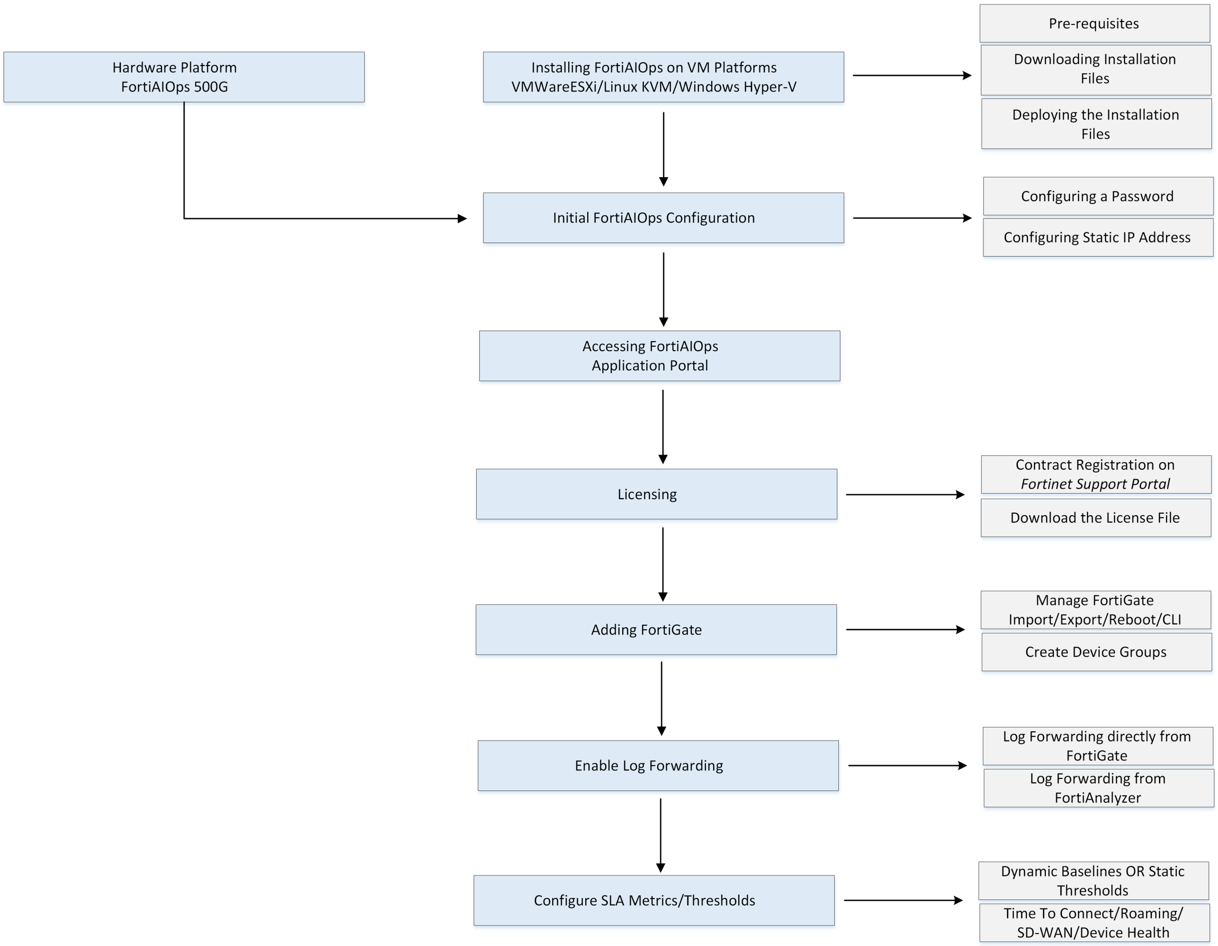
FortiExtender integrates with FortiGate and WAN to become a part of Fortinet's security fabric. This integration enables FortiGate’s WAN to have an extension using FortiExtender, providing continuous connectivity in case FortiGate's primary WAN link fails. Also, FortiExtender enables network access for remote sites and branches located beyond fixed broadband.

FortiExtender also facilitates load balancing for network traffic along with the primary WAN link. When FortiExtender is a part of your network, FortiAIOps monitors and reports related issues/failures.

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

Getting Started

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


Hardware Platform
FortiAIOps 500G
Installing FortiAIOps on VM Platforms
VMWareESXi/Linux KVM/Windows Hyper-V
Pre-requisites
Downloading Installation Files
Deploying the Installation Files
Initial FortiAIOps Configuration
Configuring a Password
Configuring Static IP Address
Accessing FortiAIOps Application Portal
Licensing
Contract Registration on *Fortinet Support Portal*
Download the License File
Adding FortiGate
Manage FortiGate Import/Export/Reboot/CLI
Create Device Groups
Enable Log Forwarding
Log Forwarding directly from FortiGate
Log Forwarding from FortiAnalyzer
Configure SLA Metrics/Thresholds
Dynamic Baselines OR Static Thresholds
Time To Connect/Roaming/ SD-WAN/Device Health

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
- Configure SLA Metrics
- 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.

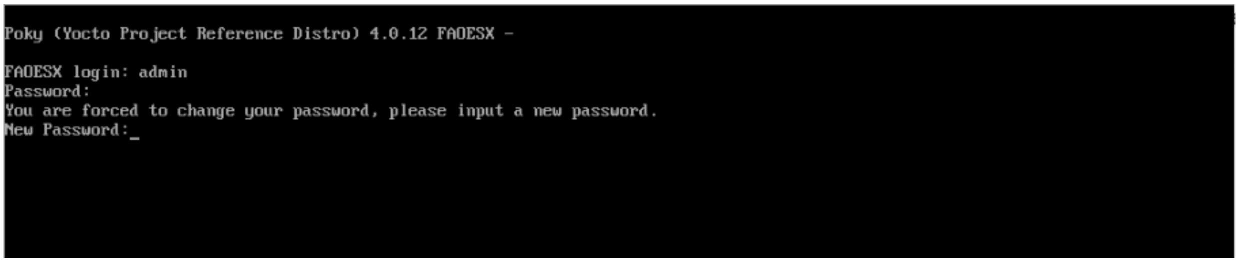
Initial FortiAIOps Configuration

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.



```
Poky (Yocto Project Reference Distro) 4.0.12 FAOESX -

FAOESX login: admin
Password:
You are forced to change your password, please input a new password.
New 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.

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

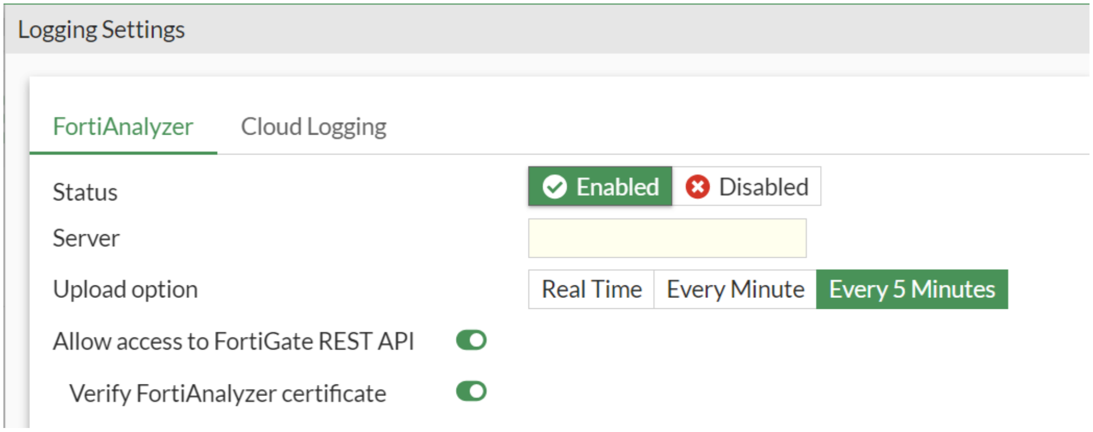
In the FortiAIOps application portal, manually add the FortiGate controller. Navigate to **Inventory > Managed FortiGates > Add** and provide the required configuration details. Standalone and HA FortiGate controllers can be added. Optionally, you can add FortiGates in bulk using the import operation.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

FortiAIOps supports direct FortiGate log forwarding and FortiAnalyzer log forwarding.

- Run the following command to configure syslog in FortiGate.
  - `config log syslogd setting`
  - `set status enable`
  - `set server 10.34.xxx.xxx`
- Direct FortiGate log forwarding - Navigate to **Fabric Connectors > Logging & Analytics > Log Settings** in the FortiGate GUI and specify the FortiAIOps IP address. Enable FortiAnalyzer log forwarding.



Logging Settings

FortiAnalyzer | Cloud Logging

Status: [✓ Enabled] Disabled

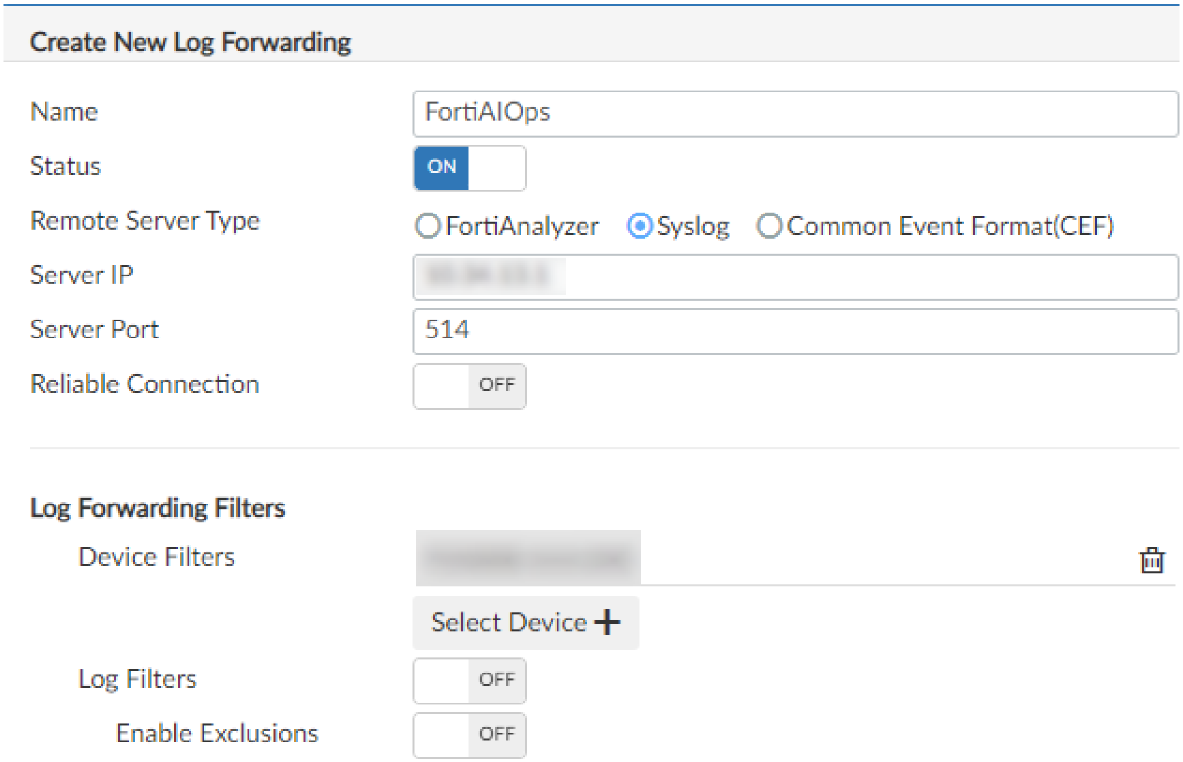
Server:

Upload option: Real Time | Every Minute | [✓ Every 5 Minutes]

Allow access to FortiGate REST API: ●

Verify FortiAnalyzer certificate: ●

- Navigate to **Log Forwarding** in the FortiAnalyzer GUI, specify the FortiAIOps IP address and select the FortiGate controller in **Device Filters**.



Create New Log Forwarding

Name	FortiAIOps
Status	ON
Remote Server Type	○ FortiAnalyzer ● Syslog ○ Common Event Format(CEF)
Server IP	[redacted]
Server Port	514
Reliable Connection	OFF

Log Forwarding Filters

Device Filters	[redacted]
	Select Device +
Log Filters	OFF
Enable Exclusions	OFF

Note: The syslog port is the default UDP port 514.

Monitoring

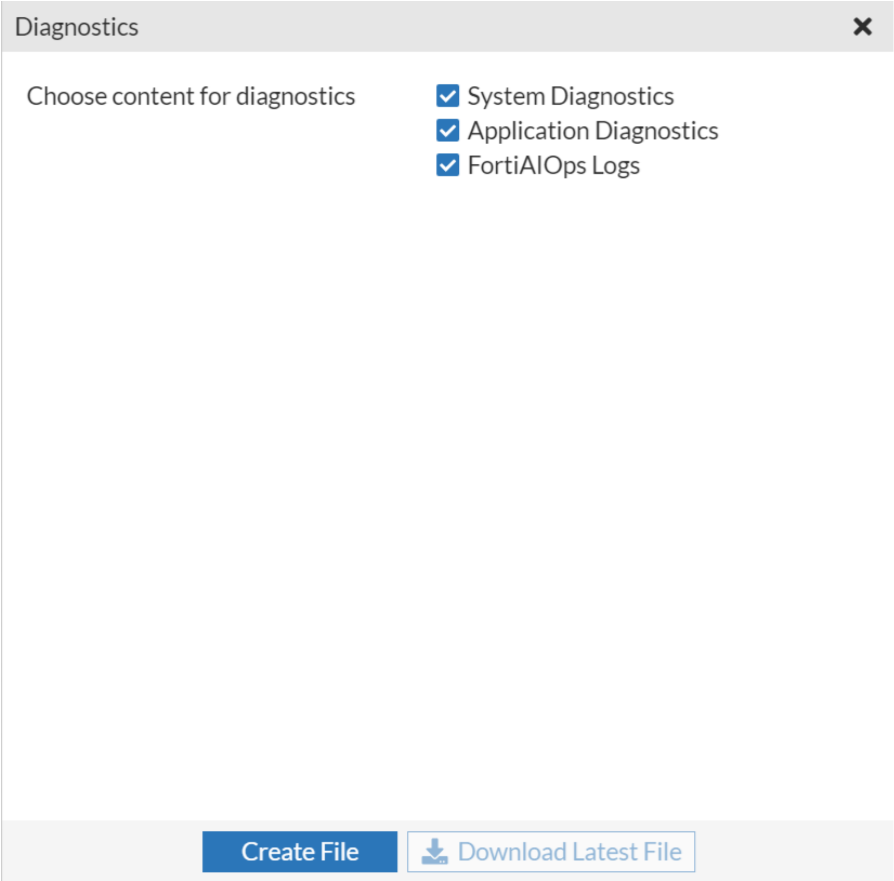
After the FortiAIOps setup and configurations are complete, you can view different aspects of your network in the following panels of the FortiAIOps application portal.

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.

GUI Panels	Description
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 provides detailed WiFi and FortiSwitch event logs, you can also generate detailed FortiAIOps reports.
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.
Service Assurance	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.



Diagnostics

Choose content for diagnostics

☑ System Diagnostics
☑ Application Diagnostics
☑ FortiAIOps Logs

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 35
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.

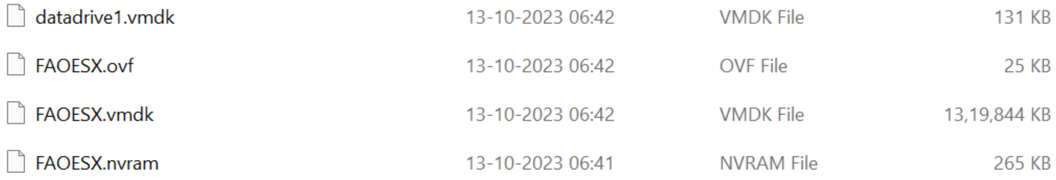
CPU	Memory	Storage	
		Disk 1	Disk 2
8	32 GB	8 GB	500 GB

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

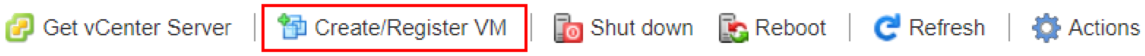
Perform the following steps to deploy FortiAIOps.

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.

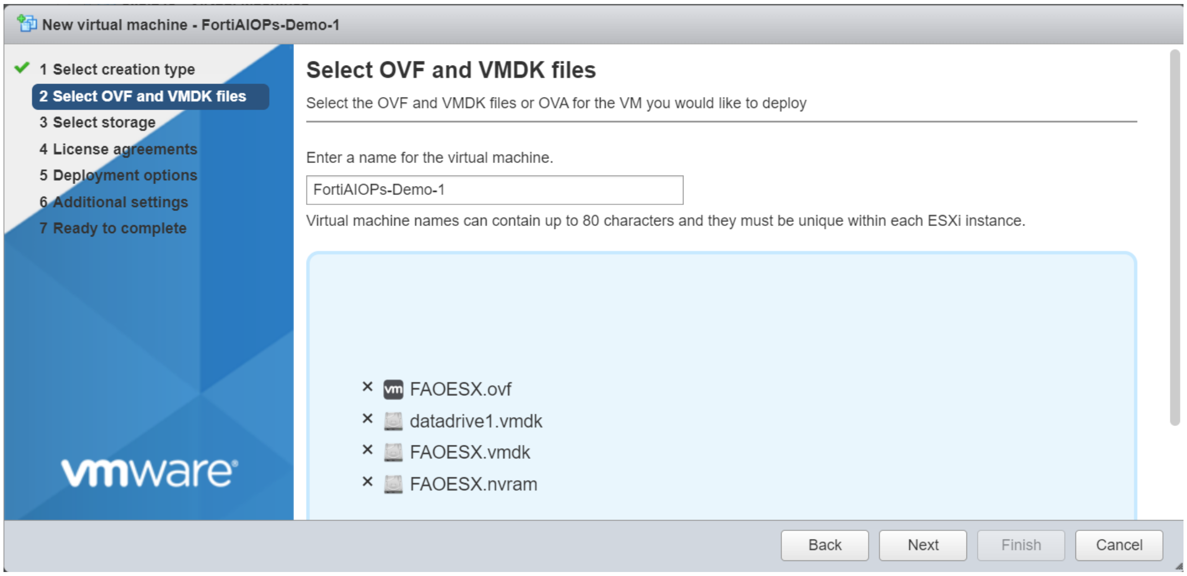


datadrive1.vmdk	13-10-2023 06:42	VMDK File	131 KB
FAOESX.ovf	13-10-2023 06:42	OVF File	25 KB
FAOESX.vmdk	13-10-2023 06:42	VMDK File	13,19,844 KB
FAOESX.nvram	13-10-2023 06:41	NVRAM File	265 KB

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.



Select OVF and VMDK files

Select the OVF and VMDK files or OVA for the VM you would like to deploy

Enter a name for the virtual machine.

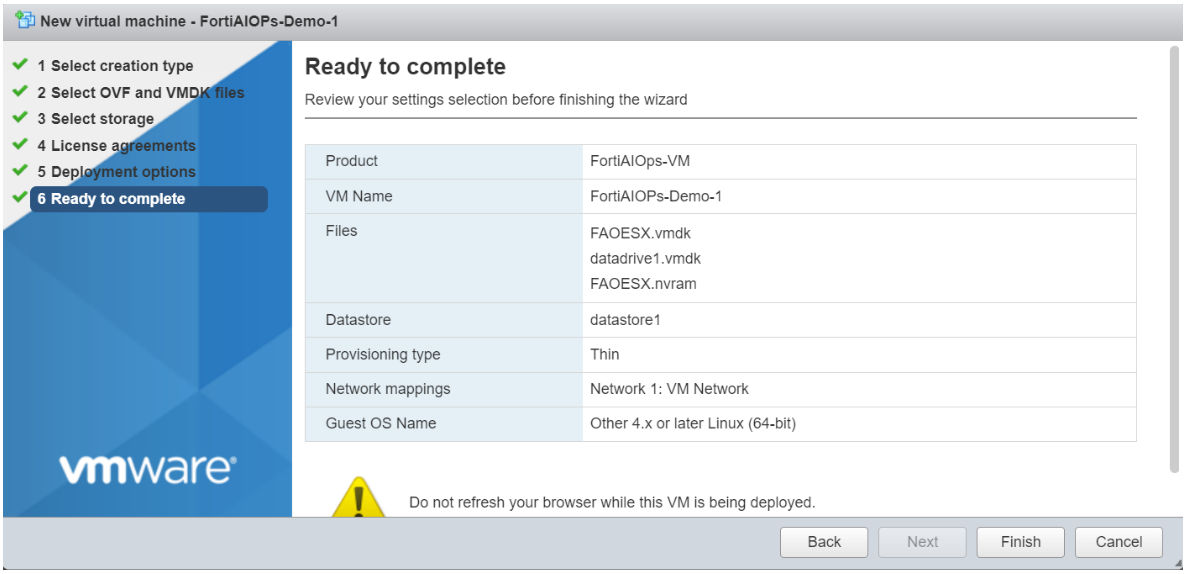
FortiAIOPs-Demo-1

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

× FAOESX.ovf
× datadrive1.vmdk
× FAOESX.vmdk
× FAOESX.nvram

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.**



Ready to complete

Review your settings selection before finishing the wizard

Product	FortiAIOps-VM
VM Name	FortiAIOPs-Demo-1
Files	FAOESX.vmdk datadrive1.vmdk FAOESX.nvram
Datastore	datastore1
Provisioning type	Thin
Network mappings	Network 1: VM Network
Guest OS Name	Other 4.x or later Linux (64-bit)

Do not refresh your browser while this VM is being deployed.

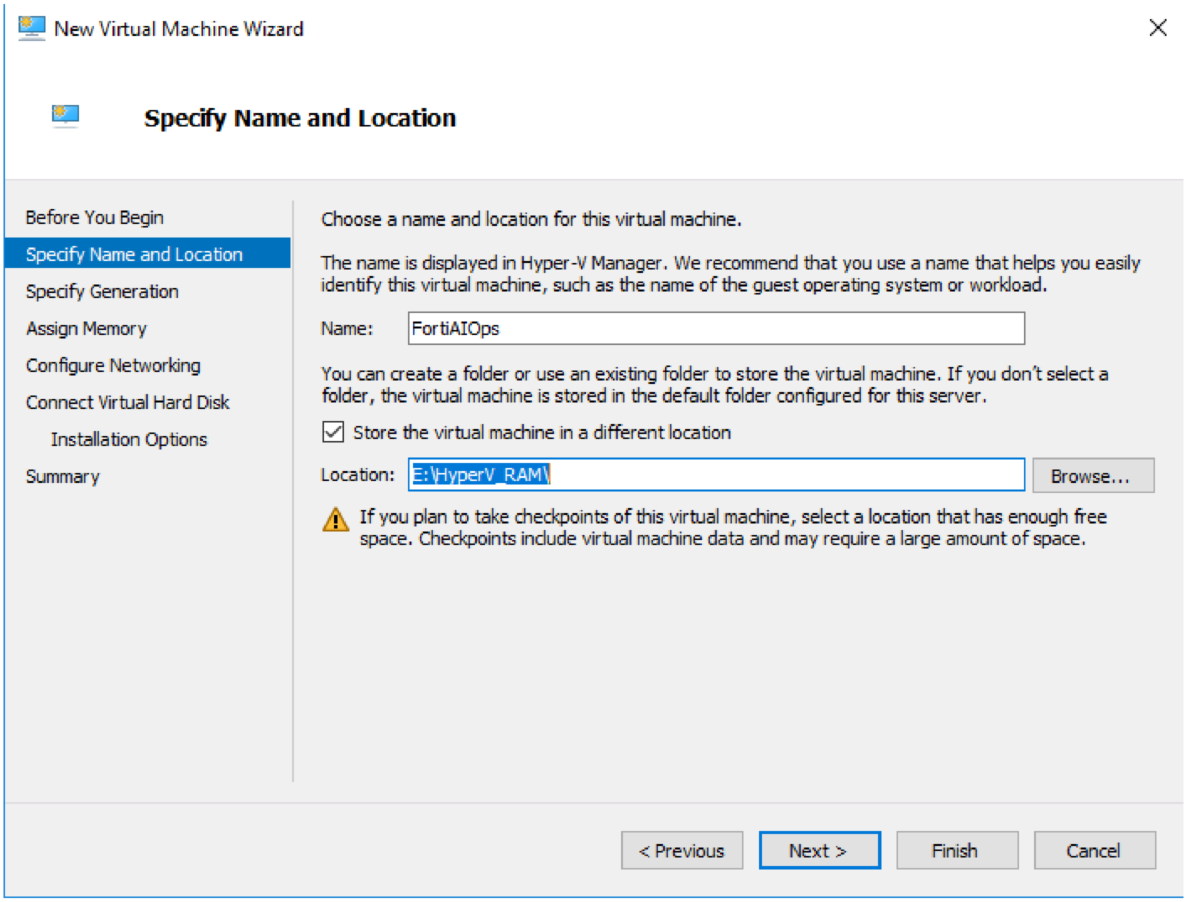
10. You can monitor the progress of the deployment in the **Recent Tasks** pane. When the installation is complete, the virtual machine will be listed in the **Inventory** pane.
11. Perform post-installation tasks.

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**.



New Virtual Machine Wizard

Specify Name and Location

Choose a name and location for this virtual machine.

The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name: FortiAIOps

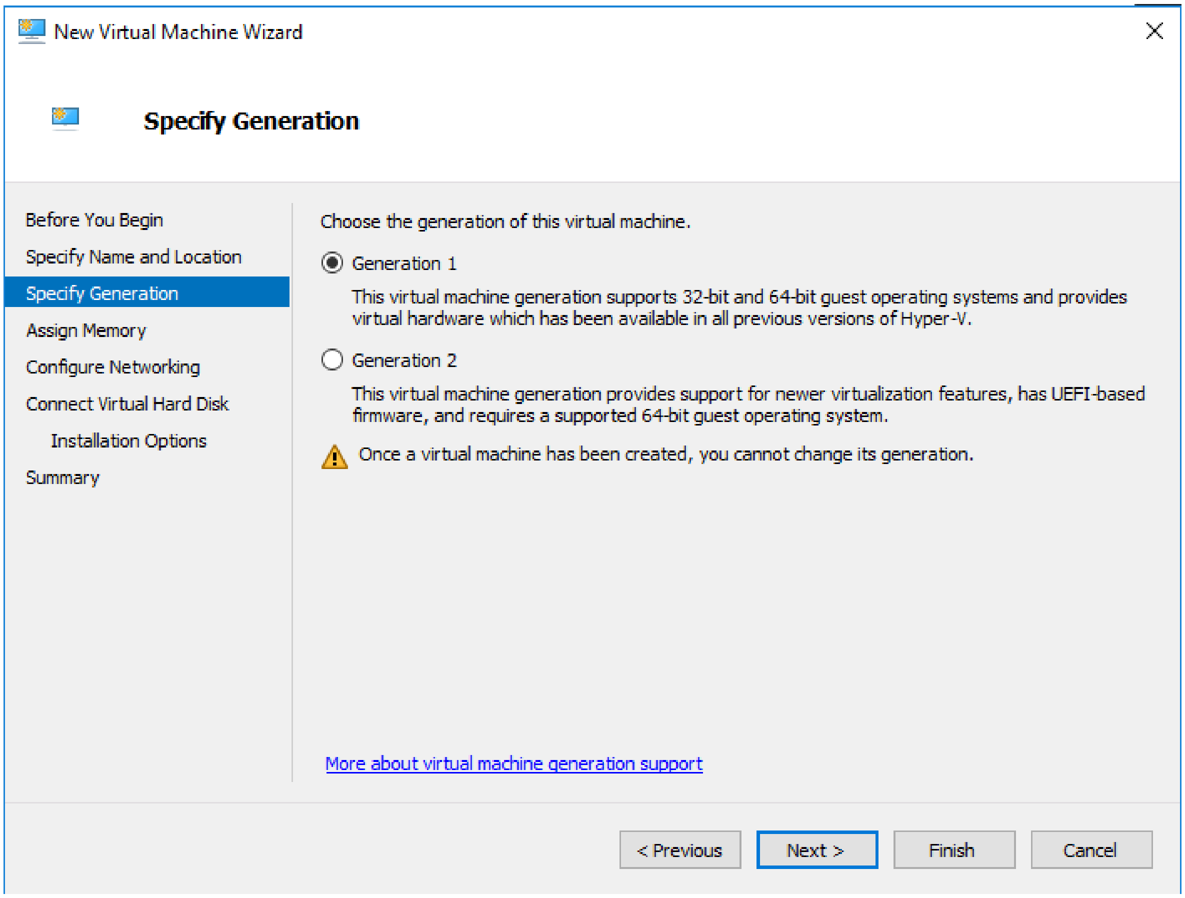
You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

☑ Store the virtual machine in a different location

Location: E:\HyperV_RAM\

If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

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



New Virtual Machine Wizard

Specify Generation

Choose the generation of this virtual machine.

● Generation 1

This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V.

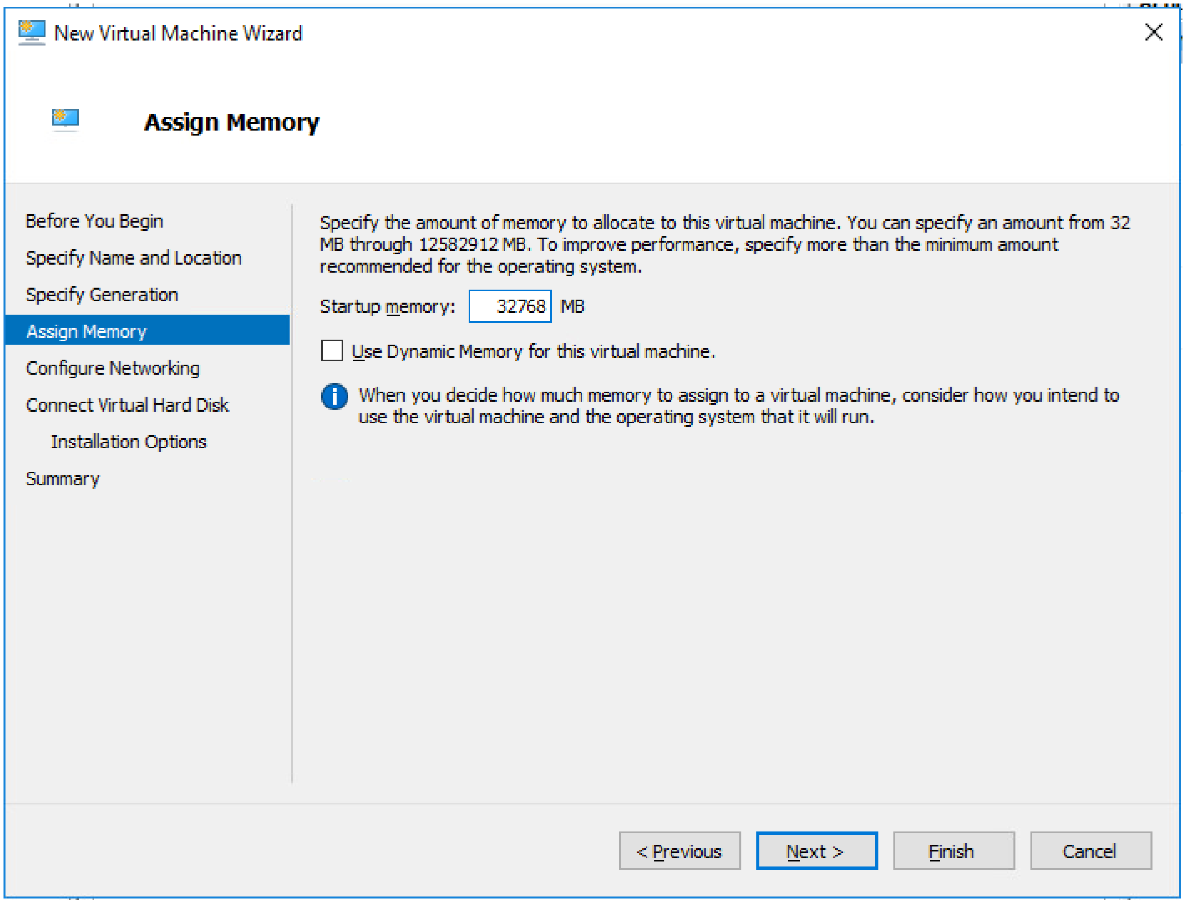
○ Generation 2

This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system.

⚠ Once a virtual machine has been created, you cannot change its generation.

More about virtual machine generation support

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



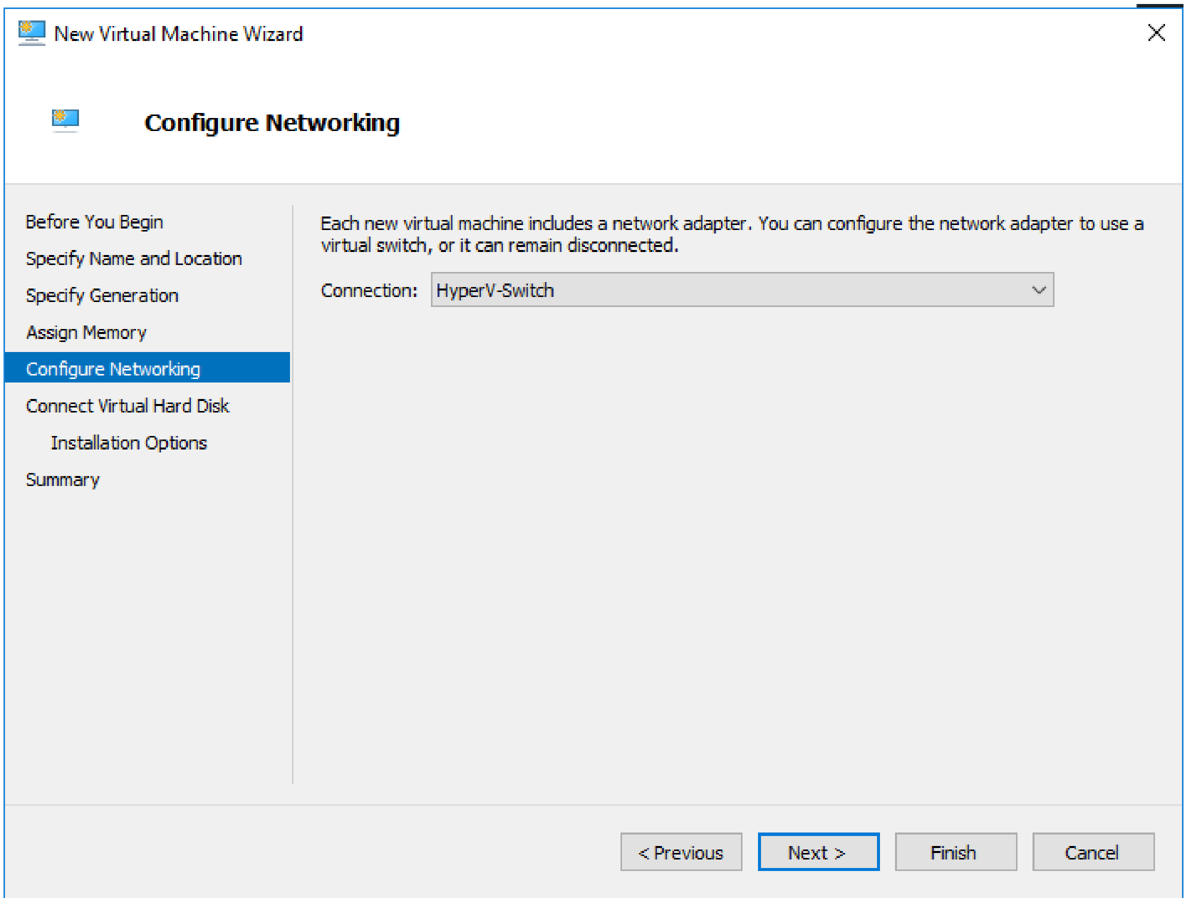
Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

Startup memory: 32768 MB

☐ Use Dynamic Memory for this virtual machine.

When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

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



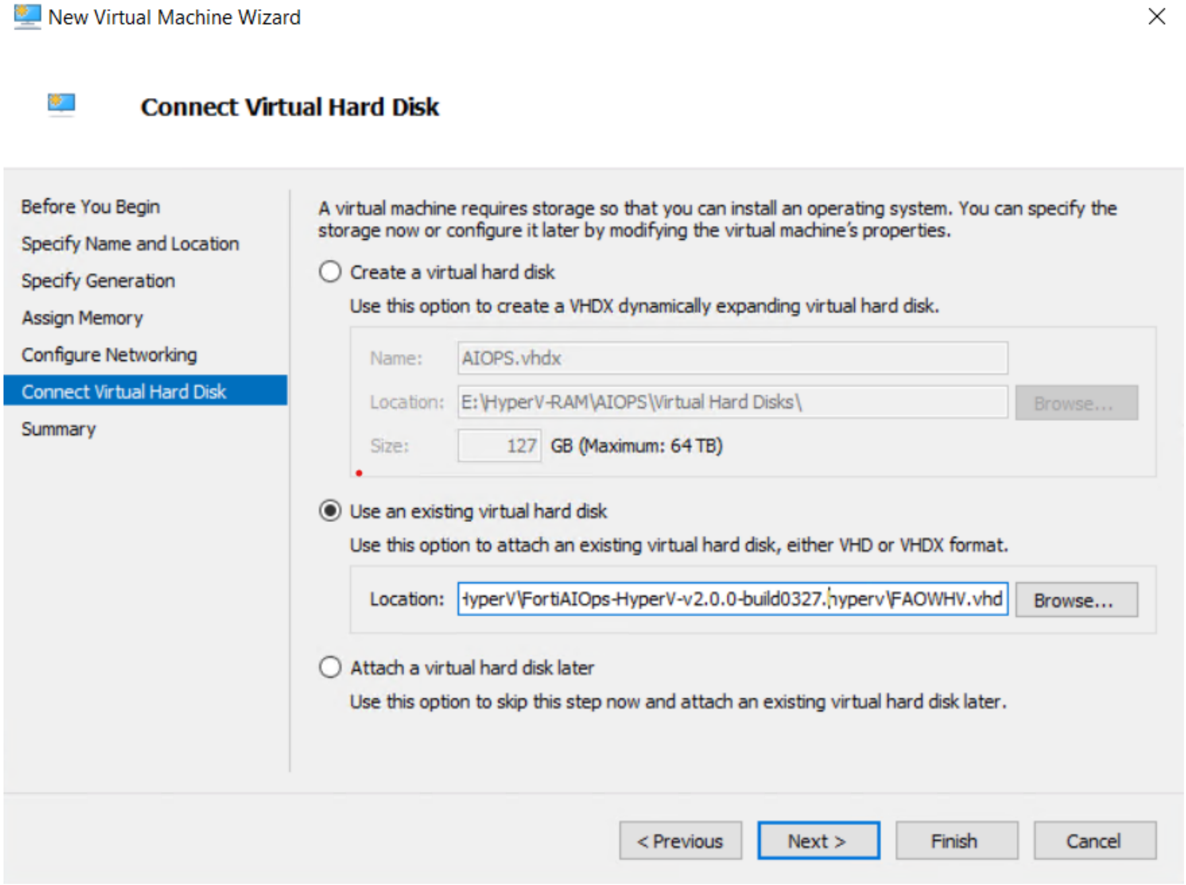
New Virtual Machine Wizard

Configure Networking

Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.

Connection: HyperV-Switch

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



A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

○ Create a virtual hard disk

Use this option to create a VHDX dynamically expanding virtual hard disk.

Name: AIOPS.vhdx

Location: E:\HyperV-RAM\AIOPS\Virtual Hard Disks\

Size: 127 GB (Maximum: 64 TB)

● Use an existing virtual hard disk

Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

Location: HyperV\FortiAIOps-HyperV-v2.0.0-build0327.hyperv\FAOWHV.vhd

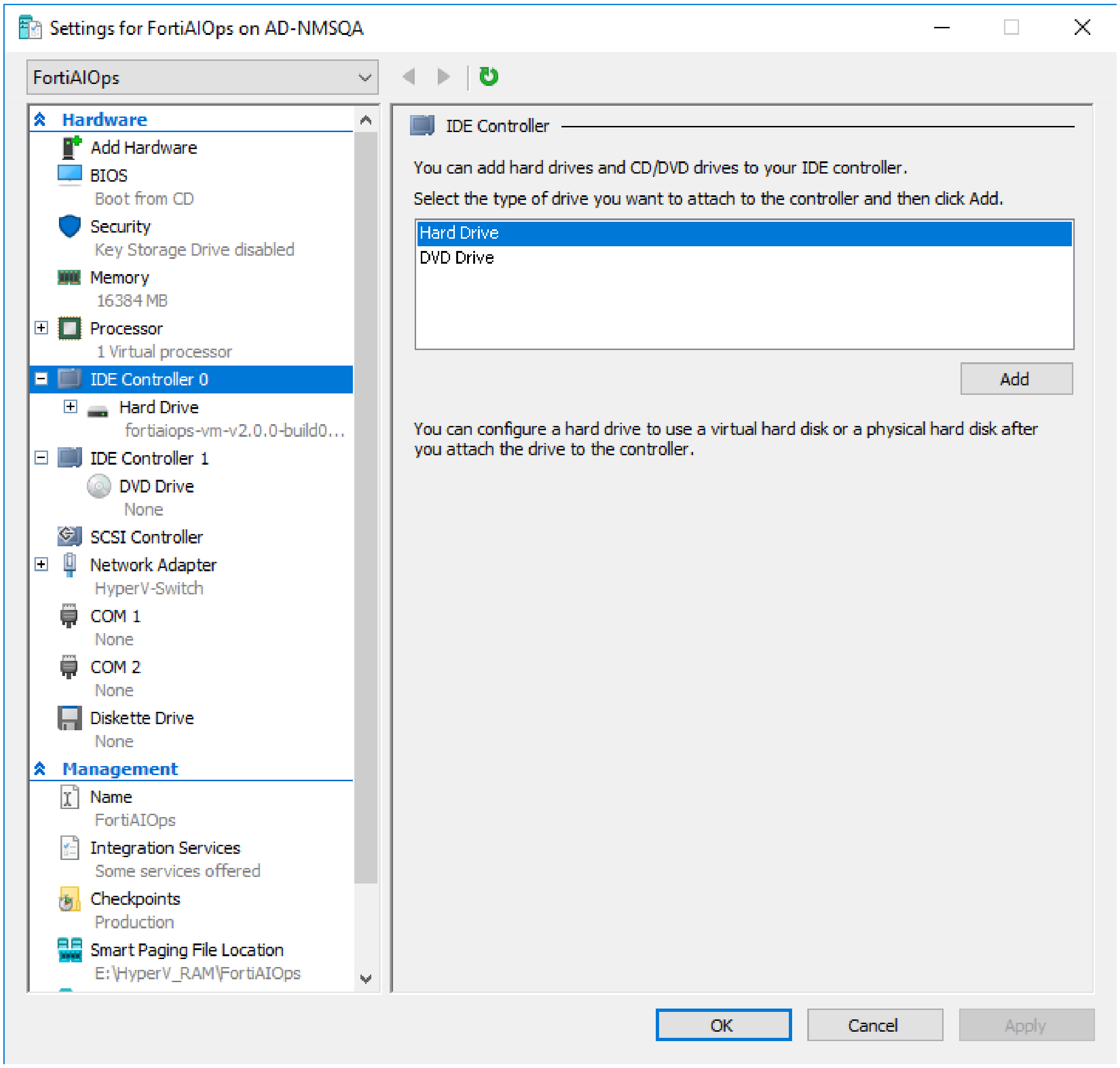
○ Attach a virtual hard disk later

Use this option to skip this step now and attach an existing virtual hard disk later.

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**.



Settings for FortiAIOps on AD-NMSQA

FortiAIOps

Hardware
- Add Hardware
- BIOS — Boot from CD
- Security — Key Storage Drive disabled
- Memory — 16384 MB
- Processor — 1 Virtual processor
- IDE Controller 0
  - Hard Drive — fortiaiops-vm-v2.0.0-build0...
- IDE Controller 1
  - DVD Drive — None
- SCSI Controller
- Network Adapter — HyperV-Switch
- COM 1 — None
- COM 2 — None
- Diskette Drive — None

Management
- Name — FortiAIOps
- Integration Services — Some services offered
- Checkpoints — Production
- Smart Paging File Location — E:\HyperV_RAM\FortiAIOps

IDE Controller

You can add hard drives and CD/DVD drives to your IDE controller.

Select the type of drive you want to attach to the controller and then click Add.

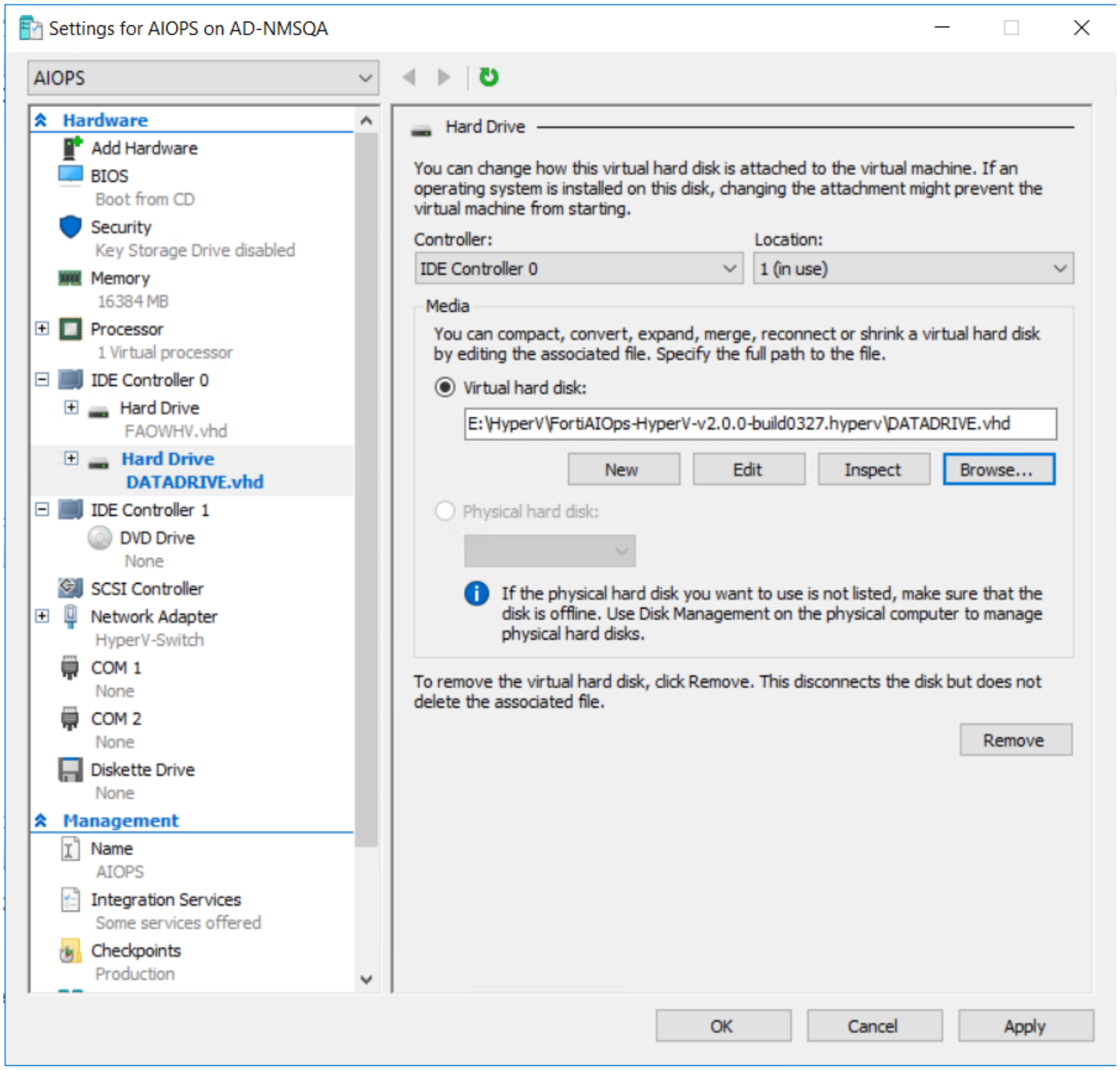
- Hard Drive
- DVD Drive

Add

You can configure a hard drive to use a virtual hard disk or a physical hard disk after you attach the drive to the controller.

OK | Cancel | Apply

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



Settings for AIOPS on AD-NMSQA

AIOPS

Hard Drive

You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting.

Controller: IDE Controller 0

Location: 1 (in use)

Media

You can compact, convert, expand, merge, reconnect or shrink a virtual hard disk by editing the associated file. Specify the full path to the file.

● Virtual hard disk:

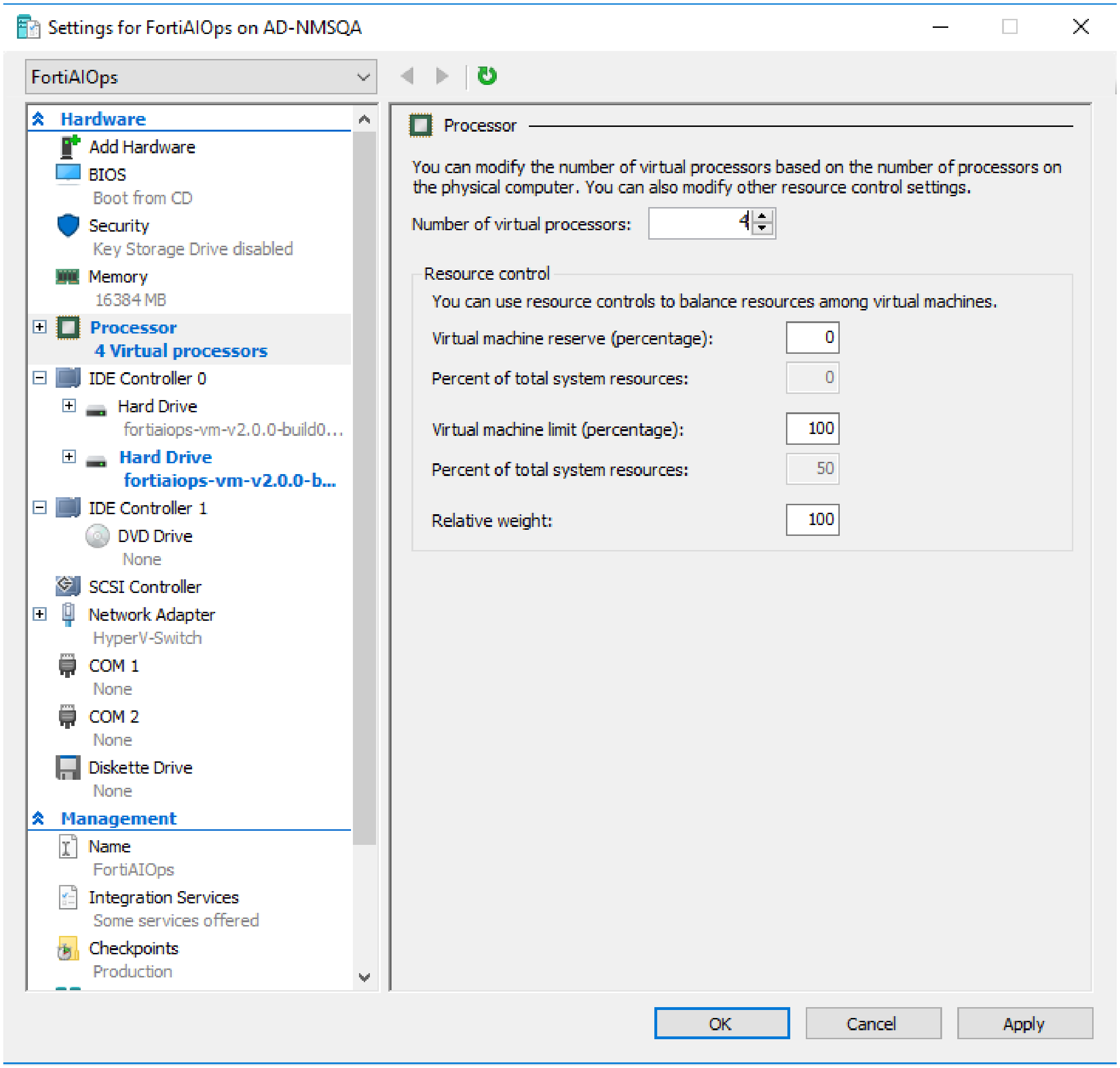
E:\HyperV\FortiAIOps-HyperV-v2.0.0-build0327.hyperv\DATADRIVE.vhd

○ Physical hard disk:

If the physical hard disk you want to use is not listed, make sure that the disk is offline. Use Disk Management on the physical computer to manage physical hard disks.

To remove the virtual hard disk, click Remove. This disconnects the disk but does not delete the associated file.

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



Settings for FortiAIOps on AD-NMSQA

FortiAIOps

Hardware
- Add Hardware
- BIOS
  Boot from CD
- Security
  Key Storage Drive disabled
- Memory
  16384 MB
- **Processor**
  4 Virtual processors
- IDE Controller 0
  - Hard Drive
    fortiaiops-vm-v2.0.0-build0...
  - **Hard Drive**
    fortiaiops-vm-v2.0.0-b...
- IDE Controller 1
  - DVD Drive
    None
- SCSI Controller
- Network Adapter
  HyperV-Switch
- COM 1
  None
- COM 2
  None
- Diskette Drive
  None

Management
- Name
  FortiAIOps
- Integration Services
  Some services offered
- Checkpoints
  Production

Processor

You can modify the number of virtual processors based on the number of processors on the physical computer. You can also modify other resource control settings.

Number of virtual processors: 4

Resource control

You can use resource controls to balance resources among virtual machines.

Virtual machine reserve (percentage):	0
Percent of total system resources:	0
Virtual machine limit (percentage):	100
Percent of total system resources:	50
Relative weight:	100

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.

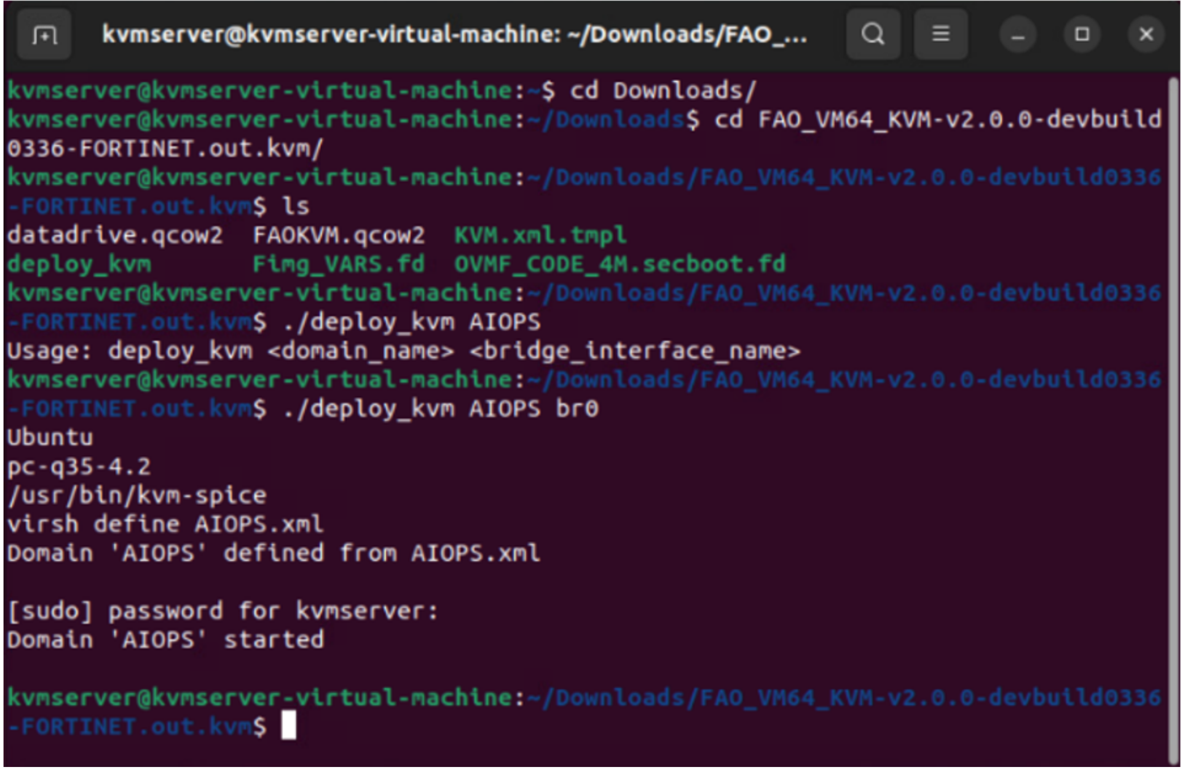
Installing FortiAIOps on KVM

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*.

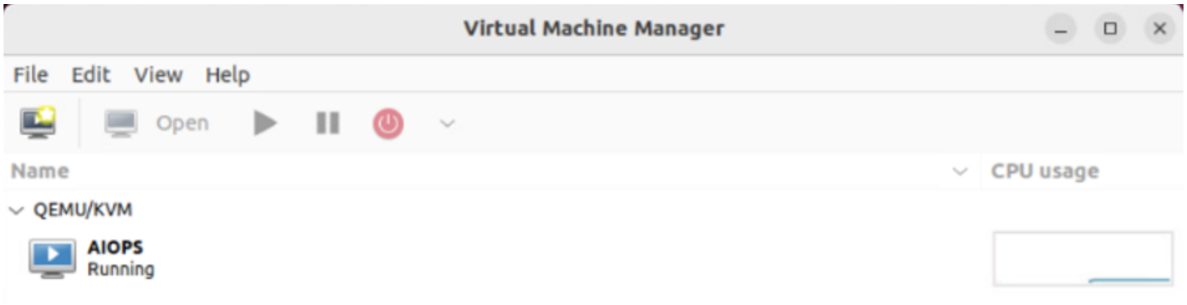
2. Open terminal and navigate to the path of the downloaded and unzipped installation files.

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

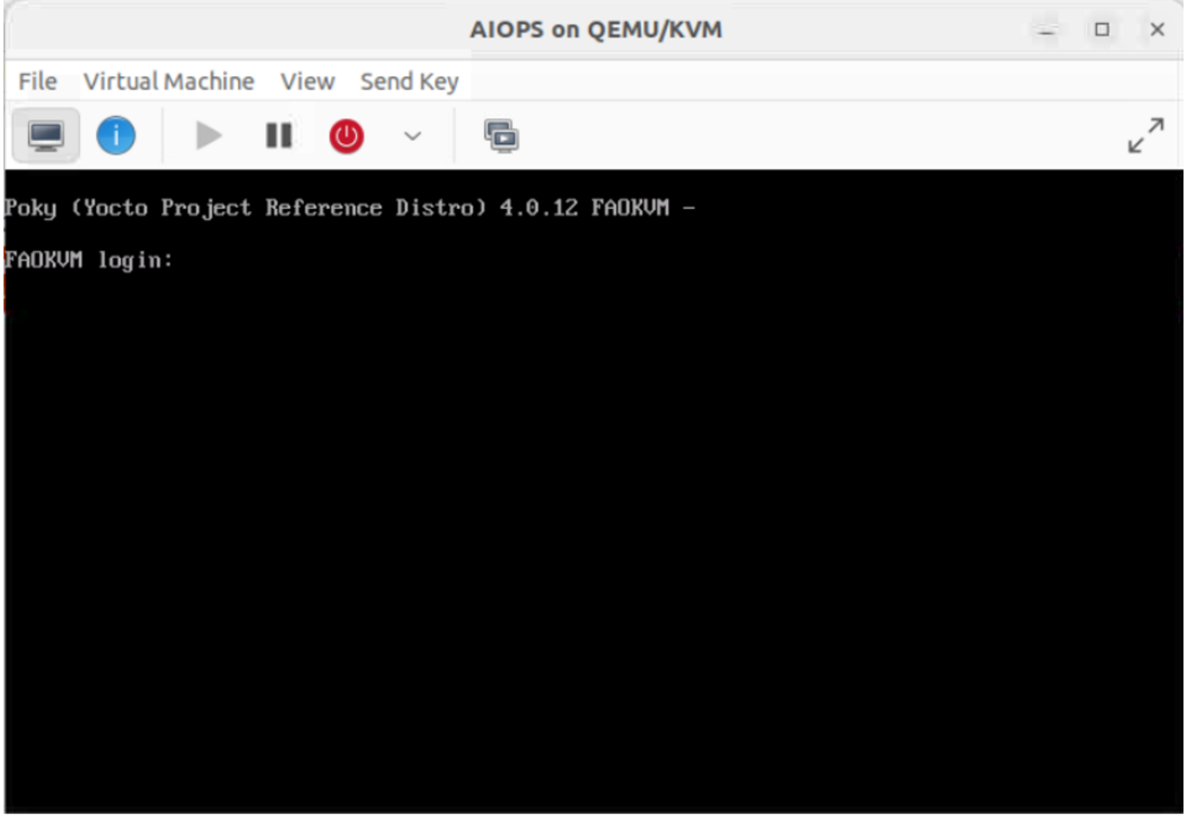


```
kvmserver@kvmserver-virtual-machine:~$ cd Downloads/
kvmserver@kvmserver-virtual-machine:~/Downloads$ cd FAO_VM64_KVM-v2.0.0-devbuild
0336-FORTINET.out.kvm/
kvmserver@kvmserver-virtual-machine:~/Downloads/FAO_VM64_KVM-v2.0.0-devbuild0336
-FORTINET.out.kvm$ ls
datadrive.qcow2  FAOKVM.qcow2  KVM.xml.tmpl
deploy_kvm       Fimg_VARS.fd  OVMF_CODE_4M.secboot.fd
kvmserver@kvmserver-virtual-machine:~/Downloads/FAO_VM64_KVM-v2.0.0-devbuild0336
-FORTINET.out.kvm$ ./deploy_kvm AIOPS
Usage: deploy_kvm <domain_name> <bridge_interface_name>
kvmserver@kvmserver-virtual-machine:~/Downloads/FAO_VM64_KVM-v2.0.0-devbuild0336
-FORTINET.out.kvm$ ./deploy_kvm AIOPS br0
Ubuntu
pc-q35-4.2
/usr/bin/kvm-spice
virsh define AIOPS.xml
Domain 'AIOPS' defined from AIOPS.xml

[sudo] password for kvmserver:
Domain 'AIOPS' started

kvmserver@kvmserver-virtual-machine:~/Downloads/FAO_VM64_KVM-v2.0.0-devbuild0336
-FORTINET.out.kvm$ 
```

4. Open the virt-manager window.



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



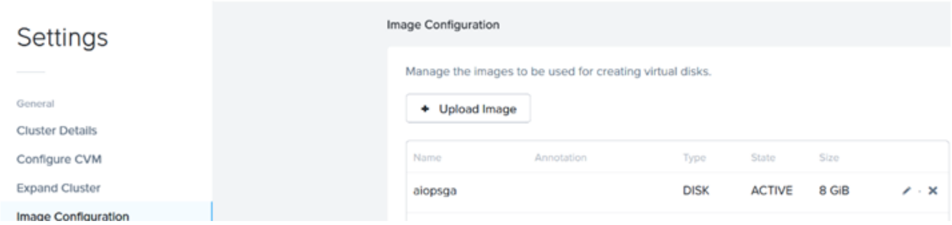
```
Poky (Yocto Project Reference Distro) 4.0.12 FAOKVM -

FAOKVM login:
```

6. Perform post-installation tasks.

Installing FortiAIOps on Nutanix

Perform the following steps to deploy FortiAIOps on Nutanix.

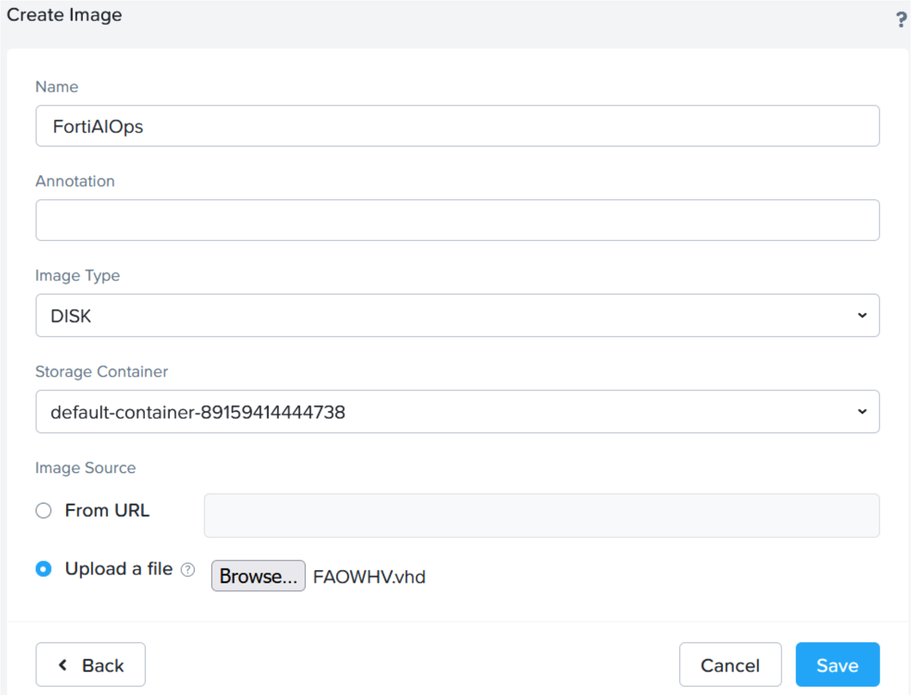
1. Obtain *FAO_VM64_HV-v2.0.1-[build0xxx]-FORTINET.out.hyperv.zip* from Fortinet and extract it to obtain the files *FAOWHV.vhd* and *DATADRIVE.vhd*.
2. Log in into the Nutanix Prism user interface and click the icon. Select **Image Configuration**.



Manage the images to be used for creating virtual disks.

Name	Annotation	Type	State	Size
aiopsga		DISK	ACTIVE	8 GiB

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.



Create Image

Name: FortiAIOps

Annotation:

Image Type: DISK

Storage Container: default-container-89159414444738

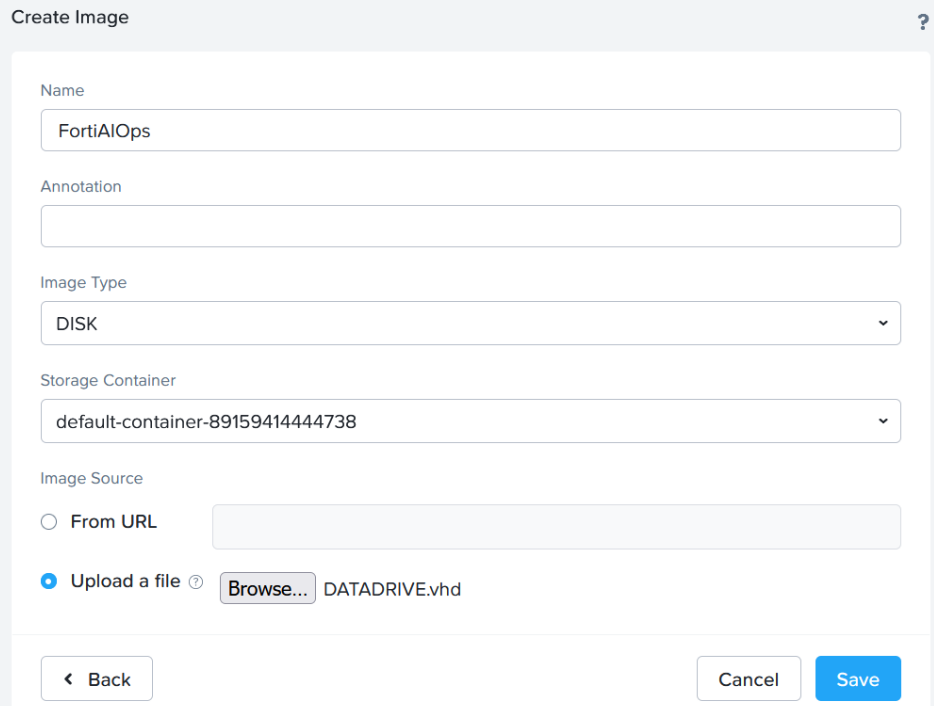
Image Source

○ From URL

● Upload a file FAOWHV.vhd

- 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*.



Create Image

Name: FortiAIOps

Annotation:

Image Type: DISK

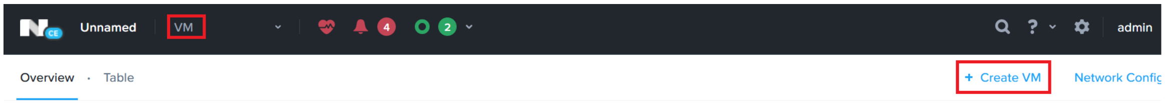
Storage Container: default-container-89159414444738

Image Source

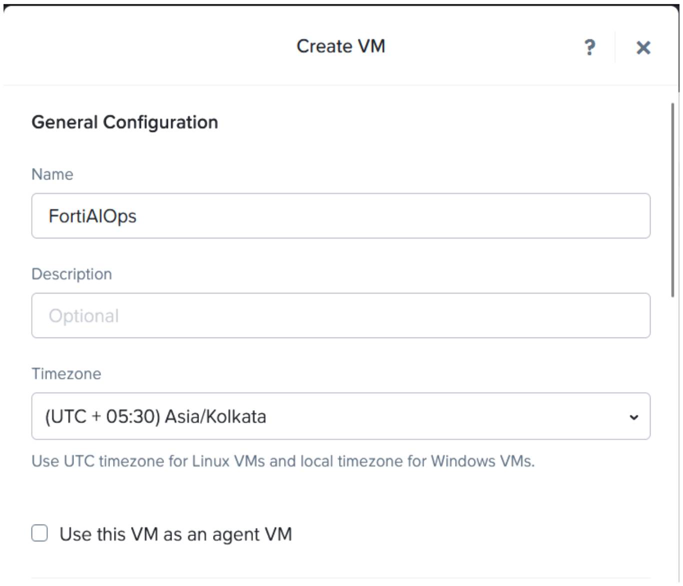
○ From URL

● Upload a file 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**.



General Configuration

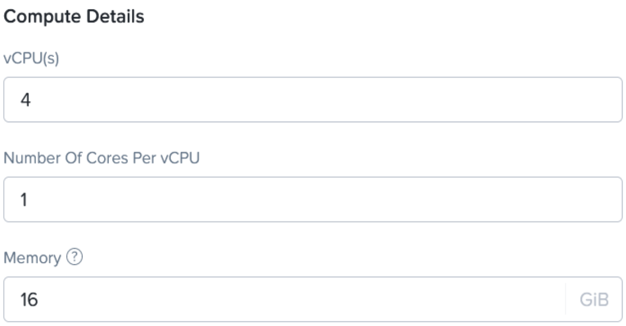
Name: FortiAIOps

Description: Optional

Timezone: (UTC + 05:30) Asia/Kolkata

Use UTC timezone for Linux VMs and local timezone for Windows VMs.

☐ Use this VM as an agent VM



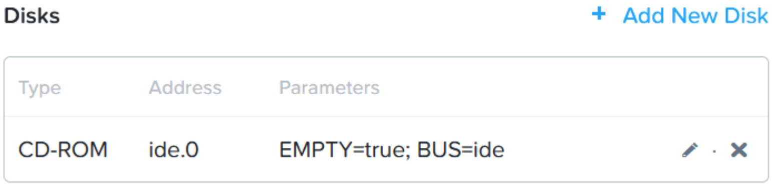
Compute Details

vCPU(s): 4

Number Of Cores Per vCPU: 1

Memory: 16 GiB

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

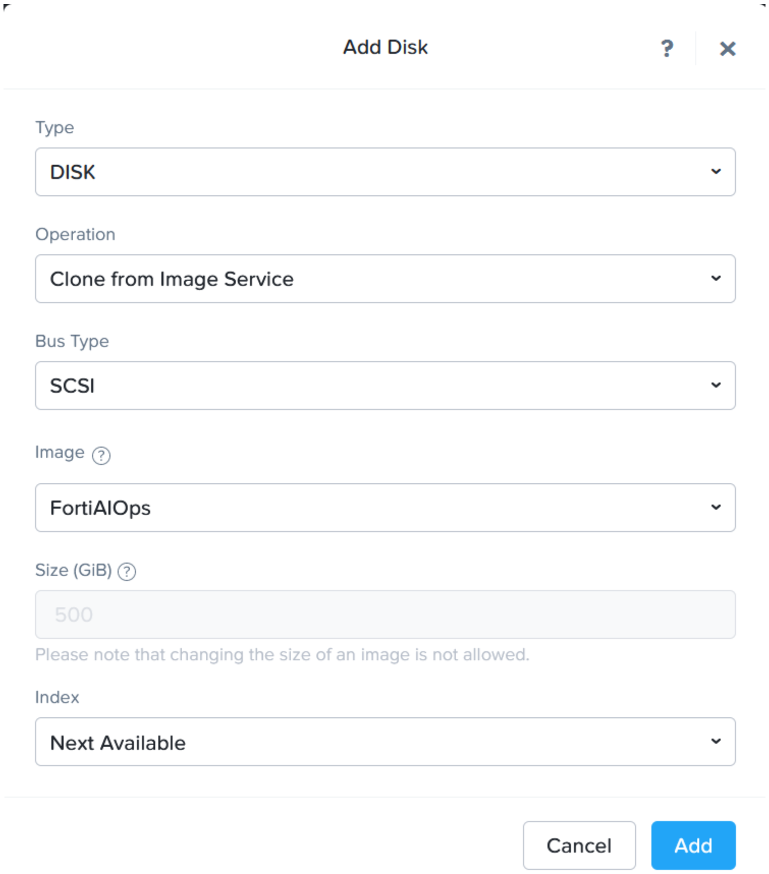


Disks

Type	Address	Parameters
CD-ROM	ide.0	EMPTY=true; BUS=ide

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*.



Add Disk

Type: DISK

Operation: Clone from Image Service

Bus Type: SCSI

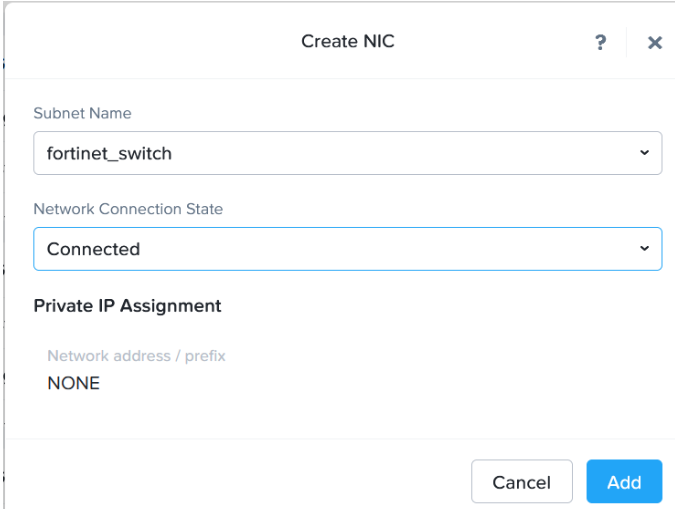
Image: FortiAIOps

Size (GiB): 500

Please note that changing the size of an image is not allowed.

Index: Next Available

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**.



Create NIC

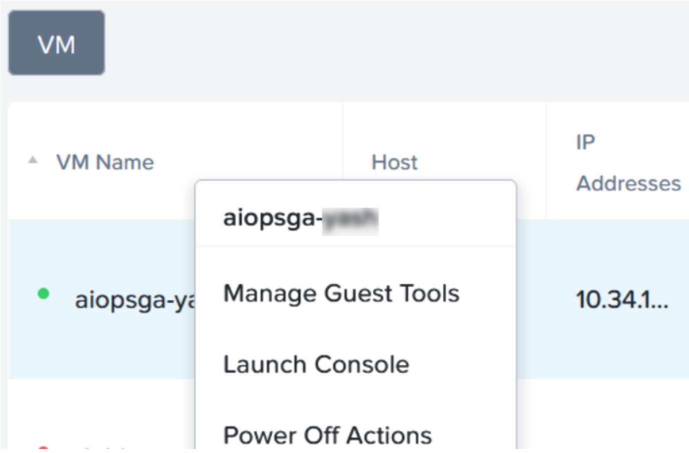
Subnet Name: fortinet_switch

Network Connection State: Connected

Private IP Assignment

Network address / prefix: NONE

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
```

