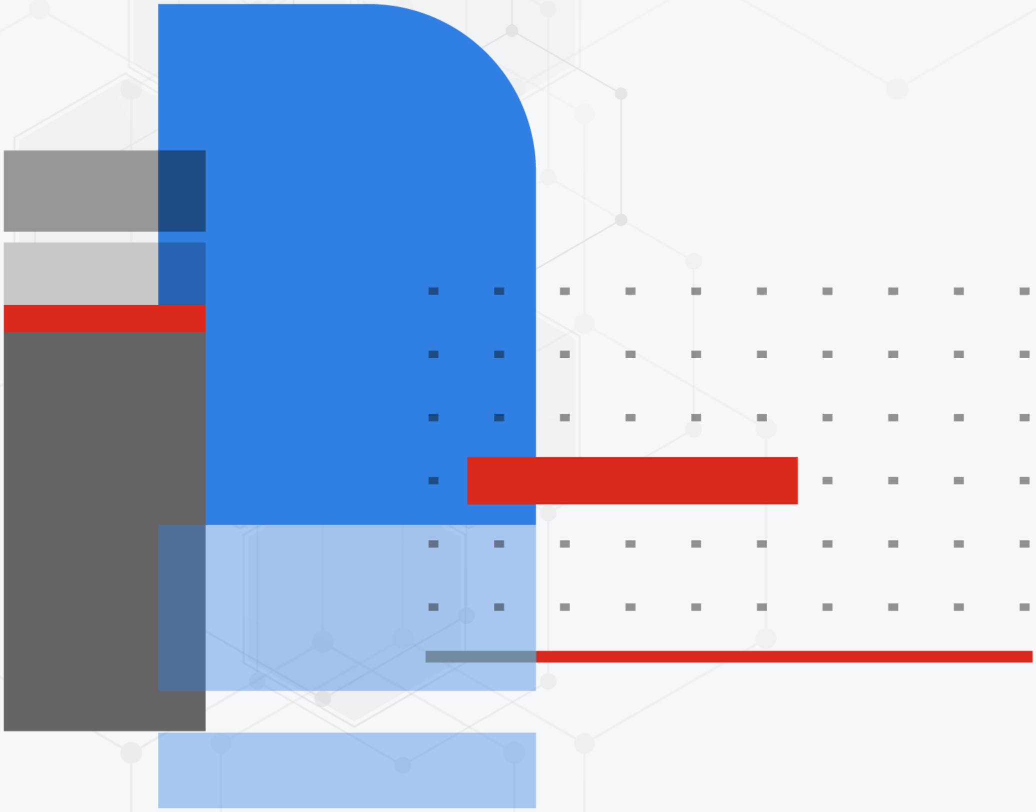
User Guide

FortiAIOps 2.0.0



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

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

October 04, 2024
FortiAIOps 2.0.0 User Guide
83-200-900211-20241004

TABLE OF CONTENTS

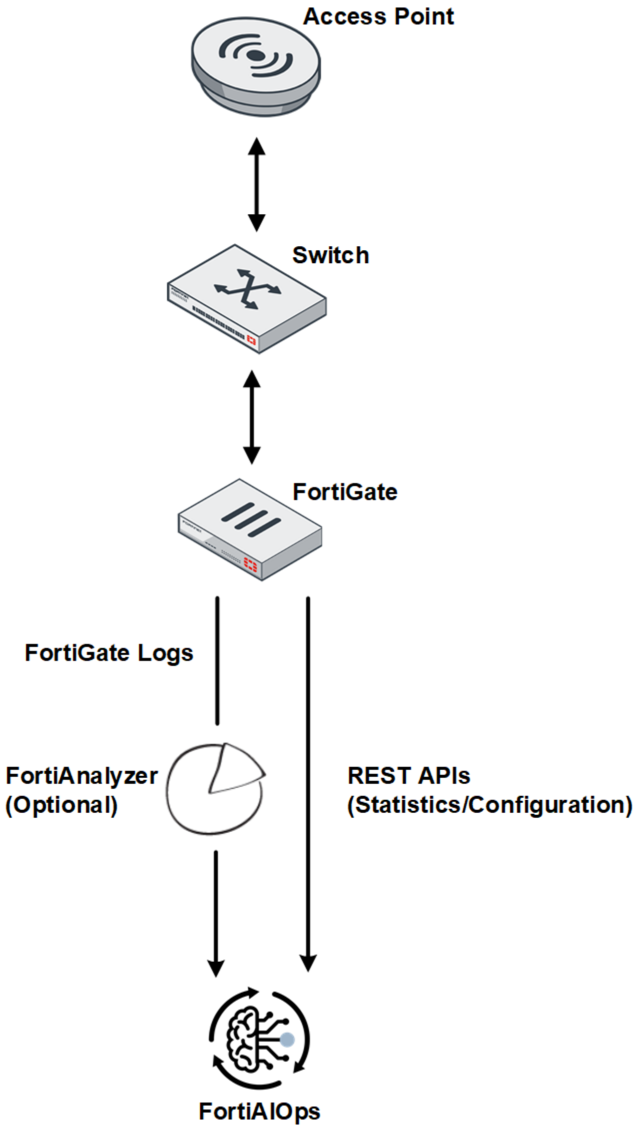
Change log

Date	Change description
2023-11-16	FortiAIOps 2.0.0 document.
2023-12-19	Updated screen shots in Installing FortiAIOps on Hyper-V.
2024-10-04	Updated Installing FortiAIOps.

Overview

FortiAIOps enables you to view and monitor the status 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 learns from your network data to report statistics on a series of comprehensive and simple dashboards, providing visibility and deep insight into your network. Thus, enabling you to effectively manage your connected devices and resolve network issues swiftly.

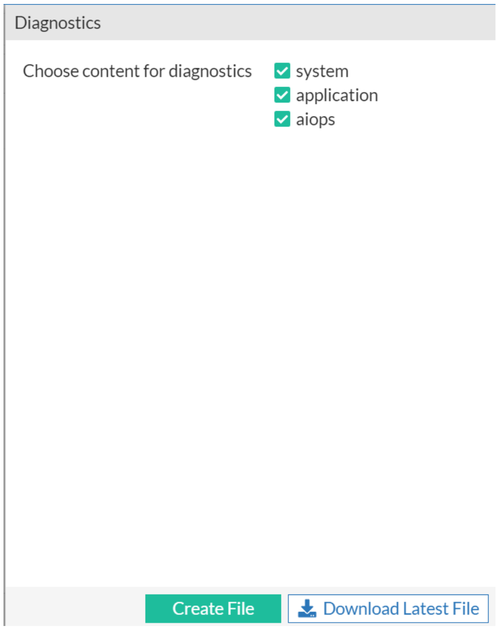
FortiAIOps monitors integrated wireless, wired, and SD-WAN networks by supporting the monitoring of FortiGate controllers. You can monitor and manage FortiGate controllers concurrently associated with FortiAPs and stations in a large deployments. The centralized real-time data and event logs offered 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.

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
☑ application
☑ aiops

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 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.

- Switch Health and Uptime
- Switch Connection Failure

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 port *down*, switch *down* and so on. FortiAIOps displays relevant SLAs under different sections on the monitor dashboard.

Switch Connection Failure

The **Switch Connection Failure** determines the failed/unsuccessful client connections based on authentication events such as MAC authentication and 801x authentication and MAC learning limit.

WAN

WAN is a software-defined approach to 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. Alternately, you can configure thresholds for these link quality parameters (latency, jitter and packet loss) in FortiAIOps for SLA monitoring. The thresholds can be configured statically or dynamically by FortiAIOps using machine learning algorithms, to identify optimal threshold values for the link parameters.

FortiExtender

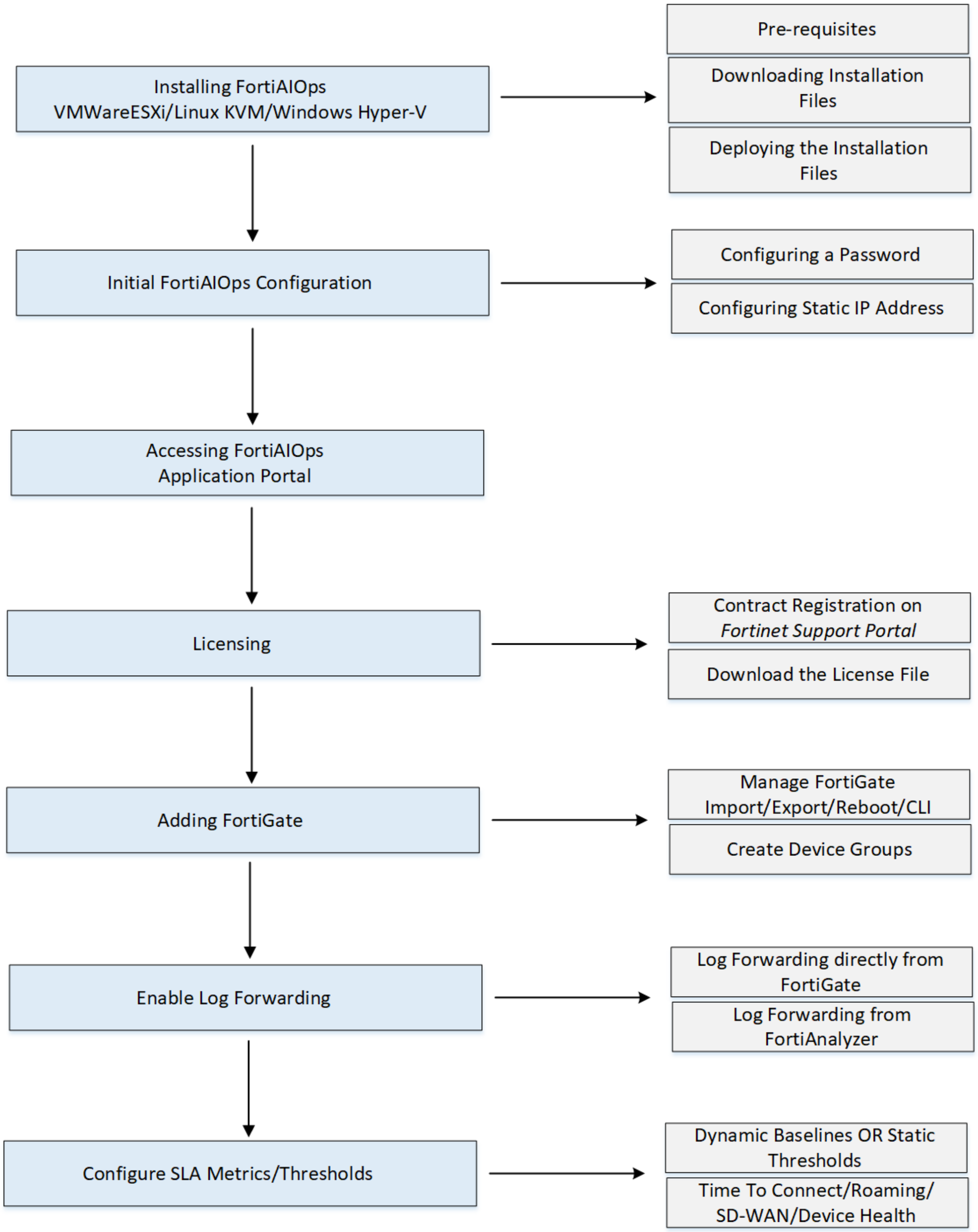
FortiExtender integrates with FortiGate and WAN to become a part of Fortinet's security fabric. This integration enables FortiGate’s WAN to have an extension using FortiExtender, providing continuous connectivity in case FortiGate's primary WAN link fails. Also, FortiExtender enables network access for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


Installing FortiAIOps
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 on page 11
- Initial FortiAIOps Configuration on page 11
- Accessing FortiAIOps on page 29
- Licensing
- Adding FortiGate on page 13
- Enable Log Forwarding on page 13
- Configure SLA Metrics
- Monitoring

Installing FortiAIOps

To deploy FortiAIOps in your network, download and install the virtual image files. The FortiAIOps application is supported in the *VMWare ESXi*, *Linux KVM*, and *Windows Hyper-V* environments.

- Prior to starting the installation process, ensure that the requisite hardware and software requirements are met. See Pre-installation Requirements.
- Download the installation files as per your deployment requirements from the *Fortinet Support Portal*.
- Deploy the downloaded installation files.
  - Installing FortiAIOps on VMware ESXi
  - Installing FortiAIOps on Hyper-V
  - Installing FortiAIOps on KVM

  For detailed instructions on deploying and administering the FortiAIOps, see Deploying FortiAIOps

Note: The FortiAIOps CLI and GUI users are different.

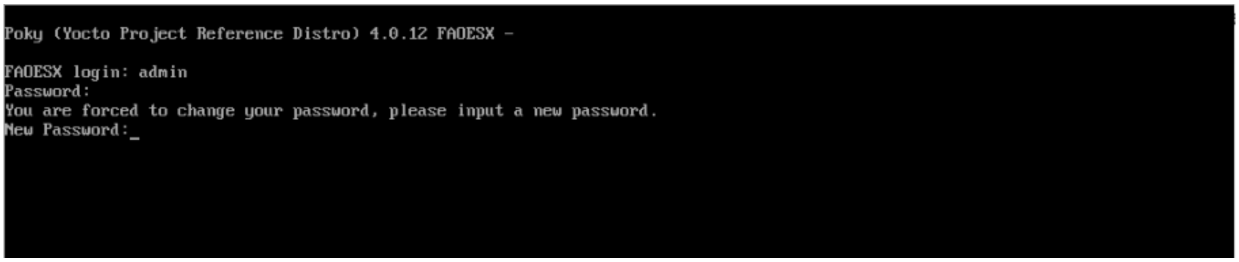
Initial FortiAIOps Configuration

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 requires a perpetual license. Follow the steps below to obtain the license.

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 > Licensing > Upload License**.

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

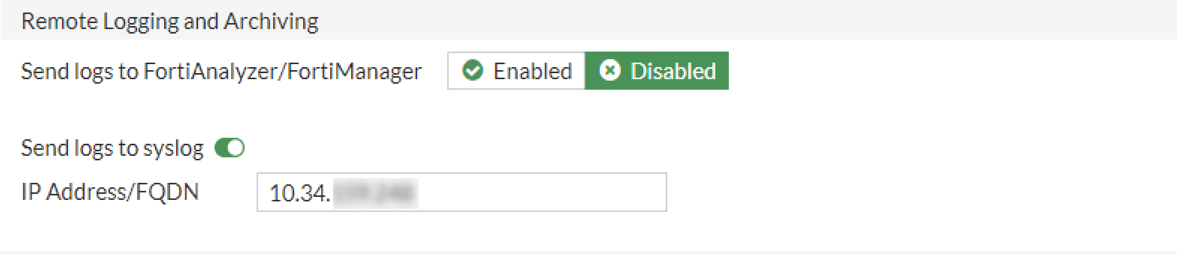
In the FortiAIOps application portal, manually add the FortiGate controller. Navigate to **Inventory > Managed FortiGates > Add** and provide the required configuration details. Standalone and HA FortiGate controllers can be added. Optionally, you can add FortiGates in bulk using the import operation.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



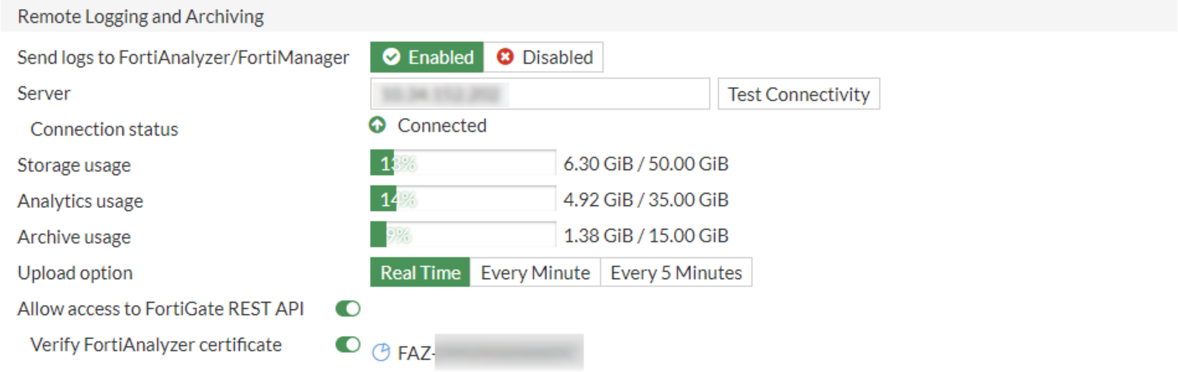
Remote Logging and Archiving

Send logs to FortiAnalyzer/FortiManager ✓ Enabled [✓ ☒ Disabled]

Send logs to syslog ●

IP Address/FQDN 10.34.[redacted]

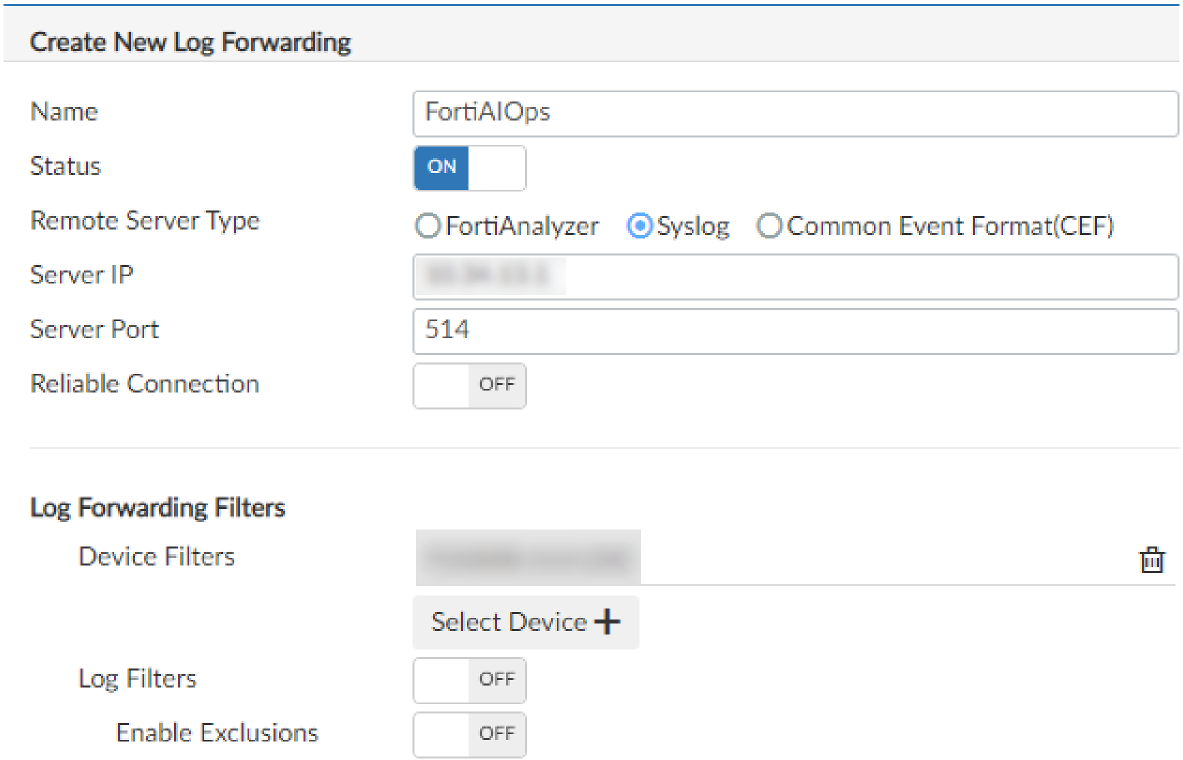
- FortiAnalyzer log forwarding - Navigate to **Log Settings** in the FortiGate GUI and enable FortiAnalyzer log forwarding.



Remote Logging and Archiving

Send logs to FortiAnalyzer/FortiManager	✓ Enabled ☒ Disabled
Server	[redacted] Test Connectivity
Connection status	Connected
Storage usage	13% 6.30 GiB / 50.00 GiB
Analytics usage	14% 4.92 GiB / 35.00 GiB
Archive usage	9% 1.38 GiB / 15.00 GiB
Upload option	Real Time · Every Minute · Every 5 Minutes
Allow access to FortiGate REST API	●
Verify FortiAnalyzer certificate	● FAZ-[redacted]

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.
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.

Deploying FortiAIOps

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.
   a. Installing FortiAIOps on VMware ESXi
   b. Installing FortiAIOps on Hyper-V
   c. Installing FortiAIOps on KVM
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.

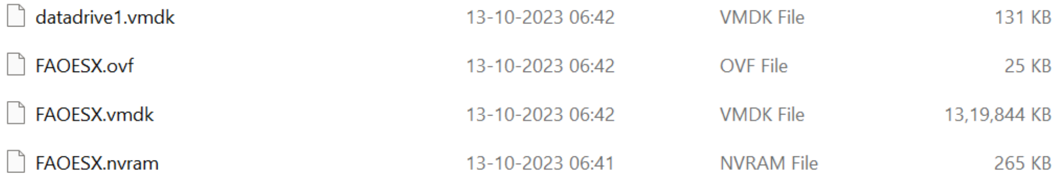
CPU	Memory	Storage	
		Disk 1	Disk 2
4	32 GB	8 GB	500 GB

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

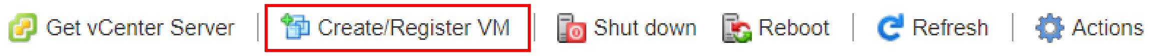
Perform the following steps to deploy FortiAIOps.

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.

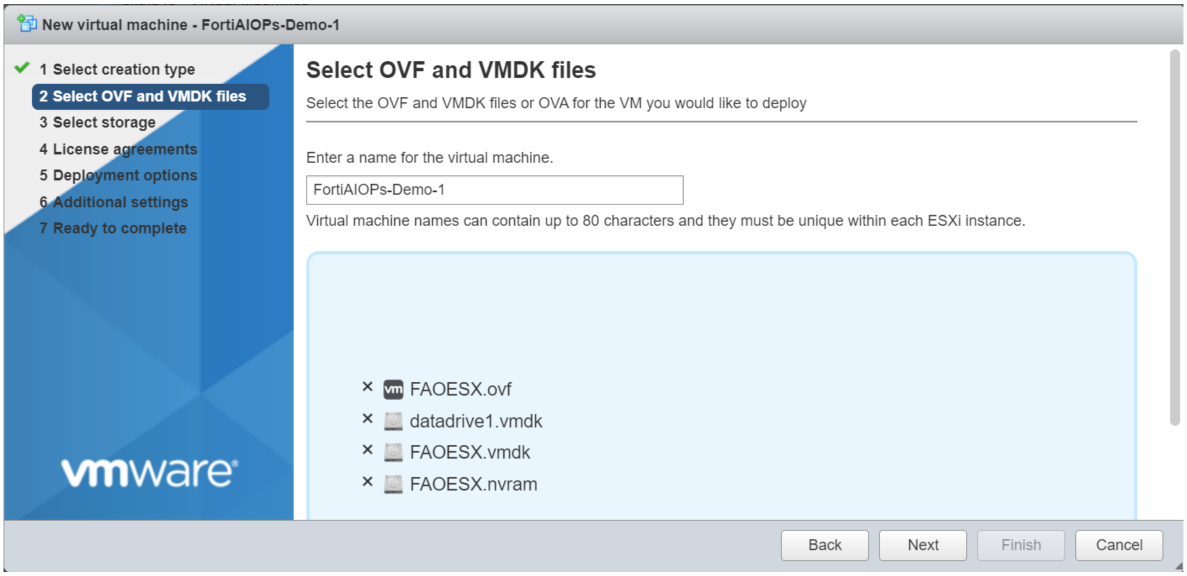


datadrive1.vmdk	13-10-2023 06:42	VMDK File	131 KB
FAOESX.ovf	13-10-2023 06:42	OVF File	25 KB
FAOESX.vmdk	13-10-2023 06:42	VMDK File	13,19,844 KB
FAOESX.nvram	13-10-2023 06:41	NVRAM File	265 KB

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.



New virtual machine - FortiAIOPs-Demo-1

✓ 1 Select creation type
2 Select OVF and VMDK files
3 Select storage
4 License agreements
5 Deployment options
6 Additional settings
7 Ready to complete

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.

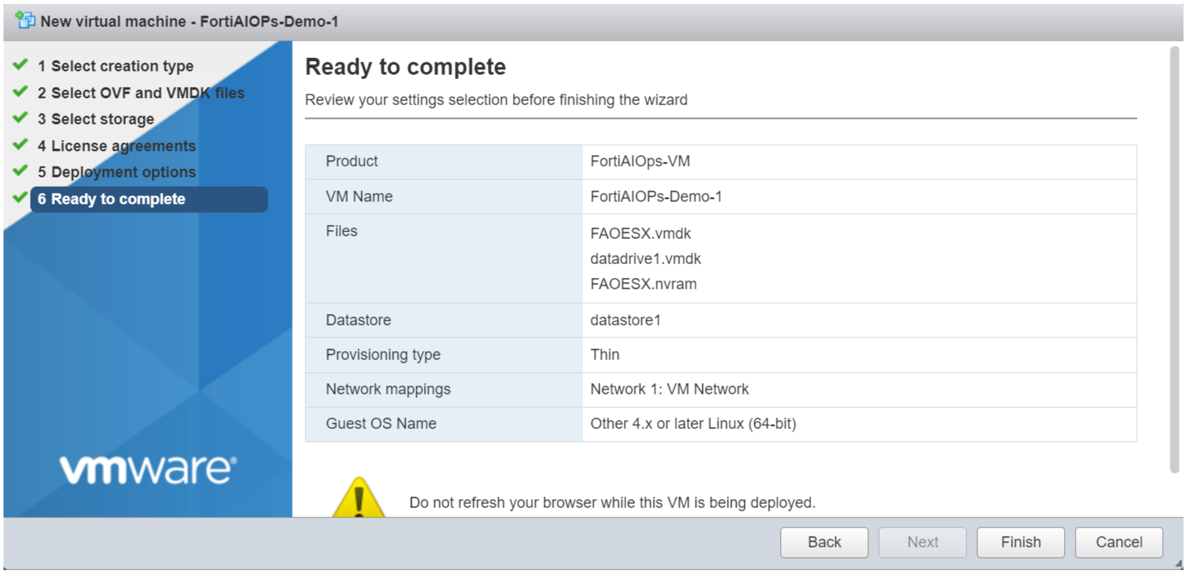
FortiAIOPs-Demo-1

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)

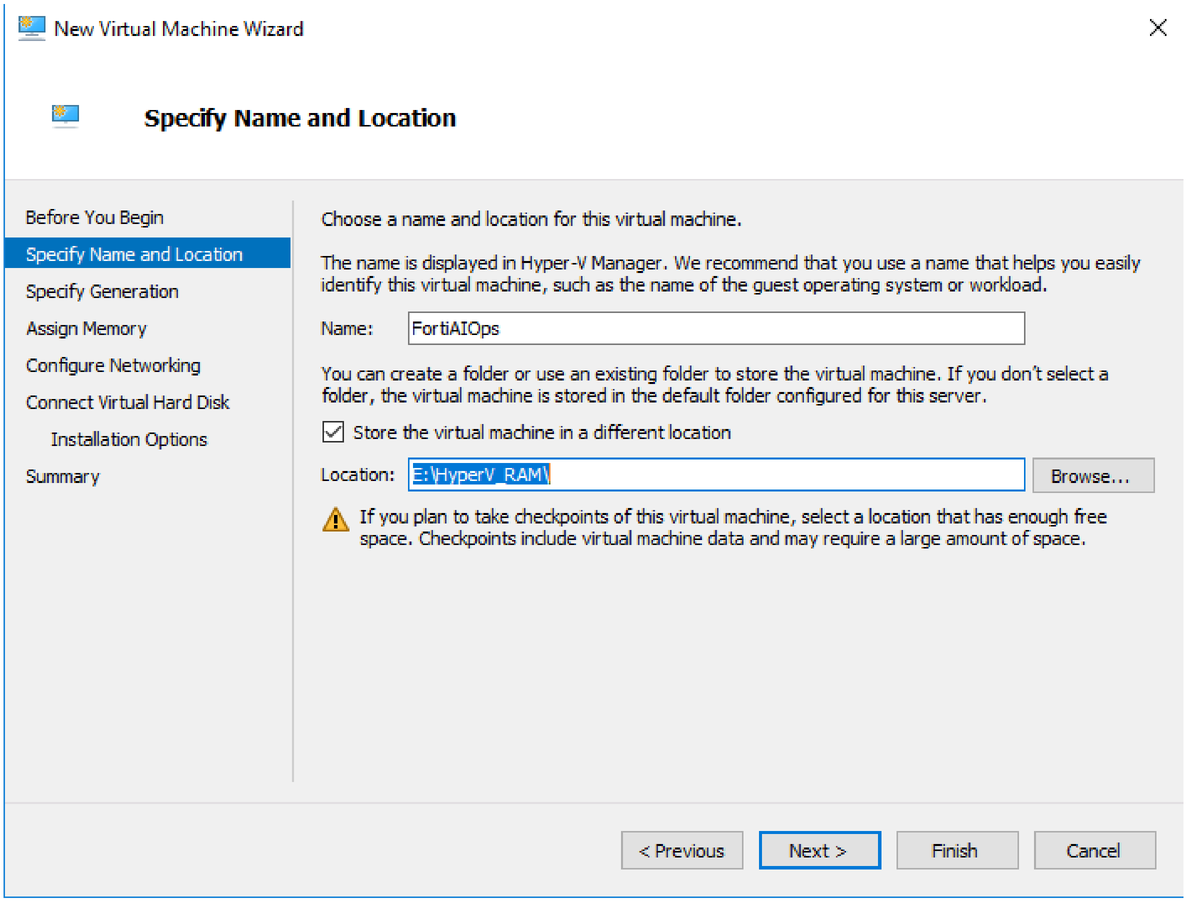
Do not refresh your browser while this VM is being deployed.

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

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**.



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

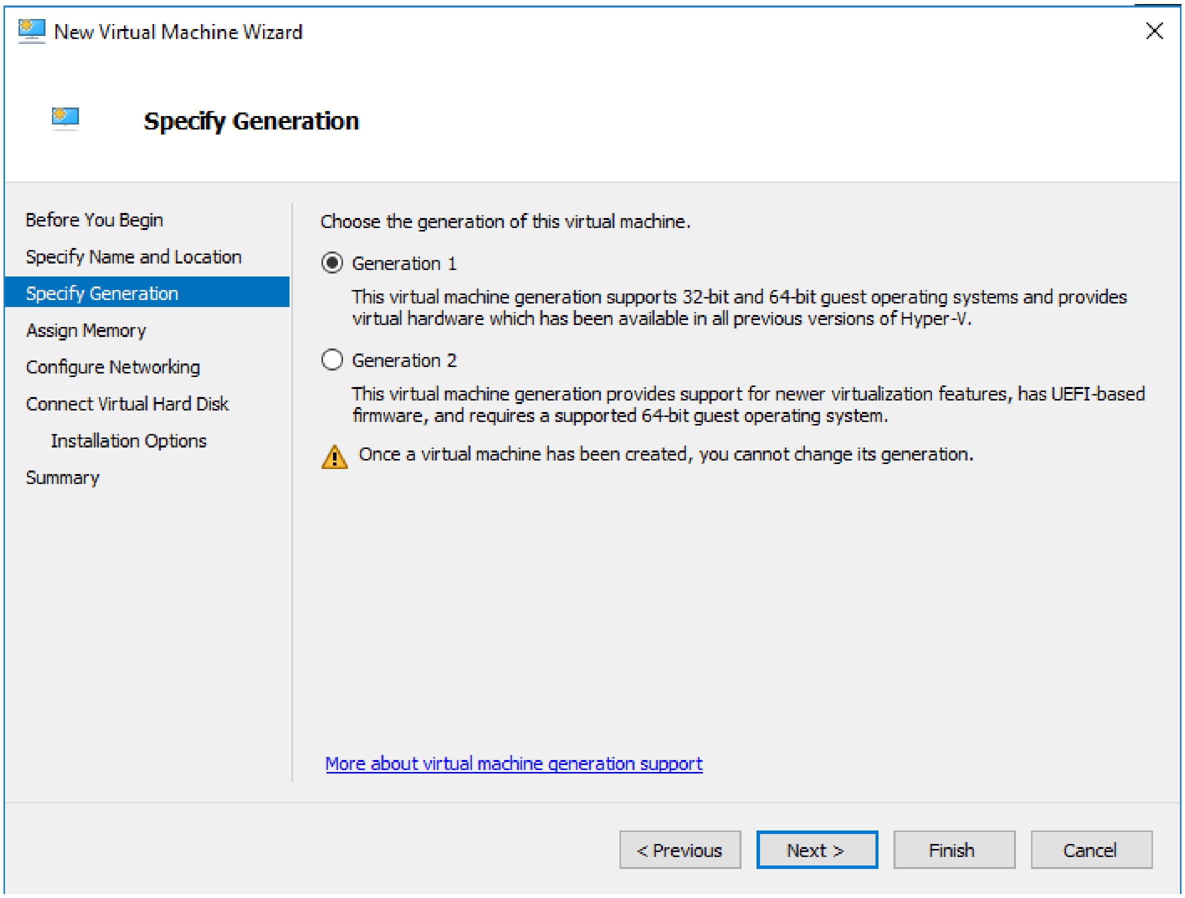
You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

☑ 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.

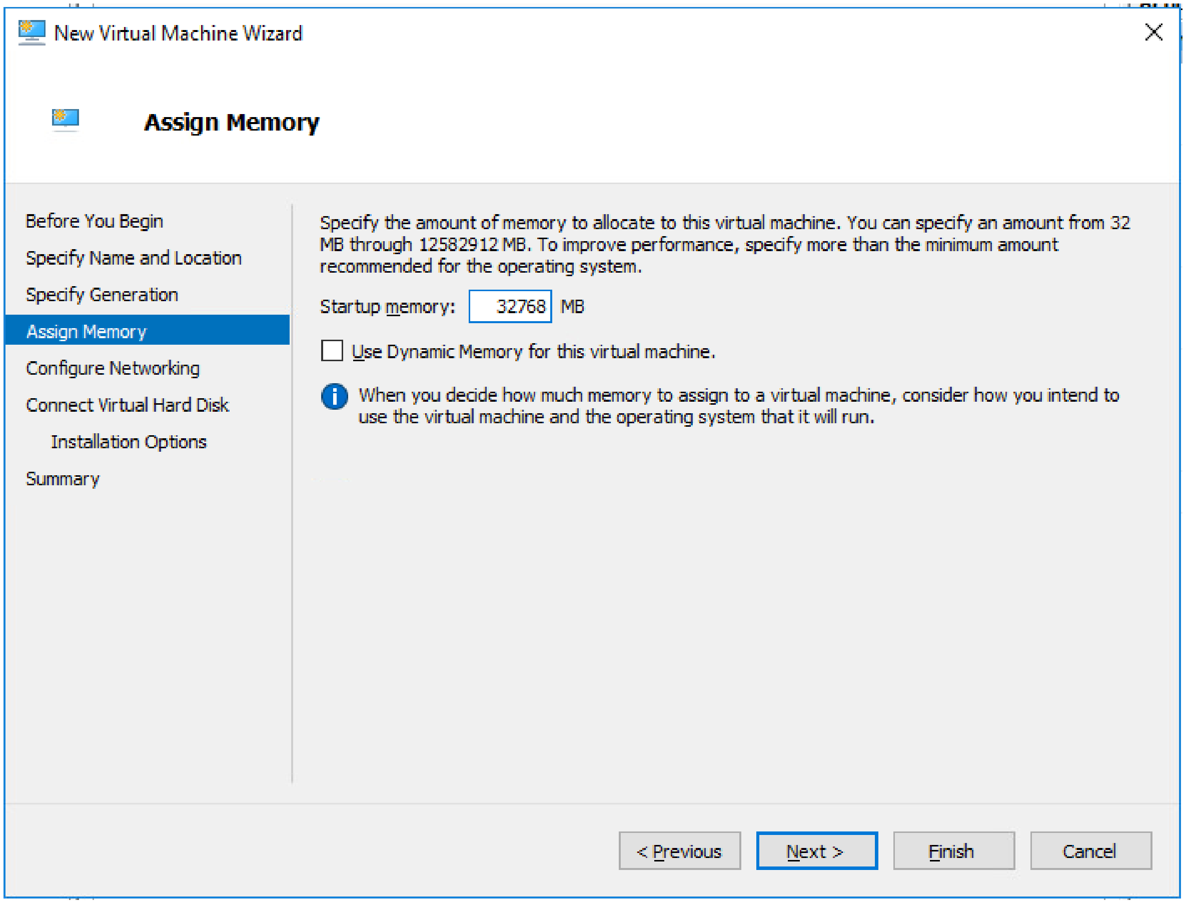
○ Generation 2

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.



New Virtual Machine Wizard

Assign Memory

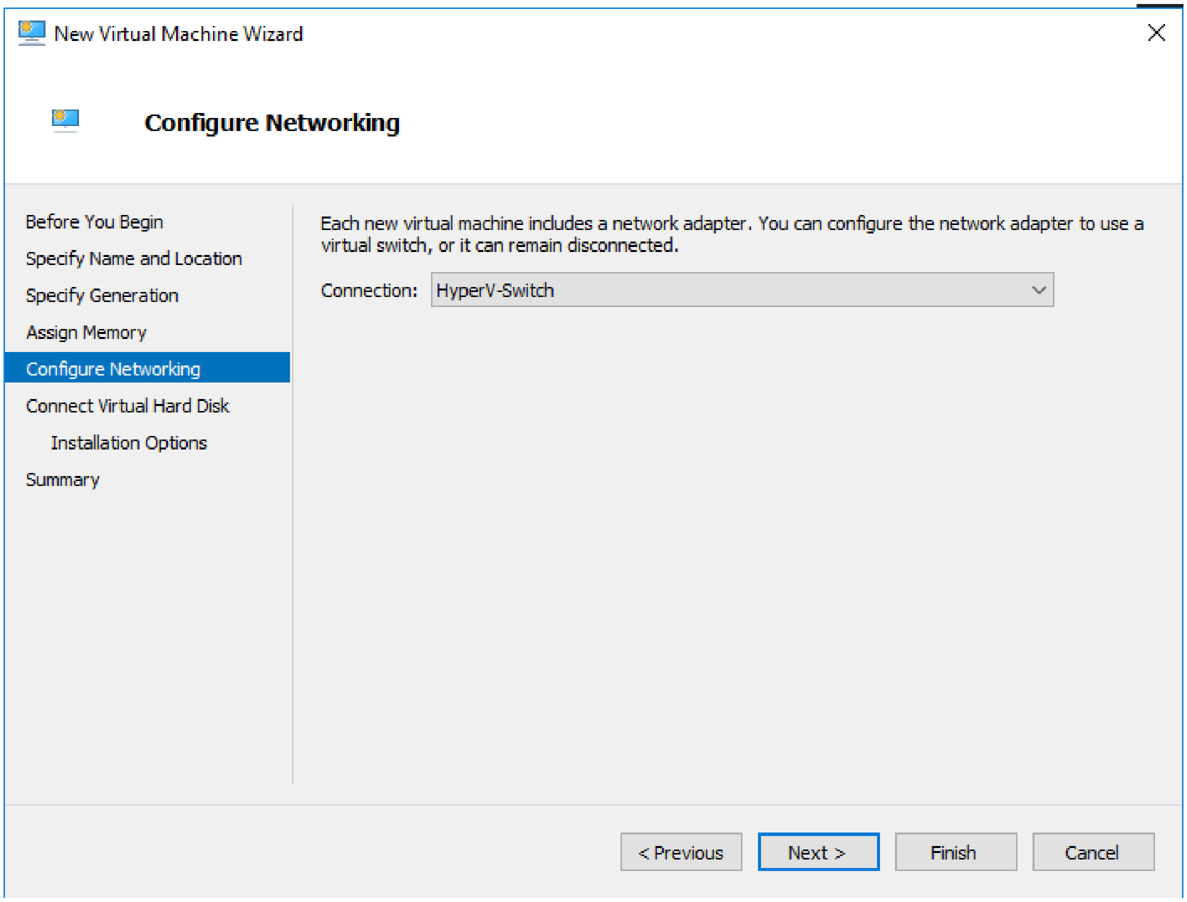
Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

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.