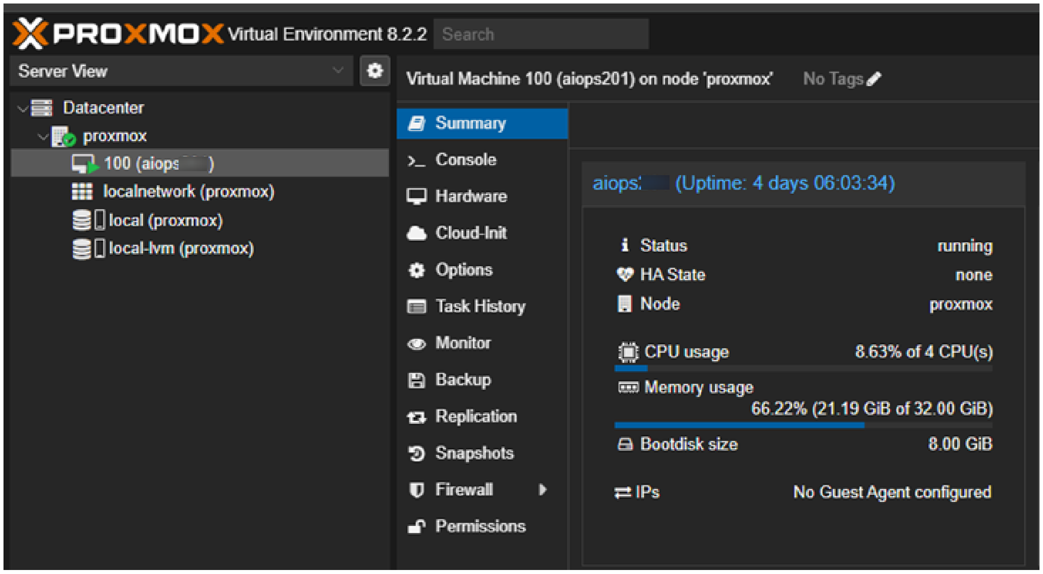
3. Import the FortiAIOps disk image manually in the Proxmox shell to create the VM.

```
./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.



PROXMOX Virtual Environment 8.2.2 Search

Server View

- Datacenter
  - proxmox
    - 100 (aiops[redacted])
    - localnetwork (proxmox)
    - local (proxmox)
    - local-lvm (proxmox)

Virtual Machine 100 (aiops201) on node 'proxmox' No Tags

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

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

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

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. The default login credentials (username/password) for the GUI are admin/admin. Configuring the CLI password does not modify the 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.

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/password is admin/admin; 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

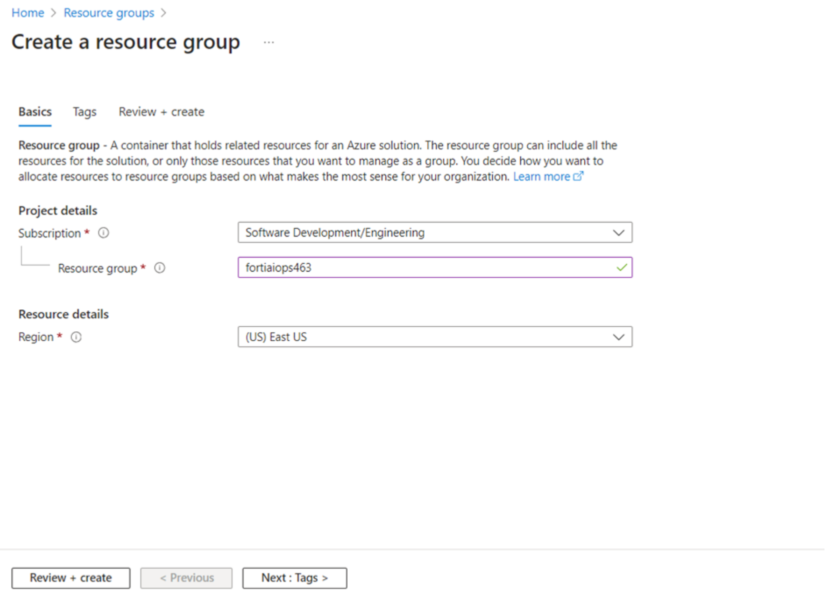
FortiAIOps can now be deployed on the following public Cloud platforms.

- 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.



Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. Learn more

Project details

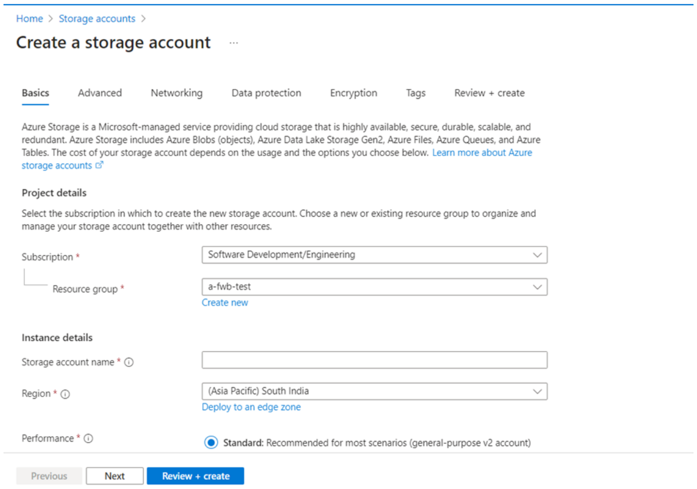
Subscription *: Software Development/Engineering

Resource group *: fortiaiops463

Resource details

Region *: (US) East US

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



Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. Learn more about Azure storage accounts

Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription * : Software Development/Engineering

Resource group * : a-fwb-test
Create new

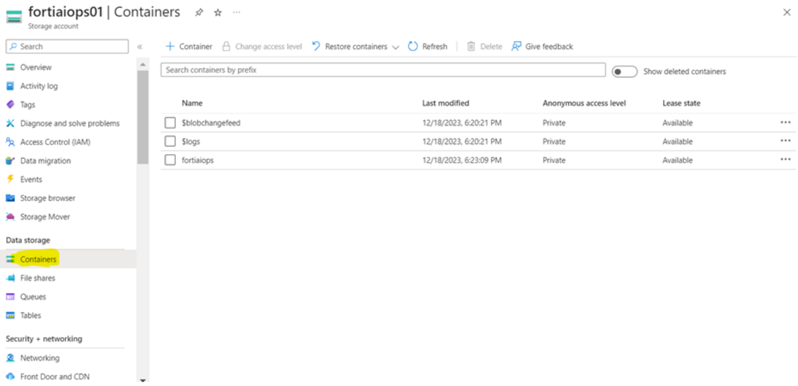
Instance details

Storage account name * :

Region * : (Asia Pacific) South India
Deploy to an edge zone

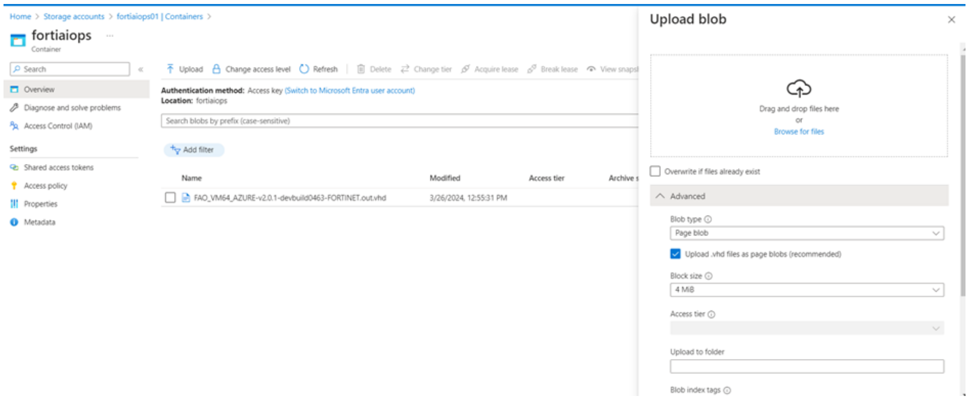
Performance * : ● Standard: Recommended for most scenarios (general-purpose v2 account)

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



Name	Last modified	Anonymous access level	Lease state
$blobchangefeed	12/18/2023, 6:20:21 PM	Private	Available
$logs	12/18/2023, 6:20:21 PM	Private	Available
fortiaiops	12/18/2023, 6:23:09 PM	Private	Available

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



Authentication method: Access key (Switch to Microsoft Entra user account)
Location: fortiaiops

Name	Modified	Access tier	Archive s
FAO_VM64_AZURE-v2.0.1-devbuild0463-FORTINET.out.vhd	3/26/2024, 12:55:31 PM		

□ Overwrite if files already exist

Blob type: Page blob

☑ Upload .vhd files as page blobs (recommended)

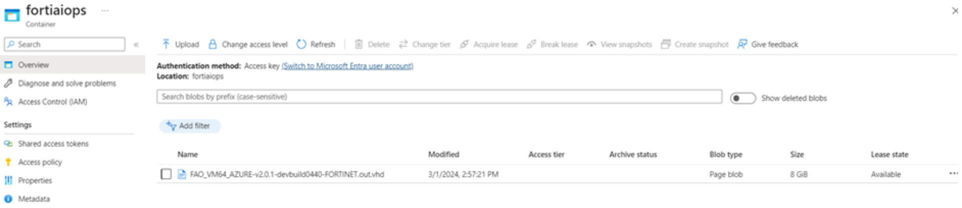
Block size: 4 MiB

Access tier:

Upload to folder:

Blob index tags

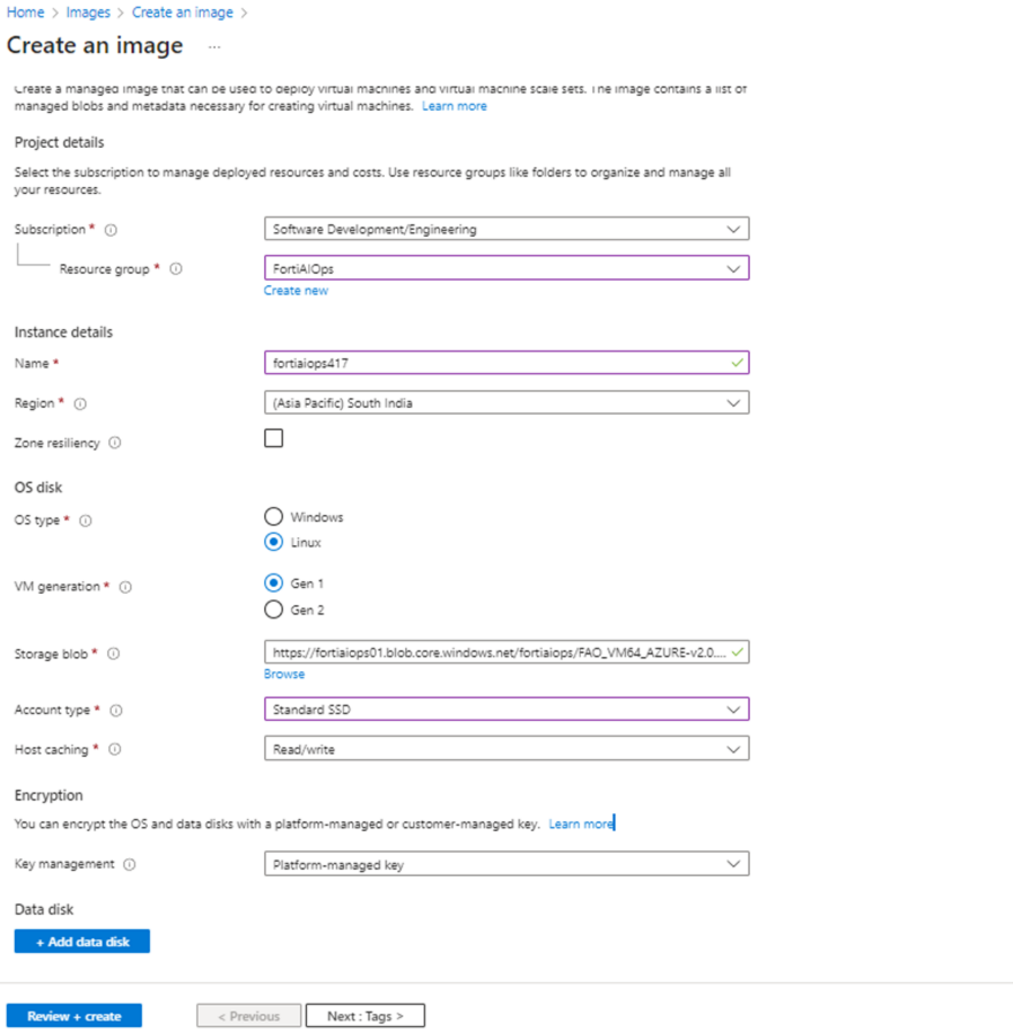
- After the upload, verify that the file is listed in the **Containers** page.



Authentication method: Access key (Switch to Microsoft Entra user account)
Location: fortiaiops

Name	Modified	Access tier	Archive status	Blob type	Size	Lease state
FAO_VM64_AZURE-v2.0.1-devbuild0440-FORTINET.out.vhd	3/1/2024, 2:57:21 PM			Page blob	8 GiB	Available

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**.



Create an image ···

Create a managed image that can be used to deploy virtual machines and virtual machine scale sets. The image contains a list of managed blobs and metadata necessary for creating virtual machines. Learn more

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ	Software Development/Engineering
Resource group * ⓘ	FortiAIOps Create new

Instance details

Name *	fortiaiops417 ✓
Region * ⓘ	(Asia Pacific) South India
Zone resiliency ⓘ	□

OS disk

OS type * ⓘ	○ Windows ● Linux
VM generation * ⓘ	● Gen 1 ○ Gen 2
Storage blob * ⓘ	https://fortiaiops01.blob.core.windows.net/fortiaiops/FAO_VM64_AZURE-v2.0.... ✓ Browse
Account type * ⓘ	Standard SSD
Host caching * ⓘ	Read/write

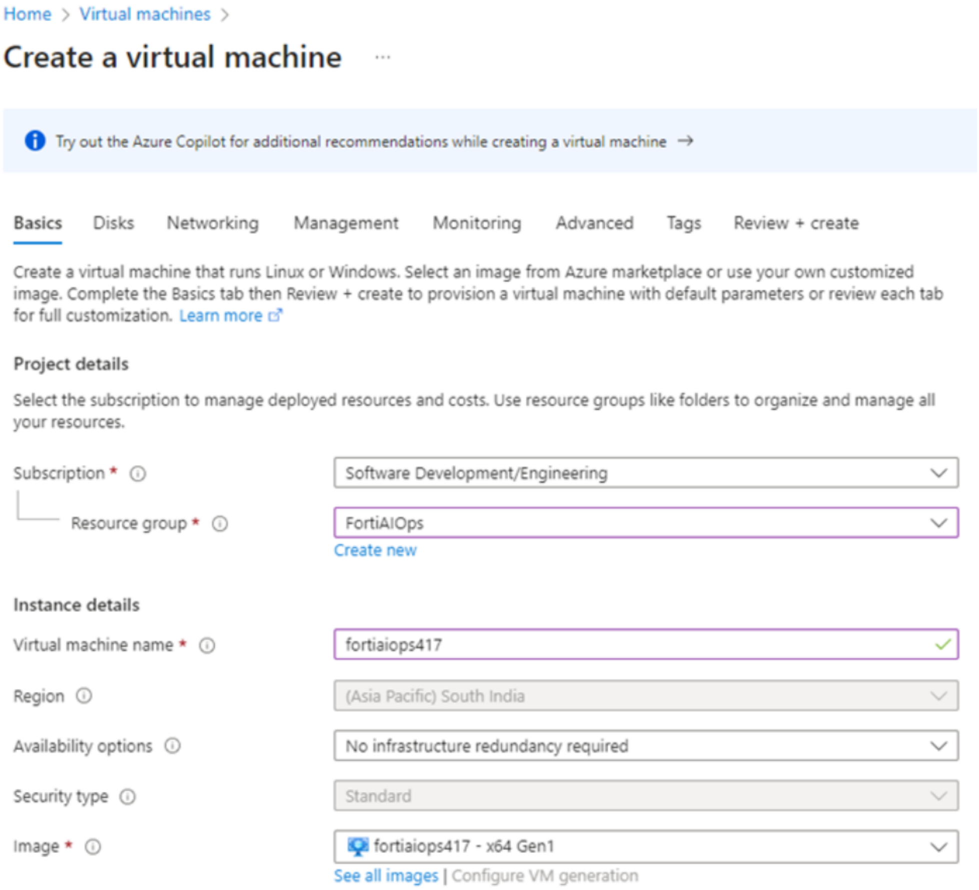
Encryption

You can encrypt the OS and data disks with a platform-managed or customer-managed key. Learn more

Key management ⓘ	Platform-managed key

Data disk

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.



Home > Virtual machines >

Create a virtual machine ...

Try out the Azure Copilot for additional recommendations while creating a virtual machine →

Basics | Disks | Networking | Management | Monitoring | Advanced | Tags | Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Software Development/Engineering

Resource group * : FortiAIOps

Create new

Instance details

Virtual machine name * : fortiaiops417

Region : (Asia Pacific) South India

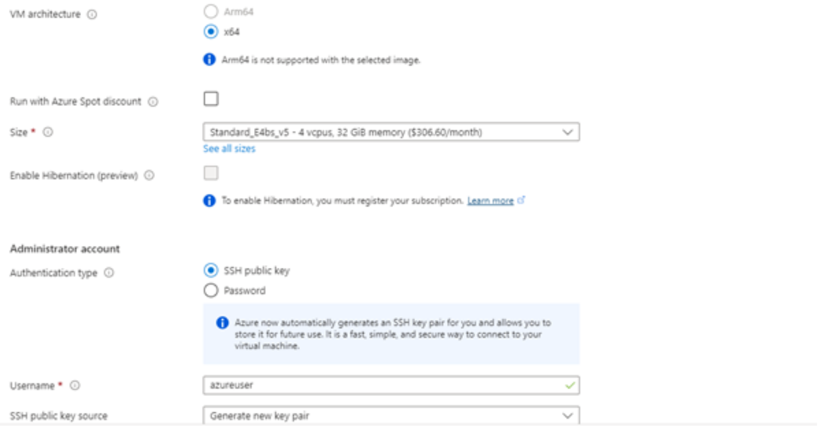
Availability options : No infrastructure redundancy required

Security type : Standard

Image * : fortiaiops417 - x64 Gen1

See all images | Configure VM generation

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



VM architecture : ○ Arm64 ● x64

Arm64 is not supported with the selected image.

Run with Azure Spot discount : □

Size * : Standard_E4bs_v5 - 4 vcpus, 32 GiB memory ($306.60/month)

See all sizes

Enable Hibernation (preview) : □

To enable Hibernation, you must register your subscription. Learn more

Administrator account

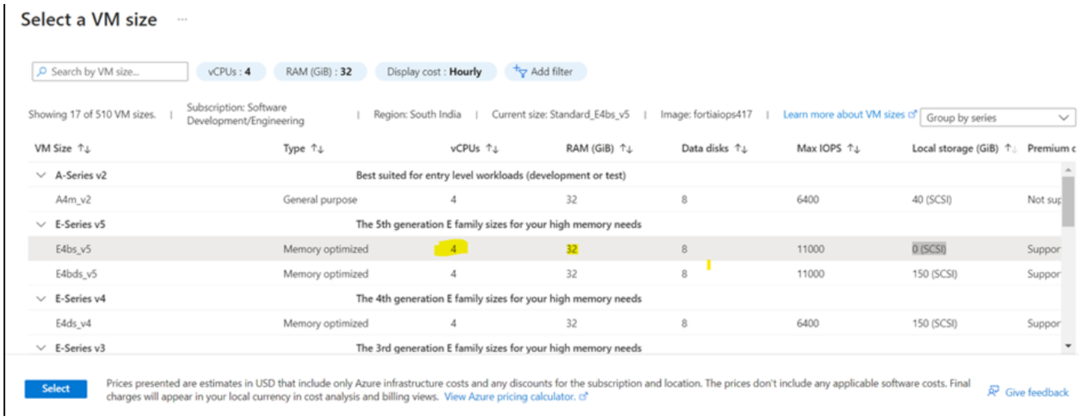
Authentication type : ● SSH public key ○ Password

Azure now automatically generates an SSH key pair for you and allows you to store it for future use. It is a fast, simple, and secure way to connect to your virtual machine.

Username * : azureuser

SSH public key source : Generate new key pair

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.



Select a VM size ···

Search by VM size... | vCPUs : **4** | RAM (GiB) : **32** | Display cost : **Hourly** | Add filter

Showing 17 of 510 VM sizes. | Subscription: Software Development/Engineering | Region: South India | Current size: Standard_E4bs_v5 | Image: fortiaiops417 | Learn more about VM sizes | Group by series

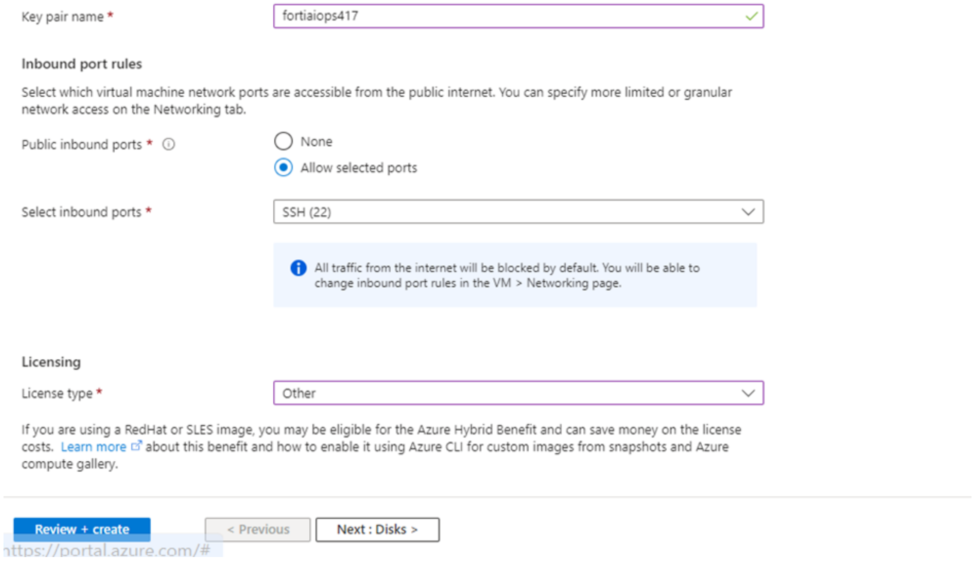
VM Size ↑↓	Type ↑↓	vCPUs ↑↓	RAM (GiB) ↑↓	Data disks ↑↓	Max IOPS ↑↓	Local storage (GiB) ↑↓	Premium c
A-Series v2	Best suited for entry level workloads (development or test)						
A4m_v2	General purpose	4	32	8	6400	40 (SCSI)	Not sup
E-Series v5	The 5th generation E family sizes for your high memory needs						
E4bs_v5	Memory optimized	4	32	8	11000	0 (SCSI)	Suppor
E4bds_v5	Memory optimized	4	32	8	11000	150 (SCSI)	Suppor
E-Series v4	The 4th generation E family sizes for your high memory needs						
E4ds_v4	Memory optimized	4	32	8	6400	150 (SCSI)	Suppor
E-Series v3	The 3rd generation E family sizes for your high memory needs						

Select

Prices presented are estimates in USD that include only Azure infrastructure costs and any discounts for the subscription and location. The prices don't include any applicable software costs. Final charges will appear in your local currency in cost analysis and billing views. View Azure pricing calculator.

Give feedback

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



Key pair name * fortiaiops417

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ○ None ● Allow selected ports

Select inbound ports * SSH (22)

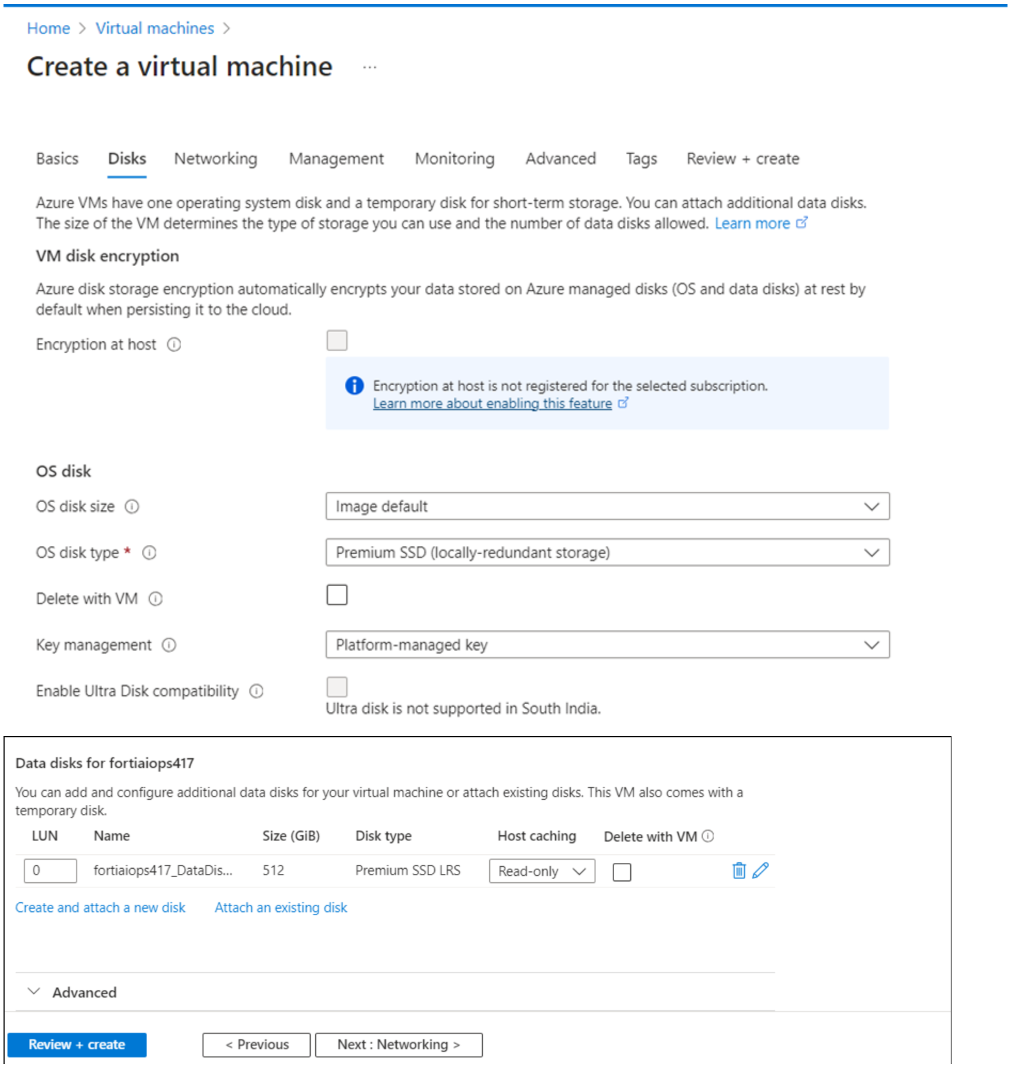
All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

Licensing

License type * Other

If you are using a RedHat or SLES image, you may be eligible for the Azure Hybrid Benefit and can save money on the license costs. Learn more about this benefit and how to enable it using Azure CLI for custom images from snapshots and Azure compute gallery.

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



Create a virtual machine

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

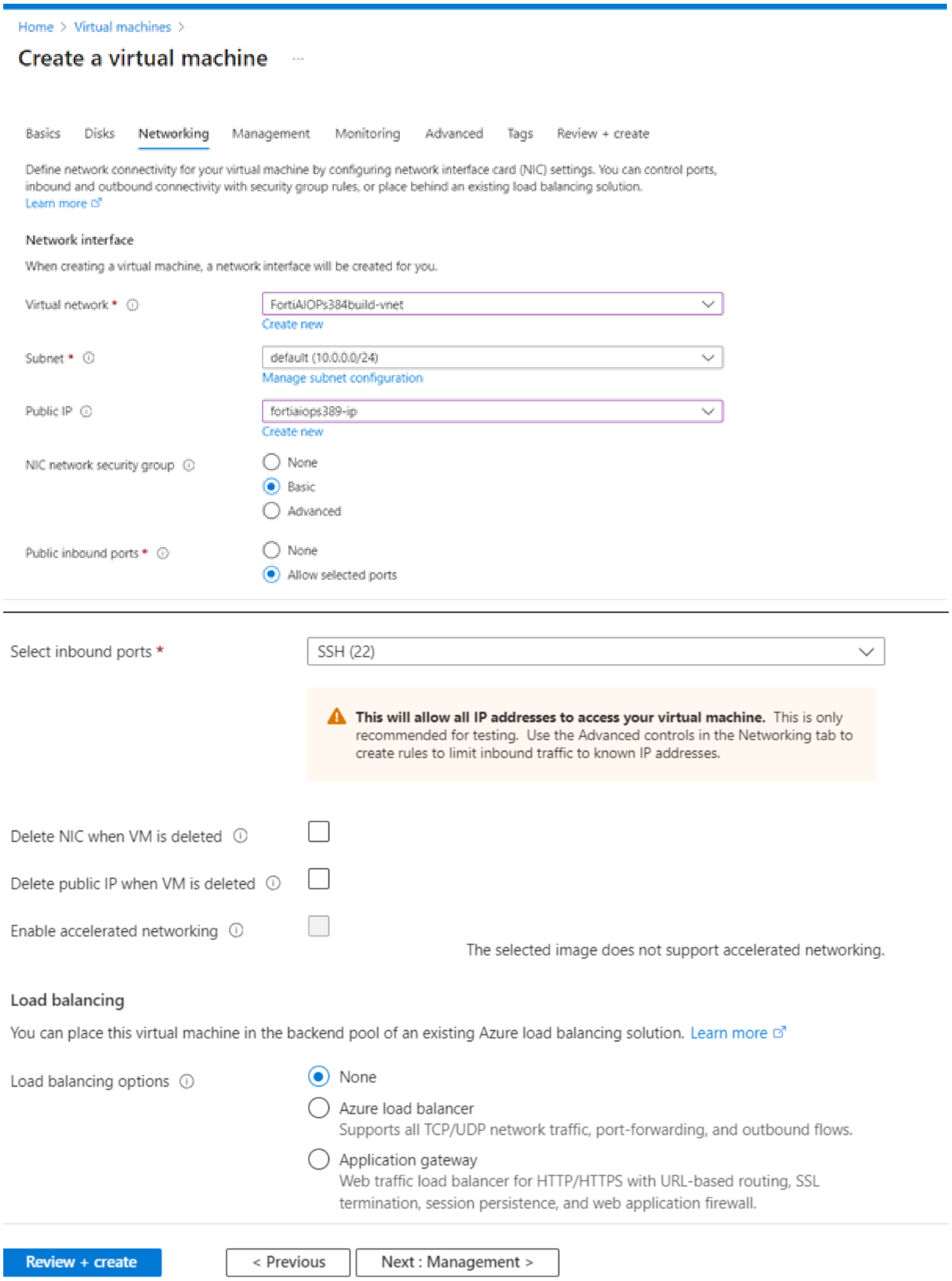
OS disk size	Image default
OS disk type *	Premium SSD (locally-redundant storage)
Delete with VM	□
Key management	Platform-managed key
Enable Ultra Disk compatibility	□ Ultra disk is not supported in South India.

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	□

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



Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. Learn more

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * : FortiAIOPs384build-vnet (Create new)

Subnet * : default (10.0.0.0/24) (Manage subnet configuration)

Public IP : fortiaiops389-ip (Create new)

NIC network security group : ○ None ● Basic ○ Advanced

Public inbound ports * : ○ None ● Allow selected ports

Select inbound ports * : SSH (22)

This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Delete NIC when VM is deleted □

Delete public IP when VM is deleted □

Enable accelerated networking □

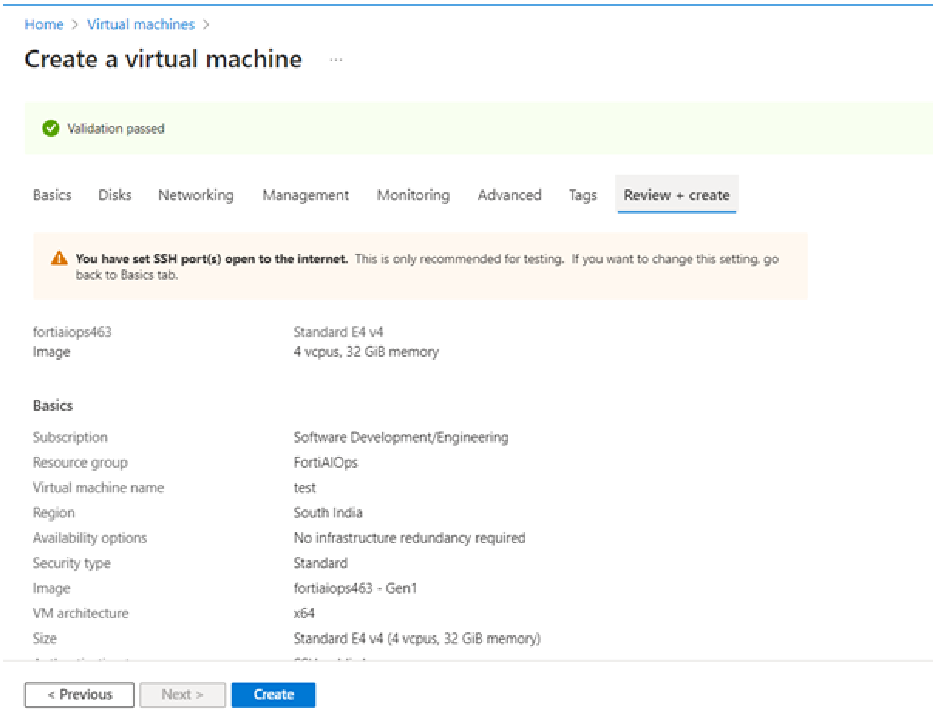
The selected image does not support accelerated networking.

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more

Load balancing options:
● None
○ Azure load balancer
Supports all TCP/UDP network traffic, port-forwarding, and outbound flows.
○ Application gateway
Web traffic load balancer for HTTP/HTTPS with URL-based routing, SSL termination, session persistence, and web application firewall.

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.



Validation passed

You have set SSH port(s) open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.

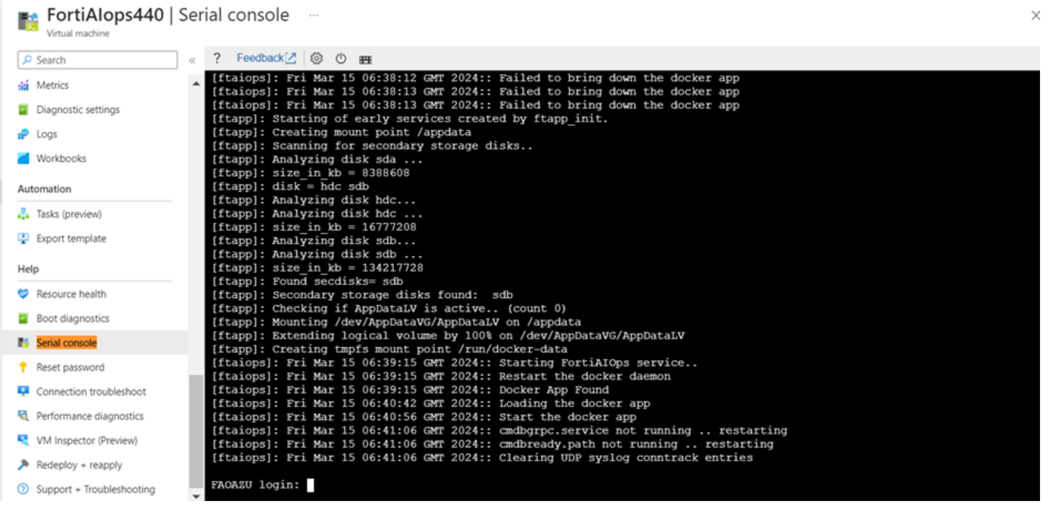
fortiaiops463 Image	Standard E4 v4 4 vcpus, 32 GiB memory

Basics

Subscription	Software Development/Engineering
Resource group	FortiAIOps
Virtual machine name	test
Region	South India
Availability options	No infrastructure redundancy required
Security type	Standard
Image	fortiaiops463 - Gen1
VM architecture	x64
Size	Standard E4 v4 (4 vcpus, 32 GiB memory)

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.



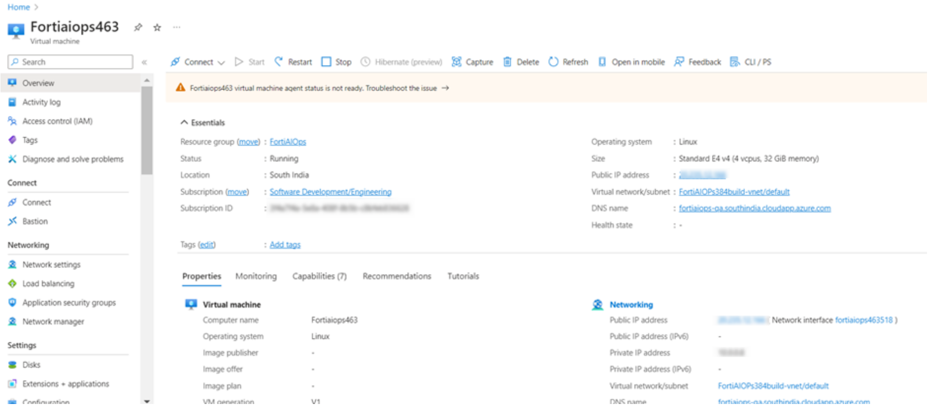
```
[ftaiops]: Fri Mar 15 06:38:12 GMT 2024:: Failed to bring down the docker app
[ftaiops]: Fri Mar 15 06:38:13 GMT 2024:: Failed to bring down the docker app
[ftaiops]: Fri Mar 15 06:38:13 GMT 2024:: Failed to bring down the docker app
[ftapp]: Starting of early services created by ftapp_init.
[ftapp]: Creating mount point /appdata
[ftapp]: Scanning for secondary storage disks..
[ftapp]: Analyzing disk sda ...
[ftapp]: size_in_kb = 8388608
[ftapp]: disk = hdc sdb
[ftapp]: Analyzing disk hdc...
[ftapp]: Analyzing disk hdc ...
[ftapp]: size_in_kb = 16777208
[ftapp]: Analyzing disk sdb...
[ftapp]: Analyzing disk sdb ...
[ftapp]: size_in_kb = 134217728
[ftapp]: Found secdisks= sdb
[ftapp]: Secondary storage disks found:  sdb
[ftapp]: Checking if AppDataLV is active.. (count 0)
[ftapp]: Mounting /dev/AppDataVG/AppDataLV on /appdata
[ftapp]: Extending logical volume by 100% on /dev/AppDataVG/AppDataLV
[ftapp]: Creating tmpfs mount point /run/docker-data
[ftaiops]: Fri Mar 15 06:39:15 GMT 2024:: Starting FortiAIOps service..
[ftaiops]: Fri Mar 15 06:39:15 GMT 2024:: Restart the docker daemon
[ftaiops]: Fri Mar 15 06:39:15 GMT 2024:: Docker App Found
[ftaiops]: Fri Mar 15 06:40:42 GMT 2024:: Loading the docker app
[ftaiops]: Fri Mar 15 06:40:56 GMT 2024:: Start the docker app
[ftaiops]: Fri Mar 15 06:41:06 GMT 2024:: cmdbgrpc.service not running .. restarting
[ftaiops]: Fri Mar 15 06:41:06 GMT 2024:: cmdbready.path not running .. restarting
[ftaiops]: Fri Mar 15 06:41:06 GMT 2024:: Clearing UDP syslog conntrack entries

FAOAZU login: █
```

- **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.



Fortiaiops463 virtual machine agent status is not ready. Troubleshoot the issue →

Essentials

Resource group (move) : FortiAIOps
Status : Running
Location : South India
Subscription (move) : Software Development/Engineering
Subscription ID : [redacted]
Tags (edit) : Add tags

Operating system : Linux
Size : Standard E4 v4 (4 vcpus, 32 GiB memory)
Public IP address : [redacted]
Virtual network/subnet : FortiAIOPs384build-vnet/default
DNS name : fortiaiops-qa.southindia.cloudapp.azure.com
Health state : -

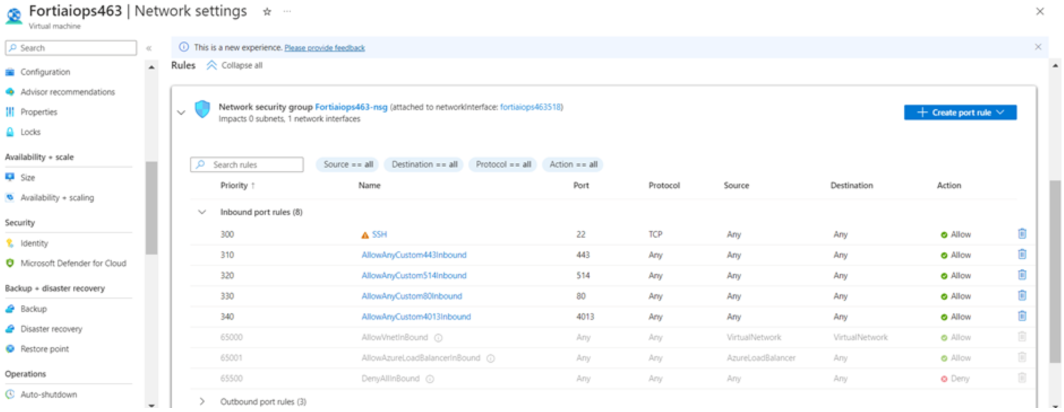
Virtual machine

Computer name	Fortiaiops463
Operating system	Linux
Image publisher	-
Image offer	-
Image plan	-
VM generation	V1

Networking

Public IP address	[redacted] (Network interface fortiaiops463518)
Public IP address (IPv6)	-
Private IP address	[redacted]
Private IP address (IPv6)	-
Virtual network/subnet	FortiAIOPs384build-vnet/default
DNS name	fortiaiops-qa.southindia.cloudapp.azure.com

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



This is a new experience. Please provide feedback

Network security group Fortiaiops463-nsg (attached to networkInterface: fortiaiops463518)
Impacts 0 subnets, 1 network interfaces

Inbound port rules (8)

Priority ↑	Name	Port	Protocol	Source	Destination	Action
300	SSH	22	TCP	Any	Any	Allow
310	AllowAnyCustom443Inbound	443	Any	Any	Any	Allow
320	AllowAnyCustom514Inbound	514	Any	Any	Any	Allow
330	AllowAnyCustom80Inbound	80	Any	Any	Any	Allow
340	AllowAnyCustom4013Inbound	4013	Any	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Outbound port rules (3)

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.

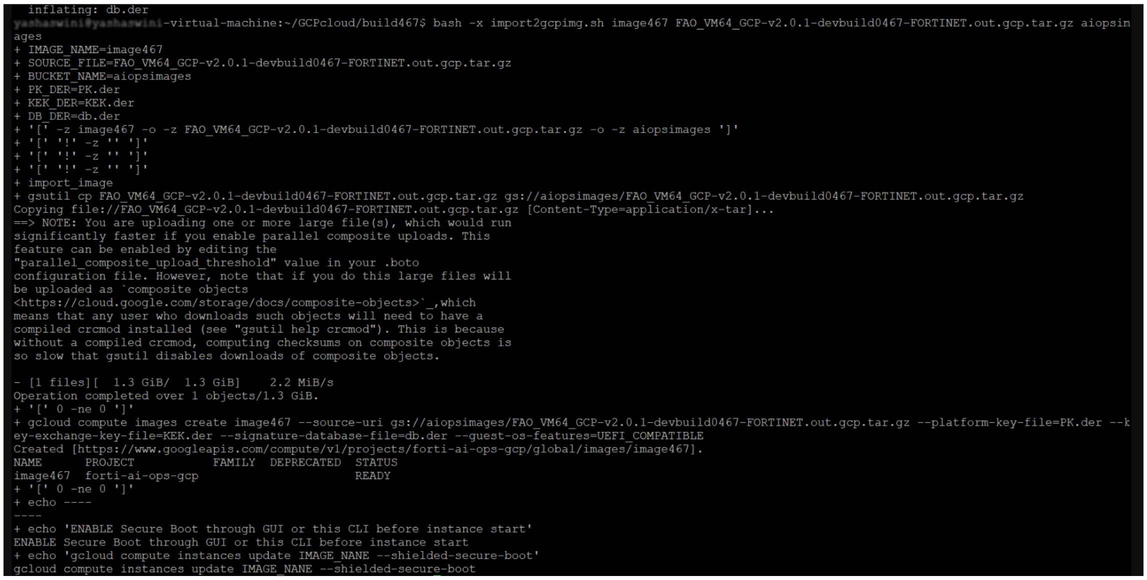
   ```
   ./google-cloud-sdk/bin/gsutil FAO_VM64_GCP-v2.0.1-[build0xxx]-
   FORTINET.out.gcp.tar.gz gs://my-some-bucket
   ```

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*.

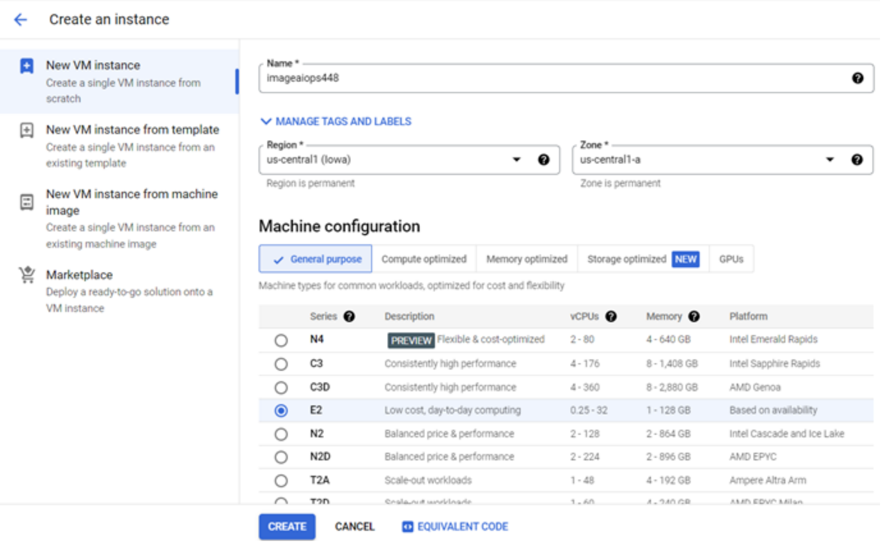
   Note: Make sure to create a storage bucket in the GCP GUI where the FortiAIOps image files are uploaded.

   ```
     inflating: db.der
   [redacted]-virtual-machine:~/GCPcloud/build467$ bash -x import2gcpimg.sh image467 FAO_VM64_GCP-v2.0.1-devbuild0467-FORTINET.out.gcp.tar.gz aiopsin
   ages
   + IMAGE_NAME=image467
   + SOURCE_FILE=FAO_VM64_GCP-v2.0.1-devbuild0467-FORTINET.out.gcp.tar.gz
   + BUCKET_NAME=aiopsimages
   + PK_DER=PK.der
   + KEK_DER=KEK.der
   + DB_DER=db.der
   + '[' -z image467 -o -z FAO_VM64_GCP-v2.0.1-devbuild0467-FORTINET.out.gcp.tar.gz -o -z aiopsimages ']'
   + '[' '!' -z '' ']'
   + '[' '!' -z '' ']'
   + '[' '!' -z '' ']'
   + import_image
   + gsutil cp FAO_VM64_GCP-v2.0.1-devbuild0467-FORTINET.out.gcp.tar.gz gs://aiopsimages/FAO_VM64_GCP-v2.0.1-devbuild0467-FORTINET.out.gcp.tar.gz
   Copying file://FAO_VM64_GCP-v2.0.1-devbuild0467-FORTINET.out.gcp.tar.gz [Content-Type=application/x-tar]...
   ==> NOTE: You are uploading one or more large file(s), which would run
   significantly faster if you enable parallel composite uploads. This
   feature can be enabled by editing the
   "parallel_composite_upload_threshold" value in your .boto
   configuration file. However, note that if you do this large files will
   be uploaded as `composite objects
   <https://cloud.google.com/storage/docs/composite-objects>`_,which
   means that any user who downloads such objects will need to have a
   compiled crcmod installed (see "gsutil help crcmod"). This is because
   without a compiled crcmod, computing checksums on composite objects is
   so slow that gsutil disables downloads of composite objects.

   - [1 files][  1.3 GiB/  1.3 GiB]    2.2 MiB/s
   Operation completed over 1 objects/1.3 GiB.
   + '[' 0 -ne 0 ']'
   + gcloud compute images create image467 --source-uri gs://aiopsimages/FAO_VM64_GCP-v2.0.1-devbuild0467-FORTINET.out.gcp.tar.gz --platform-key-file=PK.der --k
   ey-exchange-key-file=KEK.der --signature-database-file=db.der --guest-os-features=UEFI_COMPATIBLE
   Created [https://www.googleapis.com/compute/v1/projects/forti-ai-ops-gcp/global/images/image467].
   NAME      PROJECT           FAMILY  DEPRECATED  STATUS
   image467  forti-ai-ops-gcp                      READY
   + '[' 0 -ne 0 ']'
   + echo ----
   ----
   + echo 'ENABLE Secure Boot through GUI or this CLI before instance start'
   ENABLE Secure Boot through GUI or this CLI before instance start
   + echo 'gcloud compute instances update IMAGE_NANE --shielded-secure-boot'
   gcloud compute instances update IMAGE_NANE --shielded-secure-boot
   ```

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.



Create an instance

- New VM instance — Create a single VM instance from scratch
- New VM instance from template — Create a single VM instance from an existing template
- New VM instance from machine image — Create a single VM instance from an existing machine image
- Marketplace — Deploy a ready-to-go solution onto a VM instance

Name *: imageaiops448

MANAGE TAGS AND LABELS

Region *: us-central1 (Iowa) — Region is permanent

Zone *: us-central1-a — Zone is permanent

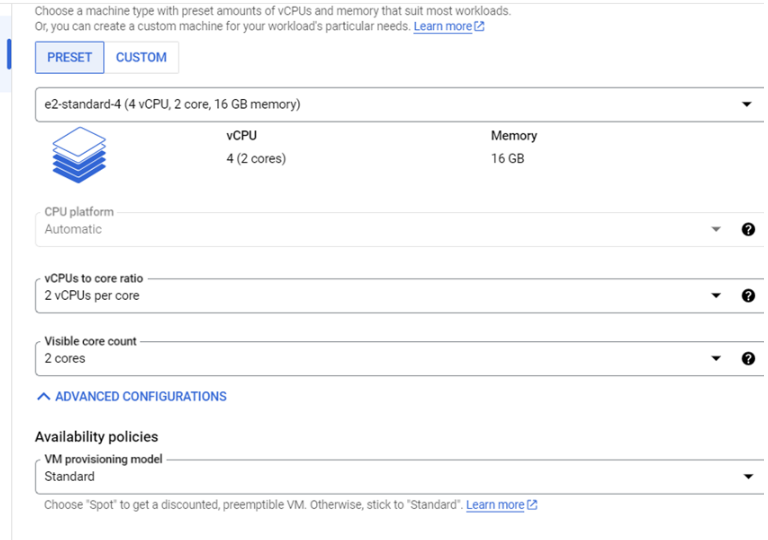
Machine configuration

✓ General purpose | Compute optimized | Memory optimized | Storage optimized NEW | GPUs

Machine types for common workloads, optimized for cost and flexibility

	Series	Description	vCPUs	Memory	Platform
○	N4	PREVIEW Flexible & cost-optimized	2 - 80	4 - 640 GB	Intel Emerald Rapids
○	C3	Consistently high performance	4 - 176	8 - 1,408 GB	Intel Sapphire Rapids
○	C3D	Consistently high performance	4 - 360	8 - 2,880 GB	AMD Genoa
●	E2	Low cost, day-to-day computing	0.25 - 32	1 - 128 GB	Based on availability
○	N2	Balanced price & performance	2 - 128	2 - 864 GB	Intel Cascade and Ice Lake
○	N2D	Balanced price & performance	2 - 224	2 - 896 GB	AMD EPYC
○	T2A	Scale-out workloads	1 - 48	4 - 192 GB	Ampere Altra Arm
○	T2D	Scale-out workloads	1 - 60	4 - 240 GB	AMD EPYC Milan

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



Choose a machine type with preset amounts of vCPUs and memory that suit most workloads.
Or, you can create a custom machine for your workload's particular needs. Learn more

e2-standard-4 (4 vCPU, 2 core, 16 GB memory)

vCPU: 4 (2 cores)

Memory: 16 GB

CPU platform: Automatic

vCPUs to core ratio: 2 vCPUs per core

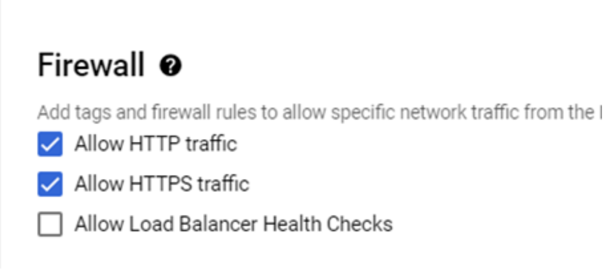
Visible core count: 2 cores

Availability policies

VM provisioning model: Standard

Choose "Spot" to get a discounted, preemptible VM. Otherwise, stick to "Standard". Learn more

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



Firewall

Add tags and firewall rules to allow specific network traffic from the I

☑ Allow HTTP traffic

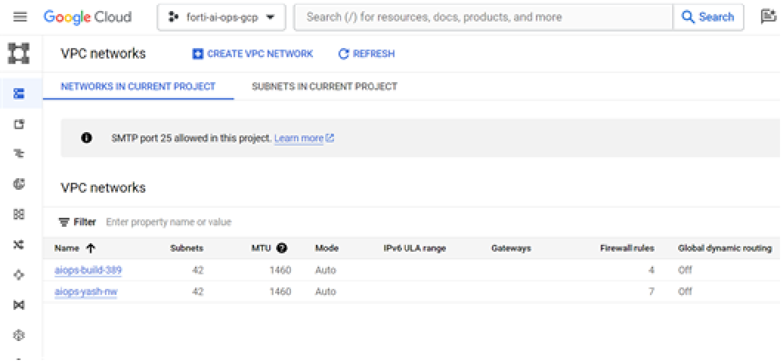
☑ Allow HTTPS traffic

□ Allow Load Balancer Health Checks

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.

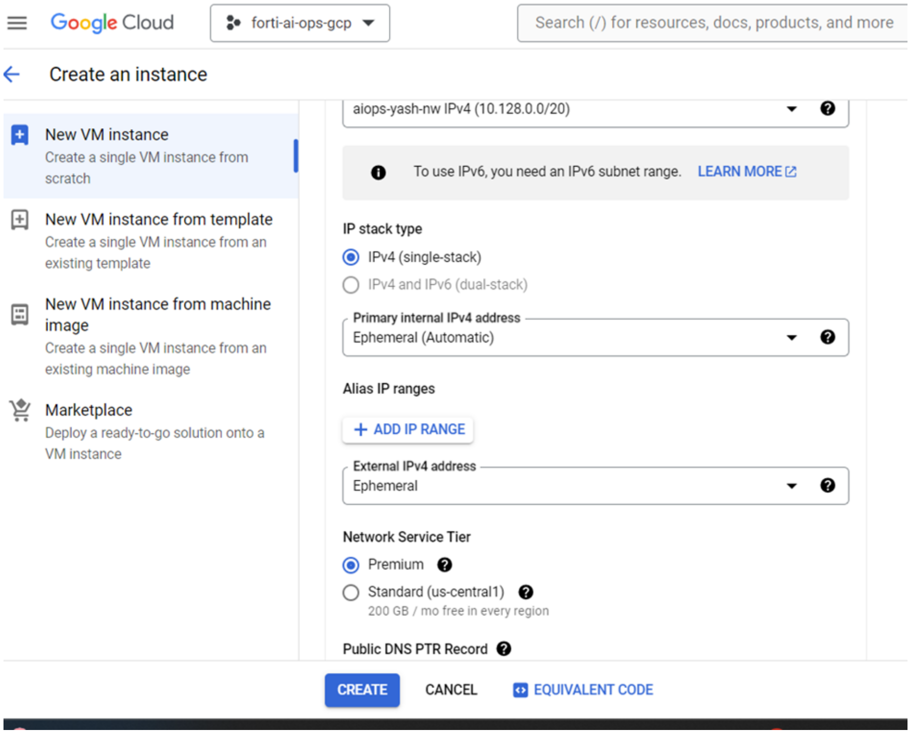

Google Cloud
forti-ai-ops-gcp
Search (/) for resources, docs, products, and more
Search
VPC networks
CREATE VPC NETWORK
REFRESH
NETWORKS IN CURRENT PROJECT
SUBNETS IN CURRENT PROJECT
Learn more
Filter
Enter property name or value

SMTP port 25 allowed in this project.

VPC networks

Name	Subnets	MTU	Mode	IPv6 ULA range	Gateways	Firewall rules	Global dynamic routing
aiops-build-389	42	1460	Auto			4	Off
aiops-yash-nw	42	1460	Auto			7	Off

- 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.


Google Cloud
forti-ai-ops-gcp
Search (/) for resources, docs, products, and more
Create an instance
New VM instance
Create a single VM instance from scratch
New VM instance from template
Create a single VM instance from an existing template
New VM instance from machine image
Create a single VM instance from an existing machine image
Marketplace
Deploy a ready-to-go solution onto a VM instance
LEARN MORE
ADD IP RANGE
CREATE
CANCEL
EQUIVALENT CODE

aiops-yash-nw IPv4 (10.128.0.0/20)

To use IPv6, you need an IPv6 subnet range.

IP stack type

● IPv4 (single-stack)

○ IPv4 and IPv6 (dual-stack)

Primary internal IPv4 address: Ephemeral (Automatic)

Alias IP ranges

External IPv4 address: Ephemeral

Network Service Tier

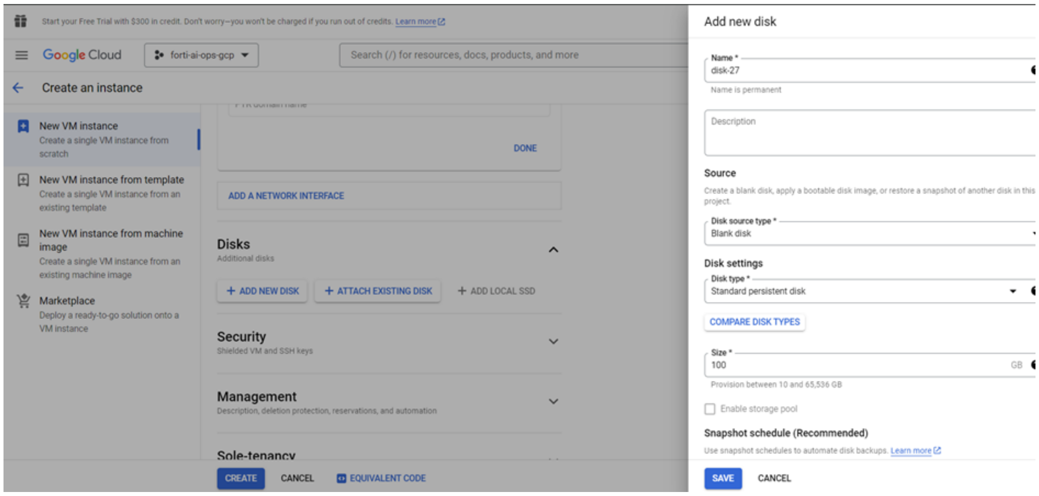
● Premium

○ Standard (us-central1)
200 GB / mo free in every region

Public DNS PTR Record

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.



Start your Free Trial with $300 in credit. Don't worry—you won't be charged if you run out of credits. Learn more

Add new disk

Name *: disk-27

Name is permanent

Description

Source

Create a blank disk, apply a bootable disk image, or restore a snapshot of another disk in this project.

Disk source type *: Blank disk

Disk settings

Disk type *: Standard persistent disk

Size *: 100 GB

Provision between 10 and 65,536 GB

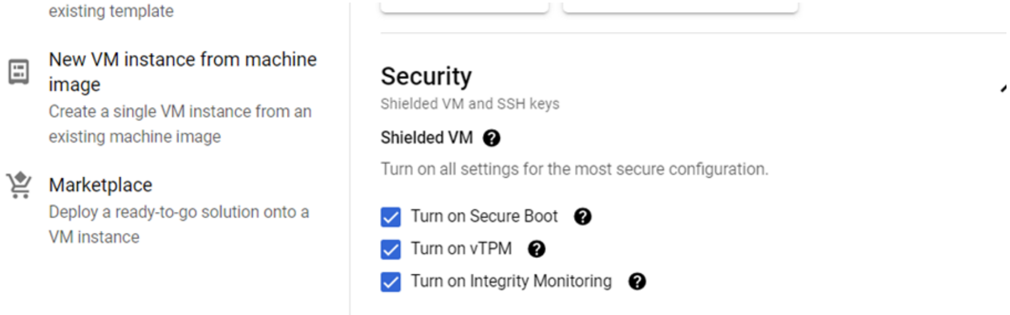
□ Enable storage pool

Snapshot schedule (Recommended)

Use snapshot schedules to automate disk backups. Learn more

Google Cloud
forti-ai-ops-gcp
Search (/) for resources, docs, products, and more
Create an instance
New VM instance
Create a single VM instance from scratch
New VM instance from template
Create a single VM instance from an existing template
New VM instance from machine image
Create a single VM instance from an existing machine image
Marketplace
Deploy a ready-to-go solution onto a VM instance
DONE
ADD A NETWORK INTERFACE
Disks
Additional disks
+ ADD NEW DISK
+ ATTACH EXISTING DISK
+ ADD LOCAL SSD
Security
Shielded VM and SSH keys
Management
Description, deletion protection, reservations, and automation
Sole-tenancy
CREATE
CANCEL
EQUIVALENT CODE
COMPARE DISK TYPES
SAVE
CANCEL

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



Security

Shielded VM and SSH keys

Shielded VM

Turn on all settings for the most secure configuration.

☑ Turn on Secure Boot

☑ Turn on vTPM

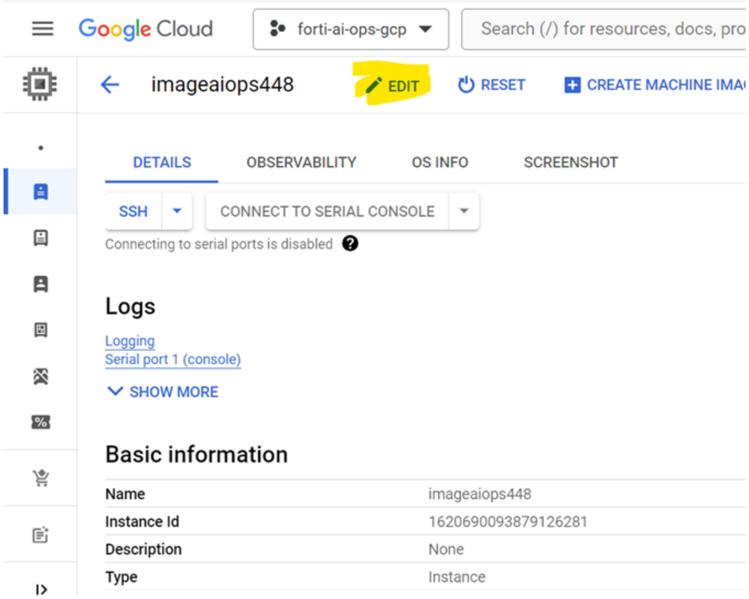
☑ Turn on Integrity Monitoring

existing template
New VM instance from machine image
Create a single VM instance from an existing machine image
Marketplace
Deploy a ready-to-go solution onto a VM instance

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.



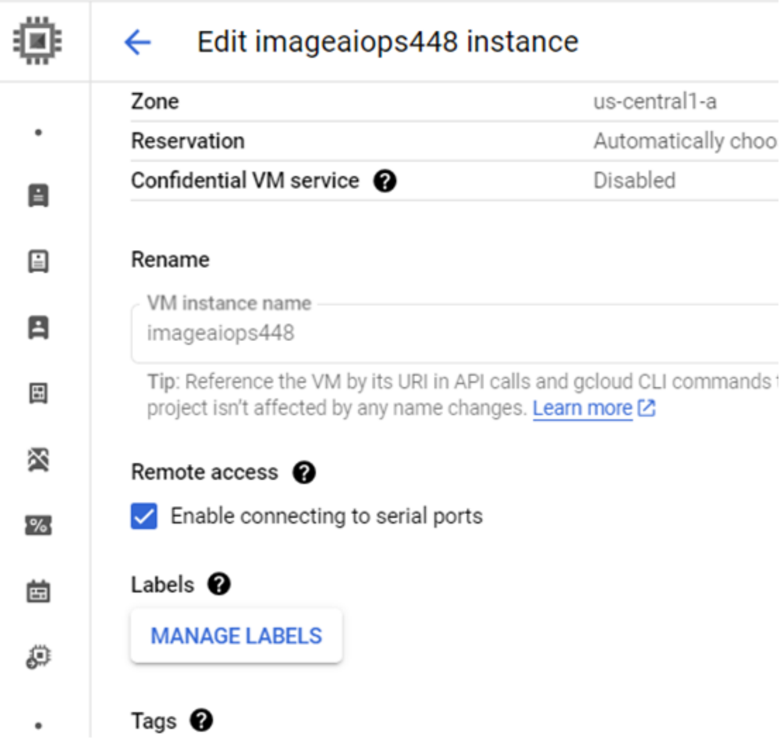
Connecting to serial ports is disabled

Logs

Basic information

Name	imageaiops448
Instance Id	1620690093879126281
Description	None
Type	Instance

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



Edit imageaiops448 instance

Zone	us-central1-a
Reservation	Automatically choo
Confidential VM service	Disabled

Rename

VM instance name: imageaiops448

Tip: Reference the VM by its URI in API calls and gcloud CLI commands project isn't affected by any name changes. Learn more

Remote access

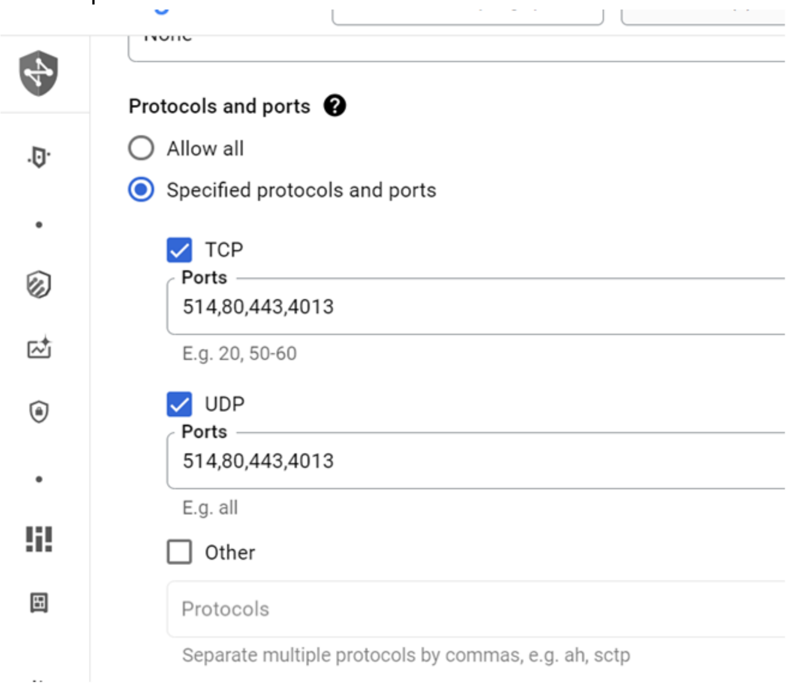
☑ Enable connecting to serial ports

Labels

Tags

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

- 80:80/tcp



Protocols and ports

○ Allow all

● Specified protocols and ports

☑ TCP

Ports: 514,80,443,4013

E.g. 20, 50-60

☑ UDP

Ports: 514,80,443,4013

E.g. all

□ Other

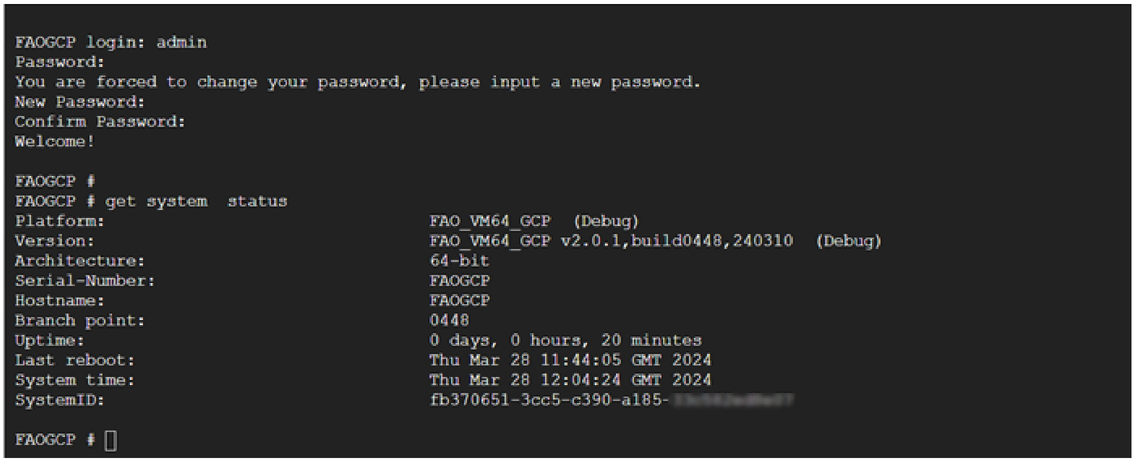
Protocols

Separate multiple protocols by commas, e.g. ah, sctp

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

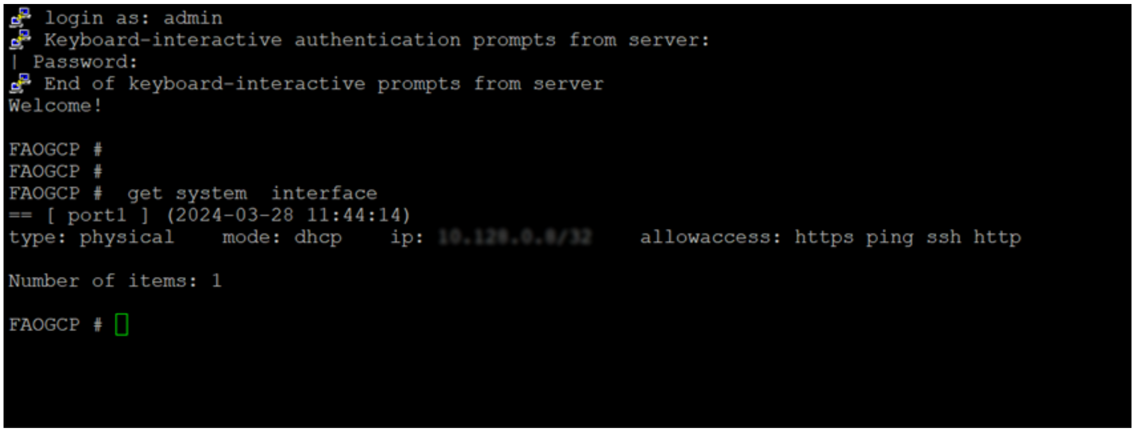
18. Connect the VM instance and login.

- 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.



```
FAOGCP login: admin
Password:
You are forced to change your password, please input a new password.
New Password:
Confirm Password:
Welcome!

FAOGCP #
FAOGCP # get system  status
Platform:                        FAO_VM64_GCP  (Debug)
Version:                         FAO_VM64_GCP v2.0.1,build0448,240310  (Debug)
Architecture:                    64-bit
Serial-Number:                   FAOGCP
Hostname:                        FAOGCP
Branch point:                    0448
Uptime:                          0 days, 0 hours, 20 minutes
Last reboot:                     Thu Mar 28 11:44:05 GMT 2024
System time:                     Thu Mar 28 12:04:24 GMT 2024
SystemID:                        fb370651-3cc5-c390-a185-[redacted]

FAOGCP # 
```

- 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.



```
login as: admin
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
Welcome!

FAOGCP #
FAOGCP #
FAOGCP #  get system  interface
== [ port1 ] (2024-03-28 11:44:14)
type: physical    mode: dhcp    ip: [redacted]    allowaccess: https ping ssh http

Number of items: 1

FAOGCP #
```

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
```

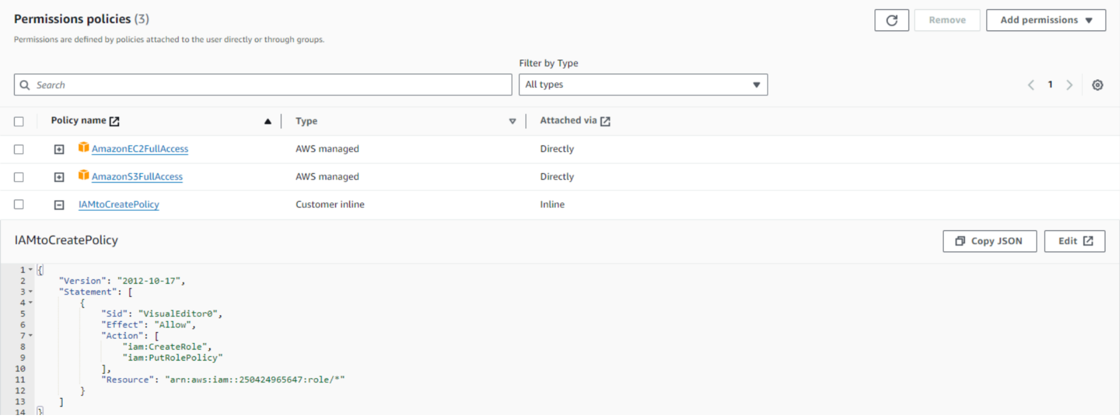
a. Create a policy for the Amazon S3 bucket and attach it to the AWS IAM user.

```
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.



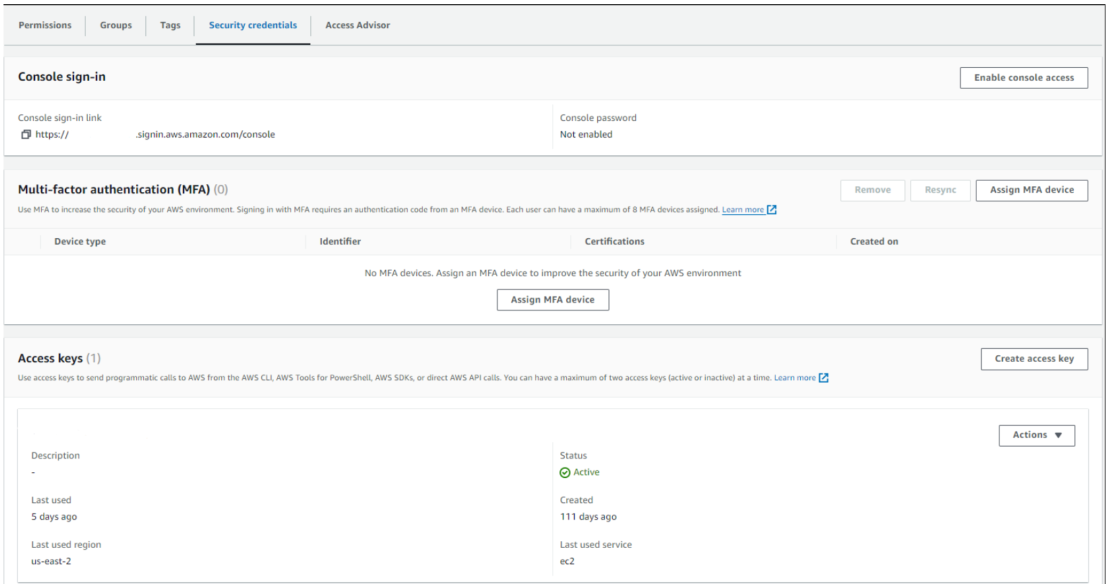
Permissions are defined by policies attached to the user directly or through groups.

☐	Policy name	Type	Attached via
☐	AmazonEC2FullAccess	AWS managed	Directly
☐	AmazonS3FullAccess	AWS managed	Directly
☐	IAMtoCreatePolicy	Customer inline	Inline

IAMtoCreatePolicy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:PutRolePolicy"
            ],
            "Resource": "arn:aws:iam::250424965647:role/*"
        }
    ]
}
```

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



Console sign-in

Console sign-in link
https:// .signin.aws.amazon.com/console

Console password
Not enabled

Multi-factor authentication (MFA) (0)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more

Device type	Identifier	Certifications	Created on

No MFA devices. Assign an MFA device to improve the security of your AWS environment

Access keys (1)

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more

Description
-

Status
✓ Active

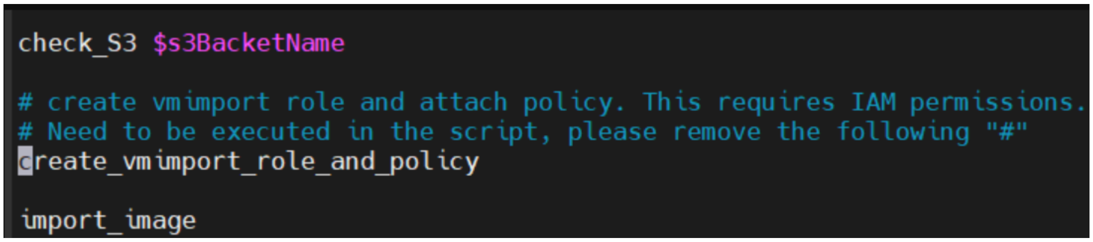
Last used
5 days ago

Created
111 days ago

Last used region
us-east-2

Last used service
ec2

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



```
check_S3 $s3BacketName

# create vmimport role and attach policy. This requires IAM permissions.
# Need to be executed in the script, please remove the following "#"
create_vmimport_role_and_policy

import_image
```

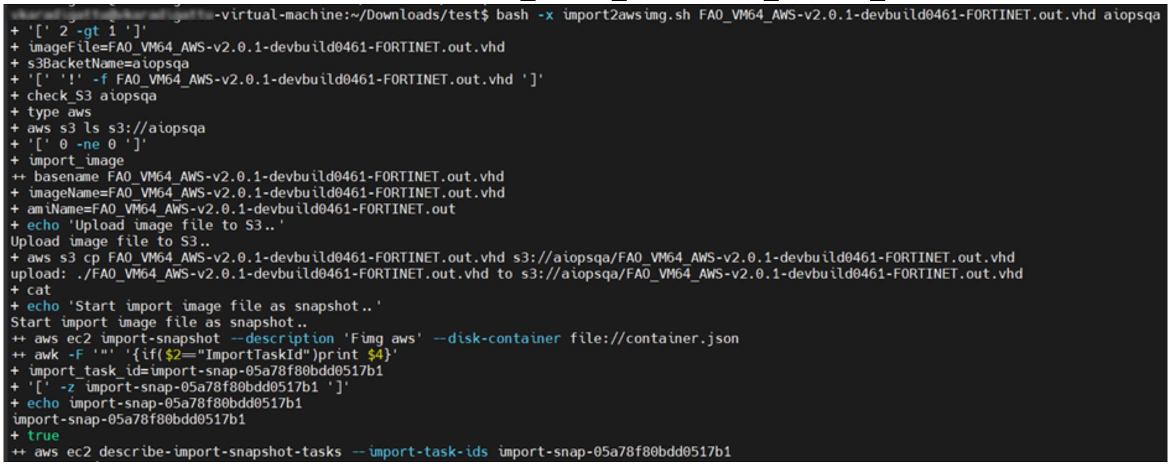
6. Extract the file *FAO_VM64_AWS-v2.0.1-[build01xx]-FORTINET.out.aws.zip*. Post extraction, you have the VHD file and the import script.

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

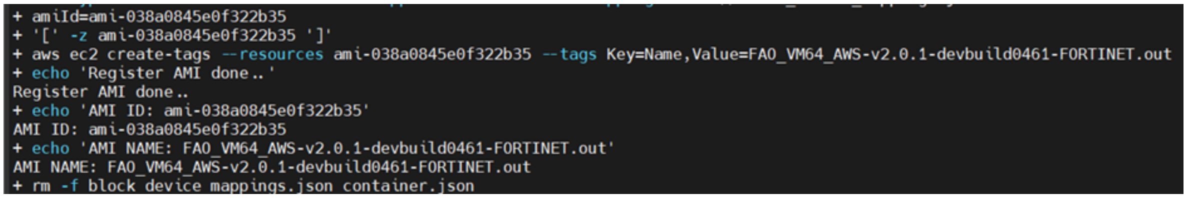
   b. Import script - *import2awsimg.sh*

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

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



```
[redacted]-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
```

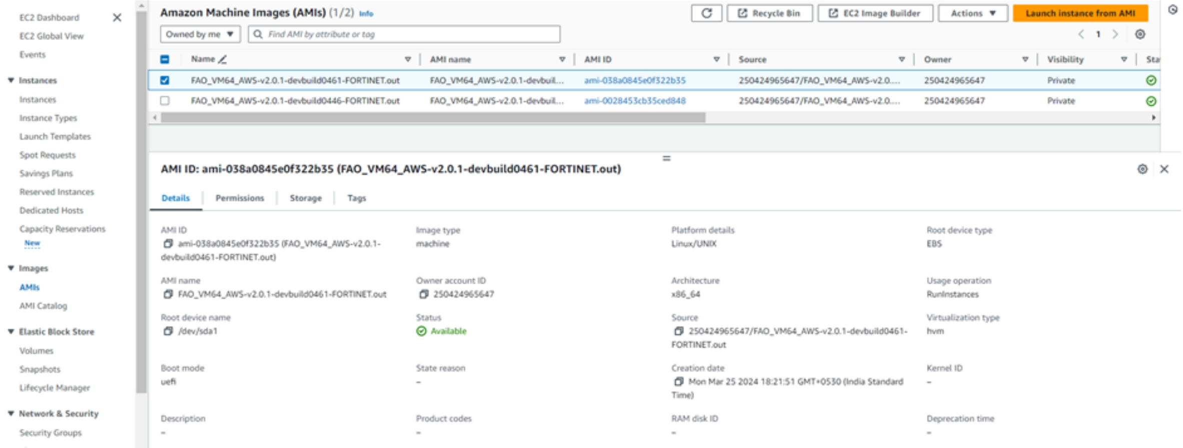


```
+ amiId=ami-038a0845e0f322b35
+ '[' -z ami-038a0845e0f322b35 ']'
+ aws ec2 create-tags --resources ami-038a0845e0f322b35 --tags Key=Name,Value=FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out
+ echo 'Register AMI done..'
Register AMI done..
+ echo 'AMI ID: ami-038a0845e0f322b35'
AMI ID: ami-038a0845e0f322b35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



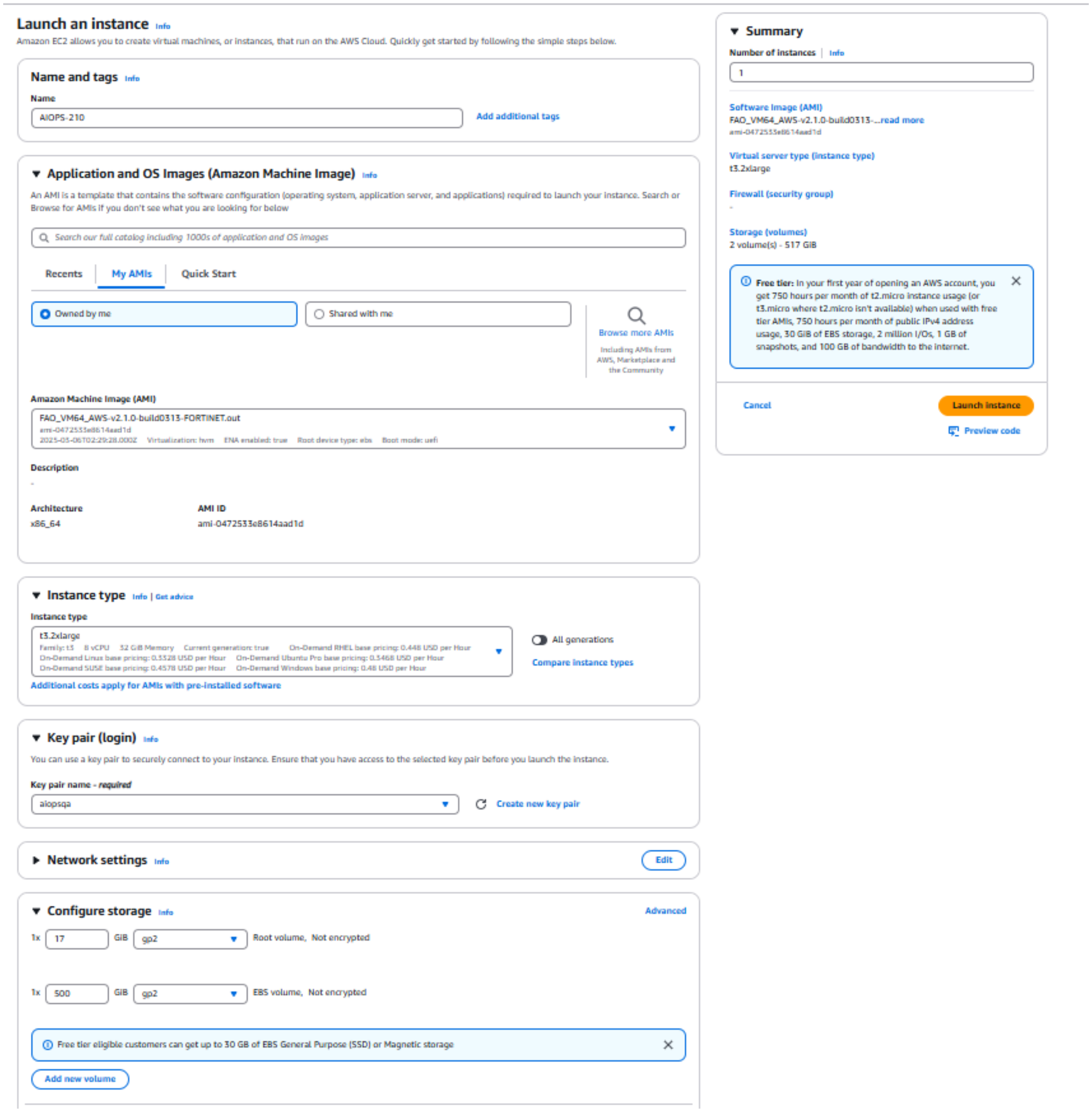
Amazon Machine Images (AMIs) (1/2) Info

	Name	AMI name	AMI ID	Source	Owner	Visibility	Sta
☑	FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out	FAO_VM64_AWS-v2.0.1-devbuil...	ami-038a0845e0f322b35	250424965647/FAO_VM64_AWS-v2.0....	250424965647	Private	✓
□	FAO_VM64_AWS-v2.0.1-devbuild0446-FORTINET.out	FAO_VM64_AWS-v2.0.1-devbuil...	ami-0028453cb35ced848	250424965647/FAO_VM64_AWS-v2.0....	250424965647	Private	✓

AMI ID: ami-038a0845e0f322b35 (FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out)

AMI ID ami-038a0845e0f322b35 (FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out)	Image type machine	Platform details Linux/UNIX	Root device type EBS
AMI name FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out	Owner account ID 250424965647	Architecture x86_64	Usage operation RunInstances
Root device name /dev/sda1	Status Available	Source 250424965647/FAO_VM64_AWS-v2.0.1-devbuild0461-FORTINET.out	Virtualization type hvm
Boot mode uefi	State reason -	Creation date Mon Mar 25 2024 18:21:51 GMT+0530 (India Standard Time)	Kernel ID -
Description -	Product codes -	RAM disk ID -	Deprecation time -

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**.



Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Name: AIOPS-210

Application and OS Images (Amazon Machine Image)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

● Owned by me ○ Shared with me

Browse more AMIs
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)
FAO_VM64_AWS-v2.1.0-build0313-FORTINET.out
ami-0472533e8614aad1d
2025-03-06T02:29:28.000Z Virtualization: hvm ENA enabled: true Root device type: ebs Boot mode: uefi

Description
-

Architecture: x86_64
AMI ID: ami-0472533e8614aad1d

Instance type

Instance type
t3.2xlarge
Family: t3 8 vCPU 32 GiB Memory Current generation: true On-Demand RHEL base pricing: 0.448 USD per Hour
On-Demand Linux base pricing: 0.3328 USD per Hour On-Demand Ubuntu Pro base pricing: 0.3468 USD per Hour
On-Demand SUSE base pricing: 0.4578 USD per Hour On-Demand Windows base pricing: 0.48 USD per Hour

Additional costs apply for AMIs with pre-installed software

Key pair (login)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*: aiopsqa

Network settings

Configure storage

1x 17 GiB gp2 Root volume, Not encrypted

1x 500 GiB gp2 EBS volume, Not encrypted

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Summary

Number of instances: 1

Software Image (AMI)
FAO_VM64_AWS-v2.1.0-build0313-...read more
ami-0472533e8614aad1d

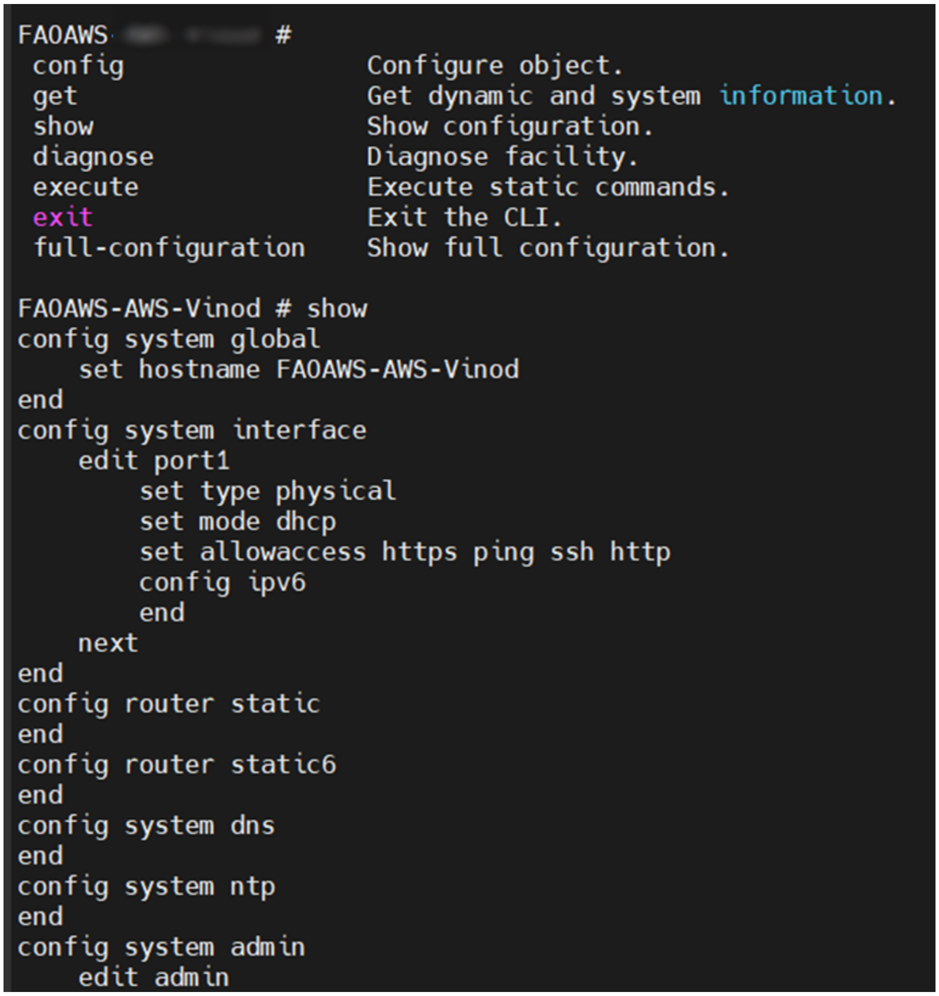
Virtual server type (instance type)
t3.2xlarge

Firewall (security group)
-

Storage (volumes)
2 volume(s) - 517 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

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



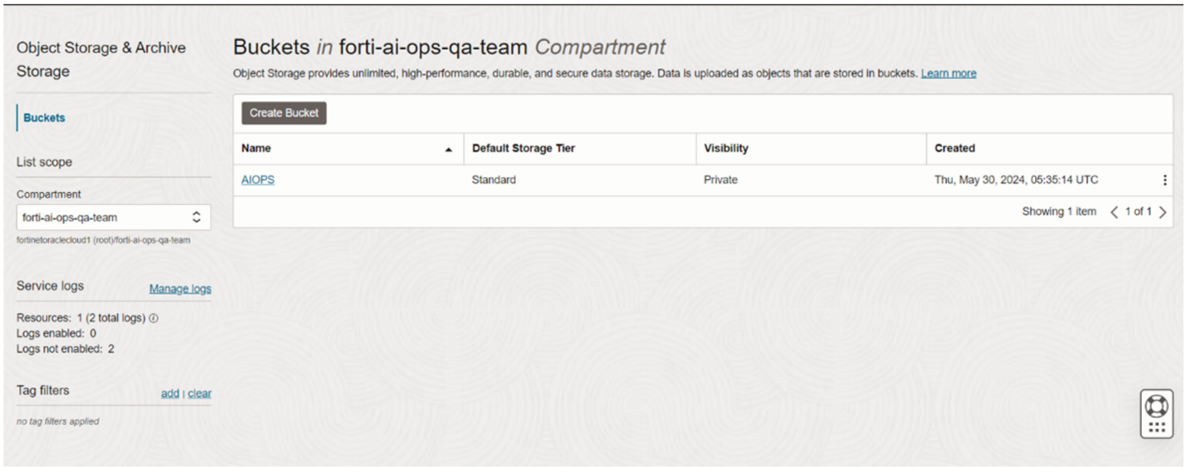
```
FAOAWS-[redacted] #
 config                 Configure object.
 get                    Get dynamic and system information.
 show                   Show configuration.
 diagnose               Diagnose facility.
 execute                Execute static commands.
 exit                   Exit the CLI.
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

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**.



Object Storage & Archive Storage

Buckets

List scope

Compartment: forti-ai-ops-qa-team

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

Service logs — Manage logs

Resources: 1 (2 total logs)

Logs enabled: 0

Logs not enabled: 2

Tag filters — add | clear

no tag filters applied

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

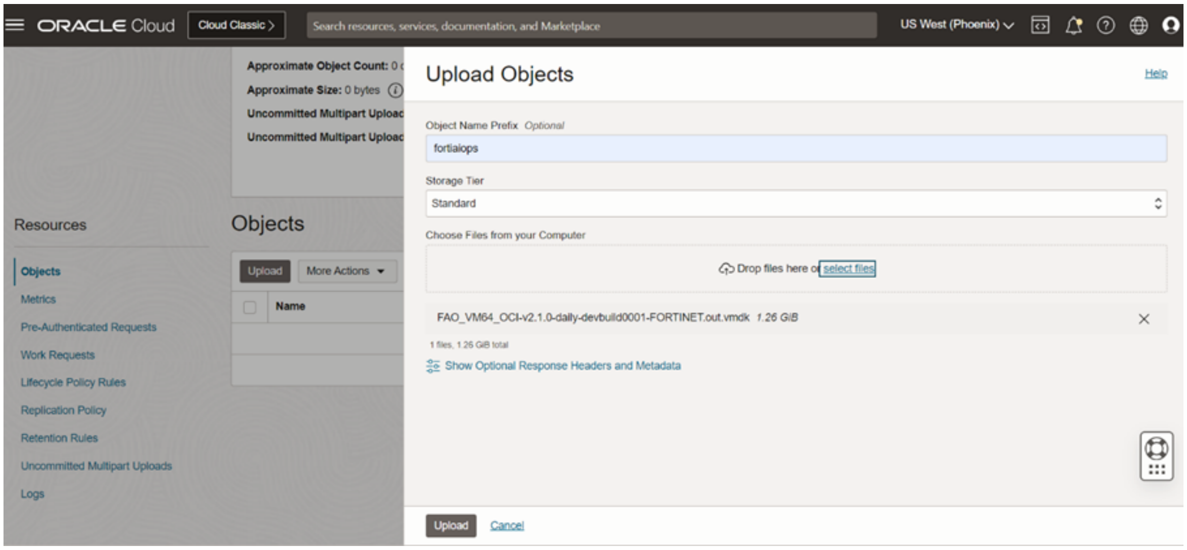
Object Storage provides unlimited, high-performance, durable, and secure data storage. Data is uploaded as objects that are stored in buckets. Learn more

Create Bucket

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

Showing 1 item < 1 of 1 >

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



ORACLE Cloud
Cloud Classic >
Search resources, services, documentation, and Marketplace
US West (Phoenix)
Approximate Object Count: 0
Approximate Size: 0 bytes
Uncommitted Multipart Uploads
Uncommitted Multipart Uploads
Resources
Objects
Metrics
Pre-Authenticated Requests
Work Requests
Lifecycle Policy Rules
Replication Policy
Retention Rules
Uncommitted Multipart Uploads
Logs
Objects
Upload
More Actions
Name

Upload Objects — Help

Object Name Prefix *Optional*: fortiaiops

Storage Tier: Standard

Choose Files from your Computer

Drop files here or select files

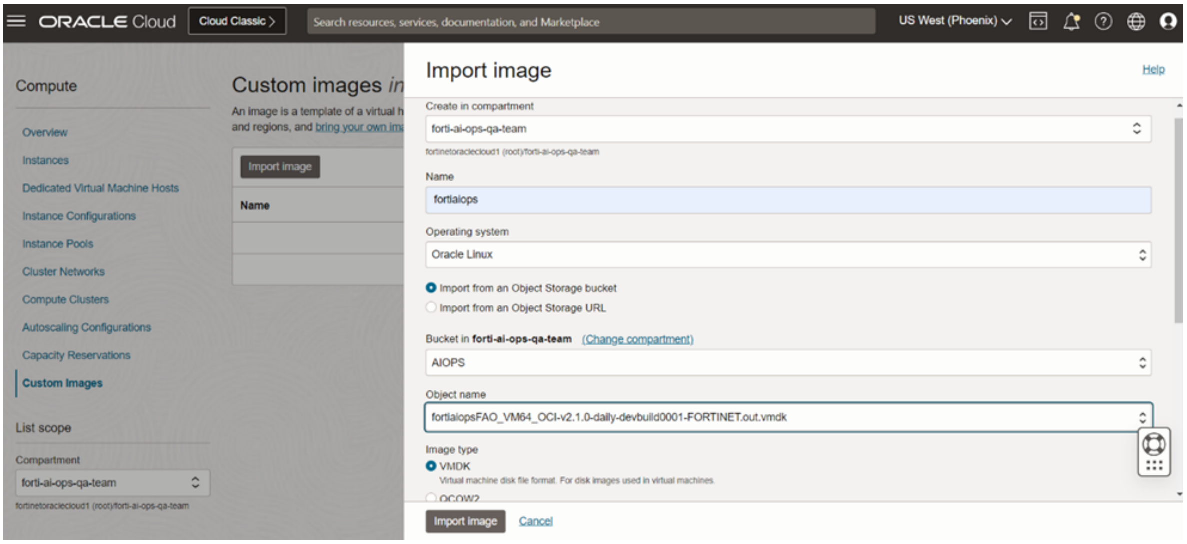
FAO_VM64_OCI-v2.1.0-daily-devbuild0001-FORTINET.out.vmdk *1.26 GiB*

1 files, 1.26 GiB total

Show Optional Response Headers and Metadata

Upload Cancel

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



Import image

Create in compartment: forti-ai-ops-qa-team
fortinetoraclecloud1 (root)/forti-ai-ops-qa-team

Name: fortiaiops

Operating system: Oracle Linux

● Import from an Object Storage bucket
○ Import from an Object Storage URL

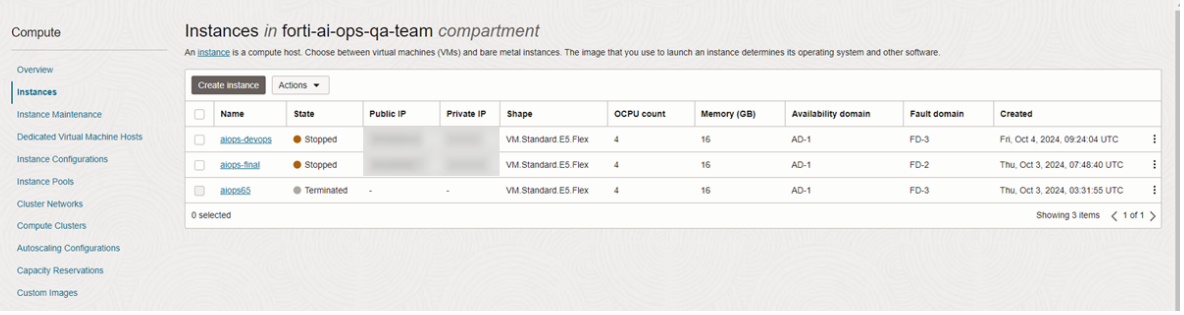
Bucket in **forti-ai-ops-qa-team** (Change compartment): AIOPS

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

Image type
● VMDK
Virtual machine disk file format. For disk images used in virtual machines.
○ QCOW2

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

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



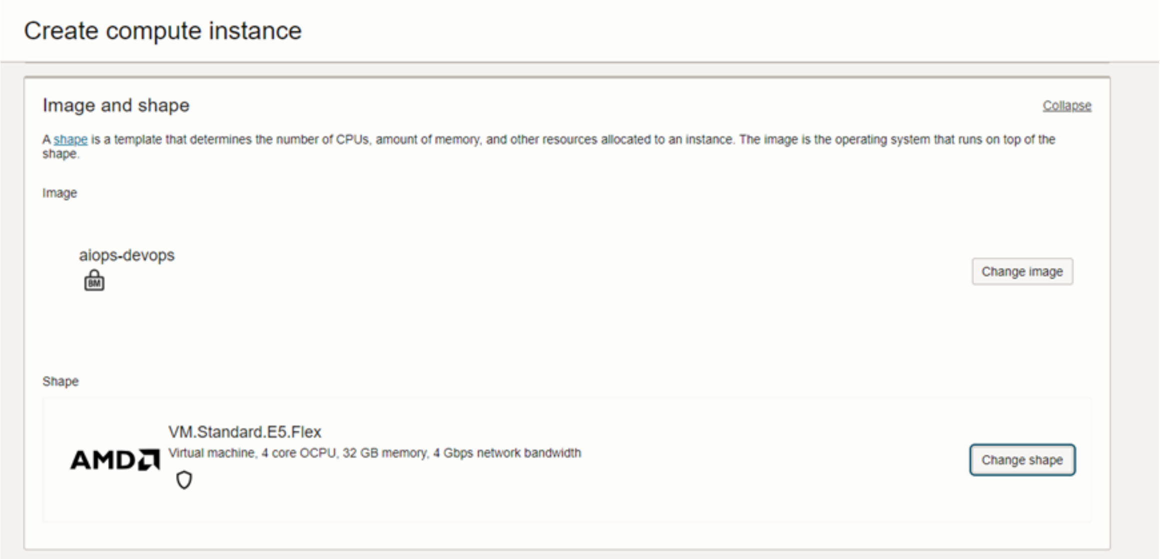
Instances *in* forti-ai-ops-qa-team *compartment*

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

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

0 selected   Showing 3 items   1 of 1

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



Create compute instance

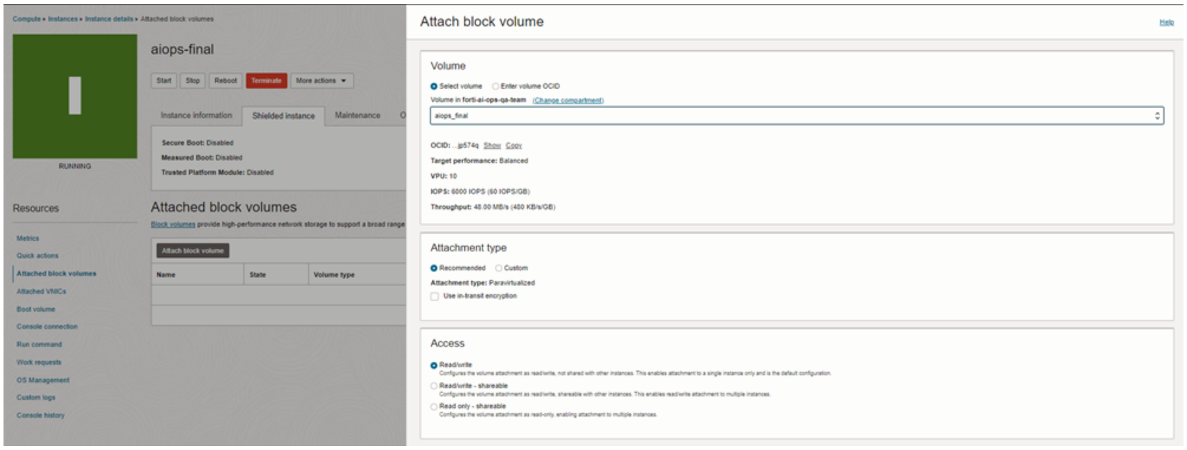
Image and shape

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

Image: aiops-devops

Shape: VM.Standard.E5.Flex
Virtual machine, 4 core OCPU, 32 GB memory, 4 Gbps network bandwidth

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



Secure Boot: Disabled
Measured Boot: Disabled
Trusted Platform Module: Disabled

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

Attach block volume

Volume

● Select volume ○ Enter volume OCID

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

aiops_final

OCID: ...jp574q Show Copy

Target performance: Balanced

VPU: 10

IOPS: 6000 IOPS (60 IOPS/GB)

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

Attachment type

● Recommended ○ Custom

Attachment type: Paravirtualized

□ Use in-transit encryption

Access

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

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

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

12. Reboot the instance after attaching the volume.

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

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

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.
   admin/*admin*

Command Line Interface (CLI) Reference

The following commands are supported for FortiAIOps.