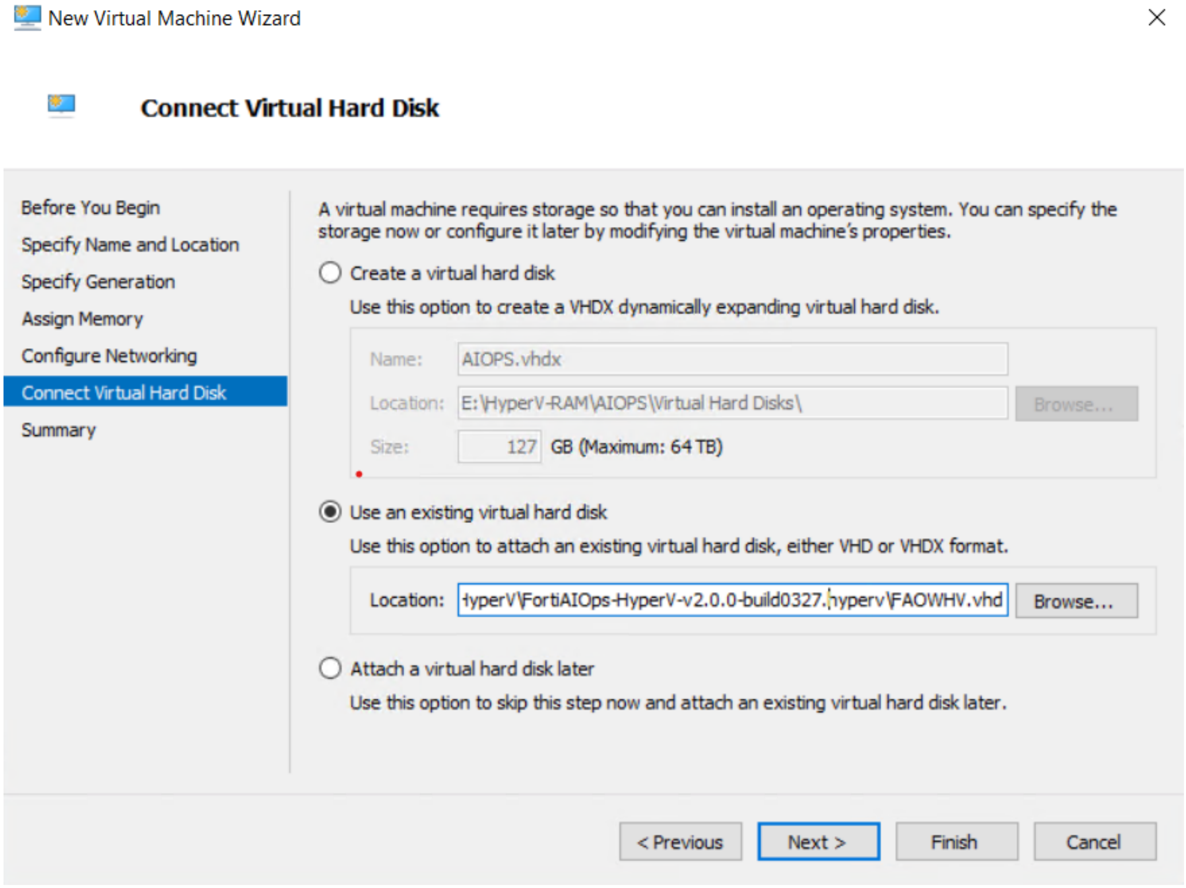
7. Select network adapter and click **Next.**



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**.



New Virtual Machine Wizard

Connect Virtual Hard Disk

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.

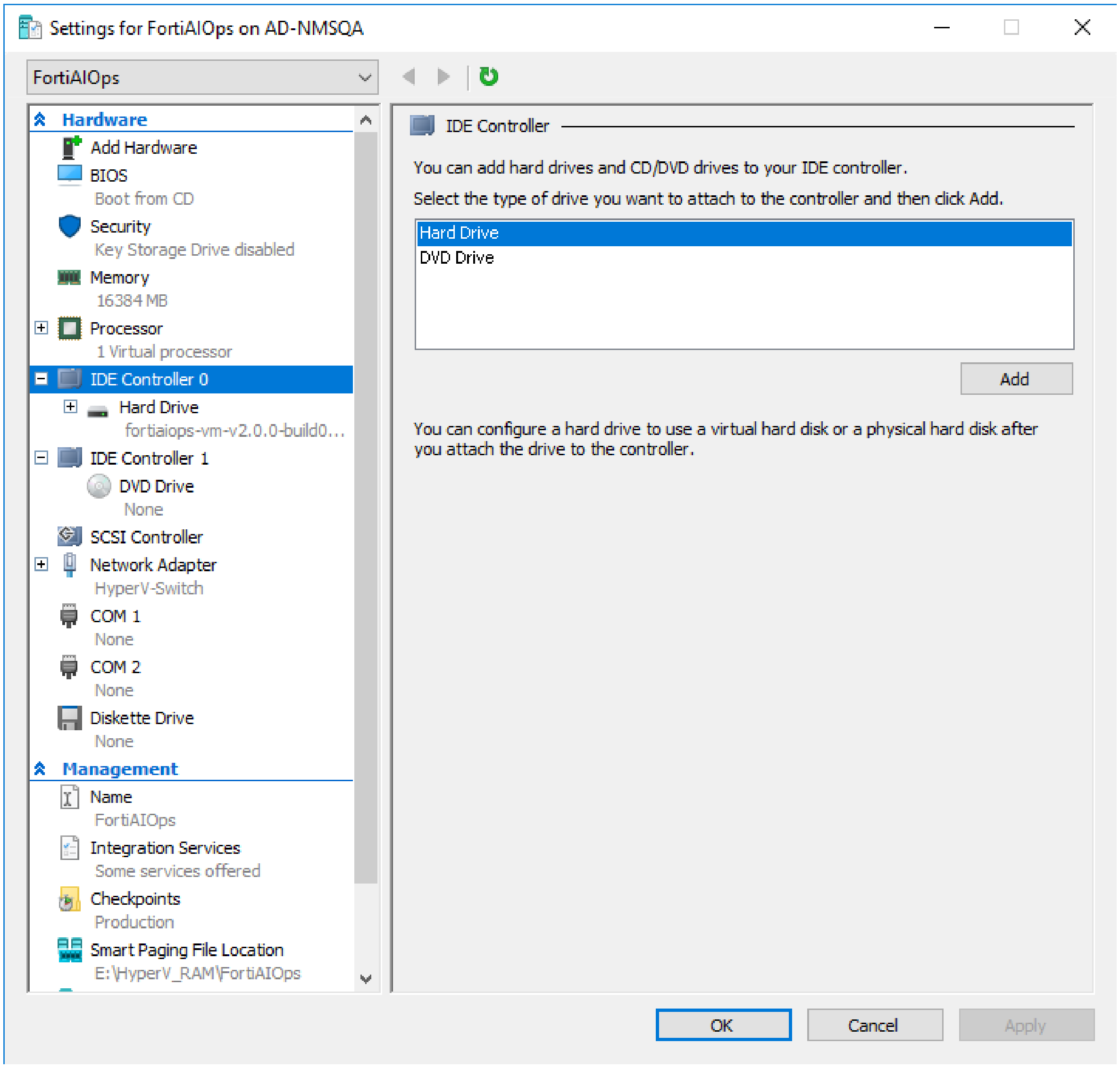
Location: ┤yperV\FortiAIOps-HyperV-v2.0.0-build0327.hyperv\FAOWHV.vhd

○ 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

IDE Controller

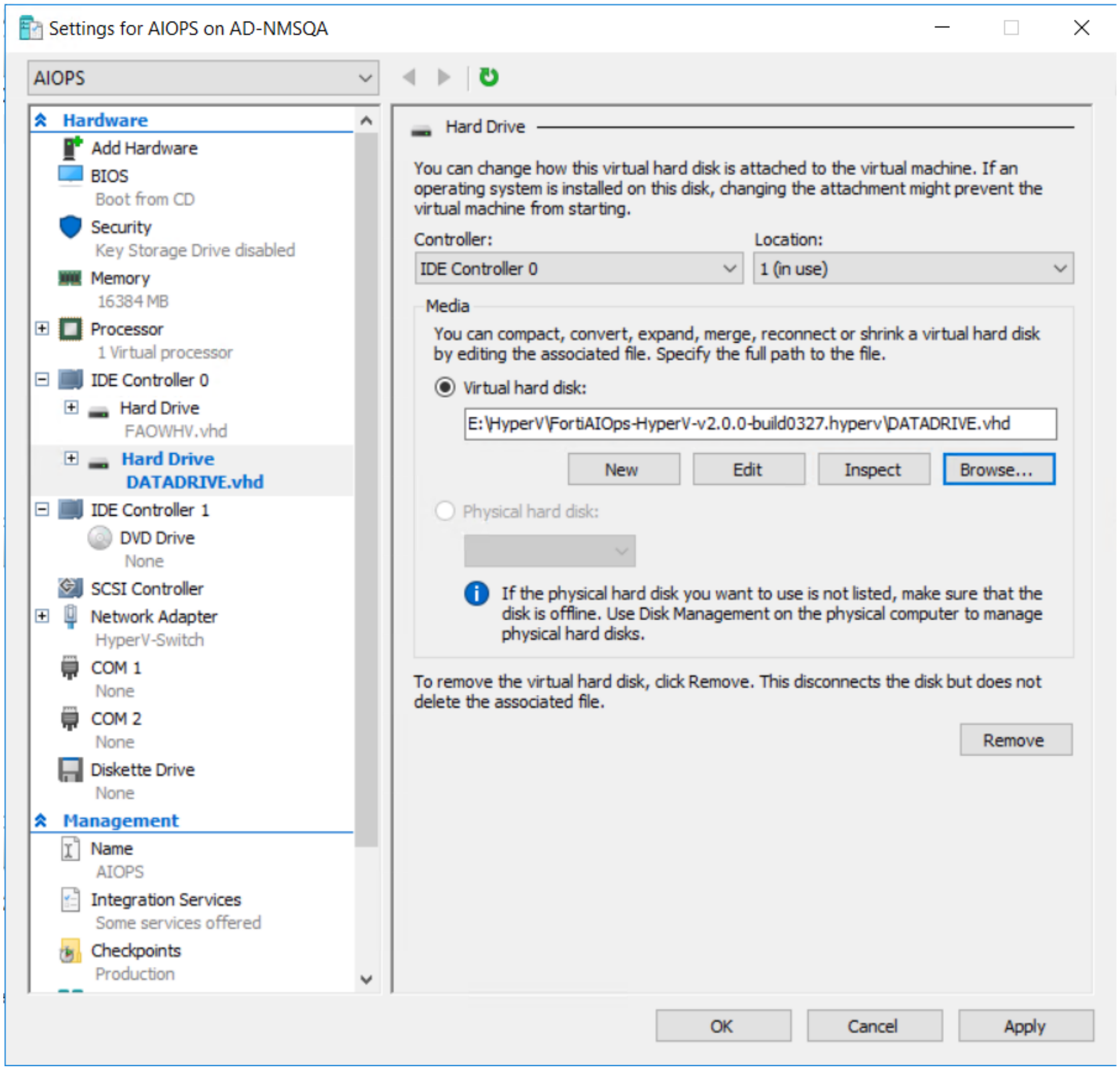
You can add hard drives and CD/DVD drives to your IDE controller.

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

Hard Drive
DVD Drive

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.

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

Hardware
- Add Hardware
- BIOS: Boot from CD
- Security: Key Storage Drive disabled
- Memory: 16384 MB
- Processor: 1 Virtual processor
- IDE Controller 0
  - Hard Drive: FAOWHV.vhd
  - Hard Drive: DATADRIVE.vhd
- IDE Controller 1
  - DVD Drive: None
- SCSI Controller
- Network Adapter: HyperV-Switch
- COM 1: None
- COM 2: None
- Diskette Drive: None

Management
- Name: AIOPS
- Integration Services: Some services offered
- Checkpoints: Production

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:

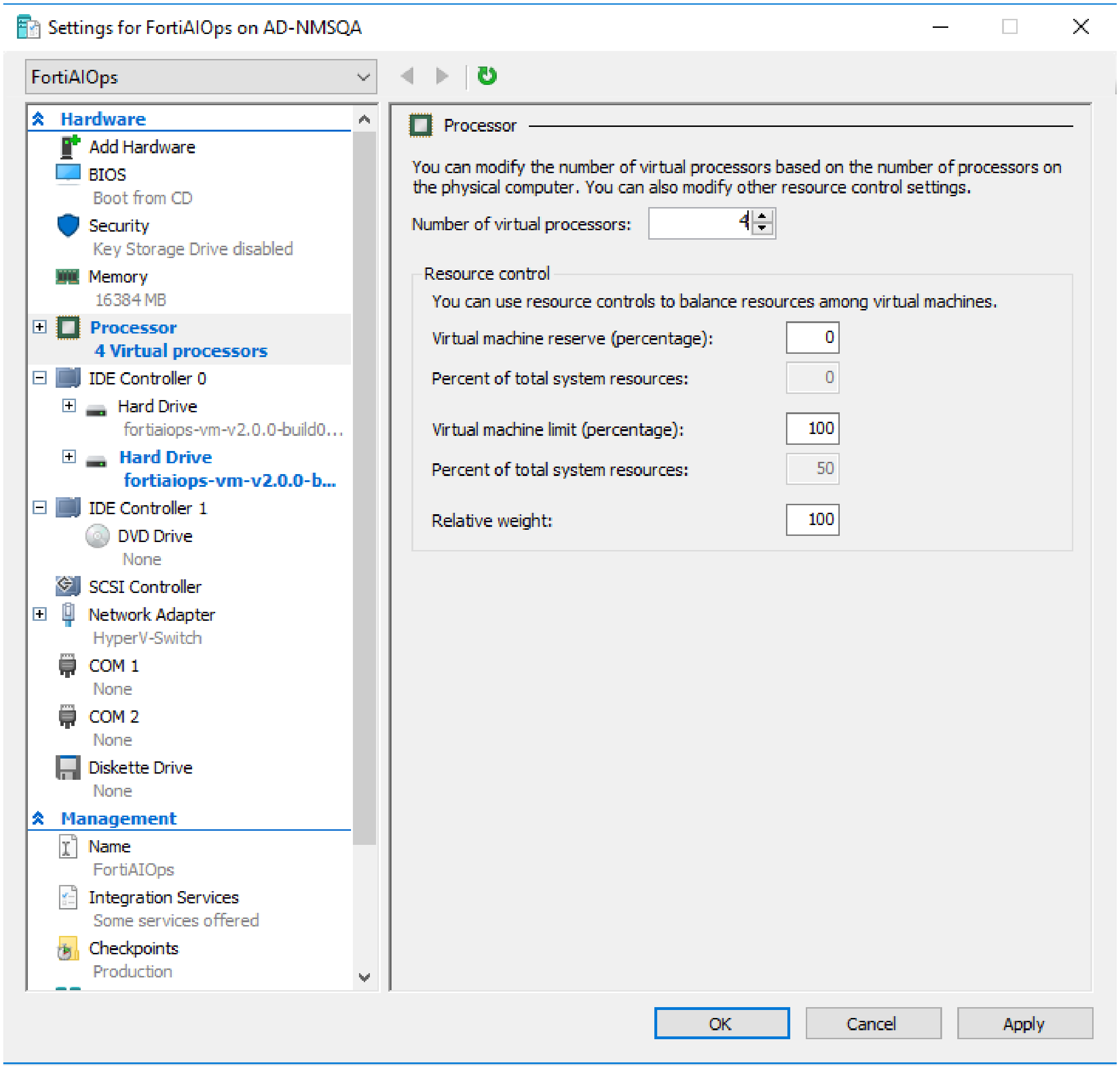
E:\HyperV\FortiAIOps-HyperV-v2.0.0-build0327.hyperv\DATADRIVE.vhd

○ 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**.



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.

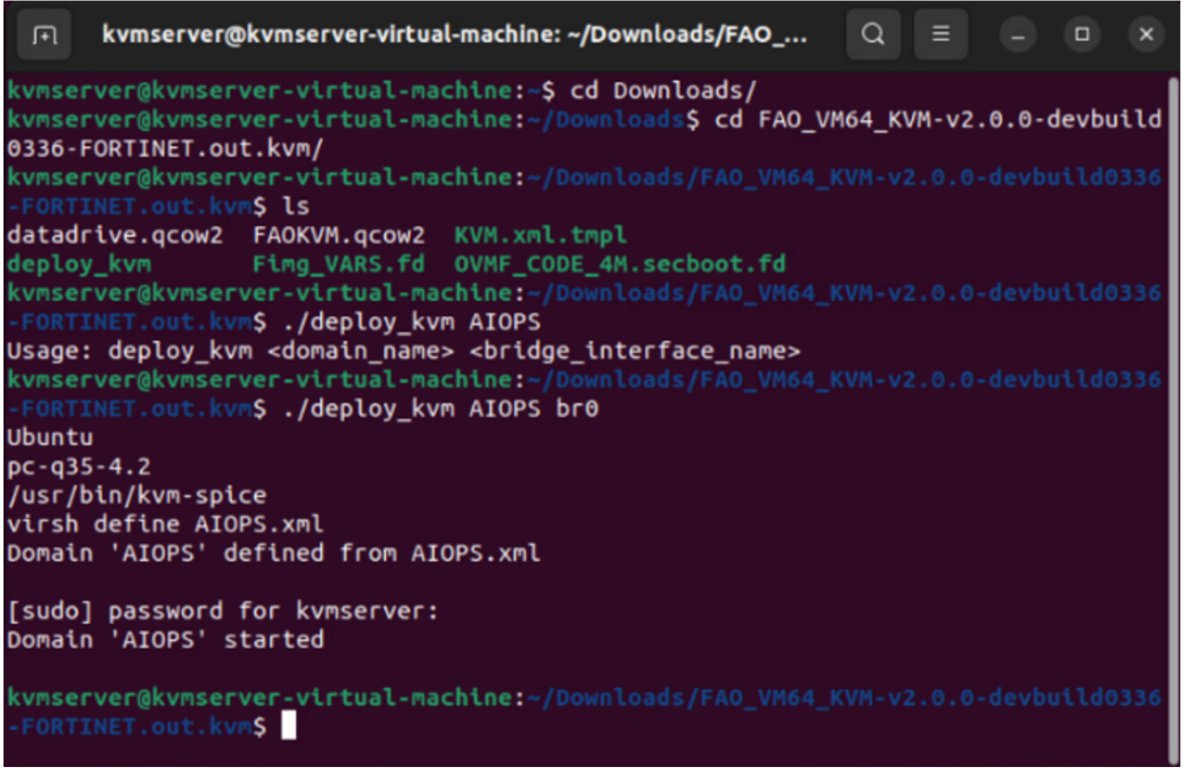
15. Perform post-installation tasks.

Installing FortiAIOps on KVM

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

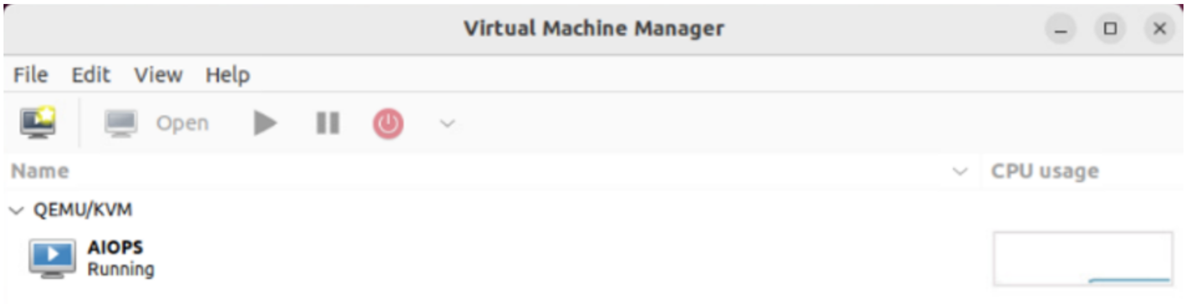
1. Download the installation file from *Fortinet Support* portal and unzip the file *FAO_VM64_KVM-vx.x.xdevbuildxxxx-FORTINET.out.kvm.zip*.
2. Open terminal and navigate to the path of the downloaded and unzipped installation files.

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

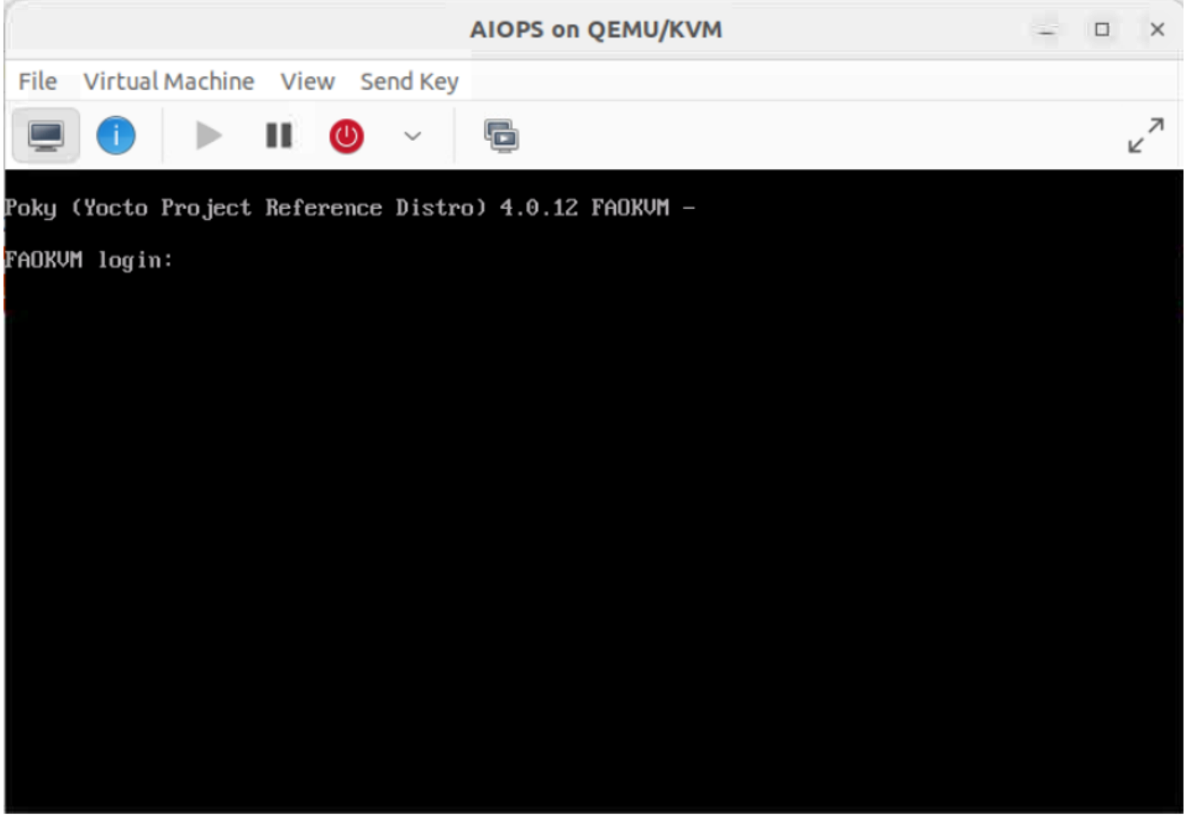


```
kvmserver@kvmserver-virtual-machine:~$ cd Downloads/
kvmserver@kvmserver-virtual-machine:~/Downloads$ cd FAO_VM64_KVM-v2.0.0-devbuild
0336-FORTINET.out.kvm/
kvmserver@kvmserver-virtual-machine:~/Downloads/FAO_VM64_KVM-v2.0.0-devbuild0336
-FORTINET.out.kvm$ ls
datadrive.qcow2  FAOKVM.qcow2  KVM.xml.tmpl
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.

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

Run the following command to upgrade FortiAIOps.

```
execute restore image ftp /home/ftpuser/FAO_VM64-v2.0.0-build0145-FORTINET.out
<IP address> <username> <password>
```

Note: Upgrading FortiAIOps is supported only via the CLI mode.

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).

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.
	`hardware deviceinfo <nic name>`	Displays information of a specific NIC.
	`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.

Command	Parameters	Description
	`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).

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`	Reset to the factory default settings. Restart the device after the second confirmation prompt.
	`formatlogdisk`	Format the log disk.
	`ping <destination>`	Ping the host name or IPv4 address.
	`traceroute <destination>`	Traceroute of the host name or IPV4 address.
	`reboot`	Reboot the system.
	`shutdown`	Shut down the device.

Command	Parameters	Description
	`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.

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.

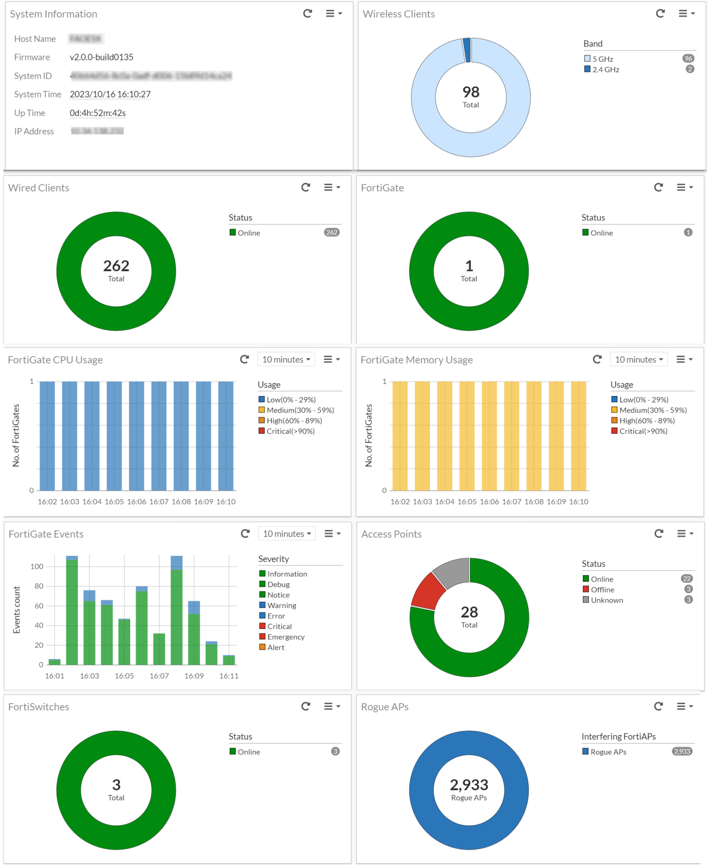
Dashboard

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.



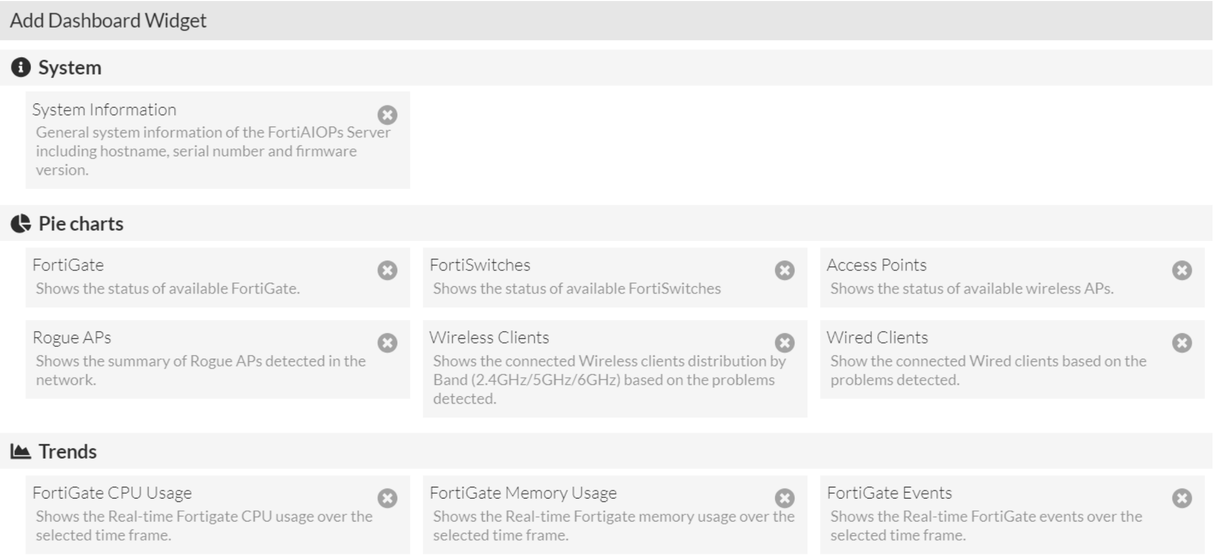
System Information

Host Name [redacted]
Firmware v2.0.0-build0135
System ID [redacted]
System Time 2023/10/16 16:10:27
Up Time 0d:4h:52m:42s
IP Address [redacted]

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 hostname, serial number and firmware version.

Pie charts

FortiGate ⊗
Shows the status of available FortiGate.

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) based on the problems detected.

Wired Clients ⊗
Show the connected Wired clients based on the problems detected.

Trends

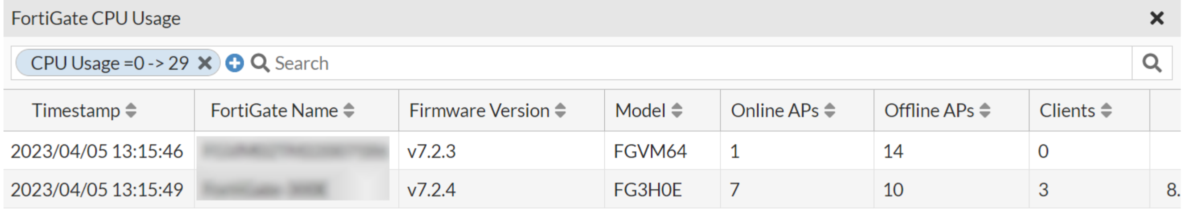
FortiGate CPU Usage ⊗
Shows the Real-time Fortigate CPU usage over the selected time frame.

FortiGate Memory Usage ⊗
Shows the Real-time Fortigate memory usage over the selected time frame.

FortiGate Events ⊗
Shows the Real-time FortiGate events over the selected time frame.

The following widgets provide network data on this dashboard.

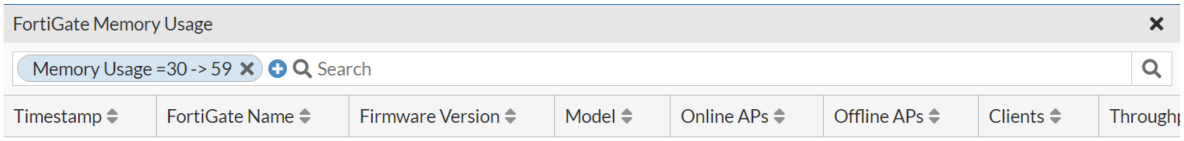
- **System Information** - This widget provides generic information about the FortiGate controller such as the host name, firmware version, system ID, current system time, uptime, and the IP address.
- **Wireless Clients** - Displays the total number of connected clients with their band categorization of 2.4GHz, 5GHz, and 6GHz. Click on the chart to navigate to **Wireless > Clients**.
- **Wired Clients** - Displays the total number of connected clients with their status.
- **FortiGate** - 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**.
- **FortiGate CPU Usage** and **FortiGate 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, 12, or 24 hours). 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.

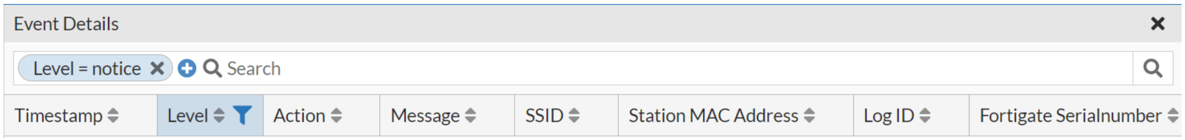


FortiGate Memory Usage ✕

Memory Usage =30 -> 59 ✕ Search

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

- **FortiGate Events** - Displays the FotiGate 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, 12, or 24 hours).



Event Details

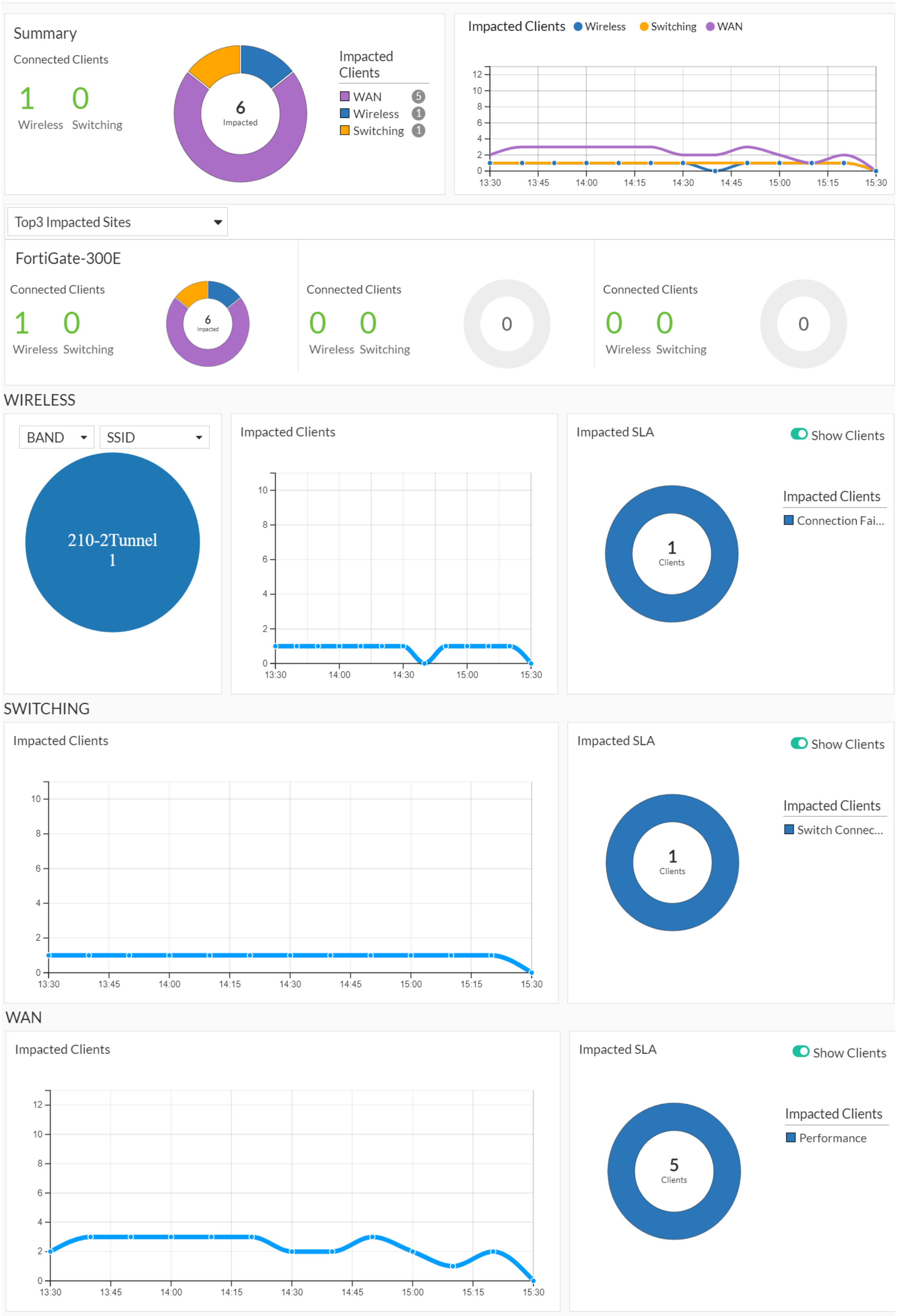
Level = notice ✕ Search

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

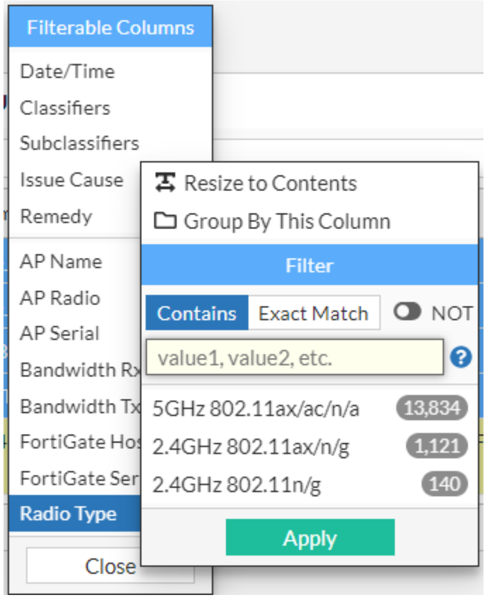
- **Access Points** - Displays the total number of access points in your network and their status (*Online*, *Offine*, *Waiting for Authorization*, or *Unknown*). Click on the chart to navigate to **Wireless > Access Points**.
- **FortiSwitches** - Displays the total number of FortiSwitches in your network and their status (*Online*, *Offine*, *Waiting for Authorization*, or *Unknown*). Click on the chart to navigate to **Switch > FortiSwitch**.
- **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 five panels - **Summary**, **Top 3 Impacted Sites**, **Wireless**, **Switching**, and **WAN**. Data is displayed in a series of charts and graphs, that you can filter based on time duration. Navigate to **Dashboard > AI Insights**.


Summary
Connected Clients
1 Wireless
0 Switching
6
Impacted
Impacted Clients
🟪 WAN 5
🟦 Wireless 1
🟧 Switching 1
Impacted Clients ● Wireless ● Switching ● WAN
12
10
8
6
4
2
0
13:30
13:45
14:00
14:15
14:30
14:45
15:00
15:15
15:30
Top3 Impacted Sites
FortiGate-300E
Connected Clients
1 Wireless
0 Switching
6
Impacted
Connected Clients
0 Wireless
0 Switching
0
Connected Clients
0 Wireless
0 Switching
0
WIRELESS
BAND
SSID
210-2Tunnel
1
Impacted Clients
10
8
6
4
2
0
13:30
14:00
14:30
15:00
15:30
Impacted SLA
Show Clients
1
Clients
Impacted Clients
🟦 Connection Fai...
SWITCHING
Impacted Clients
10
8
6
4
2
0
13:30
13:45
14:00
14:15
14:30
14:45
15:00
15:15
15:30
Impacted SLA
Show Clients
1
Clients
Impacted Clients
🟦 Switch Connec...
WAN
Impacted Clients
12
10
8
6
4
2
0
13:30
13:45
14:00
14:15
14:30
14:45
15:00
15:15
15:30
Impacted SLA
Show Clients
5
Clients
Impacted Clients
🟦 Performance

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. This is an example.

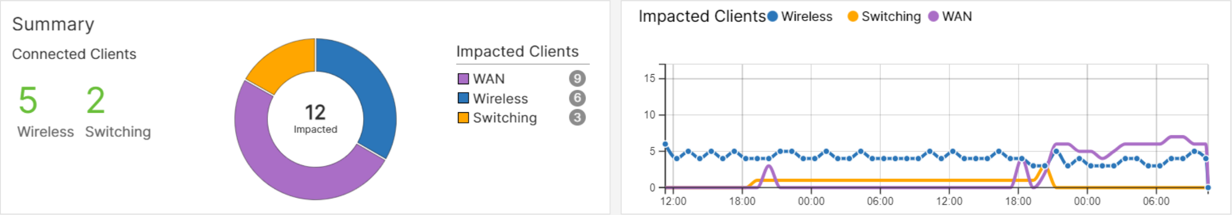


Dashboard data is refreshed at a configurable interval.

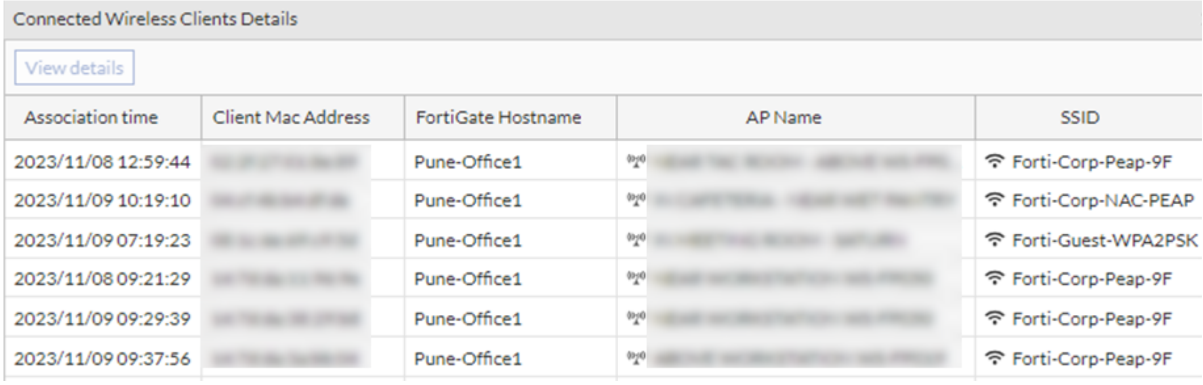
- Summary
- Top 3 Impacted Sites
- Wireless
- Switching
- WAN

Summary

The **Summary** panels displays data in charts and statistics for the total number of connected and impacted clients for switching, wireless, and WAN. Clicking on the donut charts in this panel, re-directs you to the Impacted Devices page.



FortiAIOps displays the connected client count, that is, the total number of clients connected during the selected duration in the dashboard. This is the client detail for wireless.

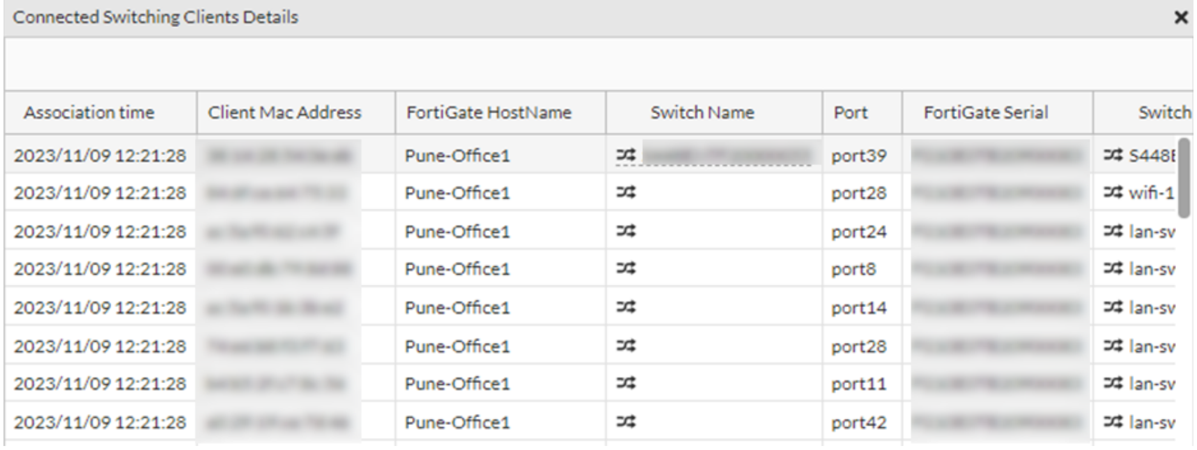


Connected Wireless Clients Details

View details

Association time	Client Mac Address	FortiGate Hostname	AP Name	SSID
2023/11/08 12:59:44	[redacted]	Pune-Office1	[redacted]	Forti-Corp-Peap-9F
2023/11/09 10:19:10	[redacted]	Pune-Office1	[redacted]	Forti-Corp-NAC-PEAP
2023/11/09 07:19:23	[redacted]	Pune-Office1	[redacted]	Forti-Guest-WPA2PSK
2023/11/08 09:21:29	[redacted]	Pune-Office1	[redacted]	Forti-Corp-Peap-9F
2023/11/09 09:29:39	[redacted]	Pune-Office1	[redacted]	Forti-Corp-Peap-9F
2023/11/09 09:37:56	[redacted]	Pune-Office1	[redacted]	Forti-Corp-Peap-9F

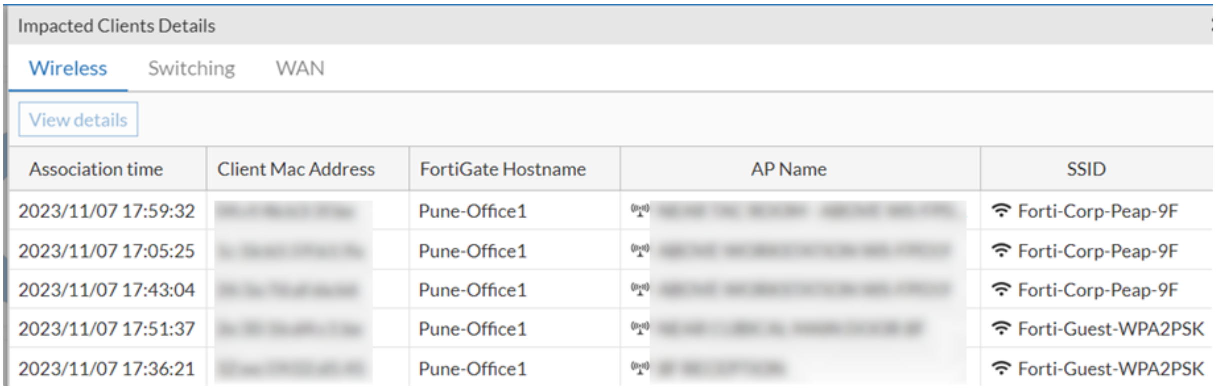
This is the client detail for switching.



Connected Switching Clients Details ✕

Association time	Client Mac Address	FortiGate HostName	Switch Name	Port	FortiGate Serial	Switch
2023/11/09 12:21:28	[redacted]	Pune-Office1	[redacted]	port39	[redacted]	S448E
2023/11/09 12:21:28	[redacted]	Pune-Office1		port28	[redacted]	wifi-1
2023/11/09 12:21:28	[redacted]	Pune-Office1		port24	[redacted]	lan-sv
2023/11/09 12:21:28	[redacted]	Pune-Office1		port8	[redacted]	lan-sv
2023/11/09 12:21:28	[redacted]	Pune-Office1		port14	[redacted]	lan-sv
2023/11/09 12:21:28	[redacted]	Pune-Office1		port28	[redacted]	lan-sv
2023/11/09 12:21:28	[redacted]	Pune-Office1		port11	[redacted]	lan-sv
2023/11/09 12:21:28	[redacted]	Pune-Office1		port42	[redacted]	lan-sv

Click on the **Impacted Clients** graph in this panel to view the client details for wireless, switching, and WAN.

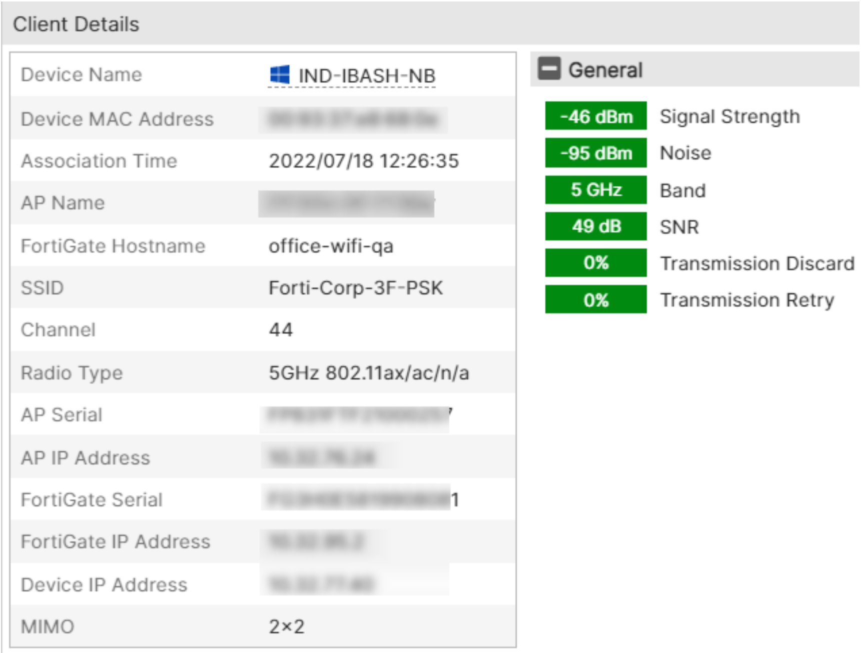


Impacted Clients Details

View details

Association time	Client Mac Address	FortiGate Hostname	AP Name	SSID
2023/11/07 17:59:32	[redacted]	Pune-Office1	[redacted]	Forti-Corp-Peap-9F
2023/11/07 17:05:25	[redacted]	Pune-Office1	[redacted]	Forti-Corp-Peap-9F
2023/11/07 17:43:04	[redacted]	Pune-Office1	[redacted]	Forti-Corp-Peap-9F
2023/11/07 17:51:37	[redacted]	Pune-Office1	[redacted]	Forti-Guest-WPA2PSK
2023/11/07 17:36:21	[redacted]	Pune-Office1	[redacted]	Forti-Guest-WPA2PSK

For each of the panels depicted for the connected and impacted clients, you can click on **View Details** to view detailed summary of each client.



Client Details

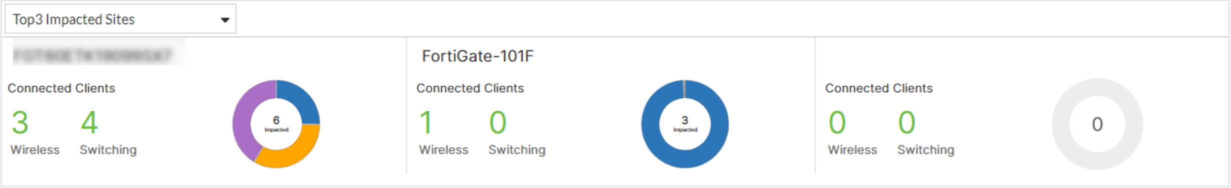
Device Name	IND-IBASH-NB
Device MAC Address	[redacted]
Association Time	2022/07/18 12:26:35
AP Name	[redacted]
FortiGate Hostname	office-wifi-qa
SSID	Forti-Corp-3F-PSK
Channel	44
Radio Type	5GHz 802.11ax/ac/n/a
AP Serial	[redacted]
AP IP Address	[redacted]
FortiGate Serial	[redacted]1
FortiGate IP Address	[redacted]
Device IP Address	[redacted]
MIMO	2×2

General

-46 dBm	Signal Strength
-95 dBm	Noise
5 GHz	Band
49 dB	SNR
0%	Transmission Discard
0%	Transmission Retry

Top 3 Impacted Sites

The **Top 3 Impacted Sites** panel allows you to view client data related to the top 3 FortiGate controllers with the highest number of impacted wireless and switching clients. It also displays the total number of connected and impacted clients for each FortiGate controller. You can view collective data for all 3 sites or select any one to view data. Clicking on the donut charts in this panel, re-directs you to the Impacted Devices page and clicking on the **Connected Clients** count, displays the client details for the specific FortiGate controller.

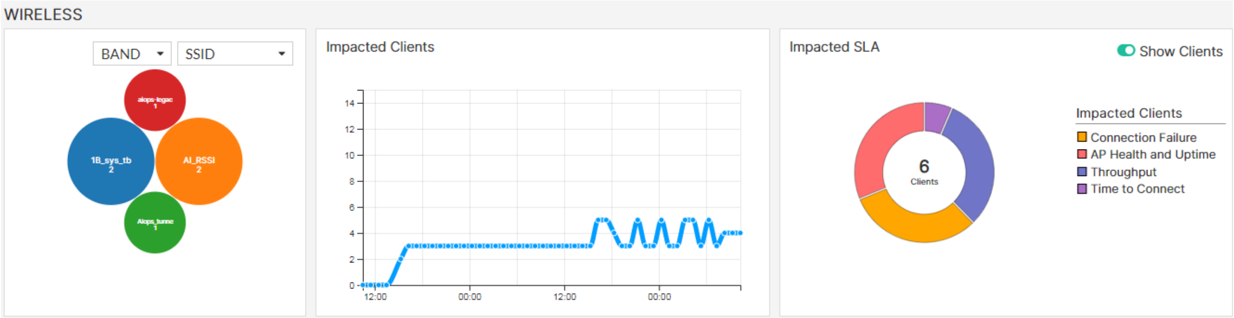


Top3 Impacted Sites

[redacted]	FortiGate-101F	
Connected Clients 3 Wireless 4 Switching 6 Impacted	Connected Clients 1 Wireless 0 Switching 3 Impacted	Connected Clients 0 Wireless 0 Switching 0

Wireless

The **Wireless** panel allows you to filter data based on a specific SSID/Band or view the consolidated data for all SSIDs. The total number of impacted wireless clients at different time duration for the selected SSID/Band are displayed. The *Impacted SLA* data is displayed for impacted clients and/or devices (FortiGate and APs).



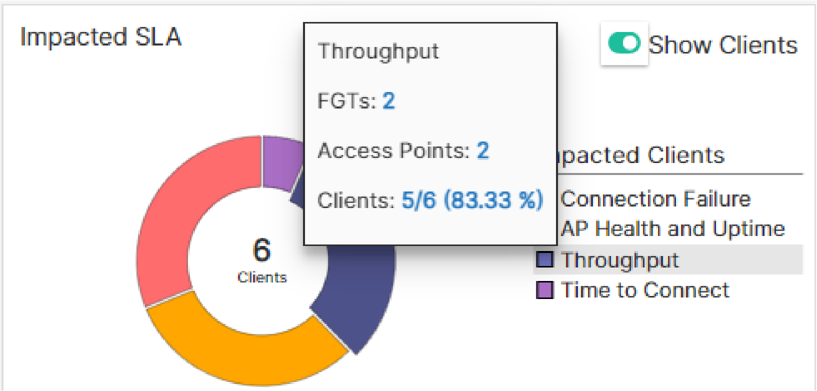
SLAs, Topology, and Logs

The following 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. In each impacted SLA panel, you can select **Show Clients** to view the impacted client count or click **Show APs** to view the impacted AP count.

- 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.



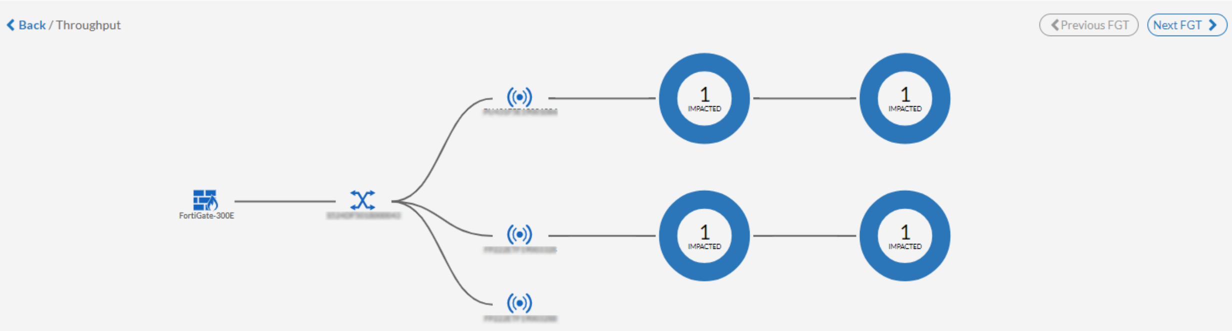
Throughput

FGTs: 2

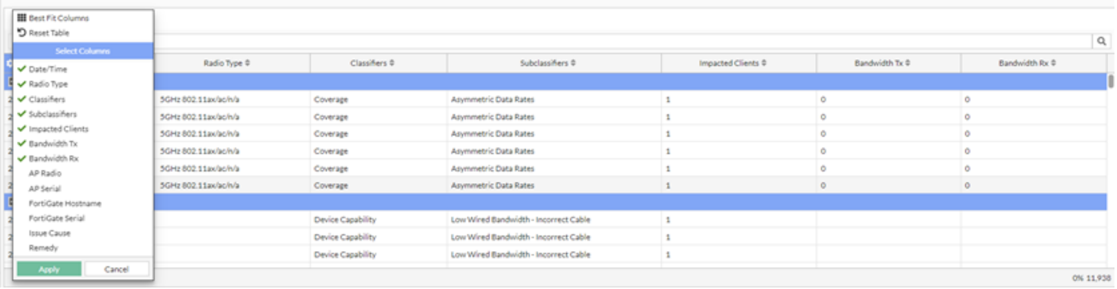
Access Points: 2

Clients: 5/6 (83.33 %)

To view the topology, click on **Throughput** in the impacted SLAs list or click on the bar in the chart.



The **Throughput Failures** 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.



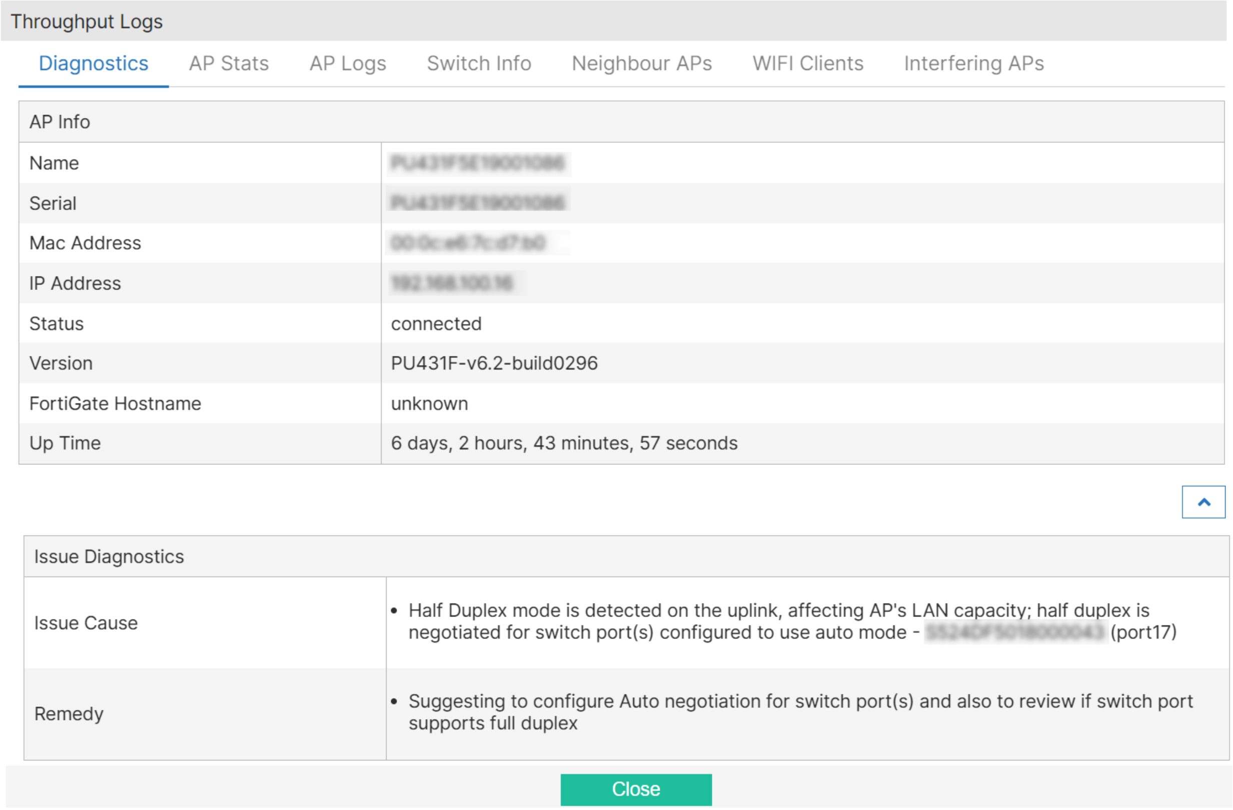
Radio Type	Classifiers	Subclassifiers	Impacted Clients	Bandwidth Tx	Bandwidth Rx
5GHz 802.11ax/ac/n/a	Coverage	Asymmetric Data Rates	1	0	0
5GHz 802.11ax/ac/n/a	Coverage	Asymmetric Data Rates	1	0	0
5GHz 802.11ax/ac/n/a	Coverage	Asymmetric Data Rates	1	0	0
5GHz 802.11ax/ac/n/a	Coverage	Asymmetric Data Rates	1	0	0
5GHz 802.11ax/ac/n/a	Coverage	Asymmetric Data Rates	1	0	0
5GHz 802.11ax/ac/n/a	Coverage	Asymmetric Data Rates	1	0	0
	Device Capability	Low Wired Bandwidth - Incorrect Cable	1		