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

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.

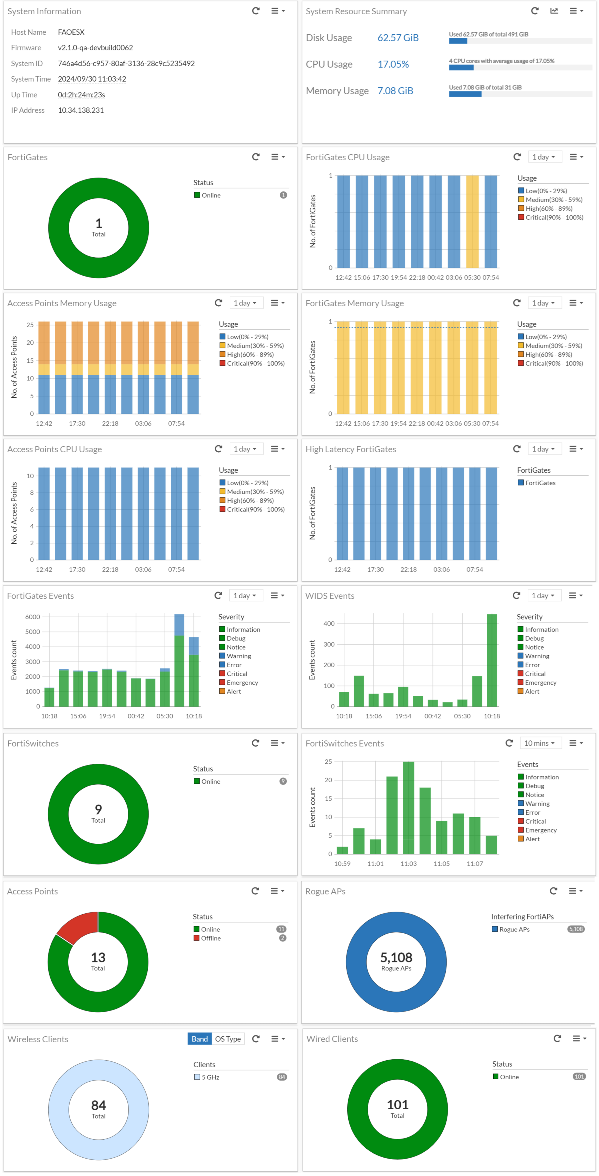
Dashboard

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

- Summary
- AI Insights
- Service Assurance

Summary

This dashboard provides visual summarization of key system information, network elements, and resource usage. The interactive graphs and charts allow you to navigate into detailed views of network statistics for analytical and monitoring purpose.



System Information

Host Name	FAOESX
Firmware	v2.1.0-qa-devbuild0062
System ID	746a4d56-c957-80af-3136-28c9c5235492
System Time	2024/09/30 11:03:42
Up Time	0d:2h:24m:23s
IP Address	10.34.138.231

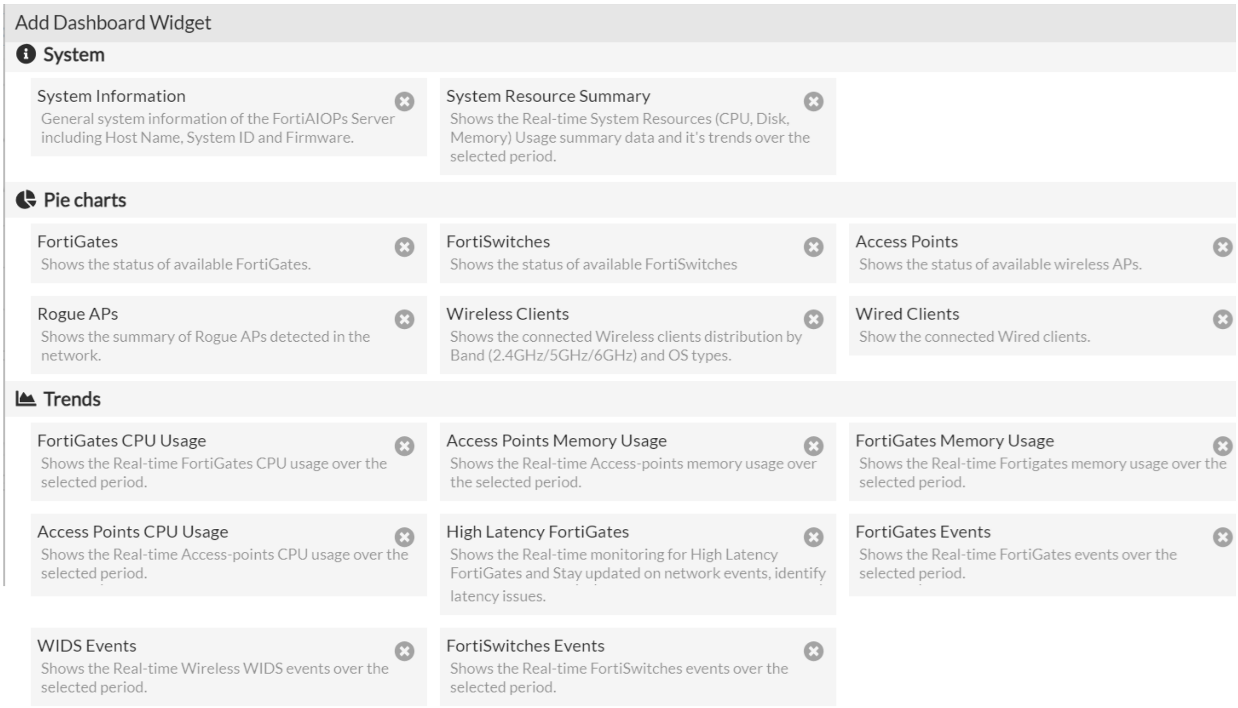
System Resource Summary

Disk Usage	62.57 GiB	Used 62.57 GiB of total 491 GiB
CPU Usage	17.05%	4 CPU cores with average usage of 17.05%
Memory Usage	7.08 GiB	Used 7.08 GiB of total 31 GiB

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.

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



Add Dashboard Widget

System

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

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

Pie charts

FortiGates
Shows the status of available FortiGates.

FortiSwitches
Shows the status of available FortiSwitches

Access Points
Shows the status of available wireless APs.

Rogue APs
Shows the summary of Rogue APs detected in the network.

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

Wired Clients
Show the connected Wired clients.

Trends

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

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

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

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

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

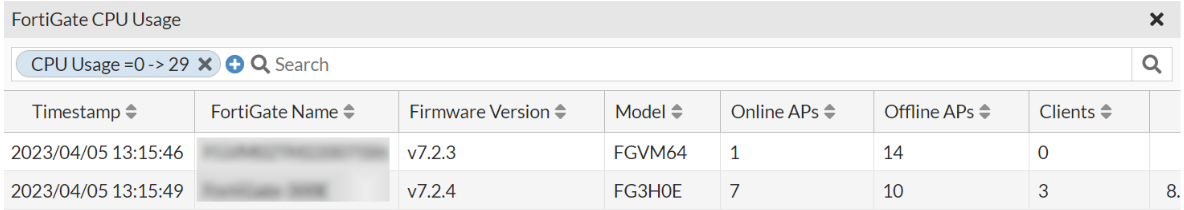
FortiGates Events
Shows the Real-time FortiGates events over the selected period.

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

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

The following widgets provide network data on this dashboard.

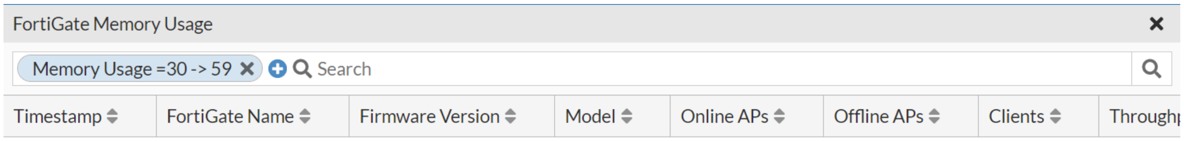
- **System Information** - This widget provides generic information about the FortiAIOps such as the host name, firmware version, system ID, current system time, uptime, and the IP address.
- **System Resource Summary** - This widget provides an overview of the current system resource usage for FortiAIOps. 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.
- **Wireless Clients** - 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 navigate to **Wireless > Clients**.
- **Wired Clients** - Displays the total number of connected clients with their status.
- **WIDS Events** – Displays the real-time wireless WIDS events and categorizes them based on the severity level as, *Information, Debug, Notice, Warning, Error, Critical, Emergency*, and Alert. You can select the period to view the data (10 or 30 minutes, 1 or 12 hours, or 1 day).
- **FortiGates** - Displays the total number of FortiGate controllers in your network and their status (*Online*/*Offline*). Click on the chart to navigate to **Inventory > Managed FortiGates**.
- **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.



FortiGate CPU Usage ✕

CPU Usage =0 -> 29 ✕ ⊕ Search

Timestamp	FortiGate Name	Firmware Version	Model	Online APs	Offline APs	Clients	
2023/04/05 13:15:46	[redacted]	v7.2.3	FGVM64	1	14	0	
2023/04/05 13:15:49	[redacted]	v7.2.4	FG3H0E	7	10	3	8.

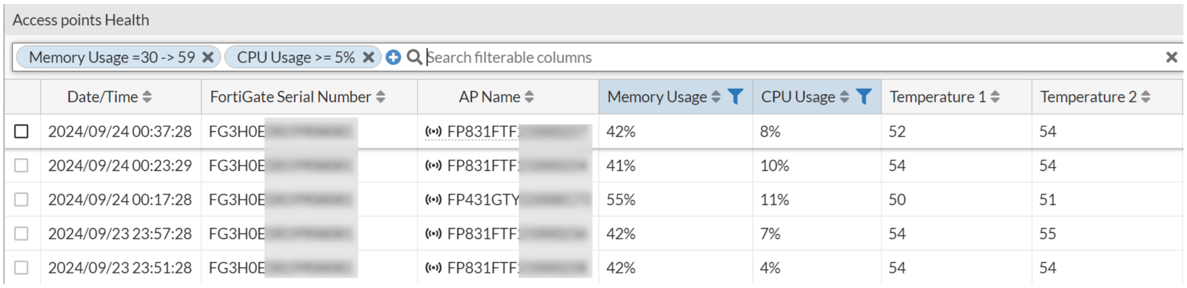


FortiGate Memory Usage ✕

Memory Usage =30 -> 59 ✕ ⊕ Search

Timestamp	FortiGate Name	Firmware Version	Model	Online APs	Offline APs	Clients	Through

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

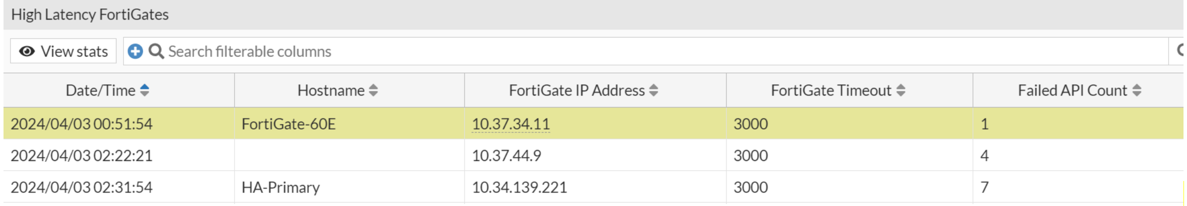


Access points Health

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

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

- **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).

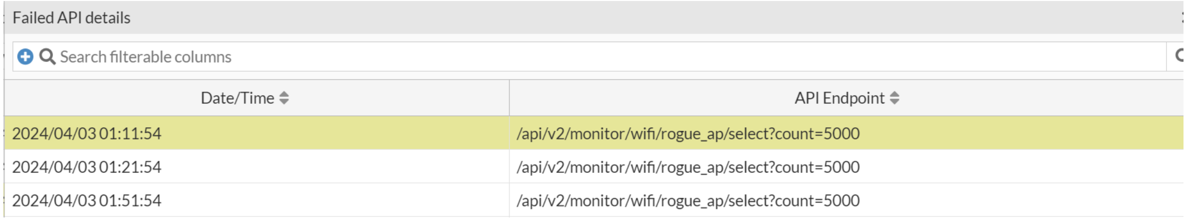


High Latency FortiGates

View stats ⊕ Search filterable columns

Date/Time	Hostname	FortiGate IP Address	FortiGate Timeout	Failed API Count
2024/04/03 00:51:54	FortiGate-60E	10.37.34.11	3000	1
2024/04/03 02:22:21		10.37.44.9	3000	4
2024/04/03 02:31:54	HA-Primary	10.34.139.221	3000	7

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

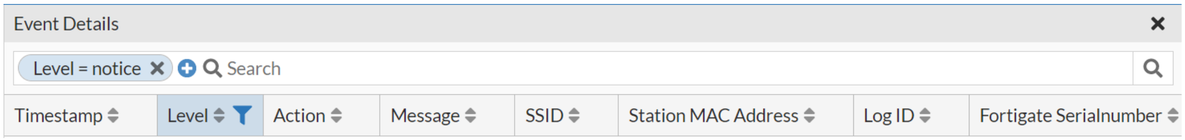


Failed API details

⊕ Search filterable columns

Date/Time	API Endpoint
2024/04/03 01:11:54	/api/v2/monitor/wifi/rogue_ap/select?count=5000
2024/04/03 01:21:54	/api/v2/monitor/wifi/rogue_ap/select?count=5000
2024/04/03 01:51:54	/api/v2/monitor/wifi/rogue_ap/select?count=5000

- **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).



Event Details ✕

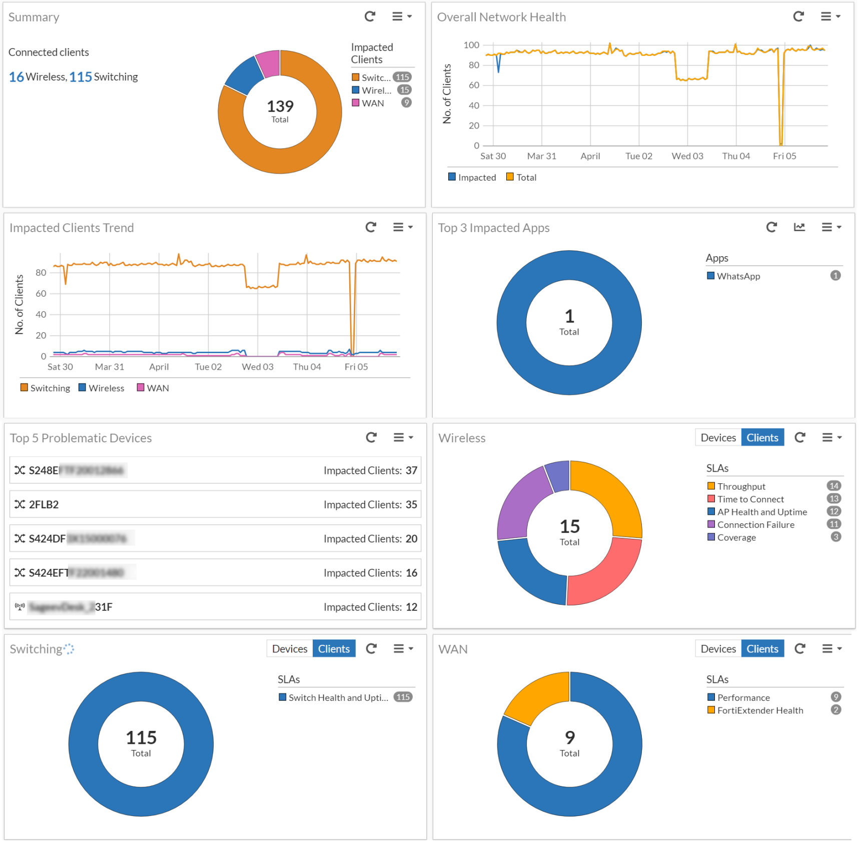
Level = notice ✕ ⊕ Search

Timestamp	Level	Action	Message	SSID	Station MAC Address	Log ID	Fortigate Serialnumber

- **Access Points** - Displays the total number of access points in your network and their status (*Online*, *Offline*, *Waiting for Authorization*, or *Unknown*). Click on the chart to navigate to **Wireless > Access Points**.
- **FortiSwitches** - Displays the total number of FortiSwitches in your network and their status (*Online*, *Offline*, *Waiting for Authorization*, or *Unknown*). Click on the chart to navigate to **Switch > FortiSwitch**.
- **FortiSwitches Events** - Displays the FortiSwitch 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).
- **Rogue APs** - Displays the total number of rogue access points detected in your network. Click on the chart to navigate to **Wireless > Rogue APs**.

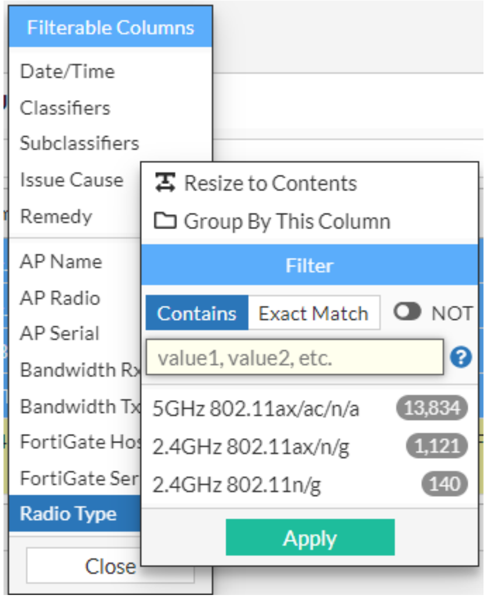
AI Insights

The AI insights dashboard present data in various panels that is displayed in a series of charts and graphs, that you can filter based on time duration. Navigate to **Dashboard > AI Insights**.

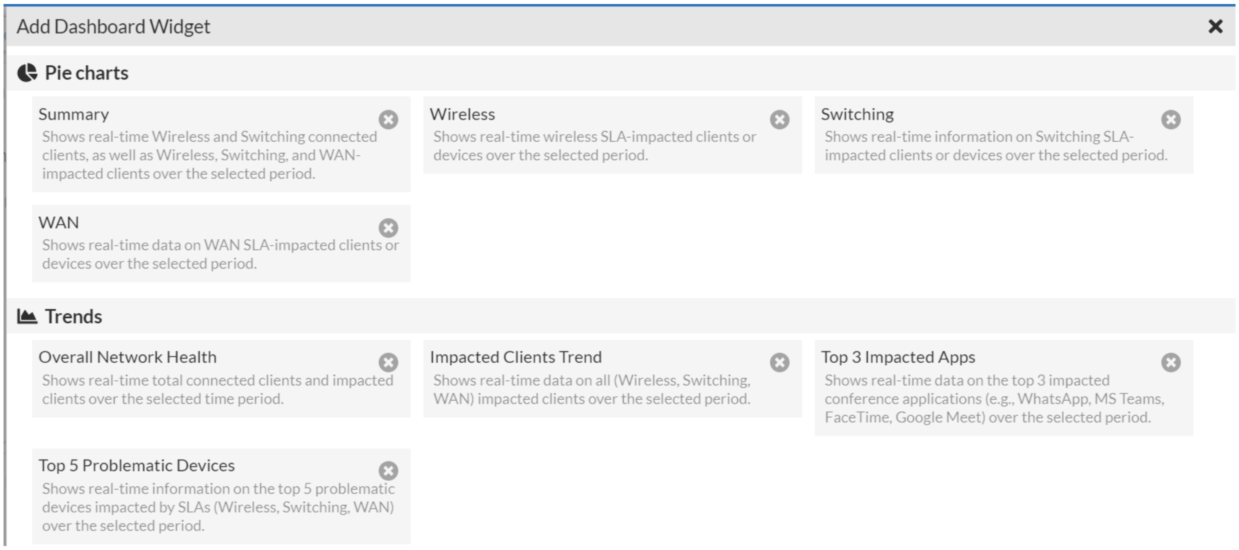


S248E[redacted]	Impacted Clients: 37
2FLB2	Impacted Clients: 35
S424DF[redacted]	Impacted Clients: 20
S424EFT[redacted]	Impacted Clients: 16
[redacted]31F	Impacted Clients: 12

Clicking on the statistics of each of the panels in the dashboard displays detailed data graphically and in a tabular format. The data displayed in tabular format is filterable based on the columns, you can group data by a specific column or filter data for specific values. This is an example.



Dashboard data is refreshed at a configurable interval. Use the **Add Widget** option to manage the widgets displayed on the dashboard; you can choose to add or remove the widgets.



Add Dashboard Widget ✕

Pie charts

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

Wireless ⊗
Shows real-time wireless SLA-impacted clients or devices over the selected period.

Switching ⊗
Shows real-time information on Switching SLA-impacted clients or devices over the selected period.

WAN ⊗
Shows real-time data on WAN SLA-impacted clients or devices over the selected period.

Trends

Overall Network Health ⊗
Shows real-time total connected clients and impacted clients over the selected time period.

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

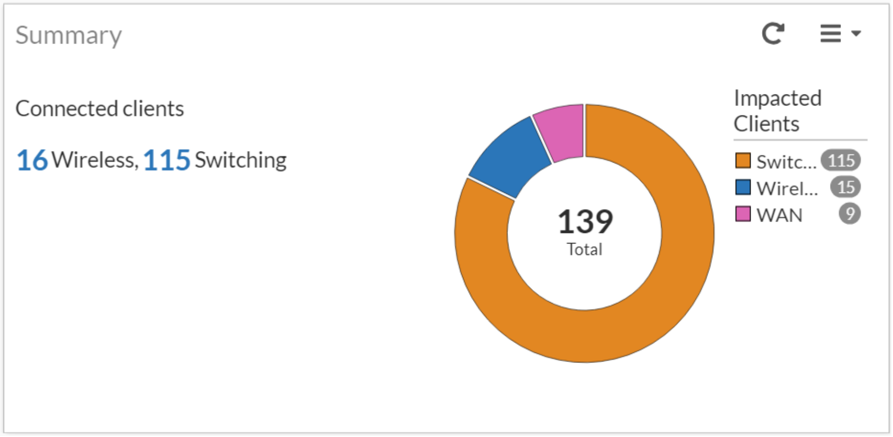
Top 3 Impacted Apps ⊗
Shows real-time data on the top 3 impacted conference applications (e.g., WhatsApp, MS Teams, FaceTime, Google Meet) over the selected period.

Top 5 Problematic Devices ⊗
Shows real-time information on the top 5 problematic devices impacted by SLAs (Wireless, Switching, WAN) over the selected period.

- Summary
- Impacted Clients Trend on page 76
- Overall Network Health
- Top 3 Impacted Apps
- Top 5 Problematic Devices
- Wireless
- WAN
- Switching

Summary

The **Summary** panel displays data in charts and statistics for the total number of connected and impacted clients for switching, wireless, and WAN. FortiAIOps displays the connected and impacted client count during the selected duration in the dashboard. Clicking on the donut chart for the connected clients or the statistics for the impacted clients in this panel, re-directs you to the Impacted Devices page.

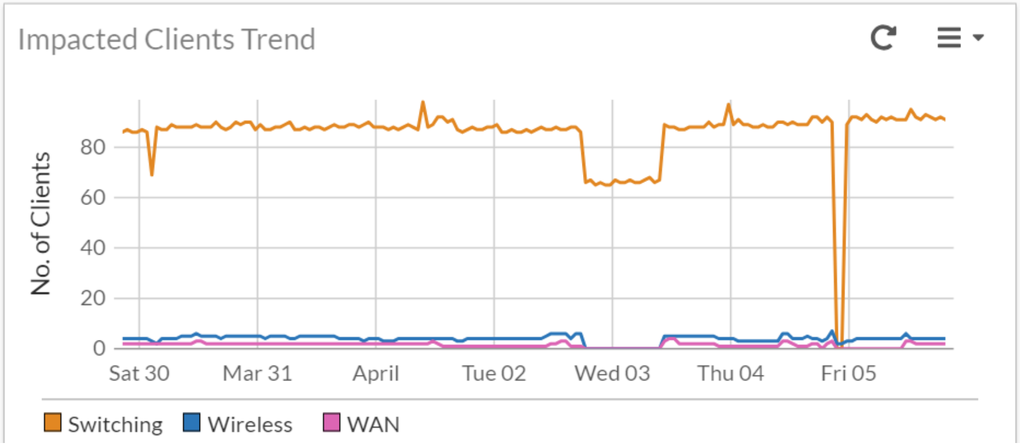


Connected clients

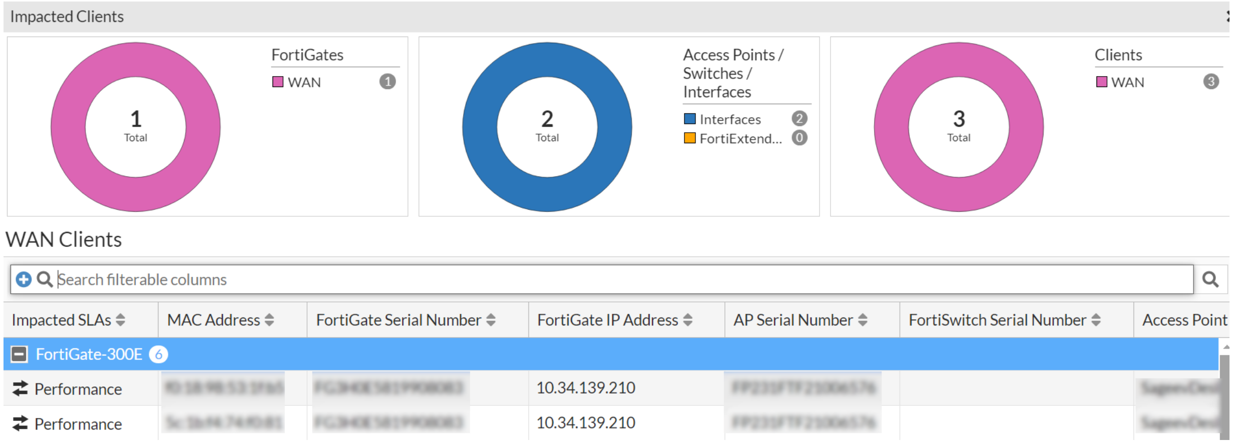
16 Wireless, 115 Switching

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.



Impacted Clients

WAN Clients

Search filterable columns

Impacted SLAs	MAC Address	FortiGate Serial Number	FortiGate IP Address	AP Serial Number	FortiSwitch Serial Number	Access Point
FortiGate-300E 6						
Performance	[redacted]	[redacted]	10.34.139.210	[redacted]		[redacted]
Performance	[redacted]	[redacted]	10.34.139.210	[redacted]		[redacted]

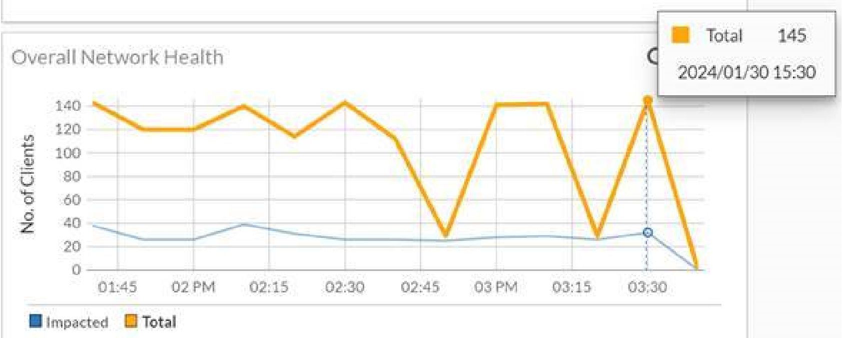
The data is displayed in the following three panels. For more information on the data and fields displayed on this page, see Impacted Devices.

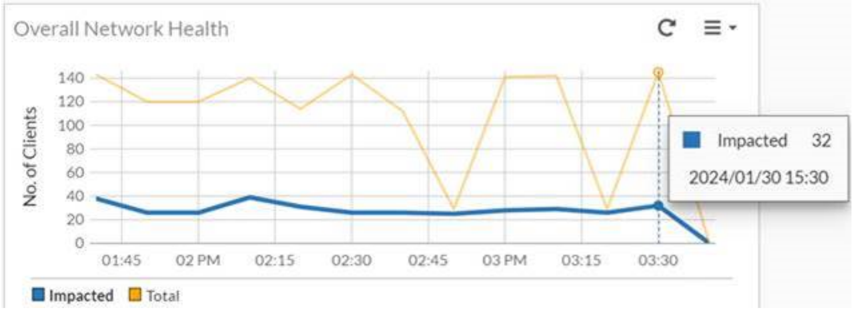
- **FortiGates** - Displays the number of deployed FortiGate controllers with impacted wireless, switching, and WAN clients.
- **Access Points/ Switches/ Interfaces/FortiExtenders** - Displays the number of devices, that is, APs, interfaces, FortiExtenders, and switches with impacted clients.
- **Clients**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

Overall Network Health

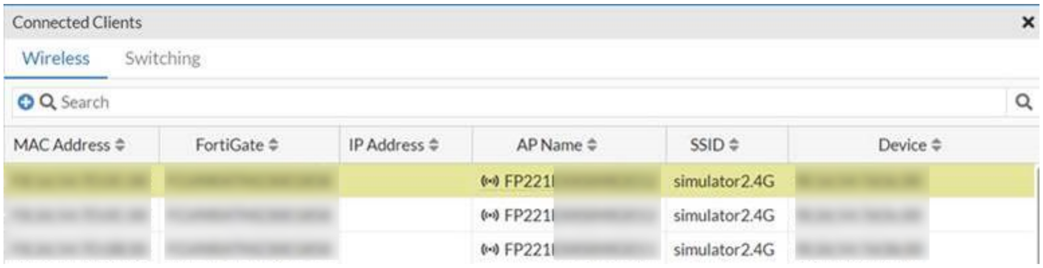
This panel displays the overall client count trends and health status of all wireless, switching, and WAN clients connected to your network, at specific intervals of 15 minutes. You can view the total number of clients in your network and the number of impacted clients at a given point in time.

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.



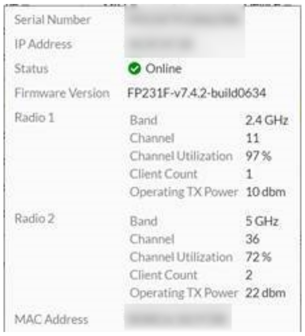


Click on any given time interval for total clients to view the **Connected Clients** panel. The data displayed in tabular format in all the monitor dashboard pages is filterable based on columns, you can group data by a specific column or filter data for specific values.



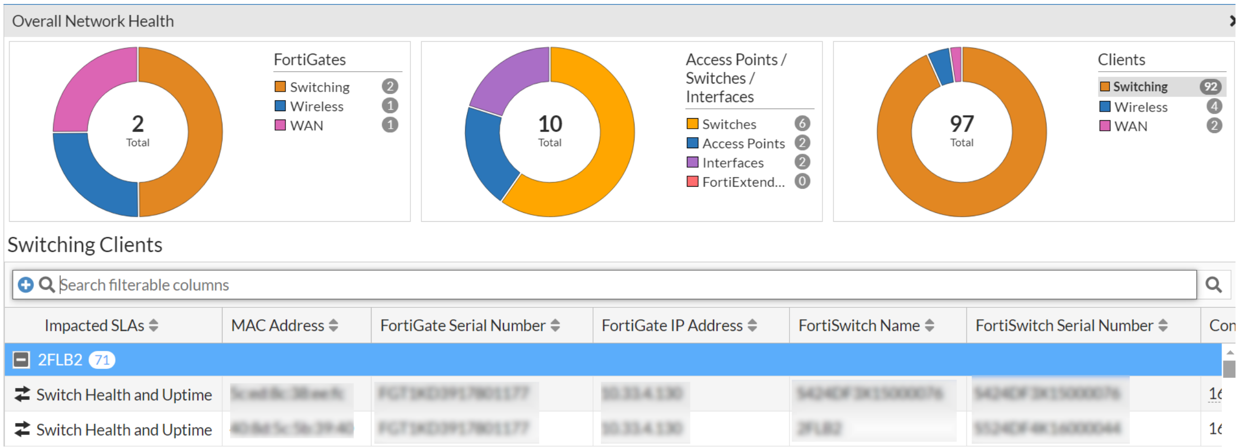
MAC Address	FortiGate	IP Address	AP Name	SSID	Device
[redacted]	[redacted]		FP221[redacted]	simulator2.4G	[redacted]
[redacted]	[redacted]		FP221[redacted]	simulator2.4G	[redacted]
[redacted]	[redacted]		FP221[redacted]	simulator2.4G	[redacted]

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



Serial Number	[redacted]	
IP Address	[redacted]	
Status	✓ Online	
Firmware Version	FP231F-v7.4.2-build0634	
Radio 1	Band	2.4 GHz
	Channel	11
	Channel Utilization	97 %
	Client Count	1
	Operating TX Power	10 dbm
Radio 2	Band	5 GHz
	Channel	36
	Channel Utilization	72 %
	Client Count	2
	Operating TX Power	22 dbm
MAC Address	[redacted]	

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.



Impacted SLAs	MAC Address	FortiGate Serial Number	FortiGate IP Address	FortiSwitch Name	FortiSwitch Serial Number	Con
⊟ 2FLB2 71						
Switch Health and Uptime	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	1(
Switch Health and Uptime	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	1(

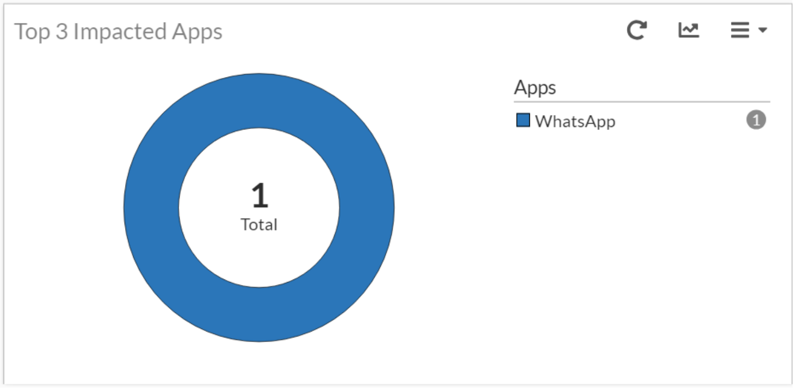
FortiGates - Displays the number of deployed FortiGate controllers with impacted wireless, switching, and WAN clients.

- **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.

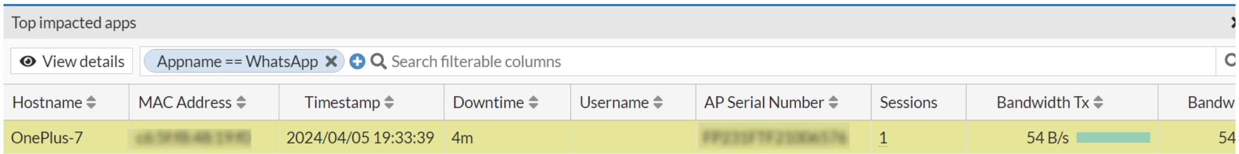
Click on the impacted SLA to view the device topology.

Top 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. To view the details, click on the bar in the chart or on the name of the application displayed in 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.



Top impacted apps

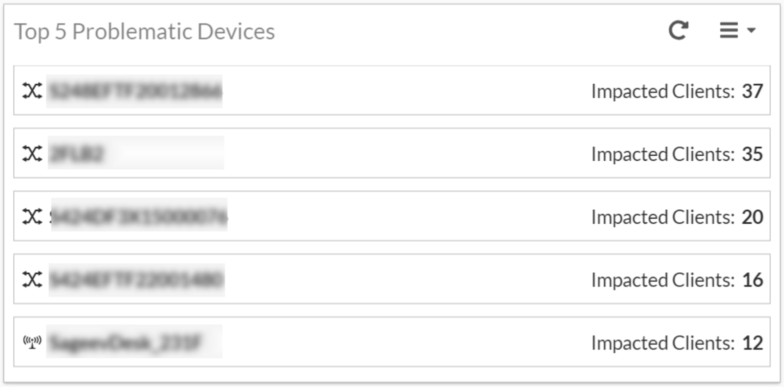
View details | Appname == WhatsApp | Search filterable columns

Hostname	MAC Address	Timestamp	Downtime	Username	AP Serial Number	Sessions	Bandwidth Tx	Bandw
OnePlus-7	[redacted]	2024/04/05 19:33:39	4m		[redacted]	1	54 B/s	54

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

Top 5 Problematic Devices

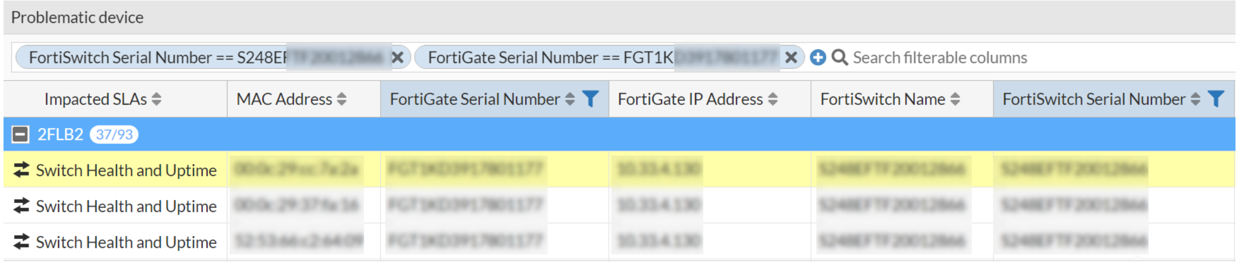
This panel displays the 5 devices with the highest number of impacted clients. The devices displayed here can be FortiAPs, FortiSwitches, FortiExtenders, and/or interfaces. The device name and the number of associated clients that are impacted are displayed in descending order.



Top 5 Problematic Devices

[redacted]	Impacted Clients: 37
[redacted]	Impacted Clients: 35
[redacted]	Impacted Clients: 20
[redacted]	Impacted Clients: 16
[redacted]	Impacted Clients: 12

Click on the device name to view details.



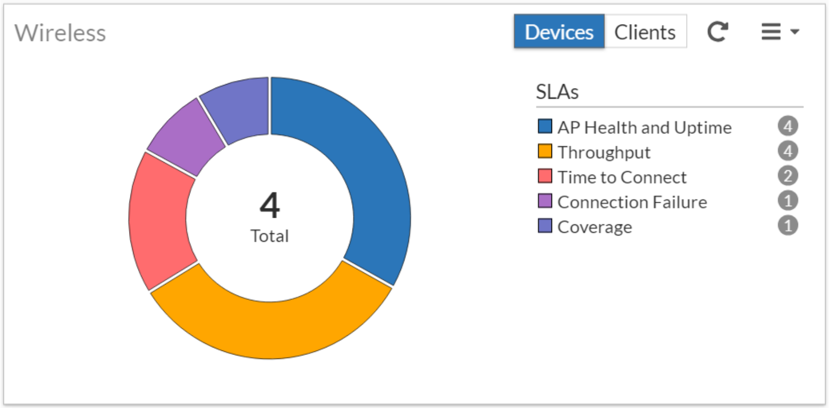
Problematic device

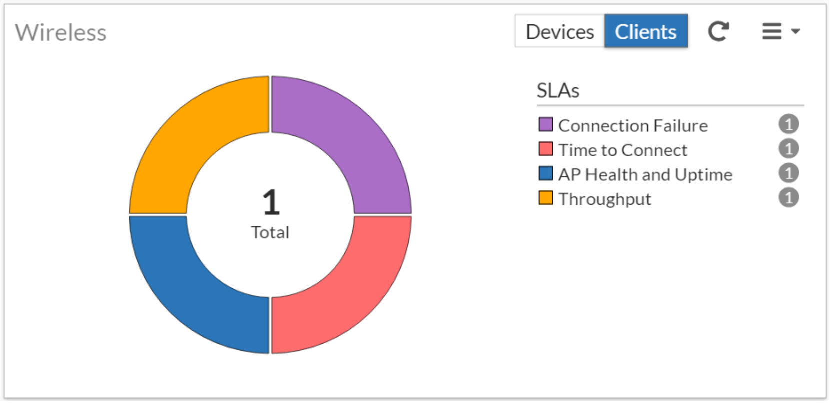
FortiSwitch Serial Number == S248EF[redacted] ✕ FortiGate Serial Number == FGT1K[redacted] ✕ Search filterable columns

Impacted SLAs	MAC Address	FortiGate Serial Number	FortiGate IP Address	FortiSwitch Name	FortiSwitch Serial Number
2FLB2 37/93					
Switch Health and Uptime	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Switch Health and Uptime	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Switch Health and Uptime	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Wireless

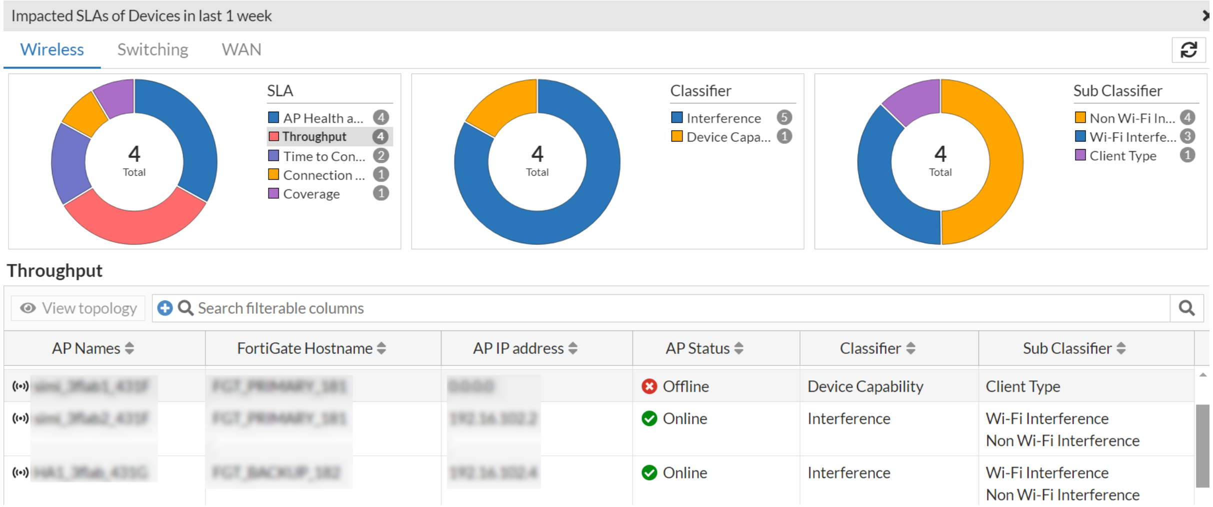
The **Wireless** panel displays the details of impacted SLAs with the associated device and client details. The **Clients** view displays the impacted client count and the **Devices** view displays the impacted AP count.





SLAs, Topology, and Logs

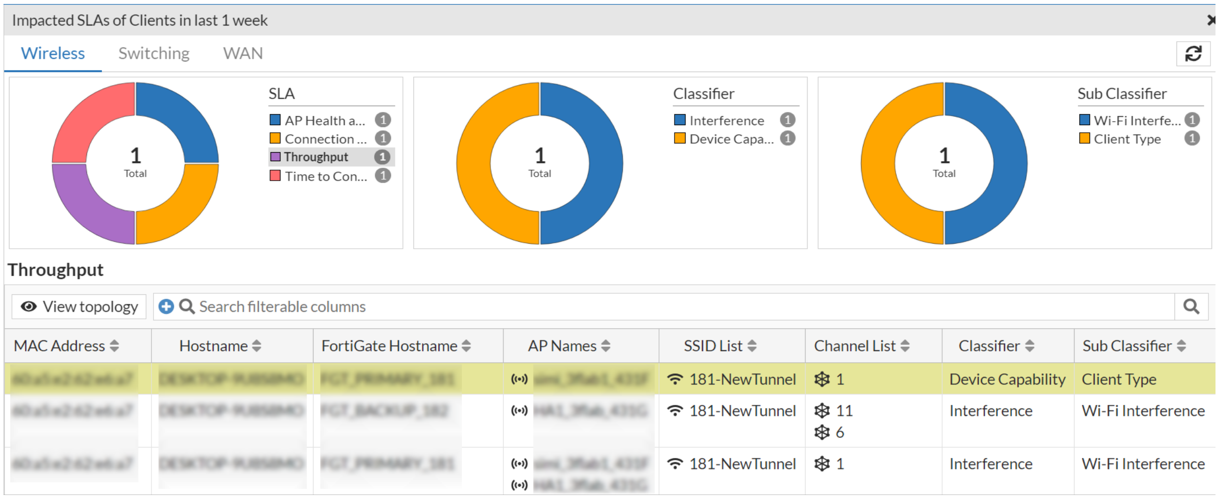
The impacted SLAs are detected and reported by FortiAIOps with device and client details. The issues reported are categorized based on classifiers and sub-classifiers, with suggested remedial measures to curtail the SLA breaches and enhance network performance. The data displayed in this panel is for 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.



Throughput

AP Names	FortiGate Hostname	AP IP address	AP Status	Classifier	Sub Classifier
[redacted]	[redacted]	[redacted]	Offline	Device Capability	Client Type
[redacted]	[redacted]	[redacted]	Online	Interference	Wi-Fi Interference Non Wi-Fi Interference
[redacted]	[redacted]	[redacted]	Online	Interference	Wi-Fi Interference Non Wi-Fi Interference

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.



Throughput

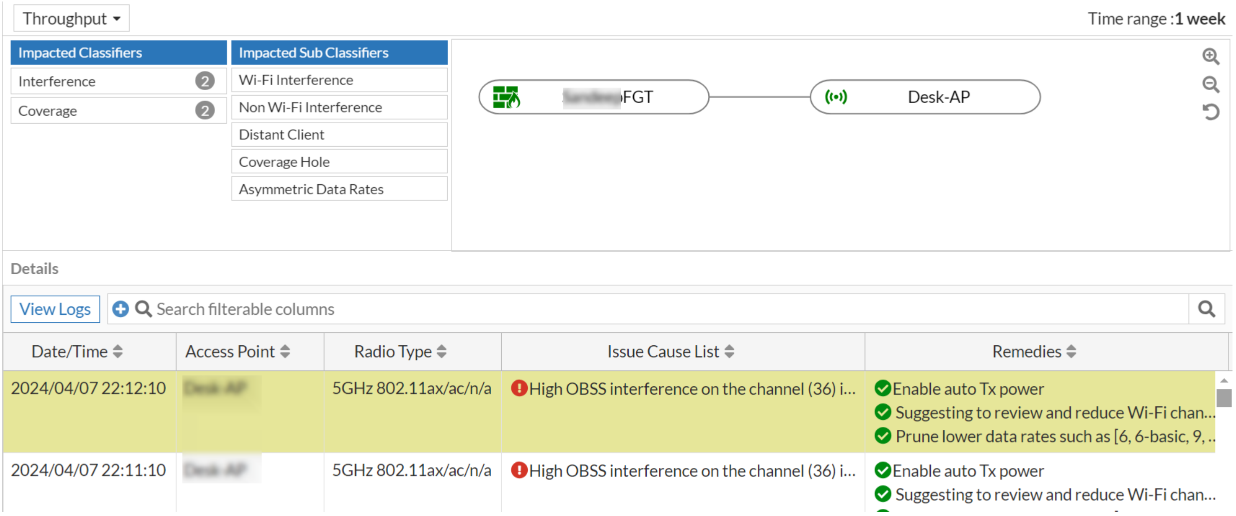
MAC Address	Hostname	FortiGate Hostname	AP Names	SSID List	Channel List	Classifier	Sub Classifier
[redacted]	[redacted]	[redacted]	[redacted]	181-NewTunnel	1	Device Capability	Client Type
[redacted]	[redacted]	[redacted]	[redacted]	181-NewTunnel	11 6	Interference	Wi-Fi Interference
[redacted]	[redacted]	[redacted]	[redacted] [redacted]	181-NewTunnel	1	Interference	Wi-Fi Interference

Select any row and click **View Topology** 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

Throughput

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



Throughput ▾ Time range :**1 week**

Impacted Classifiers	
Interference	2
Coverage	2

Impacted Sub Classifiers
Wi-Fi Interference
Non Wi-Fi Interference
Distant Client
Coverage Hole
Asymmetric Data Rates

Details

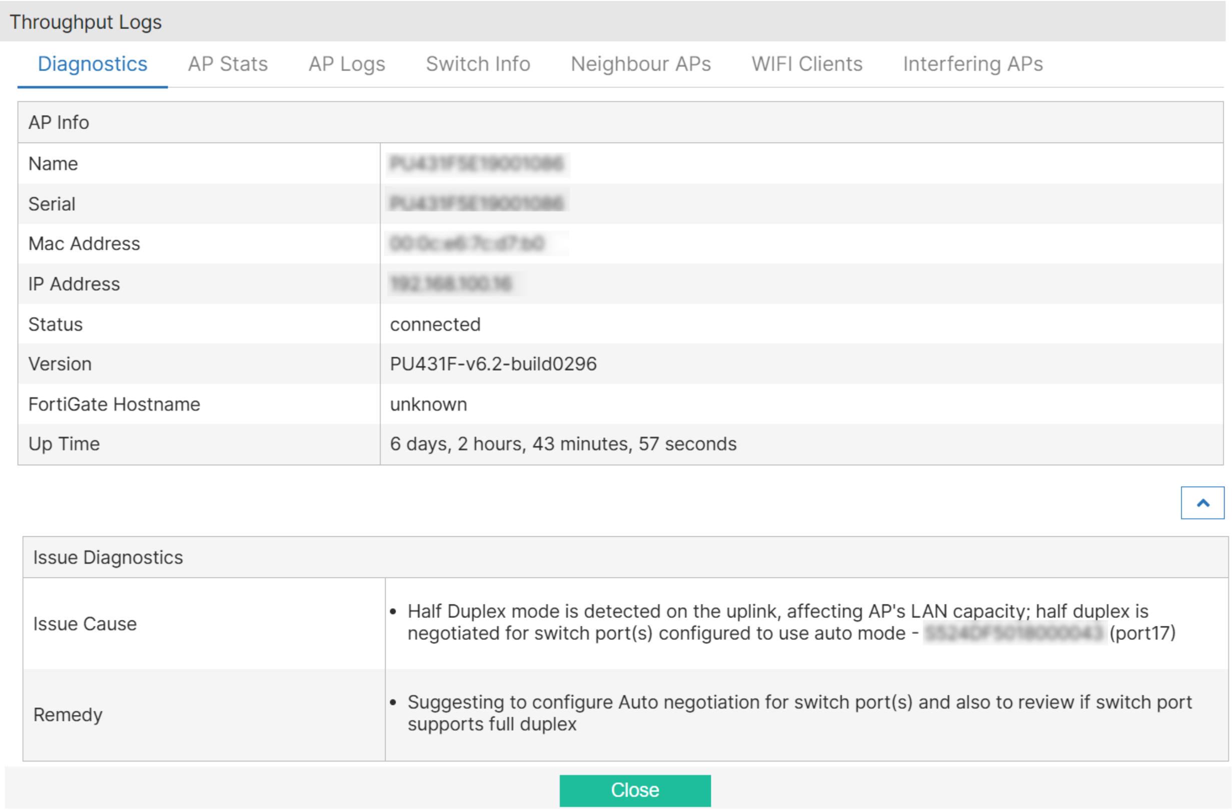
View Logs Search filterable columns

Date/Time	Access Point	Radio Type	Issue Cause List	Remedies
2024/04/07 22:12:10	[redacted]	5GHz 802.11ax/ac/n/a	High OBSS interference on the channel (36) i...	✓ Enable auto Tx power ✓ Suggesting to review and reduce Wi-Fi chan... ✓ Prune lower data rates such as [6, 6-basic, 9, ..
2024/04/07 22:11:10	[redacted]	5GHz 802.11ax/ac/n/a	High OBSS interference on the channel (36) i...	✓ Enable auto Tx power ✓ Suggesting to review and reduce Wi-Fi chan...

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.

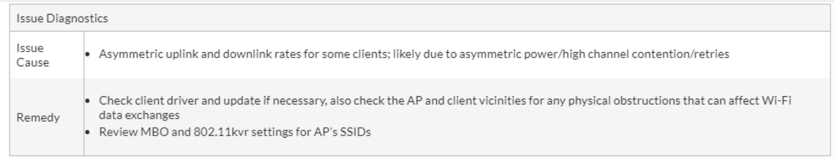
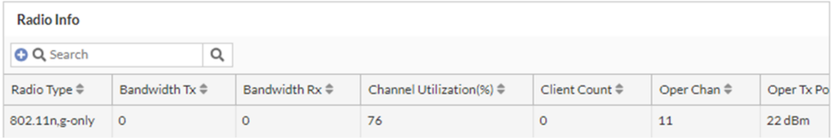
Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
Classifiers	The classifier of the issue reported for the SLA.
Sub Classifiers	The sub-classifier of the issue for the reported classifier.
Impacted Client Count	The number of impacted clients.
Issue Cause List	Detailed 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.

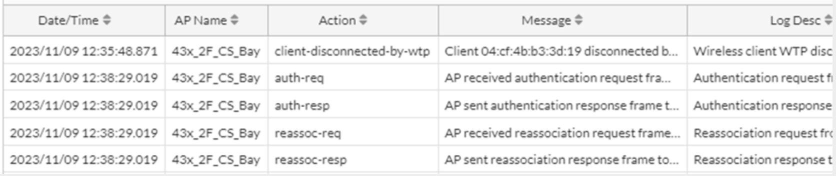
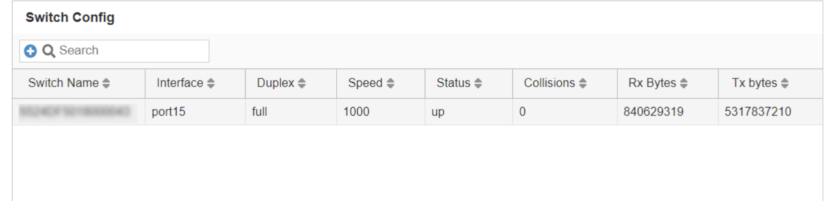
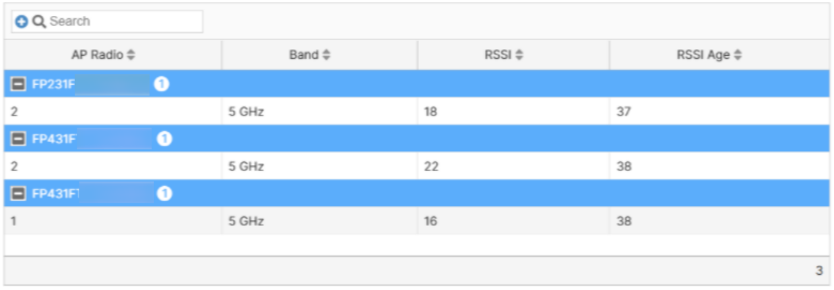
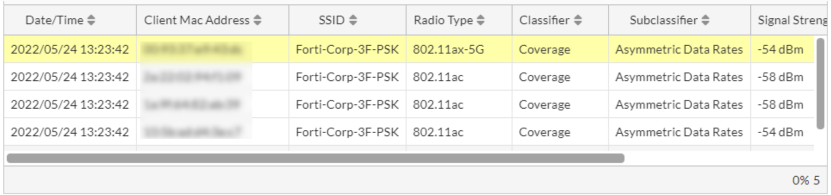
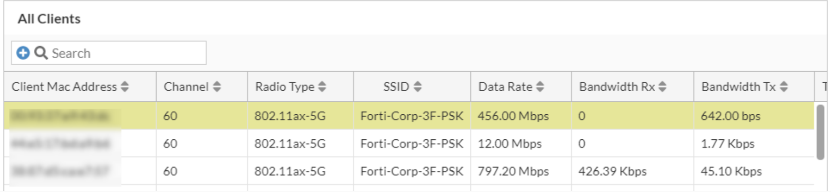
In the impacted details displayed, select a specific row of throughput failure and click **View Details**. You can view details of the impacted AP and issue diagnostics. You can view throughput logs related to **Diagnostics** with the issue description and the suggested remediation, **AP Stats** with 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.

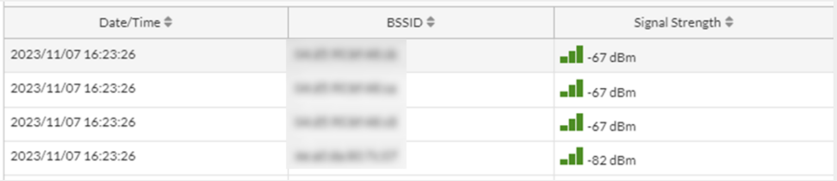


AP Info	
Name	[redacted]
Serial	[redacted]
Mac Address	[redacted]
IP Address	[redacted]
Status	connected
Version	PU431F-v6.2-build0296
FortiGate Hostname	unknown
Up Time	6 days, 2 hours, 43 minutes, 57 seconds

Issue Diagnostics	
Issue Cause	• Half Duplex mode is detected on the uplink, affecting AP's LAN capacity; half duplex is negotiated for switch port(s) configured to use auto mode - [redacted] (port17)
Remedy	• Suggesting to configure Auto negotiation for switch port(s) and also to review if switch port supports full duplex

<table>
<tr><th>Logs</th><th>Description</th></tr>
<tr><td><b>Diagnostics</b></td><td>This tab provides detailed cause of the SLA breach that impacted the client/AP/FortiGate. FortiAIOps also suggests the remedy to resolve the issue.

<table>
<tr><th colspan="2">Issue Diagnostics</th></tr>
<tr><td>Issue Cause</td><td>• Asymmetric uplink and downlink rates for some clients; likely due to asymmetric power/high channel contention/retries</td></tr>
<tr><td>Remedy</td><td>• Check client driver and update if necessary, also check the AP and client vicinities for any physical obstructions that can affect Wi-Fi data exchanges
• Review MBO and 802.11kvr settings for AP's SSIDs</td></tr>
</table></td></tr>
<tr><td><b>AP Stats</b></td><td>This tab displays the details of the AP radio that the client associated with and the WAN status details of the AP.

Radio Info
<table>
<tr><th>Radio Type</th><th>Bandwidth Tx</th><th>Bandwidth Rx</th><th>Channel Utilization(%)</th><th>Client Count</th><th>Oper Chan</th><th>Oper Tx Po</th></tr>
<tr><td>802.11n,g-only</td><td>0</td><td>0</td><td>76</td><td>0</td><td>11</td><td>22 dBm</td></tr>
</table></td></tr>
</table>

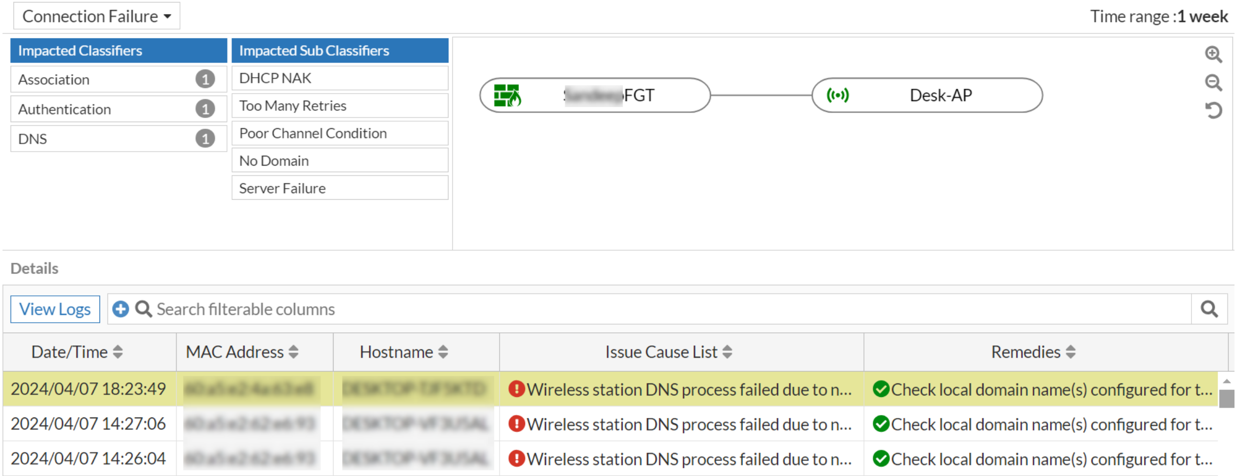
<table>
<tr><th>Logs</th><th>Description</th></tr>
<tr><td><b>AP Logs</b></td><td>This tab provides the AP event logs generated from FortiGate.

<table>
<tr><th>Date/Time ⇕</th><th>AP Name ⇕</th><th>Action ⇕</th><th>Message ⇕</th><th>Log Desc ⇕</th></tr>
<tr><td>2023/11/09 12:35:48.871</td><td>43x_2F_CS_Bay</td><td>client-disconnected-by-wtp</td><td>Client 04:cf:4b:b3:3d:19 disconnected b...</td><td>Wireless client WTP disc</td></tr>
<tr><td>2023/11/09 12:38:29.019</td><td>43x_2F_CS_Bay</td><td>auth-req</td><td>AP received authentication request fra...</td><td>Authentication request fi</td></tr>
<tr><td>2023/11/09 12:38:29.019</td><td>43x_2F_CS_Bay</td><td>auth-resp</td><td>AP sent authentication response frame t...</td><td>Authentication response</td></tr>
<tr><td>2023/11/09 12:38:29.019</td><td>43x_2F_CS_Bay</td><td>reassoc-req</td><td>AP received reassociation request frame...</td><td>Reassociation request fro</td></tr>
<tr><td>2023/11/09 12:38:29.019</td><td>43x_2F_CS_Bay</td><td>reassoc-resp</td><td>AP sent reassociation response frame to...</td><td>Reassociation response t</td></tr>
</table></td></tr>
<tr><td><b>Switch Info</b></td><td>This tab displays the configuration details of the switch port connected to the AP.

Switch Config
Search
<table>
<tr><th>Switch Name ⇕</th><th>Interface ⇕</th><th>Duplex ⇕</th><th>Speed ⇕</th><th>Status ⇕</th><th>Collisions ⇕</th><th>Rx Bytes ⇕</th><th>Tx bytes ⇕</th></tr>
<tr><td>[redacted]</td><td>port15</td><td>full</td><td>1000</td><td>up</td><td>0</td><td>840629319</td><td>5317837210</td></tr>
</table></td></tr>
<tr><td><b>Neighbour APs</b></td><td>This tab displays details of the detected neighbour APs by the client, for distant client & coverage hole issues.

Search
<table>
<tr><th>AP Radio ⇕</th><th>Band ⇕</th><th>RSSI ⇕</th><th>RSSI Age ⇕</th></tr>
<tr><td>⊟ FP231F [redacted] 1</td><td></td><td></td><td></td></tr>
<tr><td>2</td><td>5 GHz</td><td>18</td><td>37</td></tr>
<tr><td>⊟ FP431F [redacted] 1</td><td></td><td></td><td></td></tr>
<tr><td>2</td><td>5 GHz</td><td>22</td><td>38</td></tr>
<tr><td>⊟ FP431F [redacted] 1</td><td></td><td></td><td></td></tr>
<tr><td>1</td><td>5 GHz</td><td>16</td><td>38</td></tr>
</table>
3</td></tr>
<tr><td><b>WIFI Clients</b></td><td>This tab provides details of the impacted clients and also lists all the clients associated with the AP.

<table>
<tr><th>Date/Time ⇕</th><th>Client Mac Address ⇕</th><th>SSID ⇕</th><th>Radio Type ⇕</th><th>Classifier ⇕</th><th>Subclassifier ⇕</th><th>Signal Streng</th></tr>
<tr><td>2022/05/24 13:23:42</td><td>[redacted]</td><td>Forti-Corp-3F-PSK</td><td>802.11ax-5G</td><td>Coverage</td><td>Asymmetric Data Rates</td><td>-54 dBm</td></tr>
<tr><td>2022/05/24 13:23:42</td><td>[redacted]</td><td>Forti-Corp-3F-PSK</td><td>802.11ac</td><td>Coverage</td><td>Asymmetric Data Rates</td><td>-58 dBm</td></tr>
<tr><td>2022/05/24 13:23:42</td><td>[redacted]</td><td>Forti-Corp-3F-PSK</td><td>802.11ac</td><td>Coverage</td><td>Asymmetric Data Rates</td><td>-58 dBm</td></tr>
<tr><td>2022/05/24 13:23:42</td><td>[redacted]</td><td>Forti-Corp-3F-PSK</td><td>802.11ac</td><td>Coverage</td><td>Asymmetric Data Rates</td><td>-54 dBm</td></tr>
</table>
0% 5

All Clients
Search
<table>
<tr><th>Client Mac Address ⇕</th><th>Channel ⇕</th><th>Radio Type ⇕</th><th>SSID ⇕</th><th>Data Rate ⇕</th><th>Bandwidth Rx ⇕</th><th>Bandwidth Tx ⇕</th><th>T</th></tr>
<tr><td>[redacted]</td><td>60</td><td>802.11ax-5G</td><td>Forti-Corp-3F-PSK</td><td>456.00 Mbps</td><td>0</td><td>642.00 bps</td><td></td></tr>
<tr><td>[redacted]</td><td>60</td><td>802.11ax-5G</td><td>Forti-Corp-3F-PSK</td><td>12.00 Mbps</td><td>0</td><td>1.77 Kbps</td><td></td></tr>
<tr><td>[redacted]</td><td>60</td><td>802.11ax-5G</td><td>Forti-Corp-3F-PSK</td><td>797.20 Mbps</td><td>426.39 Kbps</td><td>45.10 Kbps</td><td></td></tr>
</table></td></tr>
<tr><td><b>Interfering APs</b></td><td>This tab displays details of the interfering APs in your network.</td></tr>
</table>

Logs	Description
	

Date/Time ⇕	BSSID ⇕	Signal Strength ⇕
2023/11/07 16:23:26	[redacted]	-67 dBm
2023/11/07 16:23:26	[redacted]	-67 dBm
2023/11/07 16:23:26	[redacted]	-67 dBm
2023/11/07 16:23:26	[redacted]	-82 dBm

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.



Connection Failure ▾

Time range :**1 week**

Impacted Classifiers	
Association	1
Authentication	1
DNS	1

Impacted Sub Classifiers
DHCP NAK
Too Many Retries
Poor Channel Condition
No Domain
Server Failure

Details

View Logs

Search filterable columns

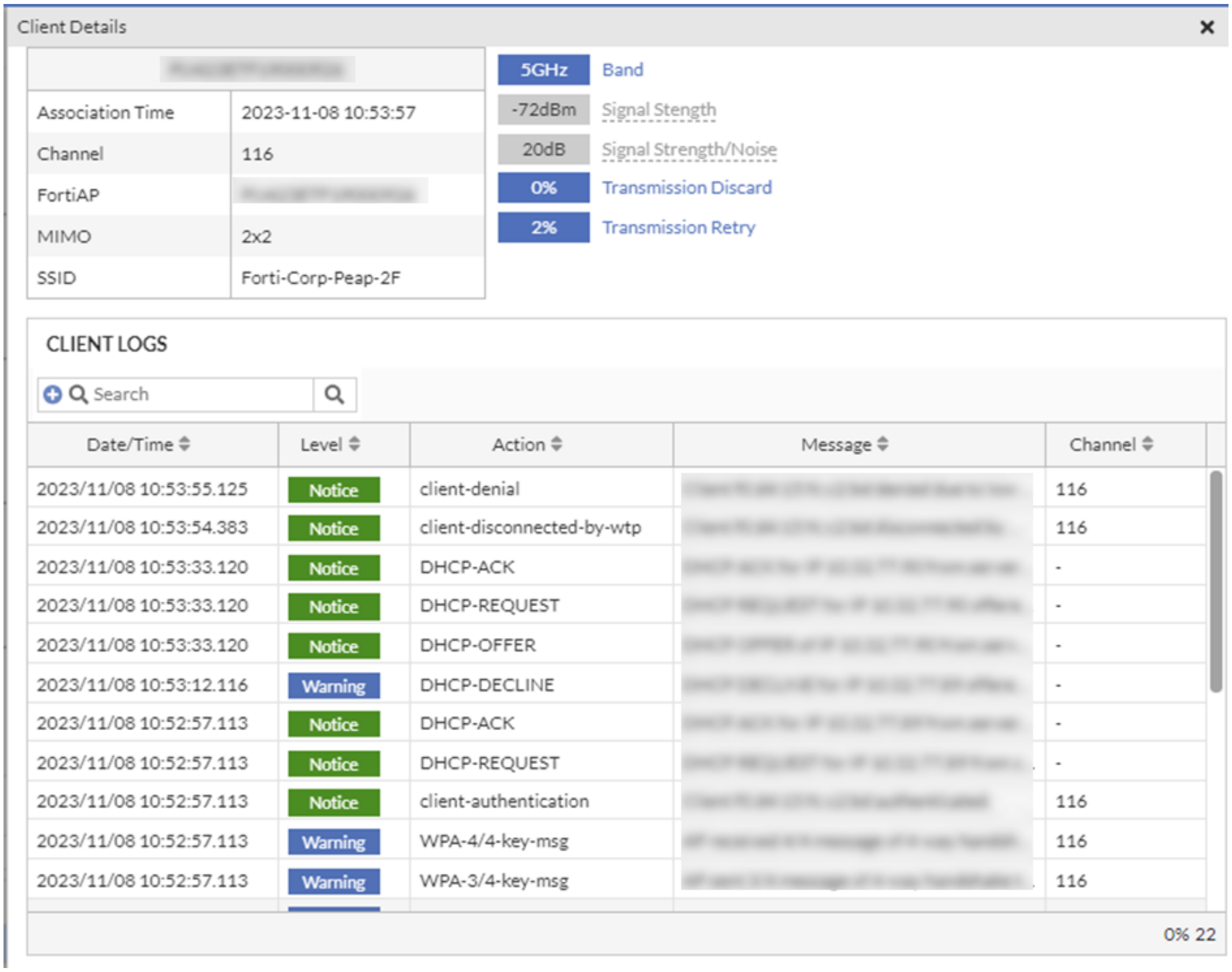
Date/Time ⇕	MAC Address ⇕	Hostname ⇕	Issue Cause List ⇕	Remedies ⇕
2024/04/07 18:23:49	[redacted]	[redacted]	Wireless station DNS process failed due to n...	Check local domain name(s) configured for t...
2024/04/07 14:27:06	[redacted]	[redacted]	Wireless station DNS process failed due to n...	Check local domain name(s) configured for t...
2024/04/07 14:26:04	[redacted]	[redacted]	Wireless station DNS process failed due to n...	Check local domain name(s) configured for t...

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.



Client Details ✕

[redacted]	
Association Time	2023-11-08 10:53:57
Channel	116
FortiAP	[redacted]
MIMO	2x2
SSID	Forti-Corp-Peap-2F

5GHz	Band
-72dBm	Signal Stength
20dB	Signal Strength/Noise
0%	Transmission Discard
2%	Transmission Retry

CLIENT LOGS

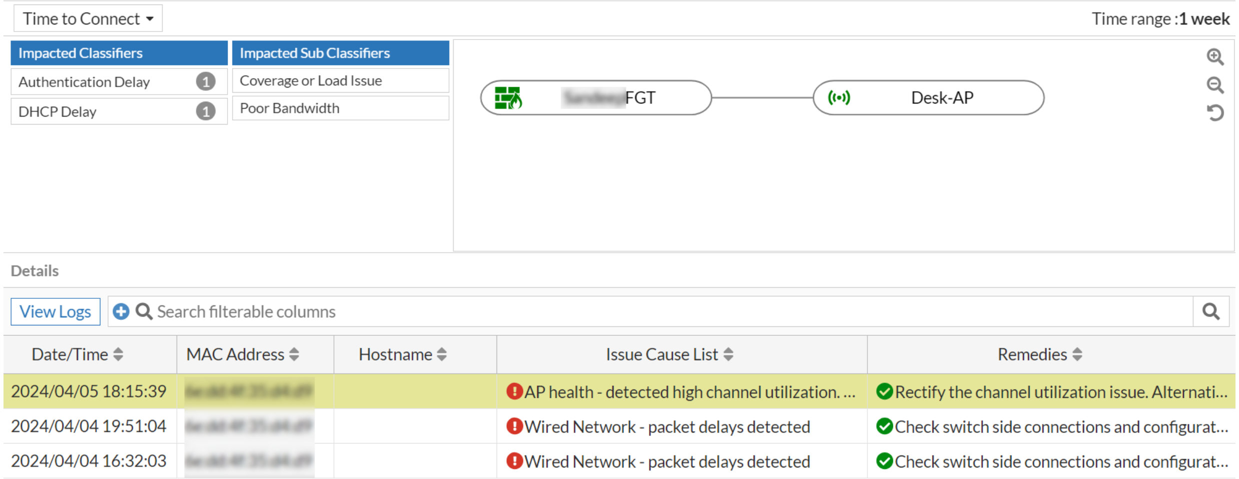
Date/Time	Level	Action	Message	Channel
2023/11/08 10:53:55.125	Notice	client-denial	[redacted]	116
2023/11/08 10:53:54.383	Notice	client-disconnected-by-wtp	[redacted]	116
2023/11/08 10:53:33.120	Notice	DHCP-ACK	[redacted]	-
2023/11/08 10:53:33.120	Notice	DHCP-REQUEST	[redacted]	-
2023/11/08 10:53:33.120	Notice	DHCP-OFFER	[redacted]	-
2023/11/08 10:53:12.116	Warning	DHCP-DECLINE	[redacted]	-
2023/11/08 10:52:57.113	Notice	DHCP-ACK	[redacted]	-
2023/11/08 10:52:57.113	Notice	DHCP-REQUEST	[redacted]	-
2023/11/08 10:52:57.113	Notice	client-authentication	[redacted]	116
2023/11/08 10:52:57.113	Warning	WPA-4/4-key-msg	[redacted]	116
2023/11/08 10:52:57.113	Warning	WPA-3/4-key-msg	[redacted]	116

0% 22

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



Time to Connect ▾

Time range :**1 week**

Impacted Classifiers	
Authentication Delay	1
DHCP Delay	1

Impacted Sub Classifiers
Coverage or Load Issue
Poor Bandwidth

Details

View Logs | Search filterable columns

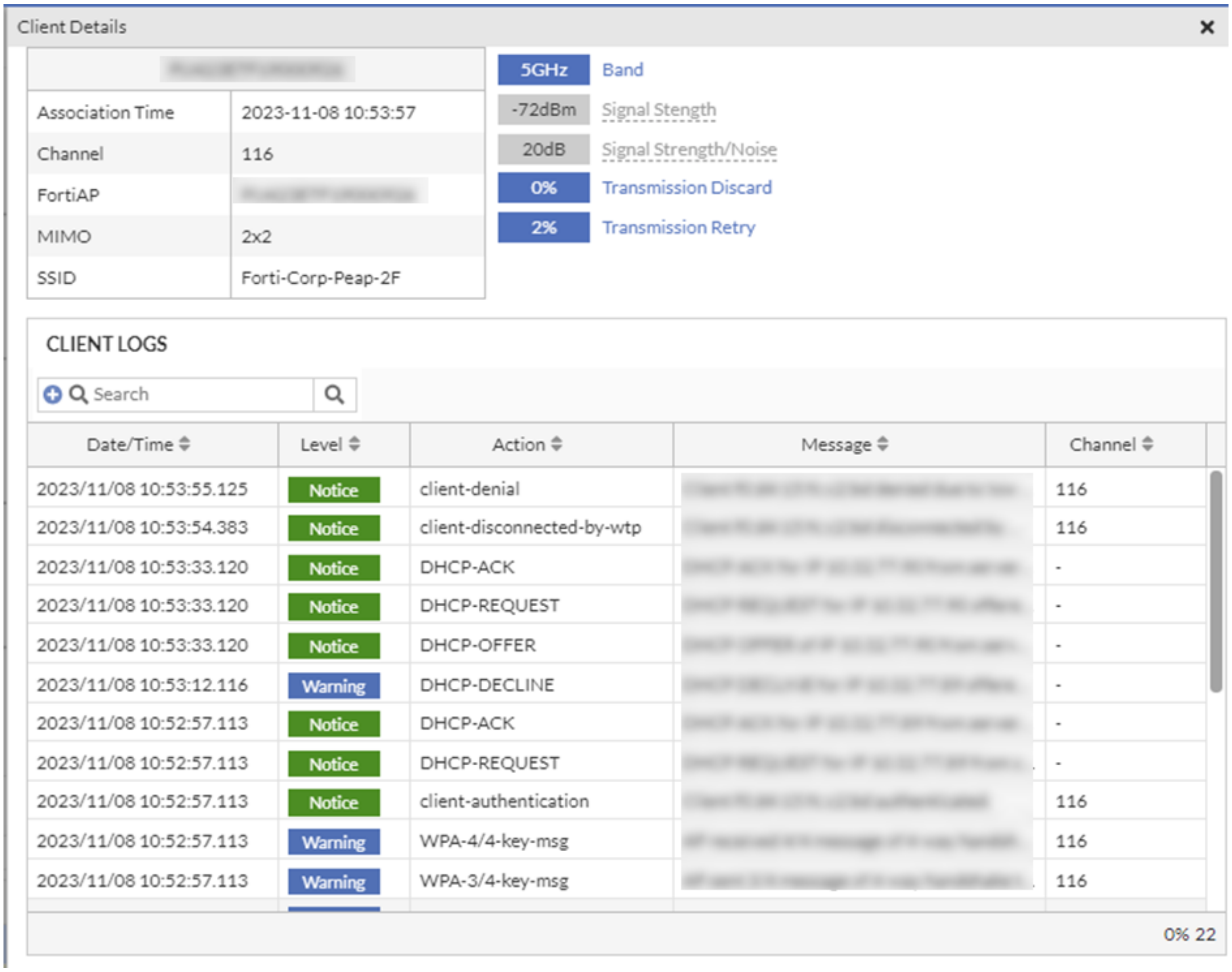
Date/Time	MAC Address	Hostname	Issue Cause List	Remedies
2024/04/05 18:15:39	[redacted]		AP health - detected high channel utilization. ...	Rectify the channel utilization issue. Alternati...
2024/04/04 19:51:04	[redacted]		Wired Network - packet delays detected	Check switch side connections and configurat...
2024/04/04 16:32:03	[redacted]		Wired Network - packet delays detected	Check switch side connections and configurat...

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.

Attribute	Description
Authentication Delay	The authentication delay measured in milliseconds.
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.



[redacted]	
Association Time	2023-11-08 10:53:57
Channel	116
FortiAP	[redacted]
MIMO	2x2
SSID	Forti-Corp-Peap-2F

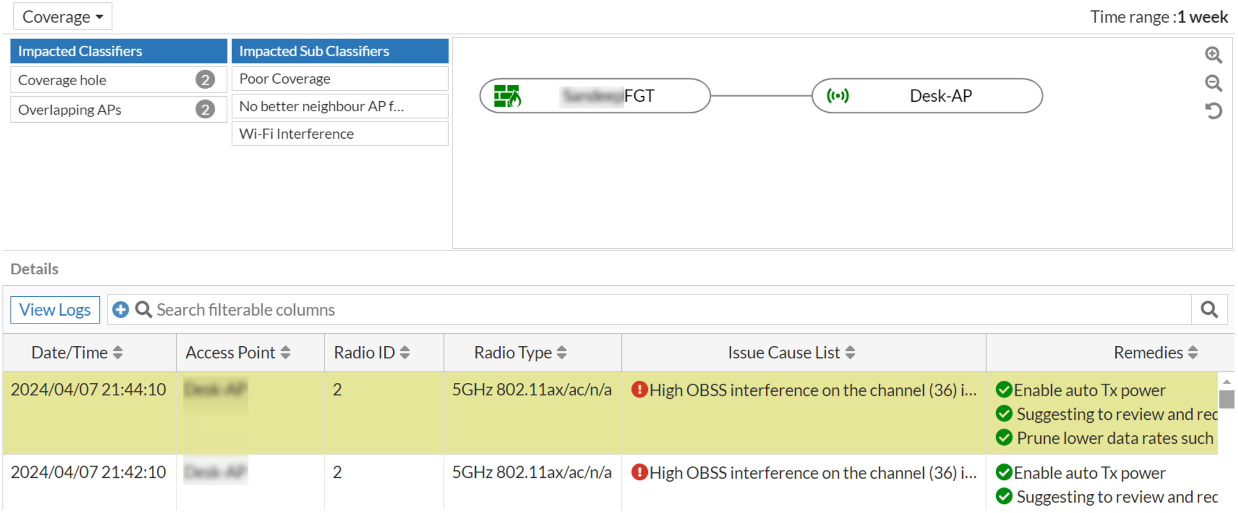
5GHz	Band
-72dBm	Signal Stength
20dB	Signal Strength/Noise
0%	Transmission Discard
2%	Transmission Retry

CLIENT LOGS

Date/Time	Level	Action	Message	Channel
2023/11/08 10:53:55.125	Notice	client-denial	[redacted]	116
2023/11/08 10:53:54.383	Notice	client-disconnected-by-wtp	[redacted]	116
2023/11/08 10:53:33.120	Notice	DHCP-ACK	[redacted]	-
2023/11/08 10:53:33.120	Notice	DHCP-REQUEST	[redacted]	-
2023/11/08 10:53:33.120	Notice	DHCP-OFFER	[redacted]	-
2023/11/08 10:53:12.116	Warning	DHCP-DECLINE	[redacted]	-
2023/11/08 10:52:57.113	Notice	DHCP-ACK	[redacted]	-
2023/11/08 10:52:57.113	Notice	DHCP-REQUEST	[redacted]	-
2023/11/08 10:52:57.113	Notice	client-authentication	[redacted]	116
2023/11/08 10:52:57.113	Warning	WPA-4/4-key-msg	[redacted]	116
2023/11/08 10:52:57.113	Warning	WPA-3/4-key-msg	[redacted]	116

Coverage

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



Impacted Classifiers	
Coverage hole	2
Overlapping APs	2

Impacted Sub Classifiers
Poor Coverage
No better neighbour AP f...
Wi-Fi Interference

Details

View Logs | Search filterable columns

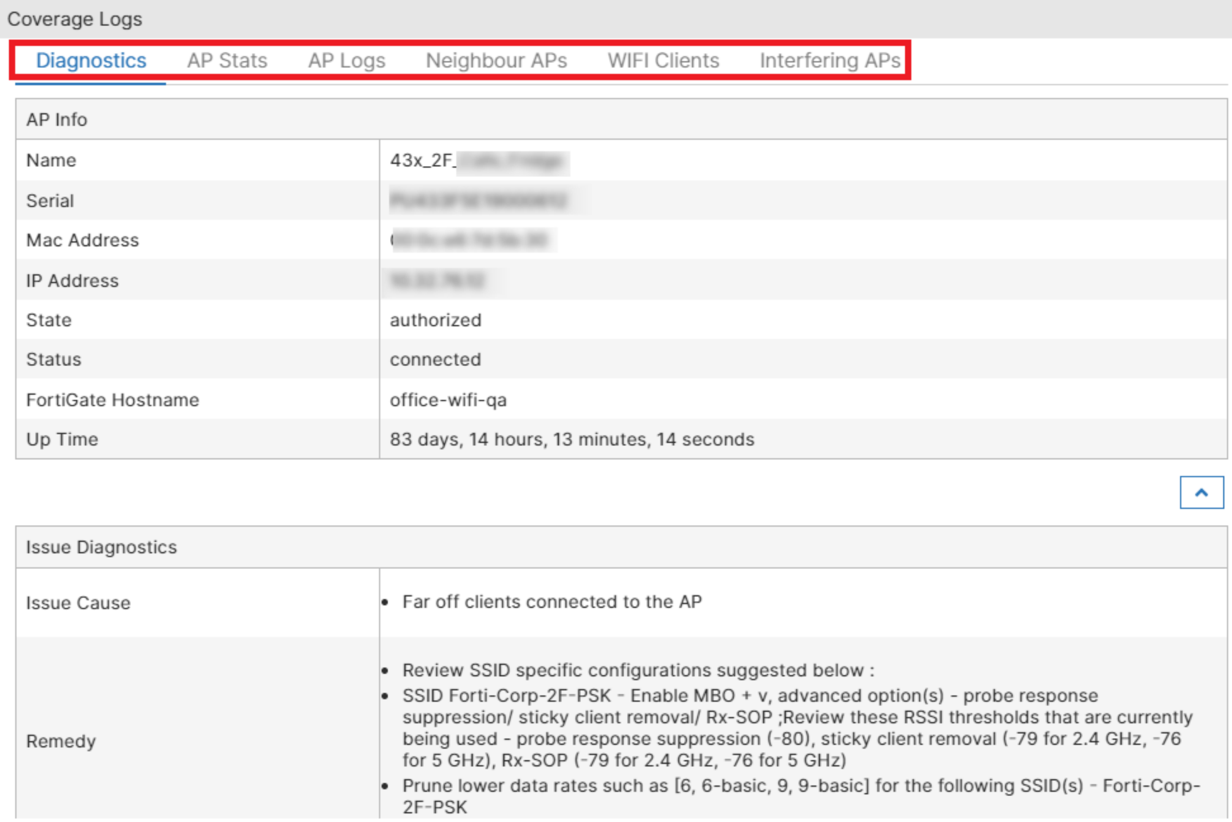
Date/Time	Access Point	Radio ID	Radio Type	Issue Cause List	Remedies
2024/04/07 21:44:10	[redacted]	2	5GHz 802.11ax/ac/n/a	High OBSS interference on the channel (36) i...	✓ Enable auto Tx power ✓ Suggesting to review and rec ✓ Prune lower data rates such
2024/04/07 21:42:10	[redacted]	2	5GHz 802.11ax/ac/n/a	High OBSS interference on the channel (36) i...	✓ Enable auto Tx power ✓ Suggesting to review and rec

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.

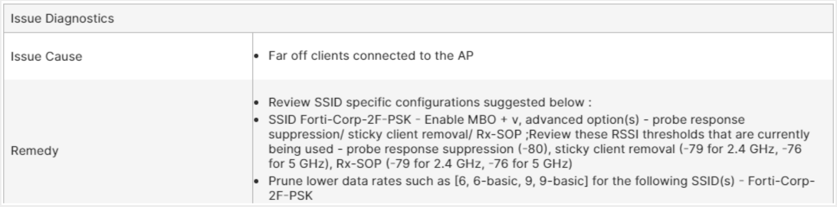
Attribute	Description
Impacted Client Count	The number of impacted clients.
Interfering AP	The list of interfering APs in the network.

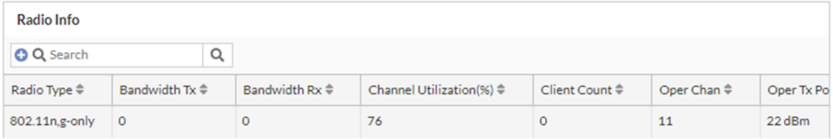
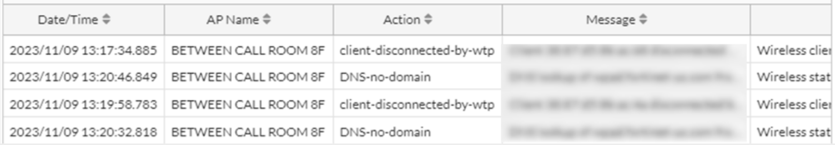
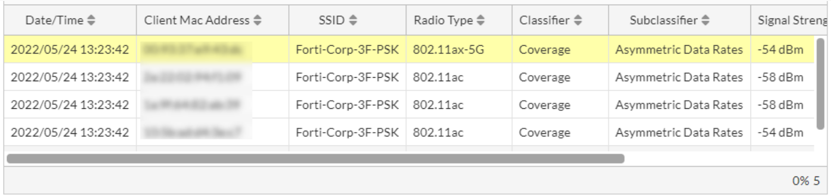
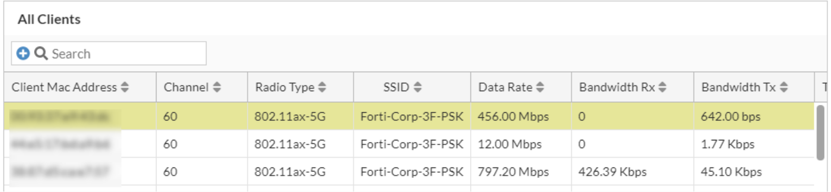
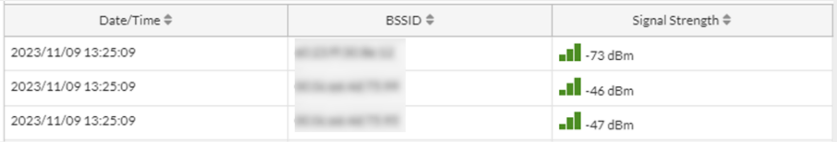
To view the logs, select a specific row of an AP event and click **View Logs**. You can view coverage logs related to **Diagnostics** with the issue description and the suggested remediation, **AP Stats** with the associated AP radio details, **AP Logs** with the time of the throughput failure event 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.



AP Info	
Name	43x_2F_[redacted]
Serial	[redacted]
Mac Address	[redacted]
IP Address	[redacted]
State	authorized
Status	connected
FortiGate Hostname	office-wifi-qa
Up Time	83 days, 14 hours, 13 minutes, 14 seconds

Issue Diagnostics	
Issue Cause	• Far off clients connected to the AP
Remedy	• Review SSID specific configurations suggested below : • SSID Forti-Corp-2F-PSK - Enable MBO + v, advanced option(s) - probe response suppression/ sticky client removal/ Rx-SOP ;Review these RSSI thresholds that are currently being used - probe response suppression (-80), sticky client removal (-79 for 2.4 GHz, -76 for 5 GHz), Rx-SOP (-79 for 2.4 GHz, -76 for 5 GHz) • Prune lower data rates such as [6, 6-basic, 9, 9-basic] for the following SSID(s) - Forti-Corp-2F-PSK

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.  Issue Diagnostics Issue Cause: • Far off clients connected to the AP Remedy: • Review SSID specific configurations suggested below : • SSID Forti-Corp-2F-PSK - Enable MBO + v, advanced option(s) - probe response suppression/ sticky client removal/ Rx-SOP ;Review these RSSI thresholds that are currently being used - probe response suppression (-80), sticky client removal (-79 for 2.4 GHz, -76 for 5 GHz), Rx-SOP (-79 for 2.4 GHz, -76 for 5 GHz) • Prune lower data rates such as [6, 6-basic, 9, 9-basic] for the following SSID(s) - Forti-Corp-2F-PSK

<table>
<tr><th>Logs</th><th>Description</th></tr>
<tr><td><b>AP Stats</b></td><td>This tab displays the details of the AP radio that the client associated with and the WAN status details of the AP.

Radio Info
<table>
<tr><th>Radio Type</th><th>Bandwidth Tx</th><th>Bandwidth Rx</th><th>Channel Utilization(%)</th><th>Client Count</th><th>Oper Chan</th><th>Oper Tx Po</th></tr>
<tr><td>802.11n,g-only</td><td>0</td><td>0</td><td>76</td><td>0</td><td>11</td><td>22 dBm</td></tr>
</table>
</td></tr>
<tr><td><b>AP Logs</b></td><td>This tab provides the AP event logs generated from FortiGate.

<table>
<tr><th>Date/Time</th><th>AP Name</th><th>Action</th><th>Message</th><th></th></tr>
<tr><td>2023/11/09 13:17:34.885</td><td>BETWEEN CALL ROOM 8F</td><td>client-disconnected-by-wtp</td><td>[redacted]</td><td>Wireless clie</td></tr>
<tr><td>2023/11/09 13:20:46.849</td><td>BETWEEN CALL ROOM 8F</td><td>DNS-no-domain</td><td>[redacted]</td><td>Wireless stat</td></tr>
<tr><td>2023/11/09 13:19:58.783</td><td>BETWEEN CALL ROOM 8F</td><td>client-disconnected-by-wtp</td><td>[redacted]</td><td>Wireless clie</td></tr>
<tr><td>2023/11/09 13:20:32.818</td><td>BETWEEN CALL ROOM 8F</td><td>DNS-no-domain</td><td>[redacted]</td><td>Wireless stat</td></tr>
</table>
</td></tr>
<tr><td><b>WIFI Clients</b></td><td>This tab provides details of the impacted clients and also lists all the clients associated with the AP.

<table>
<tr><th>Date/Time</th><th>Client Mac Address</th><th>SSID</th><th>Radio Type</th><th>Classifier</th><th>Subclassifier</th><th>Signal Streng</th></tr>
<tr><td>2022/05/24 13:23:42</td><td>[redacted]</td><td>Forti-Corp-3F-PSK</td><td>802.11ax-5G</td><td>Coverage</td><td>Asymmetric Data Rates</td><td>-54 dBm</td></tr>
<tr><td>2022/05/24 13:23:42</td><td>[redacted]</td><td>Forti-Corp-3F-PSK</td><td>802.11ac</td><td>Coverage</td><td>Asymmetric Data Rates</td><td>-58 dBm</td></tr>
<tr><td>2022/05/24 13:23:42</td><td>[redacted]</td><td>Forti-Corp-3F-PSK</td><td>802.11ac</td><td>Coverage</td><td>Asymmetric Data Rates</td><td>-58 dBm</td></tr>
<tr><td>2022/05/24 13:23:42</td><td>[redacted]</td><td>Forti-Corp-3F-PSK</td><td>802.11ac</td><td>Coverage</td><td>Asymmetric Data Rates</td><td>-54 dBm</td></tr>
</table>
0% 5

All Clients
<table>
<tr><th>Client Mac Address</th><th>Channel</th><th>Radio Type</th><th>SSID</th><th>Data Rate</th><th>Bandwidth Rx</th><th>Bandwidth Tx</th><th>T</th></tr>
<tr><td>[redacted]</td><td>60</td><td>802.11ax-5G</td><td>Forti-Corp-3F-PSK</td><td>456.00 Mbps</td><td>0</td><td>642.00 bps</td><td></td></tr>
<tr><td>[redacted]</td><td>60</td><td>802.11ax-5G</td><td>Forti-Corp-3F-PSK</td><td>12.00 Mbps</td><td>0</td><td>1.77 Kbps</td><td></td></tr>
<tr><td>[redacted]</td><td>60</td><td>802.11ax-5G</td><td>Forti-Corp-3F-PSK</td><td>797.20 Mbps</td><td>426.39 Kbps</td><td>45.10 Kbps</td><td></td></tr>
</table>
</td></tr>
<tr><td><b>Interfering APs</b></td><td>This tab displays details of the interfering APs in your network.

<table>
<tr><th>Date/Time</th><th>BSSID</th><th>Signal Strength</th></tr>
<tr><td>2023/11/09 13:25:09</td><td>[redacted]</td><td>-73 dBm</td></tr>
<tr><td>2023/11/09 13:25:09</td><td>[redacted]</td><td>-46 dBm</td></tr>
<tr><td>2023/11/09 13:25:09</td><td>[redacted]</td><td>-47 dBm</td></tr>
</table>
</td></tr>
</table>

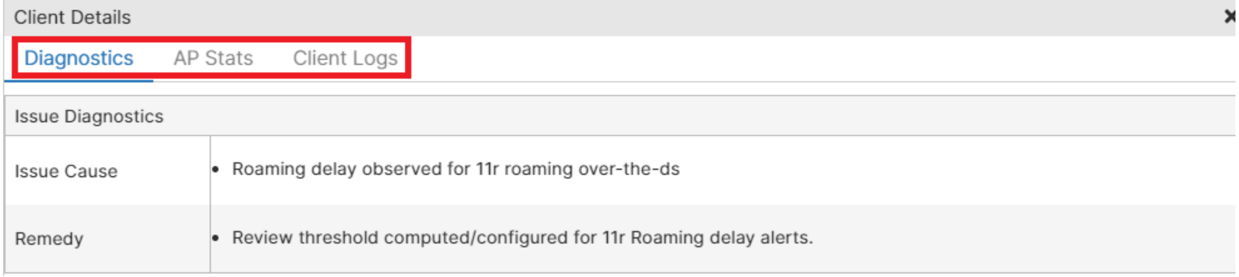
Roaming

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.

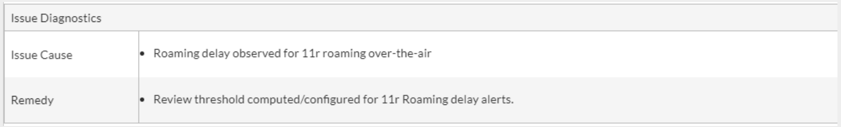
Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
MAC Address	The MAC address of the impacted client device.
Device	The name of the device as configured by the user. If the name is not configured or available, then MAC address is displayed.
SSID	The SSID that the impacted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

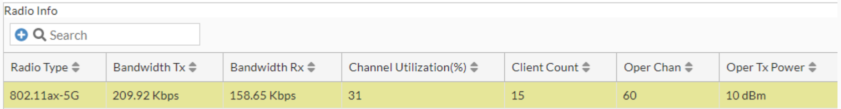
To view the logs, select a specific row of an AP event and click **View Logs**. You can view client details such as **Diagnostics** with the issue description and the suggested remediation, **AP Stats** with the associated AP radio details, and **Client Logs** with details of the impacted clients.



Issue Diagnostics

Issue Cause	• Roaming delay observed for 11r roaming over-the-ds
Remedy	• Review threshold computed/configured for 11r Roaming delay alerts.

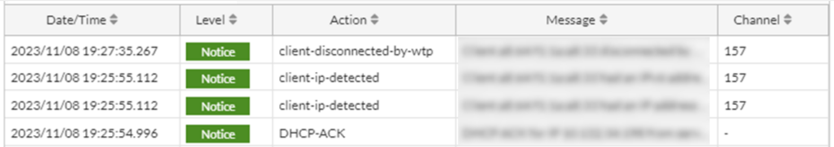
Logs	Description
Diagnostics	This tab provides detailed cause of the SLA breach that impacted the client. FortiAIOps also suggests the remedy to resolve the issue.  Issue Diagnostics Issue Cause: • Roaming delay observed for 11r roaming over-the-air Remedy: • Review threshold computed/configured for 11r Roaming delay alerts.
AP Stats	This tab displays the details of the AP radio that the client associated with.

Logs	Description
	

Radio Info

Search

Radio Type	Bandwidth Tx	Bandwidth Rx	Channel Utilization(%)	Client Count	Oper Chan	Oper Tx Power
802.11ax-5G	209.92 Kbps	158.65 Kbps	31	15	60	10 dBm

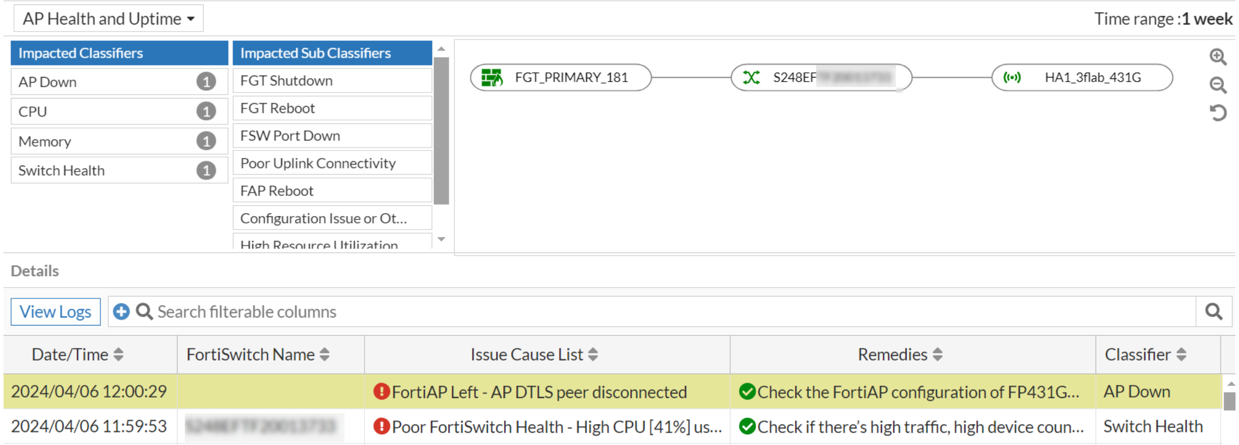
Logs	Description
Client Logs	This tab provides client event logs. 

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

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



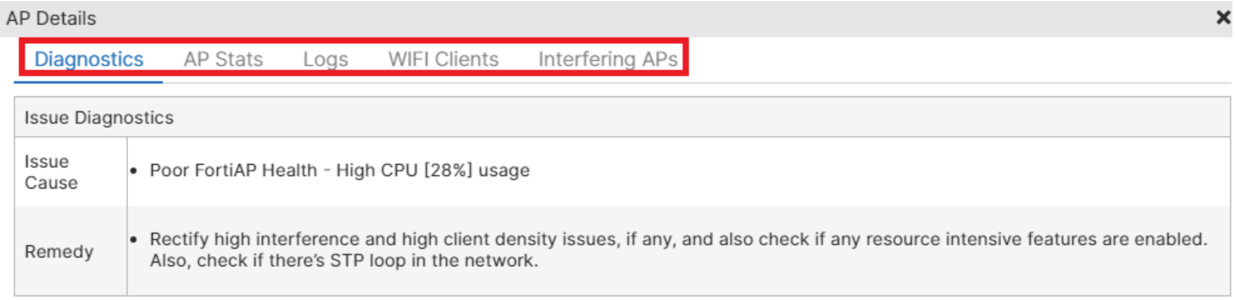
Date/Time	FortiSwitch Name	Issue Cause List	Remedies	Classifier
2024/04/06 12:00:29		FortiAP Left - AP DTLS peer disconnected	Check the FortiAP configuration of FP431G...	AP Down
2024/04/06 11:59:53	[redacted]	Poor FortiSwitch Health - High CPU [41%] us...	Check if there's high traffic, high device coun...	Switch 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.

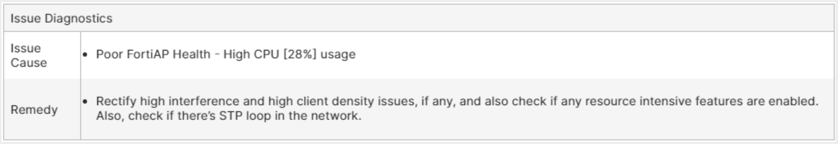
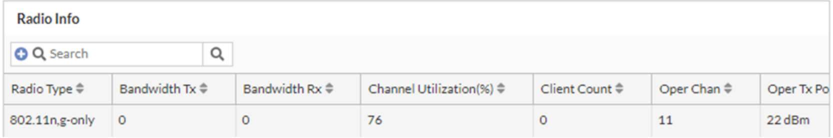
Attribute	Description
Sub Classifier	The sub-classifier of the issue for the reported classifier.
AP Serial Number	The AP serial number that the client associated with.
FortiGate Hostname	The hostname of the FortiGate associated with the AP/impacted client.
FortiGate Serial Number	The serial number of the associated FortiGate.
FortiSwitch Serial Number	The serial number of the switch associated with the impacted AP/client.

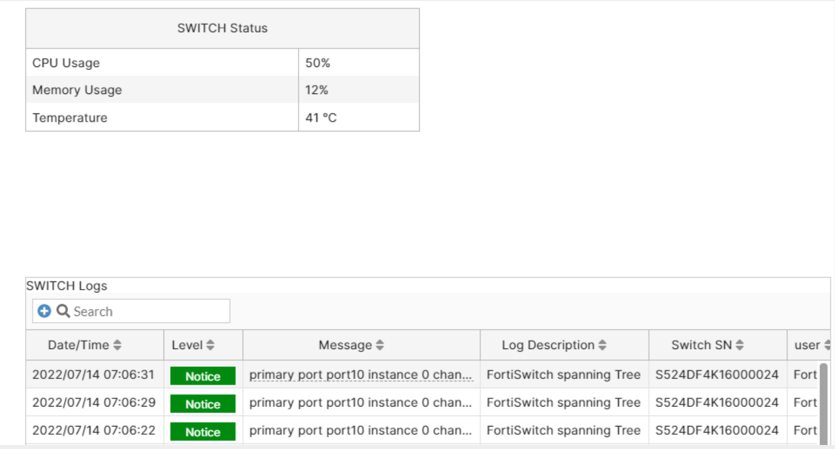
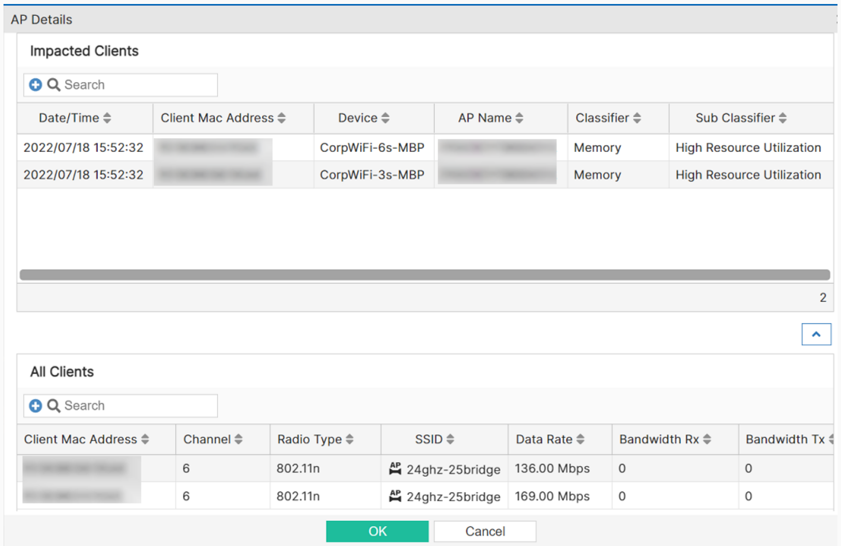
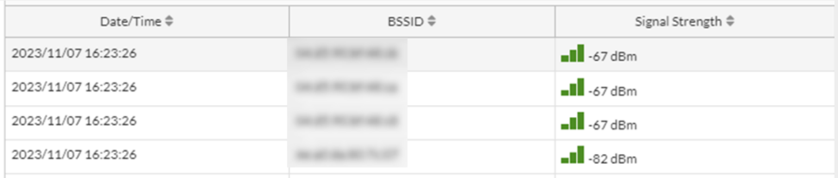
In the AP events displayed, select an event and click **View Logs**.



Issue Diagnostics

Issue Cause	• Poor FortiAP Health - High CPU [28%] usage
Remedy	• Rectify high interference and high client density issues, if any, and also check if any resource intensive features are enabled. Also, check if there's STP loop in the network.

<table>
<tr><th>Logs</th><th>Description</th></tr>
<tr><td><b>Diagnostics</b></td><td>This tab provides detailed cause of the SLA breach that impacted the client/AP/FortiGate. FortiAIOps also suggests the remedy to resolve the issue.

Issue Diagnostics
<table>
<tr><td>Issue Cause</td><td>• Poor FortiAP Health - High CPU [28%] usage</td></tr>
<tr><td>Remedy</td><td>• Rectify high interference and high client density issues, if any, and also check if any resource intensive features are enabled. Also, check if there's STP loop in the network.</td></tr>
</table></td></tr>
<tr><td><b>AP Stats</b></td><td>This tab displays the details of the AP radio that the client associated with and the WAN status details of the AP.

Radio Info
Search
<table>
<tr><th>Radio Type</th><th>Bandwidth Tx</th><th>Bandwidth Rx</th><th>Channel Utilization(%)</th><th>Client Count</th><th>Oper Chan</th><th>Oper Tx Po</th></tr>
<tr><td>802.11n,g-only</td><td>0</td><td>0</td><td>76</td><td>0</td><td>11</td><td>22 dBm</td></tr>
</table></td></tr>
<tr><td><b>Logs</b></td><td><ul>
<li>For the AP <i>down</i>/FortiSwitch health events, triggered due to FortiSwitch related failure, the FortiSwitch status and logs are displayed.</li>
<li>For AP health related events like poor CPU and memory, the AP status and logs are displayed.</li>
<li>For AP down events triggered due to FortiAP/FortiGate failure, the AP status and logs, and FortiGate logs are displayed.</li>
</ul></td></tr>
</table>

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. 

SWITCH Status

CPU Usage	50%
Memory Usage	12%
Temperature	41 °C

SWITCH Logs

Search

Date/Time	Level	Message	Log Description	Switch SN	user
2022/07/14 07:06:31	Notice	primary port port10 instance 0 chan...	FortiSwitch spanning Tree	S524DF4K16000024	Fort
2022/07/14 07:06:29	Notice	primary port port10 instance 0 chan...	FortiSwitch spanning Tree	S524DF4K16000024	Fort
2022/07/14 07:06:22	Notice	primary port port10 instance 0 chan...	FortiSwitch spanning Tree	S524DF4K16000024	Fort

AP Details

Impacted Clients

Search

Date/Time	Client Mac Address	Device	AP Name	Classifier	Sub Classifier
2022/07/18 15:52:32	[redacted]	CorpWiFi-6s-MBP	[redacted]	Memory	High Resource Utilization
2022/07/18 15:52:32	[redacted]	CorpWiFi-3s-MBP	[redacted]	Memory	High Resource Utilization

2

All Clients

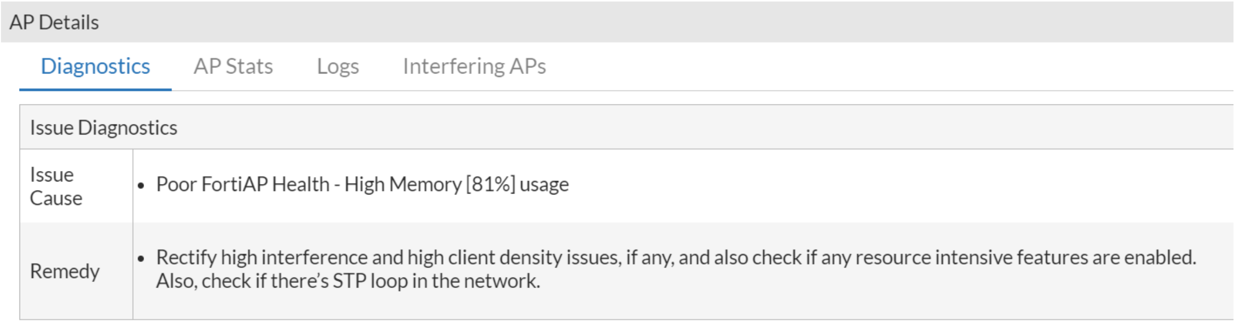
Search

Client Mac Address	Channel	Radio Type	SSID	Data Rate	Bandwidth Rx	Bandwidth Tx
[redacted]	6	802.11n	24ghz-25bridge	136.00 Mbps	0	0
[redacted]	6	802.11n	24ghz-25bridge	169.00 Mbps	0	0

OK Cancel

Date/Time	BSSID	Signal Strength
2023/11/07 16:23:26	[redacted]	-67 dBm
2023/11/07 16:23:26	[redacted]	-67 dBm
2023/11/07 16:23:26	[redacted]	-67 dBm
2023/11/07 16:23:26	[redacted]	-82 dBm

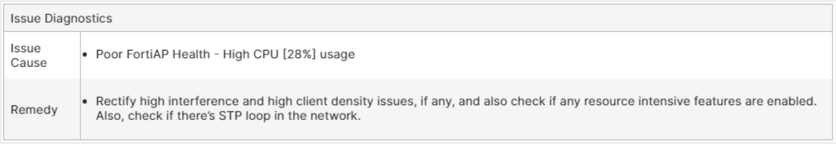
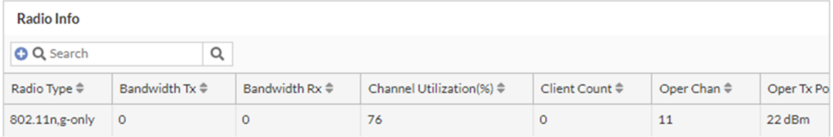
Select any impacted client and click **Show AP details** to view the detailed AP logs.

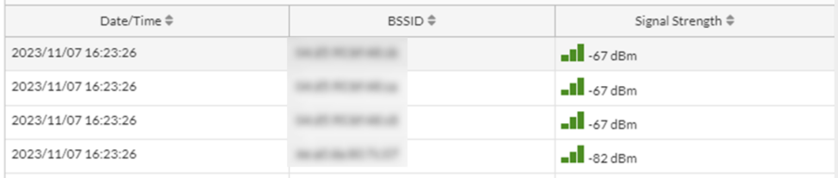


AP Details

Issue Diagnostics	
Issue Cause	• Poor FortiAP Health - High Memory [81%] usage
Remedy	• Rectify high interference and high client density issues, if any, and also check if any resource intensive features are enabled. Also, check if there's STP loop in the network.

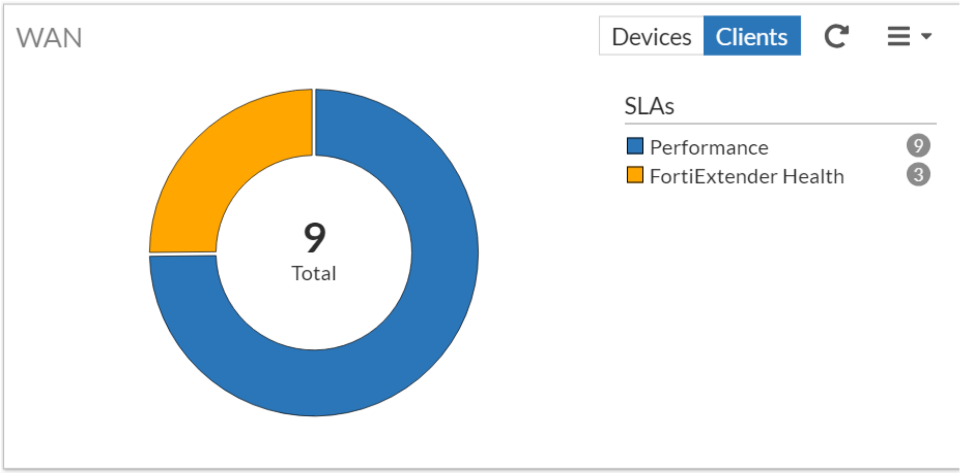
Select any of the tabs to view the data described in this table.

<table>
<tr><th>Logs</th><th>Description</th></tr>
<tr><td><b>Diagnostics</b></td><td>This tab provides detailed cause of the SLA breach that impacted the client/AP/FortiGate. FortiAIOps also suggests the remedy to resolve the issue.

<table>
<tr><th colspan="2">Issue Diagnostics</th></tr>
<tr><td>Issue Cause</td><td>• Poor FortiAP Health - High CPU [28%] usage</td></tr>
<tr><td>Remedy</td><td>• Rectify high interference and high client density issues, if any, and also check if any resource intensive features are enabled. Also, check if there's STP loop in the network.</td></tr>
</table></td></tr>
<tr><td><b>AP Stats</b></td><td>This tab displays the details of the AP radio that the client associated with and the WAN status details of the AP.

Radio Info

<table>
<tr><th>Radio Type</th><th>Bandwidth Tx</th><th>Bandwidth Rx</th><th>Channel Utilization(%)</th><th>Client Count</th><th>Oper Chan</th><th>Oper Tx Po</th></tr>
<tr><td>802.11n,g-only</td><td>0</td><td>0</td><td>76</td><td>0</td><td>11</td><td>22 dBm</td></tr>
</table></td></tr>
<tr><td><b>Interfering APs</b></td><td>This tab displays details of the interfering APs in your network.

<table>
<tr><th>Date/Time</th><th>BSSID</th><th>Signal Strength</th></tr>
<tr><td>2023/11/07 16:23:26</td><td>[redacted]</td><td>-67 dBm</td></tr>
<tr><td>2023/11/07 16:23:26</td><td>[redacted]</td><td>-67 dBm</td></tr>
<tr><td>2023/11/07 16:23:26</td><td>[redacted]</td><td>-67 dBm</td></tr>
<tr><td>2023/11/07 16:23:26</td><td>[redacted]</td><td>-82 dBm</td></tr>
</table></td></tr>
<tr><td><b>Logs</b></td><td>This tab provides the AP event logs generated from FortiGate.</td></tr>
</table>

WAN

The WAN panel displays the performance SLA metrics to monitor WAN member interface link quality and to detect failures and FortiExtender health data, along with the impacted client details. Any client that breaches the configured SLA thresholds are reported. In each SLA panel, you can select **Clients** to view the impacted client count or click **Devices** to view the impacted interface count.

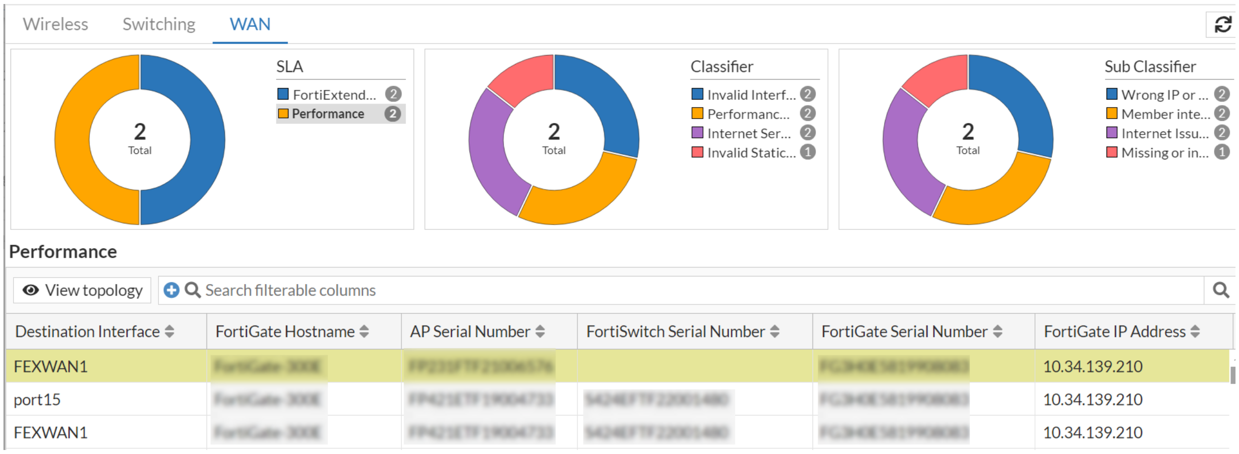


Topology and Logs

You can click on the impacted SLA listed in the panel to view the **Performance** 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.

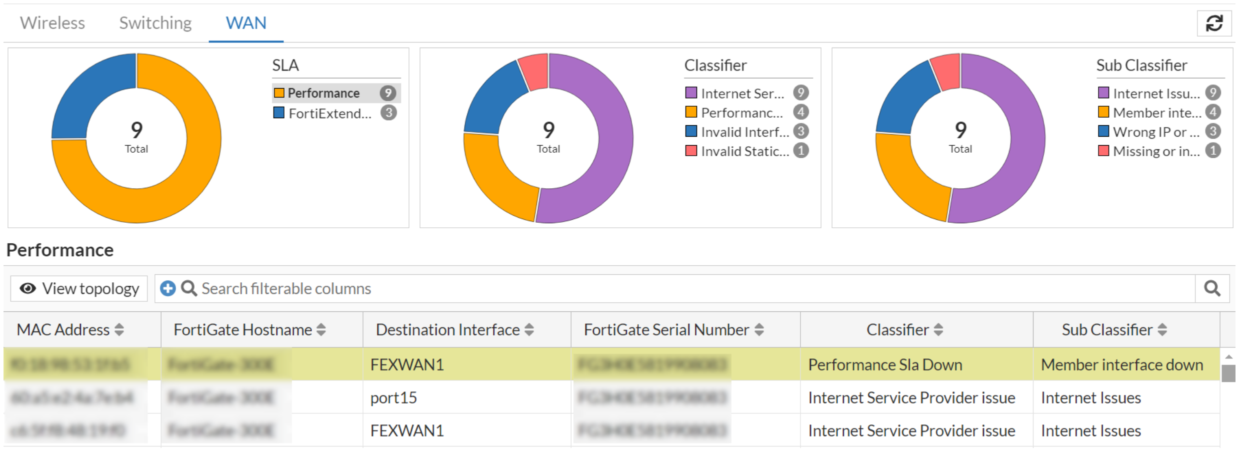
Performance SLA

If you select the **Devices** view in the 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.



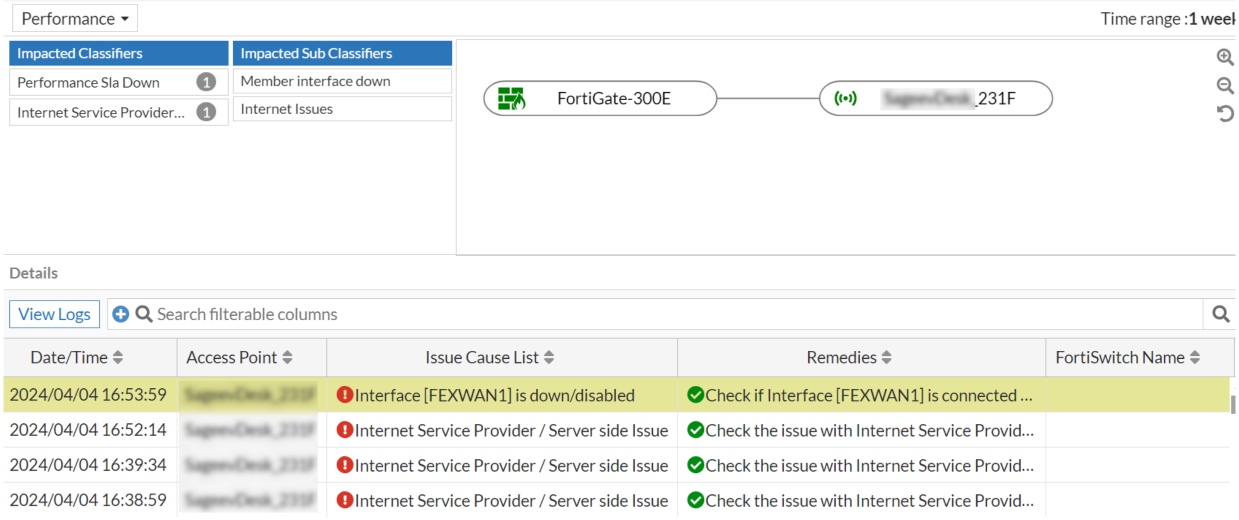
Destination Interface	FortiGate Hostname	AP Serial Number	FortiSwitch Serial Number	FortiGate Serial Number	FortiGate IP Address
FEXWAN1	[redacted]	[redacted]		[redacted]	10.34.139.210
port15	[redacted]	[redacted]	[redacted]	[redacted]	10.34.139.210
FEXWAN1	[redacted]	[redacted]	[redacted]	[redacted]	10.34.139.210

If you select the **Clients** view in the 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.



MAC Address	FortiGate Hostname	Destination Interface	FortiGate Serial Number	Classifier	Sub Classifier
[redacted]	[redacted]	FEXWAN1	[redacted]	Performance Sla Down	Member interface down
[redacted]	[redacted]	port15	[redacted]	Internet Service Provider issue	Internet Issues
[redacted]	[redacted]	FEXWAN1	[redacted]	Internet Service Provider issue	Internet Issues

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



Impacted Classifiers		Impacted Sub Classifiers
Performance Sla Down	1	Member interface down
Internet Service Provider...	1	Internet Issues

Date/Time	Access Point	Issue Cause List	Remedies	FortiSwitch Name
2024/04/04 16:53:59	[redacted]	Interface [FEXWAN1] is down/disabled	Check if Interface [FEXWAN1] is connected ...	
2024/04/04 16:52:14	[redacted]	Internet Service Provider / Server side Issue	Check the issue with Internet Service Provid...	
2024/04/04 16:39:34	[redacted]	Internet Service Provider / Server side Issue	Check the issue with Internet Service Provid...	
2024/04/04 16:38:59	[redacted]	Internet Service Provider / Server side Issue	Check the issue with Internet Service Provid...	

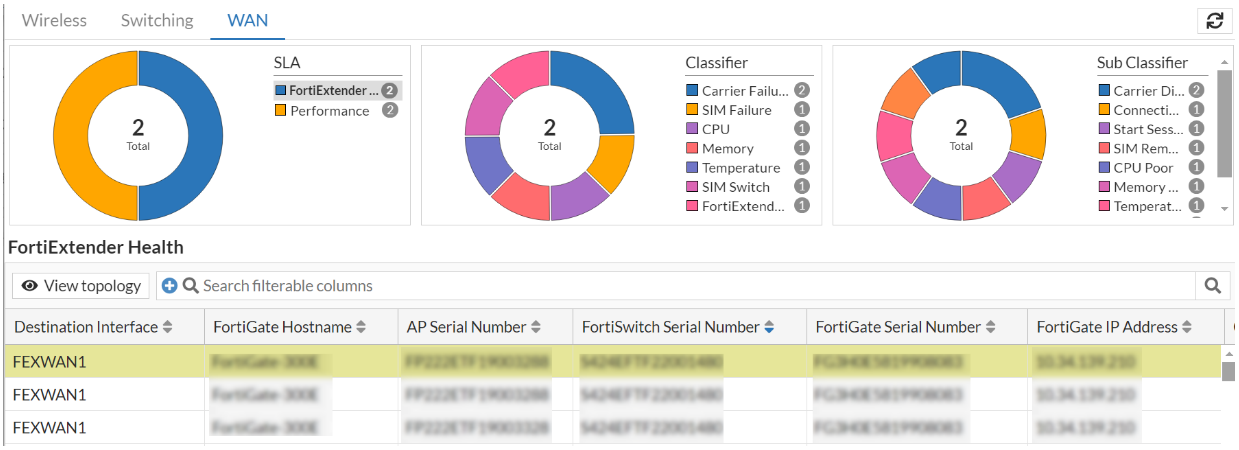
Right-click on the header of the table to select the columns that you wish to view.

Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
Access Point	The name of the associated AP.
FortiGate Serial Number	The serial number of the associated FortiGate.
FortiSwitch Name	The name of the associated FortiSwitch.
FortiSwitch Serial Number	The serial number of the associated FortiSwitch.
AP Serial Number	The serial number 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 causes of the SLA breach that impacted the

Attribute	Description
	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.
Health Check	The performance SLA check configured in FortiGate.
Source Interface	The source interface name.
Destination Interface	The destination interface name.
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.
FortiGate Hostname	The hostname of the FortiGate associated with the AP/impacted client.
Breach Summary	The WAN SLA threshold that was breached.
Client Type	The client type that is impacted, wireless or wired.

FortiExtender Health SLA

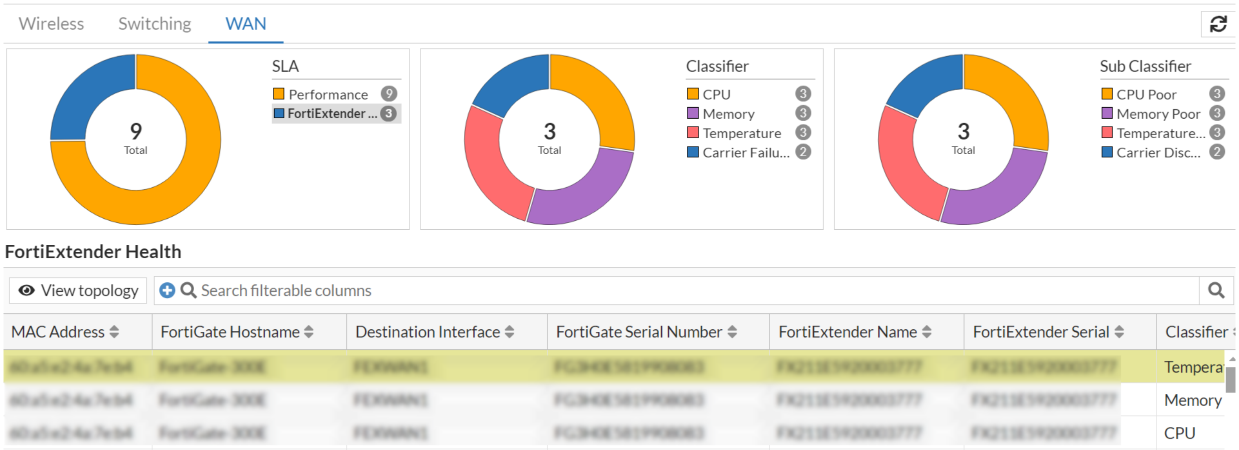
If you select the **Devices** view in the WAN panel and click on the FortiExtender Health SLA in the impacted SLAs list or click on the bar in the chart, the impacted interfaces' details such as, destination interface, AP serial number, the associated FortiGate host name, IP address, and serial number,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



FortiExtender Health

Destination Interface	FortiGate Hostname	AP Serial Number	FortiSwitch Serial Number	FortiGate Serial Number	FortiGate IP Address
FEXWAN1	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
FEXWAN1	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
FEXWAN1	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

If you select the **Clients** view in the 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.

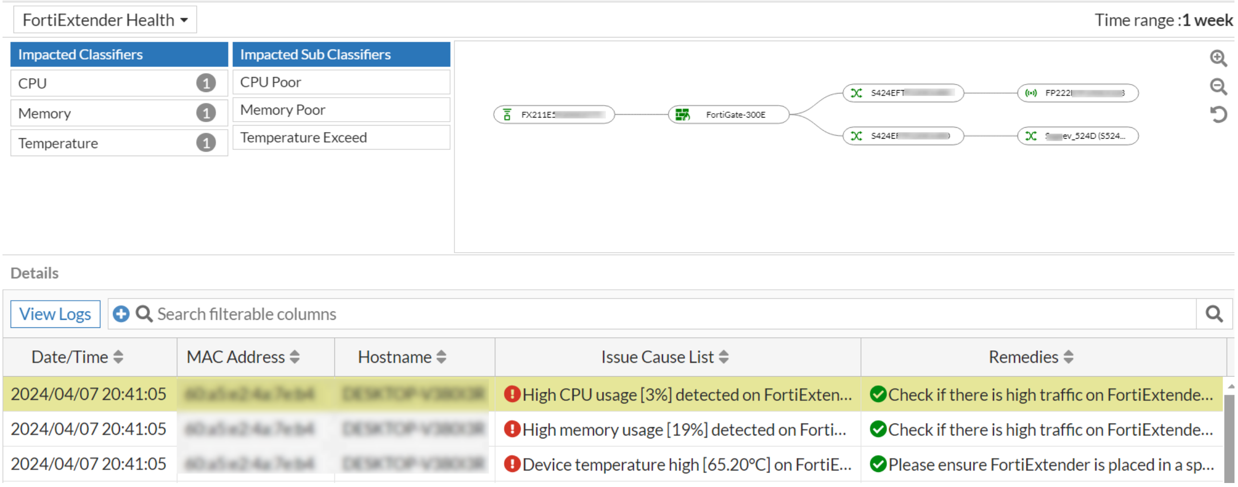


FortiExtender Health

View topology | Search filterable columns

MAC Address	FortiGate Hostname	Destination Interface	FortiGate Serial Number	FortiExtender Name	FortiExtender Serial	Classifier
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Tempera
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Memory
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	CPU

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



Impacted Classifiers		Impacted Sub Classifiers
CPU	1	CPU Poor
Memory	1	Memory Poor
Temperature	1	Temperature Exceed

Details

View Logs | Search filterable columns

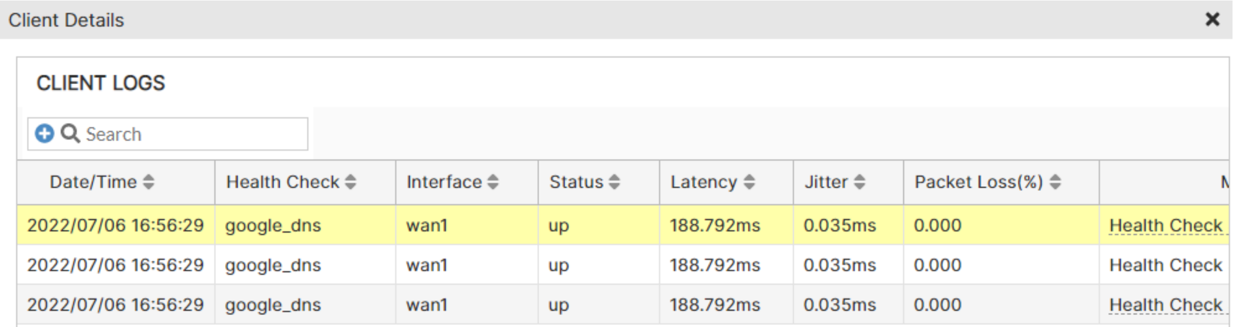
Date/Time	MAC Address	Hostname	Issue Cause List	Remedies
2024/04/07 20:41:05	[redacted]	[redacted]	High CPU usage [3%] detected on FortiExten...	Check if there is high traffic on FortiExtende...
2024/04/07 20:41:05	[redacted]	[redacted]	High memory usage [19%] detected on Forti...	Check if there is high traffic on FortiExtende...
2024/04/07 20:41:05	[redacted]	[redacted]	Device temperature high [65.20°C] on FortiE...	Please ensure FortiExtender is placed in a sp...

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.

Attribute	Description
Sub Classifier	The sub-classifier of the issue for the reported classifier.
Source and Destination Interface	The 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.



Client Details

CLIENT LOGS

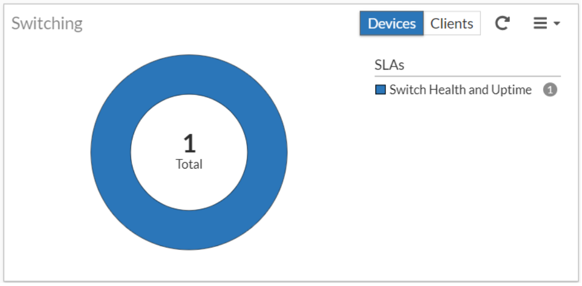
Date/Time	Health Check	Interface	Status	Latency	Jitter	Packet Loss(%)	M
2022/07/06 16:56:29	google_dns	wan1	up	188.792ms	0.035ms	0.000	Health Check
2022/07/06 16:56:29	google_dns	wan1	up	188.792ms	0.035ms	0.000	Health Check
2022/07/06 16:56:29	google_dns	wan1	up	188.792ms	0.035ms	0.000	Health Check

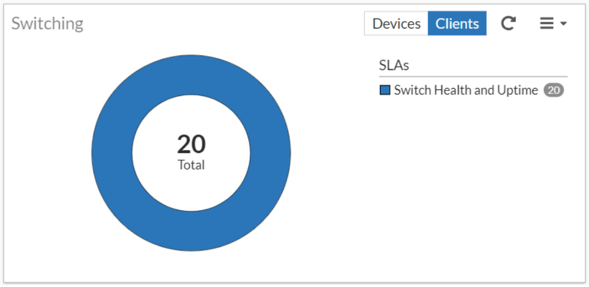
Switching

The Switching 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.





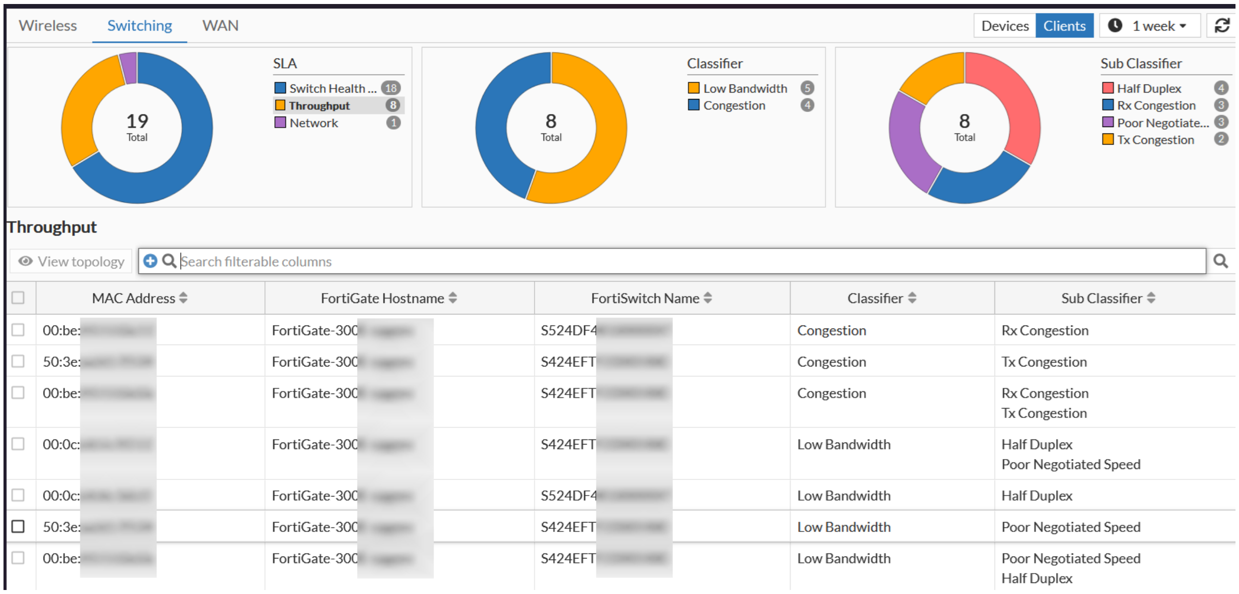
SLAs, Topology and Logs

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 Connection Failure
- Switch Health and Uptime

Throughput

Displays potential low throughput conditions, in this page you can view the details of the throughput SLA.

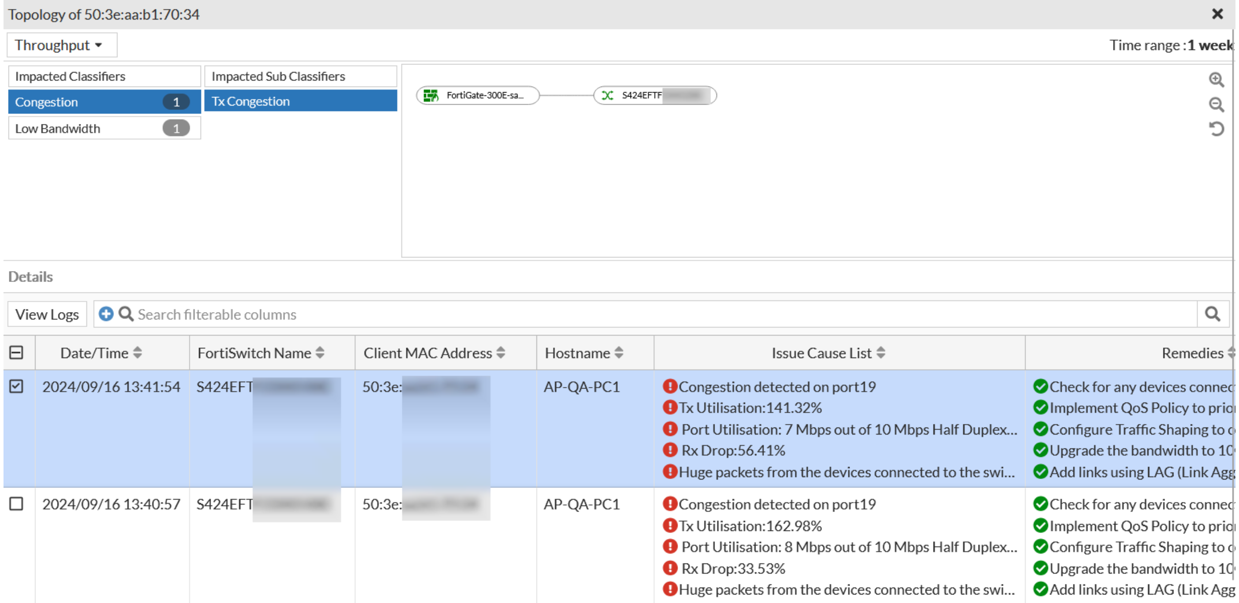


□	MAC Address	FortiGate Hostname	FortiSwitch Name	Classifier	Sub Classifier
□	00:be:[redacted]	FortiGate-300[redacted]	S524DF4[redacted]	Congestion	Rx Congestion
□	50:3e:[redacted]	FortiGate-300[redacted]	S424EFT[redacted]	Congestion	Tx Congestion
□	00:be:[redacted]	FortiGate-300[redacted]	S424EFT[redacted]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

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

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

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



Impacted Classifiers	
Congestion	1
Low Bandwidth	1

Impacted Sub Classifiers
Tx Congestion

Details

View Logs | Search filterable columns

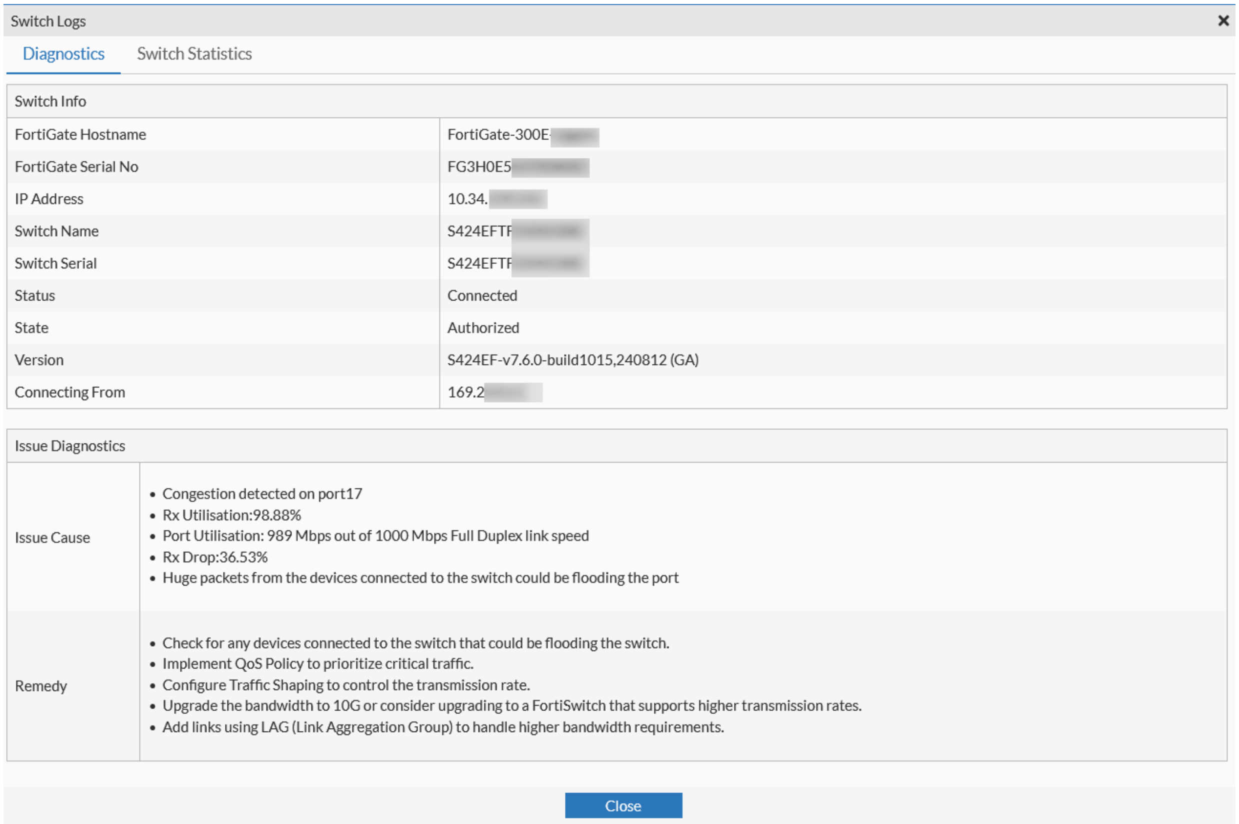
⊟	Date/Time	FortiSwitch Name	Client MAC Address	Hostname	Issue Cause List	Remedies
☑	2024/09/16 13:41:54	S424EFT[redacted]	50:3e:[redacted]	AP-QA-PC1	Congestion detected on port19 Tx Utilisation:141.32% Port Utilisation: 7 Mbps out of 10 Mbps Half Duplex... Rx Drop:56.41% Huge packets from the devices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

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

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

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

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

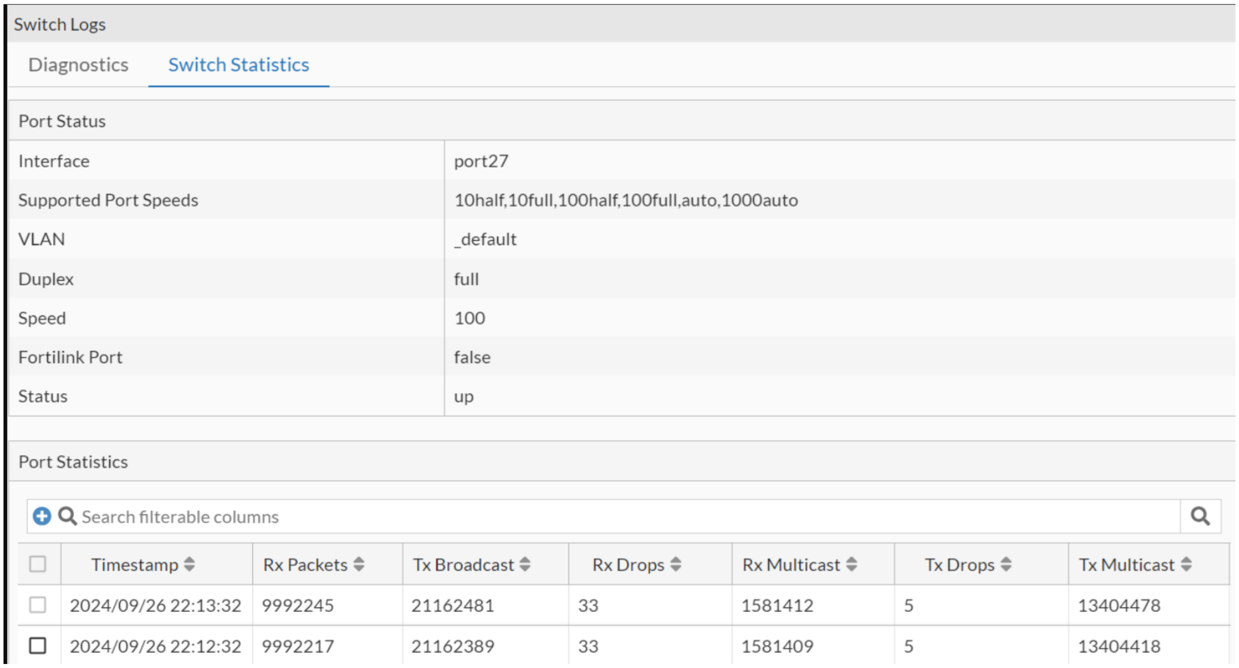


Switch Info

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

Issue Diagnostics

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



Port Status

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

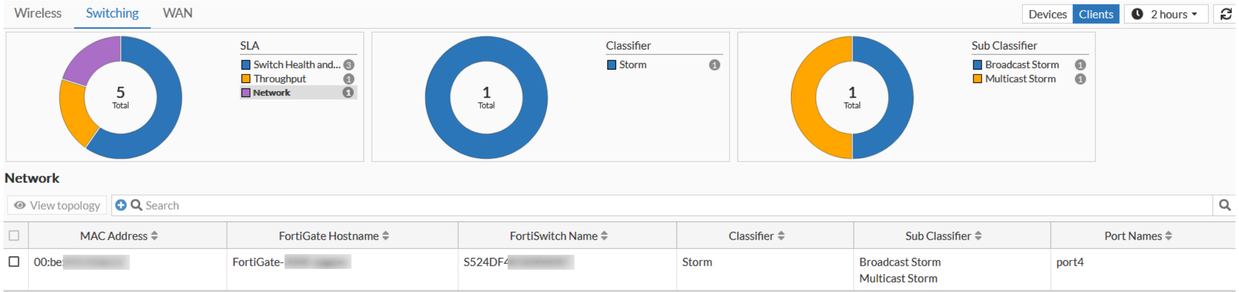
Port Statistics

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

Network

Displays potential network disruptions that may lead to poor connectivity, in this page you can view the details of the Network SLA.

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



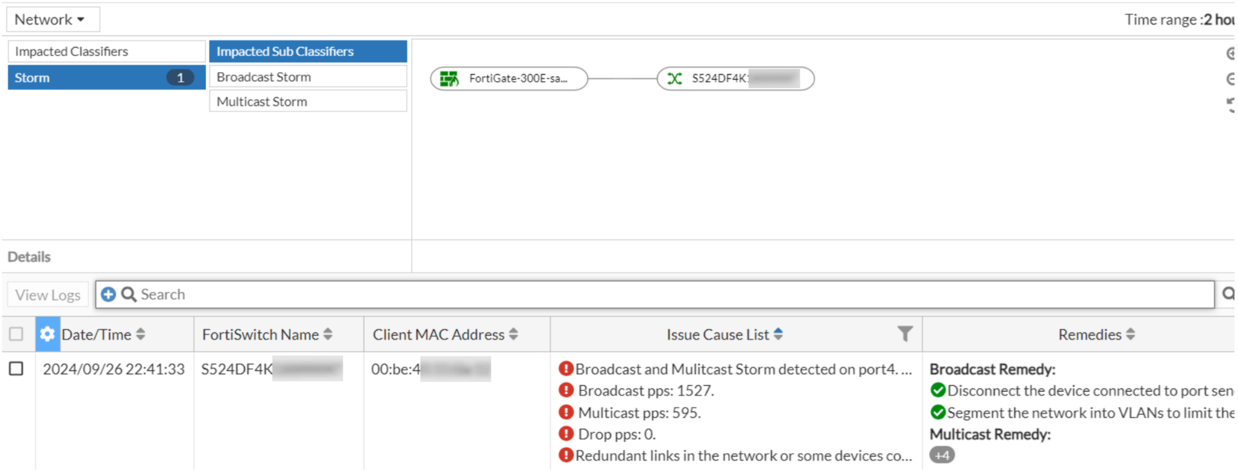
□	MAC Address	FortiGate Hostname	FortiSwitch Name	Classifier	Sub Classifier	Port Names
□	00:be[redacted]	FortiGate-[redacted]	S524DF4[redacted]	Storm	Broadcast Storm Multicast Storm	port4

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

Attribute	Description
MAC Address	The MAC address of the impacted client device.
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 Topology**. The **Details** table displays the following information.



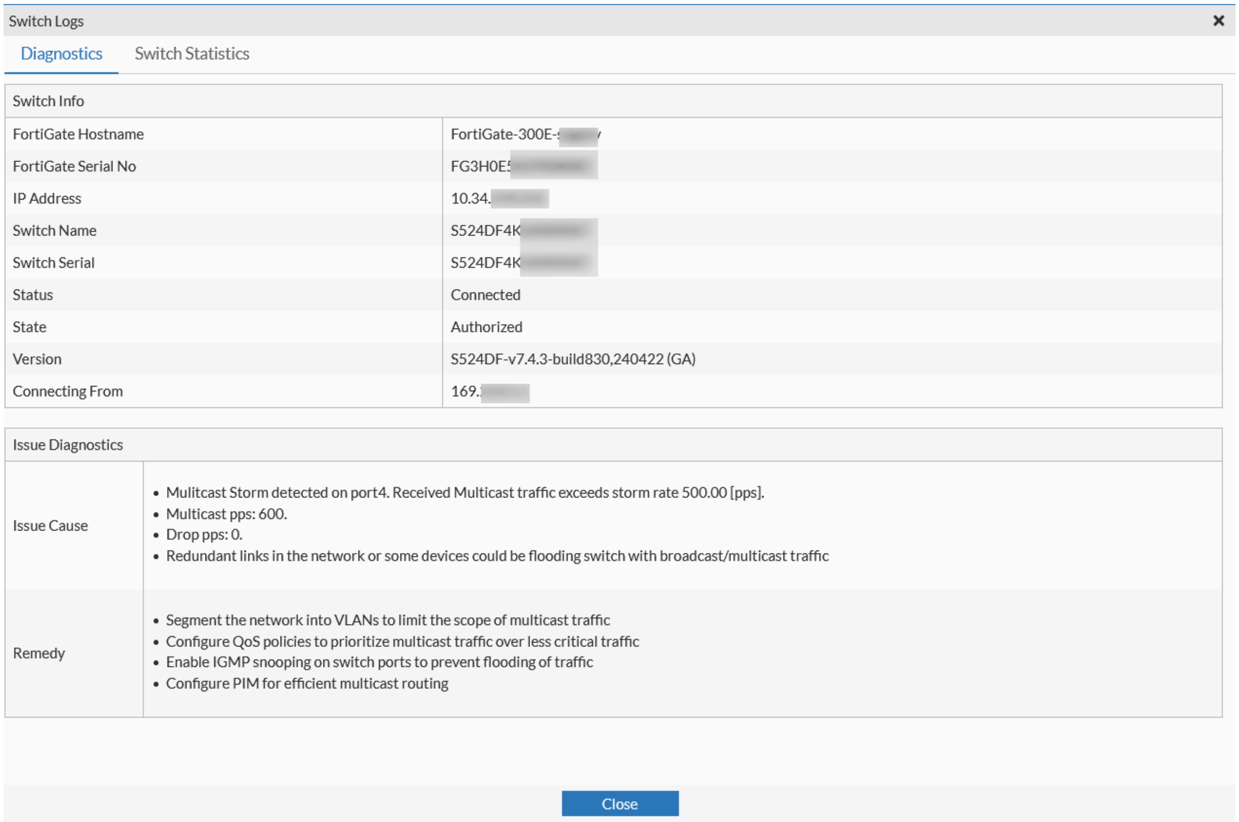
□	Date/Time	FortiSwitch Name	Client MAC Address	Issue Cause List	Remedies
□	2024/09/26 22:41:33	S524DF4K[redacted]	00:be:4[redacted]	Broadcast and Mulitcast Storm detected on port4. ... Broadcast pps: 1527. Multicast pps: 595. Drop pps: 0. Redundant links in the network or some devices co...	**Broadcast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

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

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

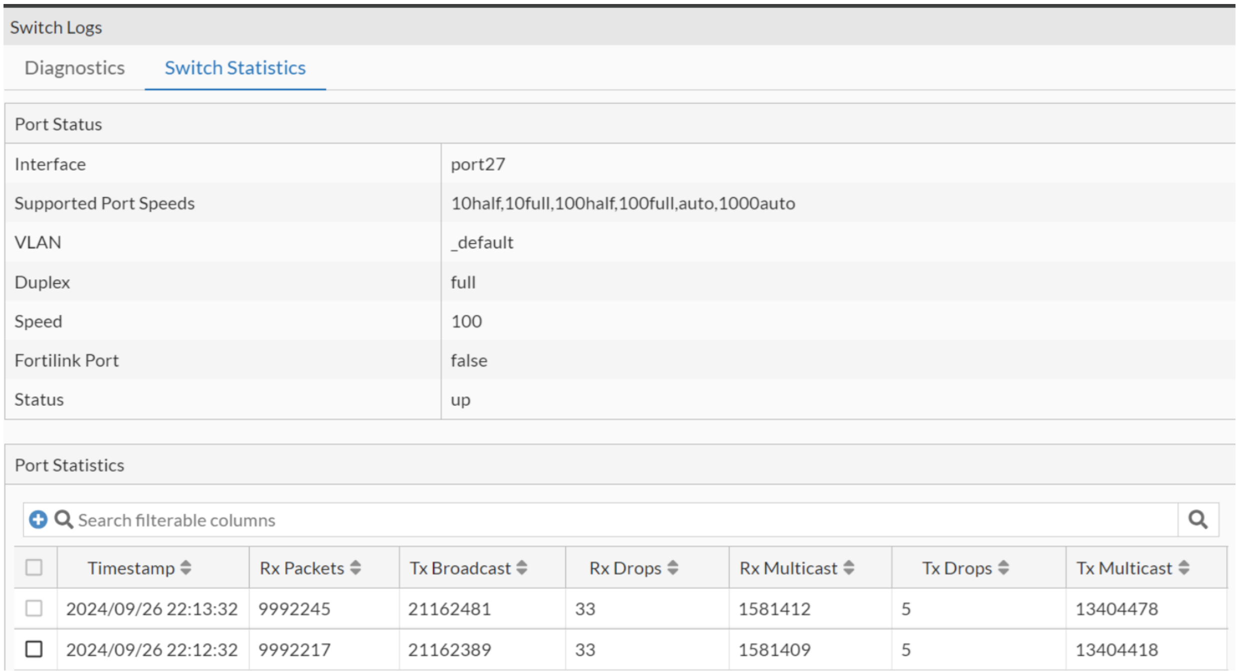
Attribute	Description
Sub Classifier	The sub-classifier of the issue for the reported classifier.
FortiGate Hostname	The hostname of the FortiGate associated with the impacted client.
FortiGate Serial Number	The serial number of the FortiGate associated with the impacted client.
FortiSwitch Serial Number	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 Info	
FortiGate Hostname	FortiGate-300E-[redacted]
FortiGate Serial No	FG3H0E5[redacted]
IP Address	10.34.[redacted]
Switch Name	S524DF4K[redacted]
Switch Serial	S524DF4K[redacted]
Status	Connected
State	Authorized
Version	S524DF-v7.4.3-build830,240422 (GA)
Connecting From	169.[redacted]

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



Port Status

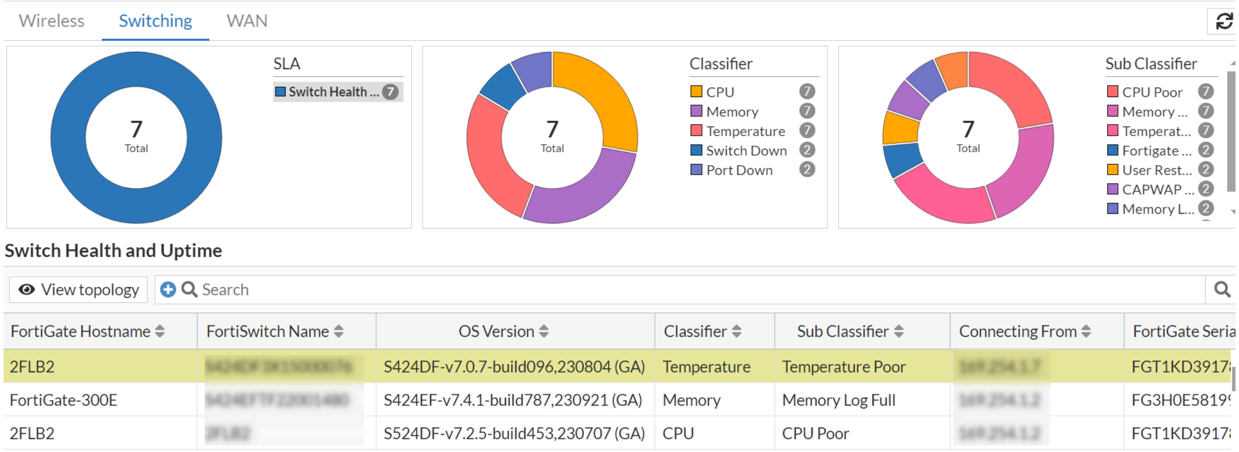
Interface	port27
Supported Port Speeds	10half,10full,100half,100full,auto,1000auto
VLAN	_default
Duplex	full
Speed	100
Fortilink Port	false
Status	up

Port Statistics

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

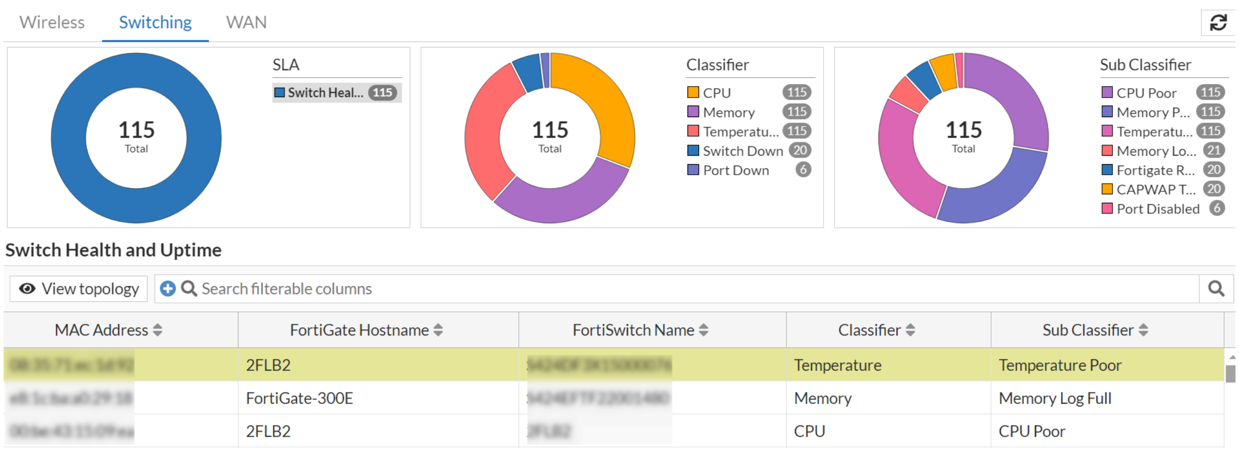
Switch Health and Uptime

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.



FortiGate Hostname	FortiSwitch Name	OS Version	Classifier	Sub Classifier	Connecting From	FortiGate Seria
2FLB2	[redacted]	S424DF-v7.0.7-build096,230804 (GA)	Temperature	Temperature Poor	[redacted]	FGT1KD3917
FortiGate-300E	[redacted]	S424EF-v7.4.1-build787,230921 (GA)	Memory	Memory Log Full	[redacted]	FG3H0E5819
2FLB2	[redacted]	S524DF-v7.2.5-build453,230707 (GA)	CPU	CPU Poor	[redacted]	FGT1KD3917

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.



SLA	
Switch Heal...	115

Classifier	
CPU	115
Memory	115
Temperatu...	115
Switch Down	20
Port Down	6

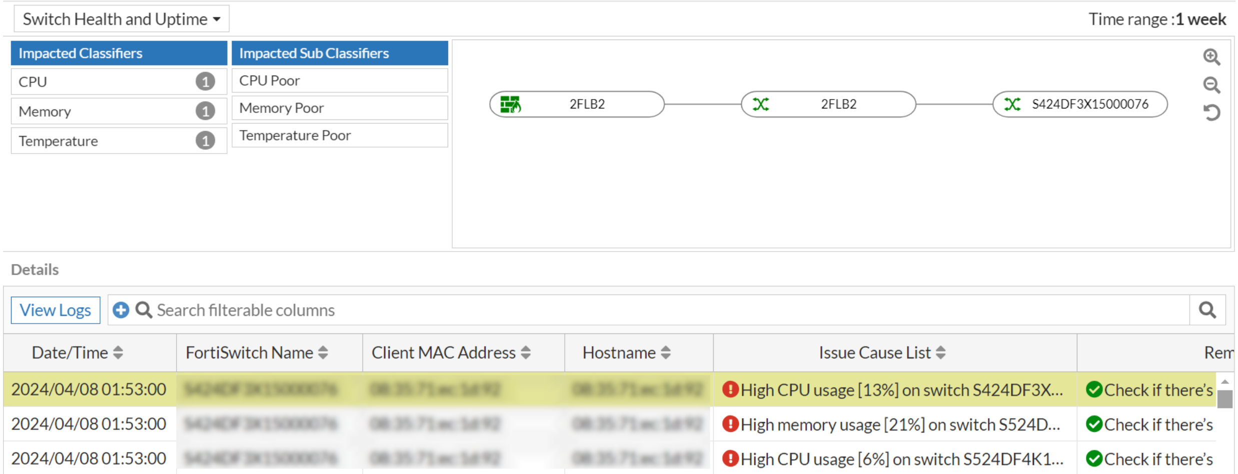
Sub Classifier	
CPU Poor	115
Memory P...	115
Temperatu...	115
Memory Lo...	21
Fortigate R...	20
CAPWAP T...	20
Port Disabled	6

Switch Health and Uptime

View topology | Search filterable columns

MAC Address	FortiGate Hostname	FortiSwitch Name	Classifier	Sub Classifier
[redacted]	2FLB2	[redacted]	Temperature	Temperature Poor
[redacted]	FortiGate-300E	[redacted]	Memory	Memory Log Full
[redacted]	2FLB2	[redacted]	CPU	CPU Poor

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



Impacted Classifiers	
CPU	1
Memory	1
Temperature	1

Impacted Sub Classifiers
CPU Poor
Memory Poor
Temperature Poor

Details

View Logs | Search filterable columns

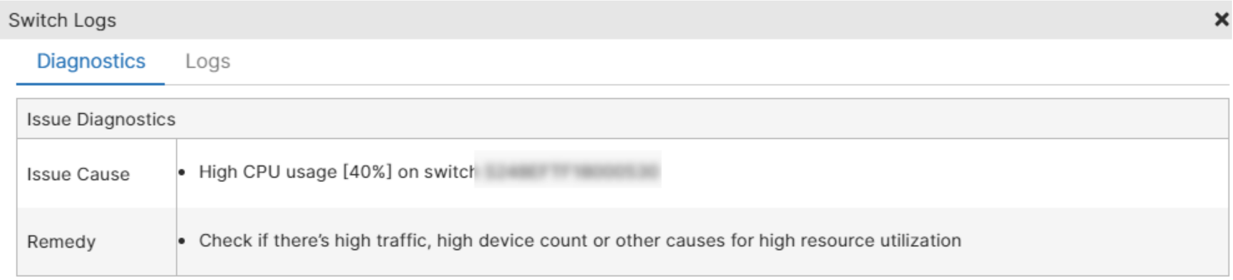
Date/Time	FortiSwitch Name	Client MAC Address	Hostname	Issue Cause List	Rem
2024/04/08 01:53:00	[redacted]	[redacted]	[redacted]	High CPU usage [13%] on switch S424DF3X...	Check if there's
2024/04/08 01:53:00	[redacted]	[redacted]	[redacted]	High memory usage [21%] on switch S524D...	Check if there's
2024/04/08 01:53:00	[redacted]	[redacted]	[redacted]	High CPU usage [6%] on switch S524DF4K1...	Check if there's

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.

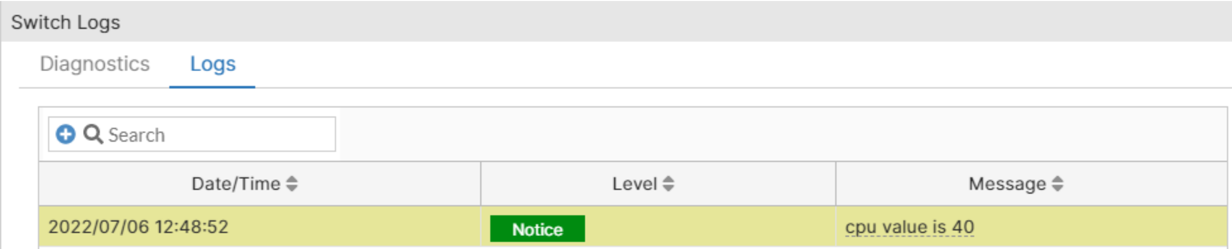
Attribute	Description
FortiGate Serial Number	The serial number of the FortiGate associated with the impacted client.
FortiSwitch Serial Number	The serial number of the impacted switch.

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



Issue Diagnostics	
Issue Cause	• High CPU usage [40%] on switch [redacted]
Remedy	• Check if there's high traffic, high device count or other causes for high resource utilization

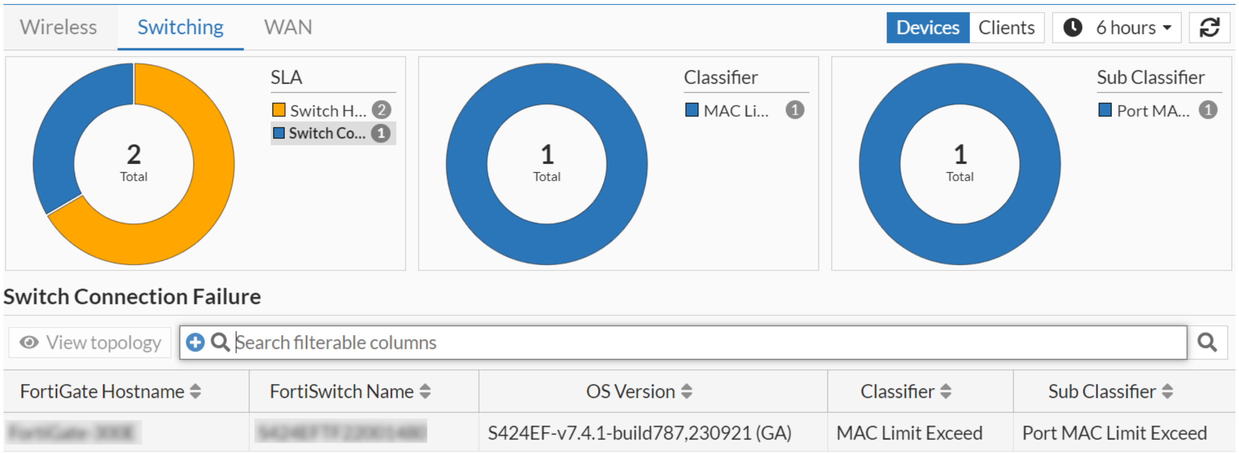
The **Logs** tab displays the time stamp of each action, the type of action such as notice, warning, etc., and the impact details are displayed. Different data tabs are displayed based on the selected issue/failure.



Date/Time	Level	Message
2022/07/06 12:48:52	Notice	cpu value is 40

Switch Connection Failure

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



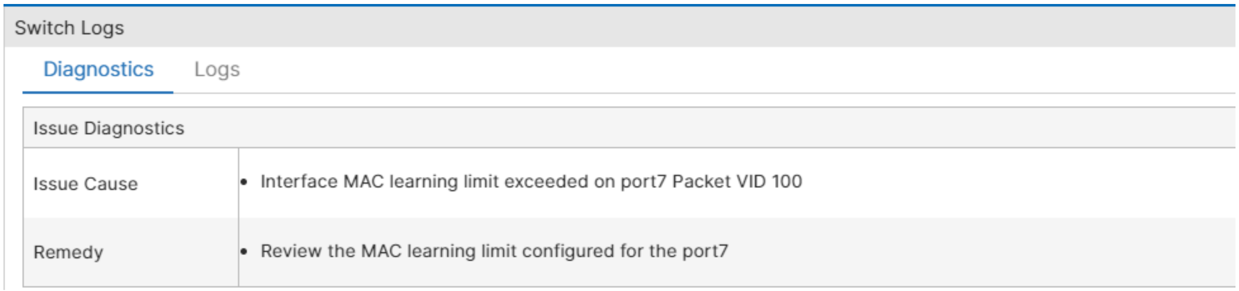
FortiGate Hostname	FortiSwitch Name	OS Version	Classifier	Sub Classifier
[redacted]	[redacted]	S424EF-v7.4.1-build787,230921 (GA)	MAC Limit Exceed	Port MAC Limit Exceed

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

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

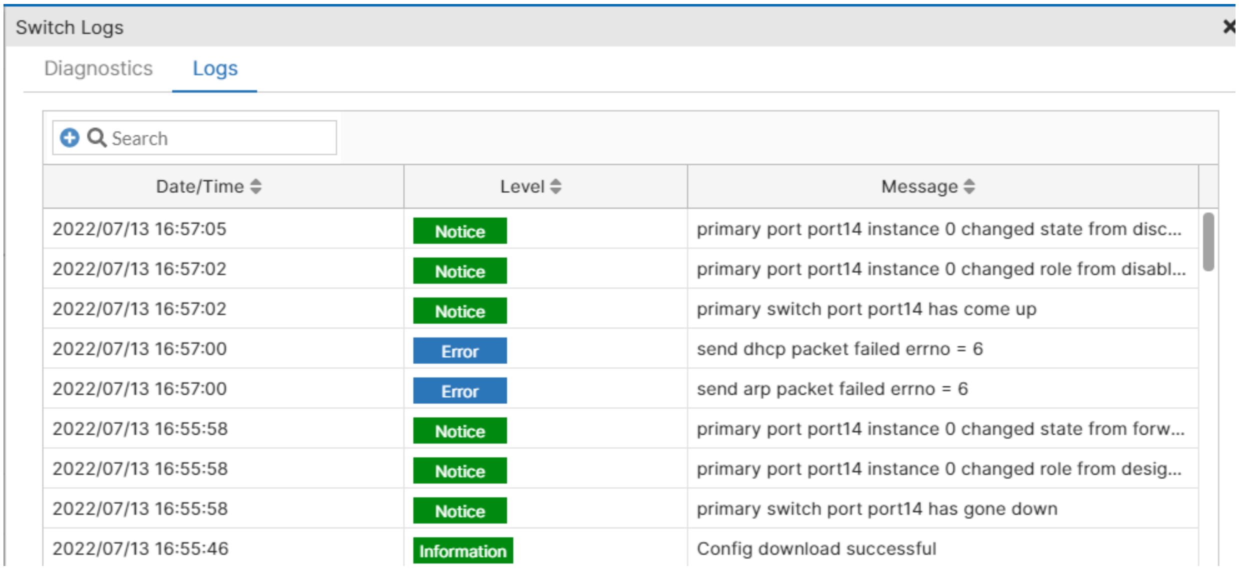
Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
FortiSwitch Name	The name of the impacted switch.
Client MAC Address	The MAC address of the impacted client device.
Hostname	The name of the device as configured by the user. If the name is not configured or available,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



Issue Diagnostics	
Issue Cause	• Interface MAC learning limit exceeded on port7 Packet VID 100
Remedy	• Review the MAC learning limit configured for the port7

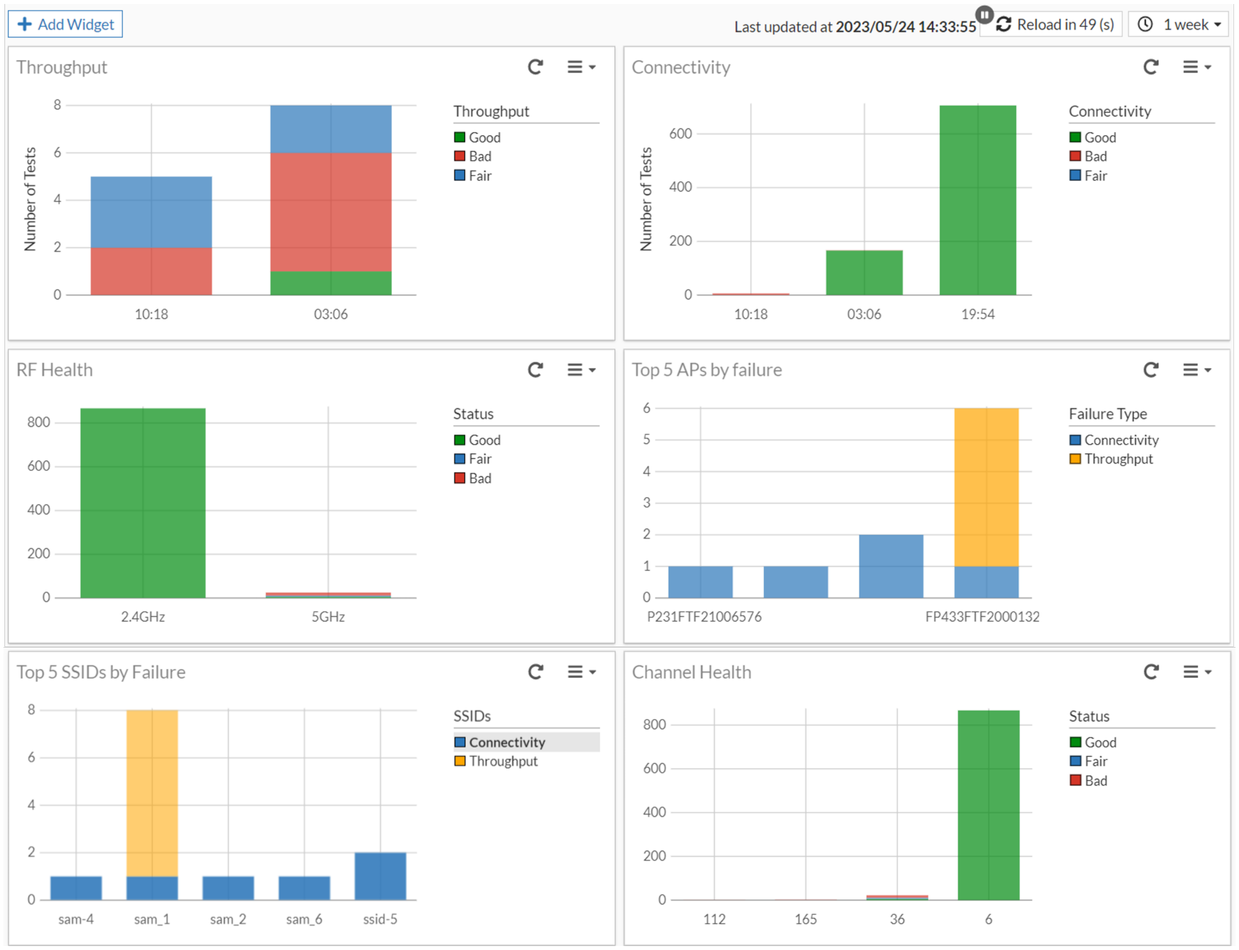
The **Logs** tab displays the time stamp of each action, the type of action such as notice, warning, etc., and the impact details are displayed. Different data tabs are displayed based on the selected issue/failure.