	Device Capability	Low Wired Bandwidth - Incorrect Cable	1		
	Device Capability	Low Wired Bandwidth - Incorrect Cable	1		

0% 11,938

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.
Classifier	The classifier of the issue reported for the SLA.
Subclassifier	The sub-classifier of the issue for the reported classifier.
Impacted Clients	The number of impacted clients.
Issue Cause	Detailed cause of the SLA breach that impacted the client/AP/FortiGate.
Remedy	The suggested remedy to resolve the issue.
AP Radio	The AP radio that the client associated with.
AP Serial	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.

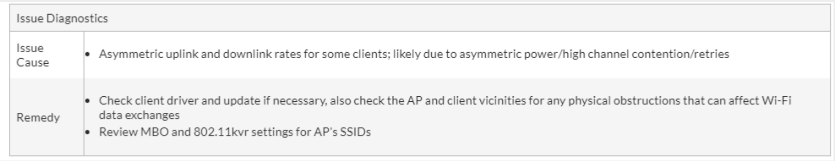
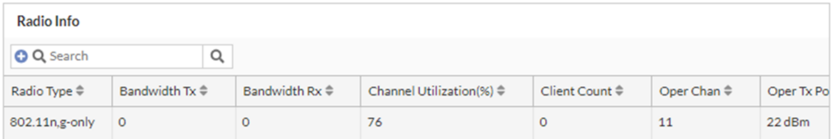
In the impacted details displayed, select a specific row of throughput failure and click **View Details**. You can view details of the impacted AP and issue diagnostics. You can view throughput logs related to **Diagnostics** with the issue description and the suggested remediation, **AP Stats** with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

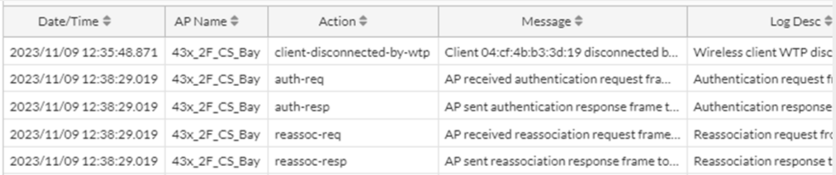
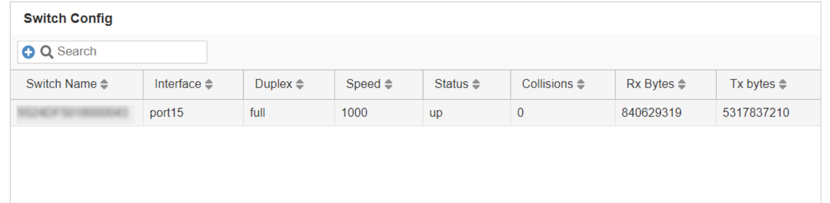
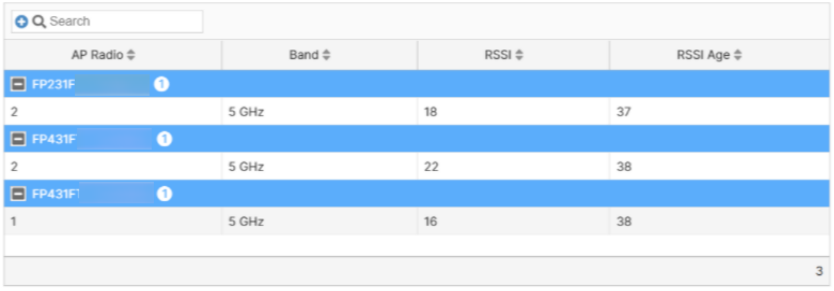
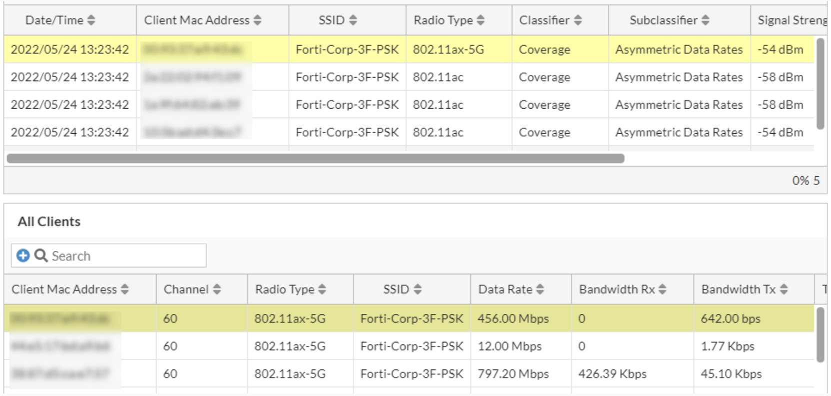


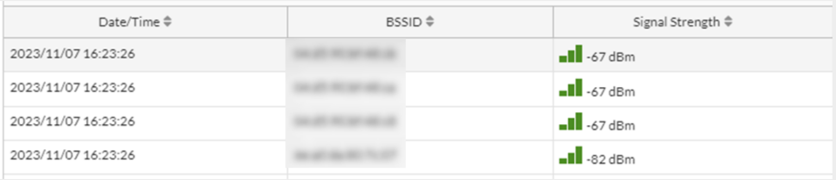
Throughput Logs

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

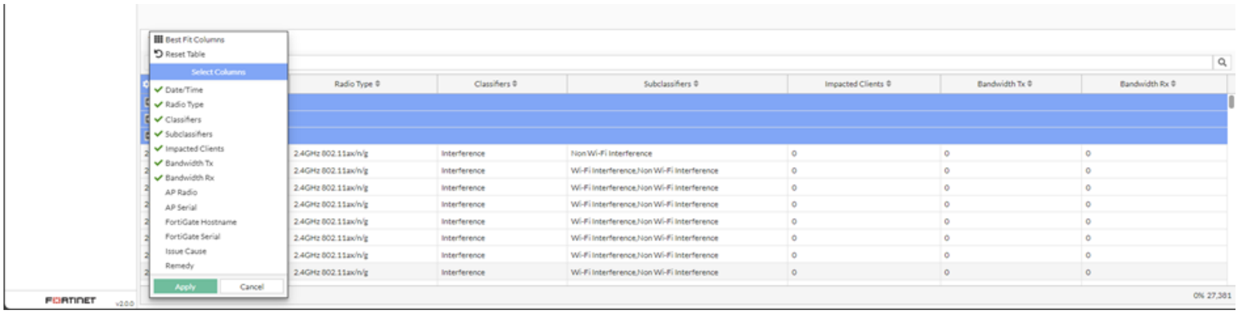
<table>
<tr><th>Logs</th><th>Description</th></tr>
<tr><td><b>Diagnostics</b></td><td>This tab provides detailed cause of the SLA breach that impacted the client/AP/FortiGate. FortiAIOps also suggests the remedy to resolve the issue.

Issue Diagnostics
Issue Cause: • Asymmetric uplink and downlink rates for some clients; likely due to asymmetric power/high channel contention/retries
Remedy: • 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>
<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>AP Logs</b></td><td>This tab provides the AP event logs generated from FortiGate.</td></tr>
</table>

<table>
<tr><th>Logs</th><th>Description</th></tr>
<tr><td></td><td>

<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 fr</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.

<b>Switch Config</b>
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]</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]</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]</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
<b>All Clients</b>
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

The donut charts that represent the classifiers and sub-classifiers in the topology, provide the count of the impacted clients associated with each AP. Click on any of these charts to view the impacted client details per AP.



Radio Type ⬍	Classifiers ⬍	Subclassifiers ⬍	Impacted Clients ⬍	Bandwidth Tx ⬍	Bandwidth Rx ⬍
2.4GHz 802.11ax/n/g	Interference	Non Wi-Fi Interference	0	0	0
2.4GHz 802.11ax/n/g	Interference	Wi-Fi Interference,Non Wi-Fi Interference	0	0	0
2.4GHz 802.11ax/n/g	Interference	Wi-Fi Interference,Non Wi-Fi Interference	0	0	0
2.4GHz 802.11ax/n/g	Interference	Wi-Fi Interference,Non Wi-Fi Interference	0	0	0
2.4GHz 802.11ax/n/g	Interference	Wi-Fi Interference,Non Wi-Fi Interference	0	0	0
2.4GHz 802.11ax/n/g	Interference	Wi-Fi Interference,Non Wi-Fi Interference	0	0	0
2.4GHz 802.11ax/n/g	Interference	Wi-Fi Interference,Non Wi-Fi Interference	0	0	0
2.4GHz 802.11ax/n/g	Interference	Wi-Fi Interference,Non Wi-Fi Interference	0	0	0

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

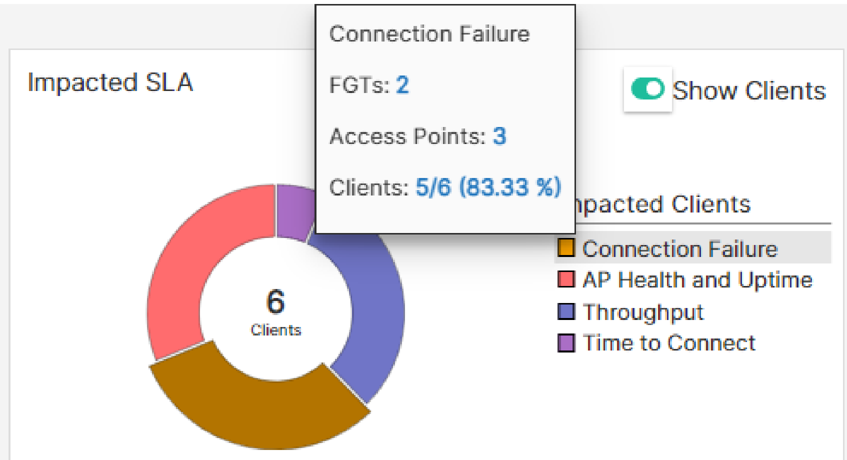
Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
Client MAC Address	The MAC address of the impacted client device.
Device	The name of the device as configured by the user. If the name is not configured or available, then MAC address is displayed.
SSID	The SSID that the impacted client is associated with.
Radio Type	The impacted radio and band information associated with the client.
Classifier	The classifier of the issue reported for the SLA.
Subclassifier	The sub-classifier of the issue for the reported classifier.
Signal Strength	The signal strength of the client at the time of impact.
Tx Rate	The Tx data rate achieved by the client.
Rx Rate	The Rx data rate achieved by the client.
AP Radio	The AP radio that the client associated with.
AP Serial	The AP serial number that the client associated with.
Channel	The channel at which the client connected.
FortiGate Hostname	The hostname of the FortiGate associated with the AP/impacted client.
FortiGate Serial	The serial number of the associated FortiGate.

Attribute	Description
Max Capacity	The maximum data rate supported by the client at the time of impact.
SNR	The client SNR reported at the time of impact.

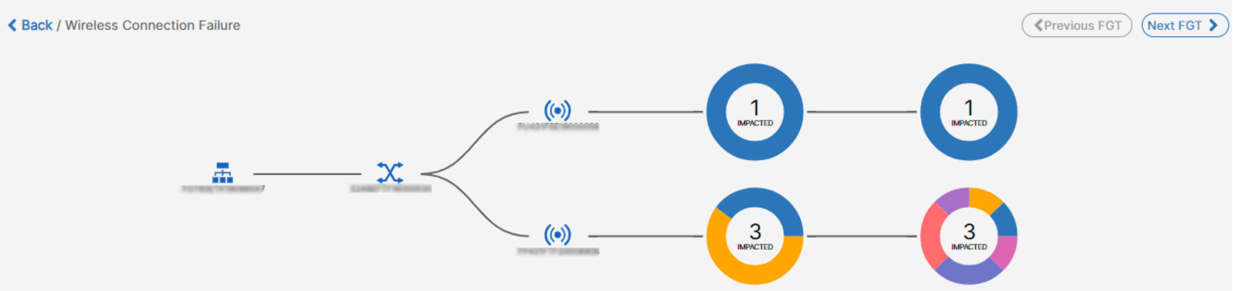
Select any impacted client and click **Show AP details** to view the detailed AP logs. For more details on each of these tabs, see **View Details** in Throughput logs described earlier in the section.

Connection Failure

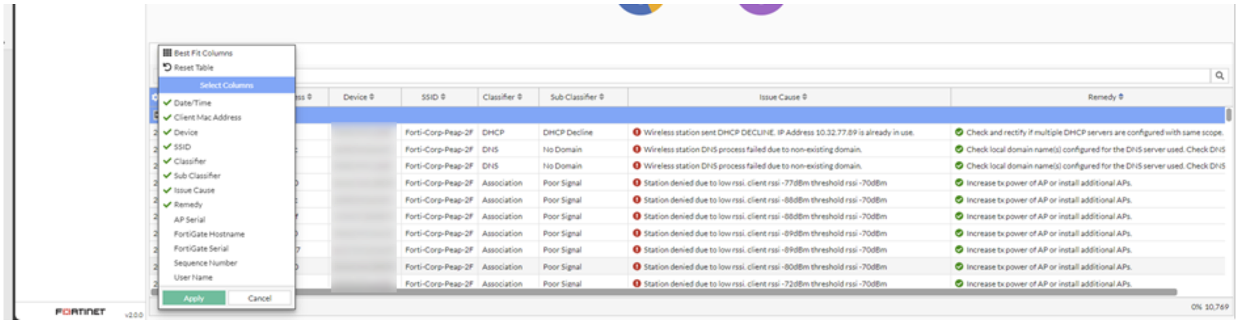
Displays the failed/unsuccessful client connections based on different stages of connection to a network. For example, association failures due to low RSSI, authentication failures due to unreachable RADIUS server, DHCP failure due to a DHCP server process crash, or DNS failure due to an invalid DNS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



To view the topology, click on **Connection Failure** in the impacted SLAs list or click on the bar in the chart.



The **Impacted Clients** 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.

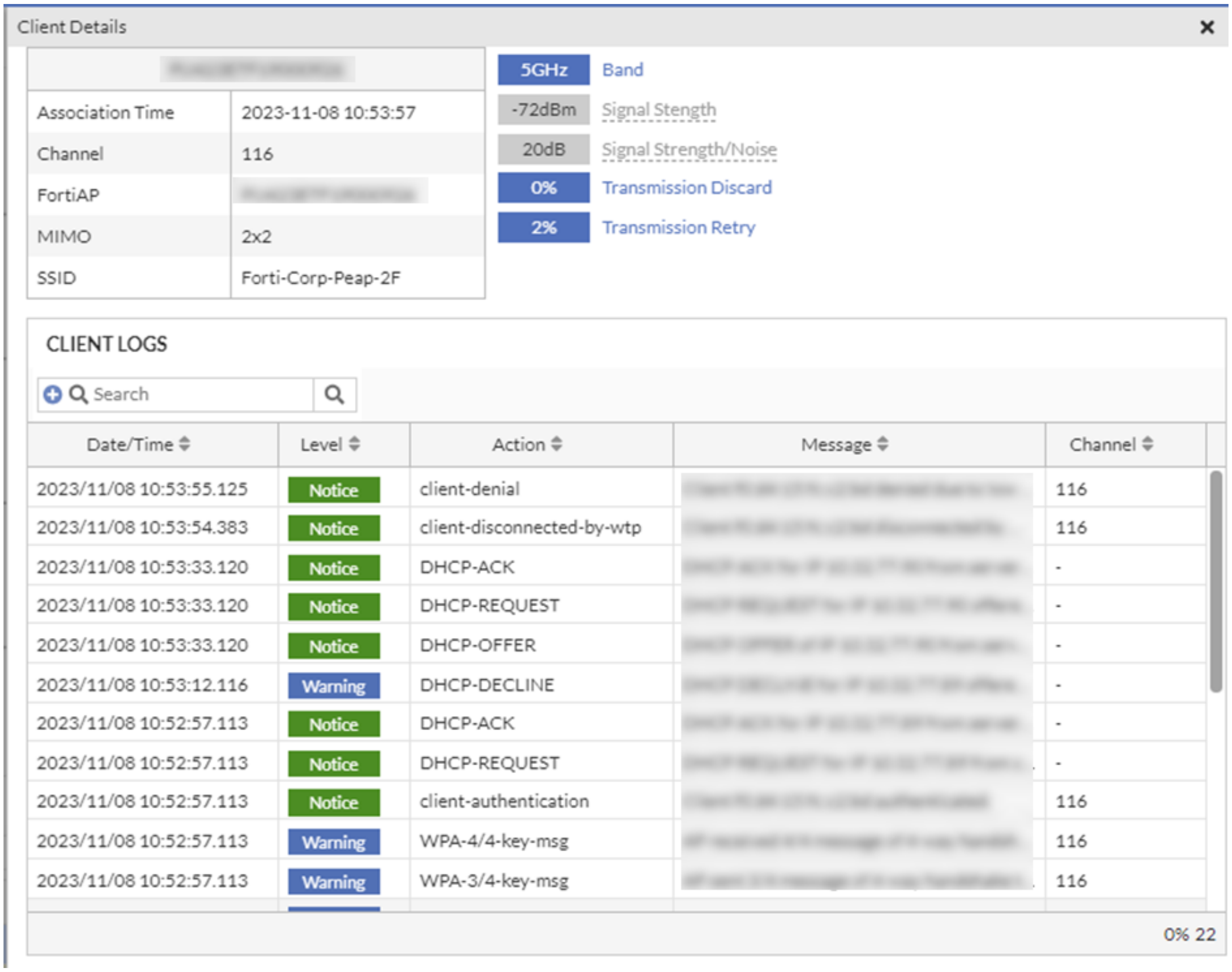


Device	SSID	Classifier	Sub Classifier	Issue Cause	Remedy
[redacted]	Forti-Corp-Peap-2F	DHCP	DHCP Decline	Wireless station sent DHCP DECLINE. IP Address 10.32.77.89 is already in use.	Check and rectify if multiple DHCP servers are configured with same scope.
[redacted]	Forti-Corp-Peap-2F	DNS	No Domain	Wireless station DNS process failed due to non-existing domain.	Check local domain name(s) configured for the DNS server used. Check DNS
[redacted]	Forti-Corp-Peap-2F	DNS	No Domain	Wireless station DNS process failed due to non-existing domain.	Check local domain name(s) configured for the DNS server used. Check DNS
[redacted]	Forti-Corp-Peap-2F	Association	Poor Signal	Station denied due to low rssi. client rssi -77dBm threshold rssi -70dBm	Increase tx power of AP or install additional APs.
[redacted]	Forti-Corp-Peap-2F	Association	Poor Signal	Station denied due to low rssi. client rssi -88dBm threshold rssi -70dBm	Increase tx power of AP or install additional APs.
[redacted]	Forti-Corp-Peap-2F	Association	Poor Signal	Station denied due to low rssi. client rssi -88dBm threshold rssi -70dBm	Increase tx power of AP or install additional APs.
[redacted]	Forti-Corp-Peap-2F	Association	Poor Signal	Station denied due to low rssi. client rssi -89dBm threshold rssi -70dBm	Increase tx power of AP or install additional APs.
[redacted]	Forti-Corp-Peap-2F	Association	Poor Signal	Station denied due to low rssi. client rssi -89dBm threshold rssi -70dBm	Increase tx power of AP or install additional APs.
[redacted]	Forti-Corp-Peap-2F	Association	Poor Signal	Station denied due to low rssi. client rssi -80dBm threshold rssi -70dBm	Increase tx power of AP or install additional APs.
[redacted]	Forti-Corp-Peap-2F	Association	Poor Signal	Station denied due to low rssi. client rssi -72dBm threshold rssi -70dBm	Increase tx power of AP or install additional APs.

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.
Client 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.
Subclassifier	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	detailed cause of the SLA breach that impacted the client/AP/FortiGate.
Remedy	The suggested remedy to resolve the issue.
AP Serial	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.

In the impacted client details displayed for **Successful Connects**, 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.



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

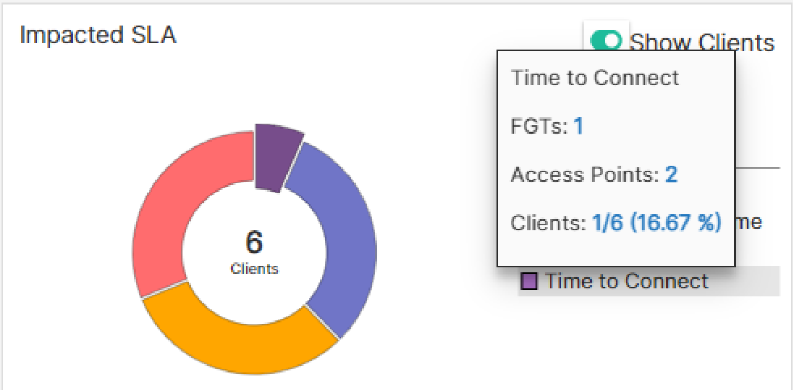
5GHz	Band
-72dBm	Signal Stength
20dB	Signal Strength/Noise
0%	Transmission Discard
2%	Transmission Retry

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

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.



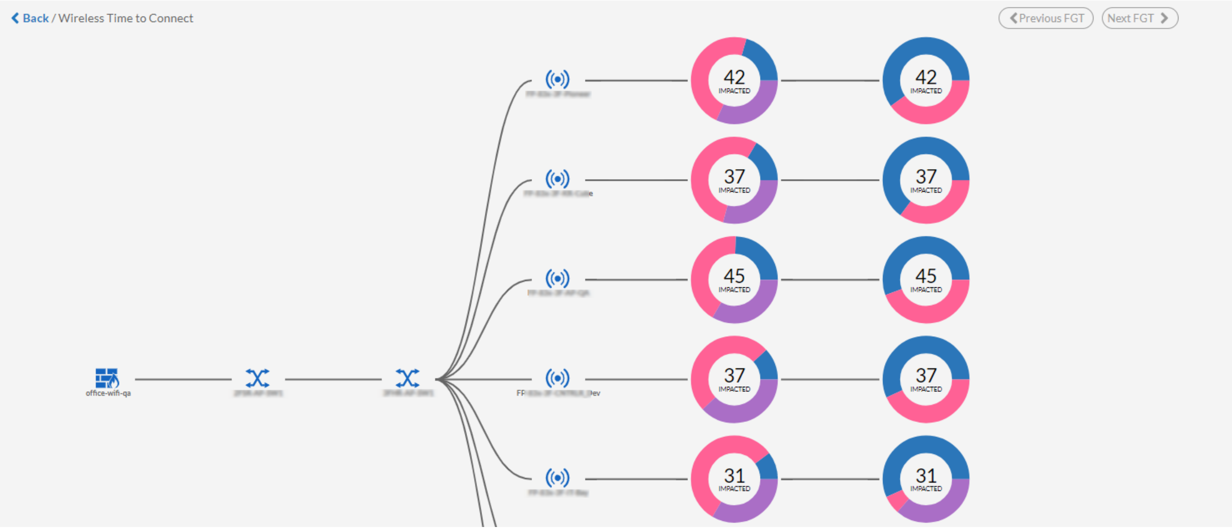
Time to Connect

FGTs: 1

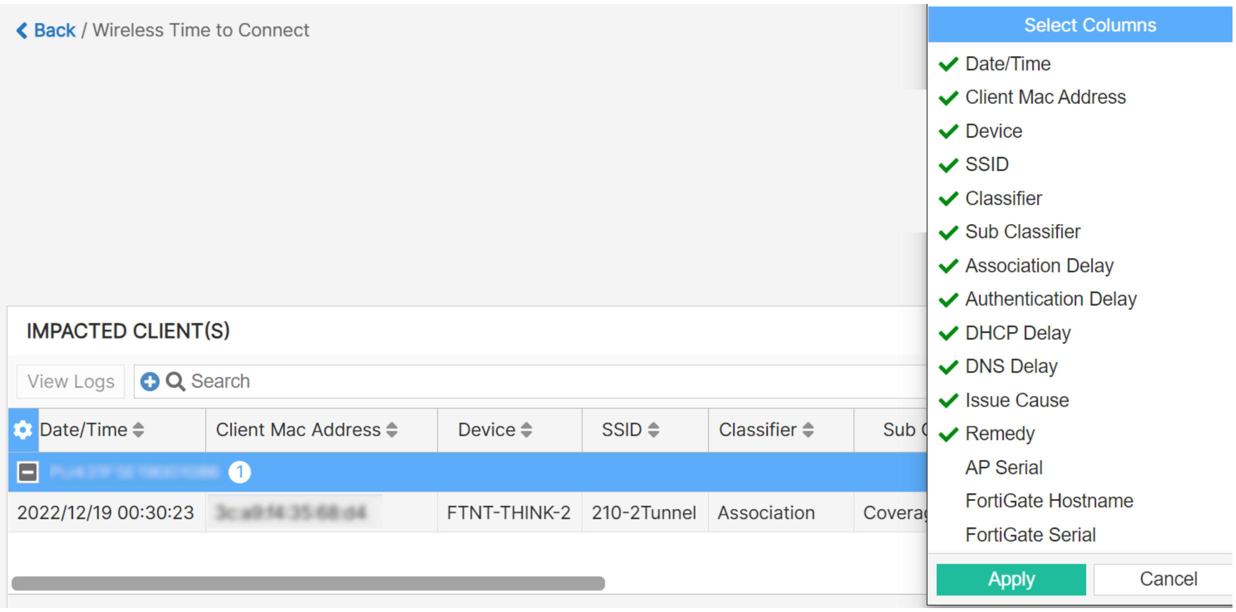
Access Points: 2

Clients: 1/6 (16.67 %)

To view the topology, click on **Time to Connect** in the impacted SLAs list or click on the bar in the chart.



The **Time to Connect** 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. In this image impacted client details for **Time to Connect** are displayed.



Back / Wireless Time to Connect

IMPACTED CLIENT(S)

View Logs | Search

Date/Time	Client Mac Address	Device	SSID	Classifier	Sub C
[redacted] 1					
2022/12/19 00:30:23	[redacted]	FTNT-THINK-2	210-2Tunnel	Association	Coverag

Select Columns

- ✓ Date/Time
- ✓ Client Mac Address
- ✓ Device
- ✓ SSID
- ✓ Classifier
- ✓ Sub Classifier
- ✓ Association Delay
- ✓ Authentication Delay
- ✓ DHCP Delay
- ✓ DNS Delay
- ✓ Issue Cause
- ✓ Remedy
- AP Serial
- FortiGate Hostname
- FortiGate Serial

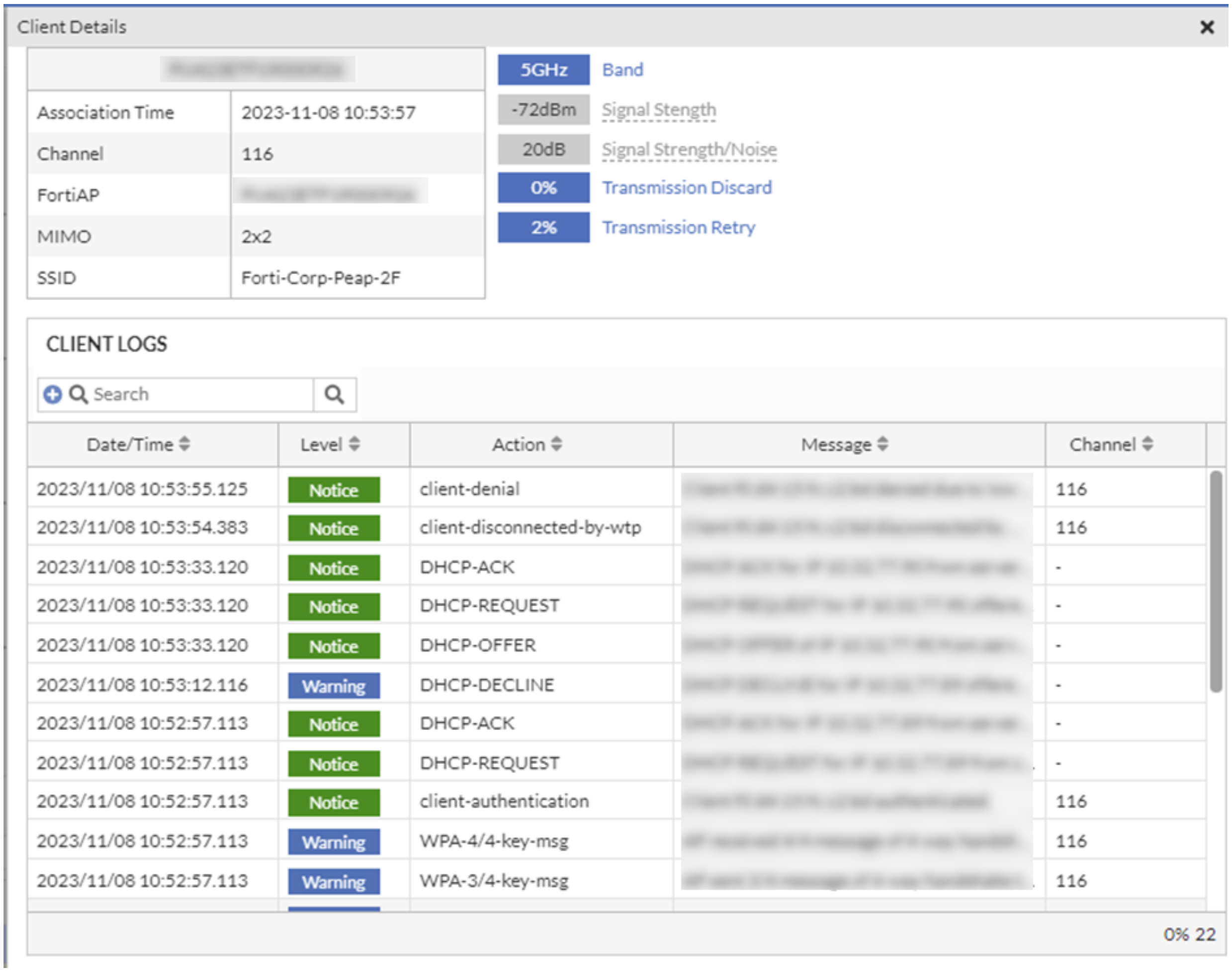
Apply | Cancel

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.
Client 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.

Attribute	Description
SSID	The SSID that the impacted client is associated with.
Classifier	The classifier of the issue reported for the SLA.
Subclassifier	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	detailed cause of the SLA breach that impacted the client/AP/FortiGate.
Remedy	The suggested remedy to resolve the issue.
AP Serial	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.
Authentication Delay	The authentication delay measured in milliseconds.
DNS Delay	The DNS delay measured in milliseconds.
DHCP Delay	The DHCP delay measured in milliseconds.

In the impacted client details displayed for **Time to Connect**, select a specific client 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.



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

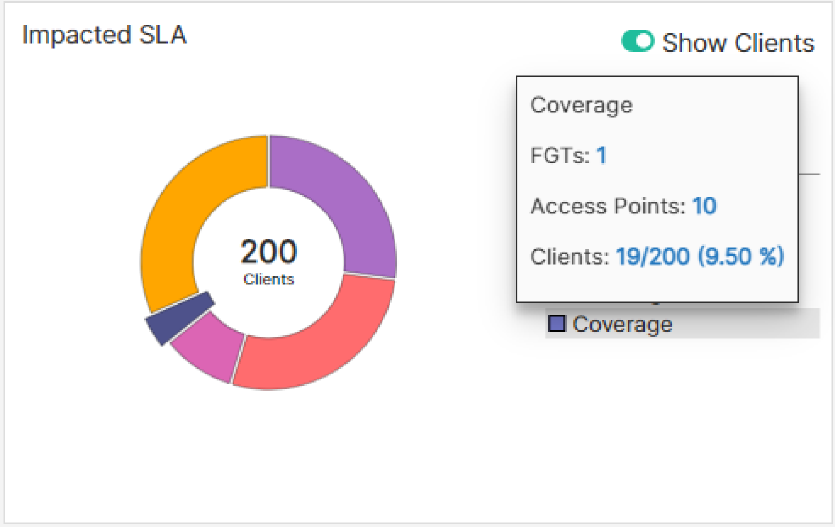
CLIENT LOGS

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

Coverage

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



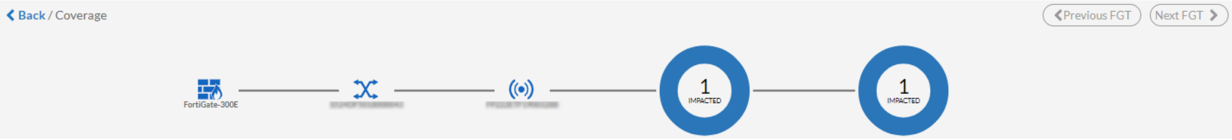
Coverage

FGTs: 1

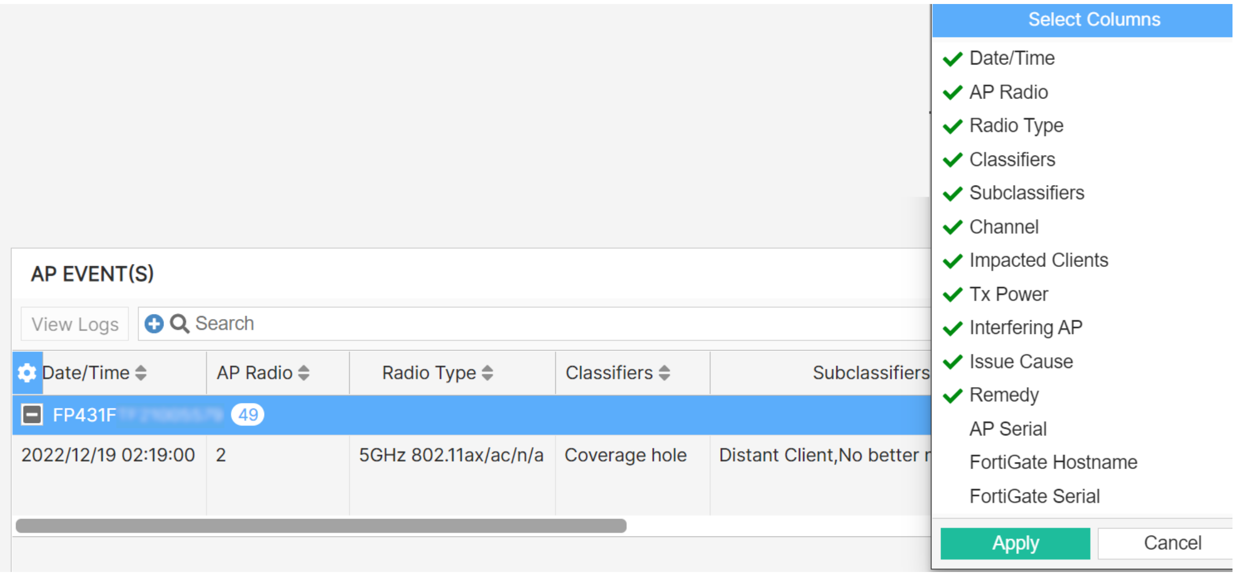
Access Points: 10

Clients: 19/200 (9.50 %)

To view the topology, click on **Coverage** in the impacted SLAs list or click on the bar in the chart.



The **AP Events** 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.



Date/Time	AP Radio	Radio Type	Classifiers	Subclassifiers
FP431F [redacted] 49				
2022/12/19 02:19:00	2	5GHz 802.11ax/ac/n/a	Coverage hole	Distant Client,No better r

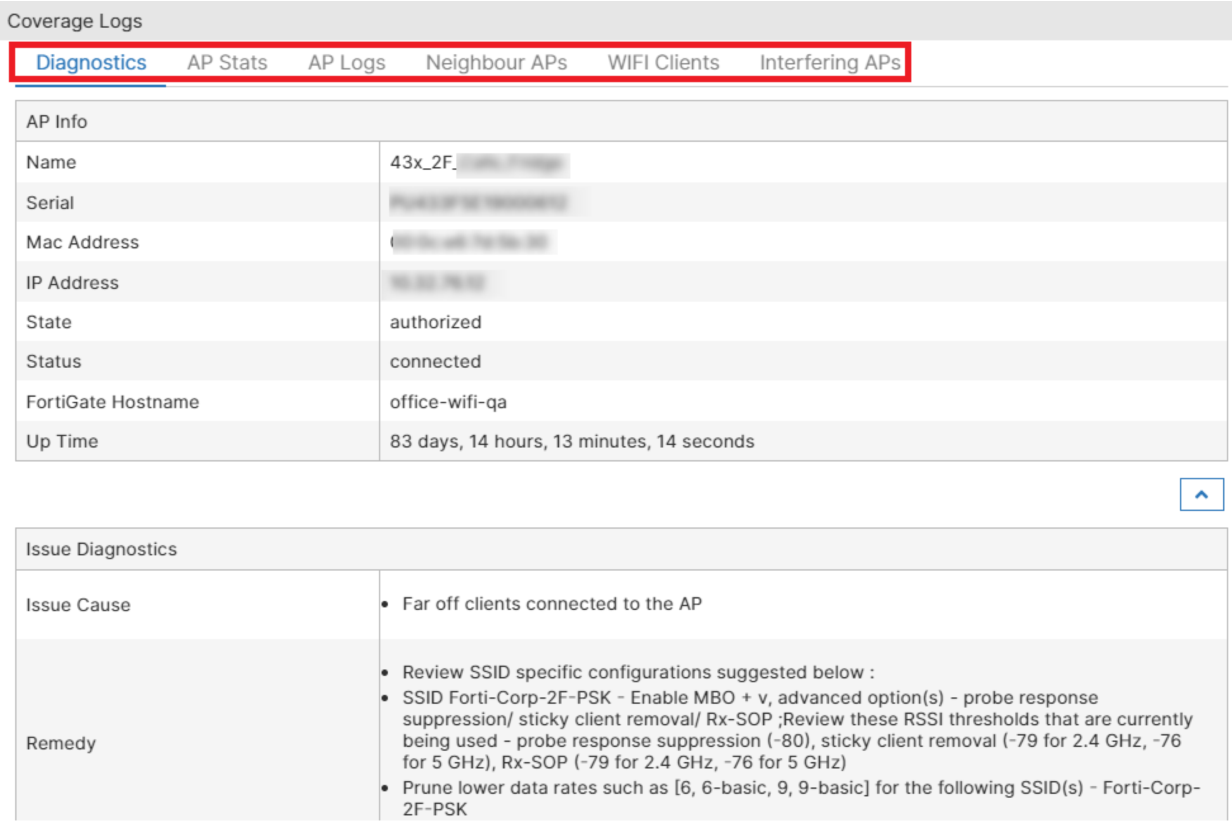
Select Columns

- ✓ Date/Time
- ✓ AP Radio
- ✓ Radio Type
- ✓ Classifiers
- ✓ Subclassifiers
- ✓ Channel
- ✓ Impacted Clients
- ✓ Tx Power
- ✓ Interfering AP
- ✓ Issue Cause
- ✓ Remedy
- AP Serial
- FortiGate Hostname
- FortiGate Serial

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.
Classifier	The classifier of the issue reported for the SLA.
Subclassifier	The sub-classifier of the issue for the reported classifier.
Issue Cause	detailed cause of the SLA breach that impacted the client/AP/FortiGate.
Remedy	The suggested remedy to resolve the issue.
AP Radio	The AP radio that the client associated with.
AP Serial	The AP serial number that the client associated with.
Tx Power	The Tx power of the AP at the time of impact.
FortiGate Hostname	The hostname of the FortiGate associated with the AP/impacted client.
FortiGate Serial	The serial number of the associated FortiGate.
Radio Type	The impacted radio and band associated with the client.
Channel	The channel at which the client connected.
Impacted Clients	The number of impacted clients.

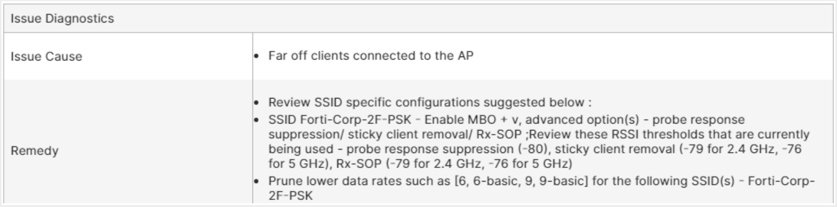
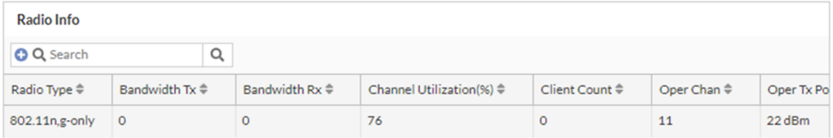
To view the logs, select a specific row of an AP event and click **View Logs**. You can view coverage logs related to **Diagnostics** with the issue description and the suggested remediation, **AP Stats** with the associated AP radio details, **AP Logs** with the time of the throughput failure event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

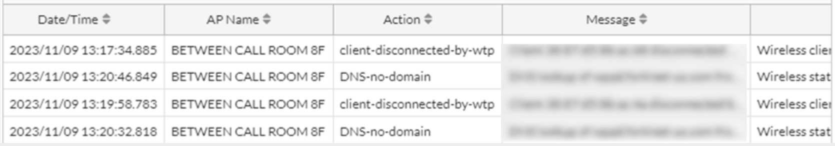
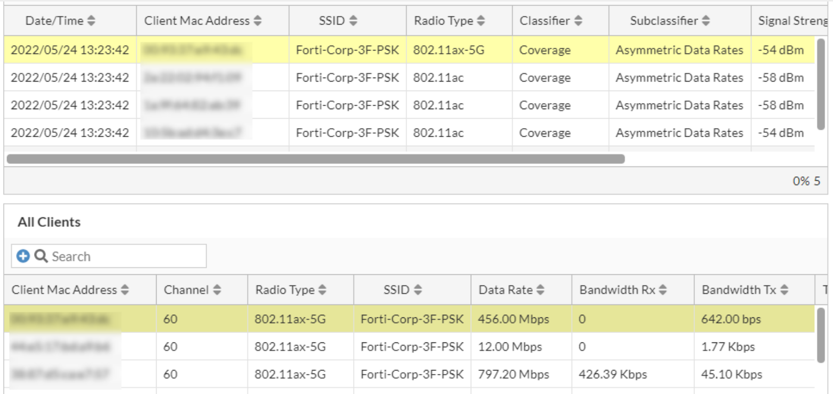
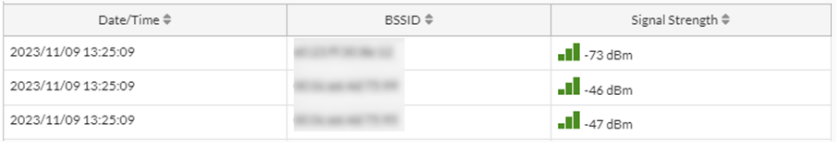


Coverage Logs

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
AP Stats	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 Radio Type: 802.11n,g-only Bandwidth Tx: 0 Bandwidth Rx: 0 Channel Utilization(%): 76 Client Count: 0 Oper Chan: 11 Oper Tx Po: 22 dBm

Logs	Description
AP Logs	This tab provides the AP event logs generated from FortiGate. 
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. 

Date/Time ⇕	AP Name ⇕	Action ⇕	Message ⇕	
2023/11/09 13:17:34.885	BETWEEN CALL ROOM 8F	client-disconnected-by-wtp	[redacted]	Wireless clie
2023/11/09 13:20:46.849	BETWEEN CALL ROOM 8F	DNS-no-domain	[redacted]	Wireless stat
2023/11/09 13:19:58.783	BETWEEN CALL ROOM 8F	client-disconnected-by-wtp	[redacted]	Wireless clie
2023/11/09 13:20:32.818	BETWEEN CALL ROOM 8F	DNS-no-domain	[redacted]	Wireless stat

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

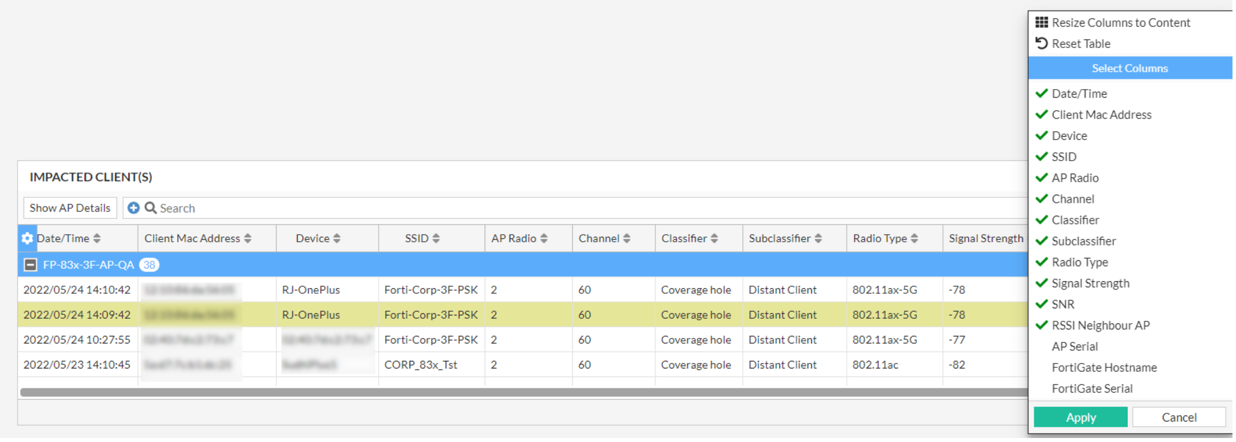
0% 5

All Clients

Client Mac Address ⇕	Channel ⇕	Radio Type ⇕	SSID ⇕	Data Rate ⇕	Bandwidth Rx ⇕	Bandwidth Tx ⇕	T
[redacted]	60	802.11ax-5G	Forti-Corp-3F-PSK	456.00 Mbps	0	642.00 bps	
[redacted]	60	802.11ax-5G	Forti-Corp-3F-PSK	12.00 Mbps	0	1.77 Kbps	
[redacted]	60	802.11ax-5G	Forti-Corp-3F-PSK	797.20 Mbps	426.39 Kbps	45.10 Kbps	

Date/Time ⇕	BSSID ⇕	Signal Strength ⇕
2023/11/09 13:25:09	[redacted]	-73 dBm
2023/11/09 13:25:09	[redacted]	-46 dBm
2023/11/09 13:25:09	[redacted]	-47 dBm

The donut charts in the topology provide the count of the impacted clients associated with each AP. Click on any of these charts to view the impacted client details per AP.



IMPACTED CLIENT(S)

Date/Time ⇕	Client Mac Address ⇕	Device ⇕	SSID ⇕	AP Radio ⇕	Channel ⇕	Classifier ⇕	Subclassifier ⇕	Radio Type ⇕	Signal Strength
FP-83x-3F-AP-QA 38									
2022/05/24 14:10:42	[redacted]	RJ-OnePlus	Forti-Corp-3F-PSK	2	60	Coverage hole	Distant Client	802.11ax-5G	-78
2022/05/24 14:09:42	[redacted]	RJ-OnePlus	Forti-Corp-3F-PSK	2	60	Coverage hole	Distant Client	802.11ax-5G	-78
2022/05/24 10:27:55	[redacted]	[redacted]	Forti-Corp-3F-PSK	2	60	Coverage hole	Distant Client	802.11ax-5G	-77
2022/05/23 14:10:45	[redacted]	[redacted]	CORP_83x_Tst	2	60	Coverage hole	Distant Client	802.11ac	-82

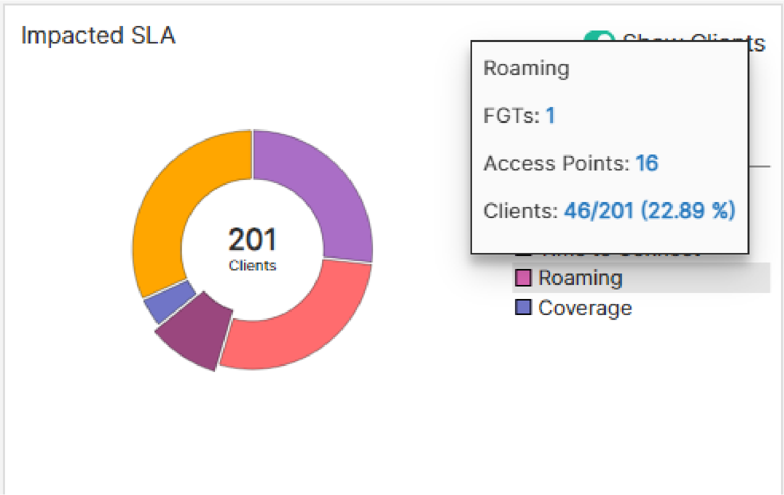
Right-click on the header of the table to select the following columns that you wish to view.

Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
Client 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.
Radio Type	The impacted radio and band information associated with the client.
Classifier	The classifier of the issue reported for the SLA.
Subclassifier	The sub-classifier of the issue for the reported classifier.
Signal Strength	The signal strength of the client at the time of impact.
AP Radio	The AP radio that the client associated with.
AP Serial	The AP serial number that the client associated with.
Channel	The channel at which the client connected.
FortiGate Hostname	The hostname of the FortiGate associated with the AP/impacted client.
FortiGate Serial	The serial number of the associated FortiGate.
RSSI Neighbour AP	The highest neighbour AP RSSI.
SNR	The client SNR reported at the time of impact.

For more details on each of these tabs, see **View Logs** described earlier in the section.

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.



Impacted SLA

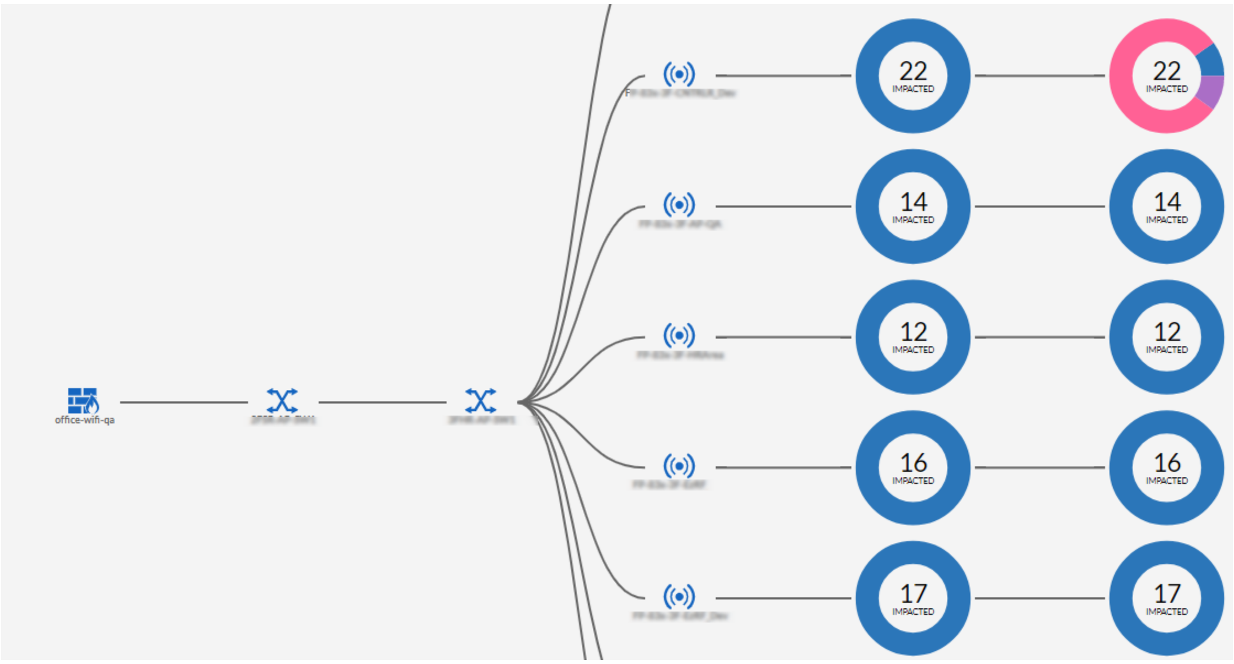
Roaming

FGTs: 1

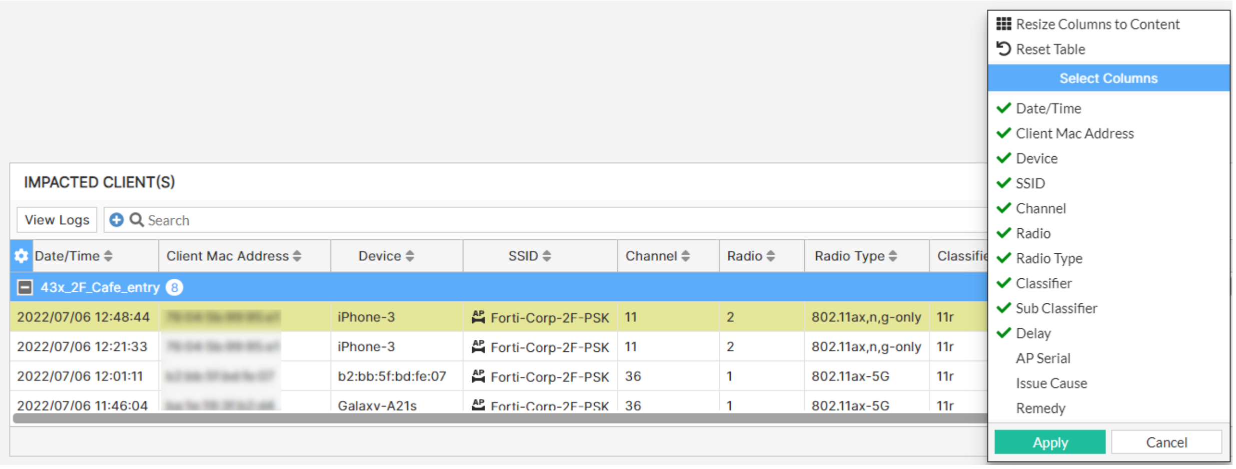
Access Points: 16

Clients: 46/201 (22.89 %)

To view the topology, click on **Roaming** in the impacted SLAs list or click on the bar in the chart.



The **Impacted Clients** 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.



IMPACTED CLIENT(S)

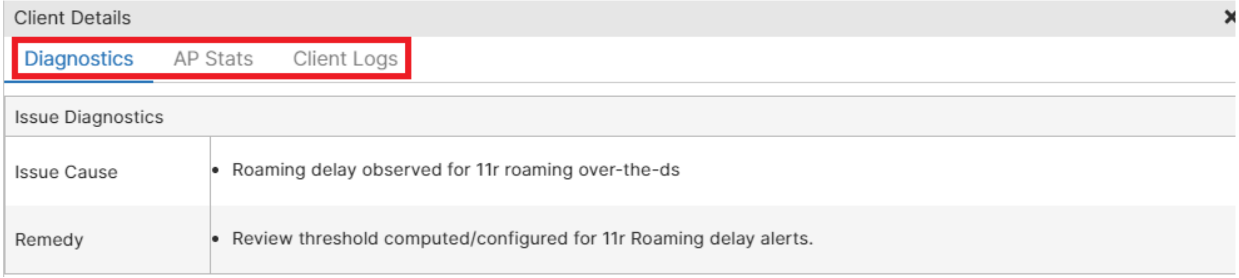
View Logs | Search

Date/Time	Client Mac Address	Device	SSID	Channel	Radio	Radio Type	Classifie
43x_2F_Cafe_entry 8							
2022/07/06 12:48:44	[redacted]	iPhone-3	Forti-Corp-2F-PSK	11	2	802.11ax,n,g-only	11r
2022/07/06 12:21:33	[redacted]	iPhone-3	Forti-Corp-2F-PSK	11	2	802.11ax,n,g-only	11r
2022/07/06 12:01:11	[redacted]	b2:bb:5f:bd:fe:07	Forti-Corp-2F-PSK	36	1	802.11ax-5G	11r
2022/07/06 11:46:04	[redacted]	Galaxy-A21s	Forti-Corp-2F-PSK	36	1	802.11ax-5G	11r

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

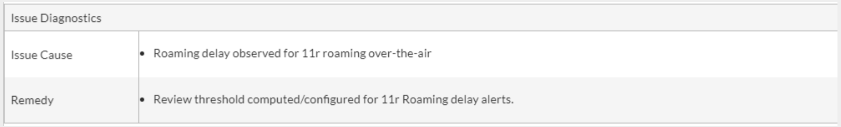
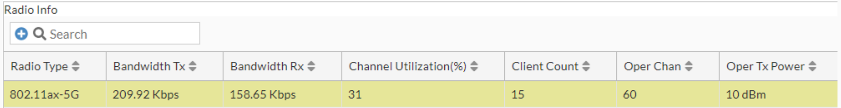
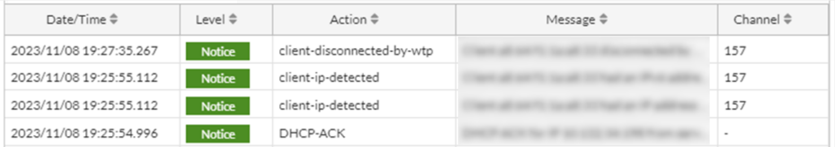
Attribute	Description
Date/Time	The date and time of the impact as per your timezone.
Client MAC Address	The MAC address of the impacted client device.
Device	The name of the device as configured by the user. If the name is not configured or available, then MAC address is displayed.
SSID	The SSID that the impacted client is associated with.
Classifier	The classifier of the issue reported for the SLA.
Subclassifier	The sub-classifier of the issue for the reported classifier.
Delay (ms)	The delay (latency) in client roaming (milliseconds) in case of threshold breach.
Radio	The AP radio that the client associated with.
AP Serial	The AP serial number that the client associated with.
Channel	The channel at which the AP/client were operating.
Issue Cause	detailed cause of the SLA breach that impacted the client/AP/FortiGate.
Remedy	The suggested remedy to resolve the issue.

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

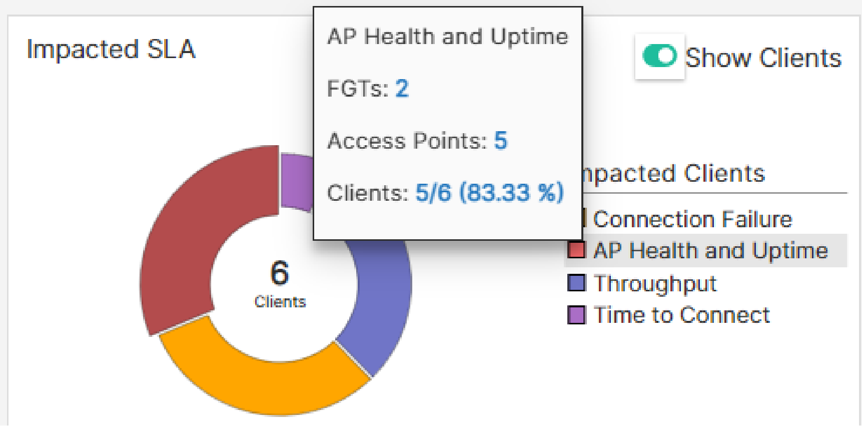
Issue Cause	- Roaming delay observed for 11r roaming over-the-ds
Remedy	- Review threshold computed/configured for 11r Roaming delay alerts.

<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. FortiAIOps also suggests the remedy to resolve the issue.

<table>
<tr><th colspan="2">Issue Diagnostics</th></tr>
<tr><td>Issue Cause</td><td>• Roaming delay observed for 11r roaming over-the-air</td></tr>
<tr><td>Remedy</td><td>• Review threshold computed/configured for 11r Roaming delay alerts.</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.

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 Power</th></tr>
<tr><td>802.11ax-5G</td><td>209.92 Kbps</td><td>158.65 Kbps</td><td>31</td><td>15</td><td>60</td><td>10 dBm</td></tr>
</table></td></tr>
<tr><td><b>Client Logs</b></td><td>This tab provides client event logs.

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

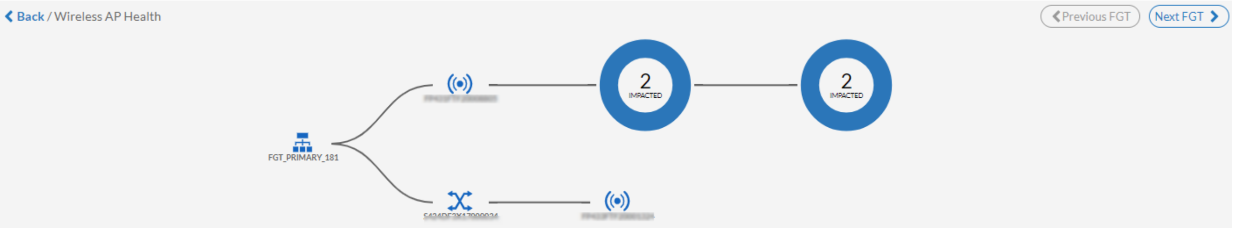
In the various throughput logs displayed, you can right-click on the table header to select the details you want to view.

AP Health and Uptime

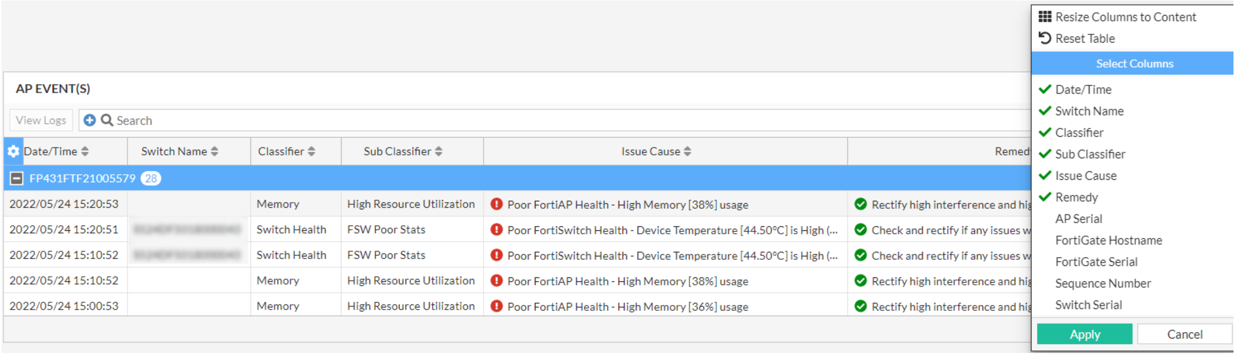
Displays the AP health based on the configured AP health threshold values and the AP down status due to AP/FortiGate reboot, disabled switch port etc. For SLA configurations, see Device Health.



To view the topology, click on **AP Health and Uptime** in the impacted SLAs list or click on the bar in the chart.



The **AP Events** 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.



AP EVENT(S)

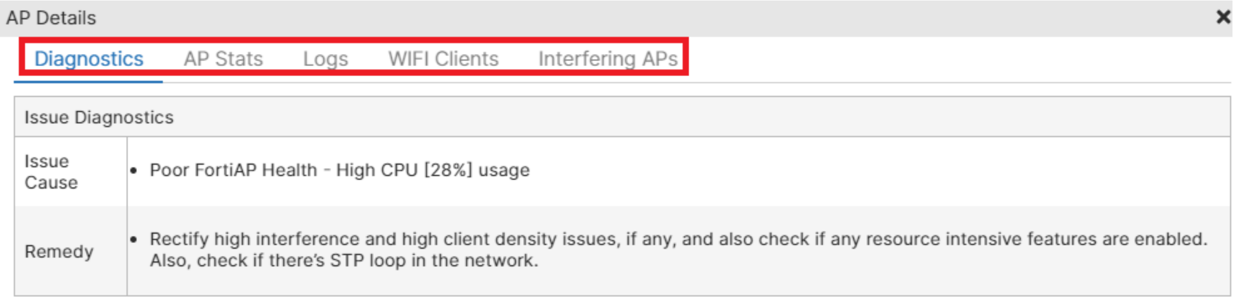
View Logs | Search

Date/Time	Switch Name	Classifier	Sub Classifier	Issue Cause	Remed
FP431FTF21005579 28					
2022/05/24 15:20:53		Memory	High Resource Utilization	Poor FortiAP Health - High Memory [38%] usage	Rectify high interference and hig
2022/05/24 15:20:51	[redacted]	Switch Health	FSW Poor Stats	Poor FortiSwitch Health - Device Temperature [44.50°C] is High (...	Check and rectify if any issues w
2022/05/24 15:10:52	[redacted]	Switch Health	FSW Poor Stats	Poor FortiSwitch Health - Device Temperature [44.50°C] is High (...	Check and rectify if any issues w
2022/05/24 15:10:52		Memory	High Resource Utilization	Poor FortiAP Health - High Memory [38%] usage	Rectify high interference and hig
2022/05/24 15:00:53		Memory	High Resource Utilization	Poor FortiAP Health - High Memory [36%] usage	Rectify high interference and hig

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.
Switch Name	The name of the switch associated with the impacted AP/client.
Issue Cause	detailed cause of the SLA breach that impacted the client/AP/FortiGate.
Remedy	The suggested remedy to resolve the issue.
Classifier	The classifier of the issue reported for the SLA.
Subclassifier	The sub-classifier of the issue for the reported classifier.
AP Serial	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.
Switch Serial	The serial number of the switch associated with the impacted AP/client.

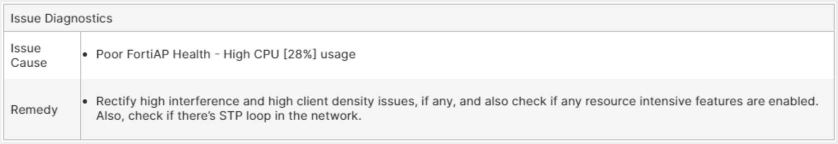
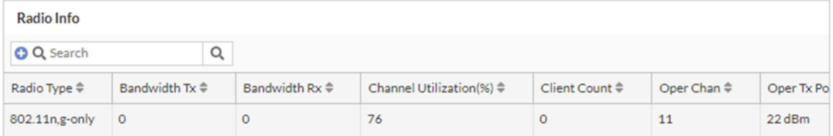
In the AP events displayed, select an event and click **View Logs**.

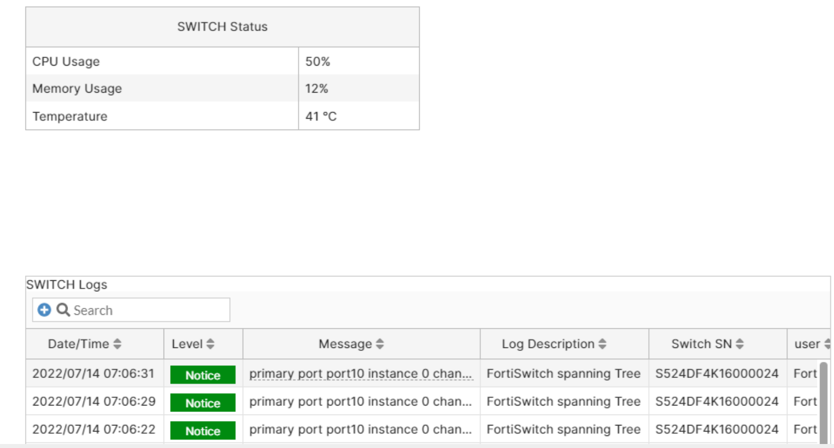


Issue Diagnostics

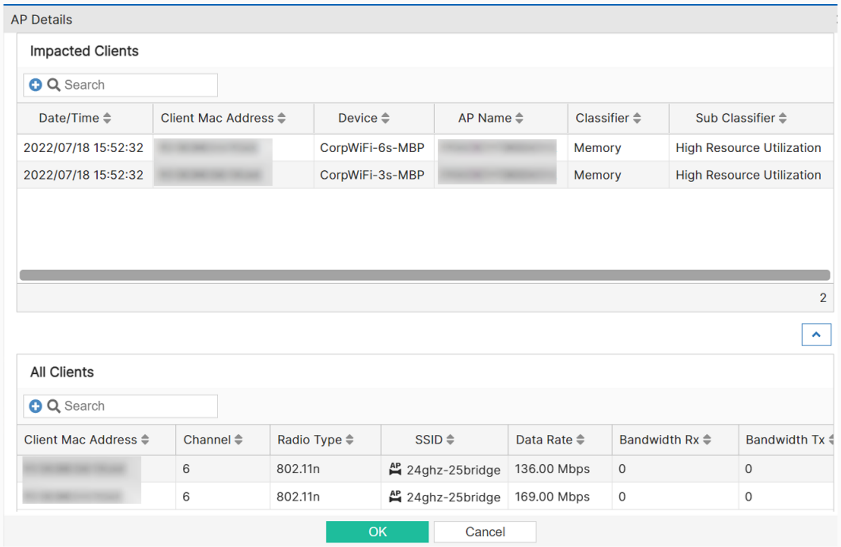
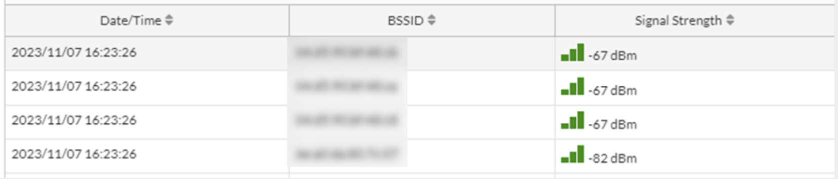
Issue Cause	• Poor FortiAP Health - High CPU [28%] usage
Remedy	• Rectify high interference and high client density issues, if any, and also check if any resource intensive features are enabled. Also, check if there's STP loop in the network.

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.

<table>
<tr><th>Logs</th><th>Description</th></tr>
<tr><td></td><td>