Date/Time	Level	Message
2022/07/13 16:57:05	Notice	primary port port14 instance 0 changed state from disc...
2022/07/13 16:57:02	Notice	primary port port14 instance 0 changed role from disabl...
2022/07/13 16:57:02	Notice	primary switch port port14 has come up
2022/07/13 16:57:00	Error	send dhcp packet failed errno = 6
2022/07/13 16:57:00	Error	send arp packet failed errno = 6
2022/07/13 16:55:58	Notice	primary port port14 instance 0 changed state from forw...
2022/07/13 16:55:58	Notice	primary port port14 instance 0 changed role from desig...
2022/07/13 16:55:58	Notice	primary switch port port14 has gone down
2022/07/13 16:55:46	Information	Config download successful

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.

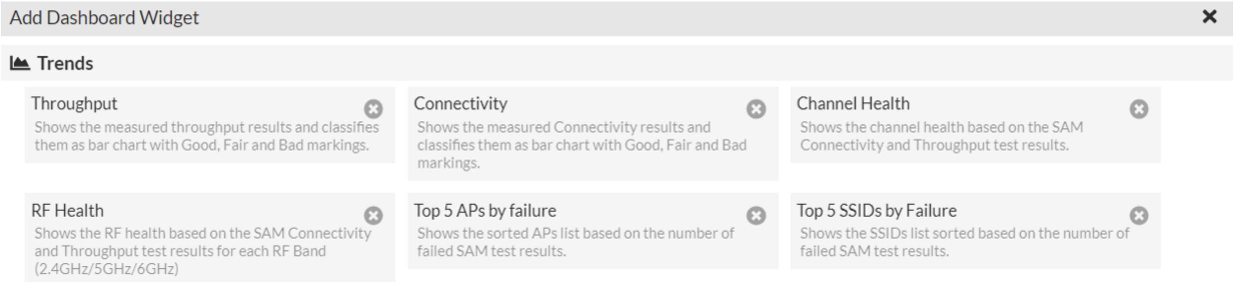


The data on this dashboard is based on scheduled test results and is automatically refreshed every 60 seconds; the following options are available to manage the auto-refresh feature for this page.

- Click ⟳ to manually refresh data.
- Click ⏸ to pause the auto-refresh.
- Click ▶ to resume the auto-refresh.

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.



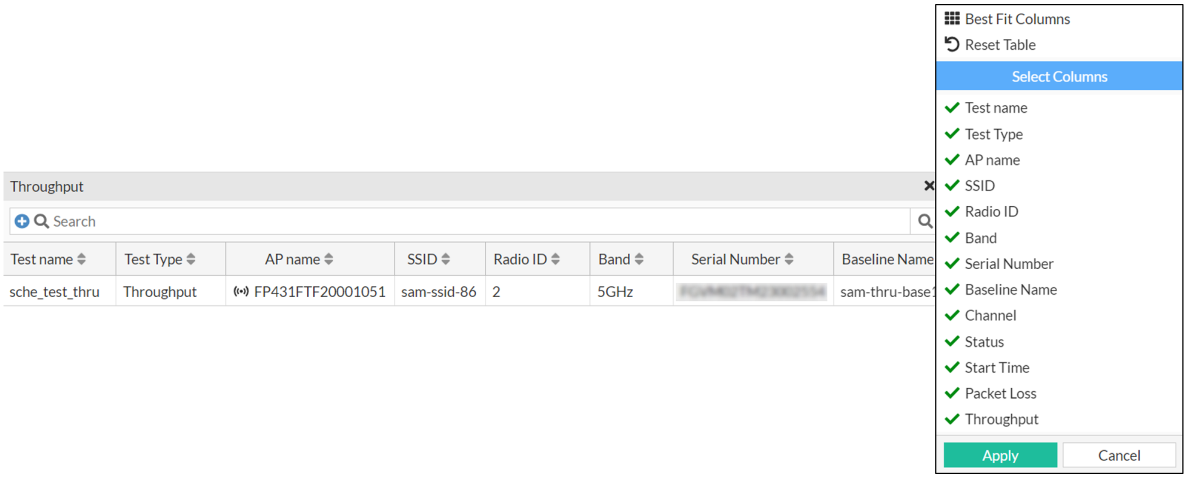
Add Dashboard Widget

Trends

Throughput Shows the measured throughput results and classifies them as bar chart with Good, Fair and Bad markings.	Connectivity Shows the measured Connectivity results and classifies them as bar chart with Good, Fair and Bad markings.	Channel Health Shows the channel health based on the SAM Connectivity and Throughput test results.
RF Health Shows the RF health based on the SAM Connectivity and Throughput test results for each RF Band (2.4GHz/5GHz/6GHz)	Top 5 APs by failure Shows the sorted APs list based on the number of failed SAM test results.	Top 5 SSIDs by Failure Shows the SSIDs list sorted based on the number of failed SAM test results.

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.



Throughput

Search

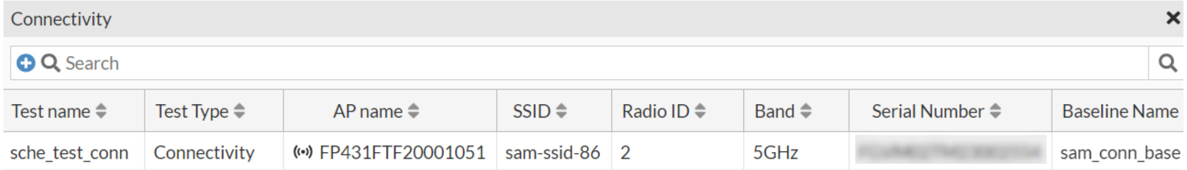
Test name	Test Type	AP name	SSID	Radio ID	Band	Serial Number	Baseline Name
sche_test_thru	Throughput	FP431FTF20001051	sam-ssid-86	2	5GHz	[redacted]	sam-thru-base1

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.

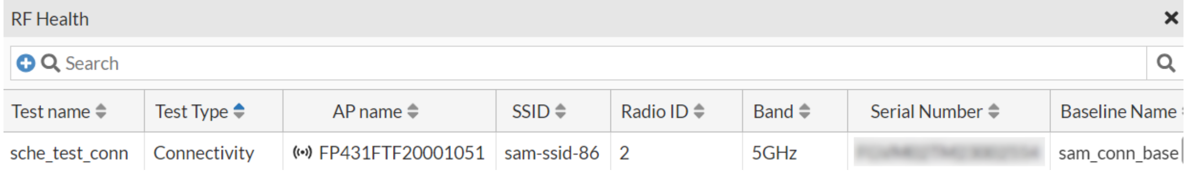


Connectivity

Search

Test name	Test Type	AP name	SSID	Radio ID	Band	Serial Number	Baseline Name
sche_test_conn	Connectivity	FP431FTF20001051	sam-ssid-86	2	5GHz	[redacted]	sam_conn_base

- **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.

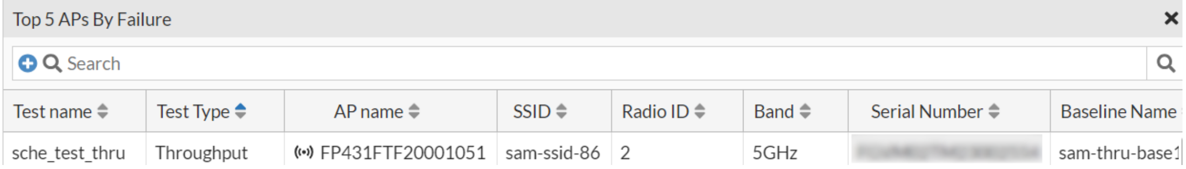


RF Health

Search

Test name	Test Type	AP name	SSID	Radio ID	Band	Serial Number	Baseline Name
sche_test_conn	Connectivity	FP431FTF20001051	sam-ssid-86	2	5GHz	[redacted]	sam_conn_base

- **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.

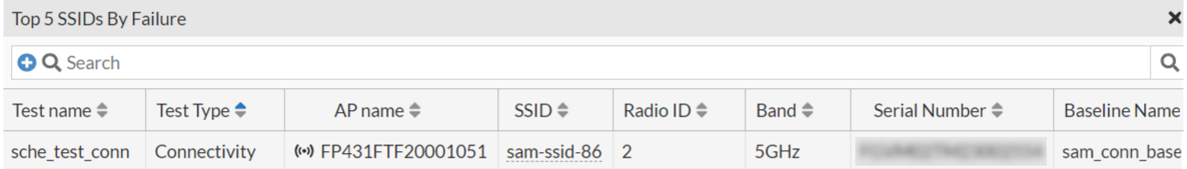


Top 5 APs By Failure

Search

Test name	Test Type	AP name	SSID	Radio ID	Band	Serial Number	Baseline Name
sche_test_thru	Throughput	FP431FTF20001051	sam-ssid-86	2	5GHz	[redacted]	sam-thru-base1

- **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.

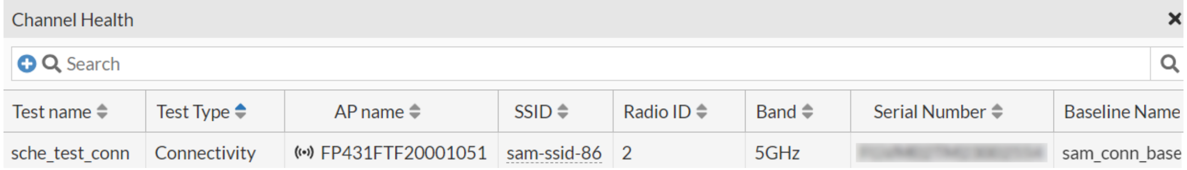


Top 5 SSIDs By Failure

Search

Test name	Test Type	AP name	SSID	Radio ID	Band	Serial Number	Baseline Name
sche_test_conn	Connectivity	FP431FTF20001051	sam-ssid-86	2	5GHz	[redacted]	sam_conn_base

- **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.



Channel Health

Search

Test name	Test Type	AP name	SSID	Radio ID	Band	Serial Number	Baseline Name
sche_test_conn	Connectivity	FP431FTF20001051	sam-ssid-86	2	5GHz	[redacted]	sam_conn_base

AI Insights

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

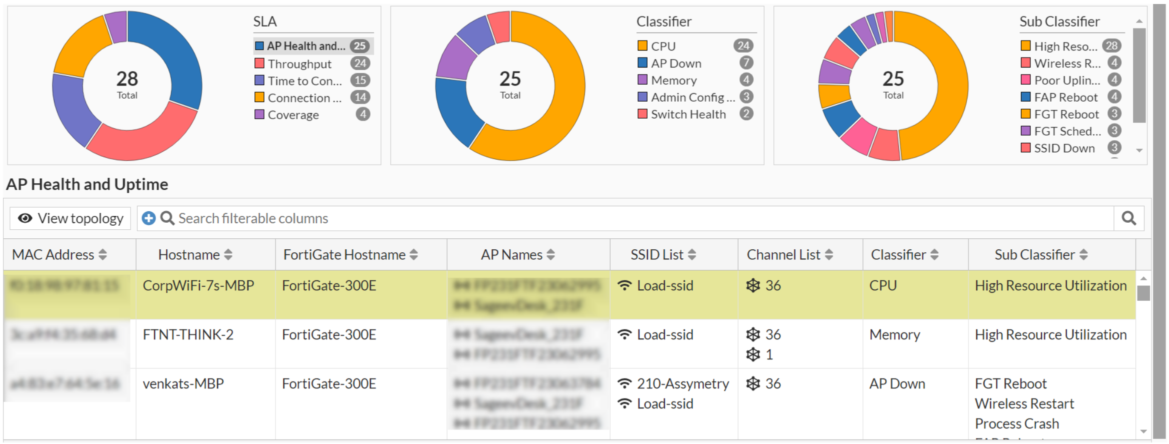
- Impacted SLA
- Impacted Devices
- Network Benchmarks

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 topology** to view the impacted SLA details.

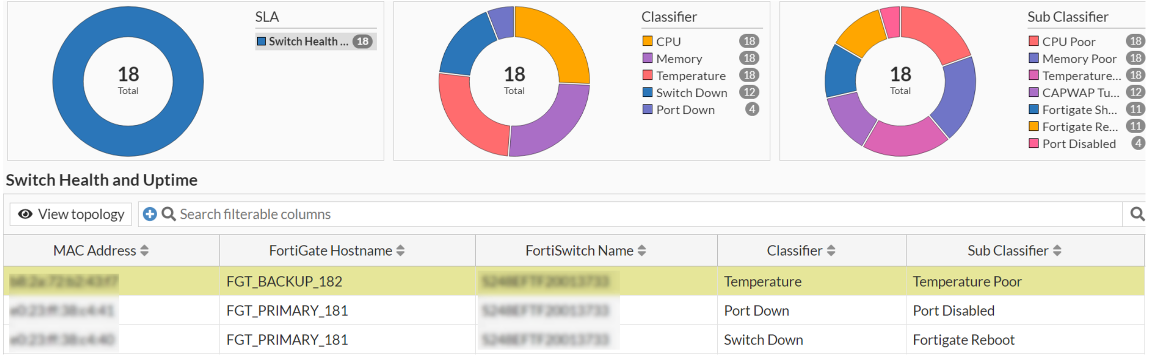


AP Health and Uptime

MAC Address	Hostname	FortiGate Hostname	AP Names	SSID List	Channel List	Classifier	Sub Classifier
[redacted]	CorpWiFi-7s-MBP	FortiGate-300E	[redacted]	Load-ssid	36	CPU	High Resource Utilization
[redacted]	FTNT-THINK-2	FortiGate-300E	[redacted]	Load-ssid	36 1	Memory	High Resource Utilization
[redacted]	venkats-MBP	FortiGate-300E	[redacted]	210-Assymetry Load-ssid	36	AP Down	FGT Reboot Wireless Restart Process Crash

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 topology** to view the impacted SLA details.

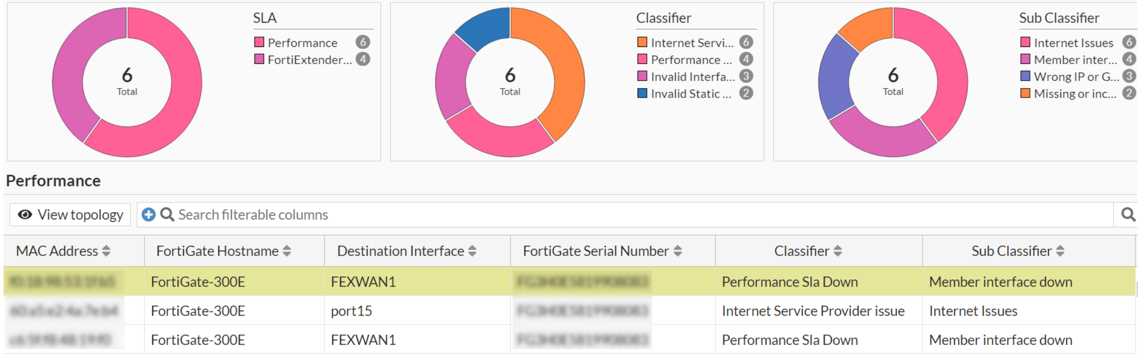


Switch Health and Uptime

MAC Address	FortiGate Hostname	FortiSwitch Name	Classifier	Sub Classifier
[redacted]	FGT_BACKUP_182	[redacted]	Temperature	Temperature Poor
[redacted]	FGT_PRIMARY_181	[redacted]	Port Down	Port Disabled
[redacted]	FGT_PRIMARY_181	[redacted]	Switch Down	Fortigate Reboot

WAN

The WAN 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, FortiSwitch name and serial number, AP name and serial number, classifier and sub-classifier, and the destination interface. Select any row and click on **View topology** to view the impacted SLA details.



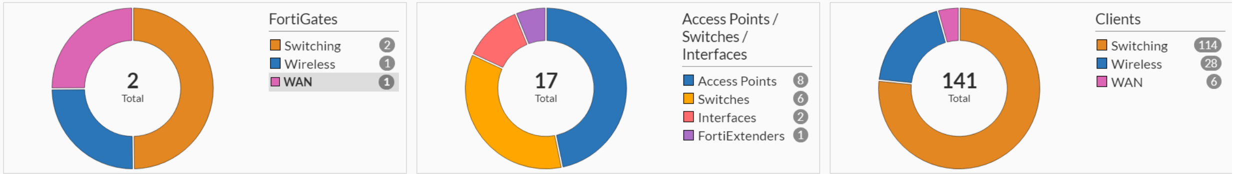
Performance

MAC Address	FortiGate Hostname	Destination Interface	FortiGate Serial Number	Classifier	Sub Classifier
[redacted]	FortiGate-300E	FEXWAN1	[redacted]	Performance Sla Down	Member interface down
[redacted]	FortiGate-300E	port15	[redacted]	Internet Service Provider issue	Internet Issues
[redacted]	FortiGate-300E	FEXWAN1	[redacted]	Performance Sla Down	Member interface down

Select any device listed in the tables and click on **View Topology** for topology and other details. For details on the SLAs, topology, and logs, see section AI Insights.

Impacted Devices

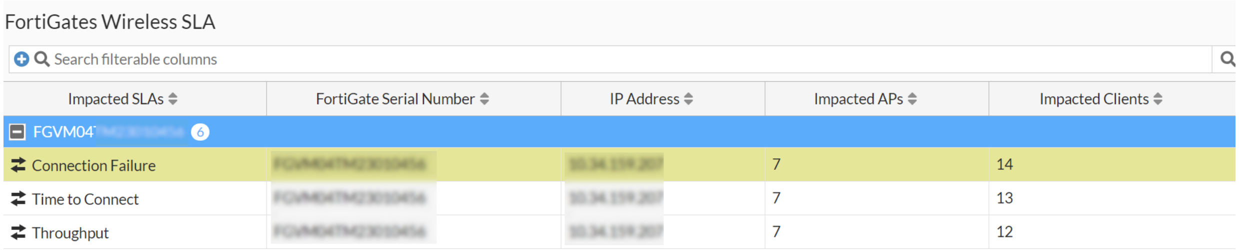
This page displays details of the various devices in your network that are associated with impacted clients, that include the wireless, switching, and WAN clients. You can view and analyze the SLA data based on the device type. The data is displayed in the following three panels. The number of devices 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.

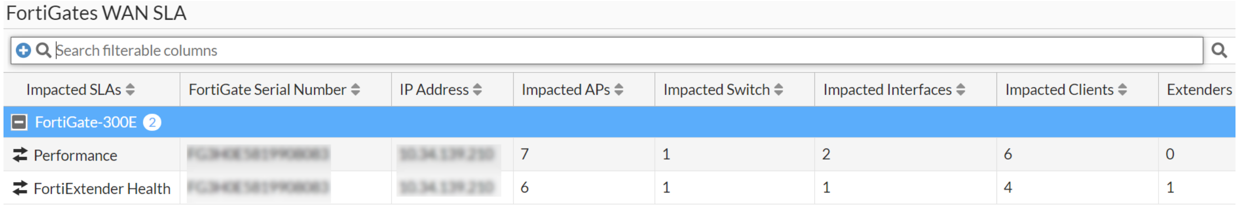


FortiGates Wireless SLA

Search filterable columns

Impacted SLAs	FortiGate Serial Number	IP Address	Impacted APs	Impacted Clients
FGVM04[redacted] 6				
Connection Failure	[redacted]	[redacted]	7	14
Time to Connect	[redacted]	[redacted]	7	13
Throughput	[redacted]	[redacted]	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.

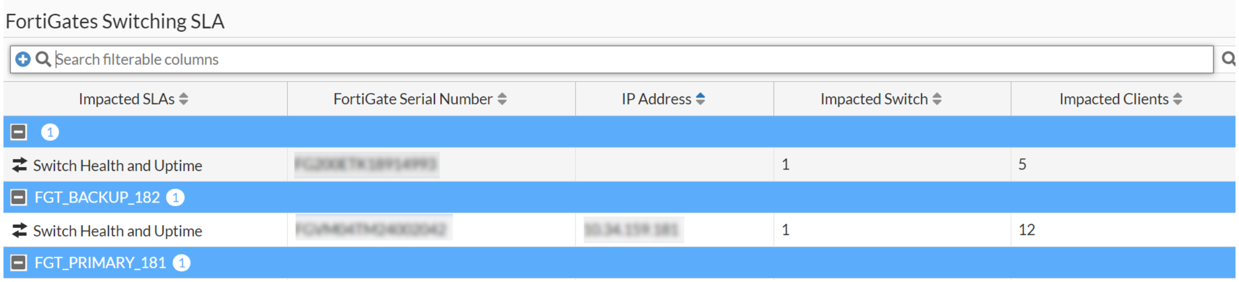


FortiGates WAN SLA

Search filterable columns

Impacted SLAs	FortiGate Serial Number	IP Address	Impacted APs	Impacted Switch	Impacted Interfaces	Impacted Clients	Extenders
FortiGate-300E 2							
Performance	[redacted]	[redacted]	7	1	2	6	0
FortiExtender Health	[redacted]	[redacted]	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

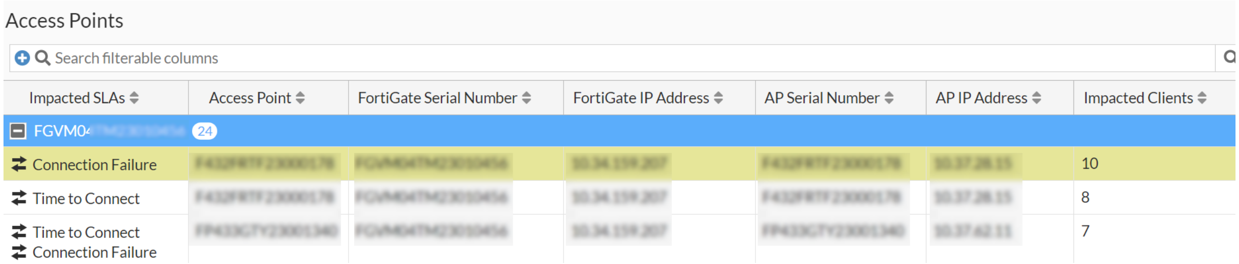
Search filterable columns

Impacted SLAs	FortiGate Serial Number	IP Address	Impacted Switch	Impacted Clients
1				
Switch Health and Uptime	[redacted]		1	5
FGT_BACKUP_182 1				
Switch Health and Uptime	[redacted]	[redacted]	1	12
FGT_PRIMARY_181 1				

Access Points/ Switches/ Interfaces/FortiExtenders

Displays the number of devices, that is, APs, 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.

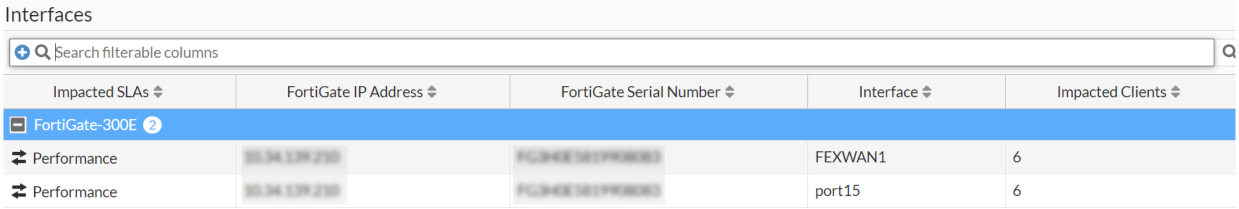


Access Points

Search filterable columns

Impacted SLAs	Access Point	FortiGate Serial Number	FortiGate IP Address	AP Serial Number	AP IP Address	Impacted Clients
FGVM04[redacted] 24						
Connection Failure	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	10
Time to Connect	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	8
Time to Connect Connection Failure	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	7

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.

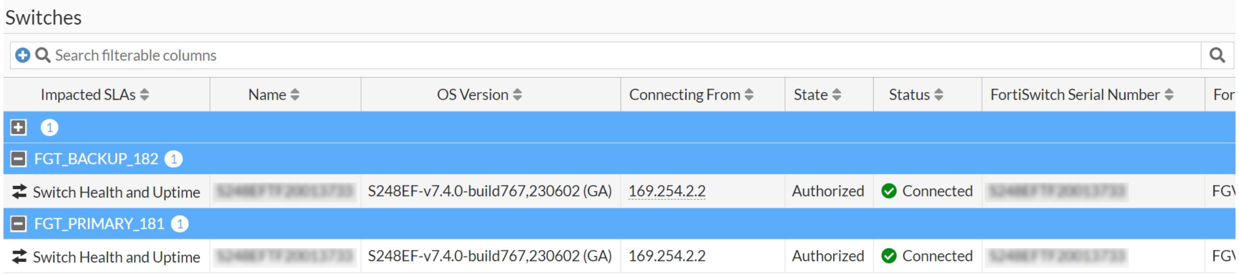


Interfaces

Search filterable columns

Impacted SLAs	FortiGate IP Address	FortiGate Serial Number	Interface	Impacted Clients
FortiGate-300E 2				
Performance	[redacted]	[redacted]	FEXWAN1	6
Performance	[redacted]	[redacted]	port15	6

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.

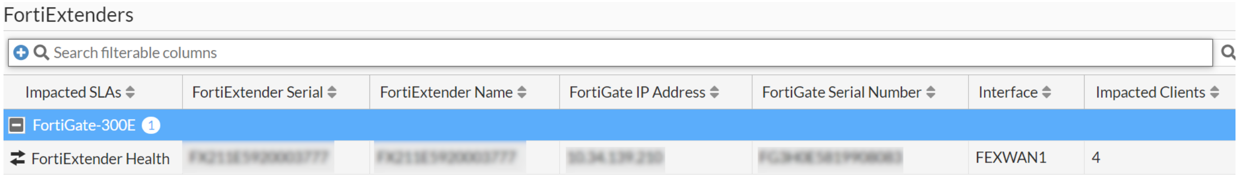


Switches

Search filterable columns

Impacted SLAs	Name	OS Version	Connecting From	State	Status	FortiSwitch Serial Number	For
1							
FGT_BACKUP_182 1							
Switch Health and Uptime	[redacted]	S248EF-v7.4.0-build767,230602 (GA)	169.254.2.2	Authorized	✓ Connected	[redacted]	FG\
FGT_PRIMARY_181 1							
Switch Health and Uptime	[redacted]	S248EF-v7.4.0-build767,230602 (GA)	169.254.2.2	Authorized	✓ Connected	[redacted]	FG\

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.



FortiExtenders

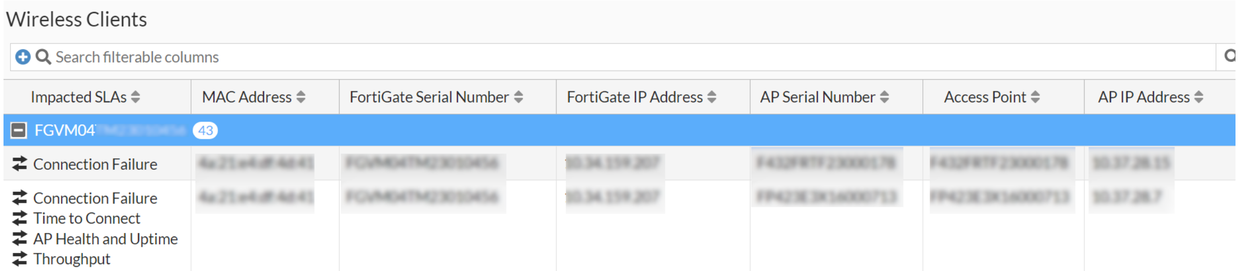
Search filterable columns

Impacted SLAs	FortiExtender Serial	FortiExtender Name	FortiGate IP Address	FortiGate Serial Number	Interface	Impacted Clients
FortiGate-300E 1						
FortiExtender Health	[redacted]	[redacted]	[redacted]	[redacted]	FEXWAN1	4

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.

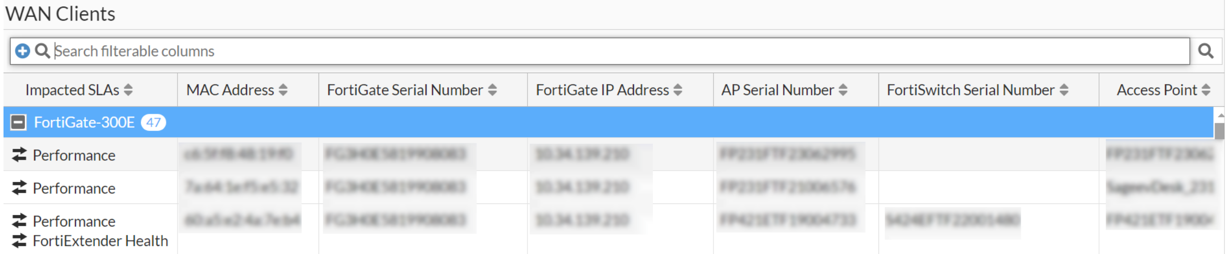


Wireless Clients

Search filterable columns

Impacted SLAs	MAC Address	FortiGate Serial Number	FortiGate IP Address	AP Serial Number	Access Point	AP IP Address
⊟ FGVM04[redacted] 43						
Connection Failure	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Connection Failure Time to Connect AP Health and Uptime Throughput	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

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.

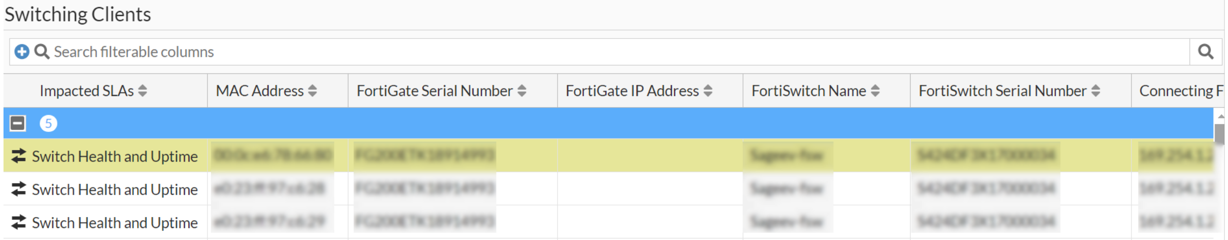


WAN Clients

Search filterable columns

Impacted SLAs	MAC Address	FortiGate Serial Number	FortiGate IP Address	AP Serial Number	FortiSwitch Serial Number	Access Point
⊟ FortiGate-300E 47						
Performance	[redacted]	[redacted]	[redacted]	[redacted]		[redacted]
Performance	[redacted]	[redacted]	[redacted]	[redacted]		[redacted]
Performance FortiExtender Health	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

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.



Switching Clients

Search filterable columns

Impacted SLAs	MAC Address	FortiGate Serial Number	FortiGate IP Address	FortiSwitch Name	FortiSwitch Serial Number	Connecting F
⊟ 5						
Switch Health and Uptime	[redacted]	[redacted]		[redacted]	[redacted]	[redacted]
Switch Health and Uptime	[redacted]	[redacted]		[redacted]	[redacted]	[redacted]
Switch Health and Uptime	[redacted]	[redacted]		[redacted]	[redacted]	[redacted]

Network Benchmarks

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

- SD-WAN
- Wireless
- Device Health

SD-WAN

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

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

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

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

- Pre-requisites
- Recommendations

Pre-requisites

The SD-WAN SLA monitors and measures the health of links that are connected to SD-WAN members based on SLA log messages (*pass* and *fail*), to predict the performance. Configure the SD-WAN health check in FortiGate as shown in the following example.

```
config system sdwan
   config health-check
      edit "<Health Check Name>"
         set sla-fail-log-period 60
         set sla-pass-log-period 60
```

For more details, see Link Health Monitor.

Recommendations

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

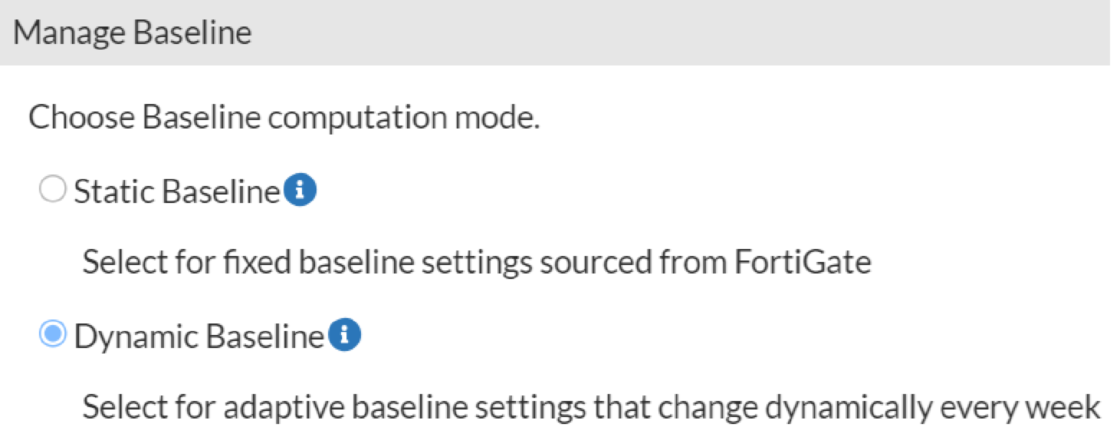
- Use a time interval of 60 seconds for `sla-fail-log-period` and `sla-pass-log-period` for high accuracy.
- Enable `ntp sync` for accurate SD-WAN forecast and anomaly detection.

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

- Configure Baselines
- Performance Summary
- Health Check Trends
- Anomalies

Configure Baselines

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



Manage Baseline

Choose Baseline computation mode.

○ Static Baseline

Select for fixed baseline settings sourced from FortiGate

● Dynamic Baseline

Select for adaptive baseline settings that change dynamically every week

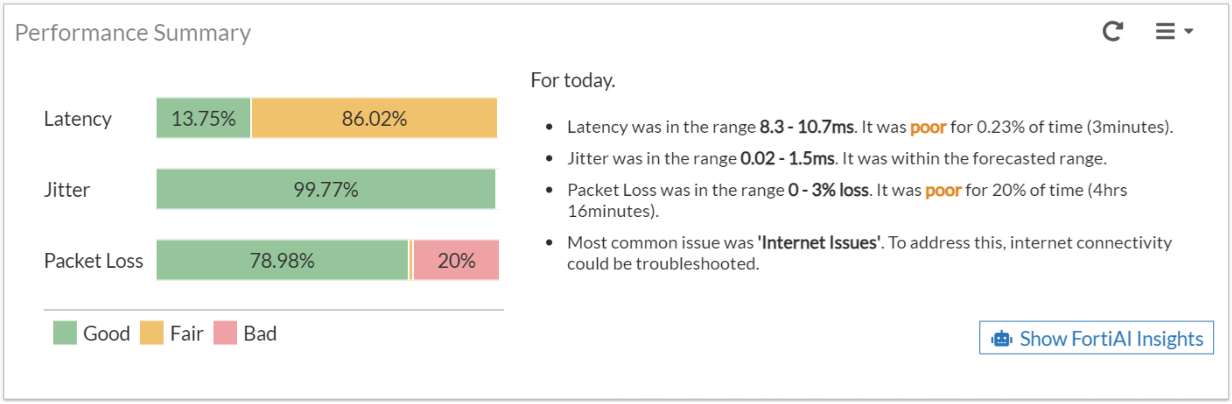
- **Static Baseline** - These baselines are SLA targets configured in FortiGate or FortiAIOps default thresholds, for jitter, packet loss, and latency. If the SLA targets are not specified in FortiGate, then the following default baselines are used for all the 3 metrics.
  - Latency - 100 ms
  - Jitter - 30 ms
  - Packet Loss - 1 %

  Dynamic Baseline - These baseline values are calculated using real-time data from the previous week and are updated dynamically, every week, for jitter, packet loss, and latency. This is the default baseline mode.

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

Performance Summary

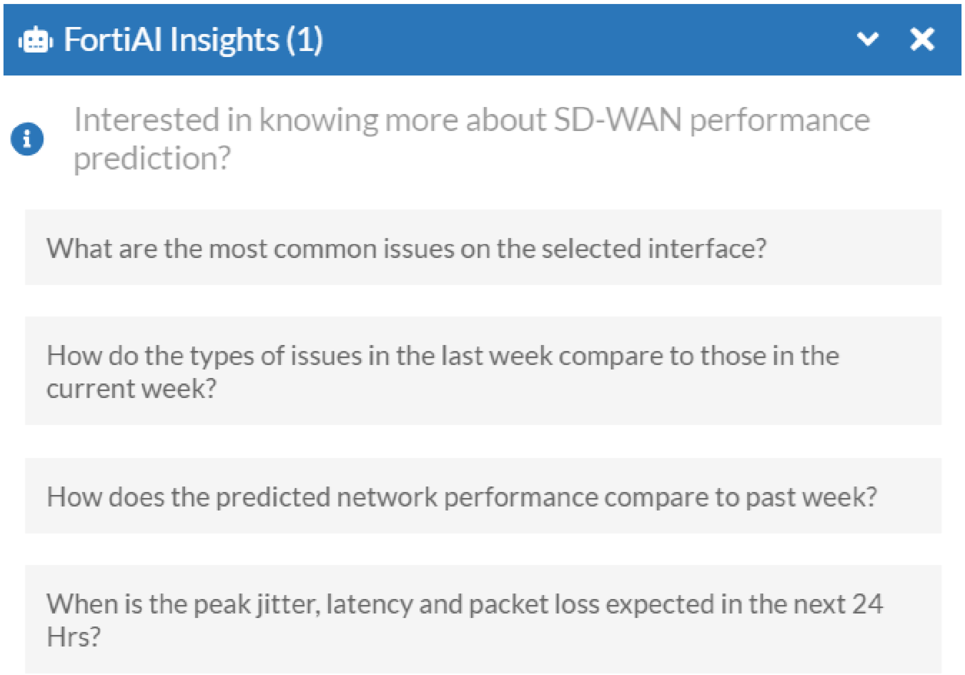
The **Performance Summary** panel provides the statistics for the WAN interface's performance based on the jitter, packet loss, and latency metrics. The events reported are categorized as good, fair, and bad, based on the metric performance with respect to the configured or calculated thresholds. This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



For today.

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

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



Interested in knowing more about SD-WAN performance prediction?

What are the most common issues on the selected interface?

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

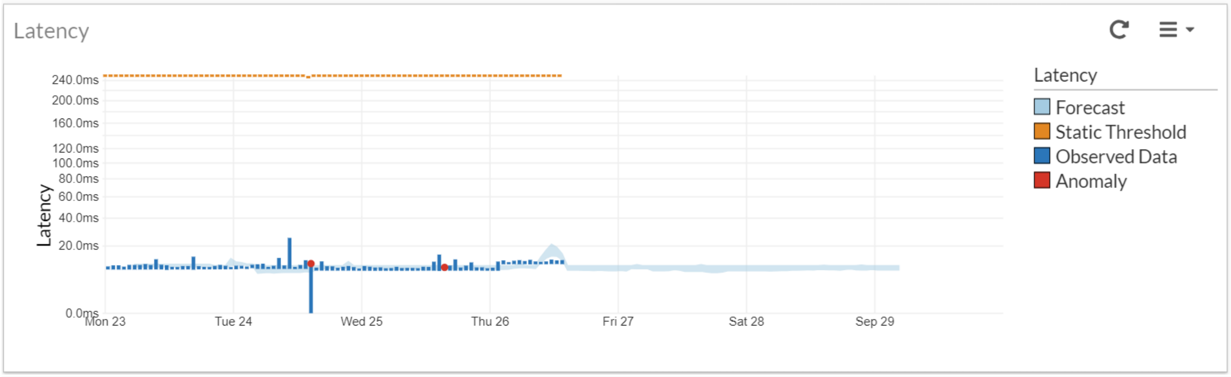
How does the predicted network performance compare to past week?

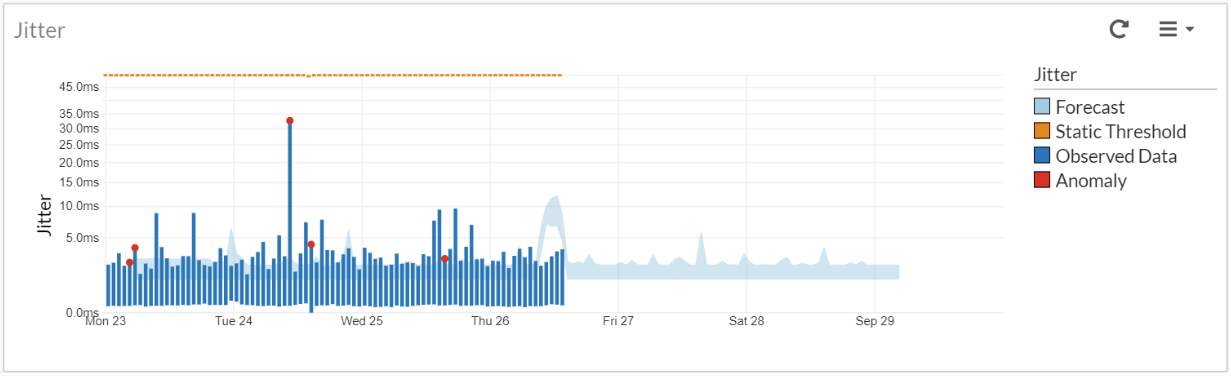
When is the peak jitter, latency and packet loss expected in the next 24 Hrs?

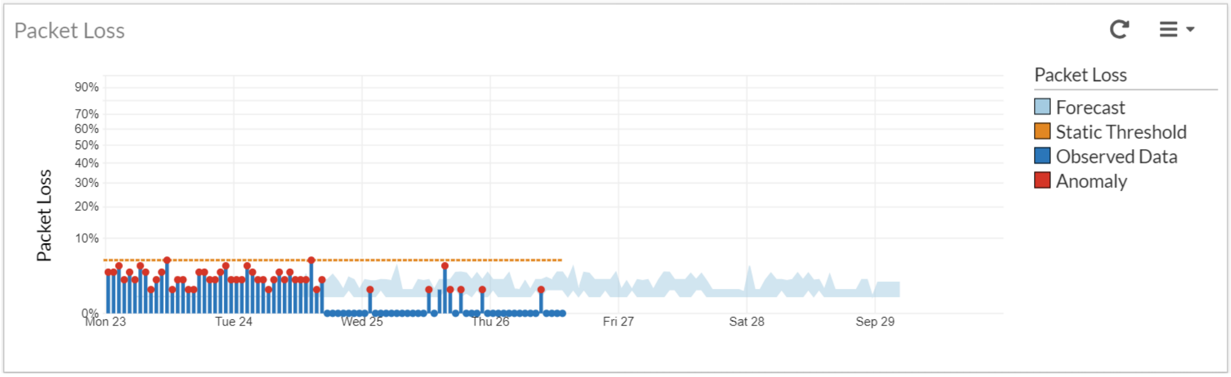
Health Check Trends

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

Note: The trends displayed are on an hourly basis.



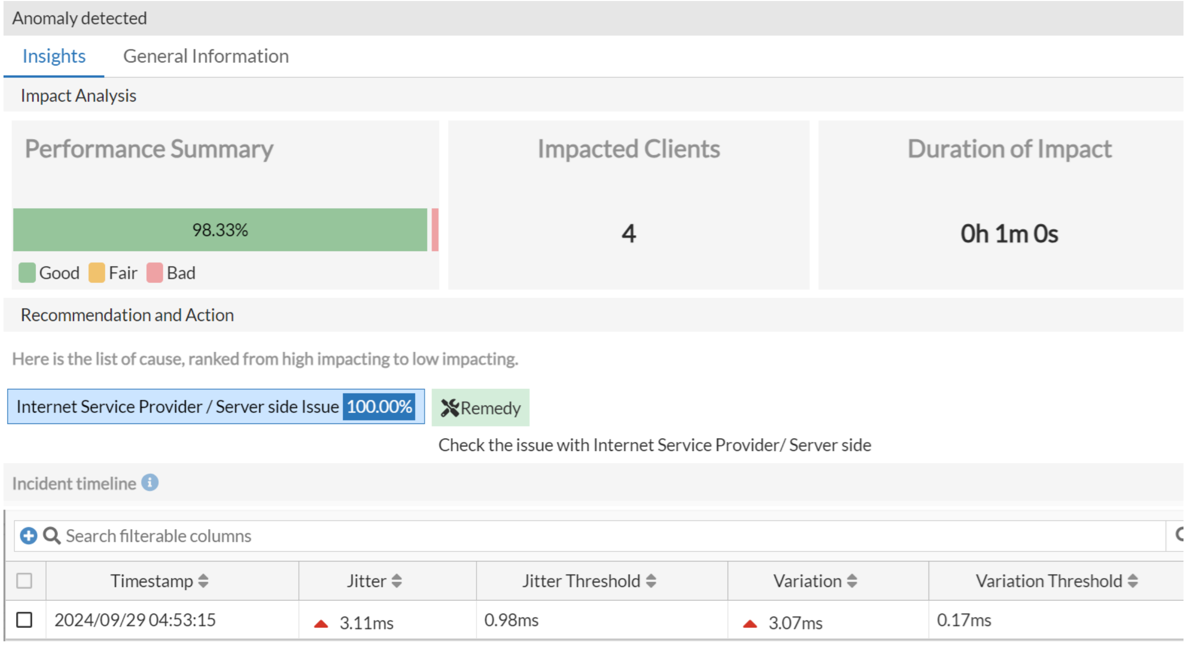




- **Forecast** - This is indicative of the range predicted by FortiAIOps based on historical statistics.
- **Observed Data** - This is the range of real time statistics observed in a given hour.
- **Anomaly** - Anomalies are reported when FortiAIOps observes a deviation in the data exceeding the usual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

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

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



Anomaly detected

Insights | General Information

Impact Analysis

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

Recommendation and Action

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

Internet Service Provider / Server side Issue 100.00% | Remedy

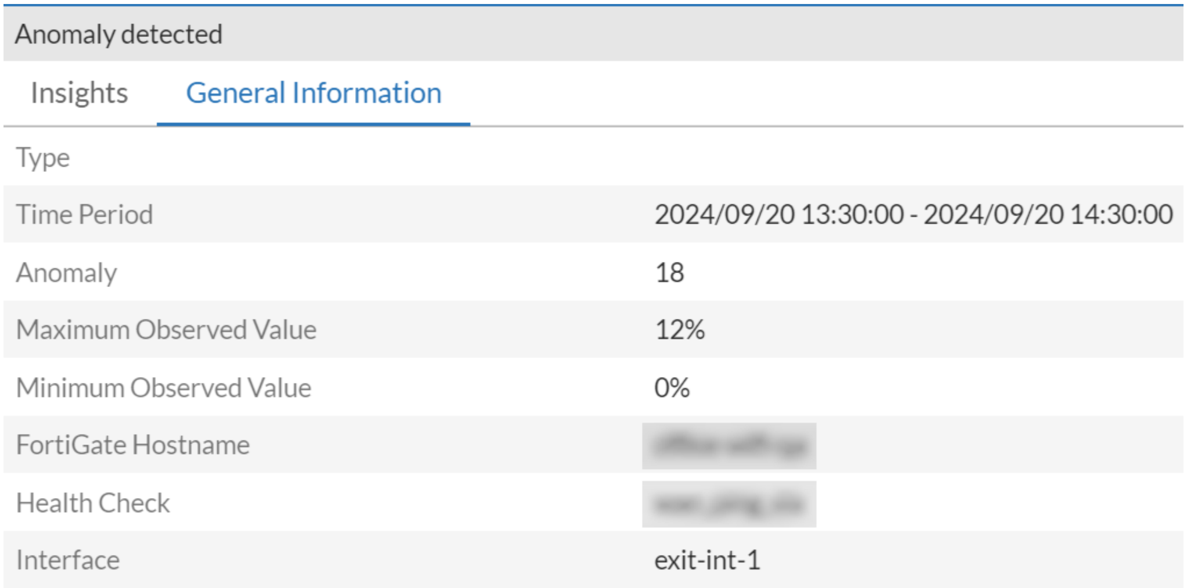
Check the issue with Internet Service Provider/ Server side

Incident timeline

Search filterable columns

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

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



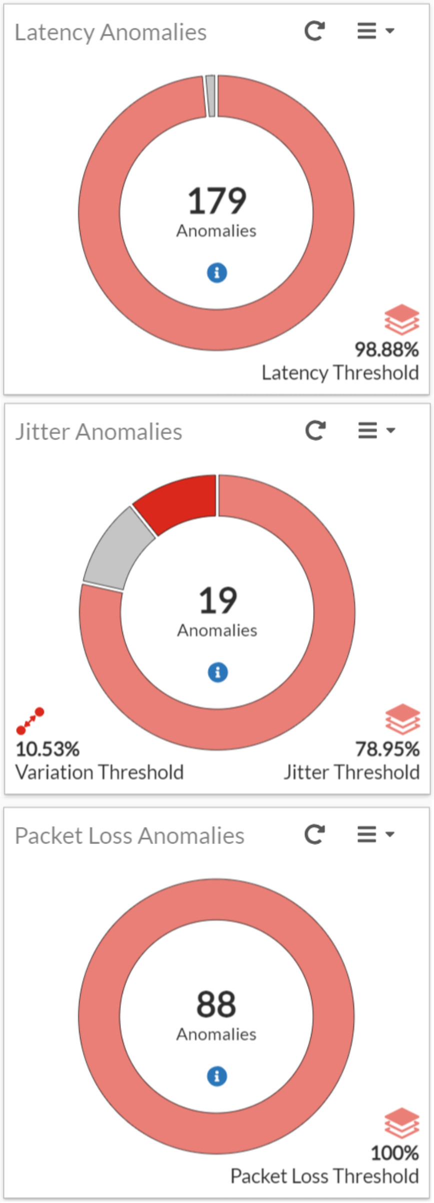
Anomaly detected

Insights | General Information

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

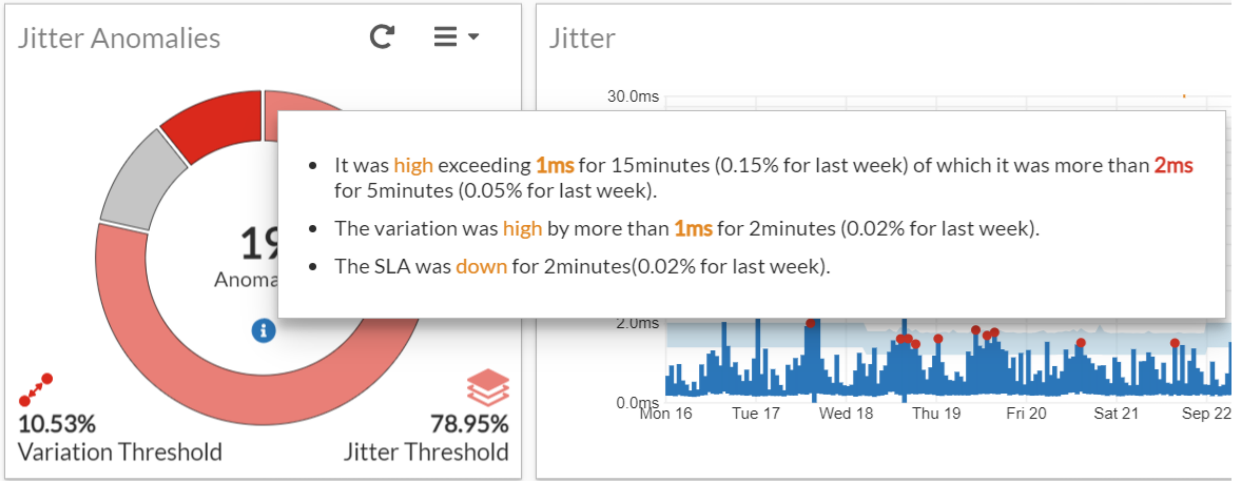
Anomalies

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



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

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



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

Wireless

You can configure the following wireless SLAs in this page.

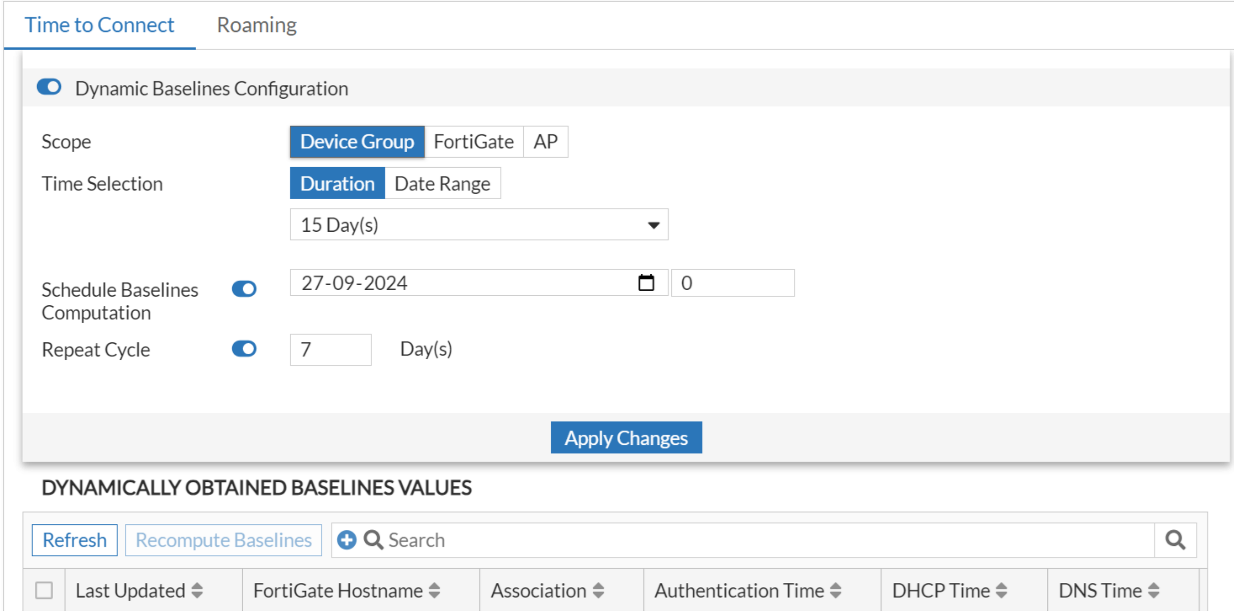
- Time To Connect
- Roaming

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: Device Group

Time Selection: Duration, 15 Day(s)

Schedule Baselines Computation: 27-09-2024 0

Repeat Cycle: 7 Day(s)

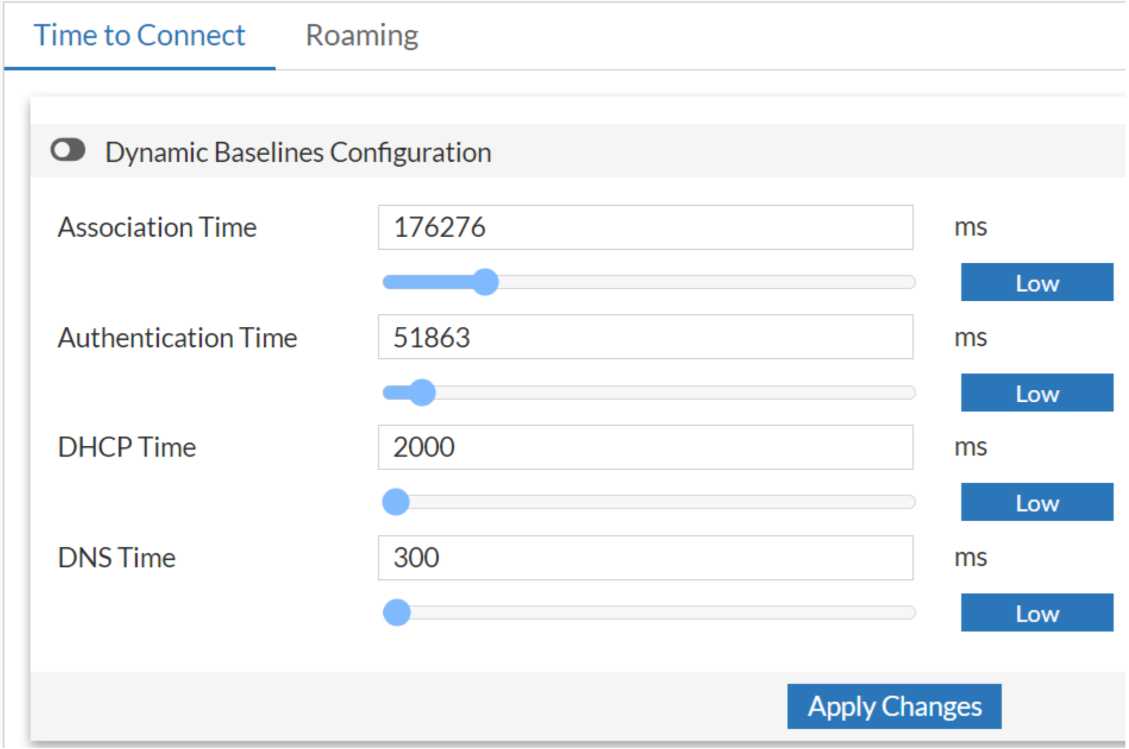
□	Last Updated	FortiGate Hostname	Association	Authentication Time	DHCP Time	DNS Time

- **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 176276 ms Low

Authentication Time 51863 ms Low

DHCP Time 2000 ms Low

DNS Time 300 ms Low

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

Notes:

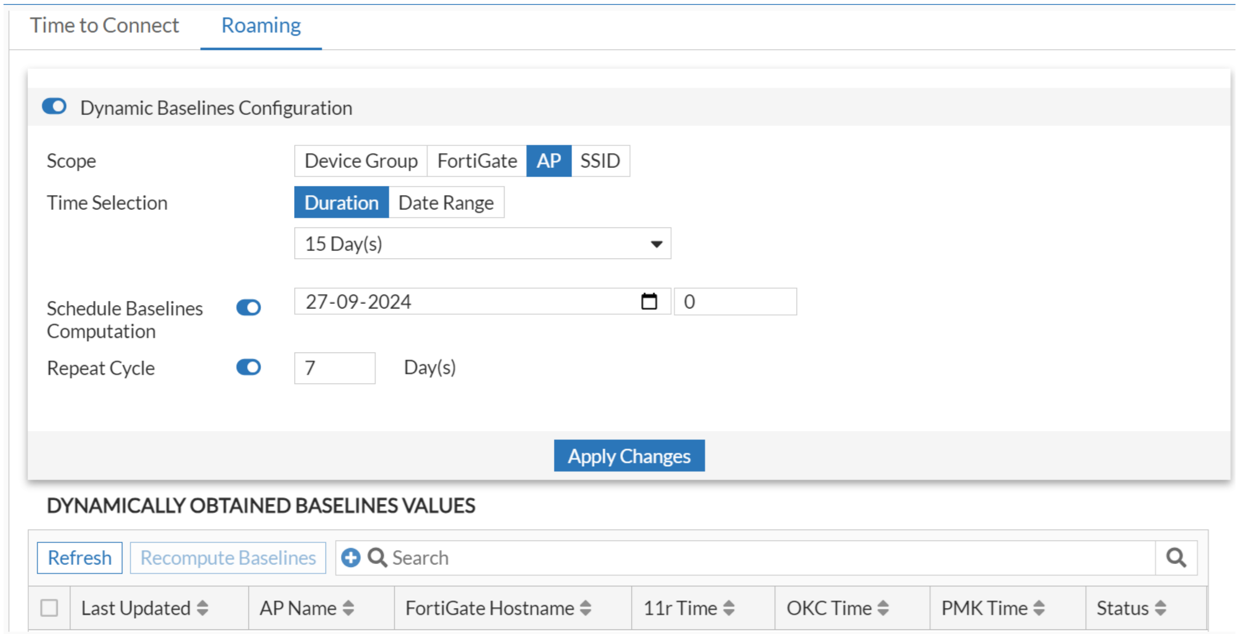
- The default value for these parameters is 300 milliseconds and the valid range is 1 - 1000000 milliseconds.
- DNS is not supported.

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.



Dynamic Baselines Configuration

Scope: Device Group | FortiGate | AP | SSID

Time Selection: Duration | Date Range

15 Day(s)

Schedule Baselines Computation: 27-09-2024 0

Repeat Cycle: 7 Day(s)

DYNAMICALLY OBTAINED BASELINES VALUES

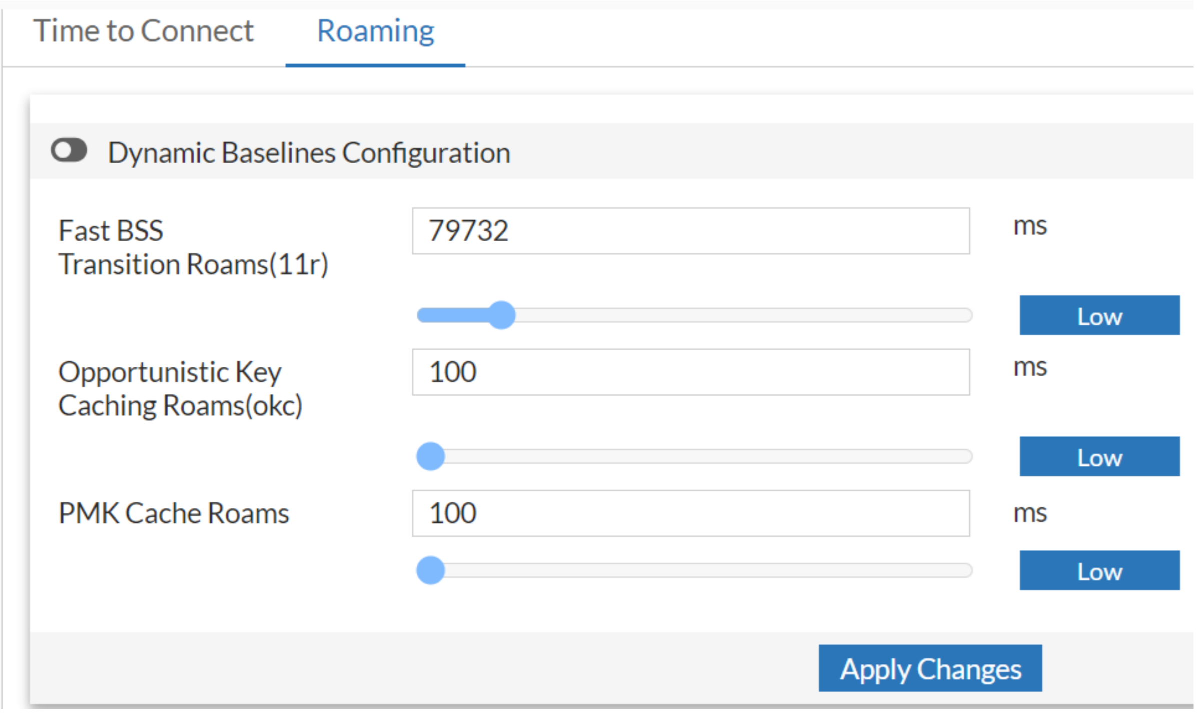
□	Last Updated	AP Name	FortiGate Hostname	11r Time	OKC Time	PMK Time	Status

- **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): 79732 ms — Low

Opportunistic Key Caching Roams(okc): 100 ms — Low

PMK Cache Roams: 100 ms — Low

- **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.

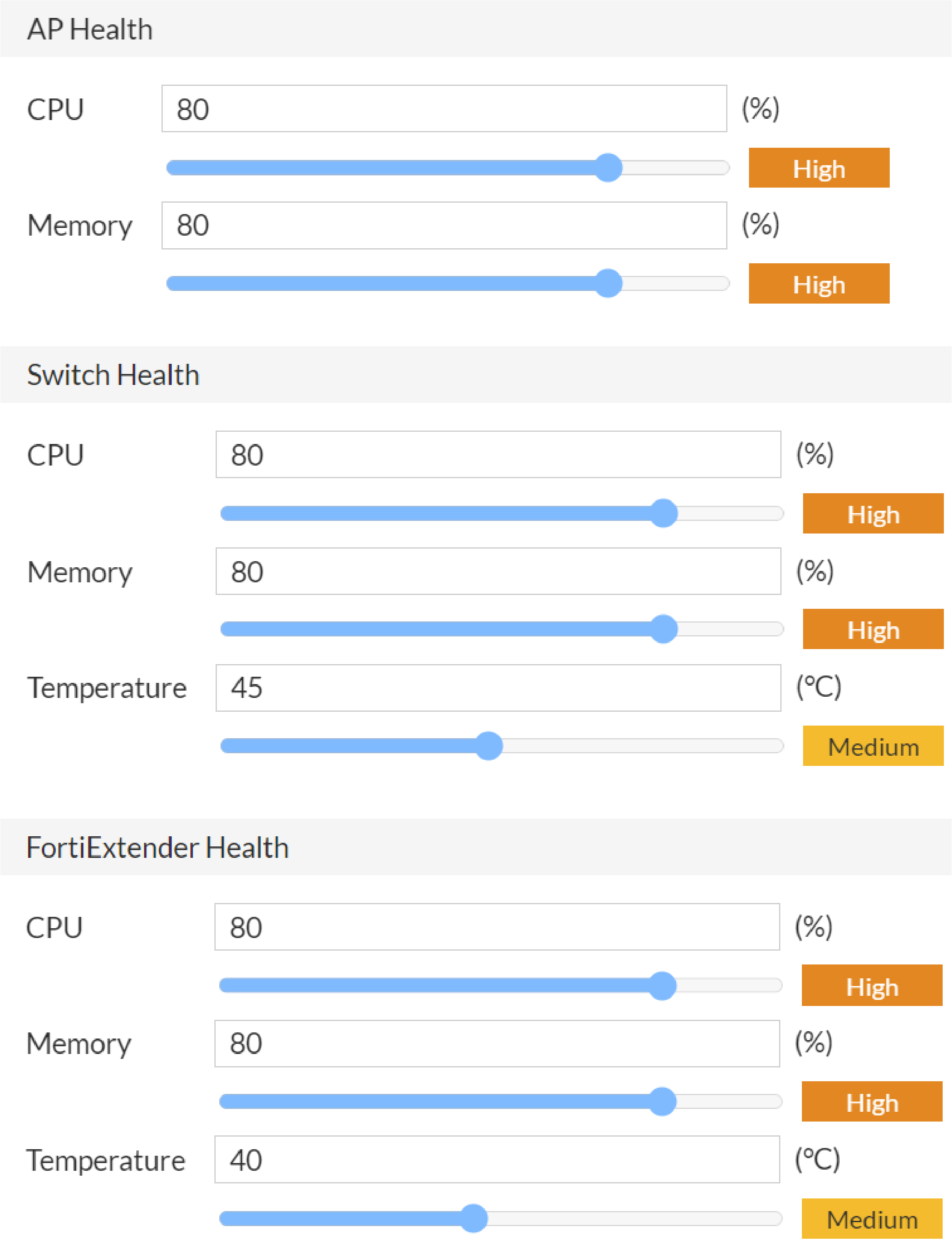
Device Health

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 configuration > Device Health** to configure the following parameters.

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

- **Temperature**



AP Health

CPU: 80 (%) — High

Memory: 80 (%) — High

Switch Health

CPU: 80 (%) — High

Memory: 80 (%) — High

Temperature: 45 (°C) — Medium

FortiExtender Health

CPU: 80 (%) — High

Memory: 80 (%) — High

Temperature: 40 (°C) — Medium

The default value for the CPU and memory parameters is 80% and the default value for the temperature is 45 degree Celsius.

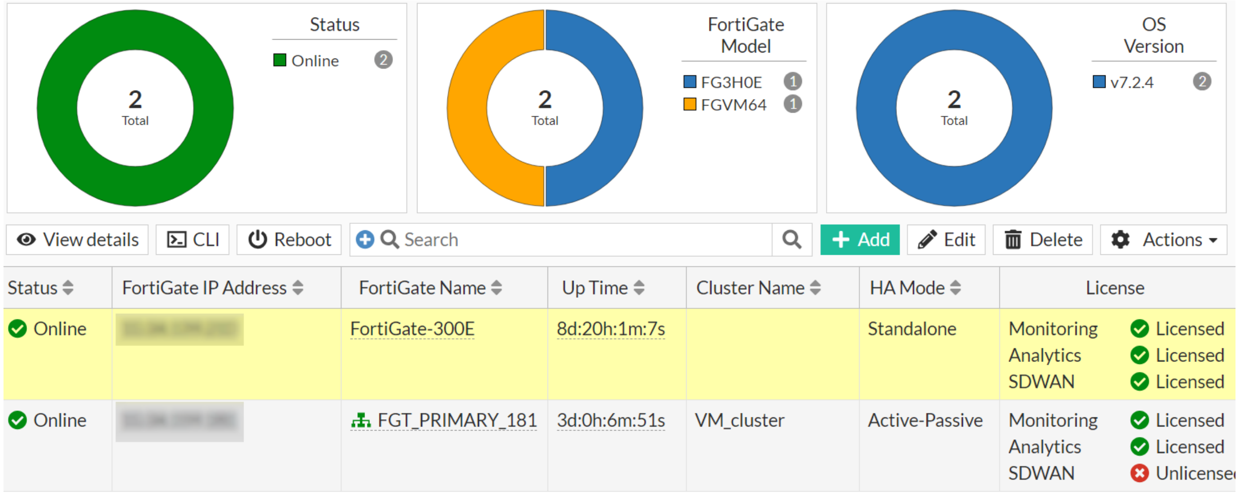
Inventory

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.



Status	FortiGate IP Address	FortiGate Name	Up Time	Cluster Name	HA Mode	License
✓ Online	[redacted]	FortiGate-300E	8d:20h:1m:7s		Standalone	Monitoring ✓ Licensed Analytics ✓ Licensed SDWAN ✓ Licensed
✓ Online	[redacted]	FGT_PRIMARY_181	3d:0h:6m:51s	VM_cluster	Active-Passive	Monitoring ✓ Licensed Analytics ✓ Licensed SDWAN ✖ Unlicense

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.

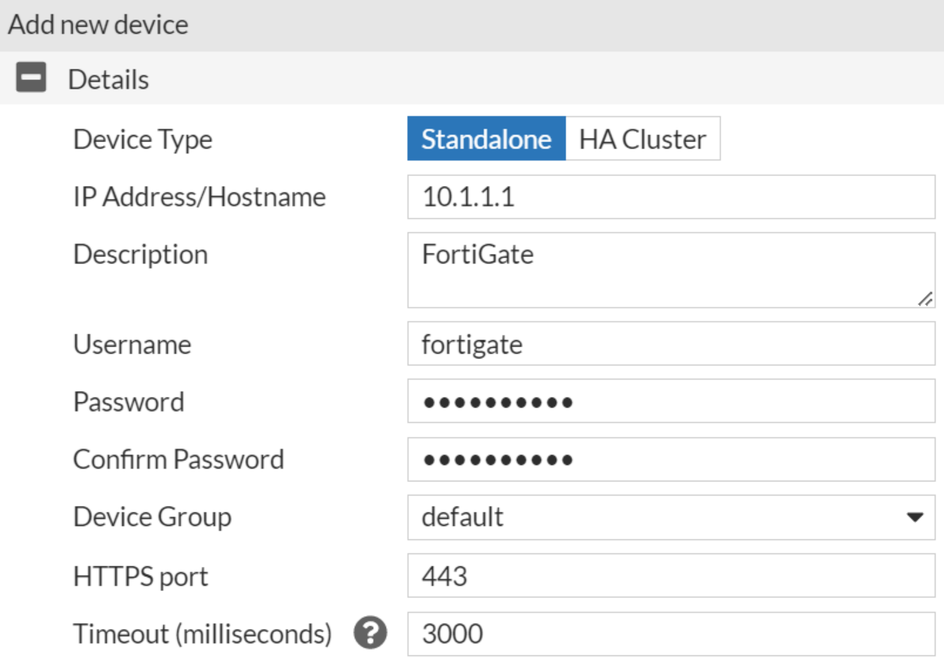
The managed FortiGate IP address/FQDN configured in FortiAIOps must match the Subject Alternative Name (SAN) in the FortiGate certificate, else, the FortiGate discovery fails.

- 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.



Add new device

Details

Device Type	Standalone / HA Cluster
IP Address/Hostname	10.1.1.1
Description	FortiGate
Username	fortigate
Password	••••••••••
Confirm Password	••••••••••
Device Group	default
HTTPS port	443
Timeout (milliseconds)	3000

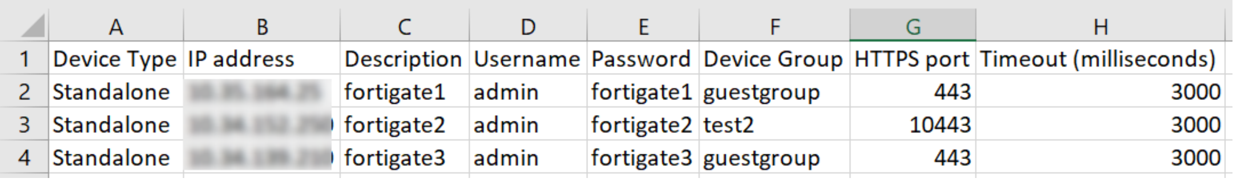
1. Select **Standalone** or **HA Cluster** if the FortiGate is an HA cluster.
2. Enter the **IP Address** or FQDN of the controller and an optional **Description**.
   Note: If a 3rd party certificate is used by FortiGate then ensure to install a valid CA certificate in FortiAIOps.
3. Enter the **Username** 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 3000 milliseconds.

The added FortiGate controller is now listed.

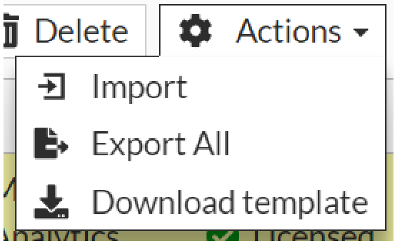
Importing and Exporting FortiGates

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.



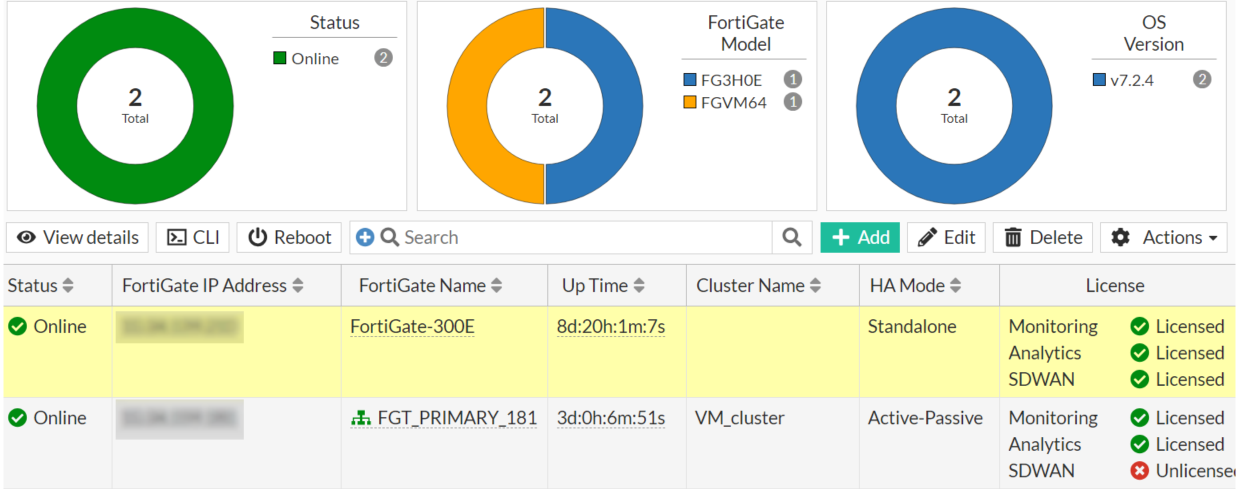
Select **Import** to upload the FortiGate configuration file.

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

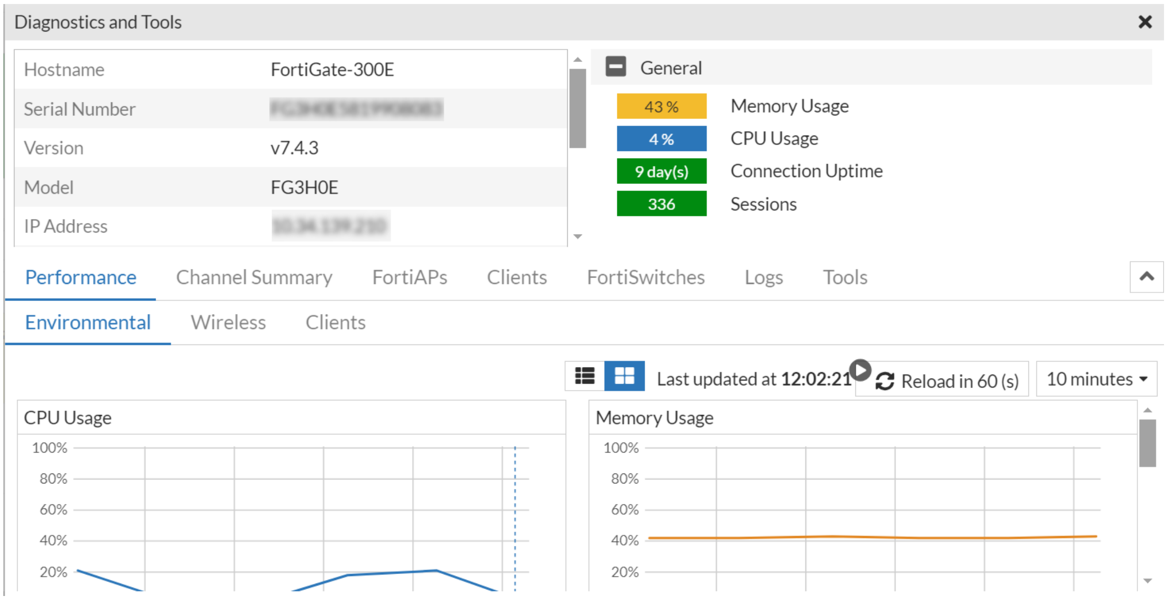
This page provides analytical information related to the performance of various elements and processes in your network. The data is visually represented with interactive options to drill-down and filter specific information. This enables monitoring, diagnostic, and troubleshooting operations for connectivity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



Status	FortiGate IP Address	FortiGate Name	Up Time	Cluster Name	HA Mode	License	
✓ Online	[redacted]	FortiGate-300E	8d:20h:1m:7s		Standalone	Monitoring Analytics SDWAN	✓ Licensed ✓ Licensed ✓ Licensed
✓ Online	[redacted]	FGT_PRIMARY_181	3d:0h:6m:51s	VM_cluster	Active-Passive	Monitoring Analytics SDWAN	✓ Licensed ✓ Licensed ✗ Unlicense

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

- **Reboot** - Select a FortiGate controller to reboot and click **Reboot**.
- **CLI** - Select a FortiGate controller and select **CLI** to access the CLI interface.
- **Edit and Delete** - Select a FortiGate controller and click **Edit** (to update configuration) or **Delete** (to remove the FortiGate).
- **View Details** - Select a FortiGate for **Diagnostics and tools**. This pane displays details about the selected FortiGate and also provides diagnostic tools for your network.



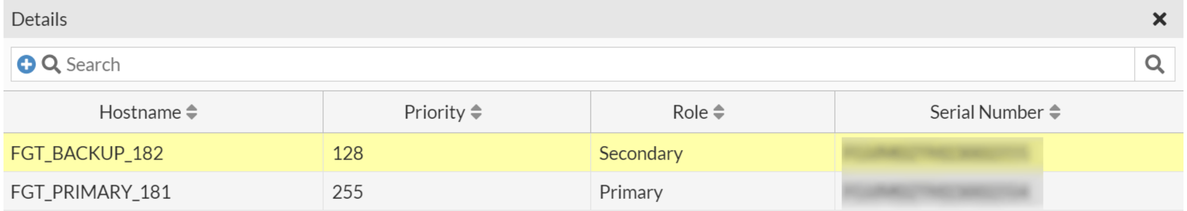
Diagnostics and Tools

Hostname	FortiGate-300E
Serial Number	[redacted]
Version	v7.4.3
Model	FG3H0E
IP Address	[redacted]

General

43 %	Memory Usage
4 %	CPU Usage
9 day(s)	Connection Uptime
336	Sessions

To view details of the HA cluster, click on the icon in the **FortiGate Name** column.



Details

Search

Hostname	Priority	Role	Serial Number
FGT_BACKUP_182	128	Secondary	[redacted]
FGT_PRIMARY_181	255	Primary	[redacted]

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.

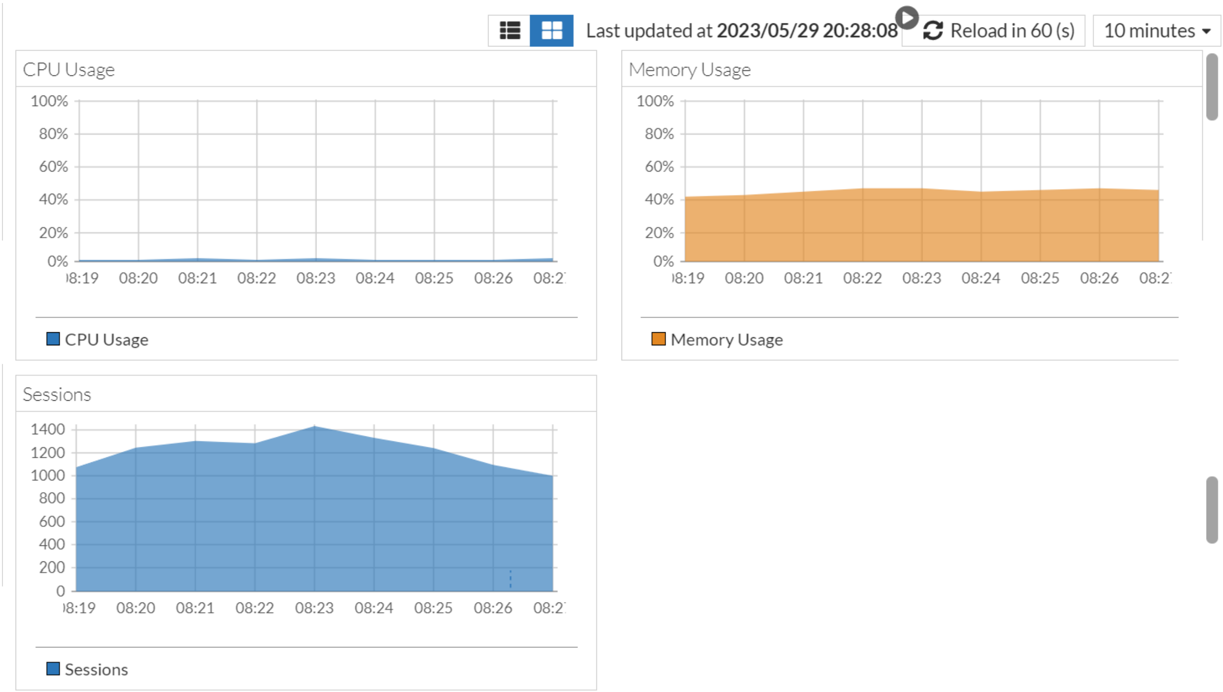
- Click ⟳ to manually refresh data.
- Click ⏸ to pause the auto-refresh.
- Click ▶ to resume the auto-refresh.

Performance is displayed for the following.

- Environmental
- Wireless
- Clients

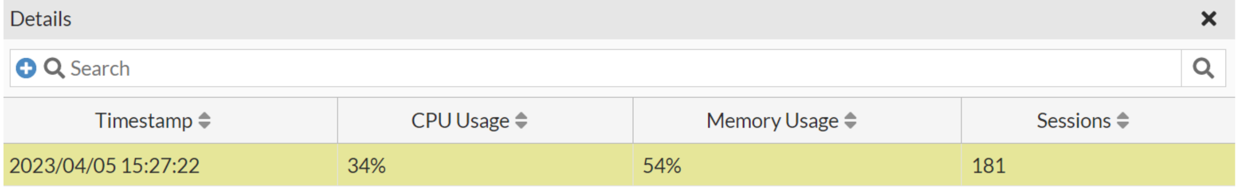
Environmental

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



Last updated at **2023/05/29 20:28:08** ⟳ Reload in 60 (s) 10 minutes

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



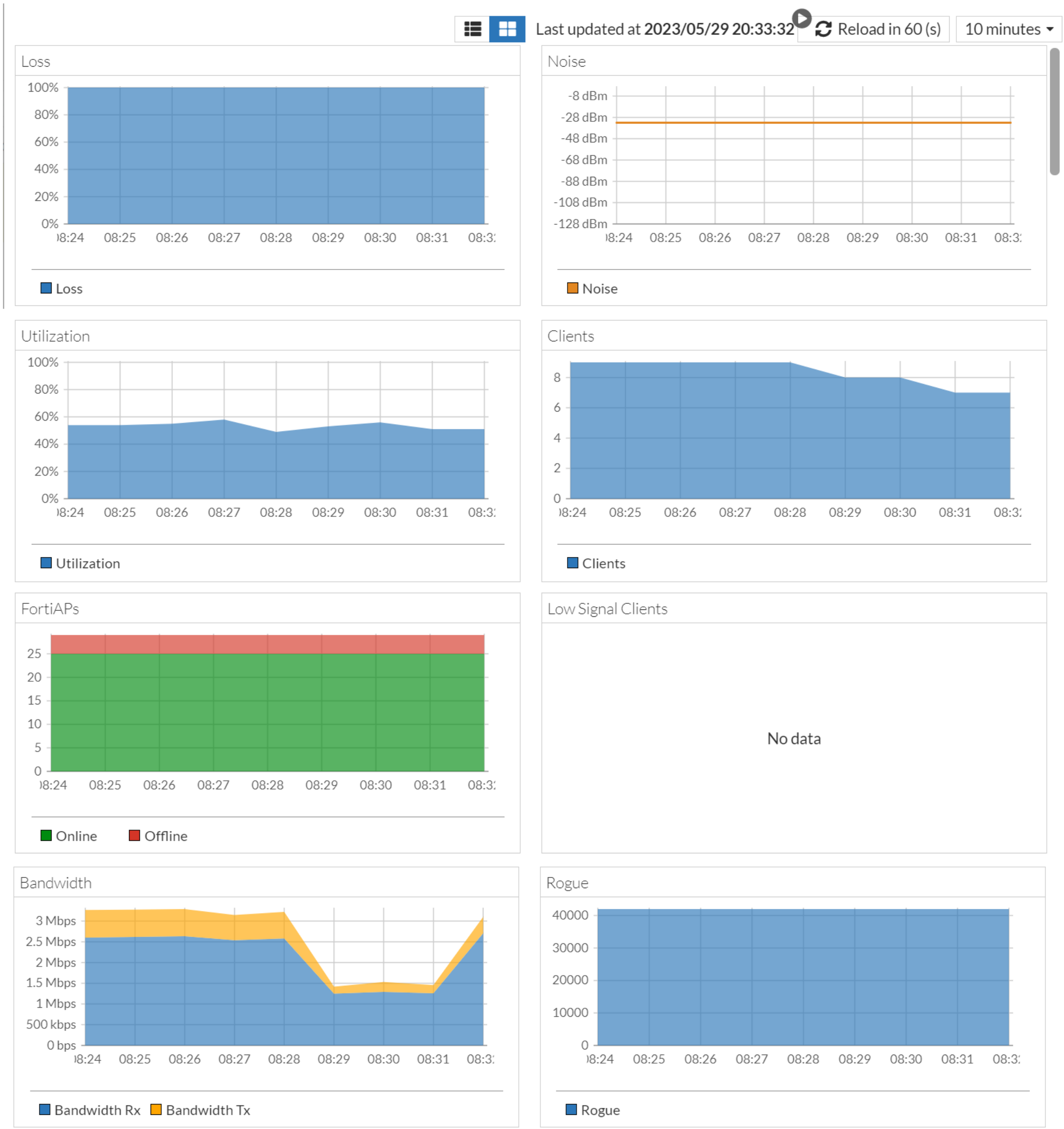
Details ✕

Search

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.