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

<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>

<table>
<tr><th colspan="2">SWITCH Status</th></tr>
<tr><td>CPU Usage</td><td>50%</td></tr>
<tr><td>Memory Usage</td><td>12%</td></tr>
<tr><td>Temperature</td><td>41 °C</td></tr>
</table>
SWITCH Logs

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

Logs	Description
	
Interfering APs	This tab displays details of the interfering APs in your network. 

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

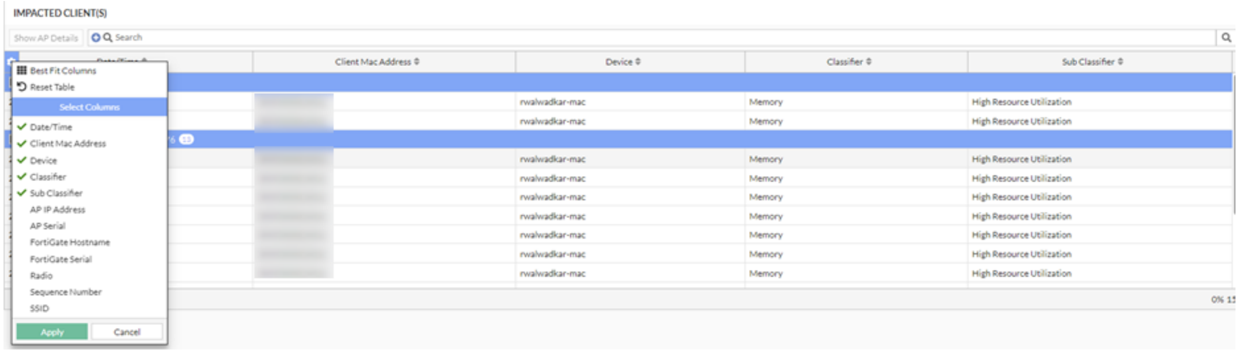
All Clients

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

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

The donut charts in the topology provide the count of the impacted clients associated with each AP. Click on any of these charts to view the impacted client details per AP.



IMPACTED CLIENT(S)

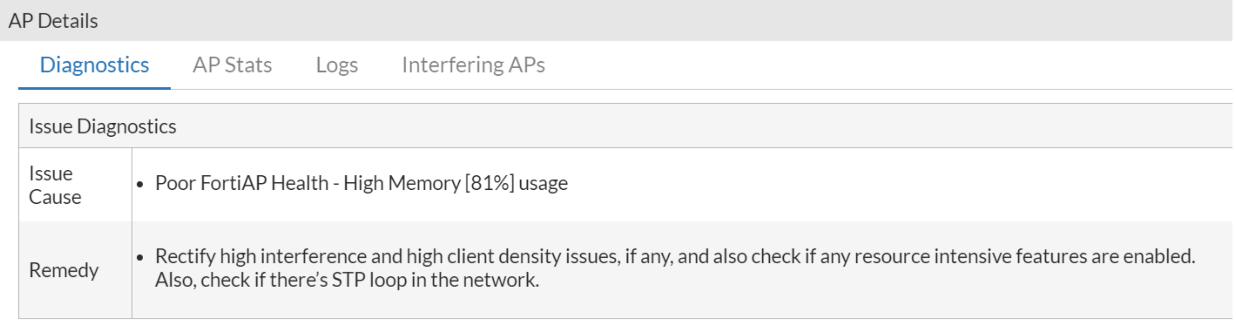
Date/Time	Client Mac Address	Device	Classifier	Sub Classifier
	[redacted]	rwalwadkar-mac	Memory	High Resource Utilization
	[redacted]	rwalwadkar-mac	Memory	High Resource Utilization
	[redacted]	rwalwadkar-mac	Memory	High Resource Utilization
	[redacted]	rwalwadkar-mac	Memory	High Resource Utilization
	[redacted]	rwalwadkar-mac	Memory	High Resource Utilization
	[redacted]	rwalwadkar-mac	Memory	High Resource Utilization
	[redacted]	rwalwadkar-mac	Memory	High Resource Utilization
	[redacted]	rwalwadkar-mac	Memory	High Resource Utilization
	[redacted]	rwalwadkar-mac	Memory	High Resource Utilization

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.
Client 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.

Attribute	Description
SSID	The SSID that the impacted client is associated with.
Classifier	The classifier of the issue reported for the SLA.
Subclassifier	The sub-classifier of the issue for the reported classifier.
AP IP Address	The IP address of the impacted AP.
Radio	The AP radio that the client associated with.
AP Serial	The AP serial number that the client associated with.
Channel	The channel at which the client connected.
FortiGate Hostname	The hostname of the FortiGate associated with the AP/impacted client.
FortiGate Serial	The serial number of the associated FortiGate.

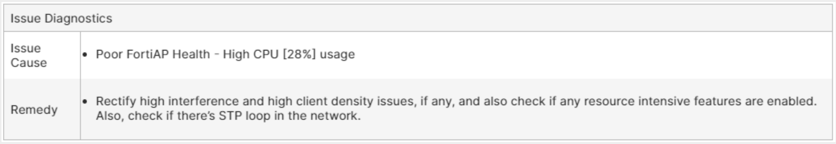
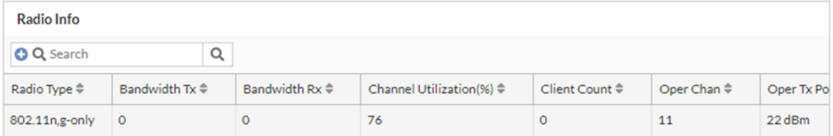
Select any impacted client and click **Show AP details** to view the detailed AP logs.

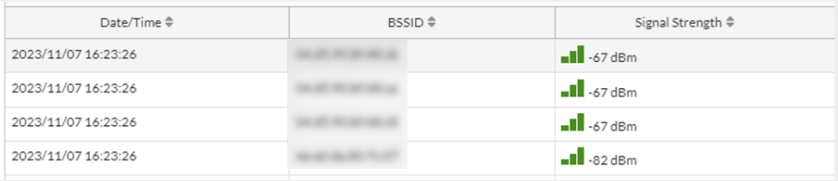


Issue Diagnostics

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.

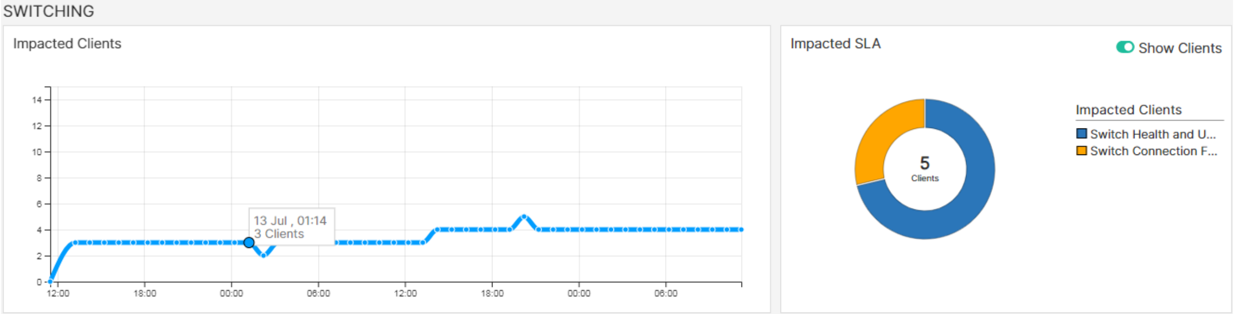
Select any of the tabs to view the data described in this table.

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: • 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.
AP Stats	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 Radio Type: 802.11n,g-only Bandwidth Tx: 0 Bandwidth Rx: 0 Channel Utilization(%): 76 Client Count: 0 Oper Chan: 11 Oper Tx Po: 22 dBm
Interfering APs	This tab displays details of the interfering APs in your network.

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
Logs	This tab provides the AP event logs generated from FortiGate.

Switching

The Switching panel displays the total number of impacted clients and SLA data. In the impacted SLA panel, you can select **Show Clients** to view the impacted client count or click **Show Switches** to view the impacted switch count.



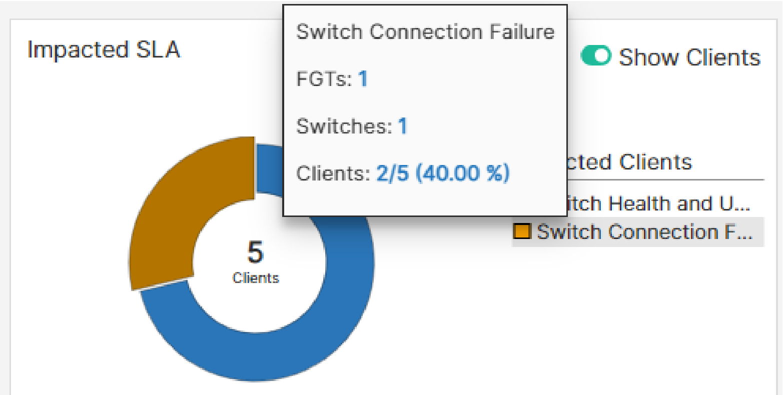
SLAs, Topology and Logs

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. In each impacted SLA panel, you can select **Show Clients** to view the impacted client count or click **Show Switches** to view the impacted switch count.

- Switch Connection Failure
- Switch Health and Uptime

Switch Connection Failure

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



Impacted SLA

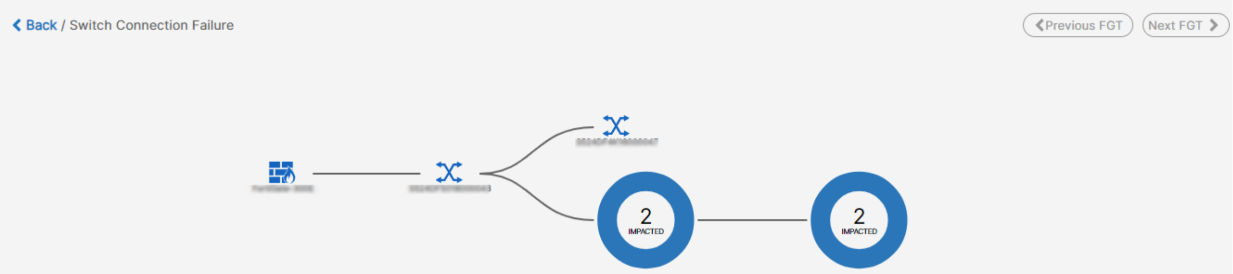
Switch Connection Failure

FGTs: 1

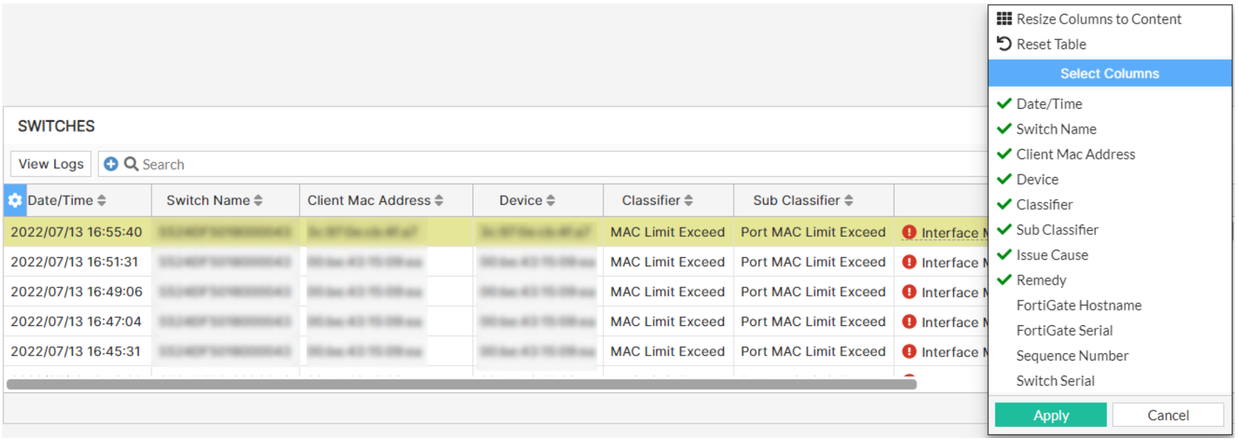
Switches: 1

Clients: 2/5 (40.00 %)

To view the topology, click on **Switch Connection Failure** in the impacted SLAs list or click on the bar in the chart.



The **Switches** table displays information such as the switch details for reported classifiers and sub-classifiers, issue description and the suggested remediation measure, and so on are displayed.



SWITCHES

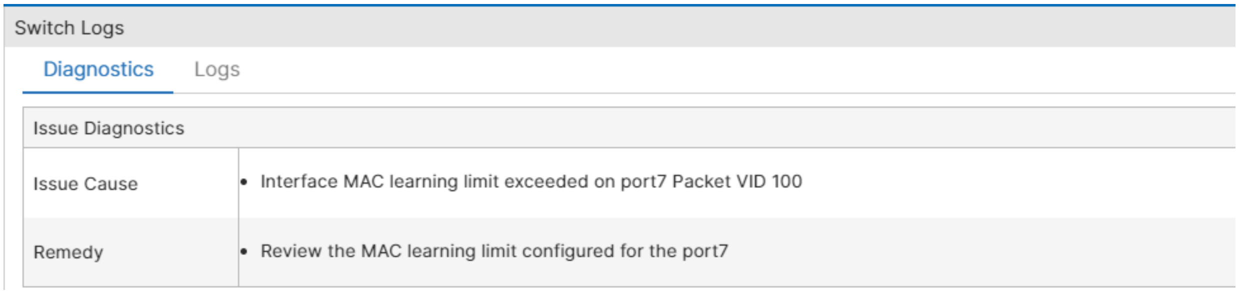
Date/Time	Switch Name	Client Mac Address	Device	Classifier	Sub Classifier	
2022/07/13 16:55:40	[redacted]	[redacted]	[redacted]	MAC Limit Exceed	Port MAC Limit Exceed	Interface
2022/07/13 16:51:31	[redacted]	[redacted]	[redacted]	MAC Limit Exceed	Port MAC Limit Exceed	Interface
2022/07/13 16:49:06	[redacted]	[redacted]	[redacted]	MAC Limit Exceed	Port MAC Limit Exceed	Interface
2022/07/13 16:47:04	[redacted]	[redacted]	[redacted]	MAC Limit Exceed	Port MAC Limit Exceed	Interface
2022/07/13 16:45:31	[redacted]	[redacted]	[redacted]	MAC Limit Exceed	Port MAC Limit Exceed	Interface

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.
Switch Name	The name of the impacted switch.
Client 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

Attribute	Description
	configured or available, then MAC address is displayed.
Issue Cause	Detailed cause of the SLA breach that impacted the client/switch.
Remedy	The suggested remedy to resolve the issue.
Classifier	The classifier of the issue reported for the SLA.
Subclassifier	The sub-classifier of the issue for the reported classifier.
FortiGate Hostname	The hostname of the FortiGate associated with the impacted client.
FortiGate Serial	The serial number of the FortiGate associated with the impacted client.
Switch Serial	The serial number of the impacted switch.

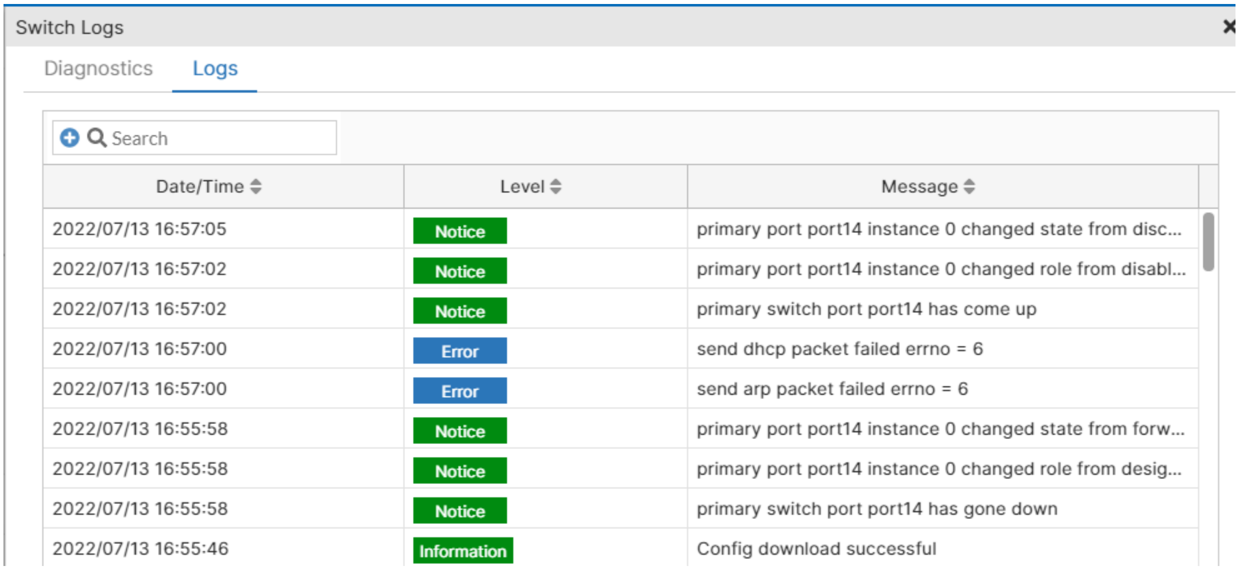
Select a particular switch and click **View Logs**, the issue diagnostics and the suggested remedy are displayed.



Issue Diagnostics

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

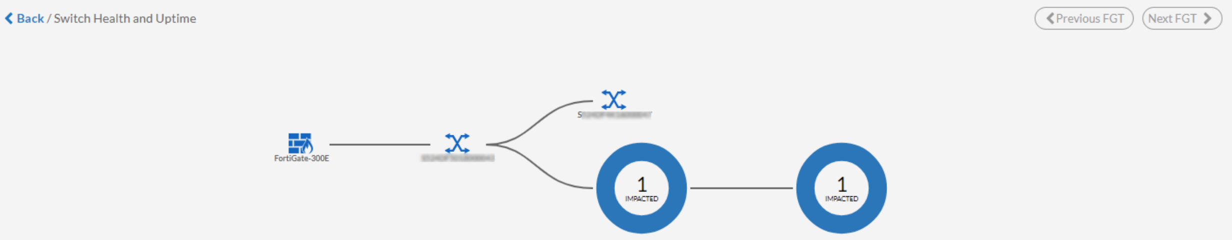
The **Logs** tab displays the time stamp of each action, the type of action such as notice, warning, etc., and the impact details are displayed. Different data tabs are displayed based on the selected issue/failure.



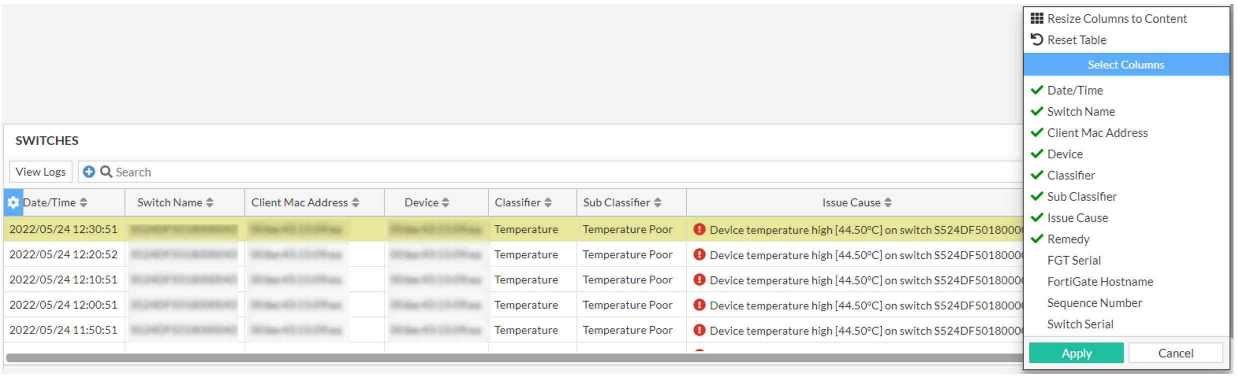
Date/Time	Level	Message
2022/07/13 16:57:05	Notice	primary port port14 instance 0 changed state from disc...
2022/07/13 16:57:02	Notice	primary port port14 instance 0 changed role from disabl...
2022/07/13 16:57:02	Notice	primary switch port port14 has come up
2022/07/13 16:57:00	Error	send dhcp packet 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

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.



The impacted switch details such as the switch serial number, MAC address, issue classifier and sub-classifier, the issues description, and suggested remediation are displayed.

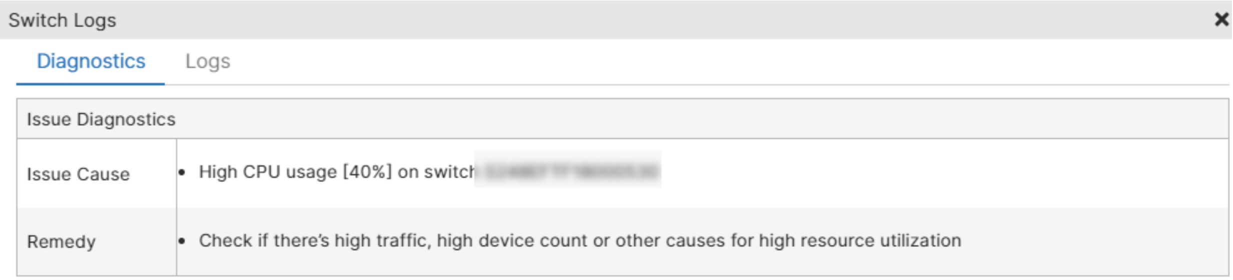


Date/Time	Switch Name	Client Mac Address	Device	Classifier	Sub Classifier	Issue Cause
2022/05/24 12:30:51	[redacted]	[redacted]	[redacted]	Temperature	Temperature Poor	Device temperature high [44.50°C] on switch S524DF5018000
2022/05/24 12:20:52	[redacted]	[redacted]	[redacted]	Temperature	Temperature Poor	Device temperature high [44.50°C] on switch S524DF5018000
2022/05/24 12:10:51	[redacted]	[redacted]	[redacted]	Temperature	Temperature Poor	Device temperature high [44.50°C] on switch S524DF5018000
2022/05/24 12:00:51	[redacted]	[redacted]	[redacted]	Temperature	Temperature Poor	Device temperature high [44.50°C] on switch S524DF5018000
2022/05/24 11:50:51	[redacted]	[redacted]	[redacted]	Temperature	Temperature Poor	Device temperature high [44.50°C] on switch S524DF5018000

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.
Switch Name	The name of the impacted switch.
Client 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.
Issue Cause	Detailed cause of the SLA breach that impacted the client/switch.
Remedy	The suggested remedy to resolve the issue.
Classifier	The classifier of the issue reported for the SLA.
Subclassifier	The sub-classifier of the issue for the reported classifier.
FortiGate Hostname	The hostname of the FortiGate associated with the impacted client.
Switch Serial	The serial number of the impacted switch.

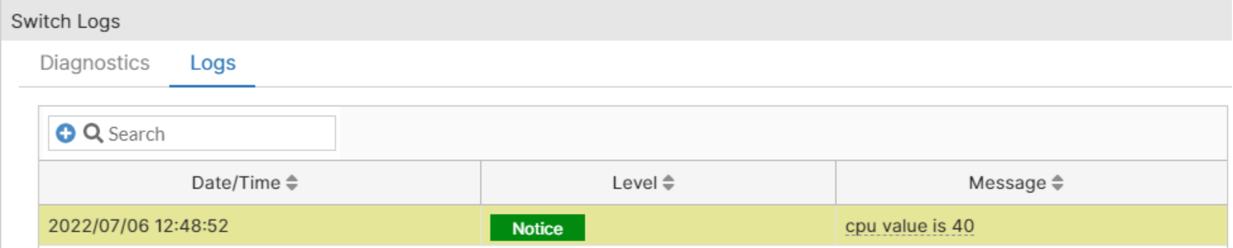
Select a particular switch and click **View Logs**, the issue diagnostics and the suggested remedy are displayed.



Switch Logs

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.

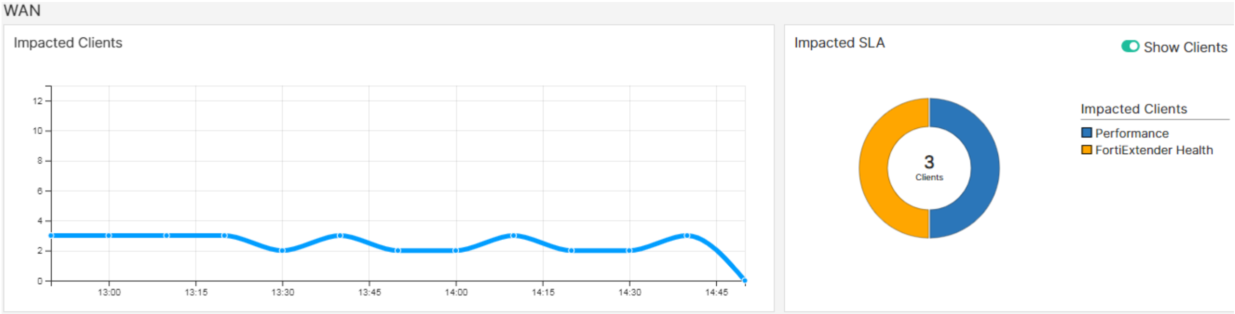


Switch Logs

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

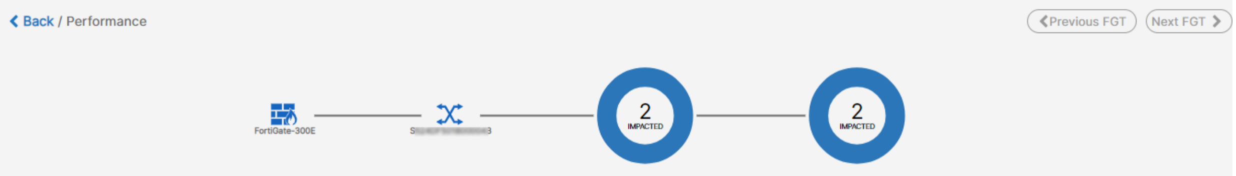
WAN

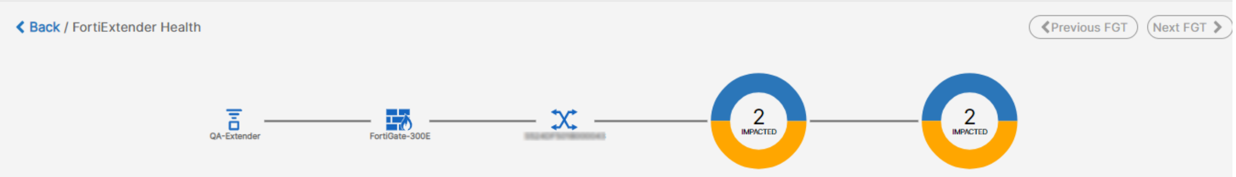
The WAN panel displays the performance SLA metrics to monitor WAN member interface link quality and to detect failures and FortiExtender health data, along with the impacted client details. Any client that breaches the configured SLA thresholds are reported. In each SLA panel, you can select **Show Clients**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



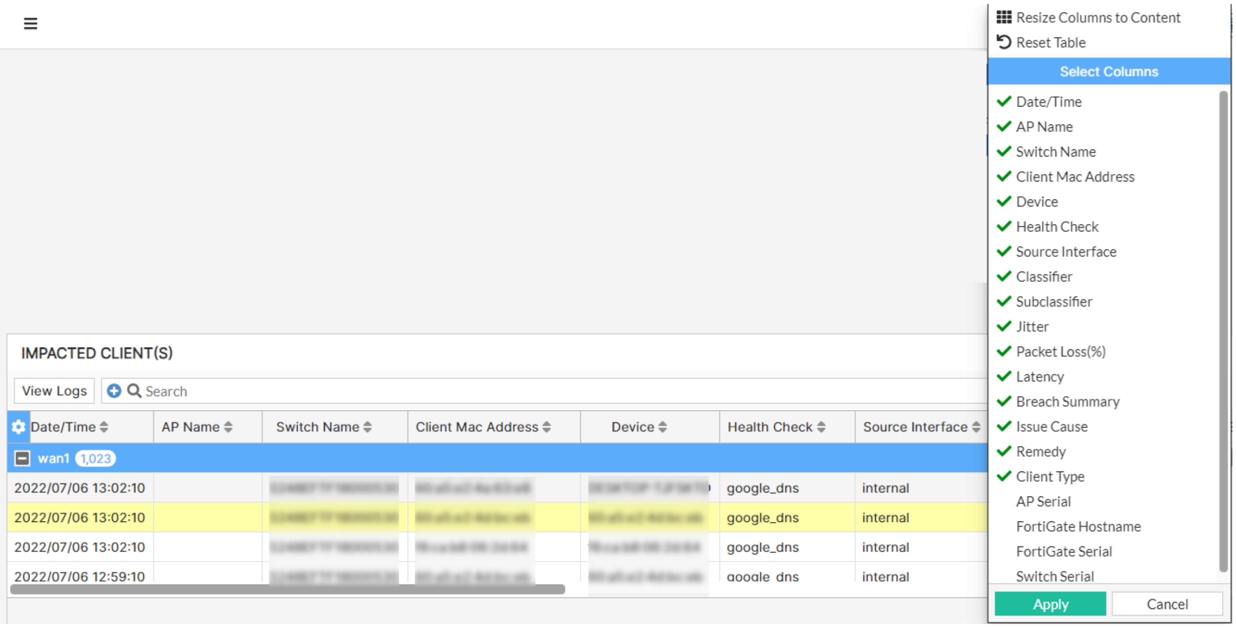
Topology and Logs

You can click on the impacted SLA listed in the panel to view the **Performance** or **FortiExtender Health** topology and the impacted client details.





The **Impacted Clients** table displays details such as the client MAC address, the associated AP serial number, the issue classifier/category and the sub-classifier, the issue description and the suggested remediation measure, and so on. The following image displays the impacted clients for performance SLAs.



IMPACTED CLIENT(S)

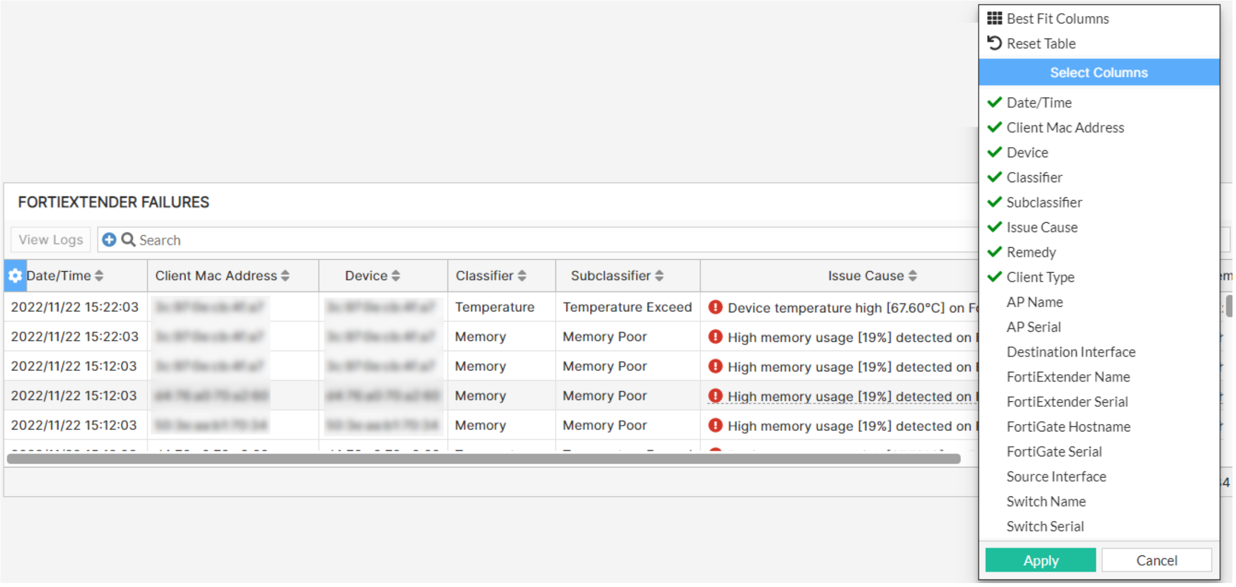
Date/Time	AP Name	Switch Name	Client Mac Address	Device	Health Check	Source Interface
wan1 1,023						
2022/07/06 13:02:10		[redacted]	[redacted]	[redacted]	google_dns	internal
2022/07/06 13:02:10		[redacted]	[redacted]	[redacted]	google_dns	internal
2022/07/06 13:02:10		[redacted]	[redacted]	[redacted]	google_dns	internal
2022/07/06 12:59:10		[redacted]	[redacted]	[redacted]	google_dns	internal

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	The serial number of the associated FortiGate.
AP Serial	The serial number of the associated AP.
Client 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.
Issue Cause	detailed cause of the SLA breach that impacted the client/AP/FortiGate.
Remedy	The suggested remedy to resolve the issue.
Classifier	The classifier of the issue reported for the SLA.
Subclassifier	The sub-classifier of the issue for the reported classifier.
Health Check	The performance SLA check configured in FortiGate.

Attribute	Description
Source Interface	The source interface name.
Jitter(ms)	The amount of jitter (milliseconds) reported for the client.
Packet Loss(%)	The percentage of packet loss reported for the client.