Last updated at 2023/05/29 20:33:32

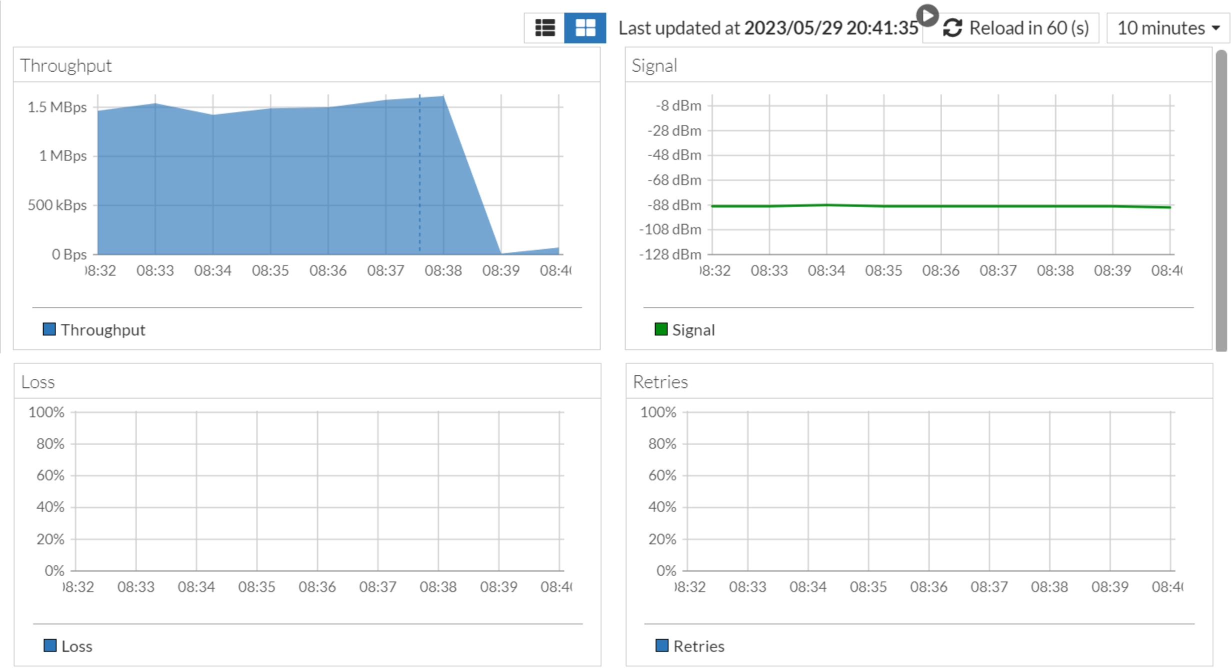
Reload in 60 (s)

10 minutes

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.

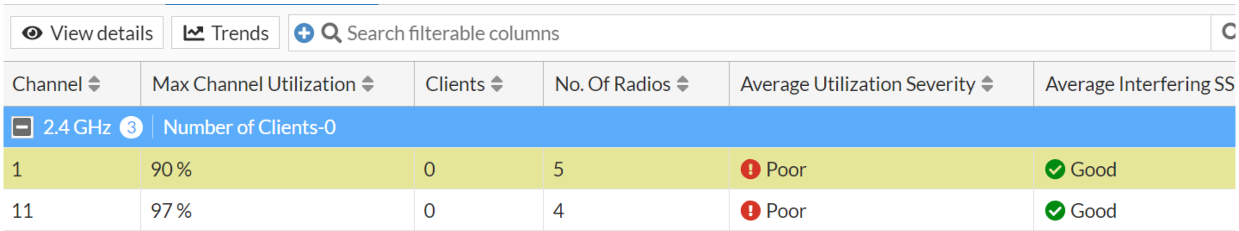


Last updated at **2023/05/29 20:41:35** Reload in 60 (s) 10 minutes

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.



Channel	Max Channel Utilization	Clients	No. Of Radios	Average Utilization Severity	Average Interfering SS
2.4 GHz 3	Number of Clients-0				
1	90 %	0	5	Poor	Good
11	97 %	0	4	Poor	Good

FortiAPs

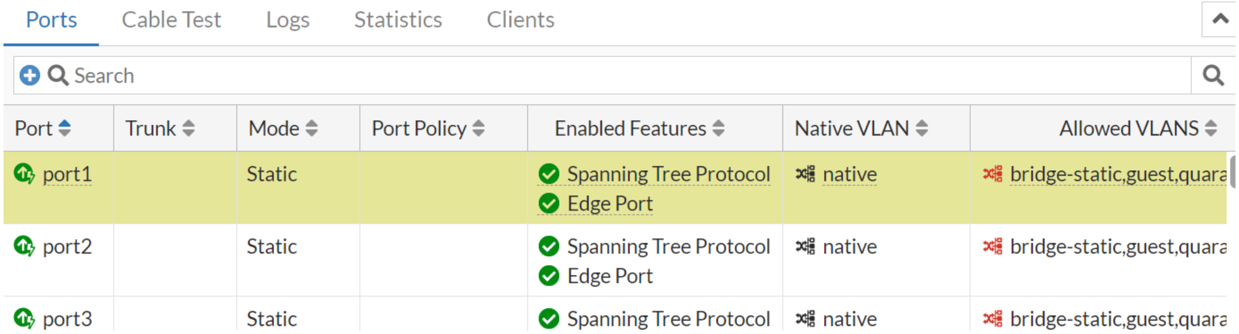
This tab displays details about the selected access point with their status and details. To view the details, select an access point and click **View Details**. For more information on the diagnostic options and details see Access Points.

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 Clients on page 160.

FortiSwitch

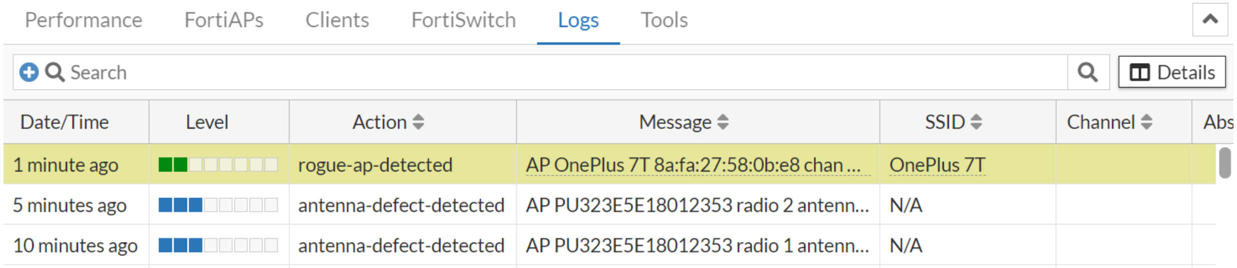
This tab displays a graphical snapshot of the FortiSwitch activity such as, the total number of FortiSwitches, their status (online/offline), and the deployed model details. To view the details, select a FortiSwitch and click **View Details**. For more information on the diagnostic options and details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



Port	Trunk	Mode	Port Policy	Enabled Features	Native VLAN	Allowed VLANS
port1		Static		✓ Spanning Tree Protocol ✓ Edge Port	native	bridge-static,guest,quara
port2		Static		✓ Spanning Tree Protocol ✓ Edge Port	native	bridge-static,guest,quara
port3		Static		✓ Spanning Tree Protocol	native	bridge-static,guest,quara

Logs

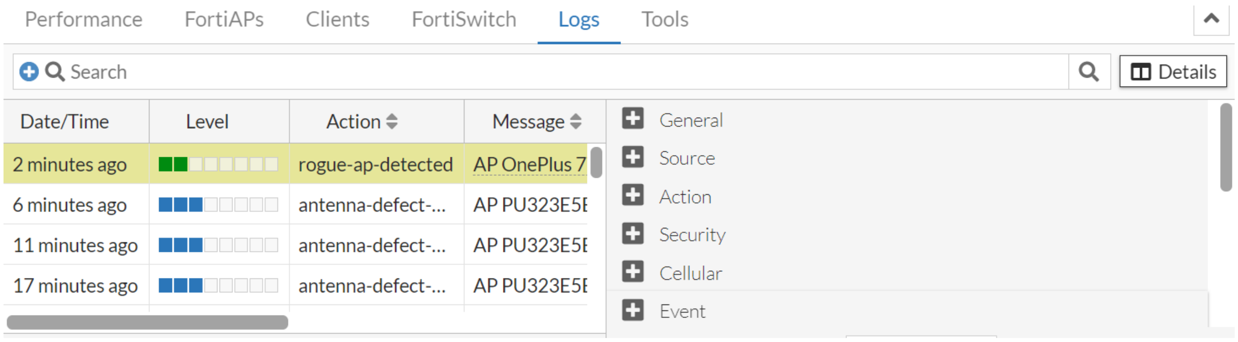
This tab displays the detailed FortiGate event logs and each event is assigned a severity, that is depicted with a color code. Hover over the color bar in the **Level** column to view the severity.



Date/Time	Level	Action	Message	SSID	Channel	Abs
1 minute ago	🟩🟩□□□□□□	rogue-ap-detected	AP OnePlus 7T 8a:fa:27:58:0b:e8 chan ...	OnePlus 7T		
5 minutes ago	🟦🟦🟦□□□□□	antenna-defect-detected	AP PU323E5E18012353 radio 2 antenn...	N/A		
10 minutes ago	🟦🟦🟦□□□□□	antenna-defect-detected	AP PU323E5E18012353 radio 1 antenn...	N/A		

- 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.



Date/Time	Level	Action	Message
2 minutes ago	🟩🟩□□□□□□	rogue-ap-detected	AP OnePlus 7
6 minutes ago	🟦🟦🟦□□□□□	antenna-defect-...	AP PU323E5E
11 minutes ago	🟦🟦🟦□□□□□	antenna-defect-...	AP PU323E5E
17 minutes ago	🟦🟦🟦□□□□□	antenna-defect-...	AP PU323E5E

- **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.

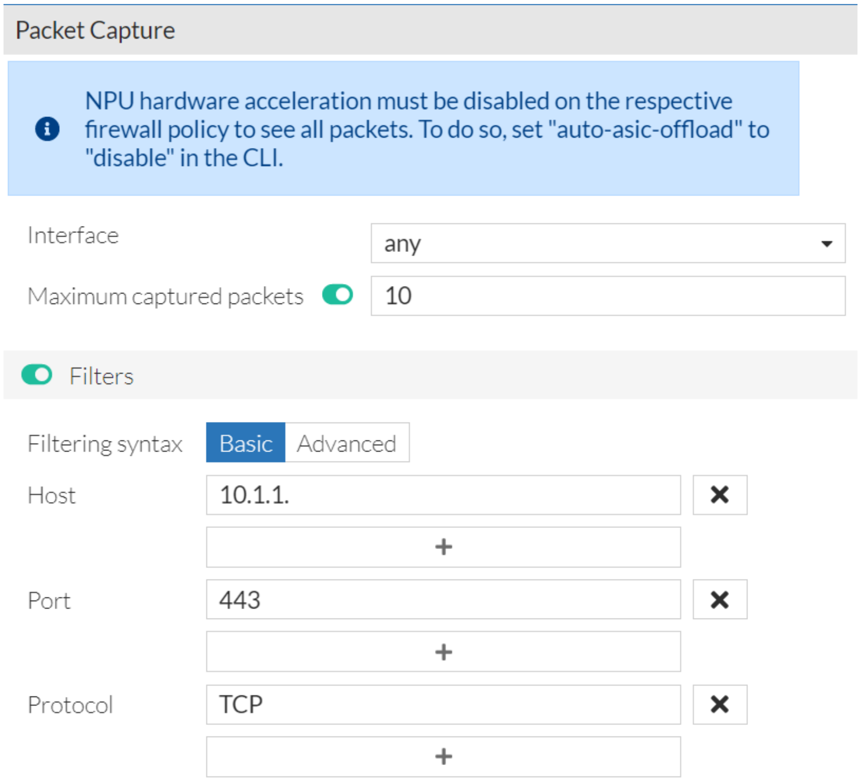
Tools

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.



Packet Capture

NPU hardware acceleration must be disabled on the respective firewall policy to see all packets. To do so, set "auto-asic-offload" to "disable" in the CLI.

Interface: any

Maximum captured packets: 10

Filters

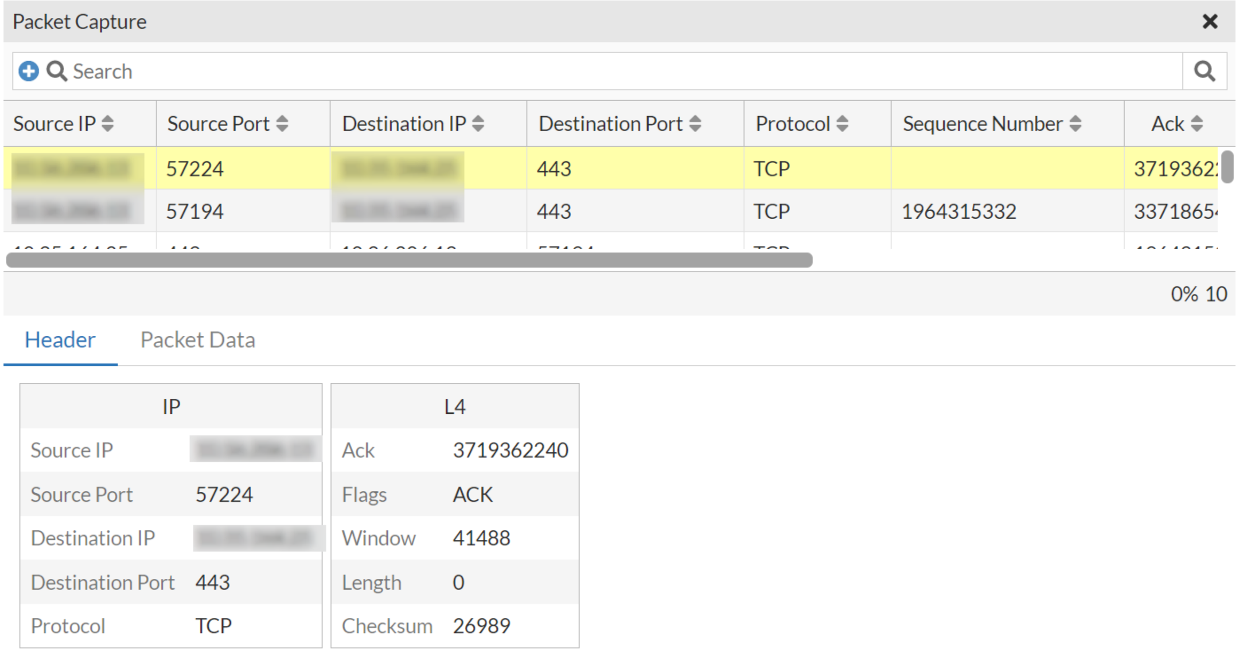
Filtering syntax: Basic | Advanced

Host: 10.1.1.

Port: 443

Protocol: TCP

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**.



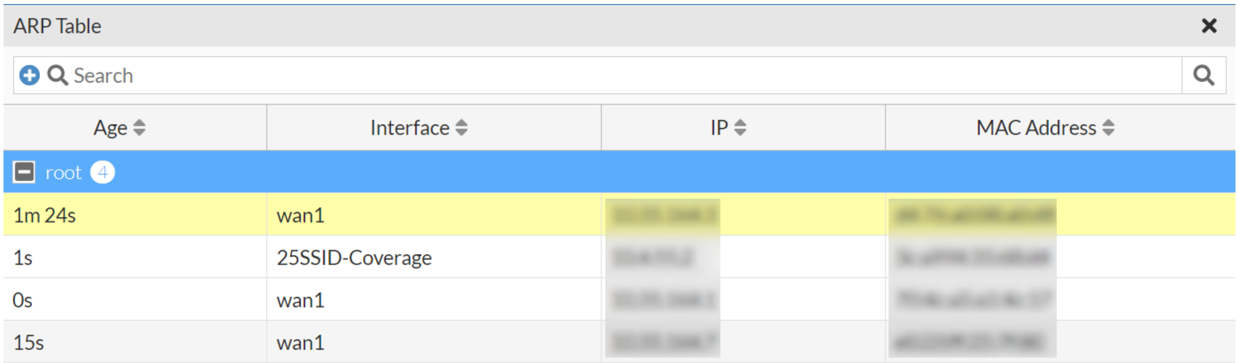
Source IP	Source Port	Destination IP	Destination Port	Protocol	Sequence Number	Ack
[redacted]	57224	[redacted]	443	TCP		3719362
[redacted]	57194	[redacted]	443	TCP	1964315332	3371865

IP	
Source IP	[redacted]
Source Port	57224
Destination IP	[redacted]
Destination Port	443
Protocol	TCP

L4	
Ack	3719362240
Flags	ACK
Window	41488
Length	0
Checksum	26989

ARP Table

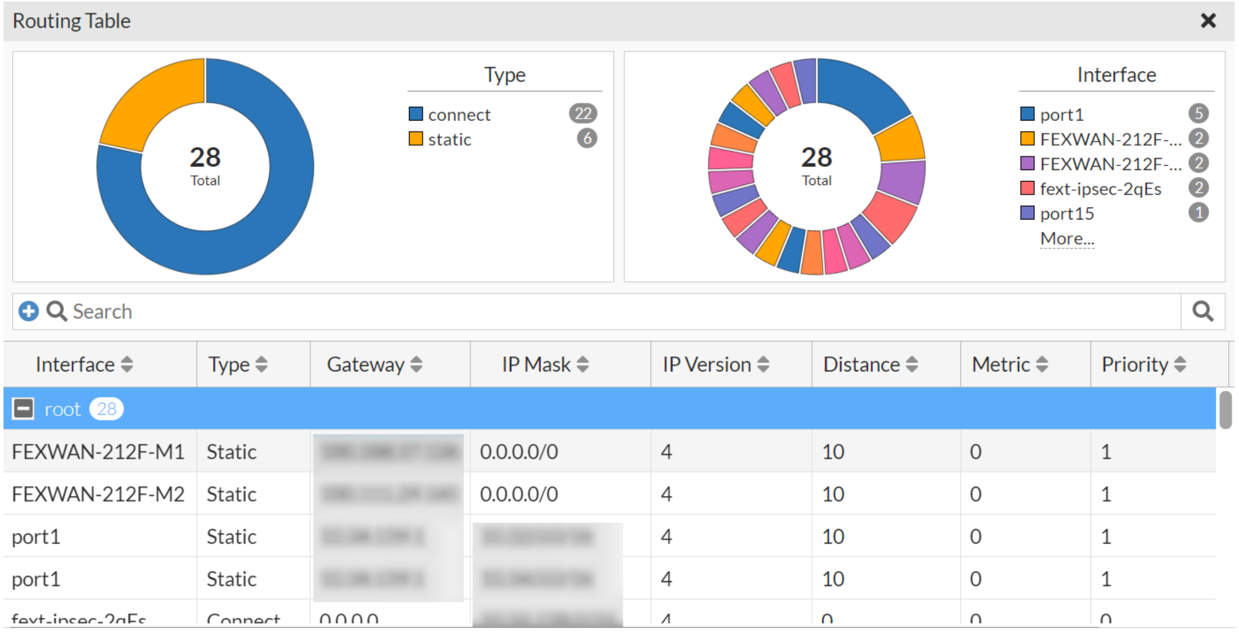
The ARP Table records the discovered MAC address - IP address pairs of devices connected to a network and the interface details. Each connected device has its own ARP table that stores the MAC-IP address pairs that the device has communicated with. Click **Run** to view the ARP table.



Age	Interface	IP	MAC Address
1m 24s	wan1	[redacted]	[redacted]
1s	25SSID-Coverage	[redacted]	[redacted]
0s	wan1	[redacted]	[redacted]
15s	wan1	[redacted]	[redacted]

Routing Table

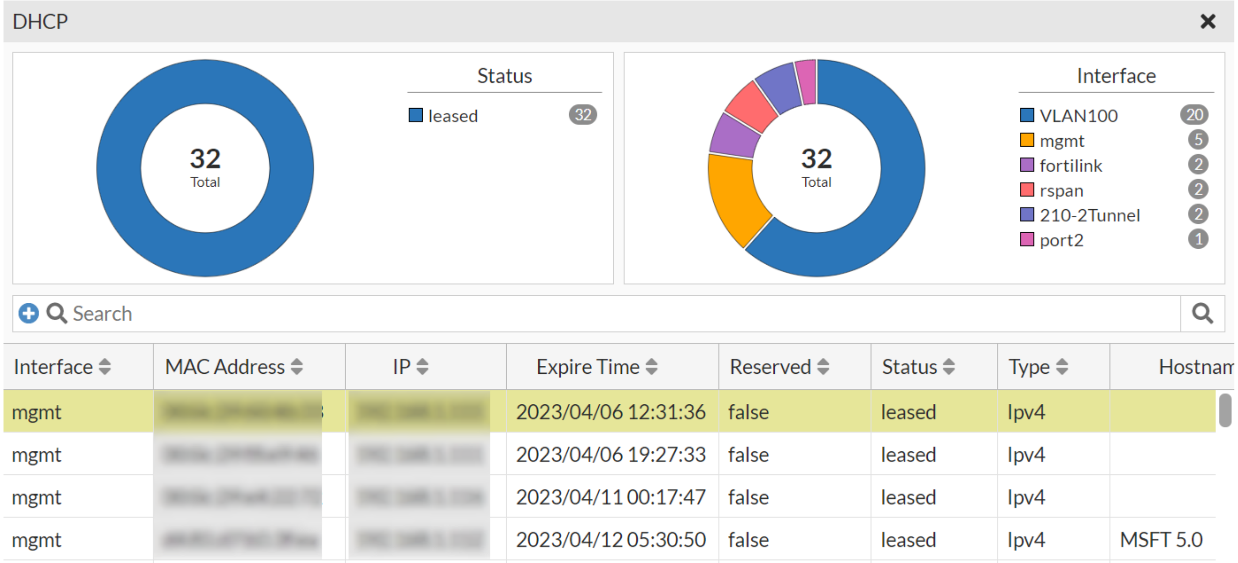
You can view the routing table on the FortiGate, including all static and dynamic routing protocols.



Interface	Type	Gateway	IP Mask	IP Version	Distance	Metric	Priority
root 28							
FEXWAN-212F-M1	Static	[redacted]	0.0.0.0/0	4	10	0	1
FEXWAN-212F-M2	Static	[redacted]	0.0.0.0/0	4	10	0	1
port1	Static	[redacted]	[redacted]	4	10	0	1
port1	Static	[redacted]	[redacted]	4	10	0	1
fext-ipsec-2qEs	Connect	0.0.0.0	[redacted]	4	0	0	0

DHCP

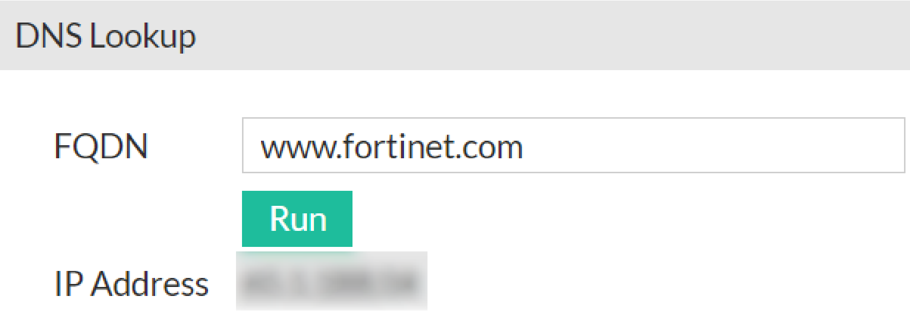
The DHCP monitor shows all the addresses leased out by FortiGate's DHCP servers.



Interface	MAC Address	IP	Expire Time	Reserved	Status	Type	Hostnam
mgmt	[redacted]	[redacted]	2023/04/06 12:31:36	false	leased	Ipv4	
mgmt	[redacted]	[redacted]	2023/04/06 19:27:33	false	leased	Ipv4	
mgmt	[redacted]	[redacted]	2023/04/11 00:17:47	false	leased	Ipv4	
mgmt	[redacted]	[redacted]	2023/04/12 05:30:50	false	leased	Ipv4	MSFT 5.0

DNS Lookup

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



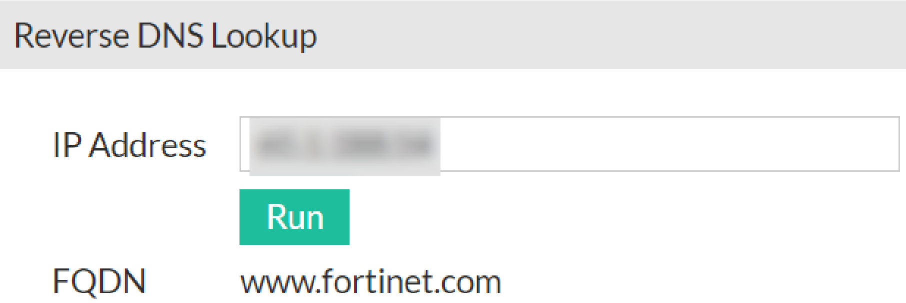
DNS Lookup

FQDN www.fortinet.com

IP Address [redacted]

Reverse DNS Lookup

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



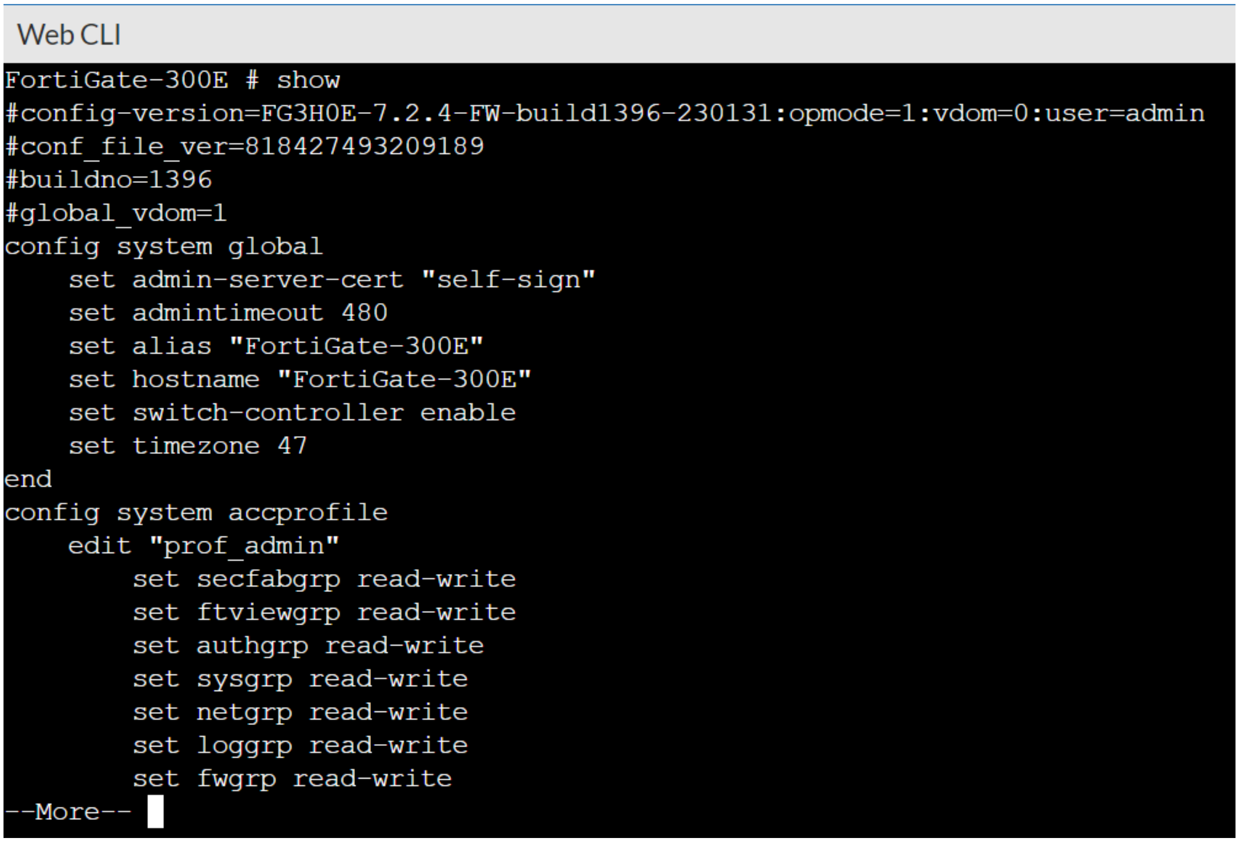
Reverse DNS Lookup

IP Address [redacted]

FQDN www.fortinet.com

Web CLI

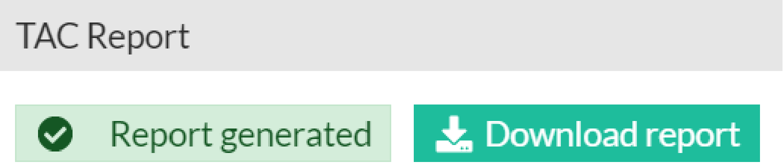
Access the FortiGate's command line interface.



```
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--
```

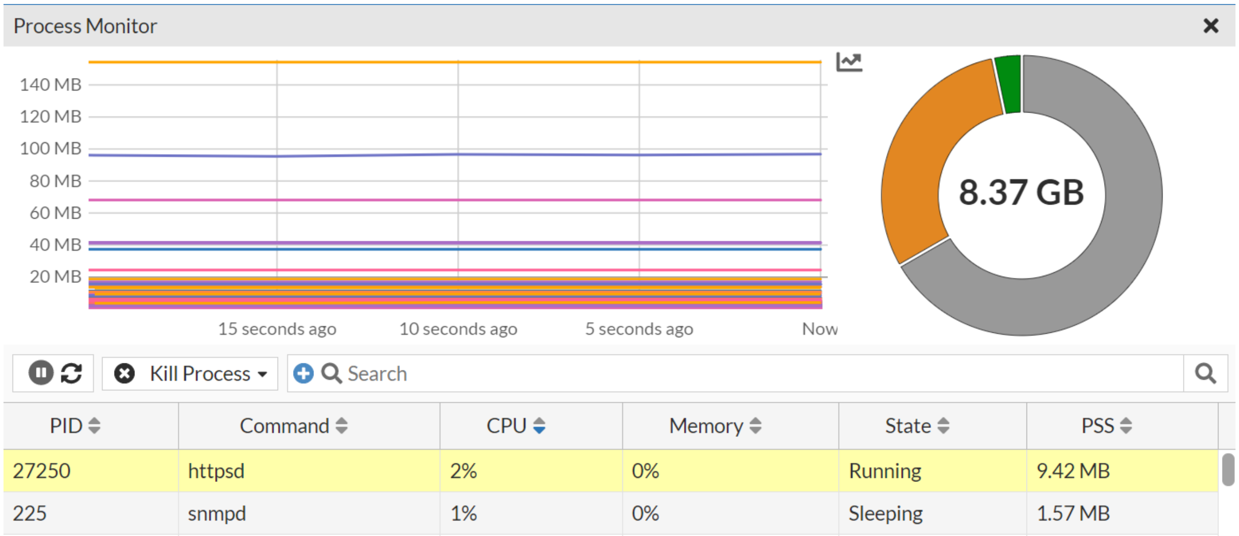
TAC Report

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.



PID	Command	CPU	Memory	State	PSS
27250	httpsd	2%	0%	Running	9.42 MB
225	snmpd	1%	0%	Sleeping	1.57 MB

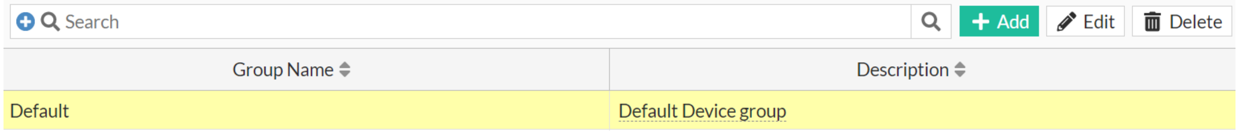
Select a process to perform any of the following operations.

- **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

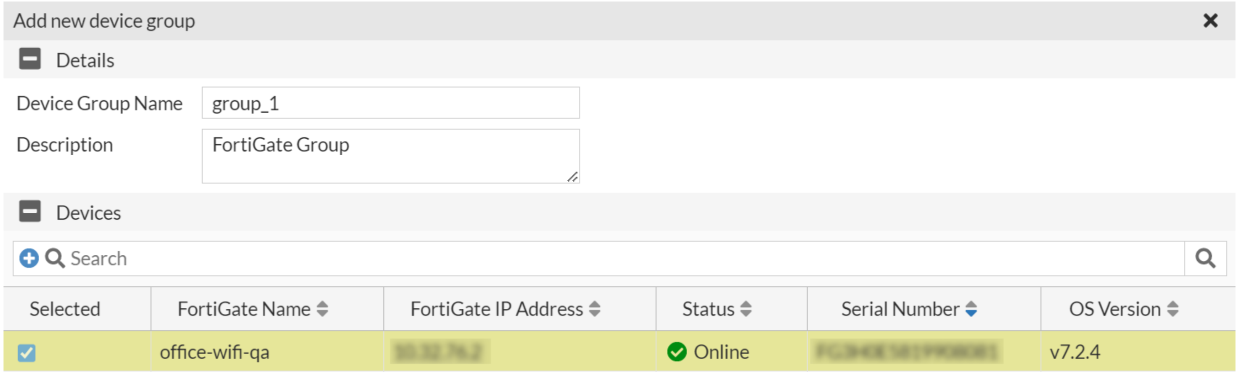
You can group FortiGate controllers for ease of management. Each controller can belong to only one group; if a controller is added to a second group, it is automatically removed from the previous group. Device groups allow administrators to manage devices in a certain way, such as, provide specific access 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.



Group Name	Description
Default	Default Device group

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.



Add new device group ✕

⊟ Details

Device Group Name	group_1
Description	FortiGate Group

⊟ Devices

Selected	FortiGate Name	FortiGate IP Address	Status	Serial Number	OS Version
☑	office-wifi-qa	[redacted]	✓ Online	[redacted]	v7.2.4

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.

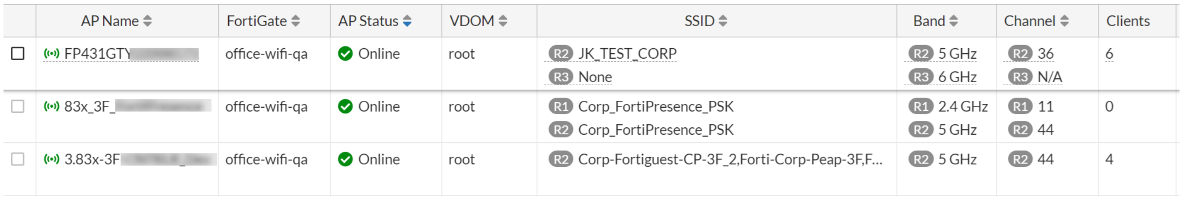
Adding/Managing VDOMs in FortiAIOps

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.

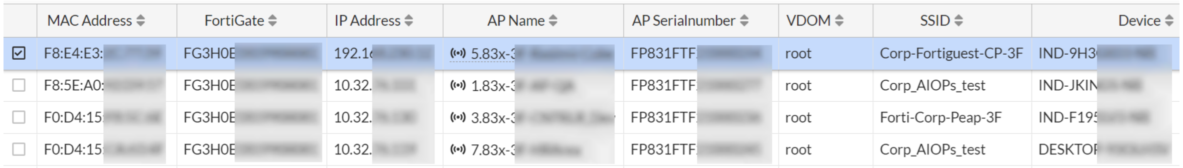
The VDOM information is displayed in the following pages of the FortiAIOps GUI. You can view VDOM information in the **VDOM** column.

- *Wireless > Access Points*



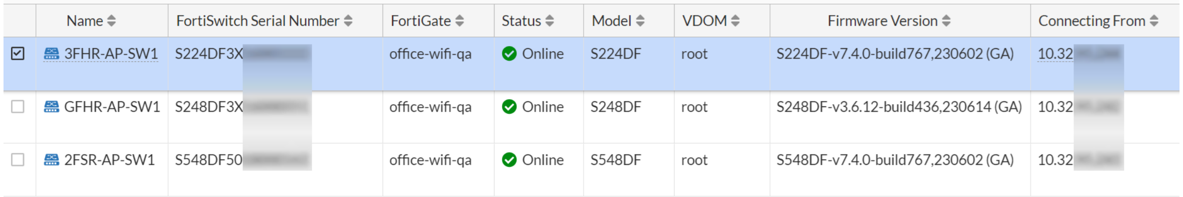
	AP Name	FortiGate	AP Status	VDOM	SSID	Band	Channel	Clients
☐	FP431GTY[redacted]	office-wifi-qa	✓ Online	root	R2 JK_TEST_CORP R3 None	R2 5 GHz R3 6 GHz	R2 36 R3 N/A	6
☐	83x_3F_[redacted]	office-wifi-qa	✓ Online	root	R1 Corp_FortiPresence_PSK R2 Corp_FortiPresence_PSK	R1 2.4 GHz R2 5 GHz	R1 11 R2 44	0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

- *Wireless > Clients*



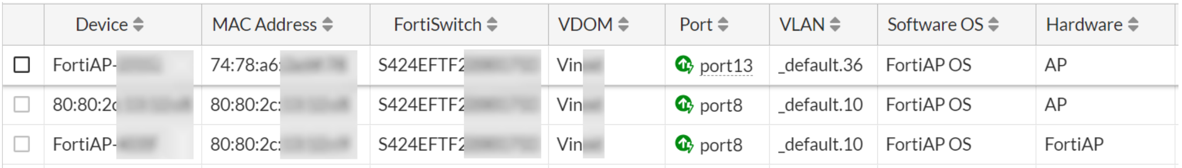
	MAC Address	FortiGate	IP Address	AP Name	AP Serialnumber	VDOM	SSID	Device
☑	F8:E4:E3:[redacted]	FG3H0E[redacted]	192.1[redacted]	5.83x-3[redacted]	FP831FTF[redacted]	root	Corp-Fortiguest-CP-3F	IND-9H3[redacted]
☐	F8:5E:A0:[redacted]	FG3H0E[redacted]	10.32.[redacted]	1.83x-3[redacted]	FP831FTF[redacted]	root	Corp_AIOPs_test	IND-JKIN[redacted]
☐	F0:D4:15[redacted]	FG3H0E[redacted]	10.32.[redacted]	3.83x-3[redacted]	FP831FTF[redacted]	root	Forti-Corp-Peap-3F	IND-F195[redacted]
☐	F0:D4:15[redacted]	FG3H0E[redacted]	10.32.[redacted]	7.83x-3[redacted]	FP831FTF[redacted]	root	Corp_AIOPs_test	DESKTOP[redacted]

- *Switch > FortiSwitch*



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

- *Switch > FortiSwitch Clients*



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

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

- Monitoring and managing individual VDOMs is not supported currently; hence, data from all VDOMs is displayed in FortiAIOps.
- Moving a FortiGate between device groups moves all the VDOMs.
- The AI Insights dashboards do not display VDOM separation.

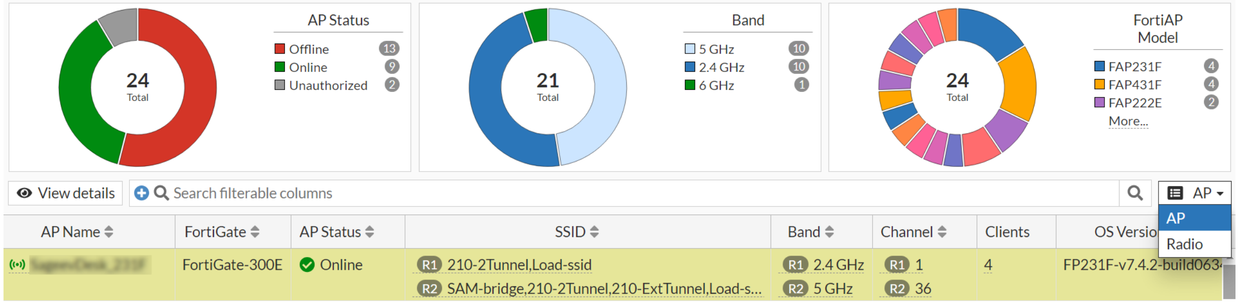
Wireless

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.

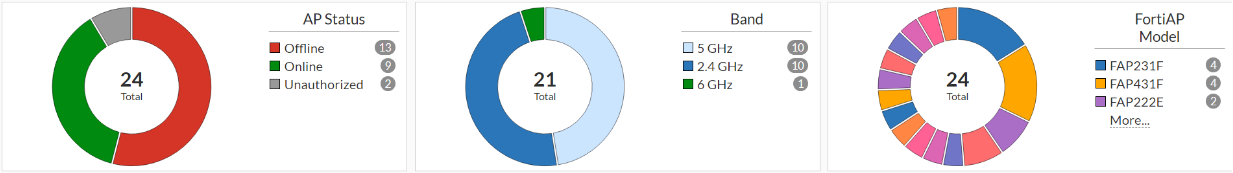


AP Name	FortiGate	AP Status	SSID	Band	Channel	Clients	OS Versio
[redacted]	FortiGate-300E	✓ Online	R1 210-2Tunnel,Load-ssid R2 SAM-bridge,210-2Tunnel,210-ExtTunnel,Load-s...	R1 2.4 GHz R2 5 GHz	R1 1 R2 36	4	FP231F-v7.4.2-build063

- 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.

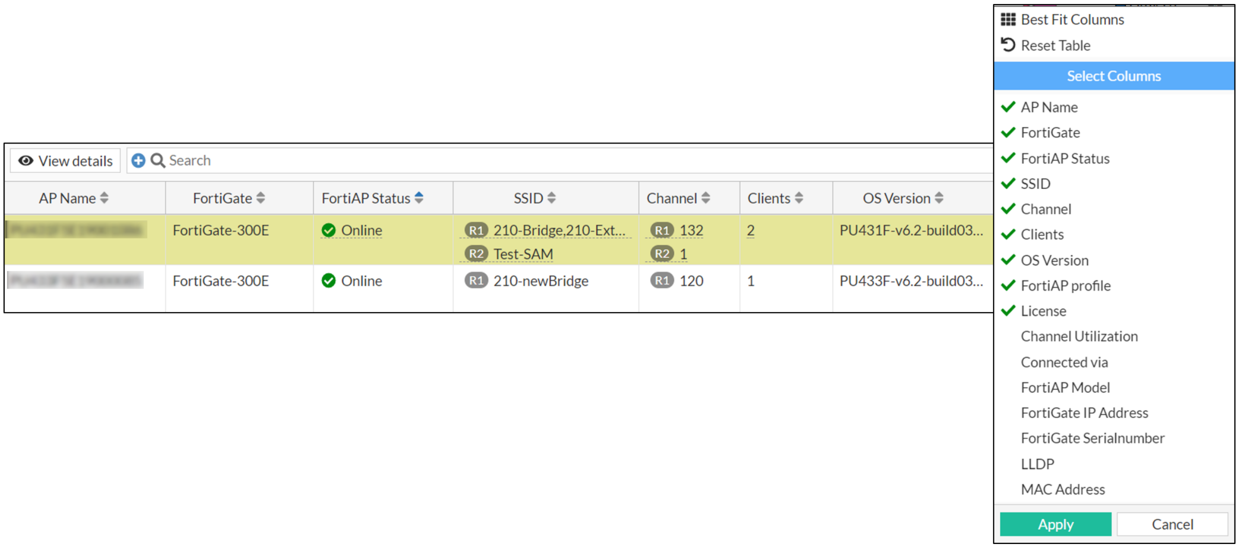
FortiAP Model

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.



AP Name	FortiGate	FortiAP Status	SSID	Channel	Clients	OS Version
[redacted]	FortiGate-300E	Online	R1 210-Bridge,210-Ext... R2 Test-SAM	R1 132 R2 1	2	PU431F-v6.2-build03...
[redacted]	FortiGate-300E	Online	R1 210-newBridge	R1 120	1	PU433F-v6.2-build03...

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.

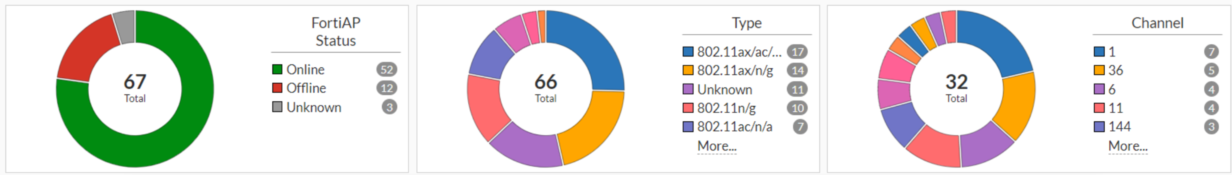
To filter the AP list based on the column data, click the filter icon in the column header next to the title, select the value to be filtered and click **Apply**.

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.

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.

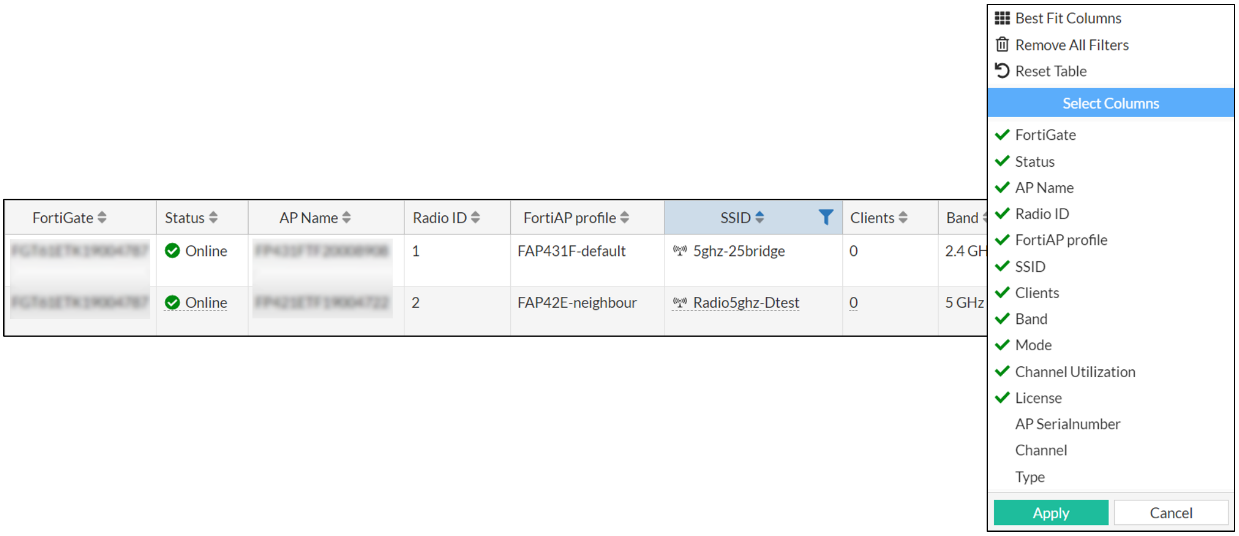
Channel

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.



FortiGate	Status	AP Name	Radio ID	FortiAP profile	SSID	Clients	Band
[redacted]	✓ Online	[redacted]	1	FAP431F-default	5ghz-25bridge	0	2.4 GH
[redacted]	✓ Online	[redacted]	2	FAP42E-neighbour	Radio5ghz-Dtest	0	5 GHz

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.

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.

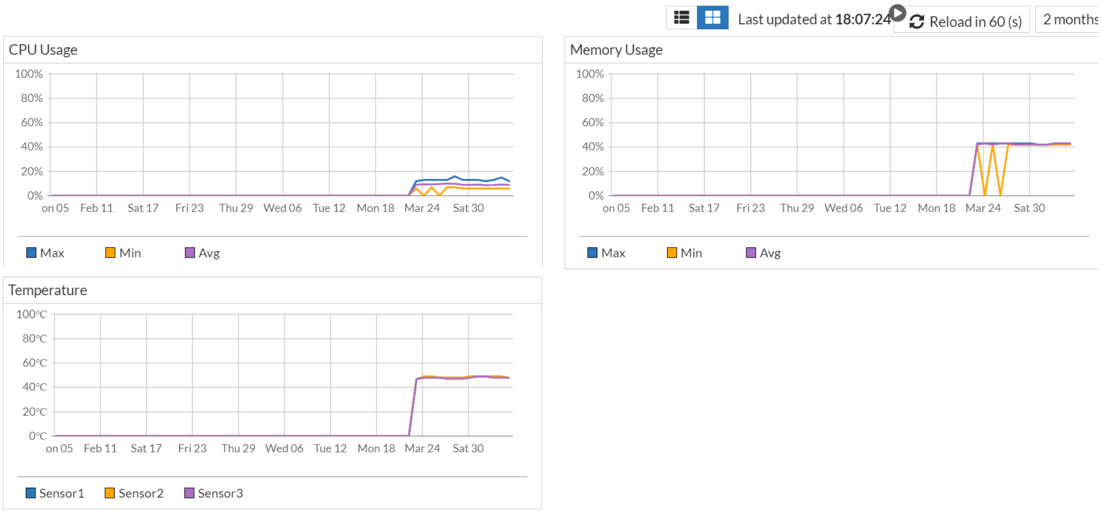
- Performance
- Channel Summary
- Clients
- Interfering SSIDs
- Logs
- Spectrum Analysis
- VLAN Probe

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.

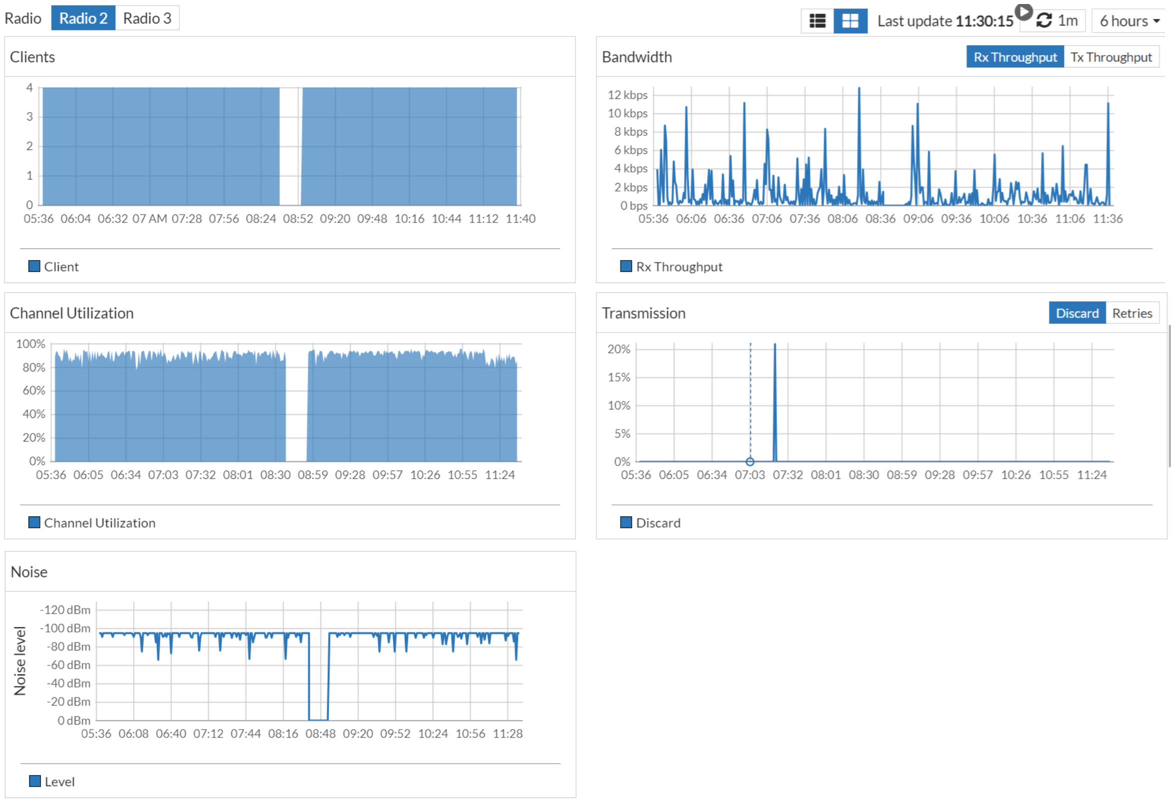
AP Health

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.

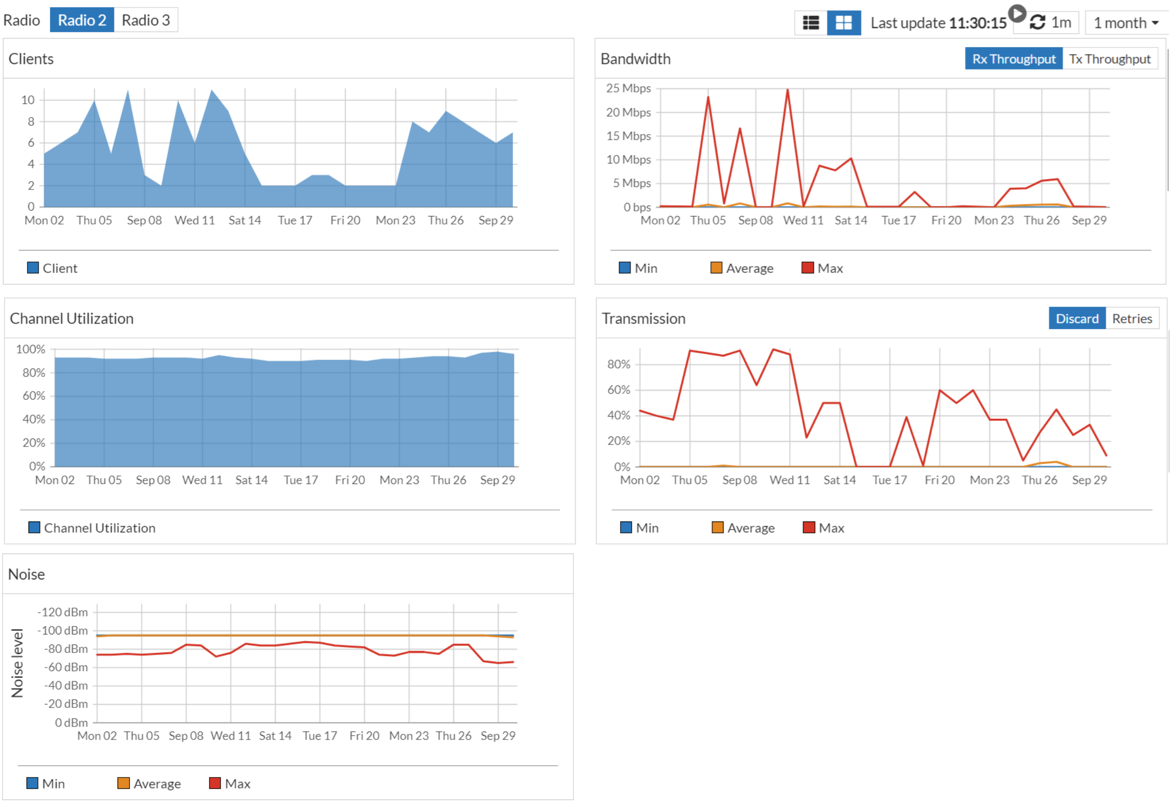

Last updated at 18:07:24
Reload in 60 (s)
2 months
CPU Usage
100%
80%
60%
40%
20%
0%
on 05 Feb 11 Sat 17 Fri 23 Thu 29 Wed 06 Tue 12 Mon 18 Mar 24 Sat 30
Max
Min
Avg
Memory Usage
100%
80%
60%
40%
20%
0%
on 05 Feb 11 Sat 17 Fri 23 Thu 29 Wed 06 Tue 12 Mon 18 Mar 24 Sat 30
Max
Min
Avg
Temperature
100°C
80°C
60°C
40°C
20°C
0°C
on 05 Feb 11 Sat 17 Fri 23 Thu 29 Wed 06 Tue 12 Mon 18 Mar 24 Sat 30
Sensor1
Sensor2
Sensor3

Wireless

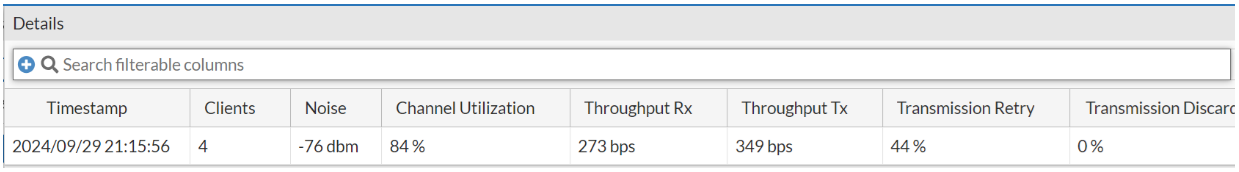
It includes charts for clients, bandwidth, channel utilization, transmission discard, retries, and noise levels on the respective radio interface. The default interval is 10 minutes and can it be changed according to your requirements.



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.

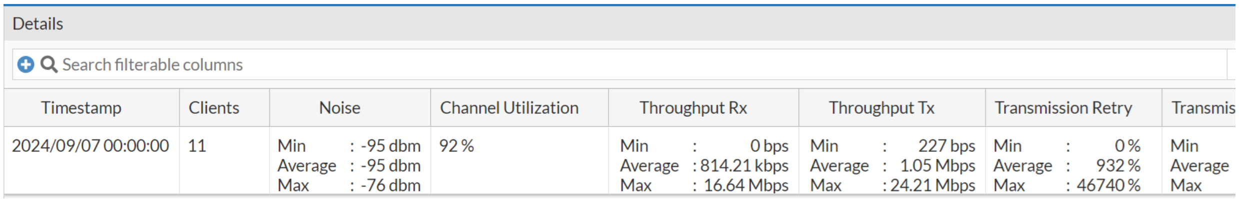


Details

Search filterable columns

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

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



Details

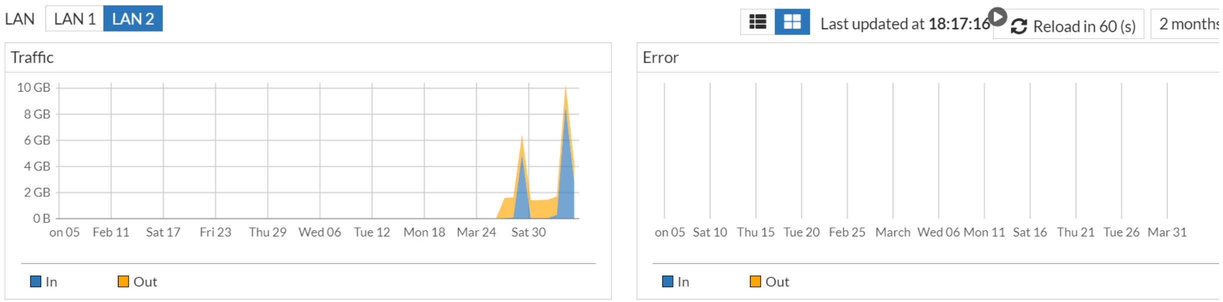
Search filterable columns

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

Wired

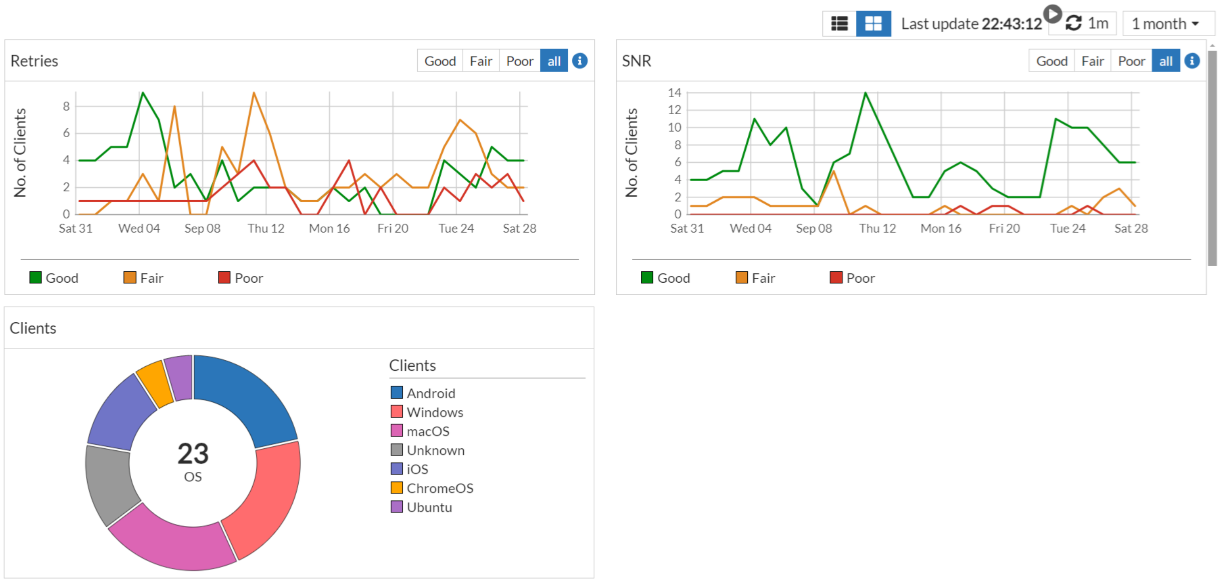
The LAN port statistics are now displayed for access points. You can view the traffic coming into a LAN port and the traffic leaving it at a given point in time. Also, the error statistics for both incoming and outgoing traffic is displayed.

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.

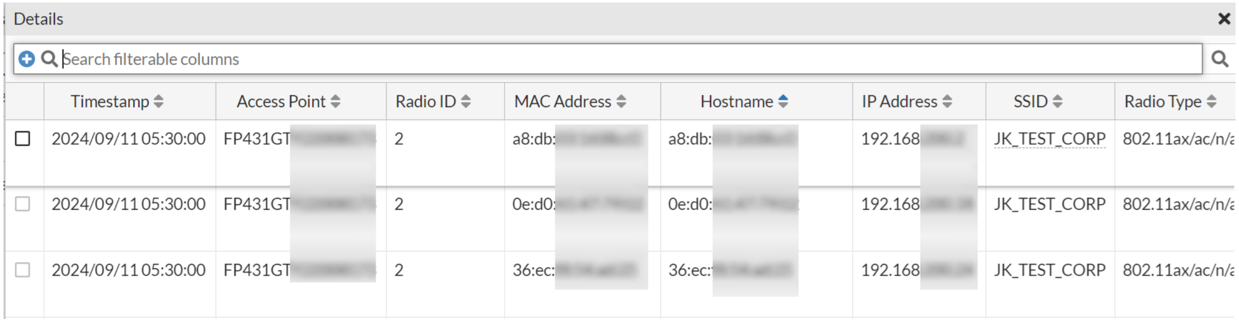
- **Good** – SNR is equal to or greater than 25 dB
- **Fair** – SNR between 15 and 24 dB

- **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.

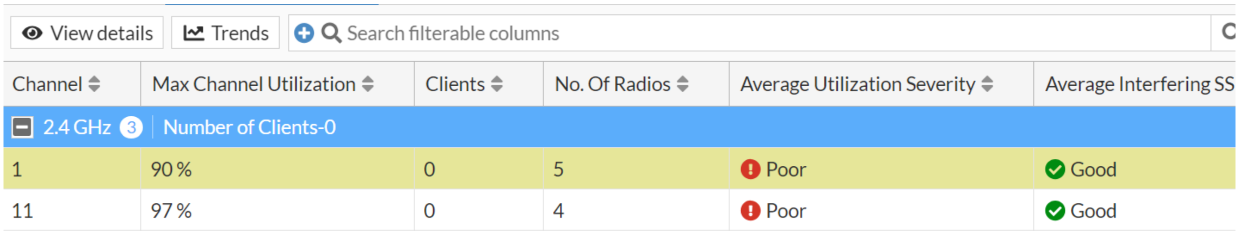
To view details for each of the 3 panels, click on the retries and SNR graphs, or on the OS name to view details. The **Details** page displays data such as, the host name, access point and radio details, associated SSID, OS type, throughput, noise, retries, and so on.



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

Channel Summary

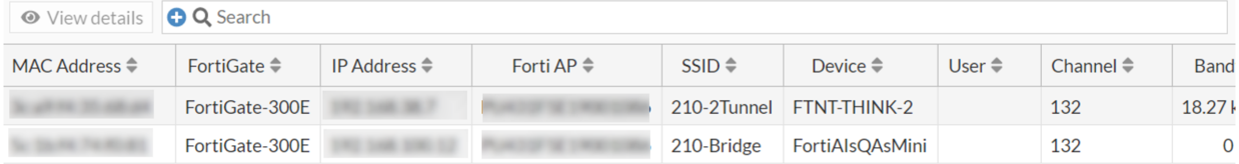
This page provides granular insights into the performance of each channel with detailed statistics and trends. For more information, see Channel Summary.



Channel	Max Channel Utilization	Clients	No. Of Radios	Average Utilization Severity	Average Interfering SS
⊟ 2.4 GHz 3	Number of Clients-0				
1	90 %	0	5	! Poor	✓ Good
11	97 %	0	4	! Poor	✓ Good

Clients

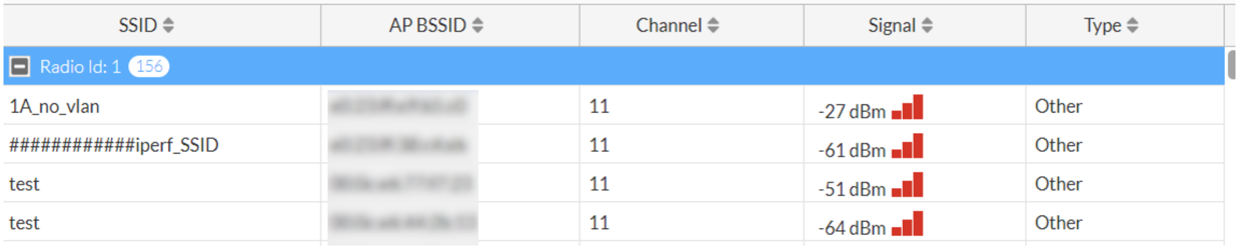
The Clients tab displays a list of clients currently connected to the selected AP, along with details such as the client MAC address, FortiGate and IP Address, FortiAP name , associated SSID, user name , operating channel and the radio details, Tx and Rx bandwidth, signal strength and noise, VLAN ID, 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**.



MAC Address	FortiGate	IP Address	Forti AP	SSID	Device	User	Channel	Band
[redacted]	FortiGate-300E	[redacted]	[redacted]	210-2Tunnel	FTNT-THINK-2		132	18.27 k
[redacted]	FortiGate-300E	[redacted]	[redacted]	210-Bridge	FortiAIsQAsMini		132	0

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).

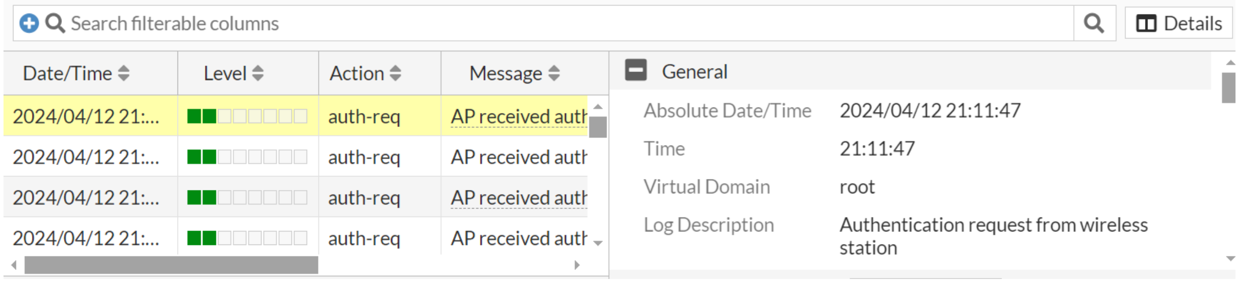


Radio Id: 1 156

SSID	AP BSSID	Channel	Signal	Type
1A_no_vlan	[redacted]	11	-27 dBm	Other
############iperf_SSID	[redacted]	11	-61 dBm	Other
test	[redacted]	11	-51 dBm	Other
test	[redacted]	11	-64 dBm	Other

Logs

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



Date/Time	Level	Action	Message
2024/04/12 21:...		auth-req	AP received auth
2024/04/12 21:...		auth-req	AP received auth
2024/04/12 21:...		auth-req	AP received auth
2024/04/12 21:...		auth-req	AP received auth

General

Absolute Date/Time	2024/04/12 21:11:47
Time	21:11:47
Virtual Domain	root
Log Description	Authentication request from wireless station

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.

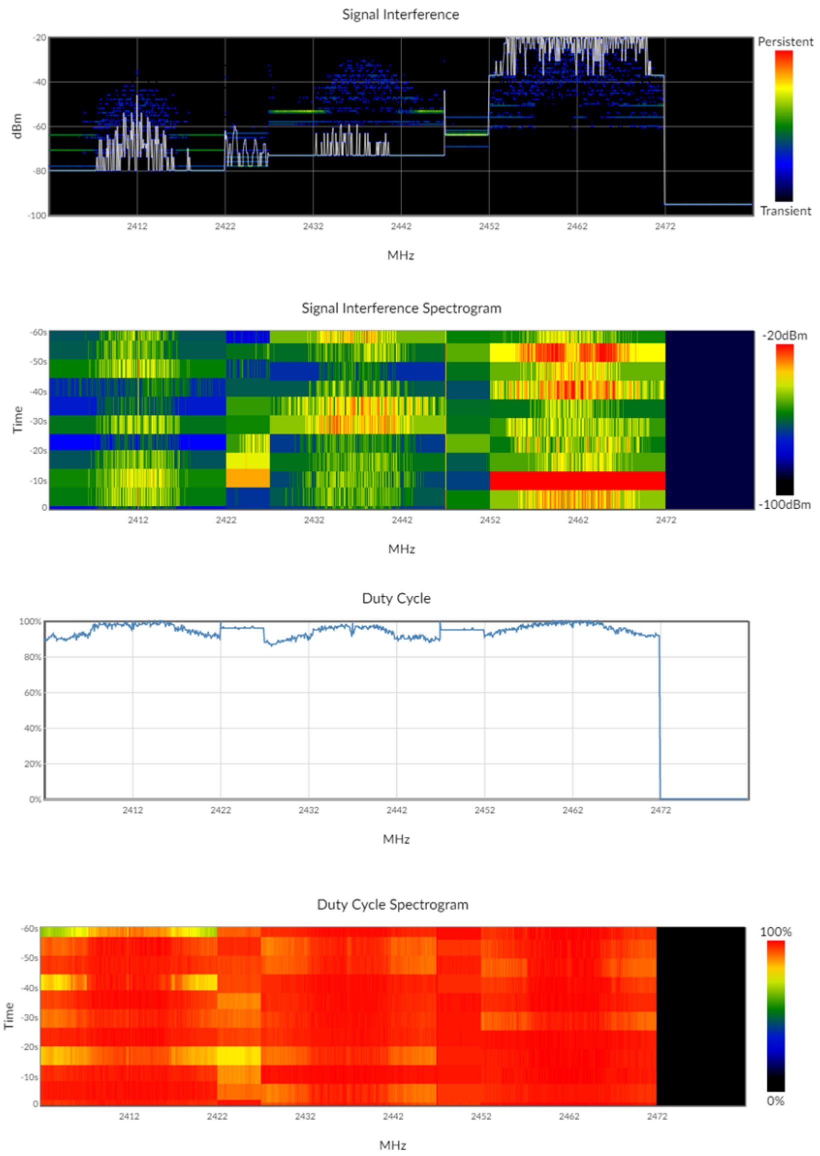
- You can select the **AP**, **Radio**, and **Channels** to be scanned for interferences.
- The **Scan Duration** can be set to 1, 5, 30, or 60 minutes.
- The **Sampling Interval** and the number of **Spectrogram Samples** cannot be modified.

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.

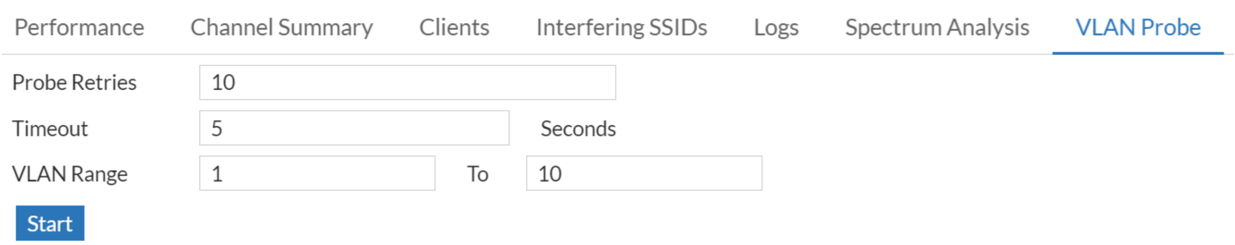


VLAN Probe

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.

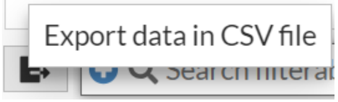


Probe Retries	10		
Timeout	5	Seconds	
VLAN Range	1	To	10

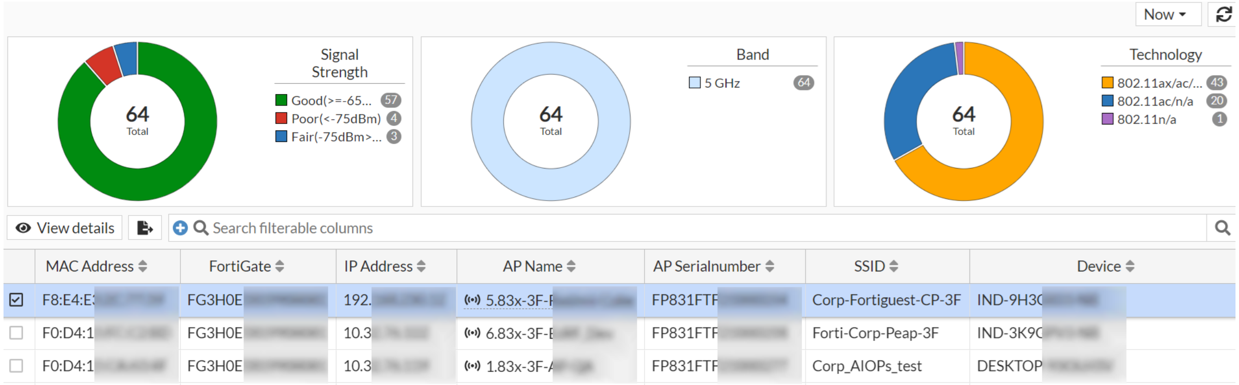
Clients

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.
- You can export data in a *.csv* file, click on the export icon on these pages.



.



	MAC Address	FortiGate	IP Address	AP Name	AP Serialnumber	SSID	Device
☑	F8:E4:E[redacted]	FG3H0E[redacted]	192.[redacted]	5.83x-3F-F[redacted]	FP831FTF[redacted]	Corp-Fortiguest-CP-3F	IND-9H3C[redacted]
□	F0:D4:1[redacted]	FG3H0E[redacted]	10.3[redacted]	6.83x-3F-E[redacted]	FP831FTF[redacted]	Forti-Corp-Peap-3F	IND-3K9C[redacted]
□	F0:D4:1[redacted]	FG3H0E[redacted]	10.3[redacted]	1.83x-3F-A[redacted]	FP831FTF[redacted]	Corp_AIOPs_test	DESKTOP[redacted]

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.

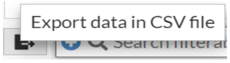
Band

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.

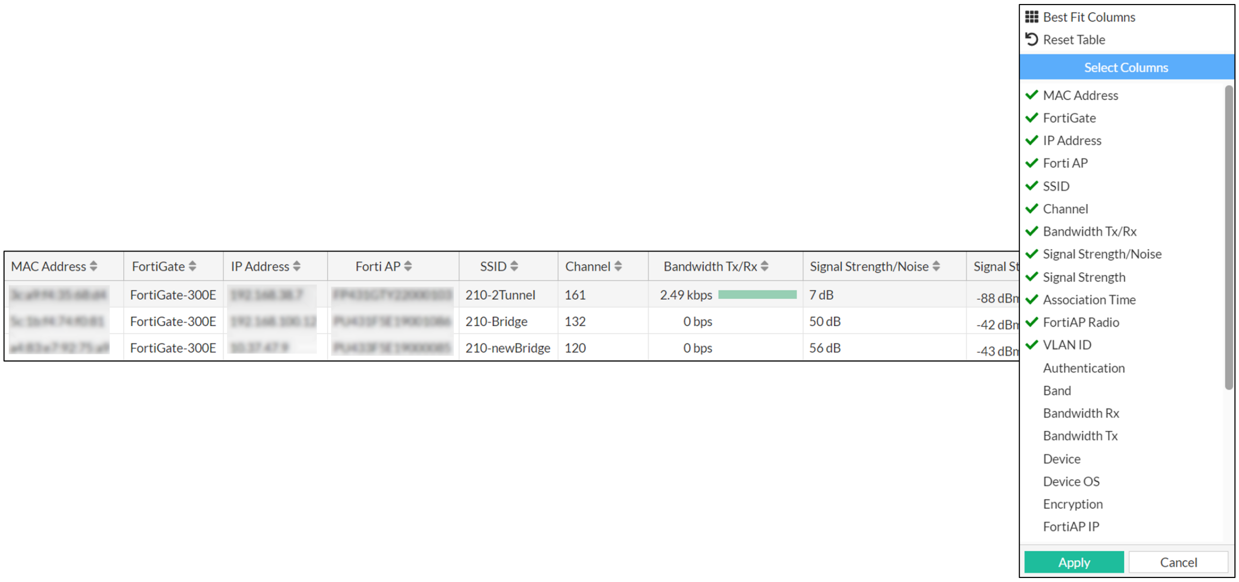
Technology

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.

You can export data in a *.csv* file, click on the export icon on these pages -  .

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.

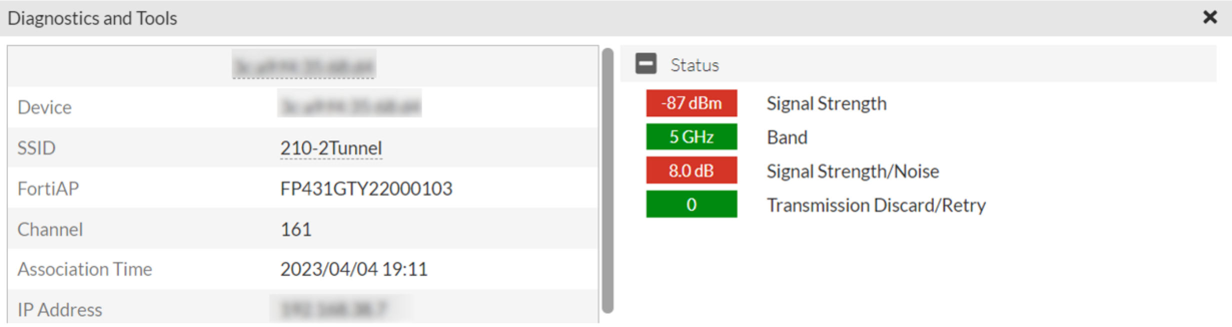


MAC Address	FortiGate	IP Address	Forti AP	SSID	Channel	Bandwidth Tx/Rx	Signal Strength/Noise	Signal St
[redacted]	FortiGate-300E	[redacted]	[redacted]	210-2Tunnel	161	2.49 kbps	7 dB	-88 dBm
[redacted]	FortiGate-300E	[redacted]	[redacted]	210-Bridge	132	0 bps	50 dB	-42 dBm
[redacted]	FortiGate-300E	[redacted]	[redacted]	210-newBridge	120	0 bps	56 dB	-43 dBm

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



Diagnostics and Tools

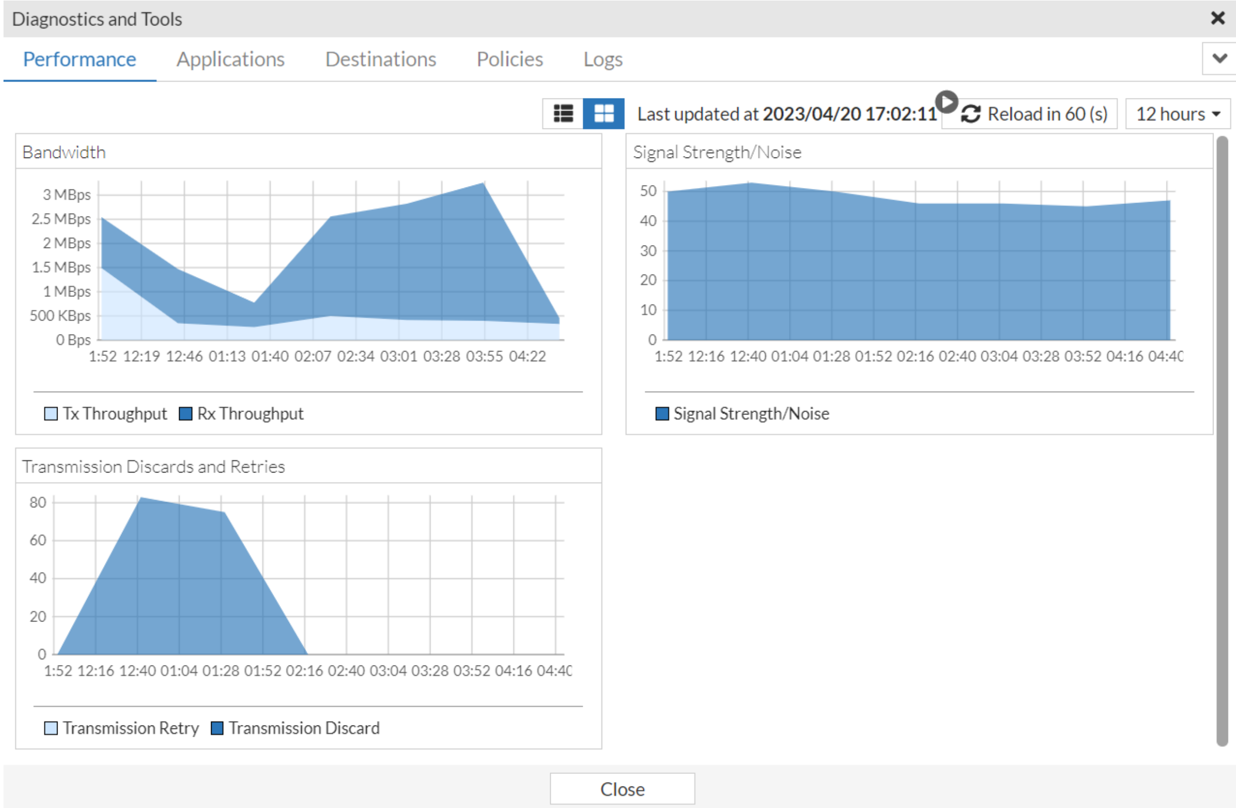
	[redacted]
Device	[redacted]
SSID	210-2Tunnel
FortiAP	FP431GTY22000103
Channel	161
Association Time	2023/04/04 19:11
IP Address	[redacted]

Status

-87 dBm	Signal Strength
5 GHz	Band
8.0 dB	Signal Strength/Noise
0	Transmission Discard/Retry

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**.

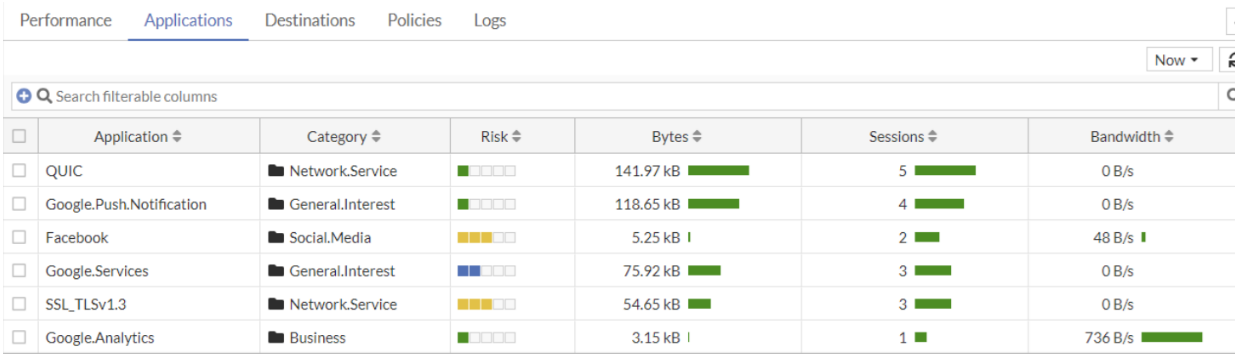


Diagnostics and Tools

Last updated at **2023/04/20 17:02:11**

Applications

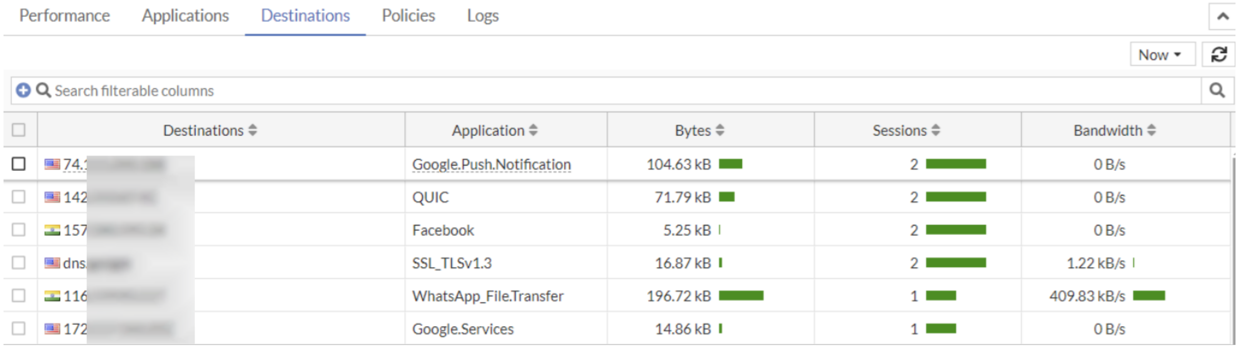
The Applications tab displays a list of applications in use by the selected client, along with details such as the application name, category, risk, data usage, session and bandwidth details.



□	Application	Category	Risk	Bytes	Sessions	Bandwidth
□	QUIC	Network.Service	■□□□□	141.97 kB	5	0 B/s
□	Google.Push.Notification	General.Interest	■□□□□	118.65 kB	4	0 B/s
□	Facebook	Social.Media	■■■□□	5.25 kB	2	48 B/s
□	Google.Services	General.Interest	■■□□□	75.92 kB	3	0 B/s
□	SSL_TLSv1.3	Network.Service	■■■□□	54.65 kB	3	0 B/s
□	Google.Analytics	Business	■□□□□	3.15 kB	1	736 B/s

Destinations

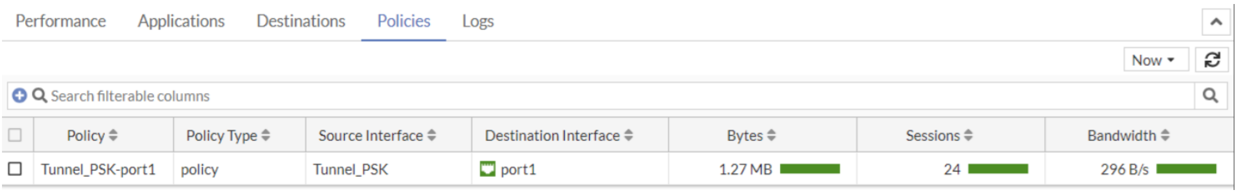
The Destinations tab displays a list of network destinations accessed by the selected client, along with details such as the destination IP address, application name, data usage, session and bandwidth details.



□	Destinations	Application	Bytes	Sessions	Bandwidth
□	74.1[redacted]	Google.Push.Notification	104.63 kB	2	0 B/s
□	142[redacted]	QUIC	71.79 kB	2	0 B/s
□	157[redacted]	Facebook	5.25 kB	2	0 B/s
□	dns[redacted]	SSL_TLSv1.3	16.87 kB	2	1.22 kB/s
□	116[redacted]	WhatsApp_File.Transfer	196.72 kB	1	409.83 kB/s
□	172[redacted]	Google.Services	14.86 kB	1	0 B/s

Policies

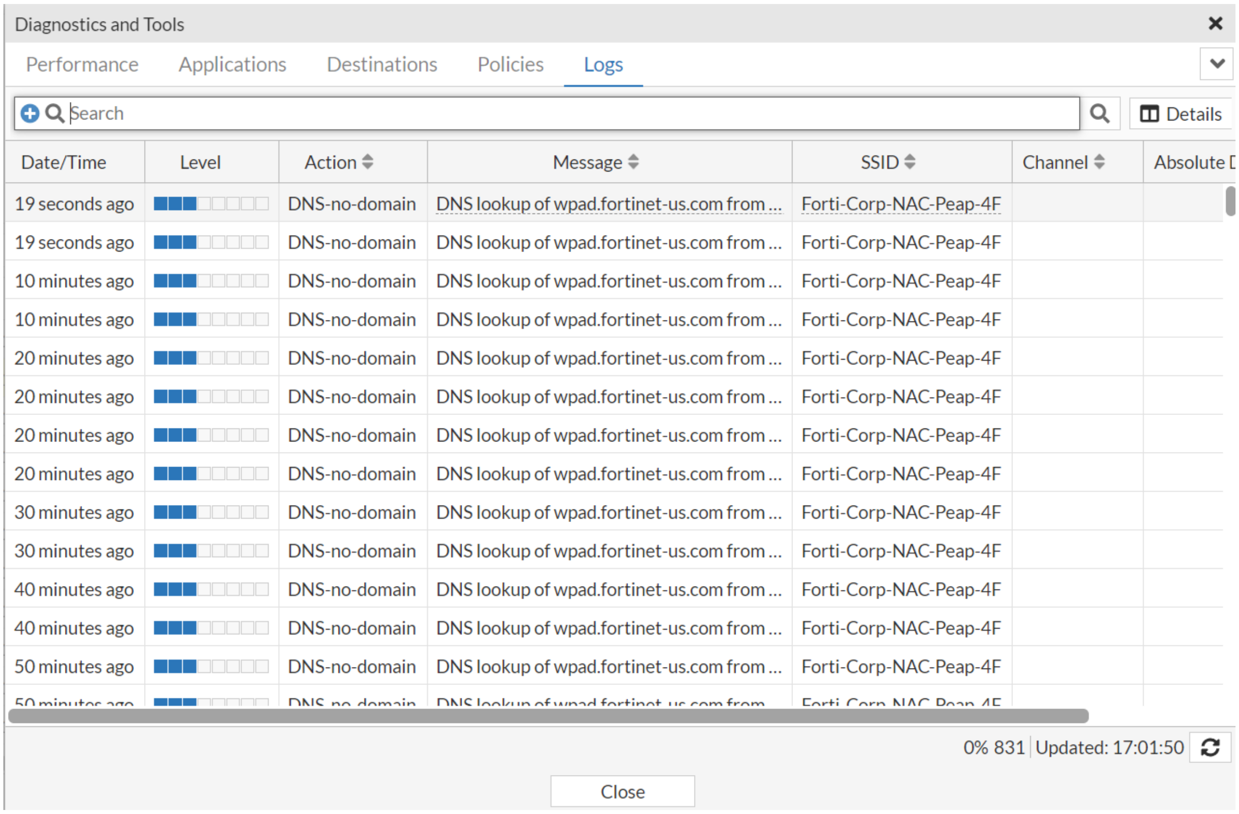
The Policies tab displays information about any policies applied to the selected client, such as policy name, policy type, source interface, destination interface, data usage, session and bandwidth details.



□	Policy	Policy Type	Source Interface	Destination Interface	Bytes	Sessions	Bandwidth
□	Tunnel_PSK-port1	policy	Tunnel_PSK	port1	1.27 MB	24	296 B/s

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**.



Diagnostics and Tools

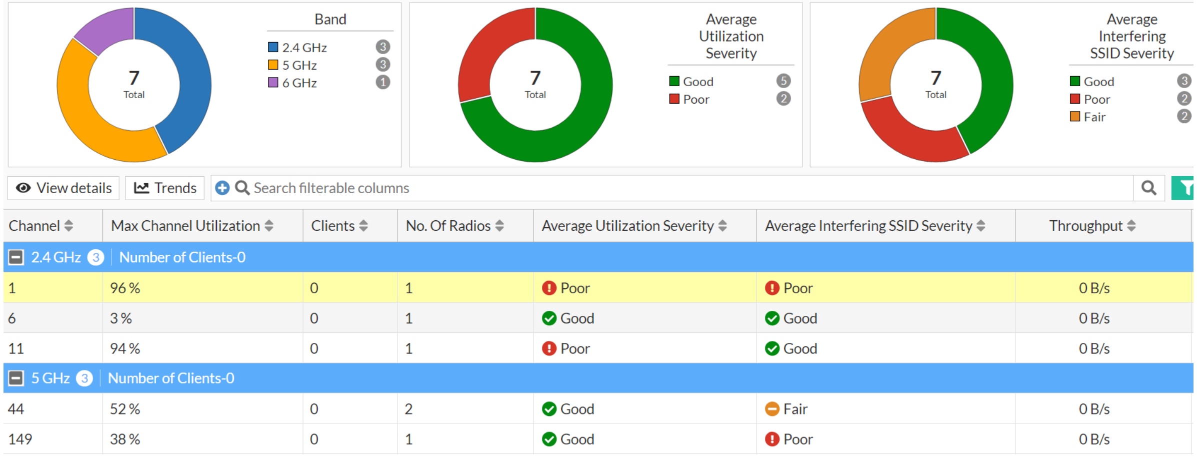
Date/Time	Level	Action	Message	SSID	Channel	Absolute D
19 seconds ago	■■■□□□□□	DNS-no-domain	DNS lookup of wpad.fortinet-us.com from ...	Forti-Corp-NAC-Peap-4F		
19 seconds ago	■■■□□□□□	DNS-no-domain	DNS lookup of wpad.fortinet-us.com from ...	Forti-Corp-NAC-Peap-4F		
10 minutes ago	■■■□□□□□	DNS-no-domain	DNS lookup of wpad.fortinet-us.com from ...	Forti-Corp-NAC-Peap-4F		
10 minutes ago	■■■□□□□□	DNS-no-domain	DNS lookup of wpad.fortinet-us.com from ...	Forti-Corp-NAC-Peap-4F		
20 minutes ago	■■■□□□□□	DNS-no-domain	DNS lookup of wpad.fortinet-us.com from ...	Forti-Corp-NAC-Peap-4F		
20 minutes ago	■■■□□□□□	DNS-no-domain	DNS lookup of wpad.fortinet-us.com from ...	Forti-Corp-NAC-Peap-4F		
20 minutes ago	■■■□□□□□	DNS-no-domain	DNS lookup of wpad.fortinet-us.com from ...	Forti-Corp-NAC-Peap-4F		
20 minutes ago	■■■□□□□□	DNS-no-domain	DNS lookup of wpad.fortinet-us.com from ...	Forti-Corp-NAC-Peap-4F		
30 minutes ago	■■■□□□□□	DNS-no-domain	DNS lookup of wpad.fortinet-us.com from ...	Forti-Corp-NAC-Peap-4F		
30 minutes ago	■■■□□□□□	DNS-no-domain	DNS lookup of wpad.fortinet-us.com from ...	Forti-Corp-NAC-Peap-4F		
40 minutes ago	■■■□□□□□	DNS-no-domain	DNS lookup of wpad.fortinet-us.com from ...	Forti-Corp-NAC-Peap-4F		
40 minutes ago	■■■□□□□□	DNS-no-domain	DNS lookup of wpad.fortinet-us.com from ...	Forti-Corp-NAC-Peap-4F		
50 minutes ago	■■■□□□□□	DNS-no-domain	DNS lookup of wpad.fortinet-us.com from ...	Forti-Corp-NAC-Peap-4F		
50 minutes ago	■■■□□□□□	DNS-no-domain	DNS lookup of wpad.fortinet-us.com from ...	Forti-Corp-NAC-Peap-4F		

0% 831 | Updated: 17:01:50

Channel Summary

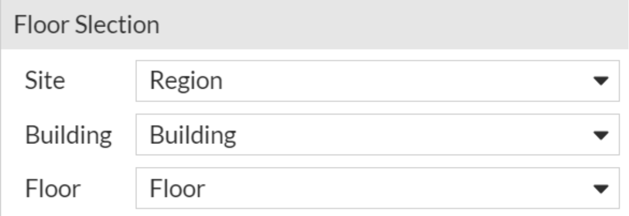
This page provides granular insights into the performance of each channel with key insights into critical statistics, that are key in determining the health of your wireless network. This facilitates effective resolution of any potential network stability issues due to the operating channel. FortiAIOps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

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



Channel	Max Channel Utilization	Clients	No. Of Radios	Average Utilization Severity	Average Interfering SSID Severity	Throughput
2.4 GHz 3	Number of Clients-0					
1	96 %	0	1	Poor	Poor	0 B/s
6	3 %	0	1	✓ Good	✓ Good	0 B/s
11	94 %	0	1	Poor	✓ Good	0 B/s
5 GHz 3	Number of Clients-0					
44	52 %	0	2	✓ Good	Fair	0 B/s
149	38 %	0	1	✓ Good	Poor	0 B/s

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



Floor Slection

Site	Region
Building	Building
Floor	Floor

Band

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

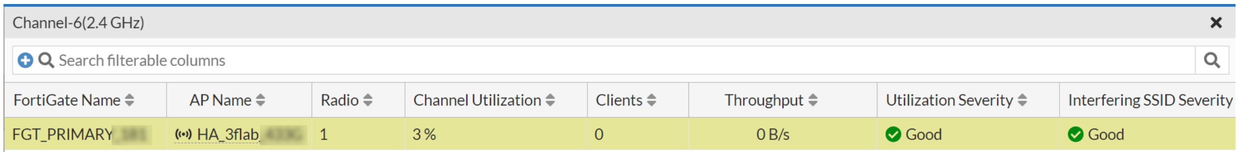
Average Utilization Severity

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

Average Interfering SSID Severity

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

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



Channel-6(2.4 GHz)

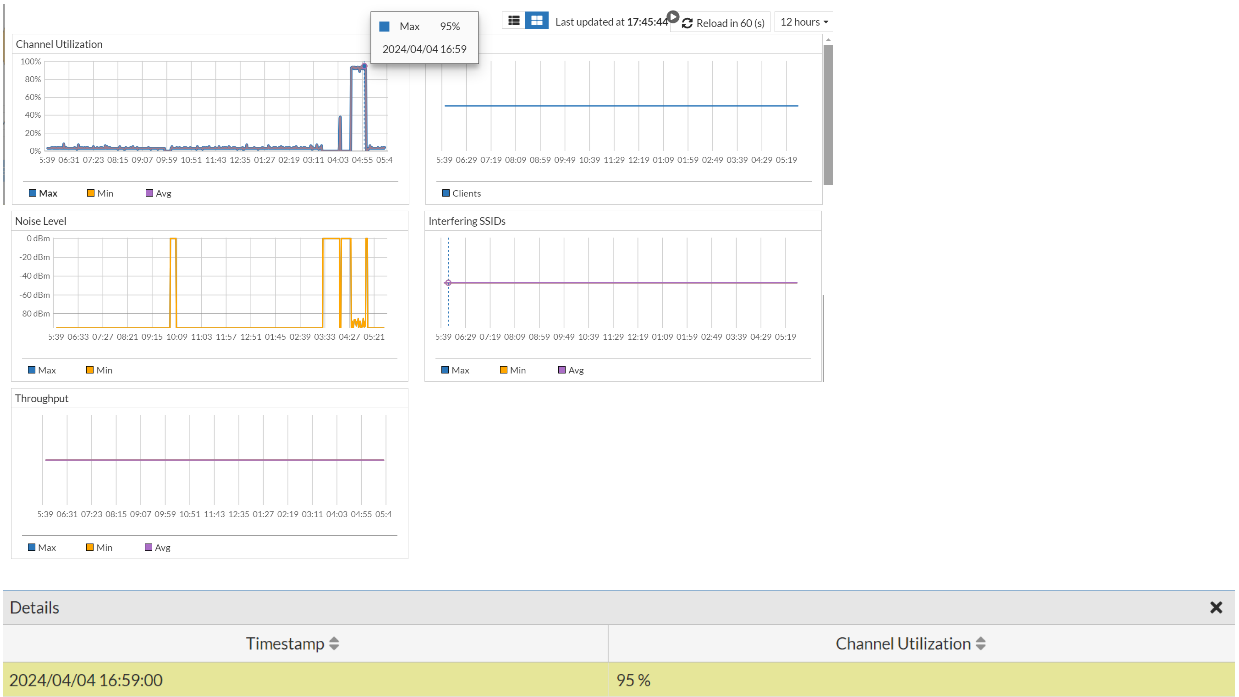
Search filterable columns

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

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

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

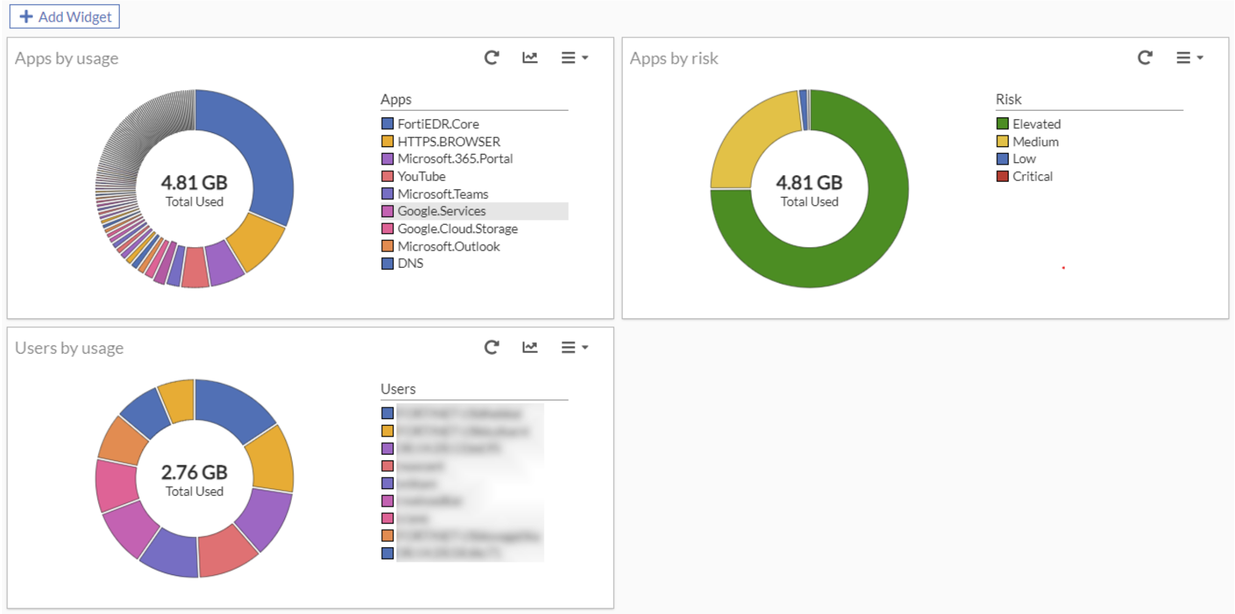
To view trends and patterns to assess the performance of specific channels, select a channel and click **Trends**. You can view a graphical representation of the channel statistics over a period of time. These trends can be filtered for the last **10 minutes**, **1 hour**, or **12 hours**. Hover over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



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

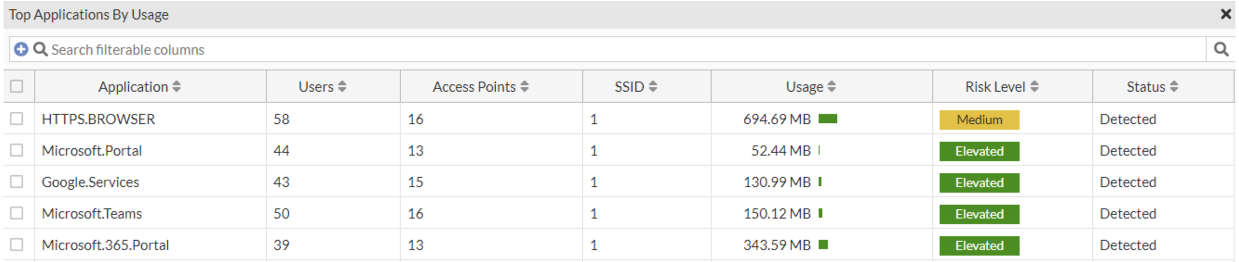
Applications

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.

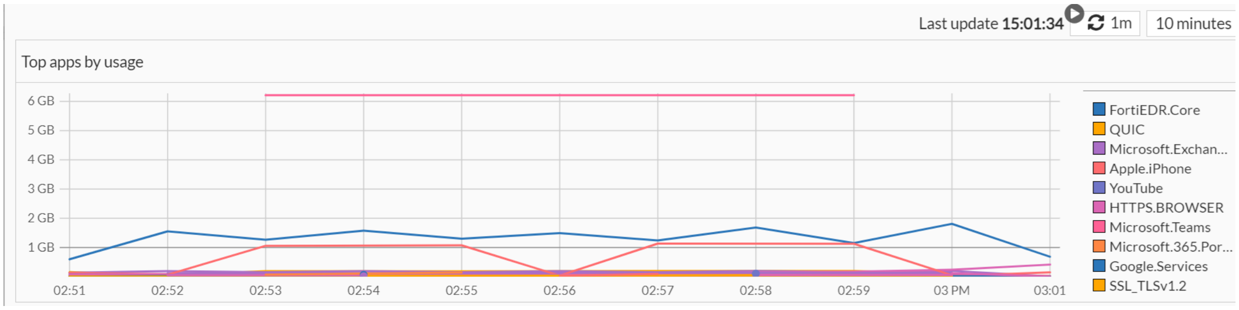


Top Applications By Usage

Search filterable columns

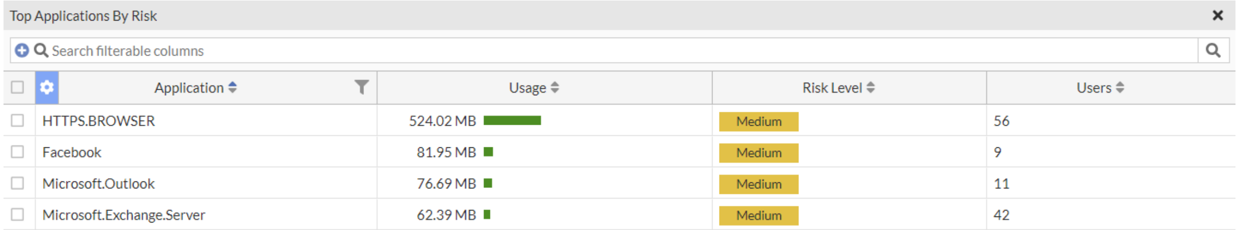
□	Application	Users	Access Points	SSID	Usage	Risk Level	Status
□	HTTPS.BROWSER	58	16	1	694.69 MB	Medium	Detected
□	Microsoft.Portal	44	13	1	52.44 MB	Elevated	Detected
□	Google.Services	43	15	1	130.99 MB	Elevated	Detected
□	Microsoft.Teams	50	16	1	150.12 MB	Elevated	Detected
□	Microsoft.365.Portal	39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



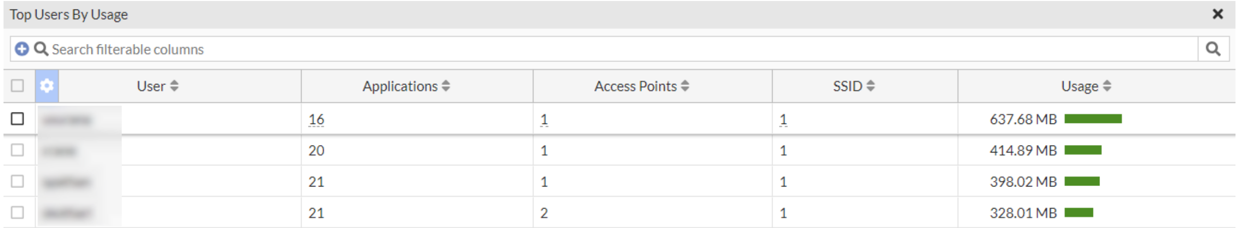
Top Applications By Risk

Search filterable columns

□	Application	Usage	Risk Level	Users
□	HTTPS.BROWSER	524.02 MB	Medium	56
□	Facebook	81.95 MB	Medium	9
□	Microsoft.Outlook	76.69 MB	Medium	11
□	Microsoft.Exchange.Server	62.39 MB	Medium	42

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.

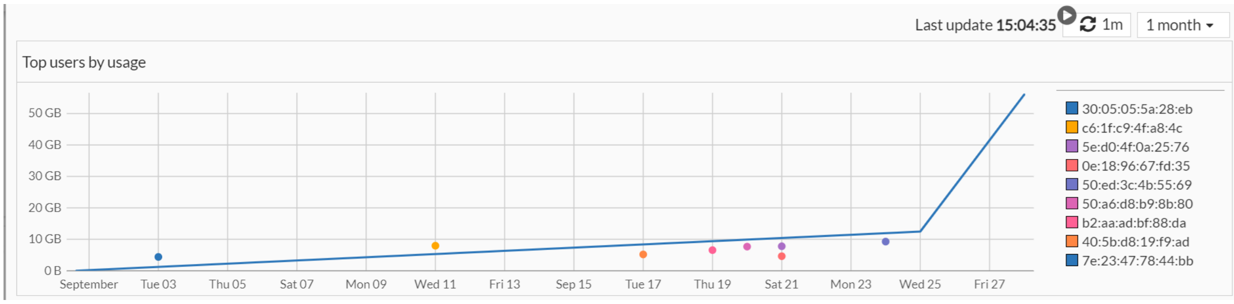


Top Users By Usage

Search filterable columns

□	User	Applications	Access Points	SSID	Usage
□	[redacted]	16	1	1	637.68 MB
□	[redacted]	20	1	1	414.89 MB
□	[redacted]	21	1	1	398.02 MB
□	[redacted]	21	2	1	328.01 MB

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**.



Last update **15:04:35** 1m 1 month

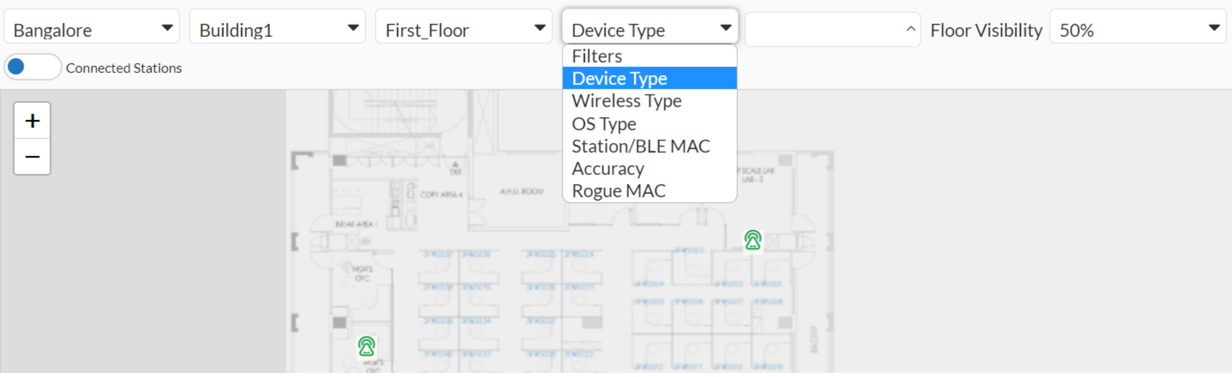
Location Services Monitor

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.

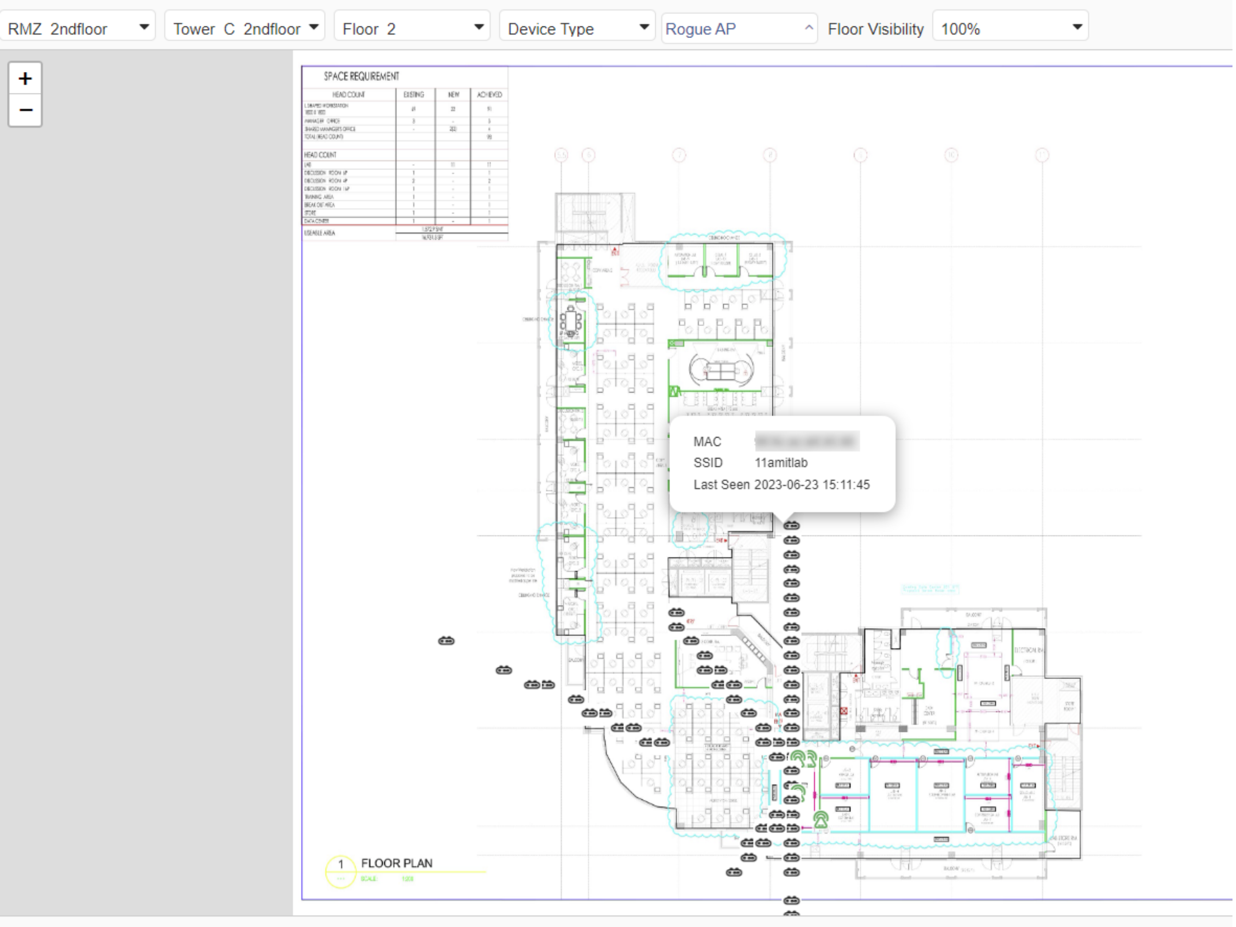
- Device Type
- Wireless Type
- OS Type
- Station/BLE MAC
- Accuracy
- Rogue MAC

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



Bangalore
Building1
First_Floor
Device Type
Floor Visibility 50%
Connected Stations

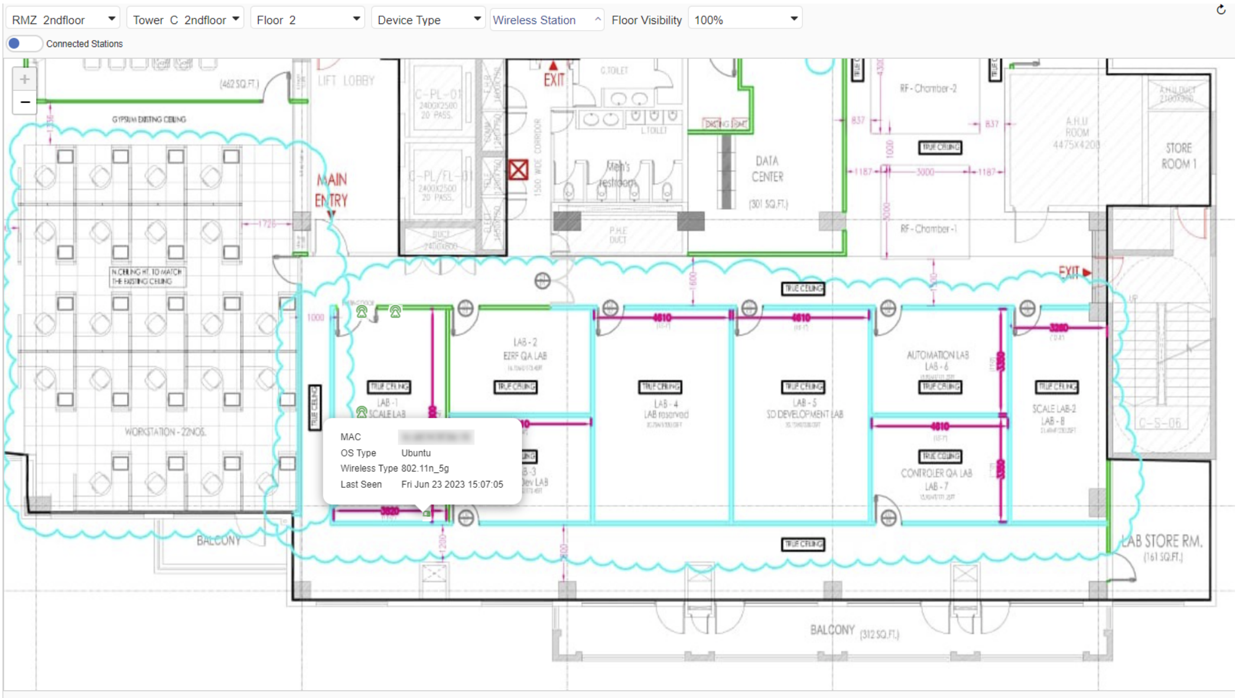
Select **Rogue AP** as the **Device Type**, to view the rouge AP location.



RMZ 2ndfloor
Tower C 2ndfloor
Floor 2
Device Type
Rogue AP
Floor Visibility 100%

MAC [redacted]
SSID 11amitlab
Last Seen 2023-06-23 15:11:45

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



RMZ 2ndfloor | Tower C 2ndfloor | Floor 2 | Device Type: Wireless Station | Floor Visibility: 100%

Connected Stations

MAC [redacted]
OS Type Ubuntu
Wireless Type 802.11n_5g
Last Seen Fri Jun 23 2023 15:07:05

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

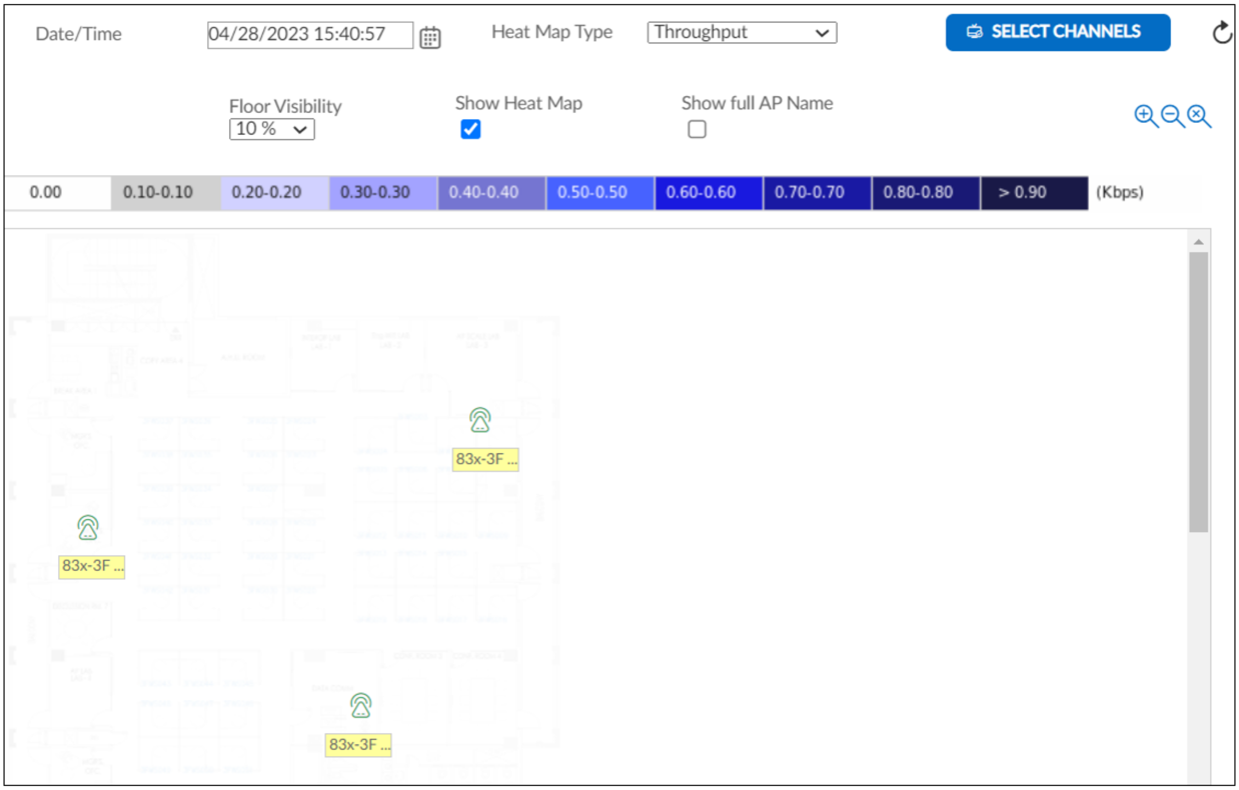
Heat Maps

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.



Date/Time 04/28/2023 15:40:57

Heat Map Type Throughput

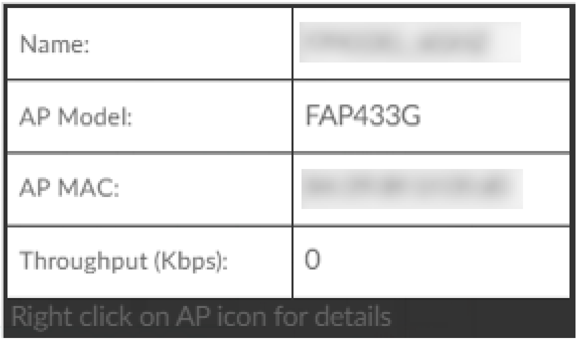
Floor Visibility 10 %

Show Heat Map ☑

Show full AP Name □

0.00	0.10-0.10	0.20-0.20	0.30-0.30	0.40-0.40	0.50-0.50	0.60-0.60	0.70-0.70	0.80-0.80	> 0.90	(Kbps)

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



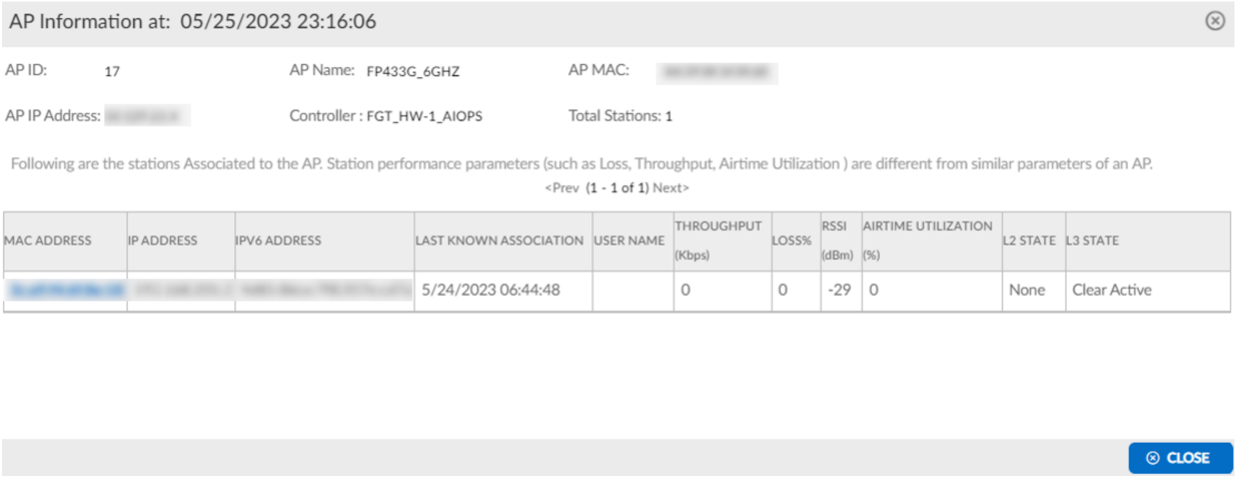
Name:	[redacted]
AP Model:	FAP433G
AP MAC:	[redacted]
Throughput (Kbps):	0

Right click on AP icon for details

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.



AP Information at: 05/25/2023 23:16:06

AP ID: 17 AP Name: FP433G_6GHZ AP MAC: [redacted]

AP IP Address: [redacted] Controller : FGT_HW-1_AIOPS Total Stations: 1

Following are the stations Associated to the AP. Station performance parameters (such as Loss, Throughput, Airtime Utilization) are different from similar parameters of an AP.

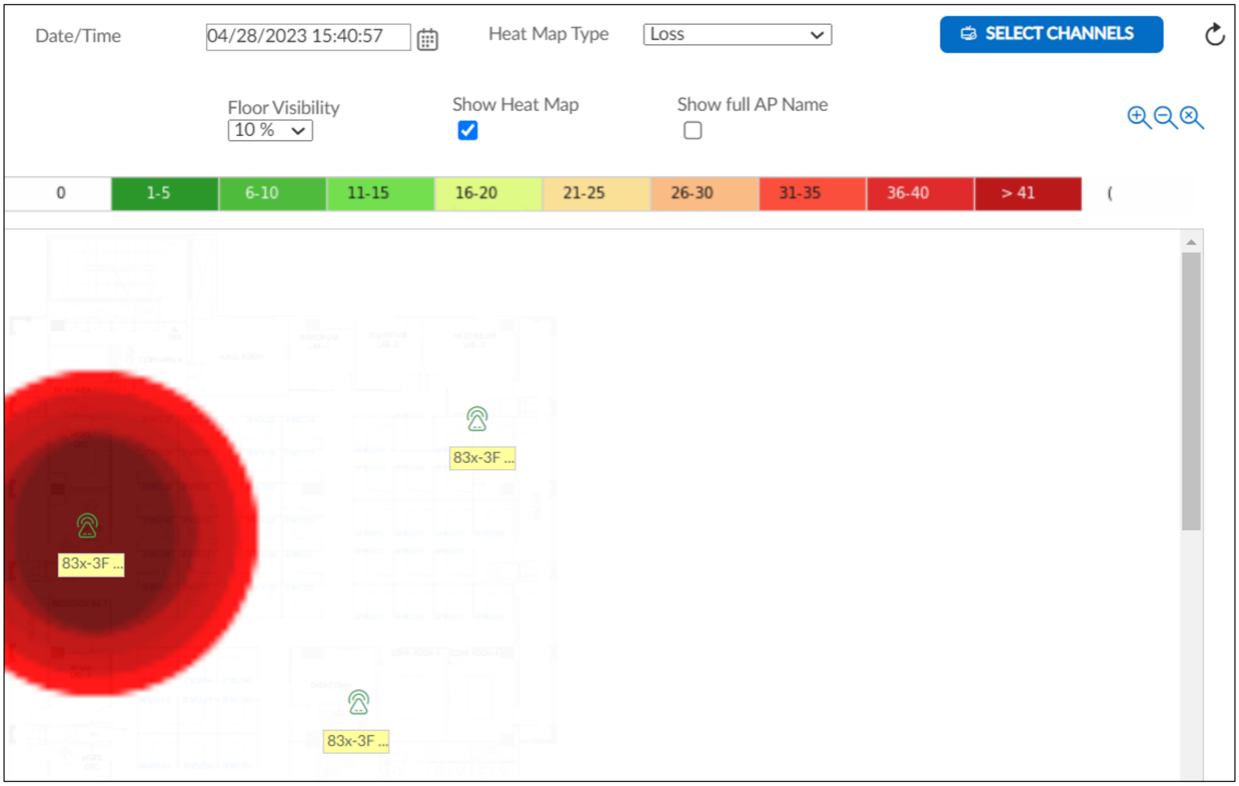
<Prev (1 - 1 of 1) Next>

MAC ADDRESS	IP ADDRESS	IPV6 ADDRESS	LAST KNOWN ASSOCIATION	USER NAME	THROUGHPUT (Kbps)	LOSS%	RSSI (dBm)	AIRTIME UTILIZATION (%)	L2 STATE	L3 STATE
[redacted]	[redacted]	[redacted]	5/24/2023 06:44:48		0	0	-29	0	None	Clear Active

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.



Date/Time 04/28/2023 15:40:57

Heat Map Type Loss

Floor Visibility 10 %

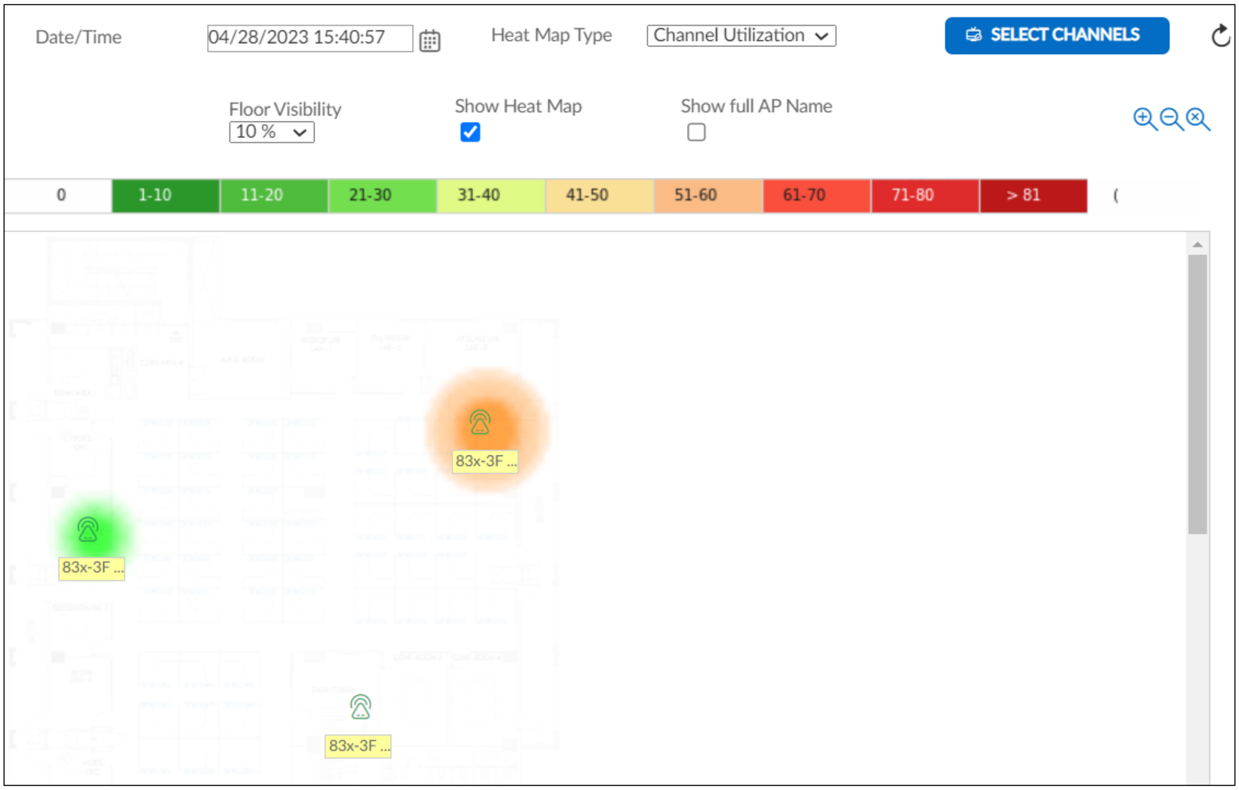
Show Heat Map ☑

Show full AP Name ☐

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.



Date/Time: 04/28/2023 15:40:57

Heat Map Type: Channel Utilization

Floor Visibility: 10 %

Show Heat Map ☑

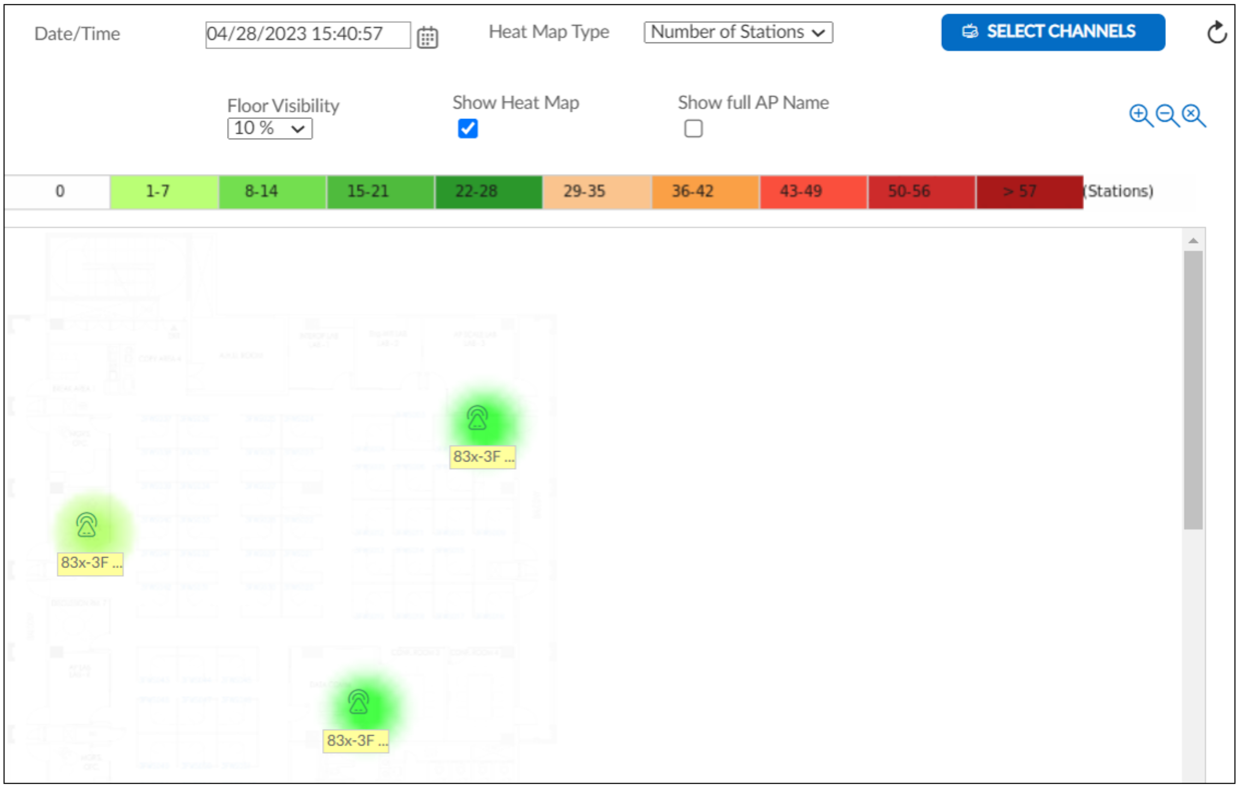
Show full AP Name ☐

0	1-10	11-20	21-30	31-40	41-50	51-60	61-70	71-80	> 81

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.



Date/Time 04/28/2023 15:40:57

Heat Map Type Number of Stations

Floor Visibility 10 %

Show Heat Map ☑

Show full AP Name ☐

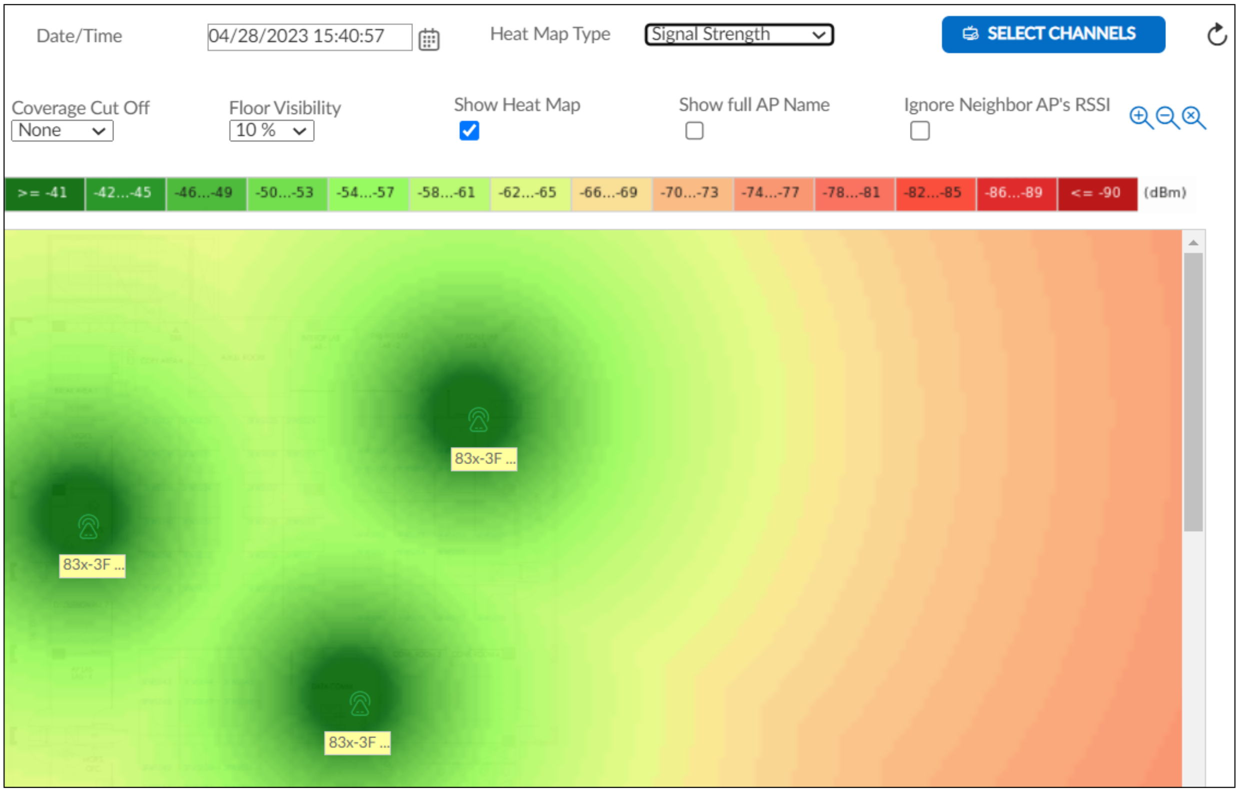
0	1-7	8-14	15-21	22-28	29-35	36-42	43-49	50-56	> 57	(Stations)

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.



Date/Time 04/28/2023 15:40:57

Heat Map Type: Signal Strength

Coverage Cut Off: None

Floor Visibility: 10 %

Show Heat Map ☑

Show full AP Name □

Ignore Neighbor AP's RSSI □

>= -41	-42...-45	-46...-49	-50...-53	-54...-57	-58...-61	-62...-65	-66...-69	-70...-73	-74...-77	-78...-81	-82...-85	-86...-89	<= -90	(dBm)

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.

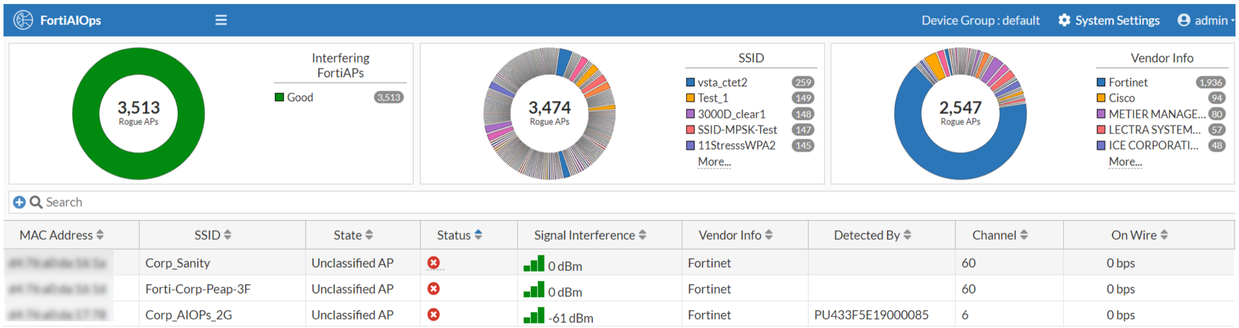
Coverage Cut Off: Coverage cutoff [default being none] can be used to see the signal coverage region within the cutoff value specified. The cutoff range is from -42dBM to -90dBM.

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 FortiAPs	
🟩 Good	3,513

SSID	
vsta_ctet2	259
Test_1	149
3000D_clear1	148
SSID-MPSK-Test	147
11StresssWPA2	145
More...	

Vendor Info	
Fortinet	1,936
Cisco	94
METIER MANAGE...	80
LECTRA SYSTEM...	57
ICE CORPORATI...	48
More...	

MAC Address	SSID	State	Status	Signal Interference	Vendor Info	Detected By	Channel	On Wire
[redacted]	Corp_Sanity	Unclassified AP	☒	0 dBm	Fortinet		60	0 bps
[redacted]	Forti-Corp-Peap-3F	Unclassified AP	☒	0 dBm	Fortinet		60	0 bps
[redacted]	Corp_AIOPs_2G	Unclassified AP	☒	-61 dBm	Fortinet	PU433F5E19000085	6	0 bps

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.

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.

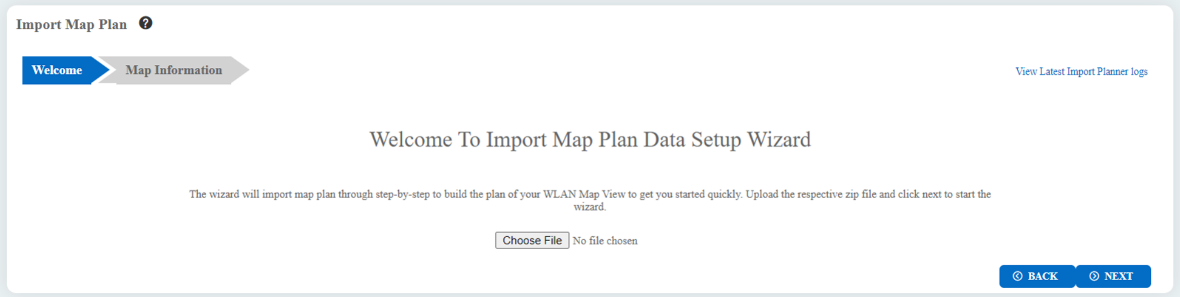
Next, add controllers and APs to the map.

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.



Import Map Plan

Welcome To Import Map Plan Data Setup Wizard

The wizard will import map plan through step-by-step to build the plan of your WLAN Map View to get you started quickly. Upload the respective zip file and click next to start the wizard.

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:

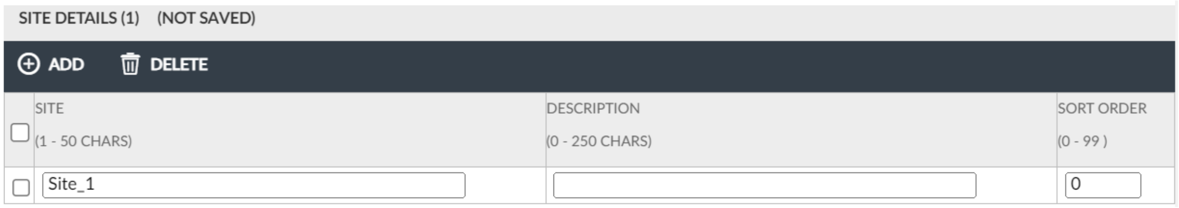
- **Add APs** - Select the APs to be added to the floor map.
- **Floor APs** - Select the APs to be deleted from the floor map.
- **Landmarks** - Add or delete landmarks on the floor map.
- **Change Image** - Upload a new image or delete an existing image from the floor map.

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.

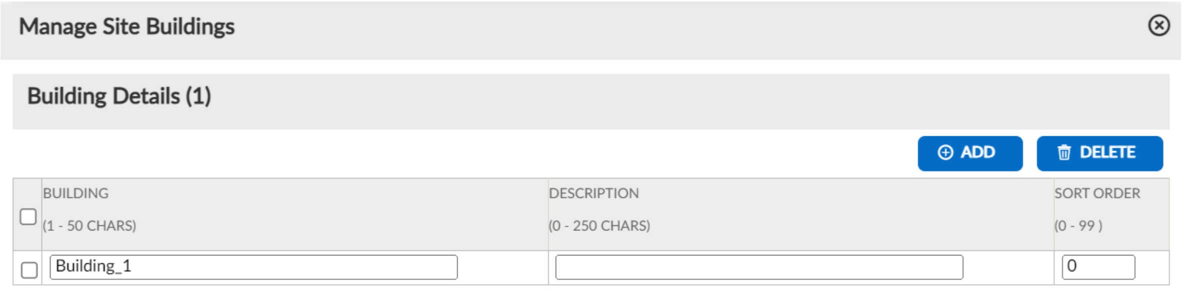


SITE DETAILS (1) (NOT SAVED)

⊕ ADD 🗑 DELETE

□	SITE (1 - 50 CHARS)	DESCRIPTION (0 - 250 CHARS)	SORT ORDER (0 - 99)
□	Site_1		0

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**.



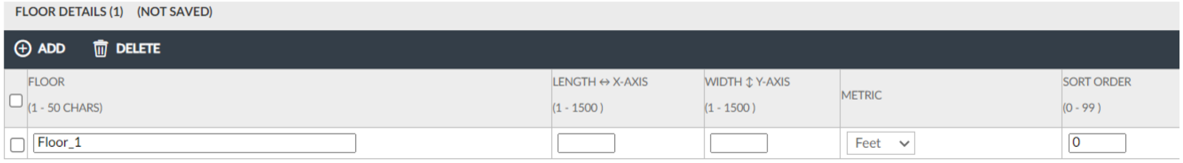
Manage Site Buildings ⊗

Building Details (1)

⊕ ADD 🗑 DELETE

□	BUILDING (1 - 50 CHARS)	DESCRIPTION (0 - 250 CHARS)	SORT ORDER (0 - 99)
□	Building_1		0

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**.



FLOOR DETAILS (1) (NOT SAVED)

⊕ ADD 🗑 DELETE

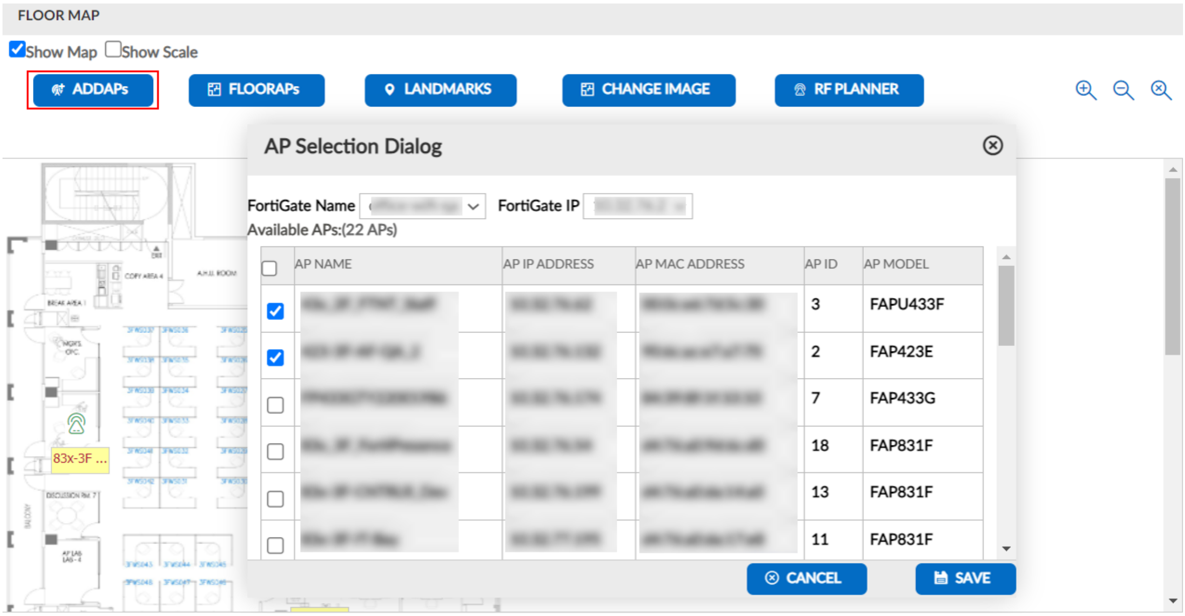
□	FLOOR (1 - 50 CHARS)	LENGTH ↔ X-AXIS (1 - 1500)	WIDTH ↕ Y-AXIS (1 - 1500)	METRIC	SORT ORDER (0 - 99)
□	Floor_1			Feet	0

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.



AP Selection Dialog

FortiGate Name [redacted] FortiGate IP [redacted]

Available APs:(22 APs)

□	AP NAME	AP IP ADDRESS	AP MAC ADDRESS	AP ID	AP MODEL
☑	[redacted]	[redacted]	[redacted]	3	FAPU433F
☑	[redacted]	[redacted]	[redacted]	2	FAP423E
□	[redacted]	[redacted]	[redacted]	7	FAP433G
□	[redacted]	[redacted]	[redacted]	18	FAP831F
□	[redacted]	[redacted]	[redacted]	13	FAP831F
□	[redacted]	[redacted]	[redacted]	11	FAP831F

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

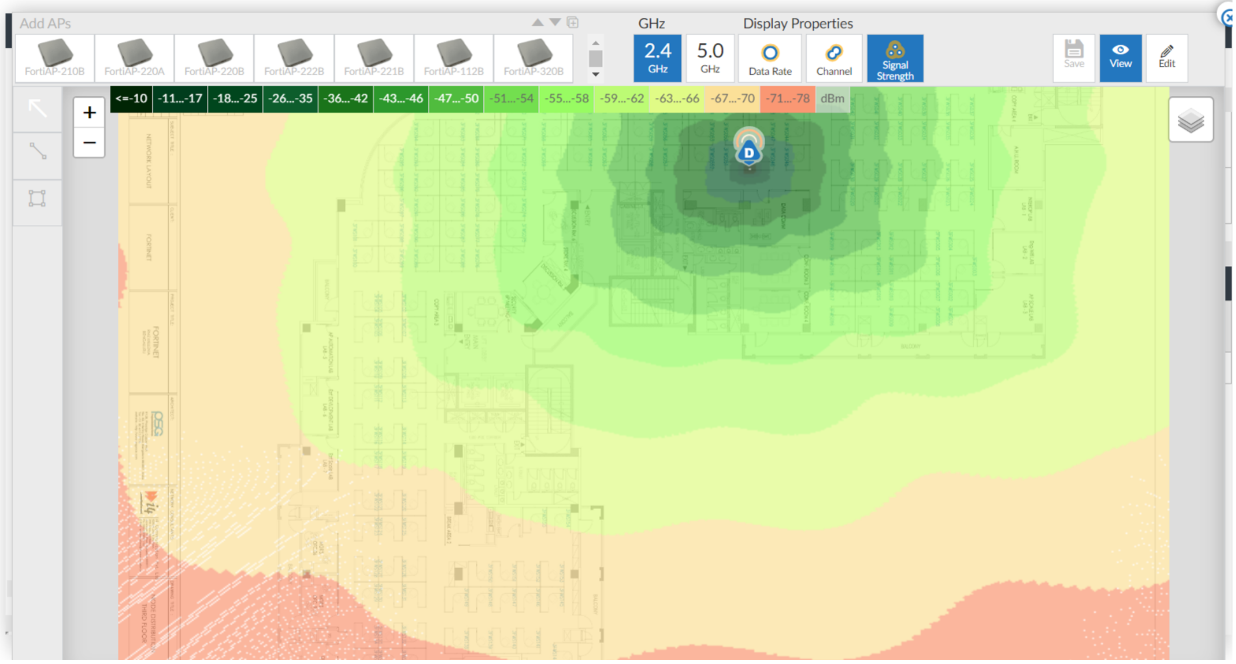
Heat map coloring depends on the distance between APs and selected attribute (throughput, loss, channel utilization, or stations) for all the APs on the floor. If there is only one AP on the floor, the entire floor will show the same coverage. See Heat Maps.

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.

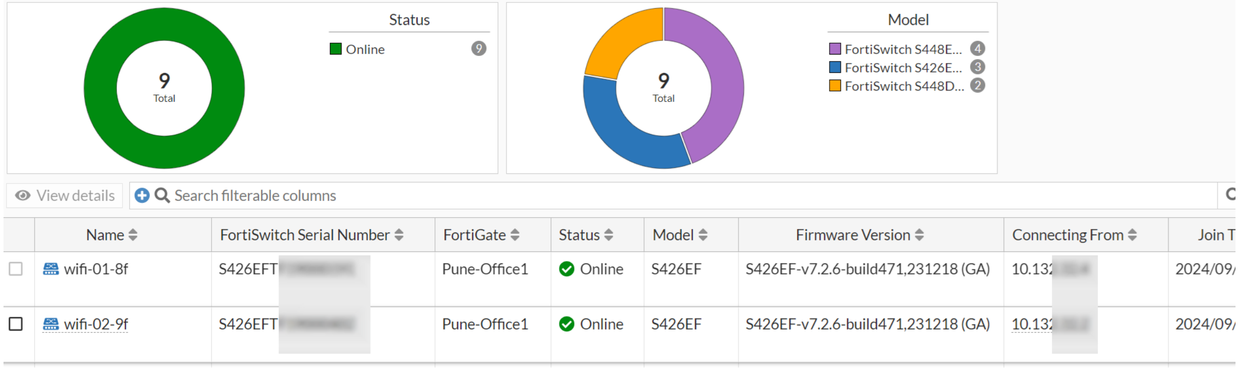
Switch

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

- FortiSwitch
- FortiSwitch Clients

FortiSwitch

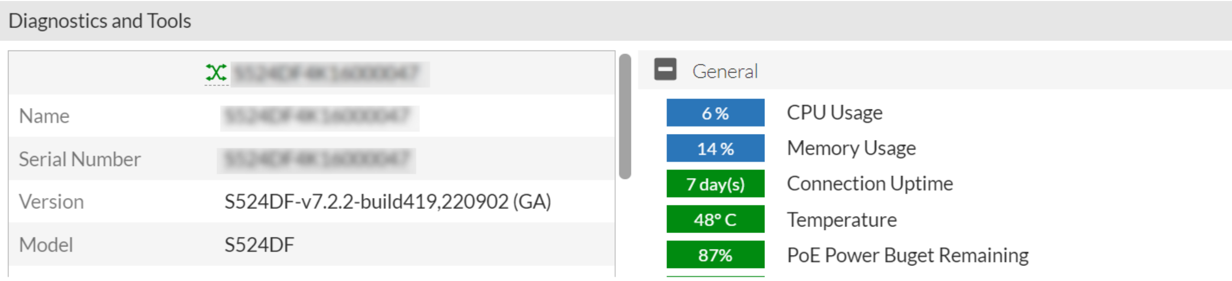
You can monitor the FortiSwitches in your network that are in the purview of FortiAIOps. This page displays a graphical snapshot of the FortiSwitch activity such as, the total number of FortiSwitches, their status (online/offline/unauthorized), and the deployed model details.



	Name	FortiSwitch Serial Number	FortiGate	Status	Model	Firmware Version	Connecting From	Join T
□	wifi-01-8f	S426EFT[redacted]	Pune-Office1	✓ Online	S426EF	S426EF-v7.2.6-build471,231218 (GA)	10.132[redacted]	2024/09/
□	wifi-02-9f	S426EFT[redacted]	Pune-Office1	✓ Online	S426EF	S426EF-v7.2.6-build471,231218 (GA)	10.132[redacted]	2024/09/

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.



Diagnostics and Tools

	[redacted]
Name	[redacted]
Serial Number	[redacted]
Version	S524DF-v7.2.2-build419,220902 (GA)
Model	S524DF

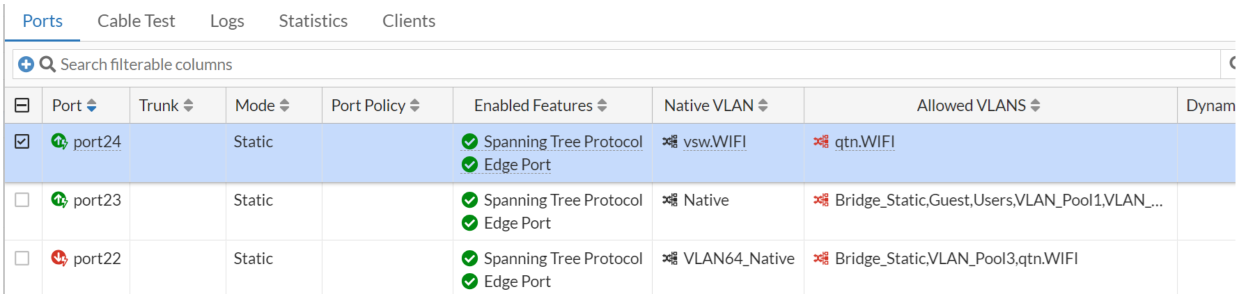
General

6 %	CPU Usage
14 %	Memory Usage
7 day(s)	Connection Uptime
48° C	Temperature
87%	PoE Power Buget Remaining

- Ports
- Cable Test
- Logs
- Statistics
- Clients

Ports

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



⊟	Port	Trunk	Mode	Port Policy	Enabled Features	Native VLAN	Allowed VLANS	Dynam
☑	port24		Static		✓ Spanning Tree Protocol ✓ Edge Port	vsw.WIFI	qtn.WIFI	
☐	port23		Static		✓ Spanning Tree Protocol ✓ Edge Port	Native	Bridge_Static,Guest,Users,VLAN_Pool1,VLAN_...	
☐	port22		Static		✓ Spanning Tree Protocol ✓ Edge Port	VLAN64_Native	Bridge_Static,VLAN_Pool3,qtn.WIFI	

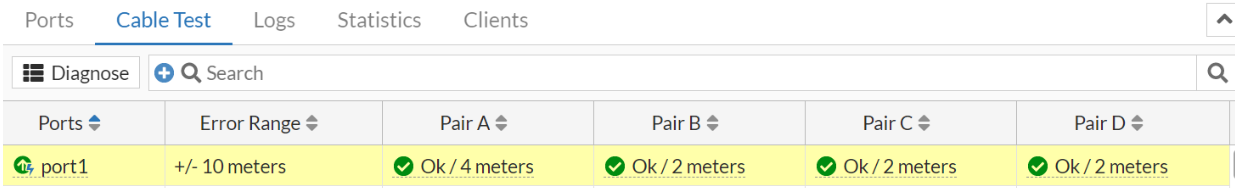
Each entry in the port list displays the following information.

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**.

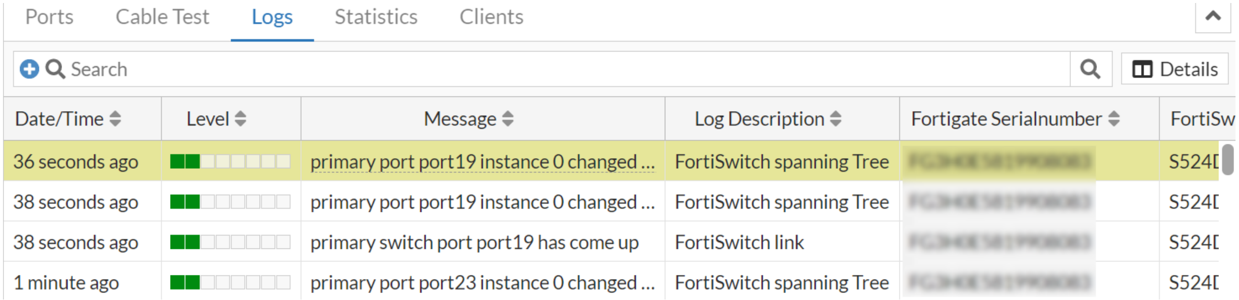


Ports	Error Range	Pair A	Pair B	Pair C	Pair D
port1	+/- 10 meters	✓ Ok / 4 meters	✓ Ok / 2 meters	✓ Ok / 2 meters	✓ Ok / 2 meters

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.

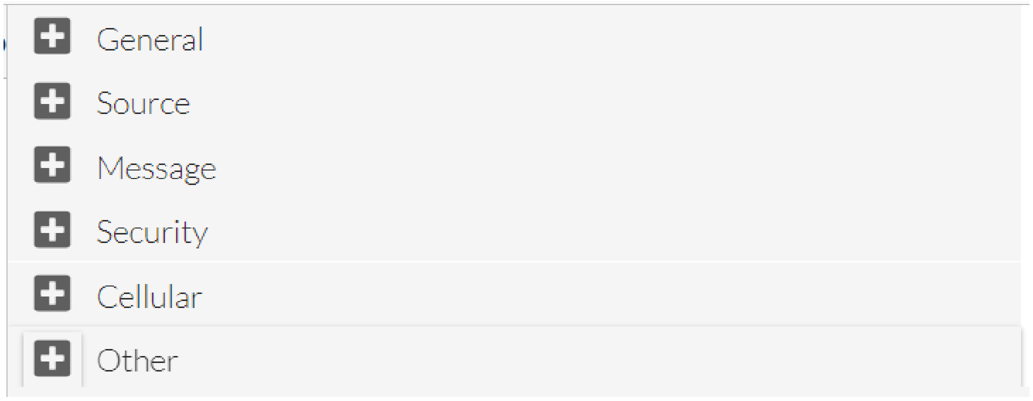


Date/Time	Level	Message	Log Description	Fortigate Serialnumber	FortiSw
36 seconds ago	🟩🟩□□□□□□	primary port port19 instance 0 changed ...	FortiSwitch spanning Tree	[redacted]	S524
38 seconds ago	🟩🟩□□□□□□	primary port port19 instance 0 changed ...	FortiSwitch spanning Tree	[redacted]	S524
38 seconds ago	🟩🟩□□□□□□	primary switch port port19 has come up	FortiSwitch link	[redacted]	S524
1 minute ago	🟩🟩□□□□□□	primary port port23 instance 0 changed ...	FortiSwitch spanning Tree	[redacted]	S524

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.

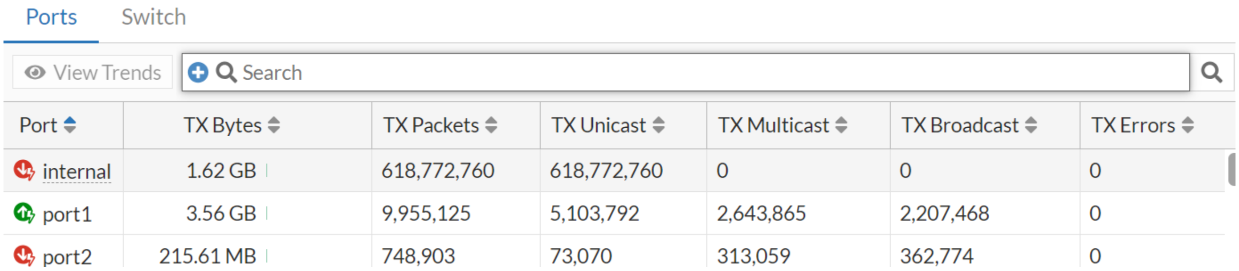
Select a log message and click **Details** to view specific related information. This view provides the following information.



- **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.



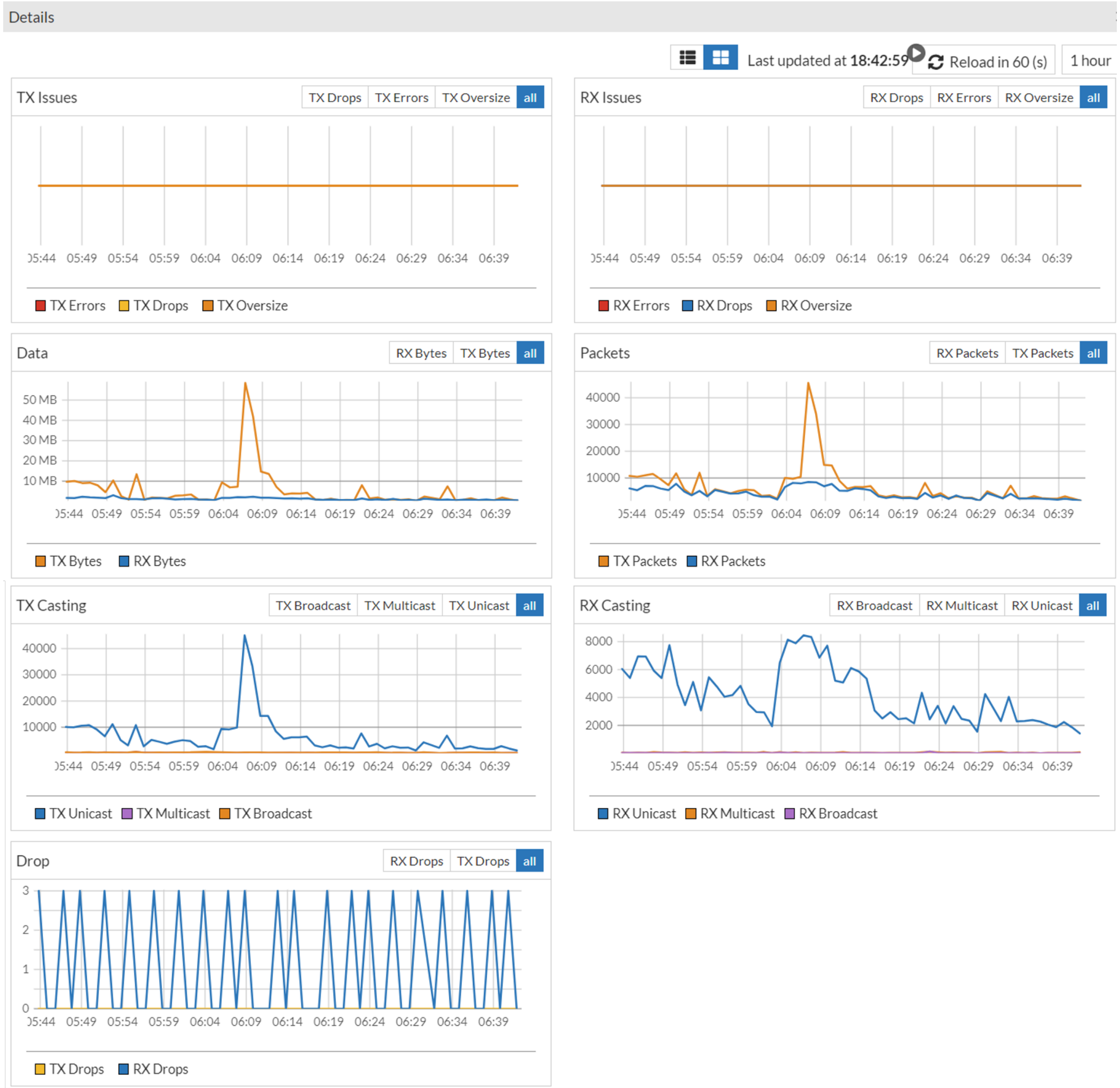
Port	TX Bytes	TX Packets	TX Unicast	TX Multicast	TX Broadcast	TX Errors
internal	1.62 GB	618,772,760	618,772,760	0	0	0
port1	3.56 GB	9,955,125	5,103,792	2,643,865	2,207,468	0
port2	215.61 MB	748,903	73,070	313,059	362,774	0

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

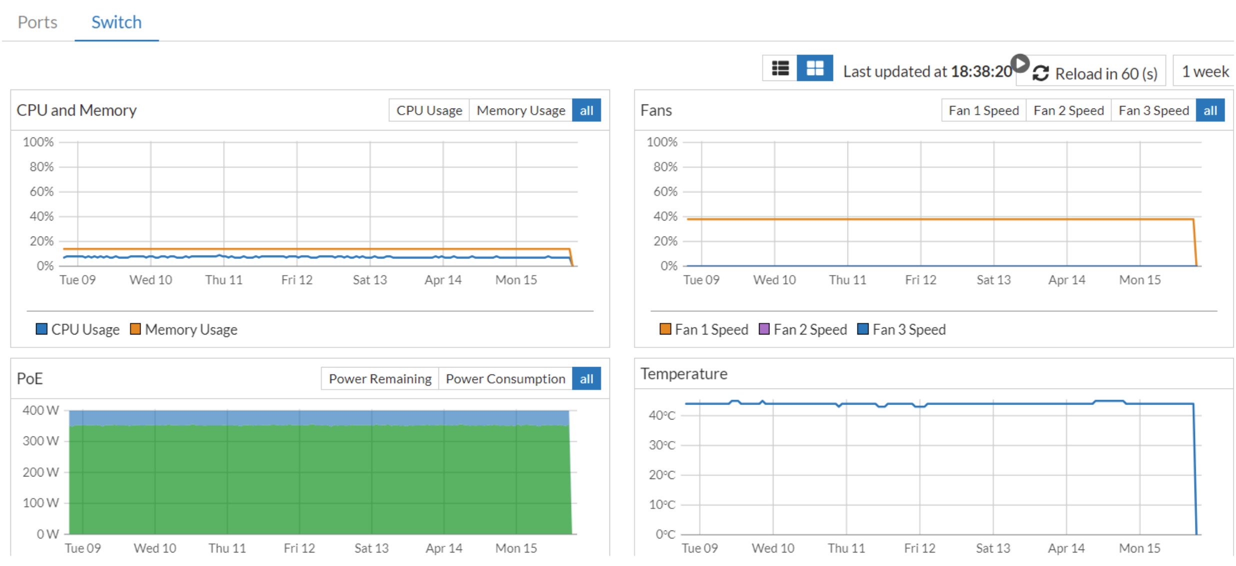
Parameter	Description
TX Bytes	The transmitted bytes.
TX Packets	The transmitted packets.
TX Unicast	The transmitted unicast packets.
TX Multicast	The transmitted multicast packets.
TX Broadcast	The transmitted broadcast packets.
TX Errors	The errors in transmitted packets.
TX Drops	The dropped packets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

Parameter	Description
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

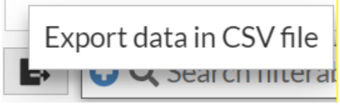
This tab displays the details of the FortiSwitch clients. The following information is displayed.

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.

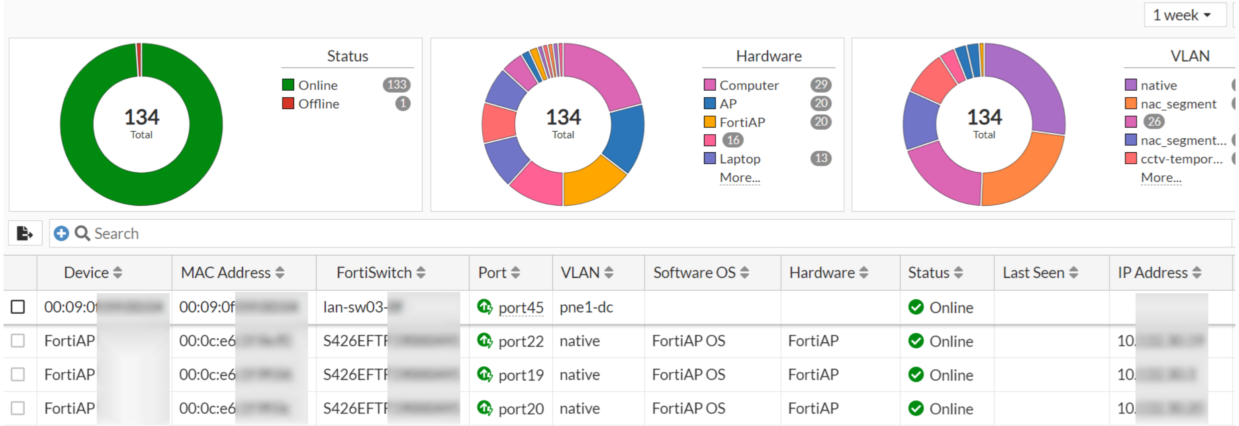
FortiSwitch Clients

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.
- You can export data in a *.csv* file, click on the export icon on these pages.



.



	Device	MAC Address	FortiSwitch	Port	VLAN	Software OS	Hardware	Status	Last Seen	IP Address
□	00:09:0f[redacted]	00:09:0f[redacted]	lan-sw03-[redacted]	port45	pne1-dc			✓ Online		[redacted]
□	FortiAP[redacted]	00:0c:e6[redacted]	S426EFTF[redacted]	port22	native	FortiAP OS	FortiAP	✓ Online		10.[redacted]
□	FortiAP[redacted]	00:0c:e6[redacted]	S426EFTF[redacted]	port19	native	FortiAP OS	FortiAP	✓ Online		10.[redacted]
□	FortiAP[redacted]	00:0c:e6[redacted]	S426EFTF[redacted]	port20	native	FortiAP OS	FortiAP	✓ Online		10.[redacted]

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.

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.

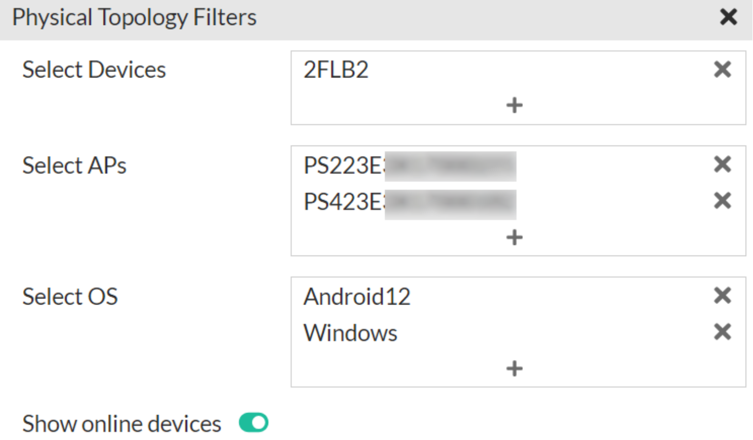
Note: The physical and logical topologies provide wireless client information.

- 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**.



Physical Topology Filters ✕

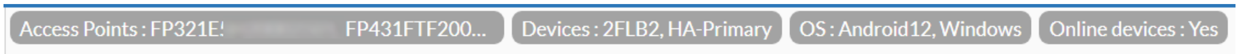
Select Devices: 2FLB2 ✕ +

Select APs: PS223E[redacted] ✕ PS423E[redacted] ✕ +

Select OS: Android12 ✕ Windows ✕ +

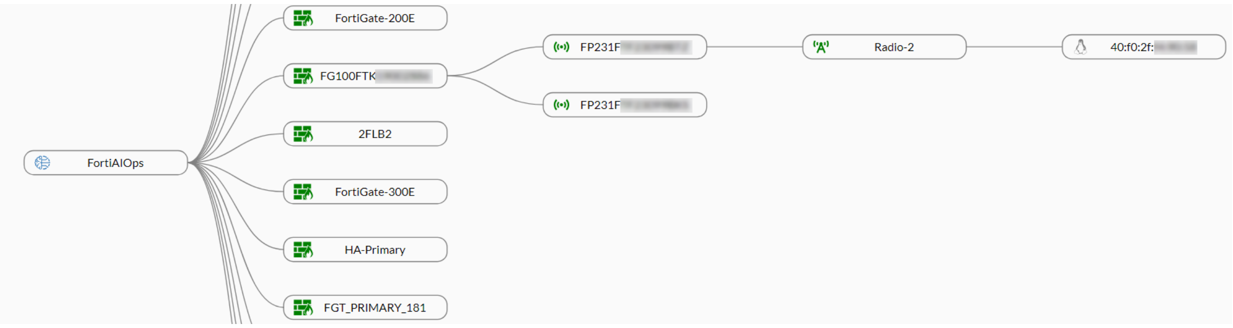
Show online devices ●

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.



Access Points : FP321E[redacted] FP431FTF200... | Devices : 2FLB2, HA-Primary | OS : Android12, Windows | Online devices : Yes

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.



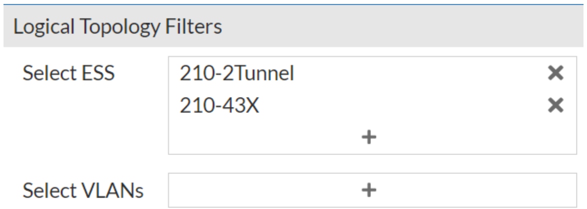
Hover over the device name to obtain additional information. The status of the FortiGate controllers and APs is marked using a color legend.

- *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.

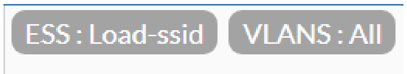
You can filter and view selective entities, the filter options available are ESS and VLANs. To apply the filter setttings, click **Apply Filter**.



Logical Topology Filters

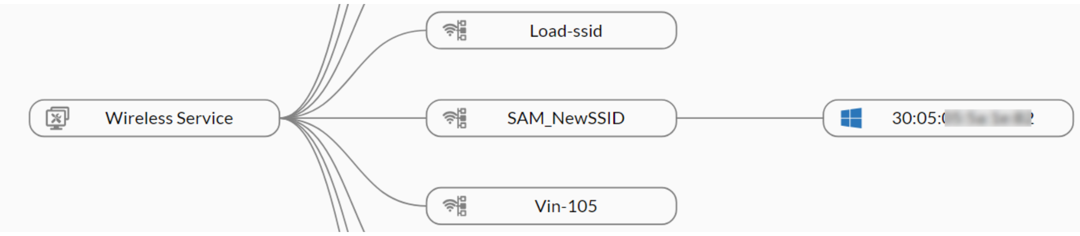
Select ESS	210-2Tunnel ✕ 210-43X ✕ +
Select VLANs	+

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.



ESS : Load-ssid VLANS : All

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.