Latency(ms)	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.

The following image displays the impacted clients for FortiExtender health SLAs.



FORTIEXTENDER FAILURES

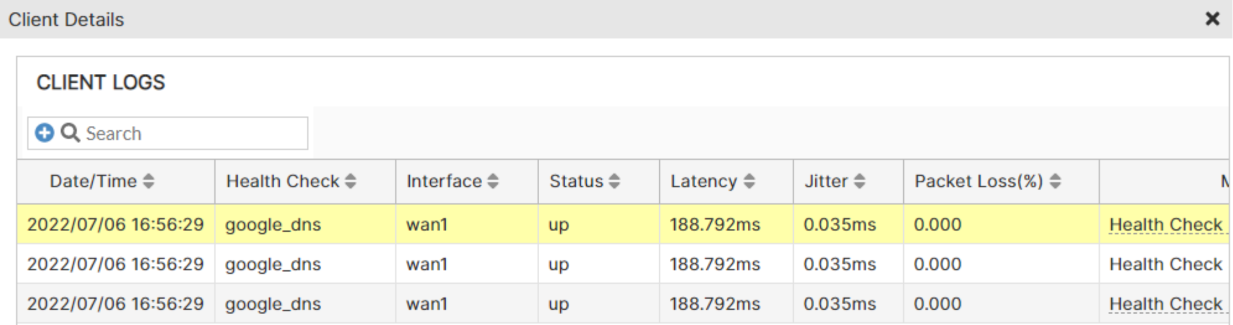
Date/Time	Client Mac Address	Device	Classifier	Subclassifier	Issue Cause
2022/11/22 15:22:03	[redacted]	[redacted]	Temperature	Temperature Exceed	Device temperature high [67.60°C] on F
2022/11/22 15:22:03	[redacted]	[redacted]	Memory	Memory Poor	High memory usage [19%] detected on
2022/11/22 15:12:03	[redacted]	[redacted]	Memory	Memory Poor	High memory usage [19%] detected on
2022/11/22 15:12:03	[redacted]	[redacted]	Memory	Memory Poor	High memory usage [19%] detected on
2022/11/22 15:12:03	[redacted]	[redacted]	Memory	Memory Poor	High memory usage [19%] detected on

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	The serial number of the associated FortiGate.
AP Serial	The serial number of the associated AP.
AP Name	The name of the associated AP.
Client 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.
Issue Cause	The detailed cause of the SLA breach that impacted the client/AP/FortiGate/FortiExtender.

Attribute	Description
Remedy	The suggested remedy to resolve the issue.
Classifier	The classifier of the issue reported for the SLA.
Subclassifier	The sub-classifier of the issue for the reported classifier.
Source Interface	The WAN interface name.
Switch Serial	The serial number of the impacted switch.
Switch Name	The name of the impacted switch.
FortiExtender Serial	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.

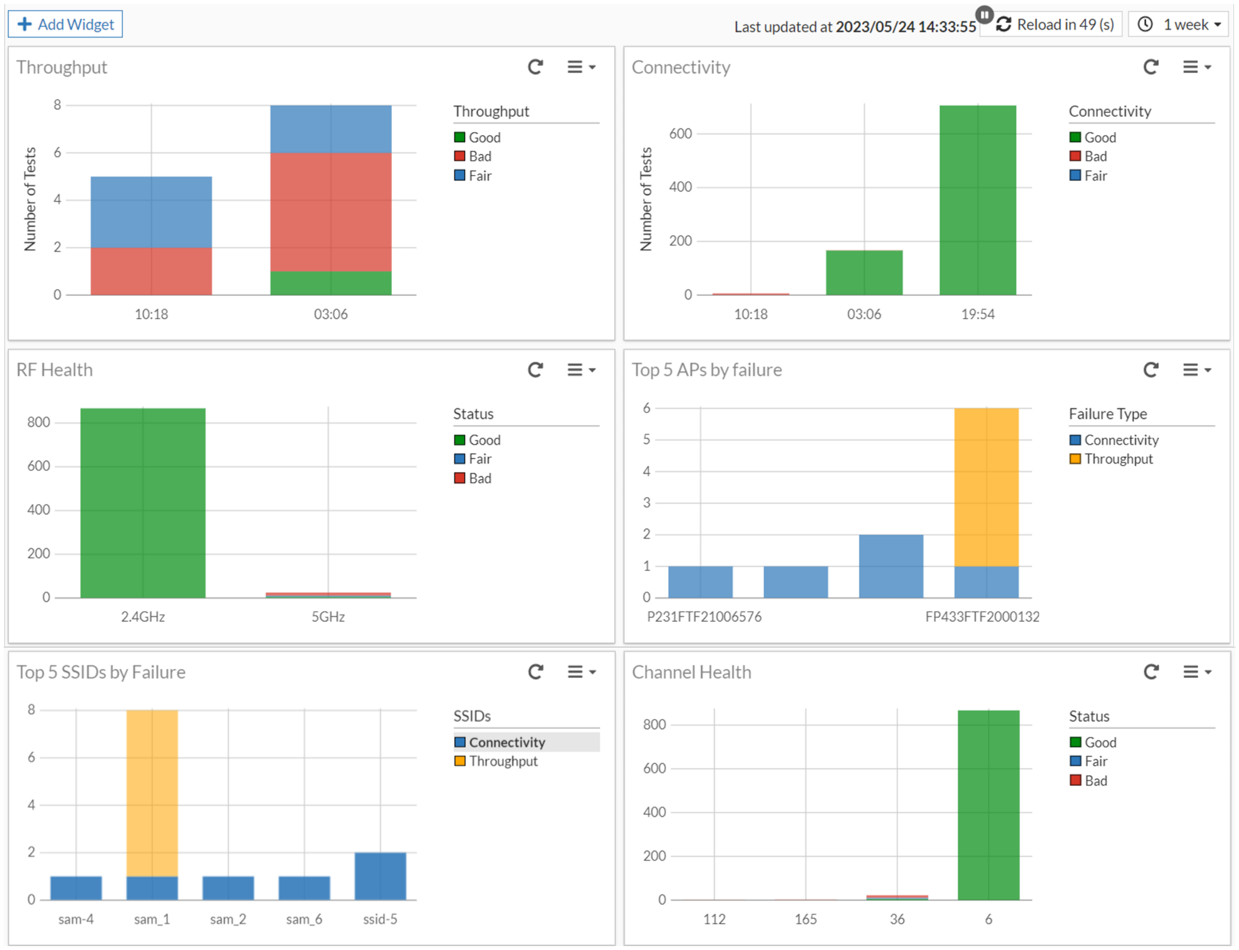
Select a particular client and click **View Logs**, to view the impacted client logs.



Date/Time	Health Check	Interface	Status	Latency	Jitter	Packet Loss(%)	N
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

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.

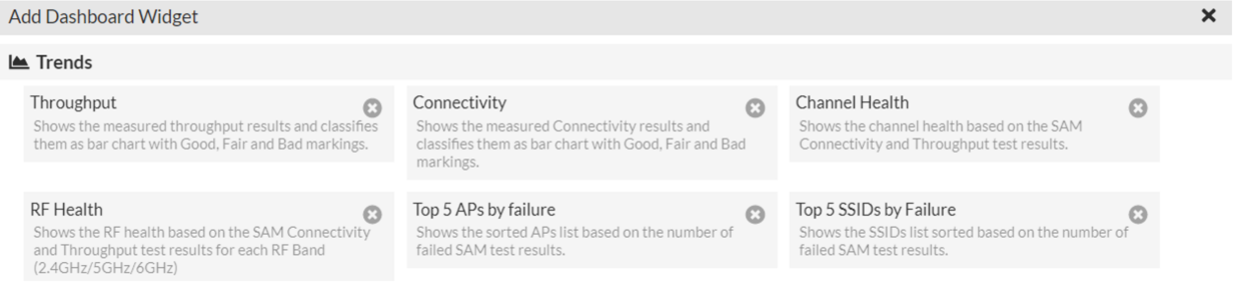


The data on this dashboard is based on scheduled test results and is automatically refreshed every 60 seconds; the following options are available to manage the auto-refresh feature for this page.

- 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.

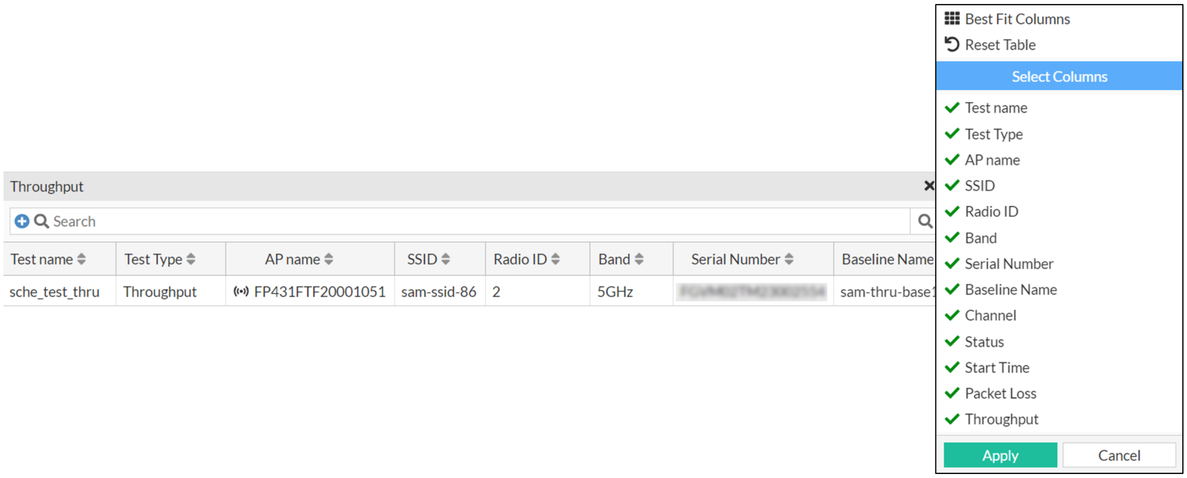
RF Health ⊗
Shows the RF health based on the SAM Connectivity and Throughput test results for each RF Band (2.4GHz/5GHz/6GHz)

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

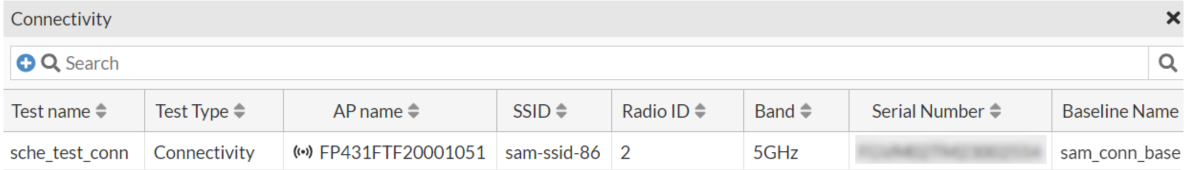
Search

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.
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.

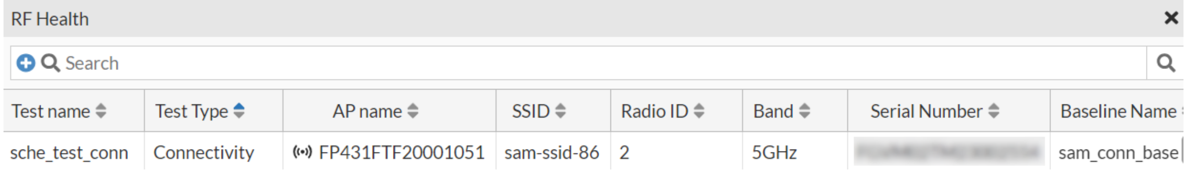


Connectivity

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.

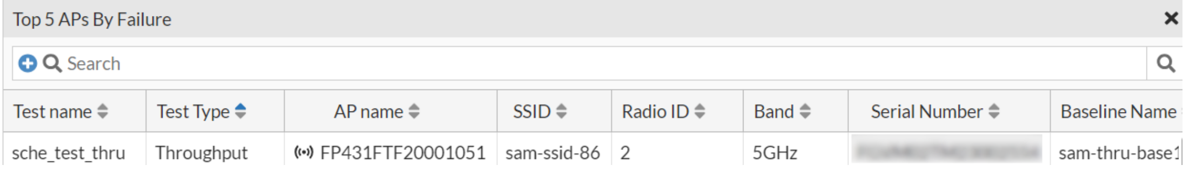


RF Health

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.

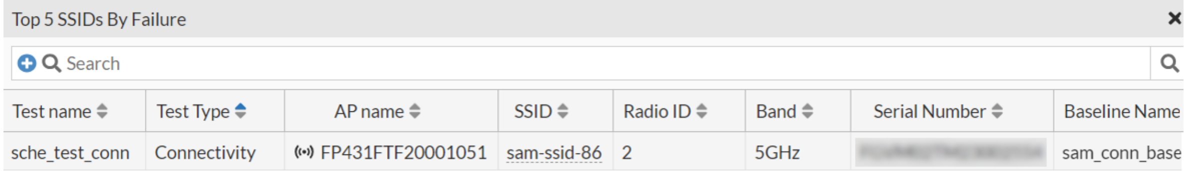


Top 5 APs By Failure

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.

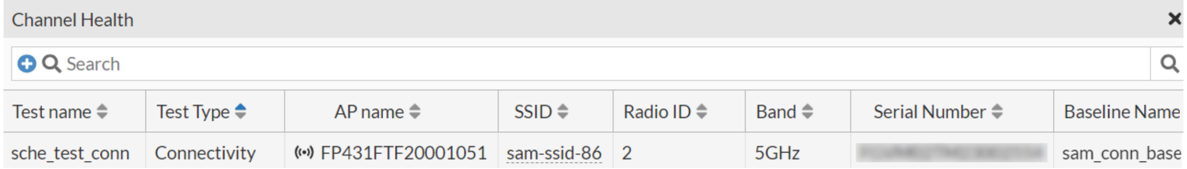


Top 5 SSIDs By Failure

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.

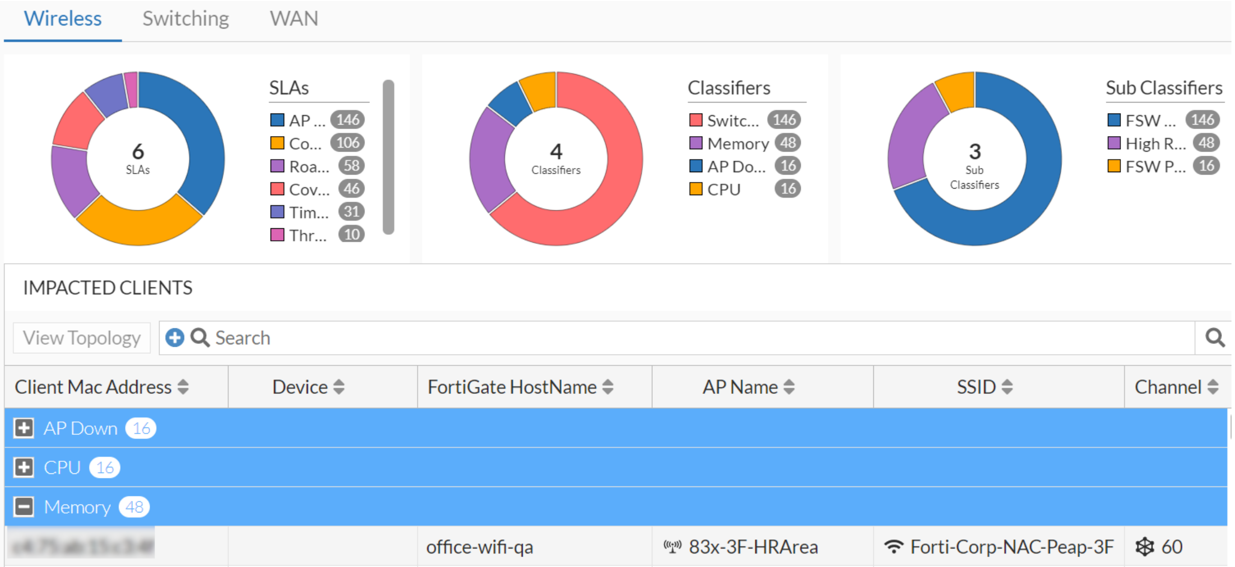
- Impacted SLA
- Impacted Devices
- SLA Configurations

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 **Show Clients** to view the impacted client count or click **Show 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.

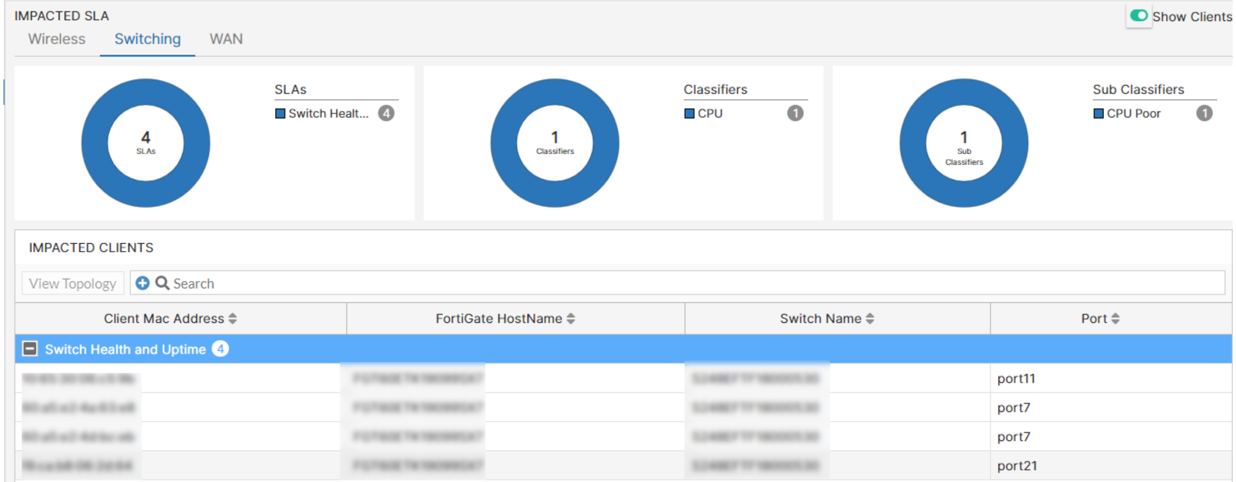


IMPACTED CLIENTS

Client Mac Address	Device	FortiGate HostName	AP Name	SSID	Channel
⊞ AP Down 16					
⊞ CPU 16					
⊟ Memory 48					
[redacted]		office-wifi-qa	83x-3F-HRArea	Forti-Corp-NAC-Peap-3F	60

Switching

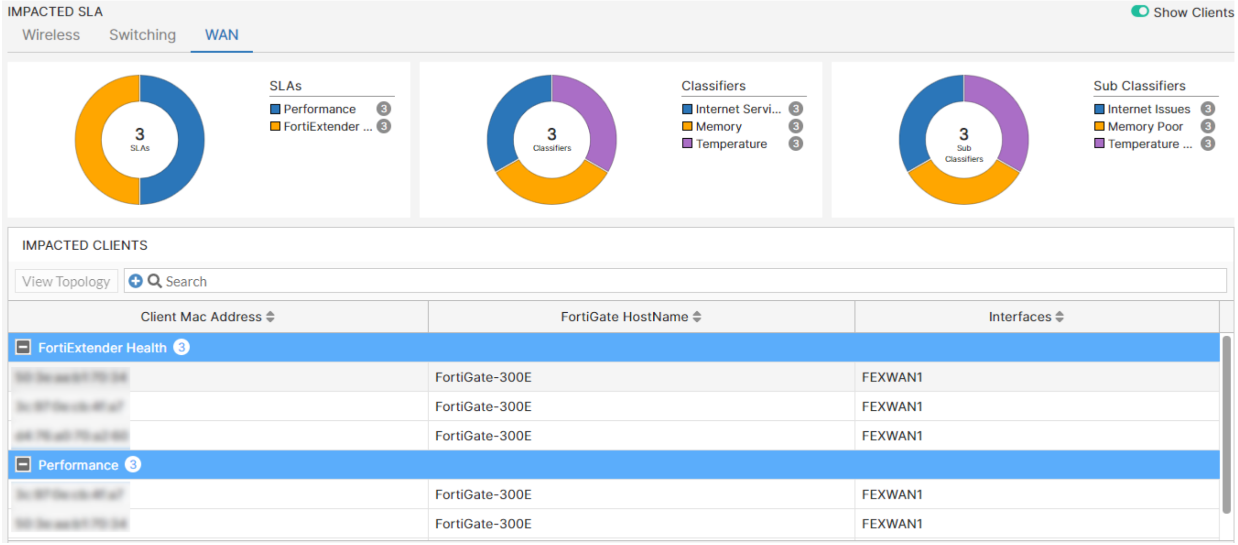
The switching SLA data is reported based on the classifiers and sub-classifiers listed displayed in this panel.



Client Mac Address	FortiGate HostName	Switch Name	Port
Switch Health and Uptime 4			
[redacted]	[redacted]	[redacted]	port11
[redacted]	[redacted]	[redacted]	port7
[redacted]	[redacted]	[redacted]	port7
[redacted]	[redacted]	[redacted]	port21

WAN

The WAN SLA data is reported based on the classifiers and sub-classifiers displayed in this panel.

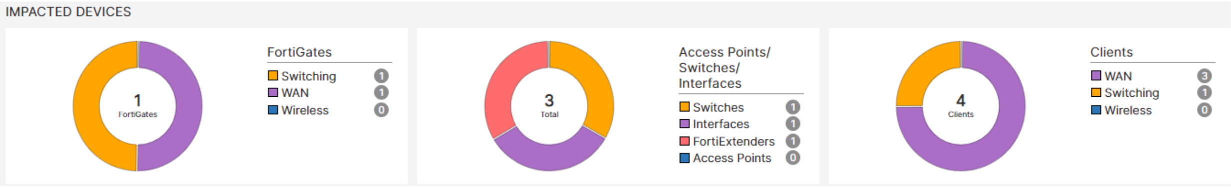


Client Mac Address	FortiGate HostName	Interfaces
FortiExtender Health 3		
[redacted]	FortiGate-300E	FEXWAN1
[redacted]	FortiGate-300E	FEXWAN1
[redacted]	FortiGate-300E	FEXWAN1
Performance 3		
[redacted]	FortiGate-300E	FEXWAN1
[redacted]	FortiGate-300E	FEXWAN1

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

Impacted Devices

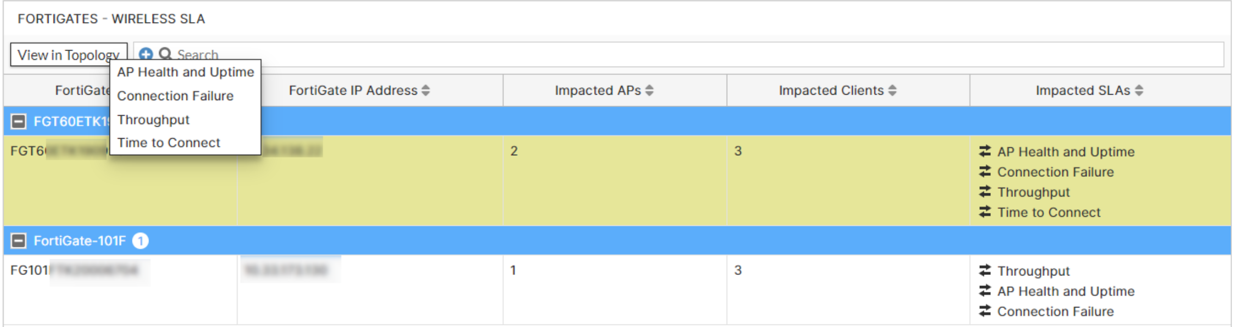
This page displays details of the various devices in your network that are associated with impacted clients, that include the wireless, switching, and WAN clients. You can view and analyze the SLA data based on the device type. The data is displayed in the following three panels. The number of devices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

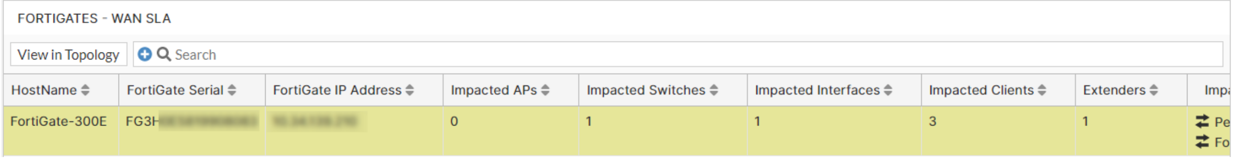
The following example displays the *FortiGates-Wireless SLA* with information such as FortiGate host name, serial number, and IP address, and lists the impacted APs, clients, and SLAs. Select any row and click **View in Topology**. You are prompted to select an SLA. Data is displayed for FortiGate wireless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



FORTIGATES - WIRELESS SLA

FortiGate	FortiGate IP Address	Impacted APs	Impacted Clients	Impacted SLAs
⊟ FGT60ETK1				
FGT6[redacted]	[redacted]	2	3	⇄ AP Health and Uptime ⇄ Connection Failure ⇄ Throughput ⇄ Time to Connect
⊟ FortiGate-101F 1				
FG101[redacted]	[redacted]	1	3	⇄ Throughput ⇄ AP Health and Uptime ⇄ Connection Failure

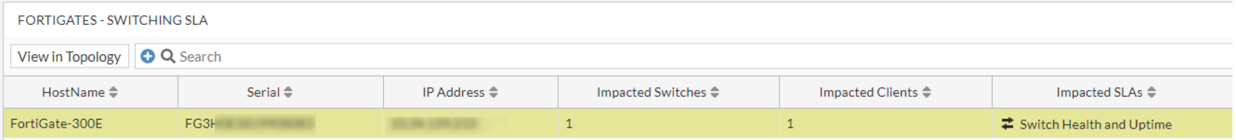
The following example displays the *FortiGates-WAN SLA* with information such as FortiGate host name, serial number, and IP address, and lists the impacted APs, clients, SLAs, switches, and interfaces. Select any row and click **View in Topology** to view the associated details.



FORTIGATES - WAN SLA

HostName	FortiGate Serial	FortiGate IP Address	Impacted APs	Impacted Switches	Impacted Interfaces	Impacted Clients	Extenders	Imp
FortiGate-300E	FG3H[redacted]	[redacted]	0	1	1	3	1	⇄ Pe ⇄ Fo

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 **View in Topology** to view the associated details.



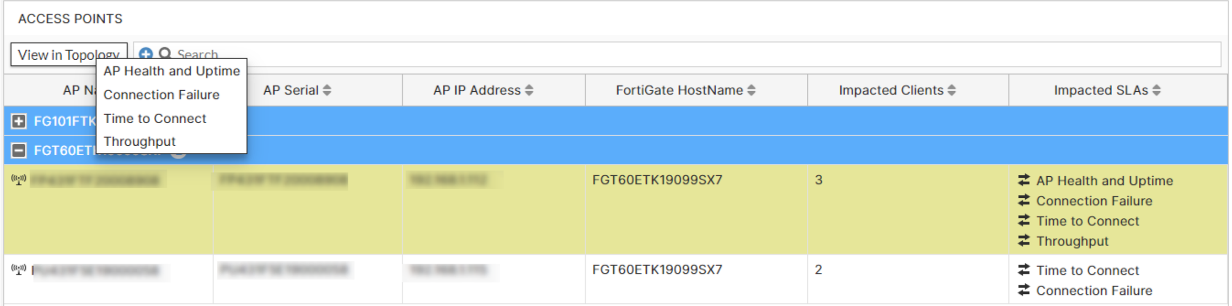
FORTIGATES - SWITCHING SLA

HostName	Serial	IP Address	Impacted Switches	Impacted Clients	Impacted SLAs
FortiGate-300E	FG3H[redacted]	[redacted]	1	1	⇄ Switch Health and Uptime

Access Points/ Switches/ Interfaces/FortiExtenders

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

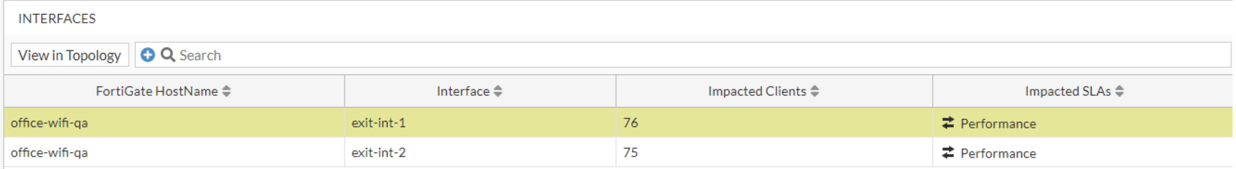
The following example displays the *Access Points* with information such as AP name, serial number, and IP address, FortiGate host name and IP address, and lists the impacted clients and SLAs. Select any row and click **View in Topology** to view the associated details.



ACCESS POINTS

AP Na	AP Serial	AP IP Address	FortiGate HostName	Impacted Clients	Impacted SLAs
FG101FTK					
FGT60ETI					
[redacted]	[redacted]	[redacted]	FGT60ETK19099SX7	3	AP Health and Uptime Connection Failure Time to Connect Throughput
[redacted]	[redacted]	[redacted]	FGT60ETK19099SX7	2	Time to Connect Connection Failure

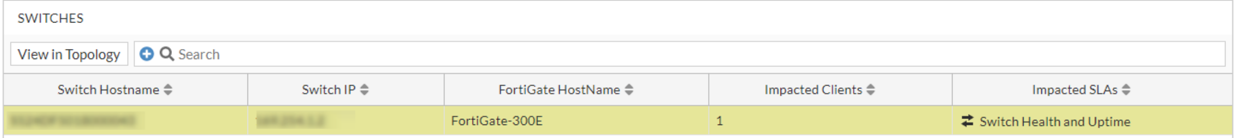
The following example displays the *Interfaces* with information such as the interface, FortiGate host name, serial number, and IP address, and lists the impacted clients and SLAs. Select any row and click **View in Topology** to view the associated details.



INTERFACES

FortiGate HostName	Interface	Impacted Clients	Impacted SLAs
office-wifi-qa	exit-int-1	76	Performance
office-wifi-qa	exit-int-2	75	Performance

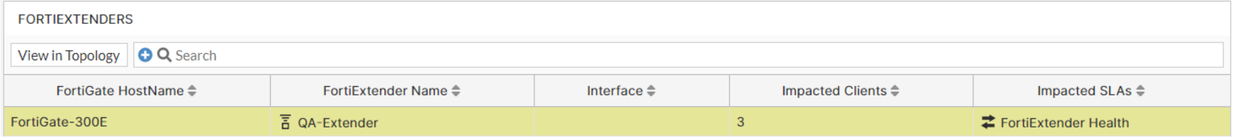
The following example displays the *Switches* with information such as the switch host name, IP address, OS version, and serial number, FortiGate host name, serial number, and IP address, and lists the impacted clients and SLAs along with the status and state of the switch. Select any row and click **View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



SWITCHES

Switch Hostname	Switch IP	FortiGate HostName	Impacted Clients	Impacted SLAs
[redacted]	[redacted]	FortiGate-300E	1	Switch Health and Uptime

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 **View in Topology** to view the associated details.



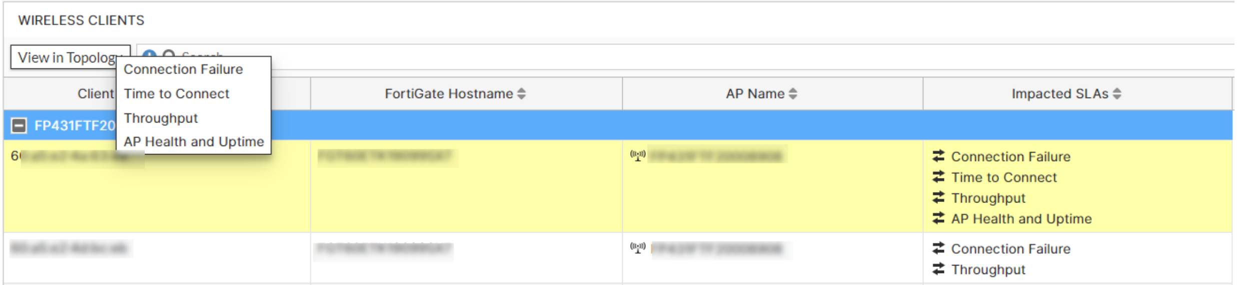
FORTIEXTENDERS

FortiGate HostName	FortiExtender Name	Interface	Impacted Clients	Impacted SLAs
FortiGate-300E	QA-Extender		3	FortiExtender Health

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 **View in Topology** to view the associated details.



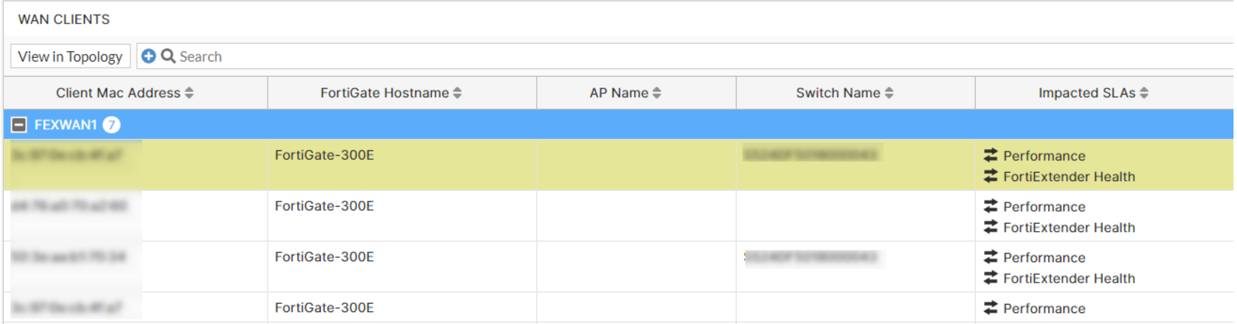
WIRELESS CLIENTS

View in Topology | Search

Connection Failure
Time to Connect
Throughput
AP Health and Uptime

Client	FortiGate Hostname	AP Name	Impacted SLAs
FP431FTF20			
6[redacted]	[redacted]	[redacted]	⇄ Connection Failure ⇄ Time to Connect ⇄ Throughput ⇄ AP Health and Uptime
[redacted]	[redacted]	[redacted]	⇄ Connection Failure ⇄ Throughput

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 **View in Topology** to view the associated details.

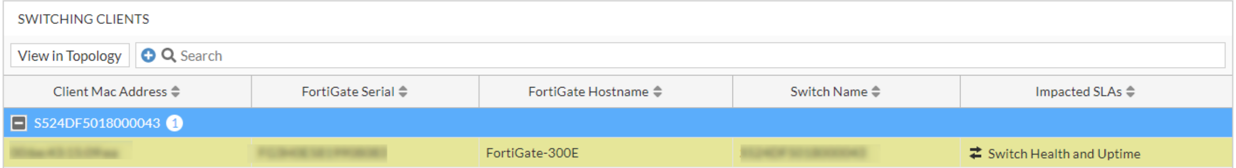


WAN CLIENTS

View in Topology | Search

Client Mac Address	FortiGate Hostname	AP Name	Switch Name	Impacted SLAs
FEXWAN1 7				
[redacted]	FortiGate-300E		[redacted]	⇄ Performance ⇄ FortiExtender Health
[redacted]	FortiGate-300E			⇄ Performance ⇄ FortiExtender Health
[redacted]	FortiGate-300E		[redacted]	⇄ Performance ⇄ FortiExtender Health
[redacted]	FortiGate-300E			⇄ Performance

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 **View in Topology** to view the associated details.



SWITCHING CLIENTS

View in Topology | Search

Client Mac Address	FortiGate Serial	FortiGate Hostname	Switch Name	Impacted SLAs
S524DF5018000043 1				
[redacted]	[redacted]	FortiGate-300E	[redacted]	⇄ Switch Health and Uptime

SLA Configurations

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

- Device Health
- Time To Connect
- Roaming
- SD-WAN

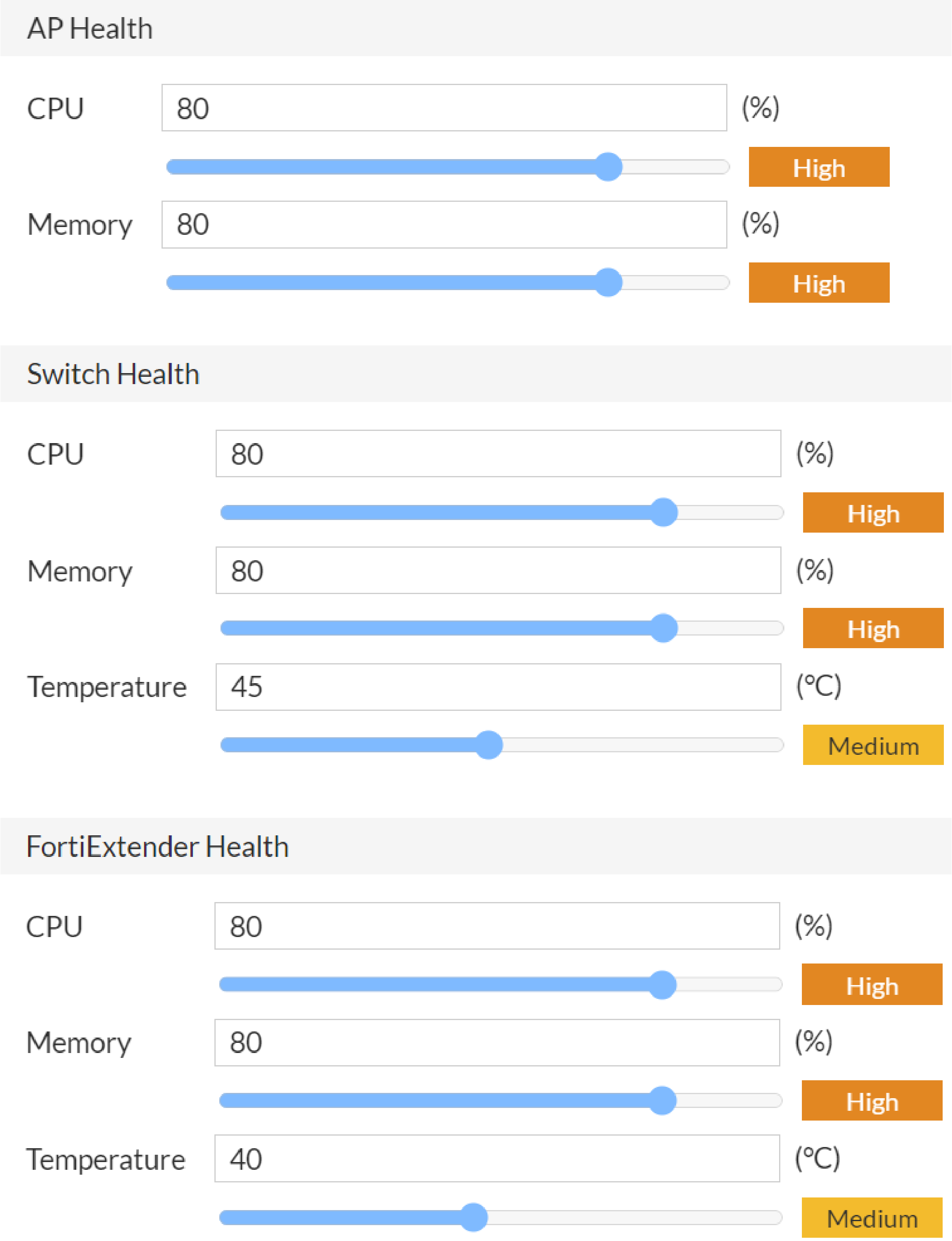
Device Health

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

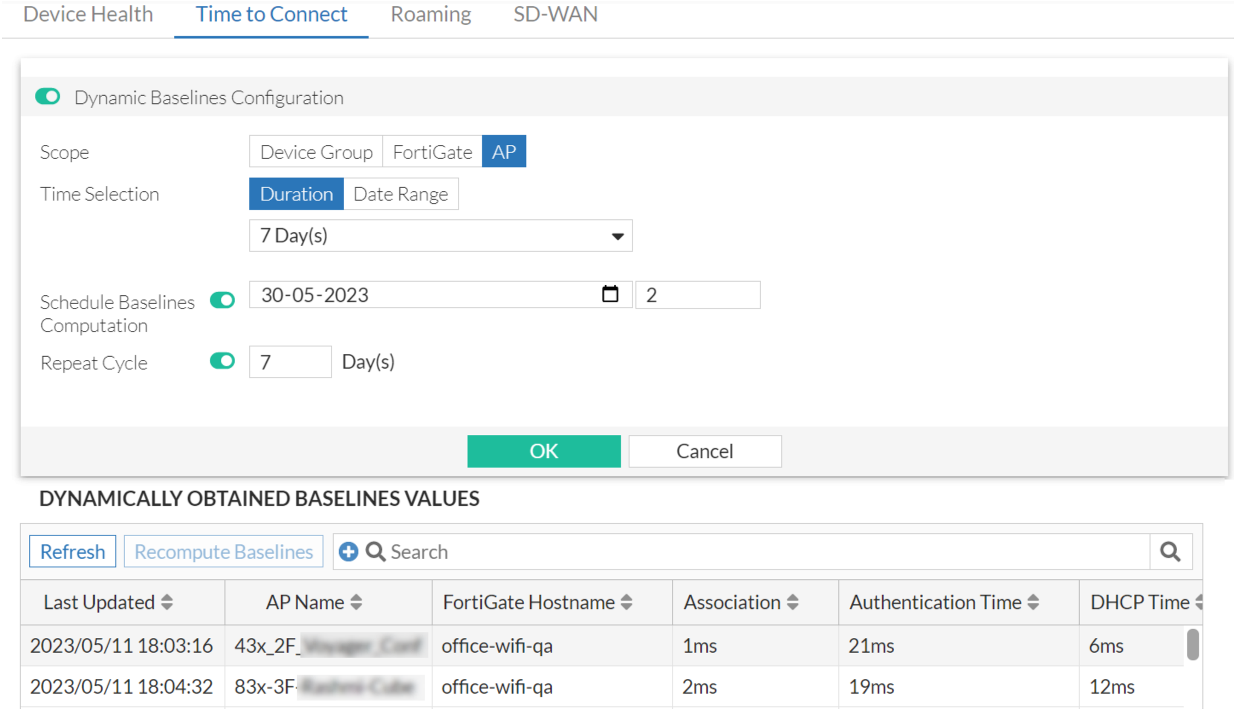
The default value for the CPU and memory parameters is 80% and the default value for the temperature is 45 degree Celsius.

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 / FortiGate / [✓ AP]
Time Selection	[✓ Duration] / Date Range 7 Day(s)
Schedule Baselines Computation ●	30-05-2023 2
Repeat Cycle ●	7 Day(s)

DYNAMICALLY OBTAINED BASELINES VALUES

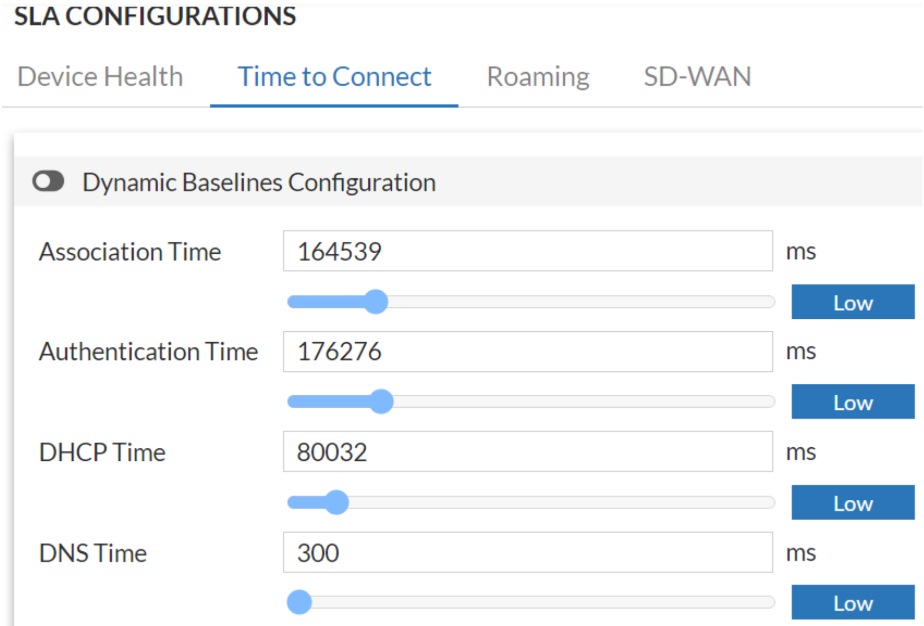
Last Updated	AP Name	FortiGate Hostname	Association	Authentication Time	DHCP Time
2023/05/11 18:03:16	43x_2F_[redacted]	office-wifi-qa	1ms	21ms	6ms
2023/05/11 18:04:32	83x-3F[redacted]	office-wifi-qa	2ms	19ms	12ms