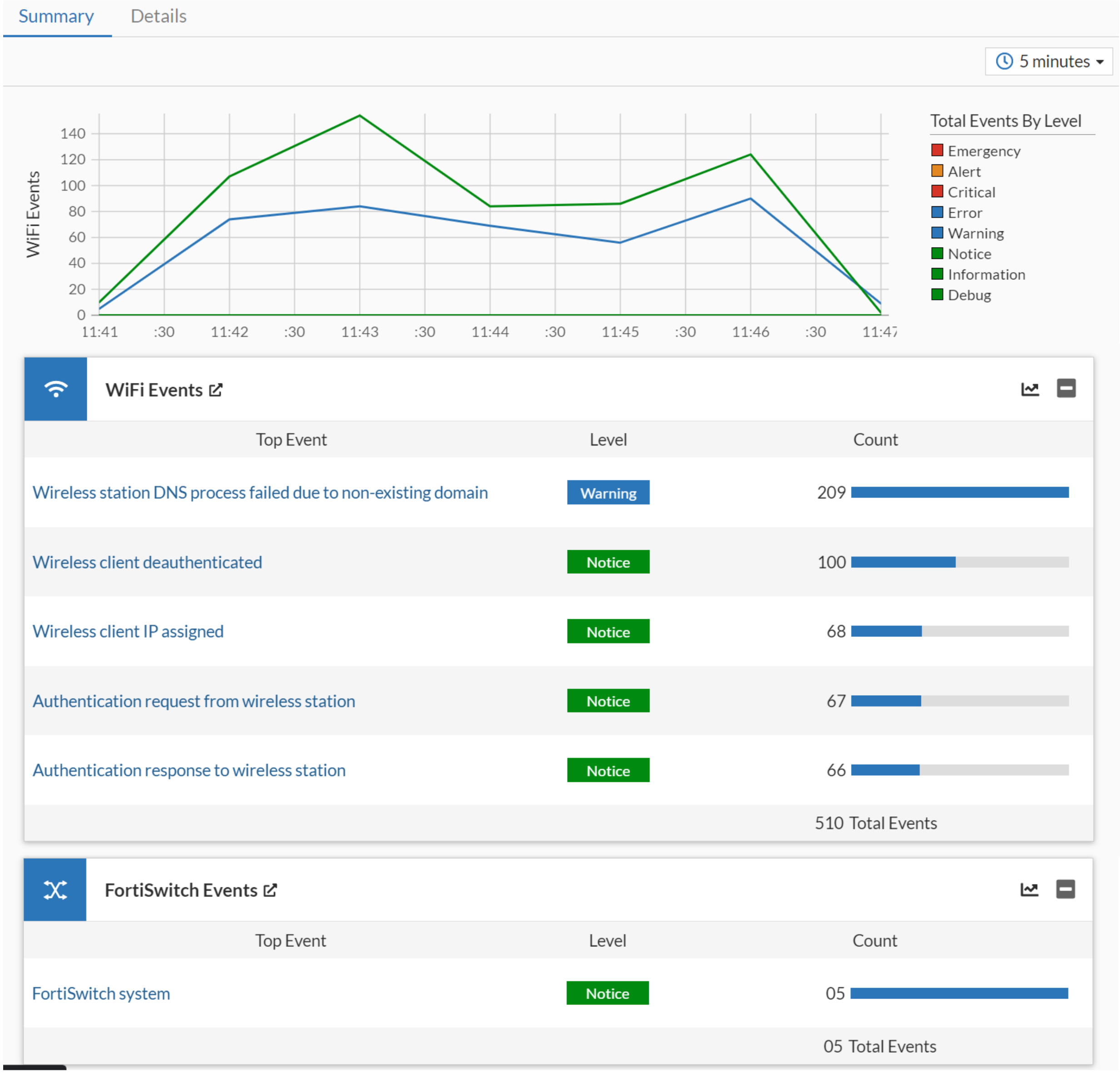
Logs and Reports

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 and FortiSwitch 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. 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.



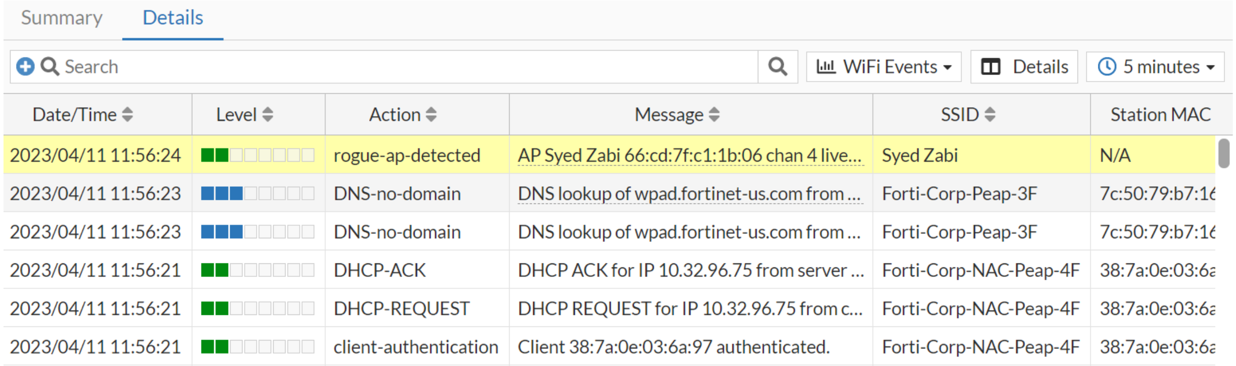
WiFi Events

Top Event	Level	Count
Wireless station DNS process failed due to non-existing domain	Warning	209
Wireless client deauthenticated	Notice	100
Wireless client IP assigned	Notice	68
Authentication request from wireless station	Notice	67
Authentication response to wireless station	Notice	66
		510 Total Events

FortiSwitch Events

Top Event	Level	Count
FortiSwitch system	Notice	05
		05 Total Events

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** data on this page.

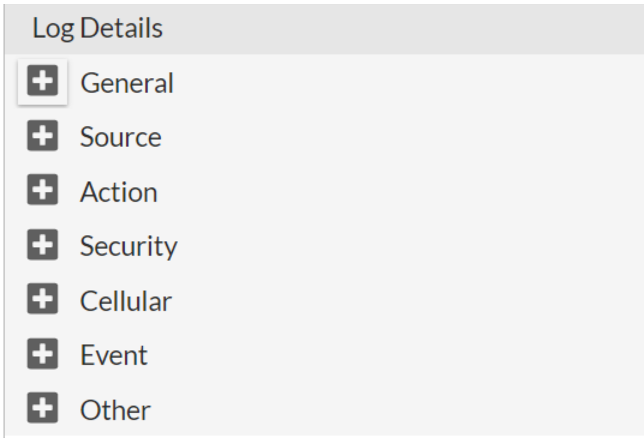


Date/Time	Level	Action	Message	SSID	Station MAC
2023/04/11 11:56:24	🟩🟩□□□□□□	rogue-ap-detected	AP Syed Zabi 66:cd:7f:c1:1b:06 chan 4 live...	Syed Zabi	N/A
2023/04/11 11:56:23	🟦🟦🟦□□□□□	DNS-no-domain	DNS lookup of wpad.fortinet-us.com from ...	Forti-Corp-Peap-3F	7c:50:79:b7:16
2023/04/11 11:56:23	🟦🟦🟦□□□□□	DNS-no-domain	DNS lookup of wpad.fortinet-us.com from ...	Forti-Corp-Peap-3F	7c:50:79:b7:16
2023/04/11 11:56:21	🟩🟩□□□□□□	DHCP-ACK	DHCP ACK for IP 10.32.96.75 from server ...	Forti-Corp-NAC-Peap-4F	38:7a:0e:03:6a
2023/04/11 11:56:21	🟩🟩□□□□□□	DHCP-REQUEST	DHCP REQUEST for IP 10.32.96.75 from c...	Forti-Corp-NAC-Peap-4F	38:7a:0e:03:6a
2023/04/11 11:56:21	🟩🟩□□□□□□	client-authentication	Client 38:7a:0e:03:6a:97 authenticated.	Forti-Corp-NAC-Peap-4F	38:7a:0e:03:6a

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.
AP Serial Number	The serial number of the access point that the client associated with.
Relative Date/Time	The time lapsed since the event log was generated.
Channel	The channel associated with the access point.
FortiSwitch Serial Number	The serial number of the associated FortiSwitch.
Log Description	The description of the event log.
Source	The event source IP/MAC address.
User	The user name/details.

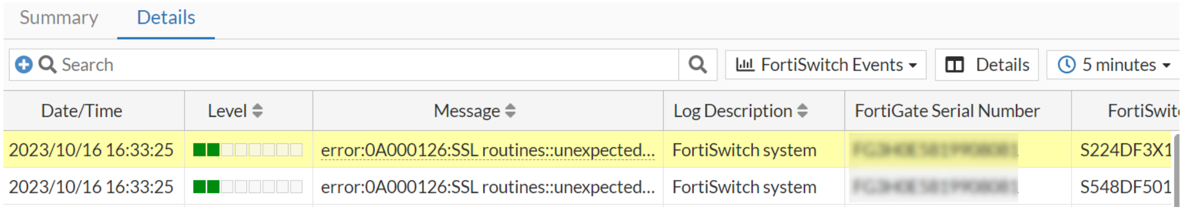
Select a log message and click **Details** to view specific related information. This view provides the following information.



- **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 log event source such as, MAC address, interface, SSID, and user details.
- **Action** - The action leading to the event log and the reason.

- **Security** - The severity of the log event, the configured security mode, and the encryption type.
- **Cellular** - The serial number of the associated access point.
- **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.\

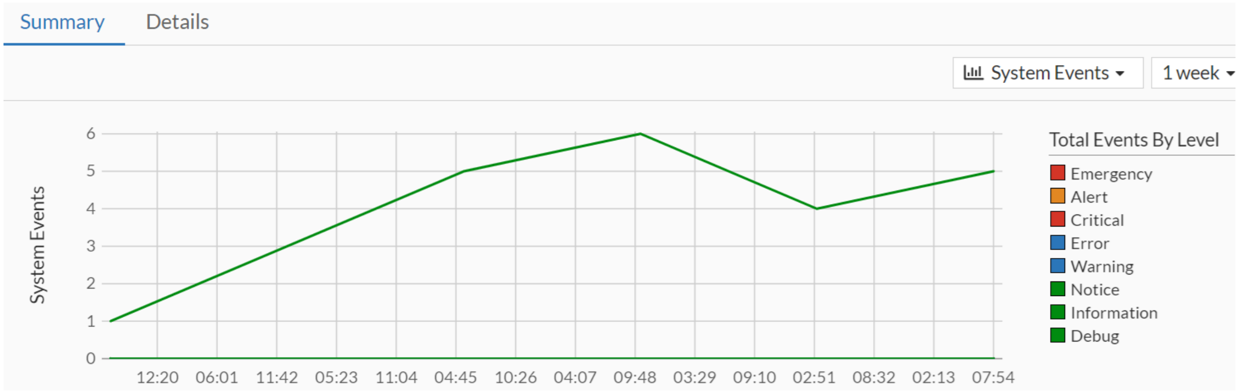
  Click on a specific FortiSwitch event to view the details.



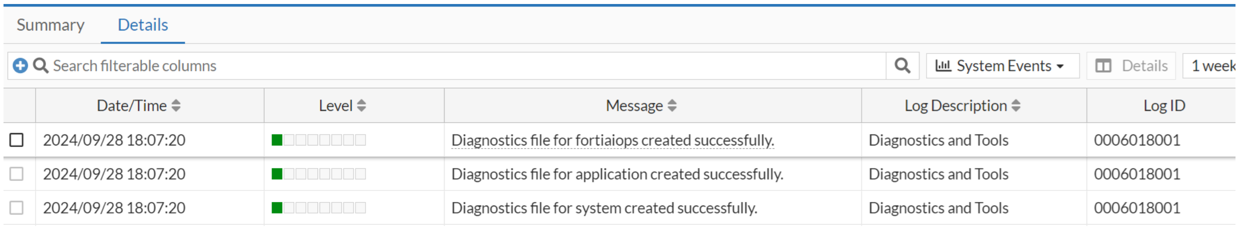
Date/Time	Level	Message	Log Description	FortiGate Serial Number	FortiSwit
2023/10/16 16:33:25	🟩🟩□□□□□□	error:0A000126:SSL routines::unexpected...	FortiSwitch system	[redacted]	S224DF3X1
2023/10/16 16:33:25	🟩🟩□□□□□□	error:0A000126:SSL routines::unexpected...	FortiSwitch system	[redacted]	S548DF501

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.



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

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.

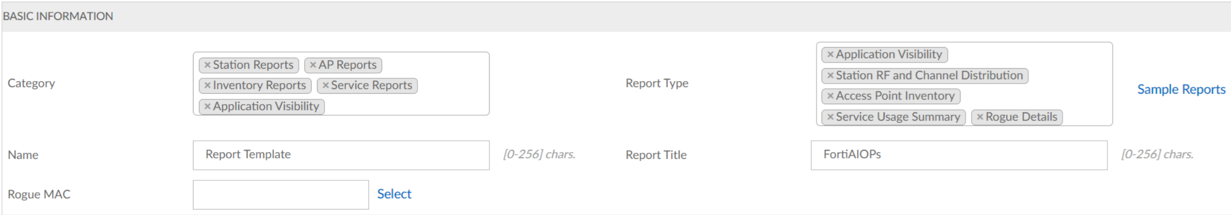
- Creating Reports
- Viewing Reports
- Scheduled Reports
- PCI Reports

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**.



BASIC INFORMATION

Category: ×Station Reports ×AP Reports ×Inventory Reports ×Service Reports ×Application Visibility

Report Type: ×Application Visibility ×Station RF and Channel Distribution ×Access Point Inventory ×Service Usage Summary ×Rogue Details

Name: Report Template [0-256] chars.

Report Title: FortiAIOPs [0-256] chars.

Rogue MAC:

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.

Category	Description
	- *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.
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

Category	Description
	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. - 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.

Category	Description
	• 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 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.

Category	Description
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

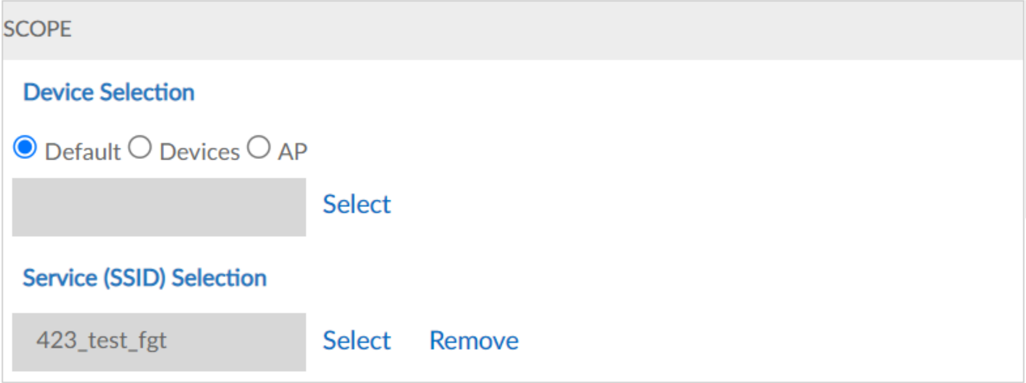
The application visibility reports provide the following information.

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

Category	Description
	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.



SCOPE

Device Selection

● Default ○ Devices ○ AP

Select

Service (SSID) Selection

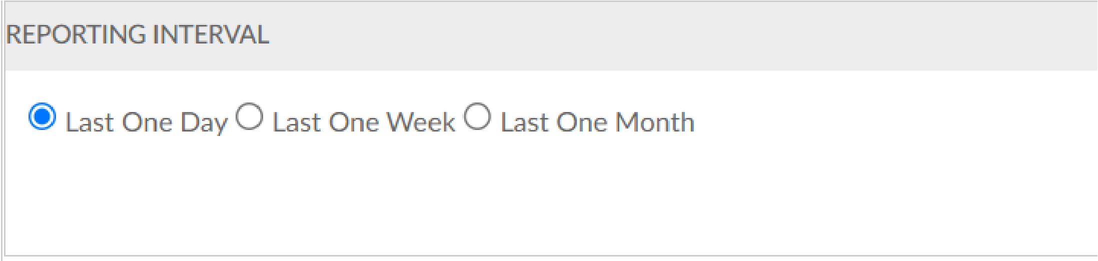
423_test_fgt Select Remove

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.



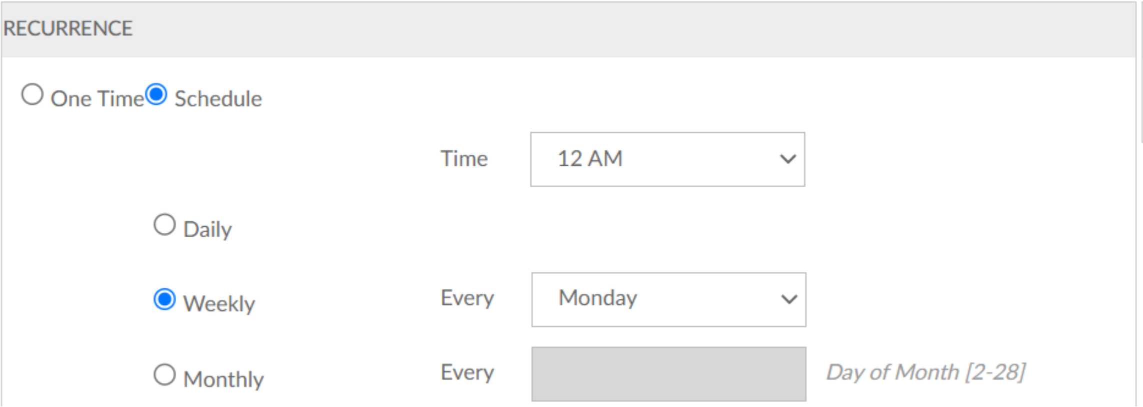
REPORTING INTERVAL

● Last One Day ○ Last One Week ○ Last One Month

- **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.



RECURRENCE

○ One Time ● Schedule

Time: 12 AM

○ Daily

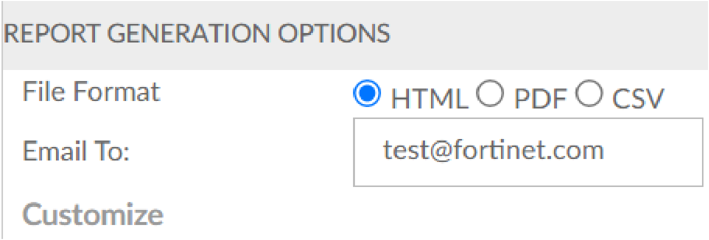
● Weekly — Every: Monday

○ Monthly — Every: Day of Month [2-28]

- **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.



REPORT GENERATION OPTIONS

File Format: ● HTML ○ PDF ○ CSV

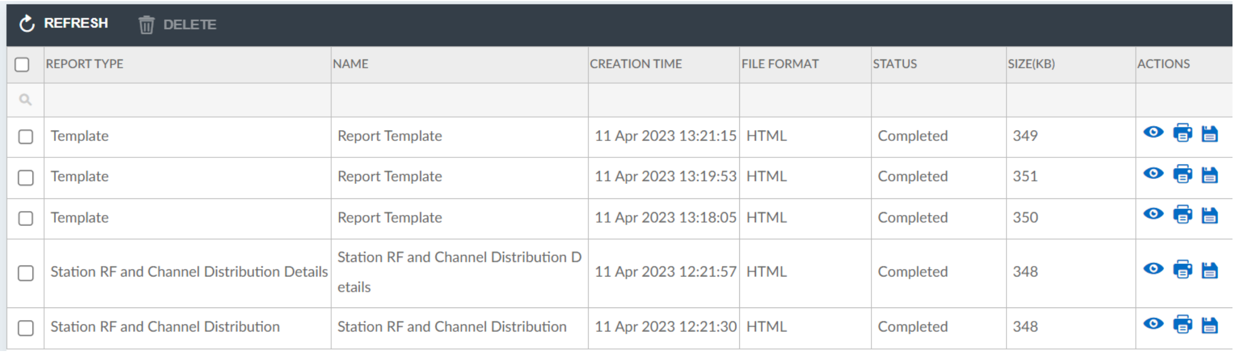
Email To: test@fortinet.com

Customize

- **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

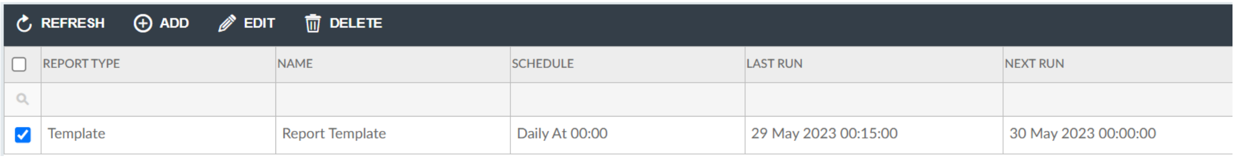
This screen displays a list of all the reports that are generated. These reports can be generated in HTML, CSV, or PDF format. They can be viewed, printed or saved locally.



□	REPORT TYPE	NAME	CREATION TIME	FILE FORMAT	STATUS	SIZE(KB)	ACTIONS
□	Template	Report Template	11 Apr 2023 13:21:15	HTML	Completed	349	👁 🖨 💾
□	Template	Report Template	11 Apr 2023 13:19:53	HTML	Completed	351	👁 🖨 💾
□	Template	Report Template	11 Apr 2023 13:18:05	HTML	Completed	350	👁 🖨 💾
□	Station RF and Channel Distribution Details	Station RF and Channel Distribution Details	11 Apr 2023 12:21:57	HTML	Completed	348	👁 🖨 💾
□	Station RF and Channel Distribution	Station RF and Channel Distribution	11 Apr 2023 12:21:30	HTML	Completed	348	👁 🖨 💾

Scheduled Reports

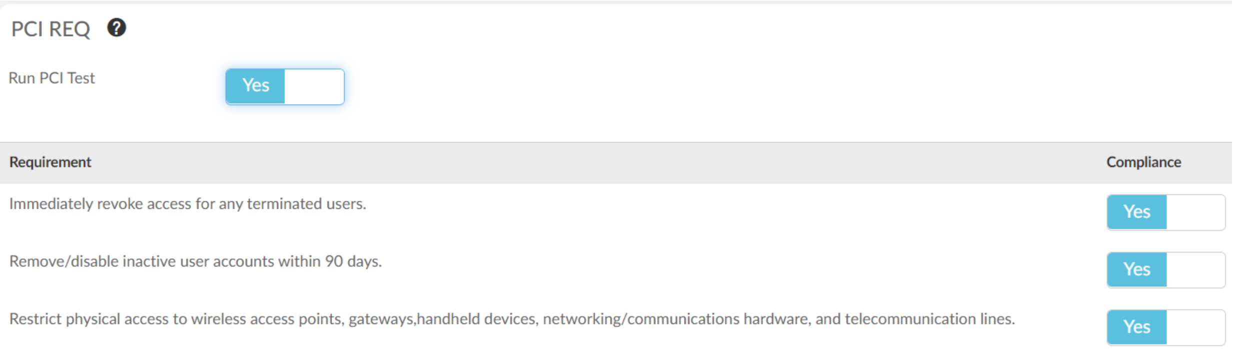
This page displays a list of current running reports and reports scheduled to run in the future. In case of recurring reports, the next run time is displayed. To create a new report, click **Add**.



□	REPORT TYPE	NAME	SCHEDULE	LAST RUN	NEXT RUN
☑	Template	Report Template	Daily At 00:00	29 May 2023 00:15:00	30 May 2023 00:00:00

PCI Reports

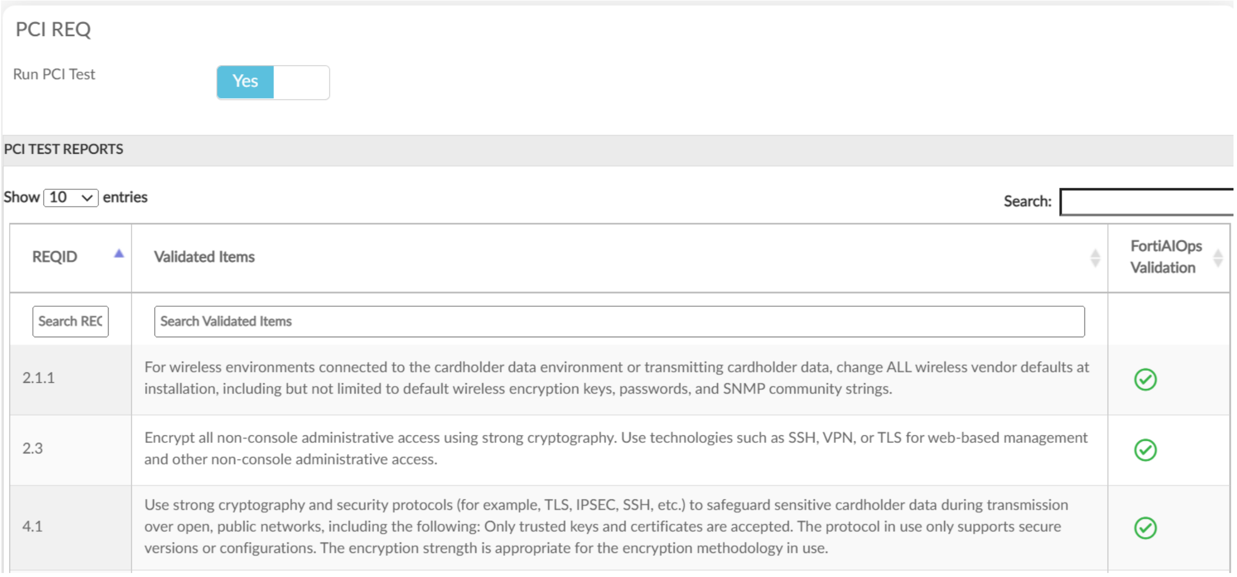
You can validate FortiAIOps against specific PCI requirement compliance. To run a compliance test, enable **Run PCI Test**. Select the tests to validate FortiAIOps and click **Run Test**.



Run PCI Test: Yes

Requirement	Compliance
Immediately revoke access for any terminated users.	Yes
Remove/disable inactive user accounts within 90 days.	Yes
Restrict physical access to wireless access points, gateways,handheld devices, networking/communications hardware, and telecommunication lines.	Yes

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 REQ	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
- Certificates

User Management

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

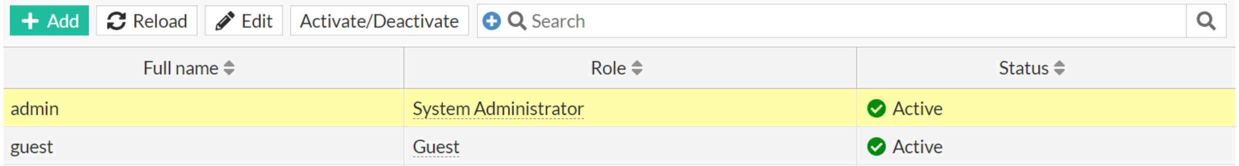
- Users
- User Groups

Users

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

User 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.



Full name	Role	Status
admin	System Administrator	✓ Active
guest	Guest	✓ Active

- Adding a New User
- Editing User Information
- Activating/Deactivating User

Adding a New User

Perform the following steps to add a new user:

- Click **+Add User**.
- Enter the user information including full name, username and password.
- 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.
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.

- 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.
- The user list for the FortiAIOps CLI and GUI are different.

Editing User Information

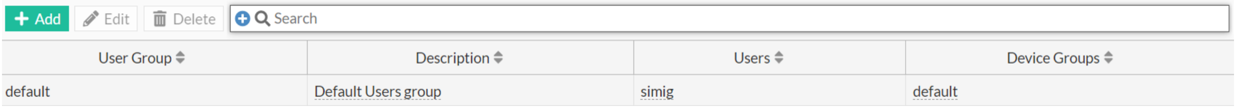
Select a user and click **Edit** to modify user information. This includes changing the user's full name, role or password.

Activating/Deactivating User

Select a user and click **Activate/Deactivate** to enable or disable the user's ability to log in or access the system. Deactivated user accounts can be reactivated at any time.

User Groups

The FortiAIOps access assigned to a user group determines what users in that user group can do.

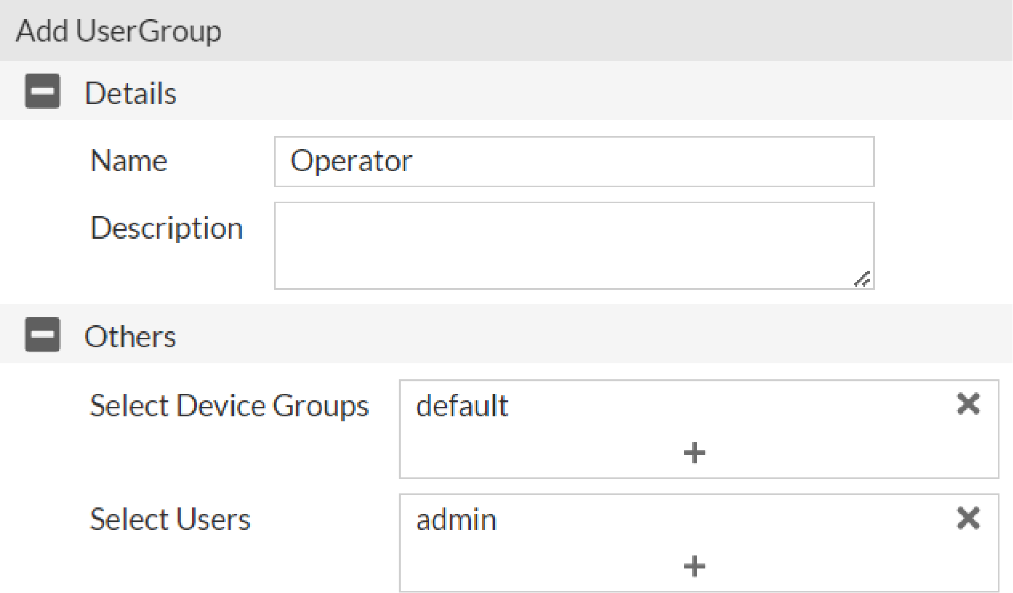


User Group	Description	Users	Device Groups
default	Default Users group	simig	default

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.**



Add UserGroup

Details

Name	Operator
Description	

Others

Select Device Groups	default
Select Users	admin

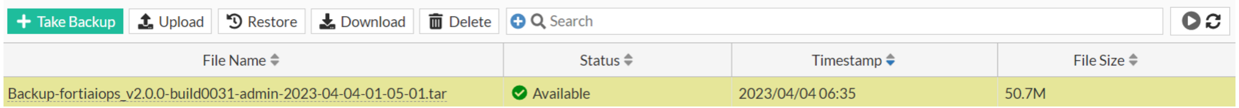
To edit an user group, select an existing user group from the list and click **Edit**.

To delete an user group, select the user group and click **Delete**.

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.



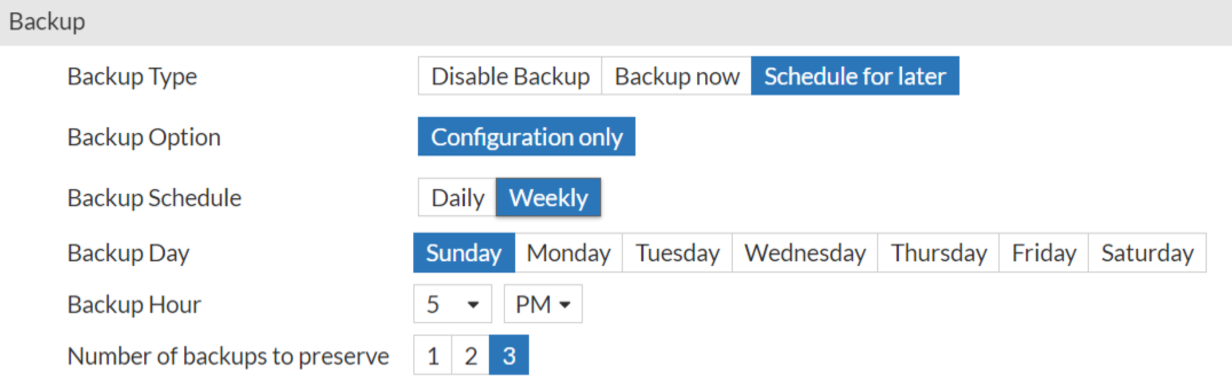
File Name	Status	Timestamp	File Size
Backup-fortiaiops_v2.0.0-build0031-admin-2023-04-04-01-05-01.tar	✓ Available	2023/04/04 06:35	50.7M

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.**



Backup

Backup Type: Disable Backup | Backup now | [✓ Schedule for later]

Backup Option: [✓ Configuration only]

Backup Schedule: Daily | [✓ Weekly]

Backup Day: [✓ Sunday] | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday

Backup Hour: 5 PM

Number of backups to preserve: 1 | 2 | [✓ 3]

Upload

To upload an existing backup file, perform the following steps:

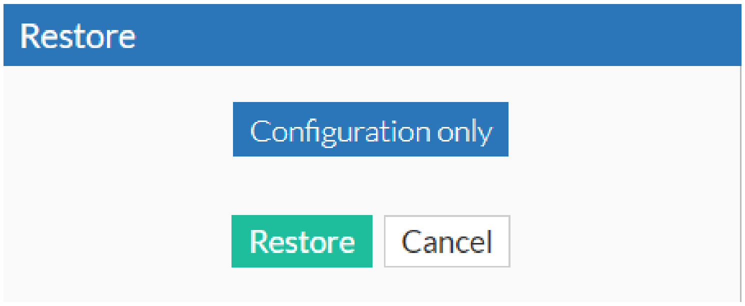
1. Navigate to **System** > **Backup and Restore**.
2. Click **Upload.**
3. Browse and select the backup file (.tar) file.
4. Click **Upload.**

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

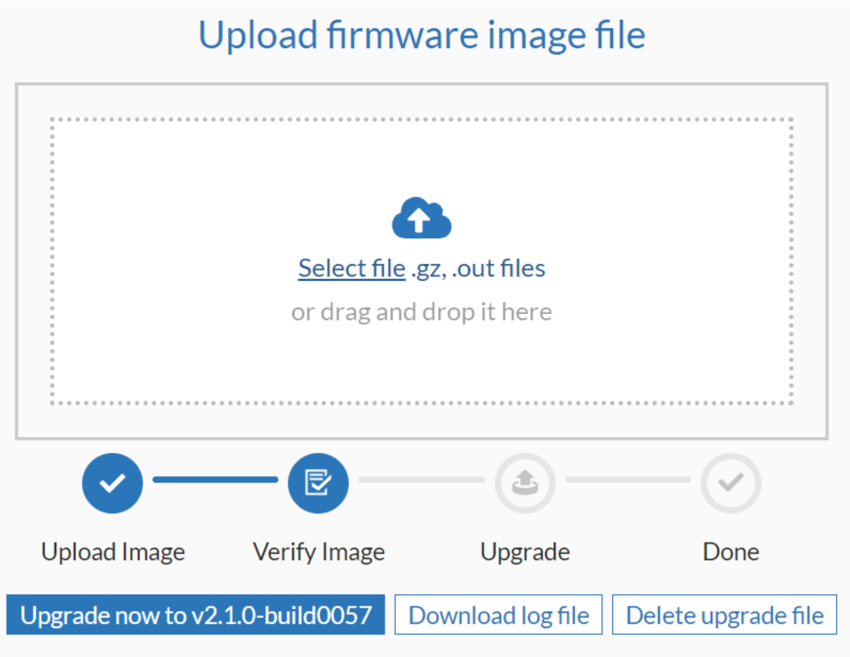
To download a backup file to your local machine, select the backup file from the list and click **Download.**

Delete

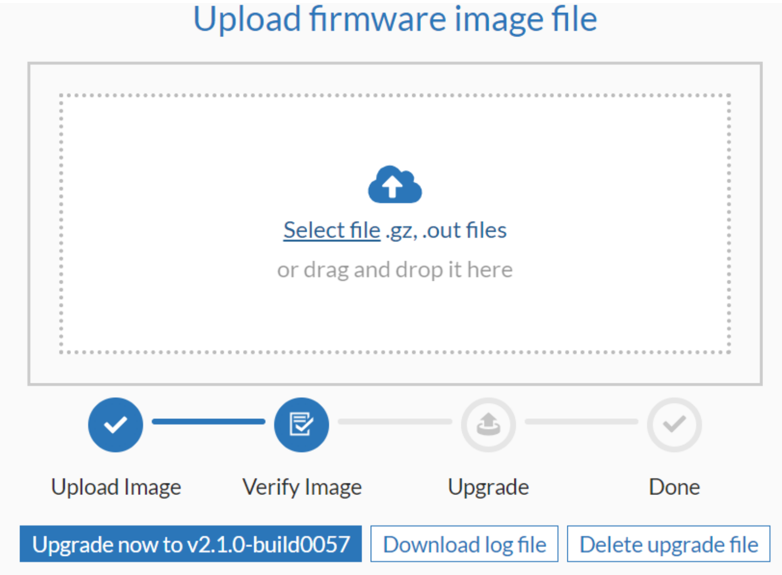
To delete a backup file, select the backup file from the list and click **Delete.**

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**.

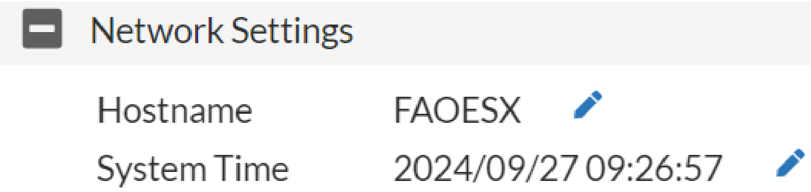
Settings

This page provides the following network and server maintenance parameters to be configured.

- Network Settings
- Statistics
- Administration Settings
- OUI Update
- General Logs
- Mail Server

Network Settings

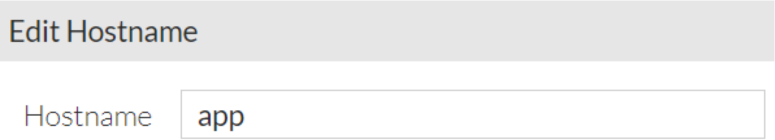
This section allows you to configure various system settings. Click ✎ icon to edit the system settings.



Hostname FAOESX

System Time 2024/09/27 09:26:57

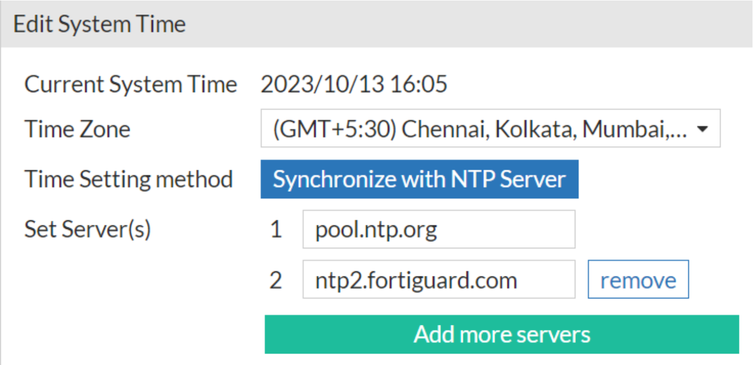
The **Hostname** displays the hostname of the system currently in use.



Edit Hostname

Hostname: app

The **System Time** displays the current system time. This setting allows you to select timezone, set time and configure NTP server.



Edit System Time

Current System Time: 2023/10/13 16:05

Time Zone: (GMT+5:30) Chennai, Kolkata, Mumbai,...

Time Setting method: Synchronize with NTP Server

Set Server(s):
1 pool.ntp.org
2 ntp2.fortiguard.com

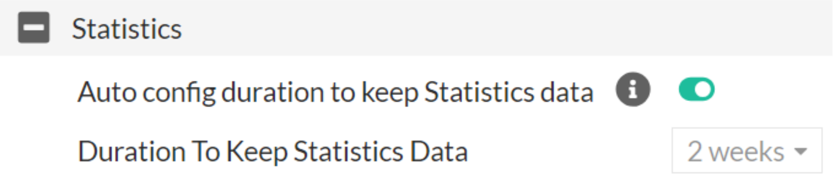
Notes:

- 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.



Statistics

Auto config duration to keep Statistics data: on

Duration To Keep Statistics Data: 2 weeks

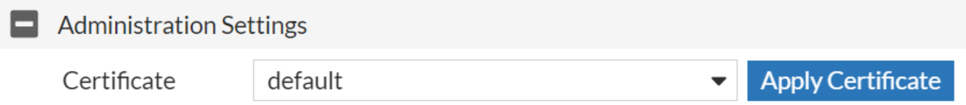
Notes:

- 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**.



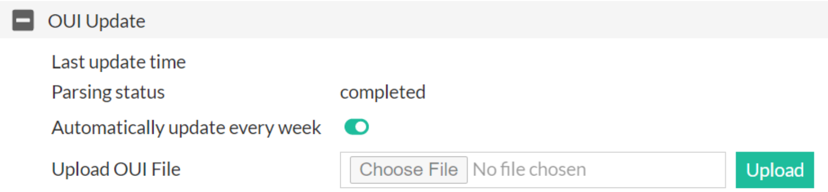
Administration Settings

Certificate: default

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**.



OUI Update

Last update time

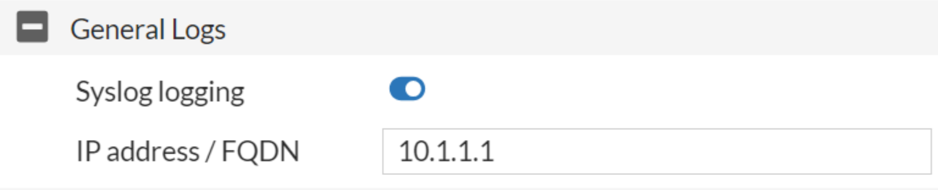
Parsing status: completed

Automatically update every week

Upload OUI File: No file chosen

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.



General Logs

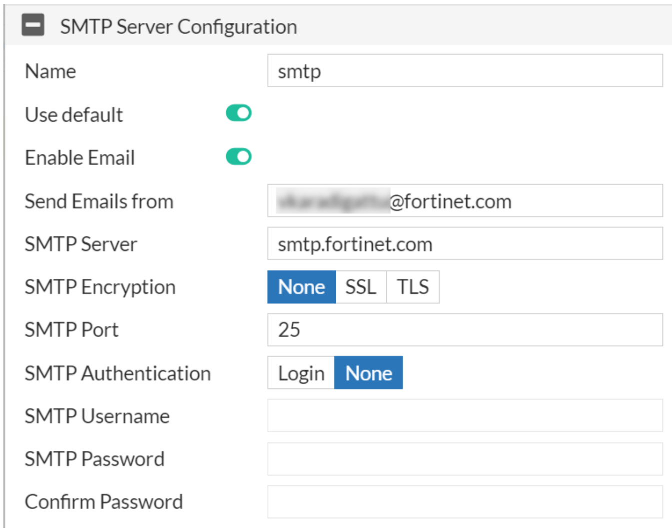
Syslog logging

IP address / FQDN: 10.1.1.1

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

Mail Server

You can configure the SMTP server to receive email notifications for report generation.



SMTP Server Configuration

Name	smtp
Use default	●
Enable Email	●
Send Emails from	[redacted]@fortinet.com
SMTP Server	smtp.fortinet.com
SMTP Encryption	[✓ None] SSL TLS
SMTP Port	25
SMTP Authentication	Login [✓ None]
SMTP Username	
SMTP Password	
Confirm Password	

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.

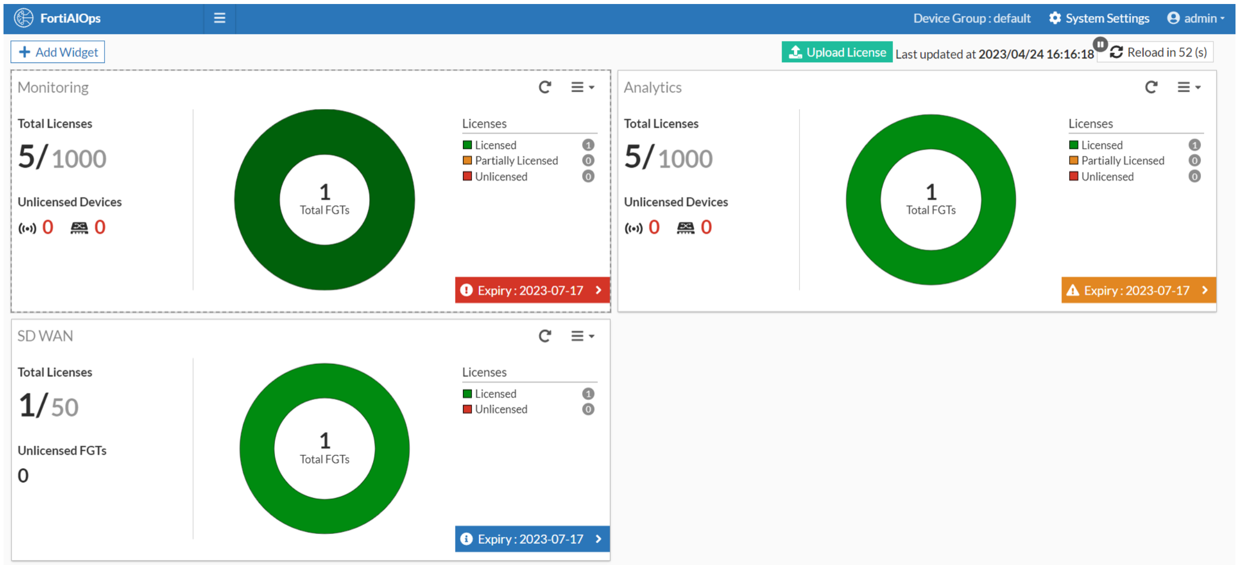
Licensing

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:

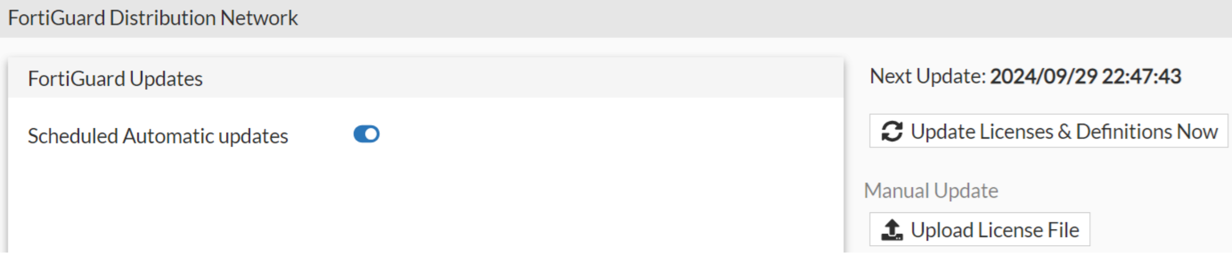
- If you buy additional licenses or extend the existing ones through FortiCare, the expiration date displayed will show the nearest expiry and will not include the newly added license. To see the accurate license details, please check FortiCare portal.
- To purchase a co-term license or add any required 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**.


FortiGuard Distribution Network

FortiGuard Updates

Scheduled Automatic updates ●

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

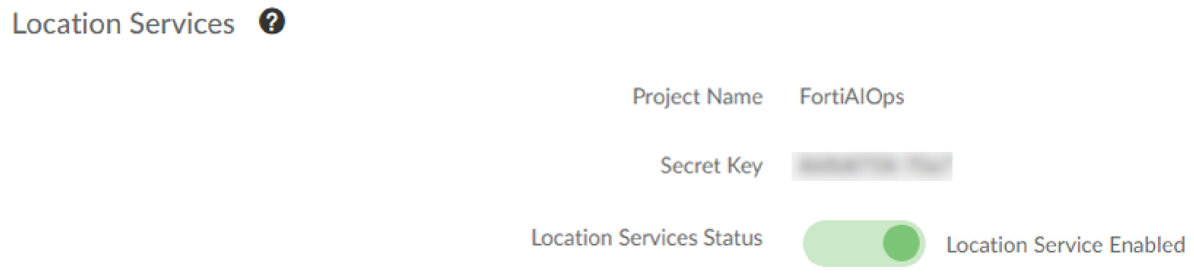
Location Services

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 the WIDS profile for the AP radio, follow these steps:

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.



Location Services

Project Name: FortiAIOps

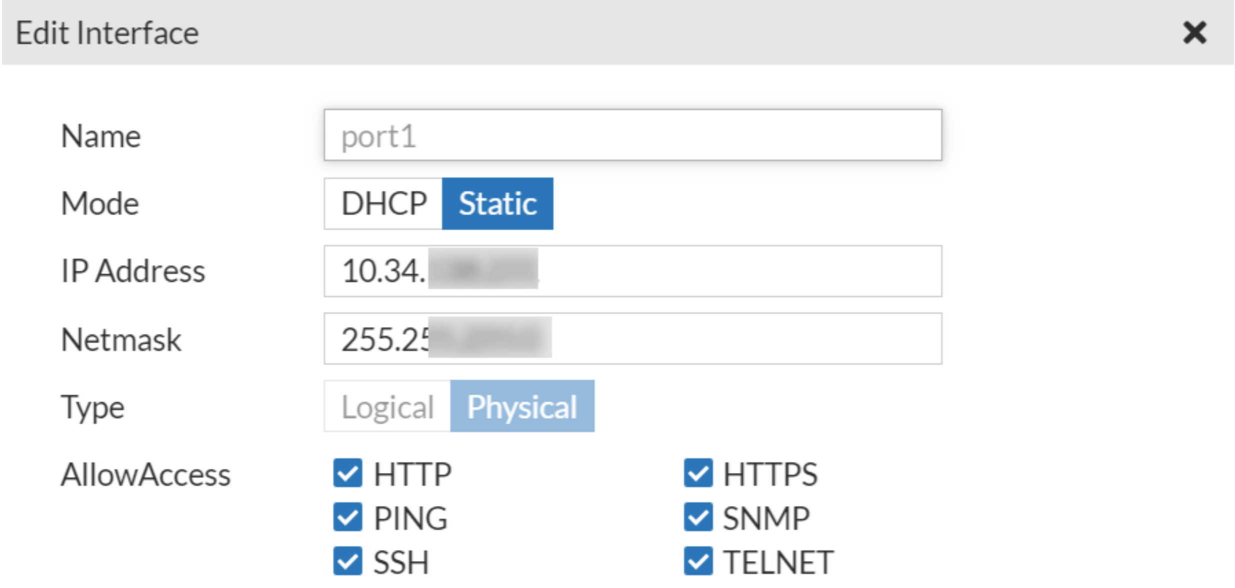
Secret Key: [redacted]

Location Services Status: Location Service Enabled

For information on the FortiGate configuration, see the Configuration Guide.

Network

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



Edit Interface

Name: port1

Mode: DHCP [✓ Static]

IP Address: 10.34.[redacted]

Netmask: 255.25[redacted]

Type: Logical [✓ Physical]

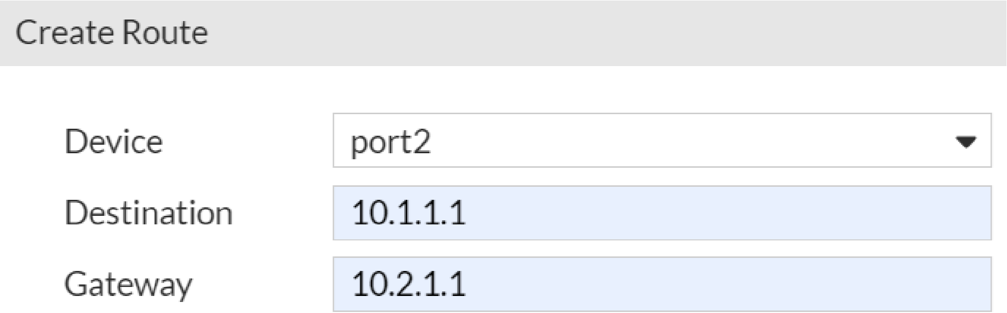
AllowAccess: ☑ HTTP ☑ HTTPS ☑ PING ☑ SNMP ☑ SSH ☑ TELNET

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

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

Click **Update**.

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

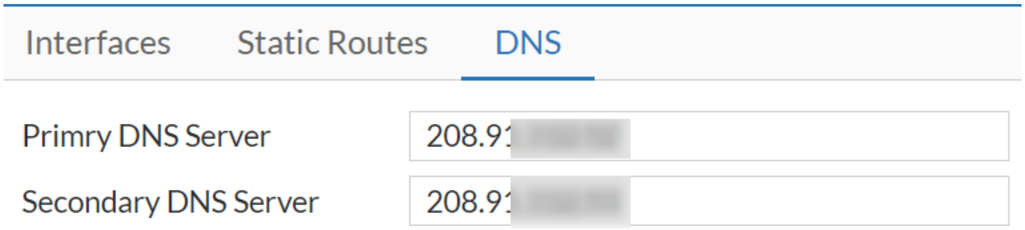


Create Route

Device	port2
Destination	10.1.1.1
Gateway	10.2.1.1

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

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



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

Certificates

The Certificates page allows you to manage both local and CA certificates. Certificates provide security assurance validated by a Certificate Authority (CA).

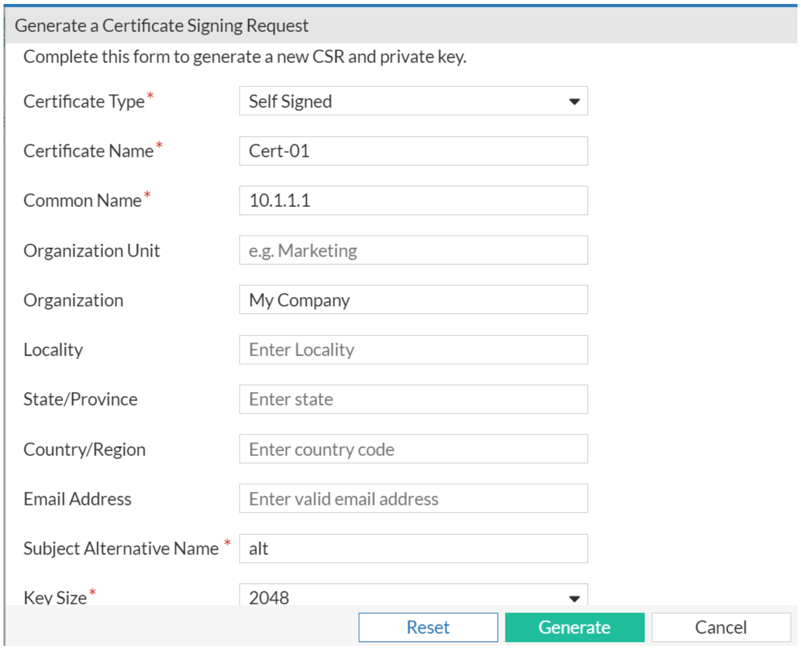
- Local Certificates
- CA Certificates

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**.



Generate a Certificate Signing Request

Complete this form to generate a new CSR and private key.

Certificate Type*	Self Signed
Certificate Name*	Cert-01
Common Name*	10.1.1.1
Organization Unit	e.g. Marketing
Organization	My Company
Locality	Enter Locality
State/Province	Enter state
Country/Region	Enter country code
Email Address	Enter valid email address
Subject Alternative Name *	alt
Key Size*	2048

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.

Service Assurance

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
- Results
- Baseline
- Schedule

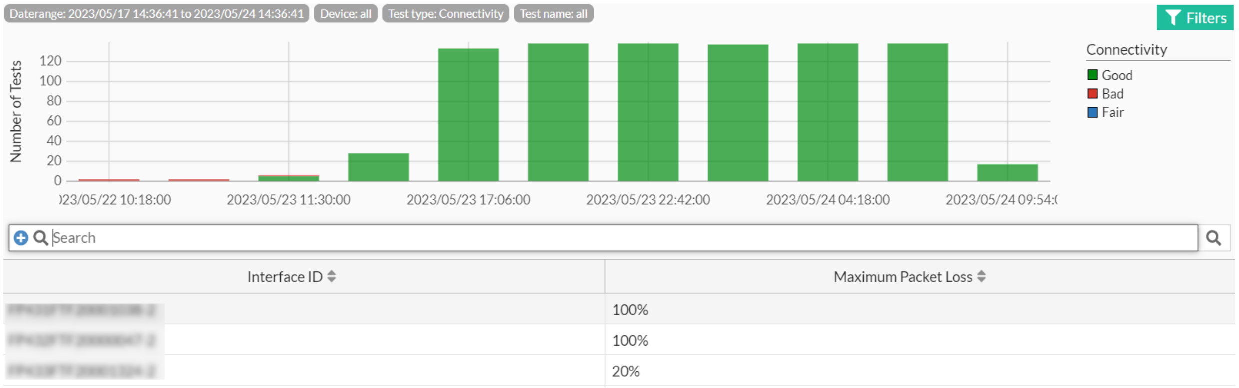
Trends

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.

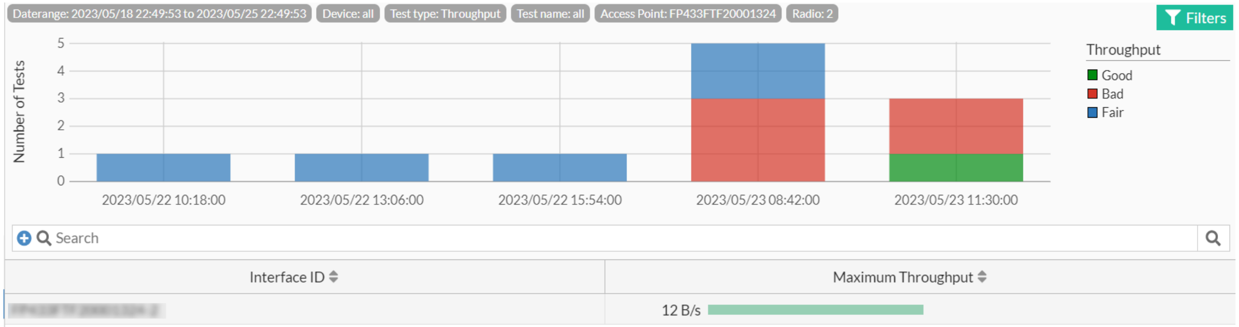
If the **connectivity** test type is selected, the Trends page presents a table with the *Interface ID* and the *Maximum Packet Loss* for each interface.



Daterange: 2023/05/17 14:36:41 to 2023/05/24 14:36:41 | Device: all | Test type: Connectivity | Test name: all

Interface ID	Maximum Packet Loss
[redacted]	100%
[redacted]	100%
[redacted]	20%

If the **throughput** test type is selected, the Trends page displays a table with the *Interface ID* and the *Maximum Throughput* for each interface.



Daterange: 2023/05/18 22:49:53 to 2023/05/25 22:49:53 | Device: all | Test type: Throughput | Test name: all | Access Point: FP433FTF20001324 | Radio: 2

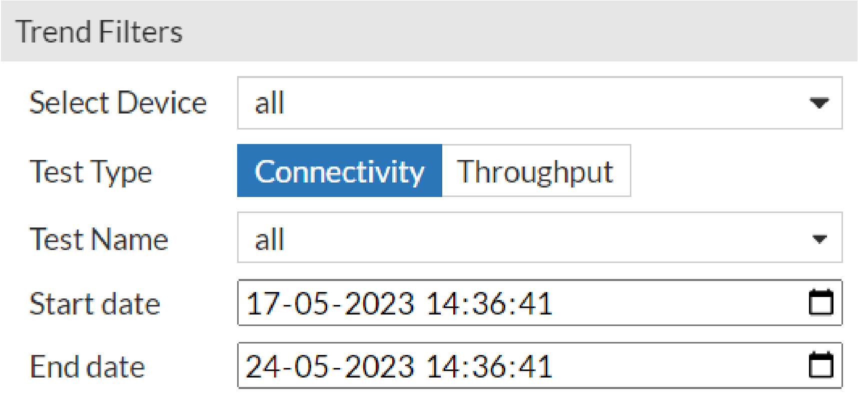
Interface ID	Maximum Throughput
[redacted]	12 B/s

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.



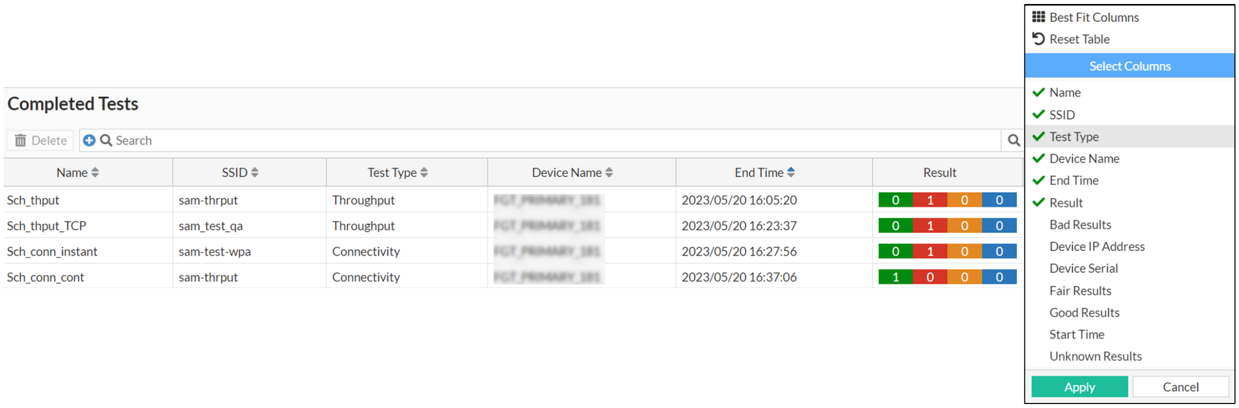
Trend Filters

Select Device	all
Test Type	Connectivity (selected) / Throughput
Test Name	all
Start date	17-05-2023 14:36:41
End date	24-05-2023 14:36:41

Results

Results page provides a comprehensive overview of the Connectivity/ Throughput test results, including completed tests and tests in progress.

Completed Tests



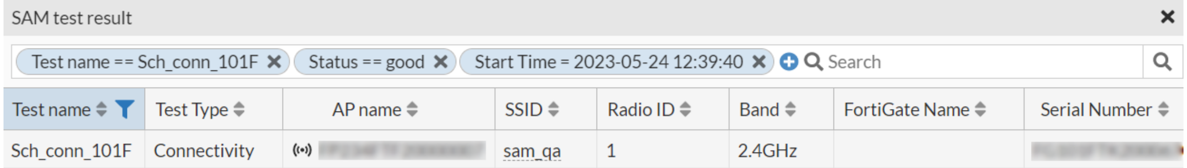
Completed Tests

Name	SSID	Test Type	Device Name	End Time	Result
Sch_thput	sam-thrput	Throughput	[redacted]	2023/05/20 16:05:20	0 1 0 0
Sch_thput_TCP	sam_test_qa	Throughput	[redacted]	2023/05/20 16:23:37	0 1 0 0
Sch_conn_instant	sam-test-wpa	Connectivity	[redacted]	2023/05/20 16:27:56	0 1 0 0
Sch_conn_cont	sam-thrput	Connectivity	[redacted]	2023/05/20 16:37:06	1 0 0 0

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.



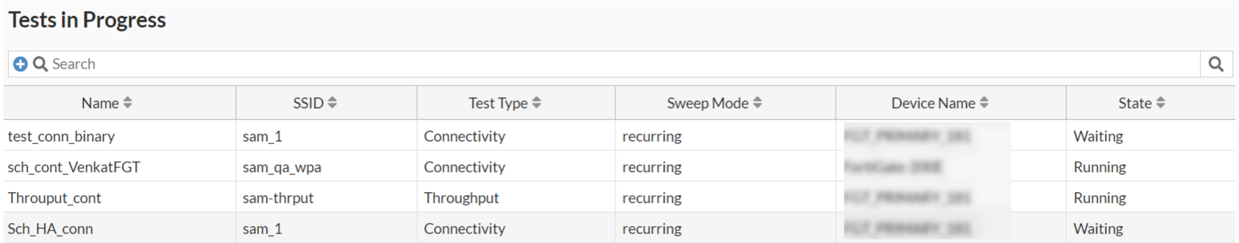
SAM test result

Test name == Sch_conn_101F ✖ Status == good ✖ Start Time = 2023-05-24 12:39:40 ✖ Search

Test name	Test Type	AP name	SSID	Radio ID	Band	FortiGate Name	Serial Number
Sch_conn_101F	Connectivity	[redacted]	sam_qa	1	2.4GHz		[redacted]

- **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



Tests in Progress

Search

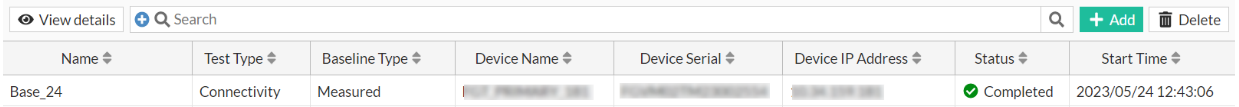
Name	SSID	Test Type	Sweep Mode	Device Name	State
test_conn_binary	sam_1	Connectivity	recurring	[redacted]	Waiting
sch_cont_VenkatFGT	sam_qa_wpa	Connectivity	recurring	[redacted]	Running
Throuput_cont	sam-thrput	Throughput	recurring	[redacted]	Running
Sch_HA_conn	sam_1	Connectivity	recurring	[redacted]	Waiting

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

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.



Name	Test Type	Baseline Type	Device Name	Device Serial	Device IP Address	Status	Start Time
Base_24	Connectivity	Measured	[redacted]	[redacted]	[redacted]	✓ Completed	2023/05/24 12:43:06

Add a Baseline

You have two options to execute the baseline tests.

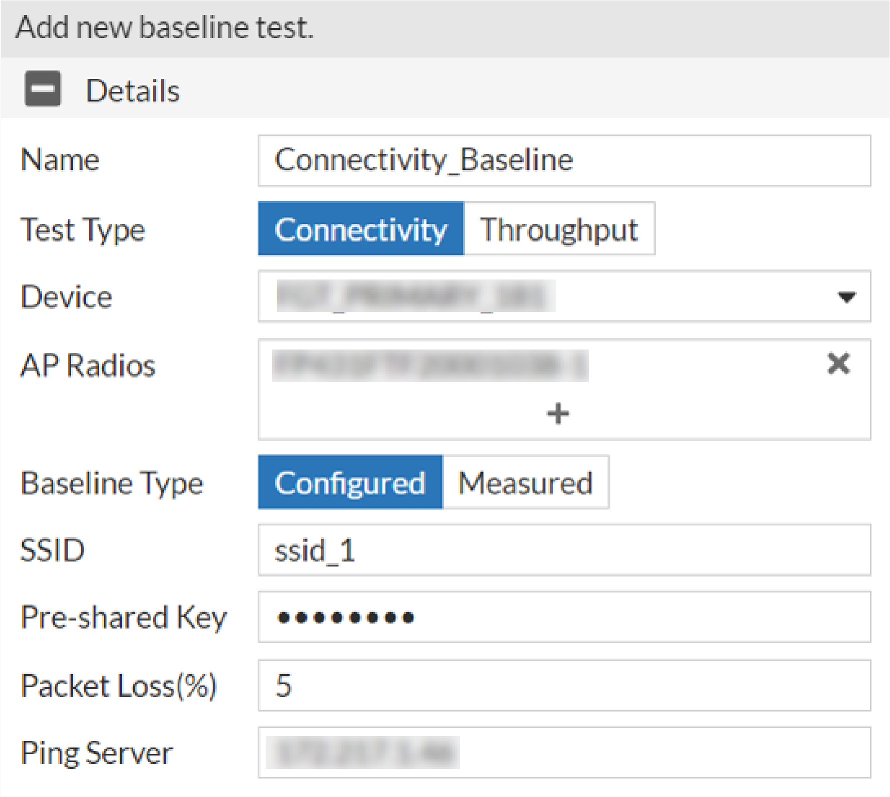
- **Configured Test**: This option allows you to create a baseline test by providing theoretical values.
- **Measured Test**: This option allows you to create a baseline test by providing the actual baseline values. It is important to run a measured baseline when the wireless network is operating either normally or under optimal conditions, as it is used to evaluate subsequent tests.

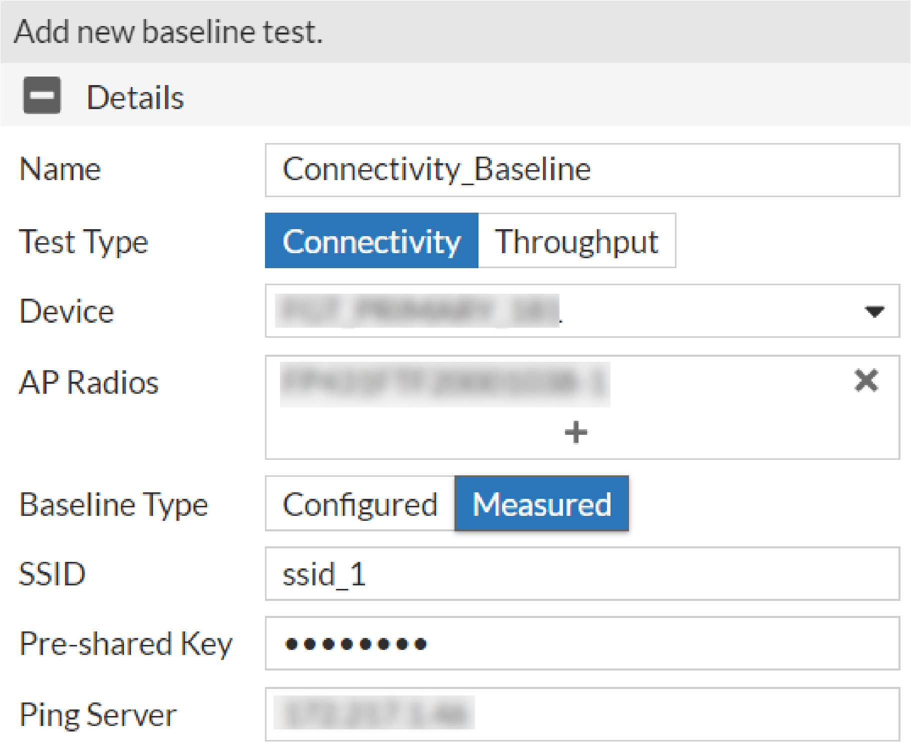
Connectivity Baseline

To create a connectivity baseline, perform the following steps:

1. Navigate to **Service Assurance>Baseline.**
2. Click **+ Add.**

3. Provide the following details:

Field	Description
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 1.	Enter the pre-shared key for the SSID.
Packet Loss(%) 1. 2.	Enter packet loss value in %. **Note**: Packet Loss(%) field is displayed only when **Configured** is selected as baseline type.  Add new baseline test. Details Name: Connectivity_Baseline Test Type: Connectivity (selected) / Throughput Device: [redacted] AP Radios: [redacted] Baseline Type: Configured (selected) / Measured SSID: ssid_1 Pre-shared Key: ●●●●●●●●● Packet Loss(%): 5 Ping Server: [redacted]
Ping Server	Enter **IP address** or **FQDN** of the ping server to perform connectivity tests.



Add new baseline test.

Details

Name	Connectivity_Baseline
Test Type	Connectivity (selected) / Throughput
Device	[redacted]
AP Radios	[redacted]
Baseline Type	Configured / Measured (selected)
SSID	ssid_1
Pre-shared Key	●●●●●●●●
Ping Server	[redacted]

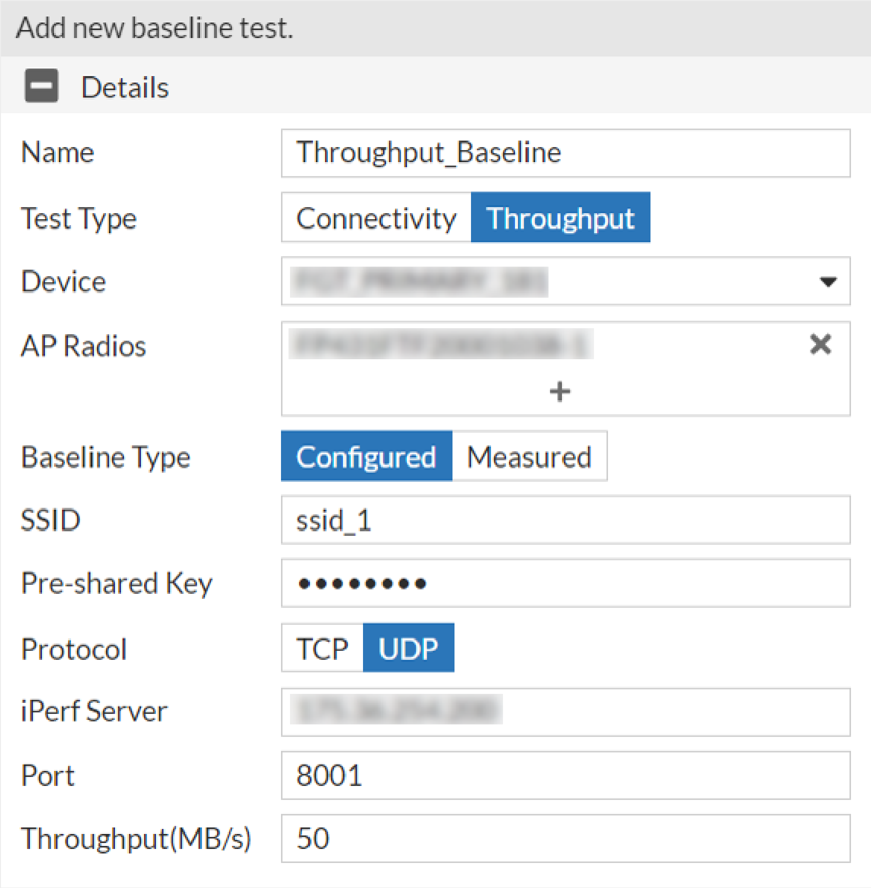
4. Click **Add.**

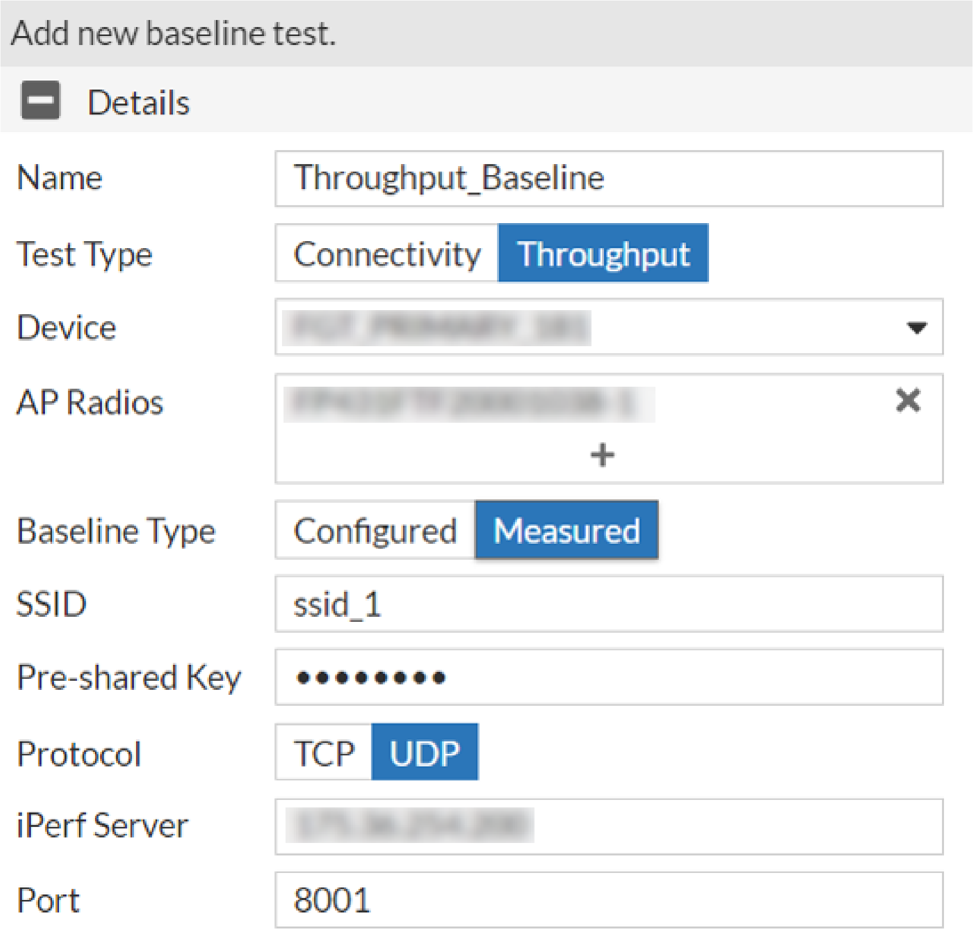
Throughput Baseline

To create a throughput baseline, perform the following steps:

1. Navigate to **Service Assurance>Baseline.**
2. Click **+ Add.**
3. Provide the following details:

Field	Description
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	1. Enter the pre-shared key for the SSID.
Protocol	Select the protocol, **TCP** or **UDP**.

Field	Description
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)	1. Enter throughput value in MB/s. **Note**: Throughput(MB/s) field is displayed only when **Configured** is selected as baseline type. 2.  Add new baseline test. Details Name: Throughput_Baseline Test Type: Connectivity [✓ Throughput] Device: [redacted] AP Radios: [redacted] Baseline Type: [✓ Configured] Measured SSID: ssid_1 Pre-shared Key: •••••••• Protocol: TCP [✓ UDP] iPerf Server: [redacted] Port: 8001 Throughput(MB/s): 50



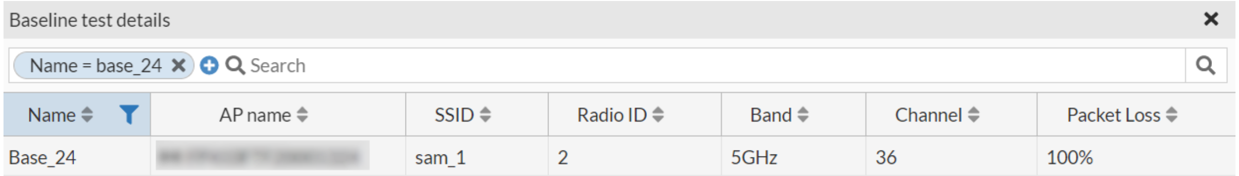
Add new baseline test.

Details

Name	Throughput_Baseline
Test Type	Connectivity [✓ Throughput]
Device	[redacted]
AP Radios	[redacted]
Baseline Type	Configured [✓ Measured]
SSID	ssid_1
Pre-shared Key	•••••••••
Protocol	TCP [✓ UDP]
iPerf Server	[redacted]
Port	8001

4. Click **Add.**

To view the detailed information of a baseline, navigate to *Service Assurance* > *Baseline*, select the desired baseline from the list and click View Details.



Baseline test details

Name = base_24

Name	AP name	SSID	Radio ID	Band	Channel	Packet Loss
Base_24	[redacted]	sam_1	2	5GHz	36	100%

To delete a baseline, navigate to *Service Assurance* > *Baseline*, select the desired baseline from the list and click Delete.

Schedule

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.

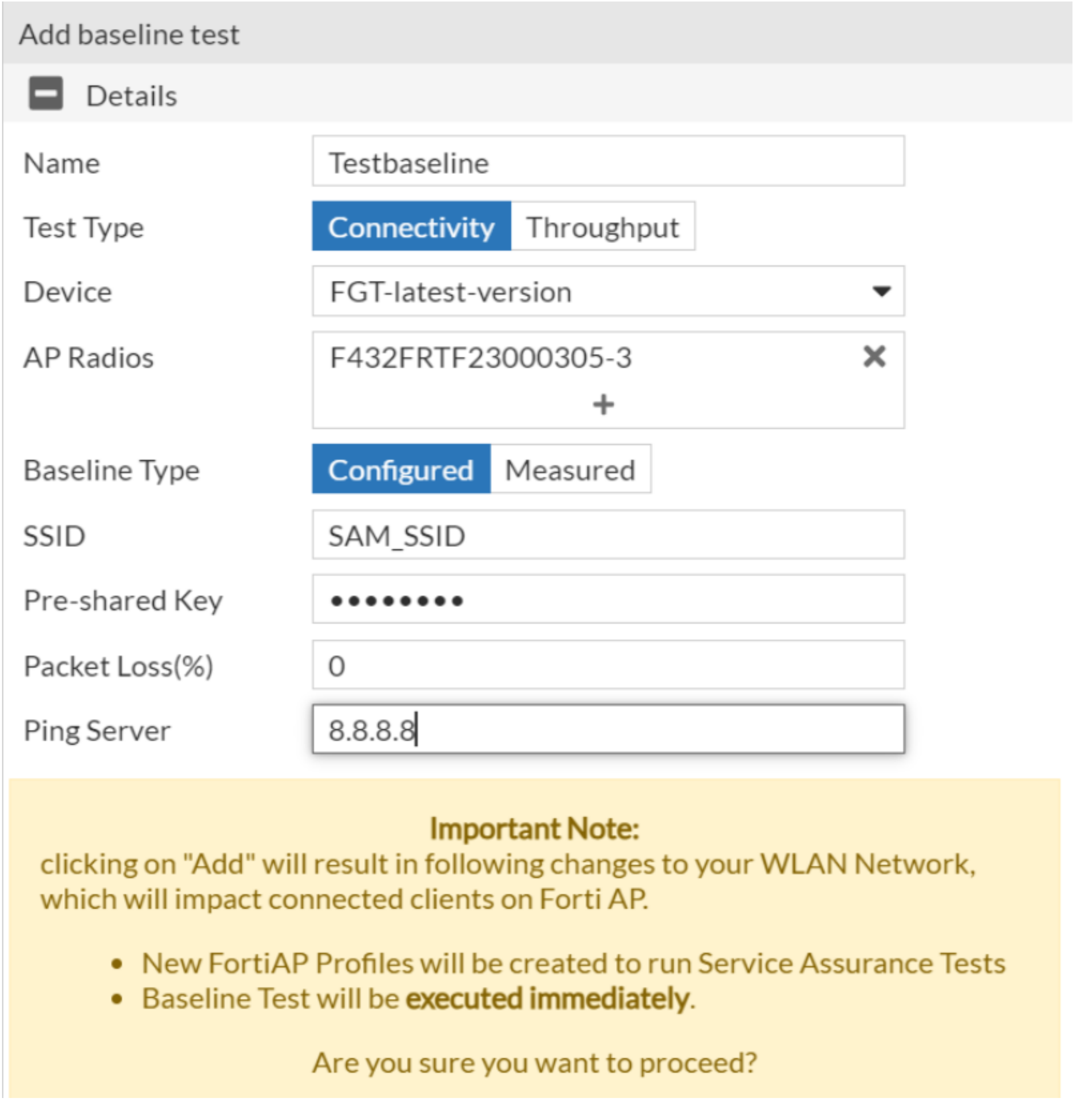
Scheduled tests are measured against a baseline test for Connectivity and Throughput using the configurations provided while creating the test. Only APs and SSIDs within the baseline test is measured in subsequent tests.

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*.



Add baseline test

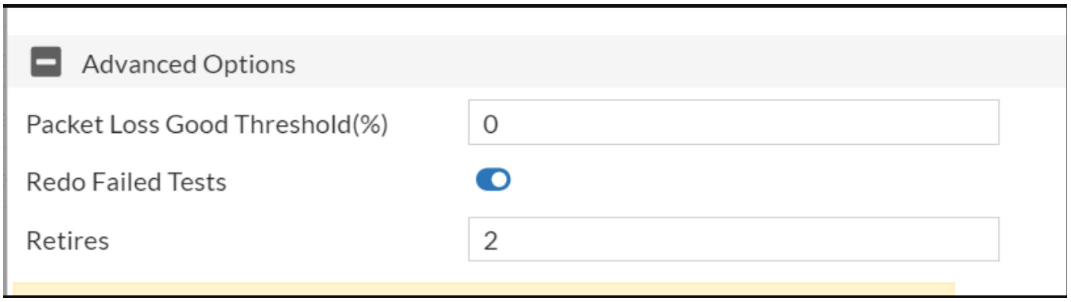
Details

Name	Testbaseline
Test Type	Connectivity (selected) | Throughput
Device	FGT-latest-version
AP Radios	F432FRTF23000305-3
Baseline Type	Configured (selected) | Measured
SSID	SAM_SSID
Pre-shared Key	●●●●●●●●●
Packet Loss(%)	0
Ping Server	8.8.8.8

Important Note:
clicking on "Add" will result in following changes to your WLAN Network, which will impact connected clients on Forti AP.

- New FortiAP Profiles will be created to run Service Assurance Tests
- Baseline Test will be **executed immediately**.

Are you sure you want to proceed?



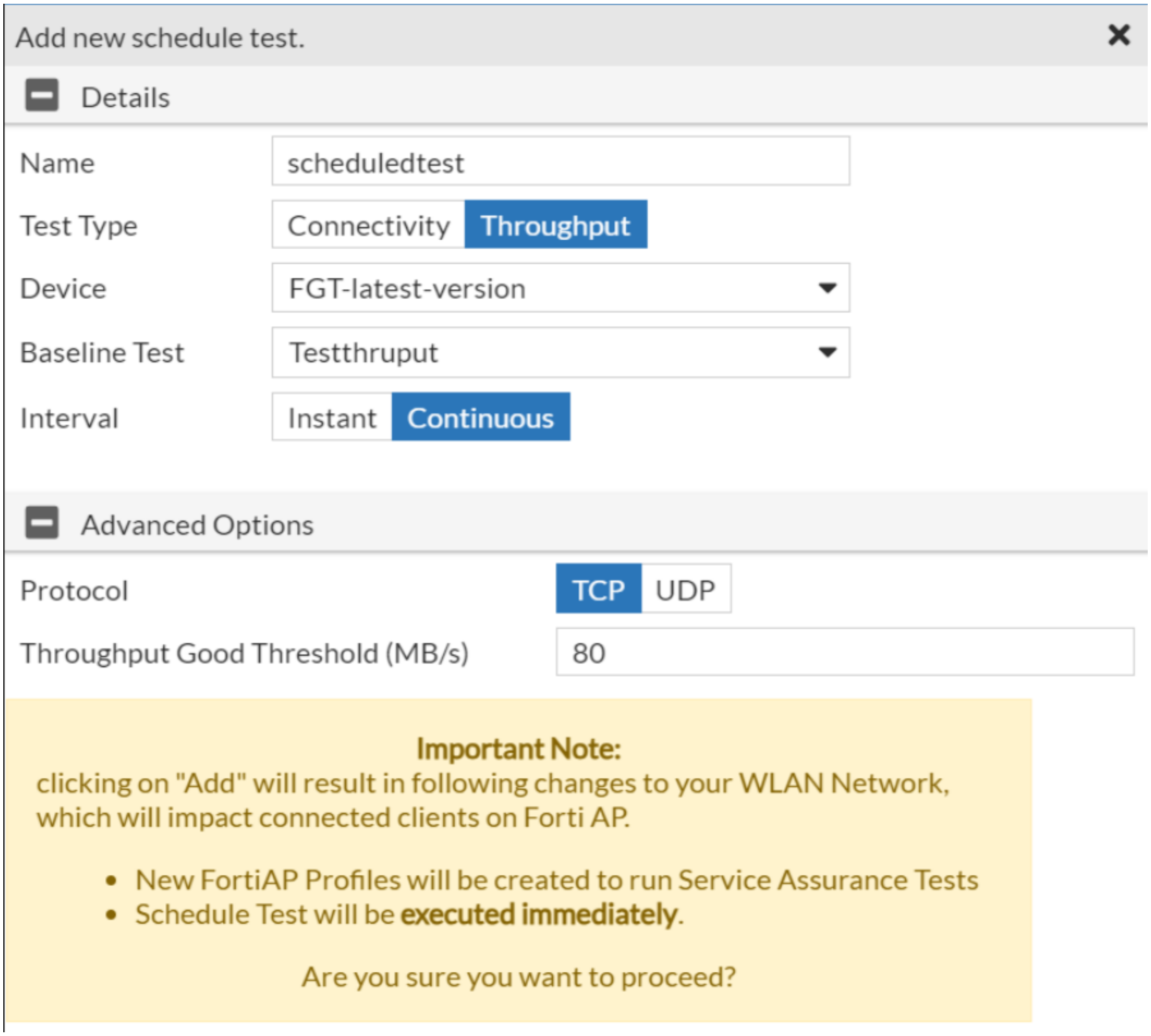
Advanced Options

Packet Loss Good Threshold(%)	0
Redo Failed Tests	●
Retires	2

- If Throughput is selected as Test Type , you can configure the following fields:

Field	Description
Protocol	Select TCP or UDP.

Field	Description
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*.



Add new schedule test.

Details

Name	scheduledtest
Test Type	Connectivity [✓ Throughput]
Device	FGT-latest-version
Baseline Test	Testthruput
Interval	Instant [✓ Continuous]

Advanced Options

Protocol	[✓ TCP] UDP
Throughput Good Threshold (MB/s)	80

Important Note:

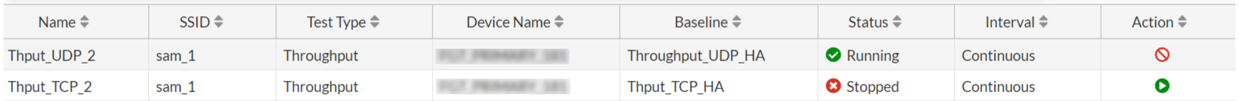
clicking on "Add" will result in following changes to your WLAN Network, which will impact connected clients on Forti AP.

- New FortiAP Profiles will be created to run Service Assurance Tests
- Schedule Test will be **executed immediately**.

Are you sure you want to proceed?

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