- **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.



SLA CONFIGURATIONS

Dynamic Baselines Configuration

Association Time 164539 ms

Authentication Time 176276 ms

DHCP Time 80032 ms

DNS Time 300 ms

- **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:

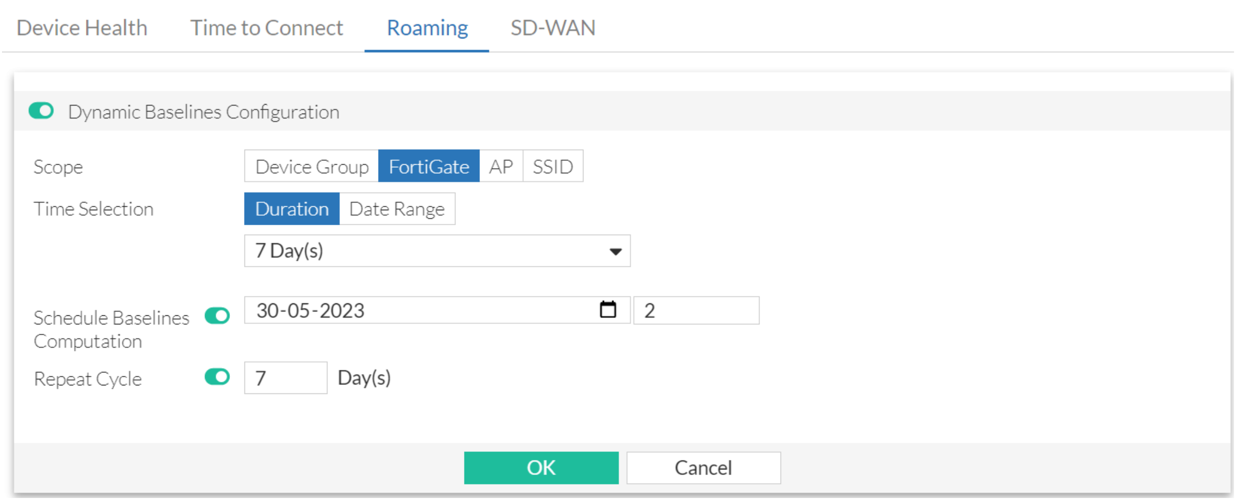
- The default value for these parameters is 300 milliseconds and the valid range is 1 - 1000000 milliseconds.
- DNS is not supported.

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

7 Day(s)

Schedule Baselines Computation: 30-05-2023 | 2

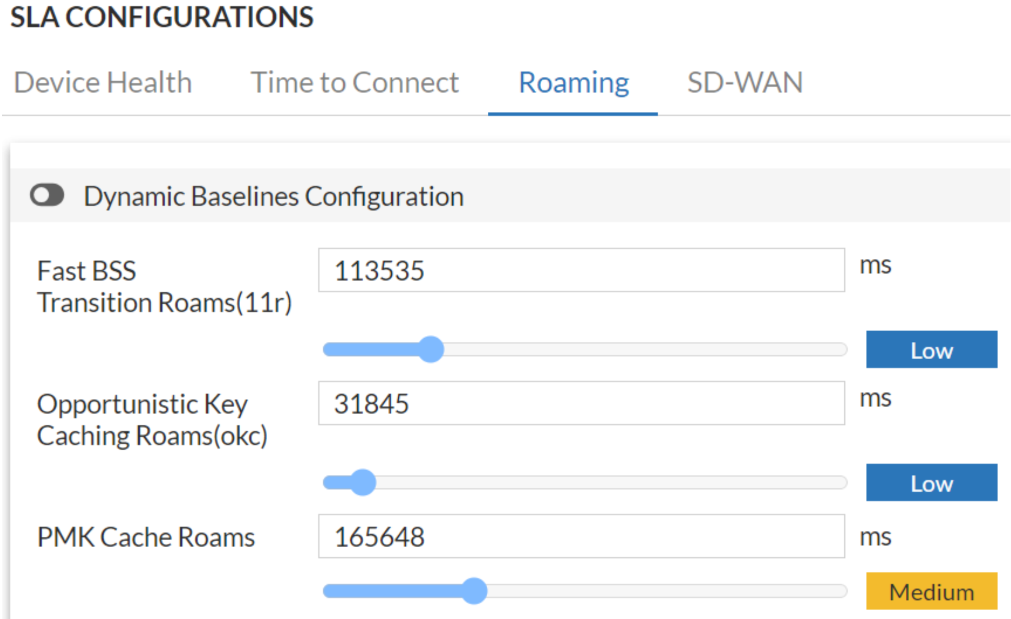
Repeat Cycle: 7 Day(s)

- **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.



SLA CONFIGURATIONS

Dynamic Baselines Configuration

Fast BSS Transition Roams(11r): 113535 ms — Low

Opportunistic Key Caching Roams(okc): 31845 ms — Low

PMK Cache Roams: 165648 ms — Medium

- **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.

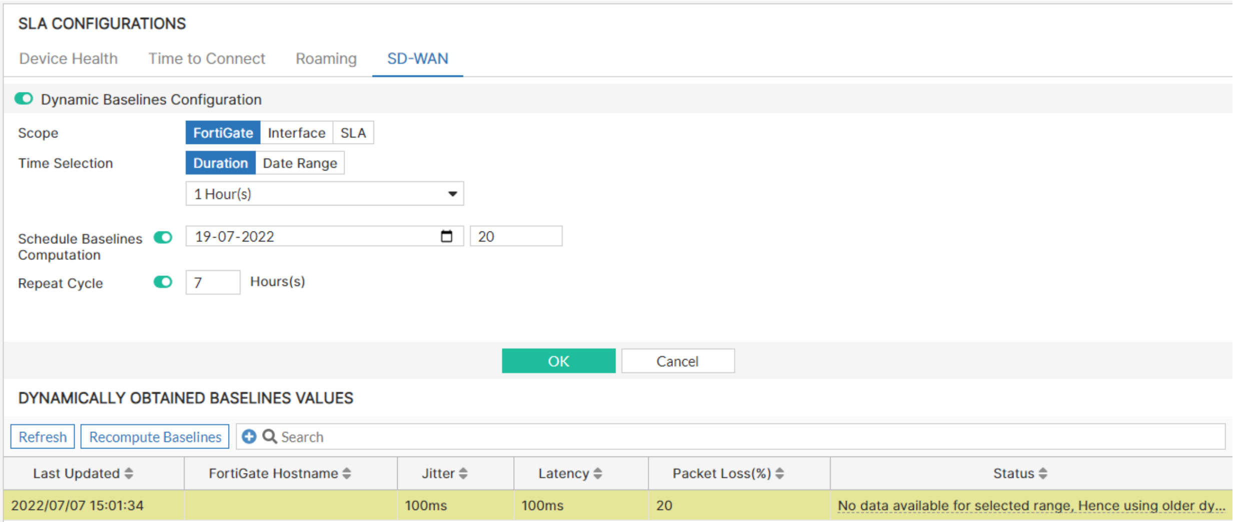
SD-WAN

You can configure the SD-WAN SLAs in FortiAIOps or in FortiGate. The following configurations are *required* in FortiGate to receive SD-WAN logs.

- Ensure that the SD-WAN monitoring license is applied in FortiGate. This is to generate congestion logs.
- Configure the *sla-fail* and *sla-pass* log failure period, the recommended duration is 30 to 60 seconds.

Dynamic Baselines

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



Dynamic Baselines Configuration

Scope: FortiGate | Interface | SLA

Time Selection: Duration | Date Range

1 Hour(s)

Schedule Baselines Computation: 19-07-2022 20

Repeat Cycle: 7 Hours(s)

DYNAMICALLY OBTAINED BASELINES VALUES

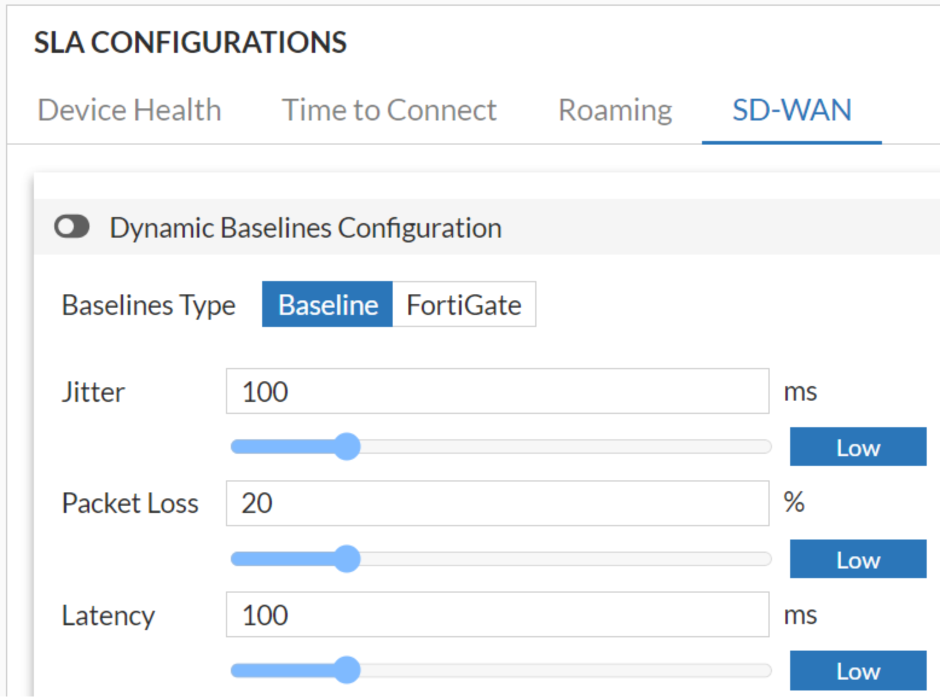
Last Updated	FortiGate Hostname	Jitter	Latency	Packet Loss(%)	Status
2022/07/07 15:01:34		100ms	100ms	20	No data available for selected range, Hence using older dy...

- **Scope** - Select the scope to calculate the thresholds which could either be per **FortiGate**, per **Interface**, or per **SLA**.
- **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

Select **Baseline** to configure the threshold configuration criteria in FortiAIOps or **FortiGate** to use the settings configured in FortiGate. For more information, see the SD-WAN minimum SLA configuration.



SLA CONFIGURATIONS

Dynamic Baselines Configuration

Baselines Type: Baseline | FortiGate

Jitter: 100 ms — Low

Packet Loss: 20 % — Low

Latency: 100 ms — Low

- **Jitter** - The maximum amount of jitter that's acceptable on the interface. The default value is 1 ms and the valid range is 1 - 500 ms.
- **Packet Loss** - The maximum percentage of packet loss that's acceptable on the interface. The default value is 20% and the valid range is 1 - 100%.
- **Latency** - The maximum amount of latency that's acceptable on the interface. The default value is 100 ms and the valid range is 0 - 500 ms.

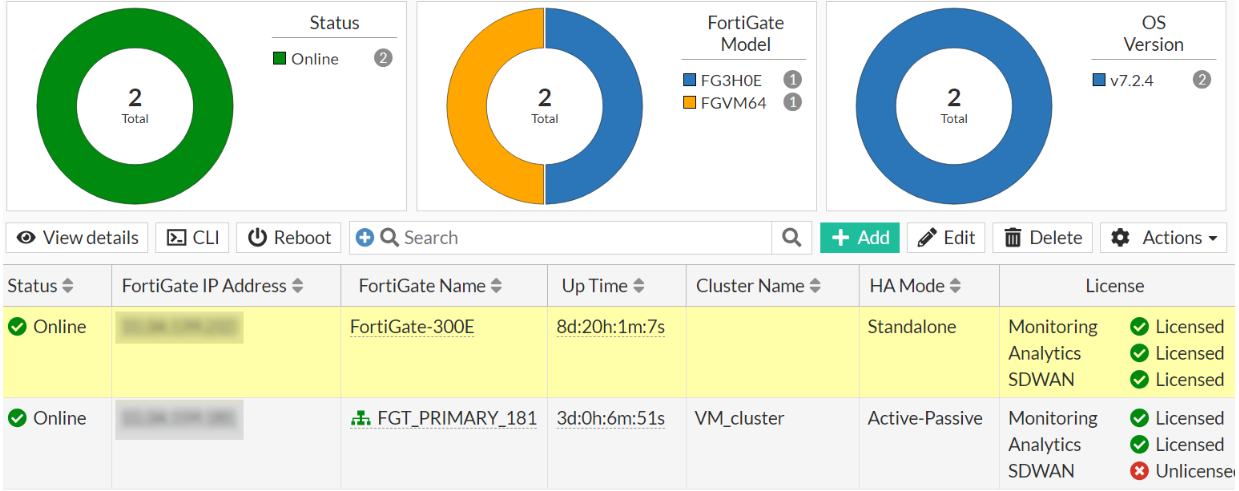
Inventory

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

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 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 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.

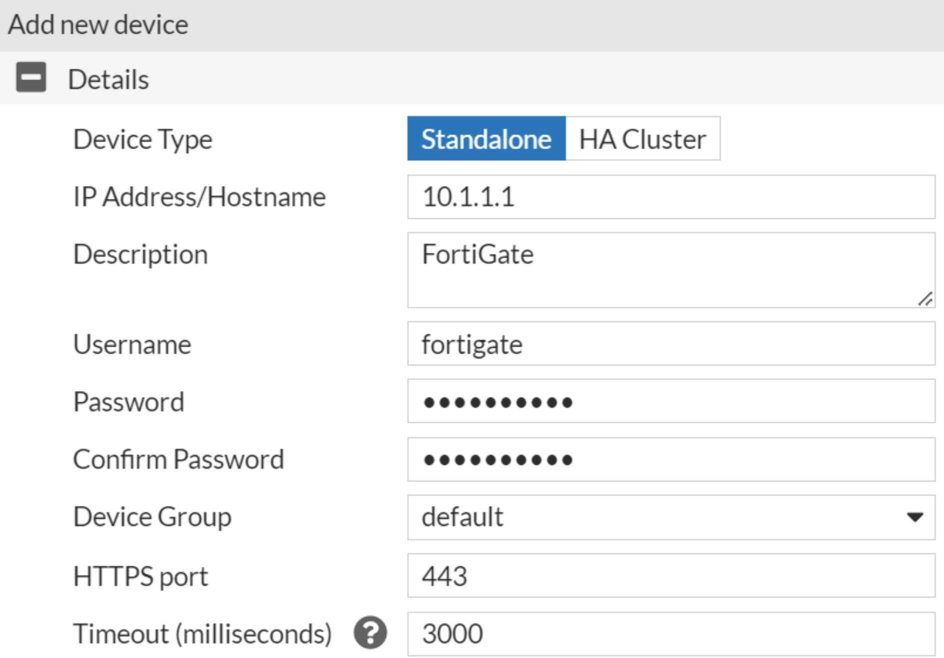
The managed FortiGate IP address/FQDN configured in FortiAIOps must match the Subject Alternative Name (SAN) in the FortiGate certificate, else, the FortiGate discovery fails.

- 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

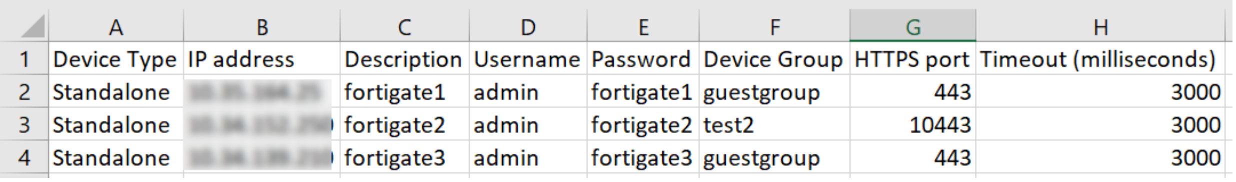
1. Select **Standalone** or **HA Cluster** if the FortiGate is an HA cluster.
2. Enter the **IP Address** or FQDN of the controller and an optional **Description**.
   Note: If a 3rd party certificate is used by FortiGate then ensure to install a valid CA certificate in FortiAIOps.
3. Enter the **Username**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

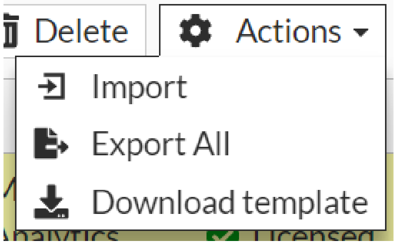
Importing and Exporting FortiGates

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.



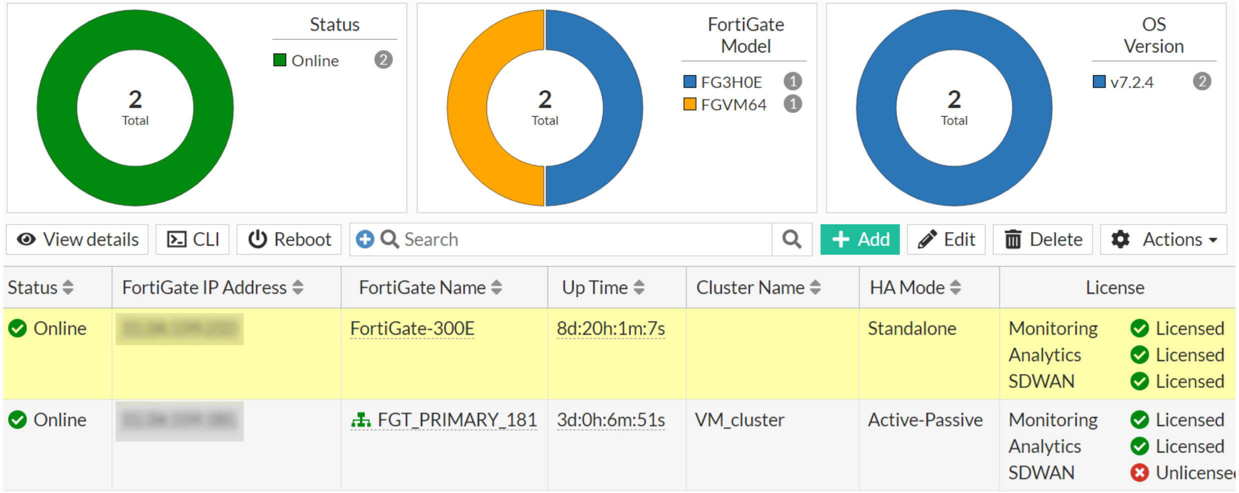
Select **Import** to upload the FortiGate configuration file.

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

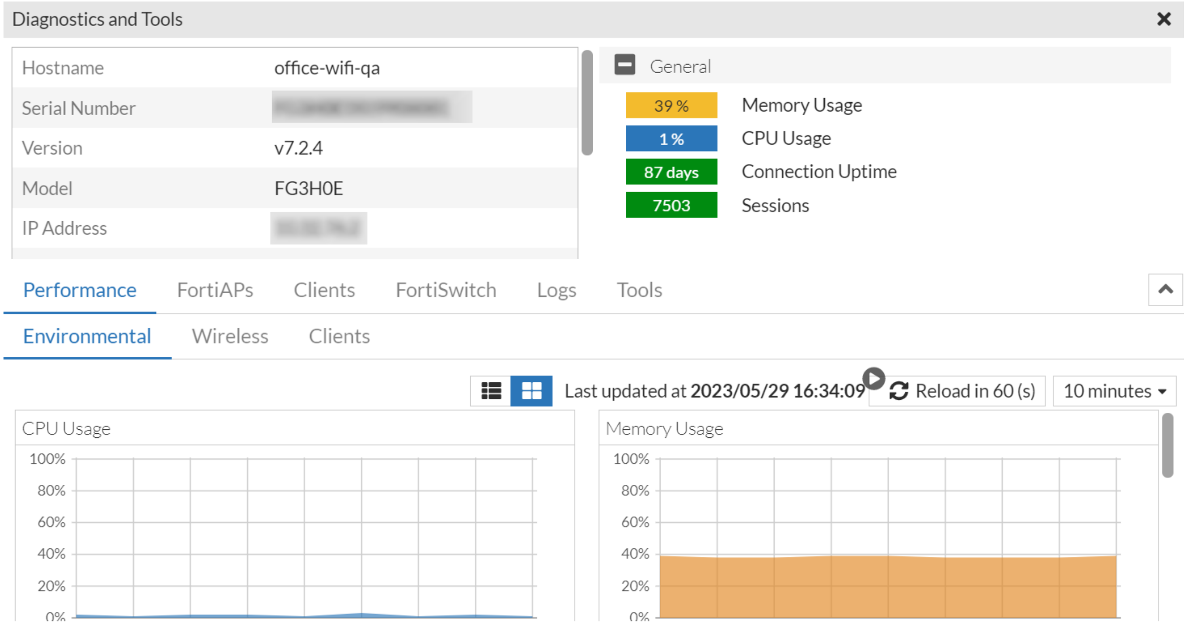
This page provides analytical information related to the performance of various elements and processes in your network. The data is visually represented with interactive options to drill-down and filter specific information. This enables monitoring, diagnostic, and troubleshooting operations for connectivity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

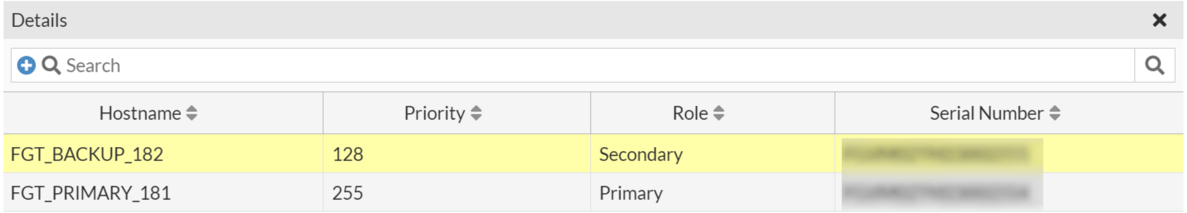


Hostname	office-wifi-qa
Serial Number	[redacted]
Version	v7.2.4
Model	FG3H0E
IP Address	[redacted]

39 %	Memory Usage
1 %	CPU Usage
87 days	Connection Uptime
7503	Sessions

Last updated at 2023/05/29 16:34:09

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



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 select the time interval to view the data (10 or 30 minutes, 1, 12, or 24 hours). The data in this tab is automatically refreshed every 60 seconds; the following options are available to manage the auto-refresh feature for this page.

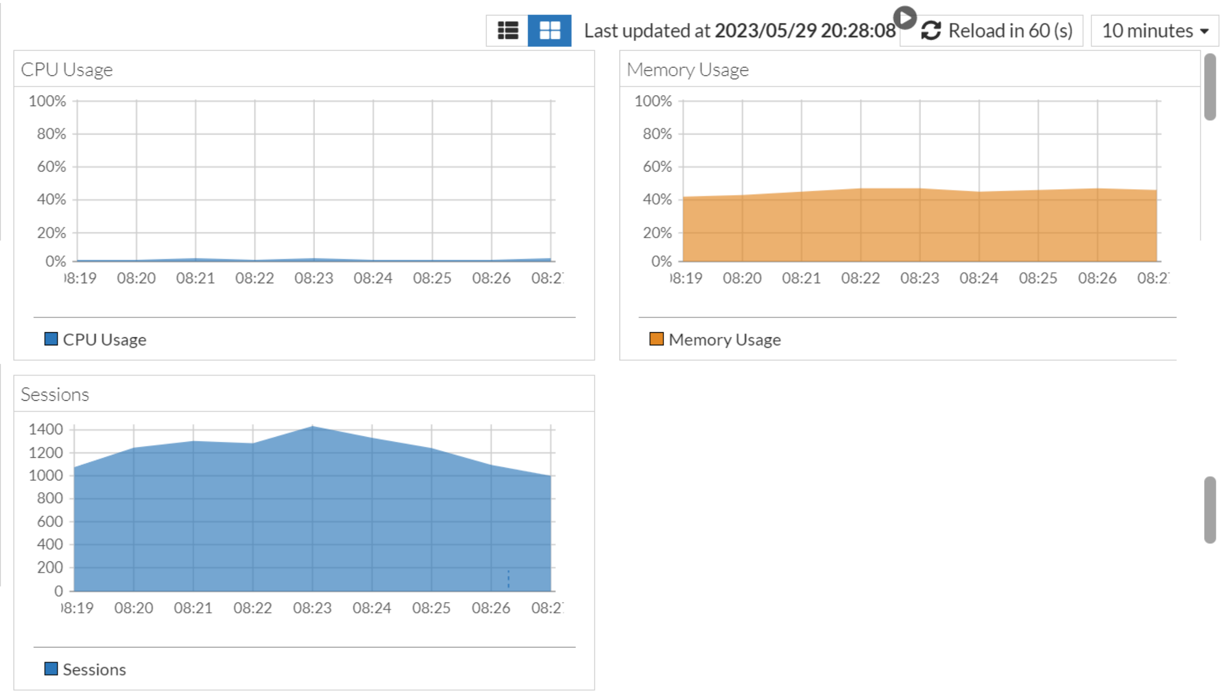
- Click ⟳ to manually refresh data.
- Click ⏸ to pause the auto-refresh.
- Click ▶ to resume the auto-refresh.

Performance is displayed for the following.

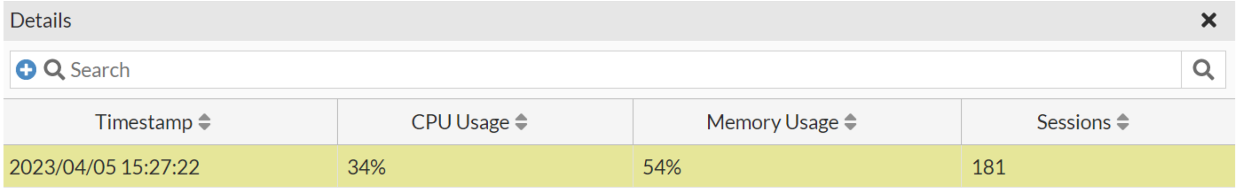
- Environmental
- Wireless
- Clients

Environmental

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



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



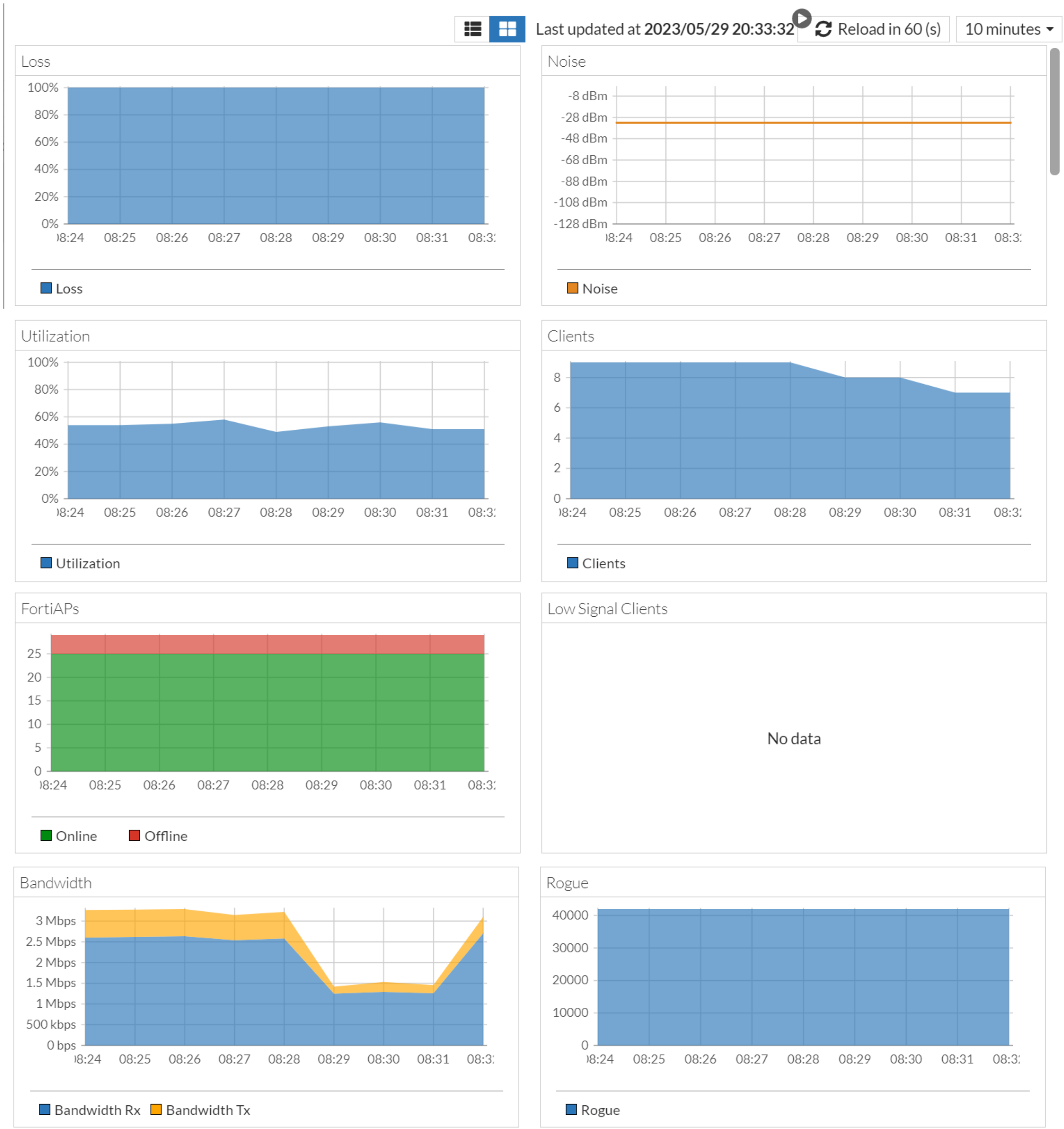
Details ✕

Search

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

Wireless

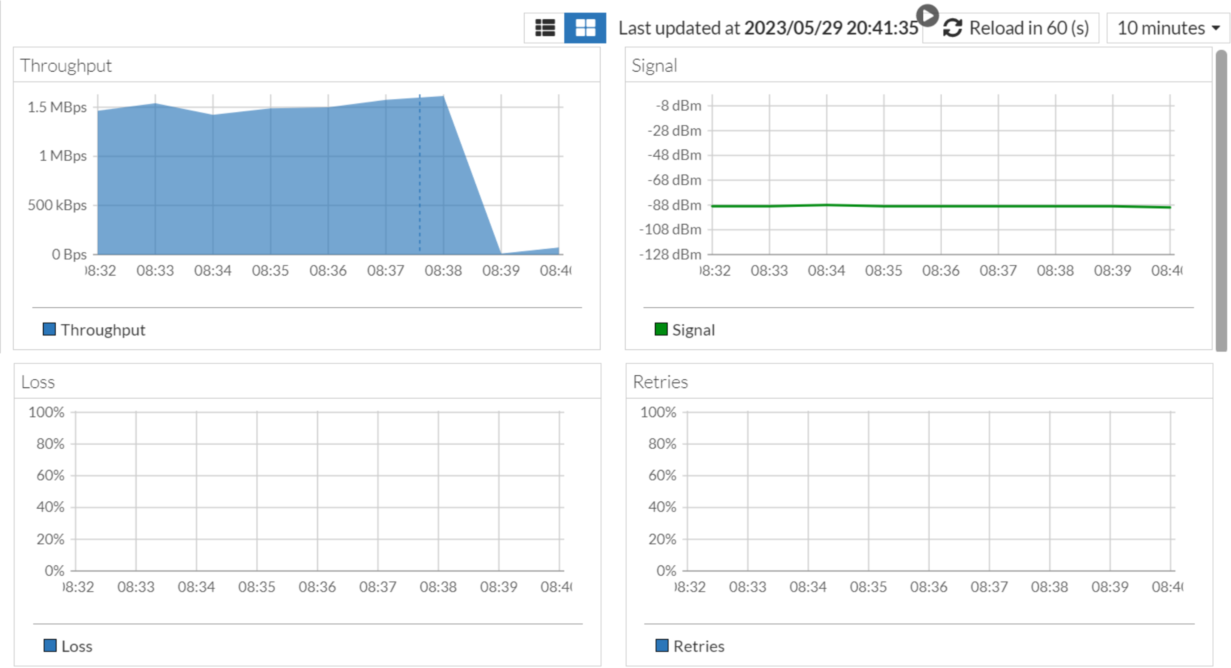
Displays detailed information about the health of the wireless connections in the network, such as, loss%, SNR, channel utilization %, number of stations, status of the FortiAPs, low signal stations, the average throughput at a given time, and the number of rogue APs at a given time.


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.



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

FortiAPs

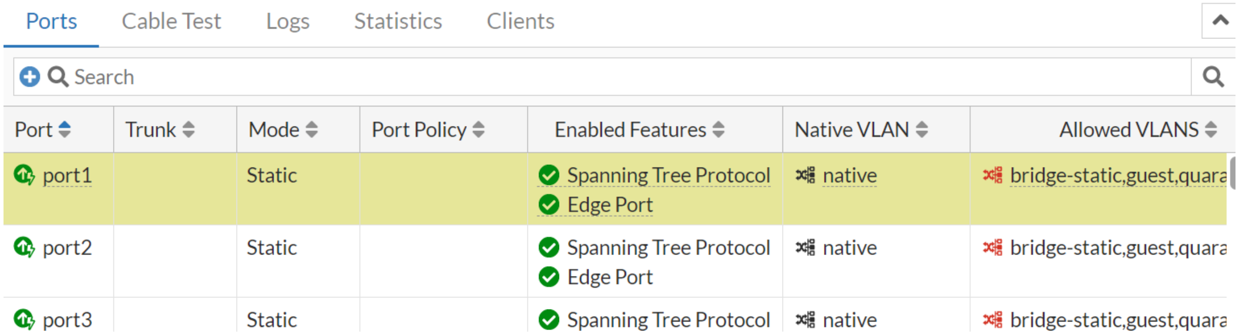
This tab displays details about the selected access point with their status and details. To view the details, select an access point and click **View Details**. For more information on the diagnostic options and details see Access Points.

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 111.

FortiSwitch

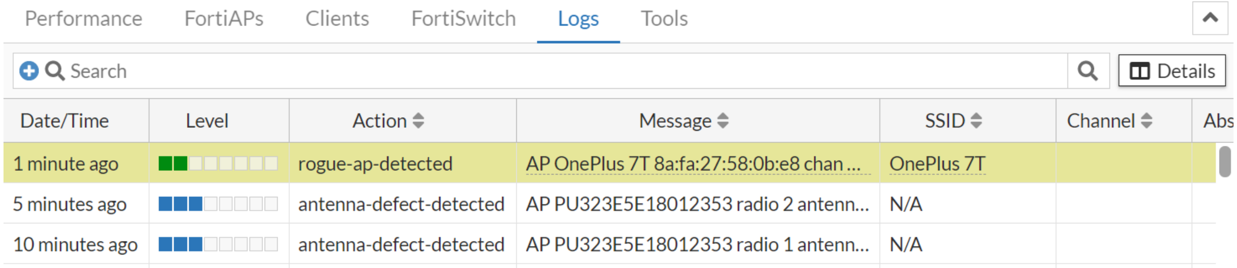
This tab displays a graphical snapshot of the FortiSwitch activity such as, the total number of FortiSwitches, their status (online/offline), and the deployed model details. To view the details, select a FortiSwitch and click **View Details**. For more information on the diagnostic options and details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

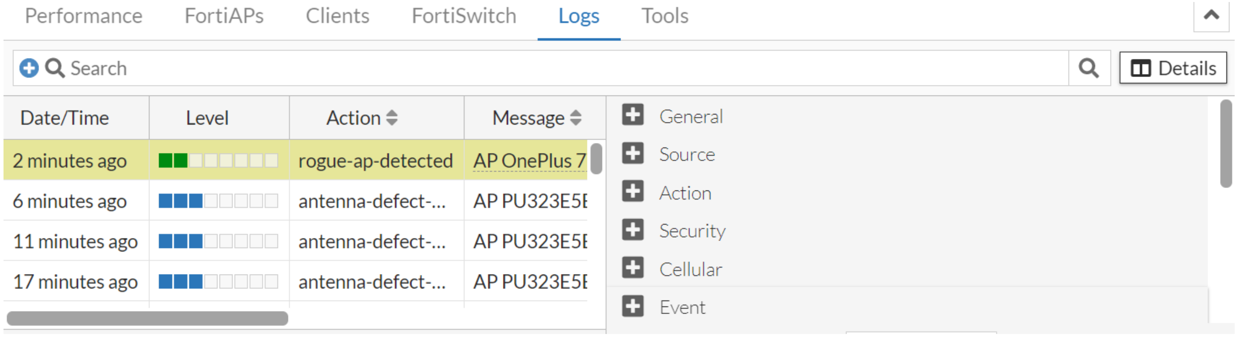
This tab displays the detailed FortiGate event logs and each event is assigned a severity, that is depicted with a color code. Hover over the color bar in the **Level** column to view the severity.



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.

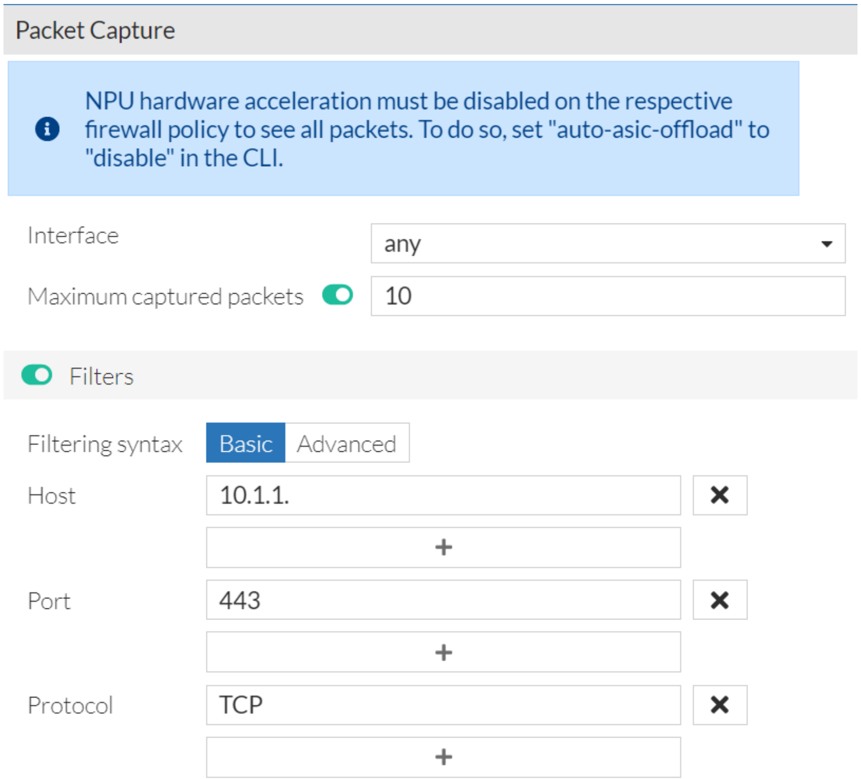
Tools

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

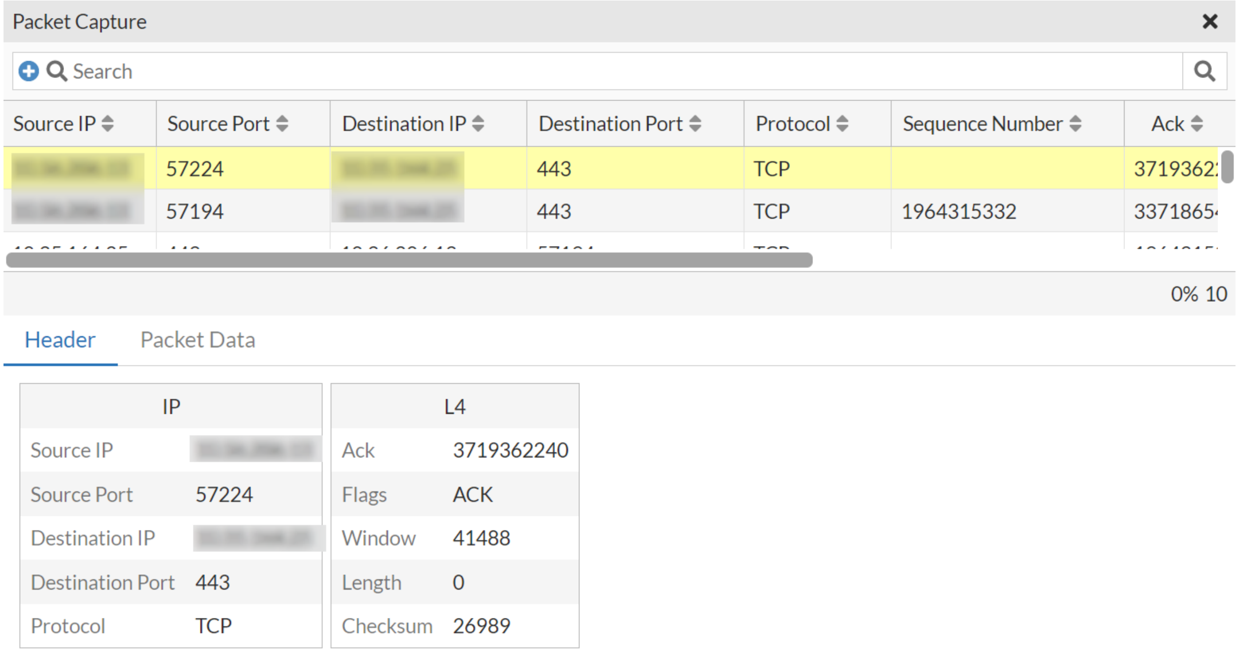
Filtering syntax: Basic | Advanced

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**.



Packet Capture

Search

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

0% 10

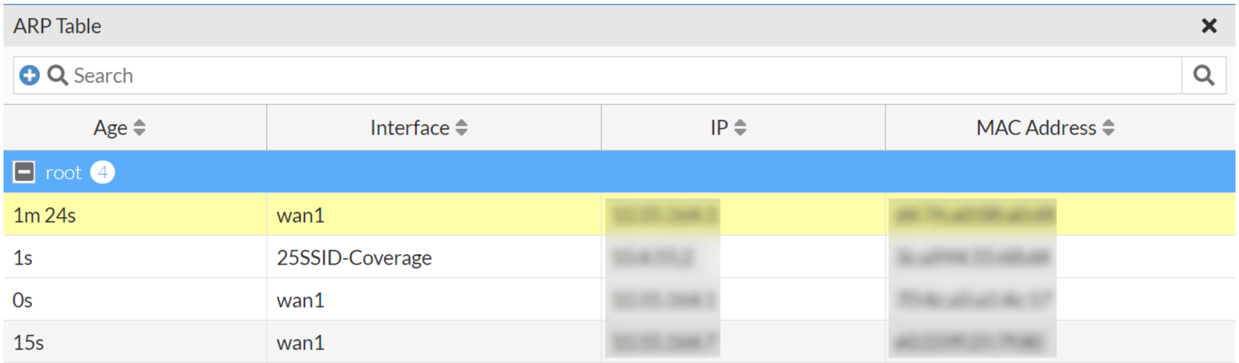
Header Packet Data

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.



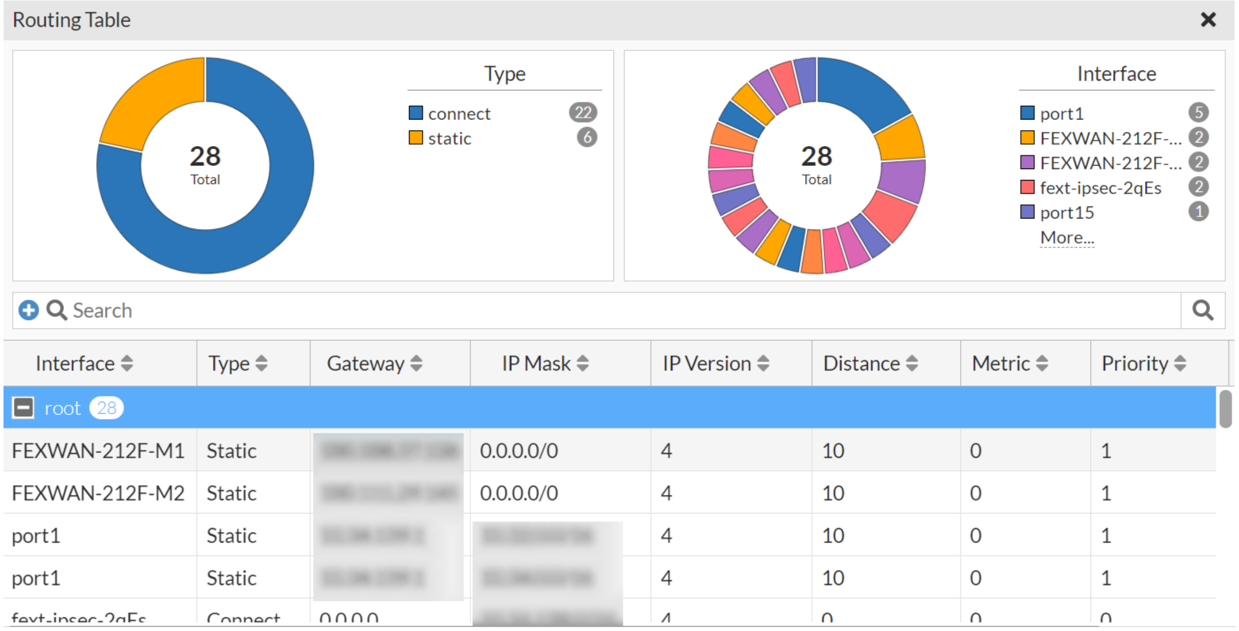
ARP Table

Search

Age	Interface	IP	MAC Address
⊟ root 4			
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.



Routing Table

Type

🟦 connect	22
🟧 static	6

Interface

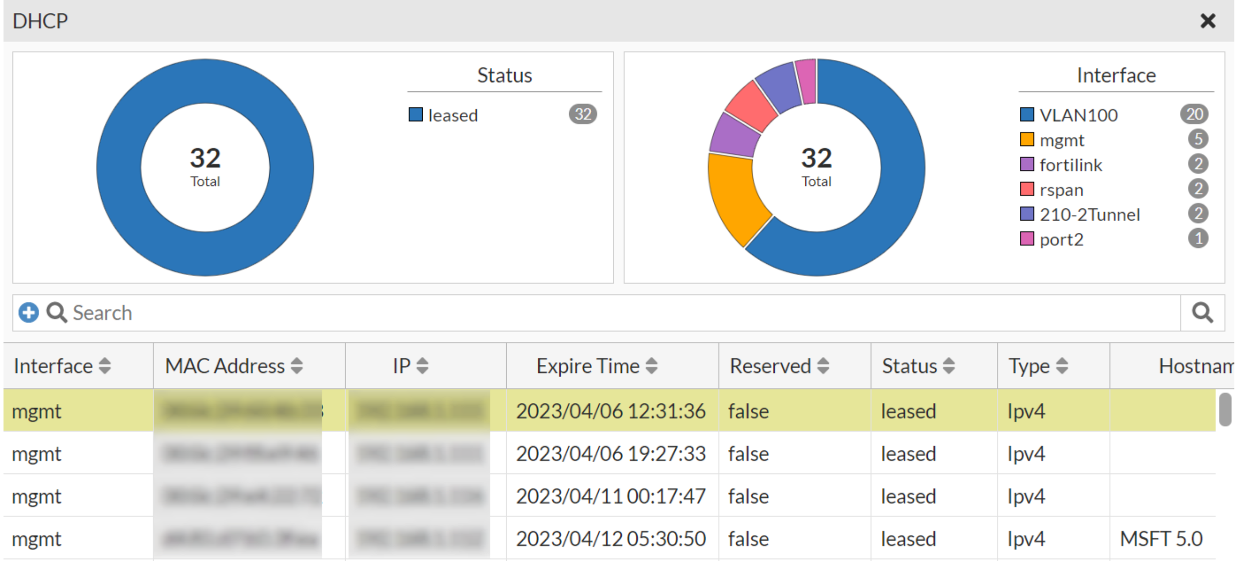
🟦 port1	5
🟧 FEXWAN-212F-...	2
🟪 FEXWAN-212F-...	2
🟥 fext-ipsec-2qEs	2
🟦 port15	1

More...

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.



DHCP

Status

🟦 leased	32

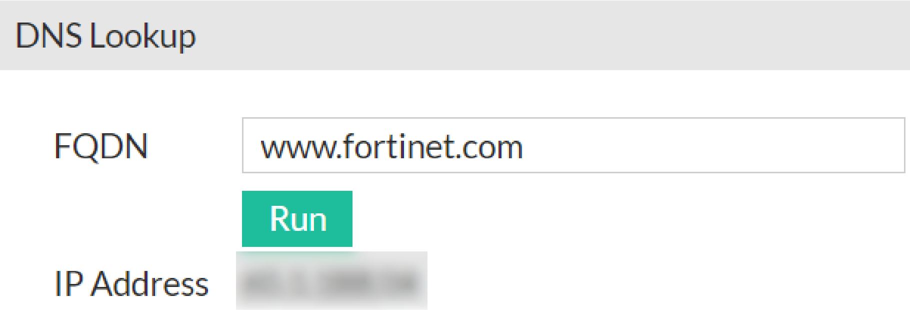
Interface

🟦 VLAN100	20
🟧 mgmt	5
🟪 fortilink	2
🟥 rspan	2
🟦 210-2Tunnel	2
🟪 port2	1

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.



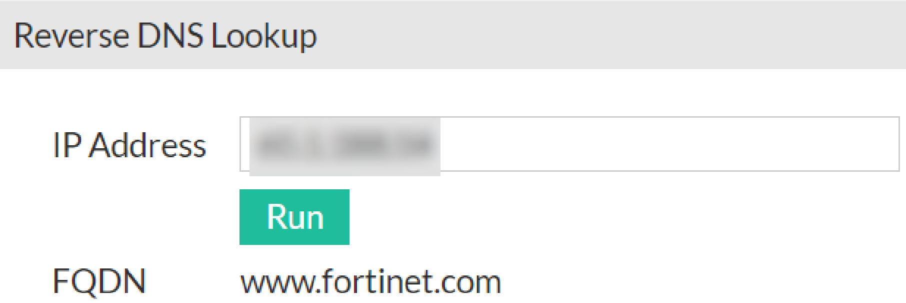
DNS Lookup

FQDN: www.fortinet.com

IP Address: [redacted]

Reverse DNS Lookup

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



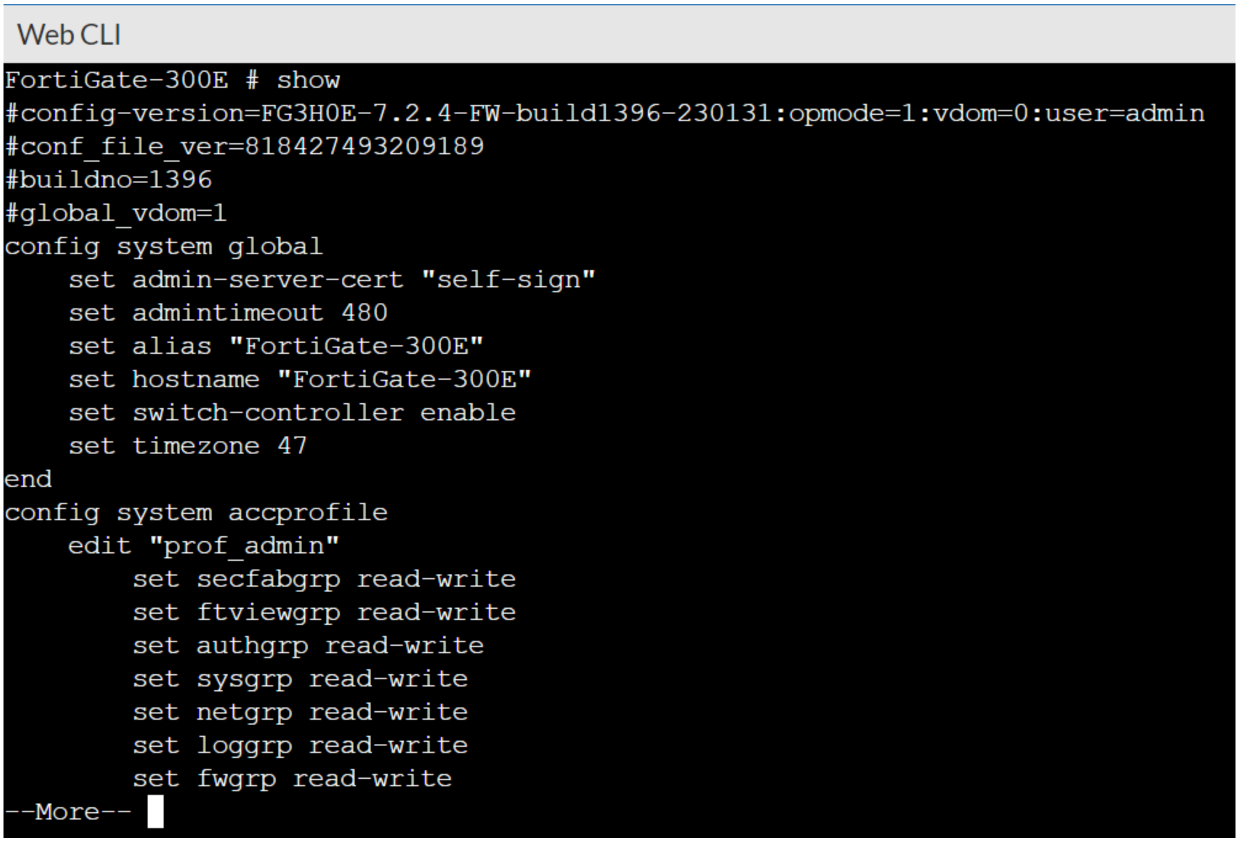
Reverse DNS Lookup

IP Address: [redacted]

FQDN: www.fortinet.com

Web CLI

Access the FortiGate's command line interface.

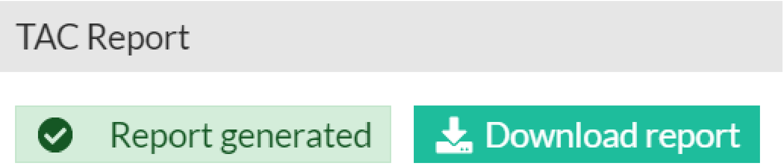


Web CLI

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

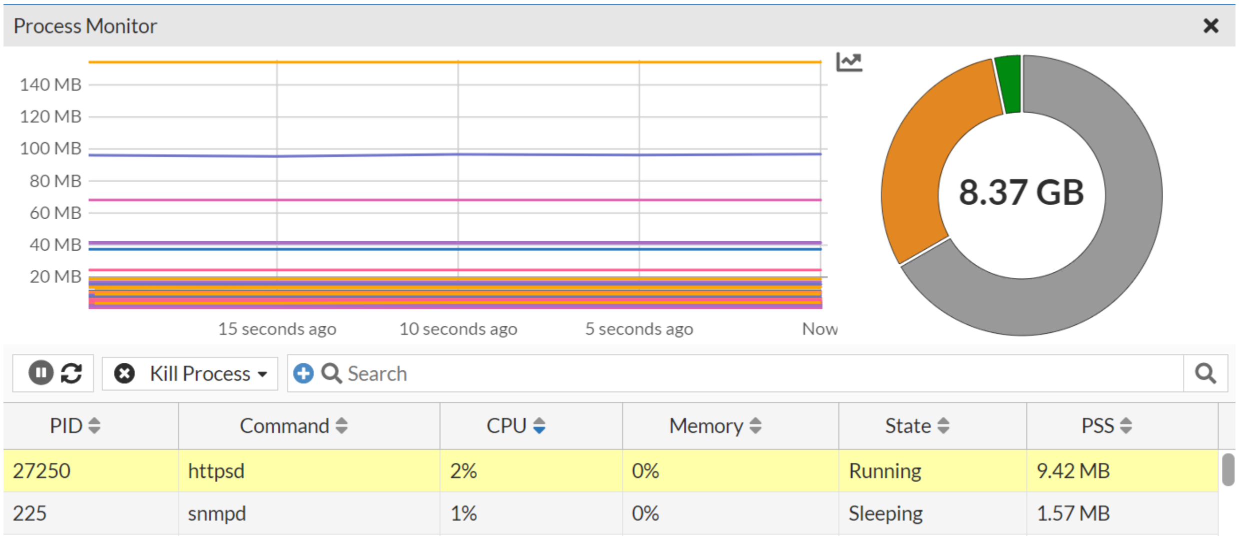
TAC Report

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



Process Monitor

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



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

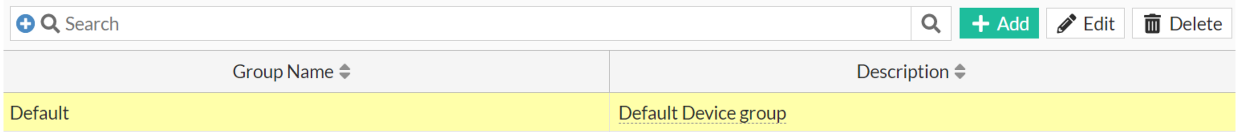
Select a process to perform any of the following operations.

- **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

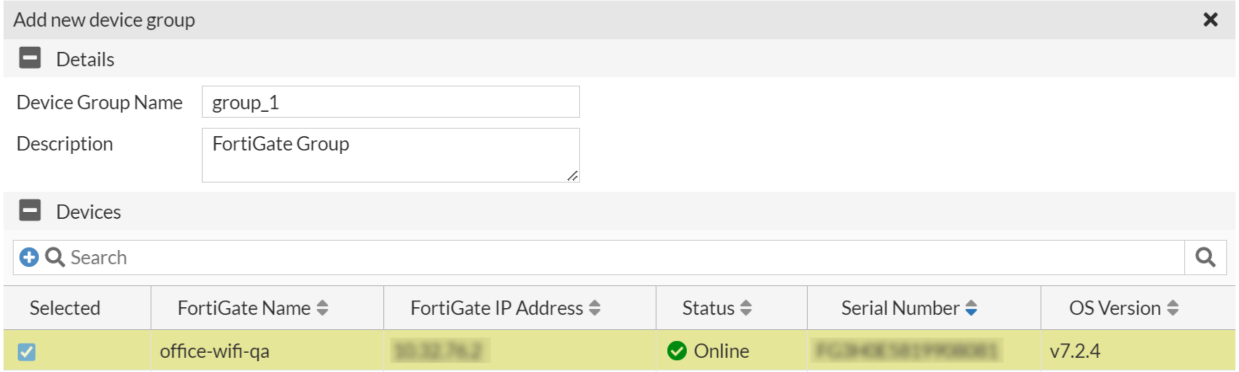
You can group FortiGate controllers for ease of management. Each controller can belong to only one group; if a controller is added to a second group, it is automatically removed from the previous group. Device groups allow administrators to manage devices in a certain way, such as, provide specific access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

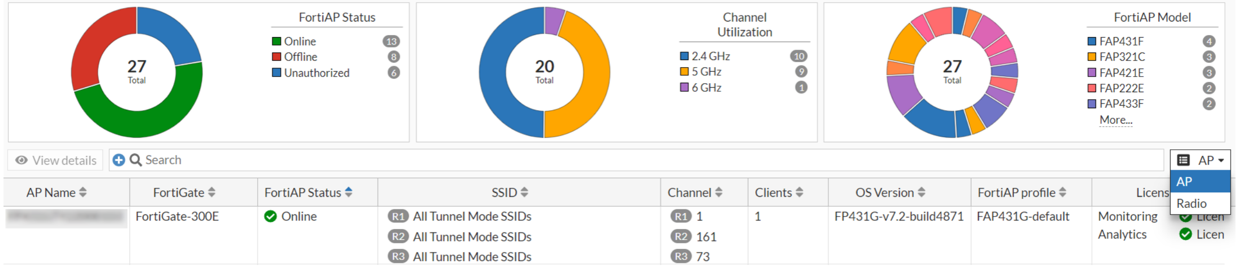
Wireless

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.

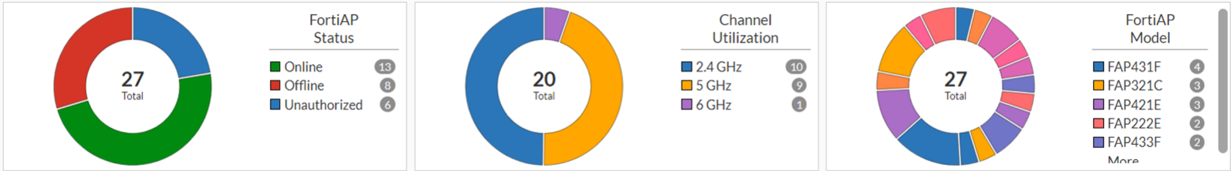


AP Name	FortiGate	FortiAP Status	SSID	Channel	Clients	OS Version	FortiAP profile	Licens
[redacted]	FortiGate-300E	✓ Online	R1 All Tunnel Mode SSIDs R2 All Tunnel Mode SSIDs R3 All Tunnel Mode SSIDs	R1 1 R2 161 R3 73	1	FP431G-v7.2-build4871	FAP431G-default	Monitoring ✓ Licen Analytics ✓ Licen

- 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**.

Channel Utilization

The Channel Utilization widget provides information about the utilization of each channel used by the APs 2.4GHz, 5GHz and 6GHz bands. Hovering over the chart displays the number of APs in that band and the state. Following states are displayed based on the channel utilization percentage.

State	Channel Utilization
Good	0 - 60%
Fair	61 - 75%
Poor	> 75%

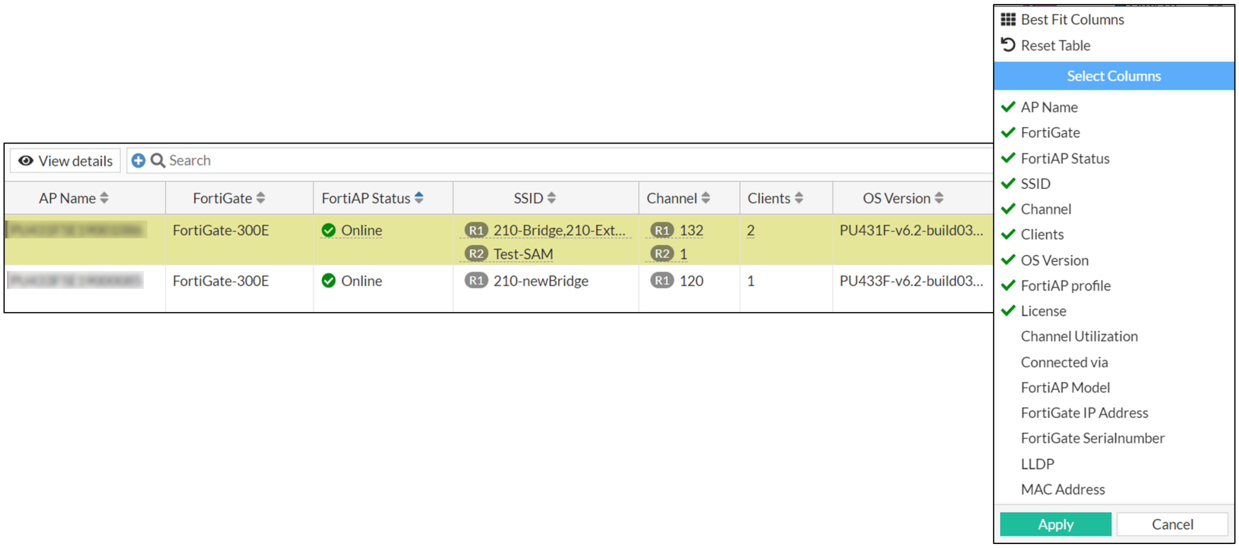
FortiAP Model

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.

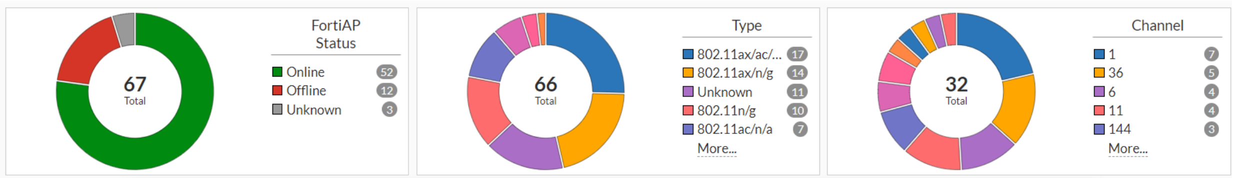
To filter the AP list based on the column data, click the filter icon in the column header next to the title, select the value to be filtered and click **Apply**.

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.

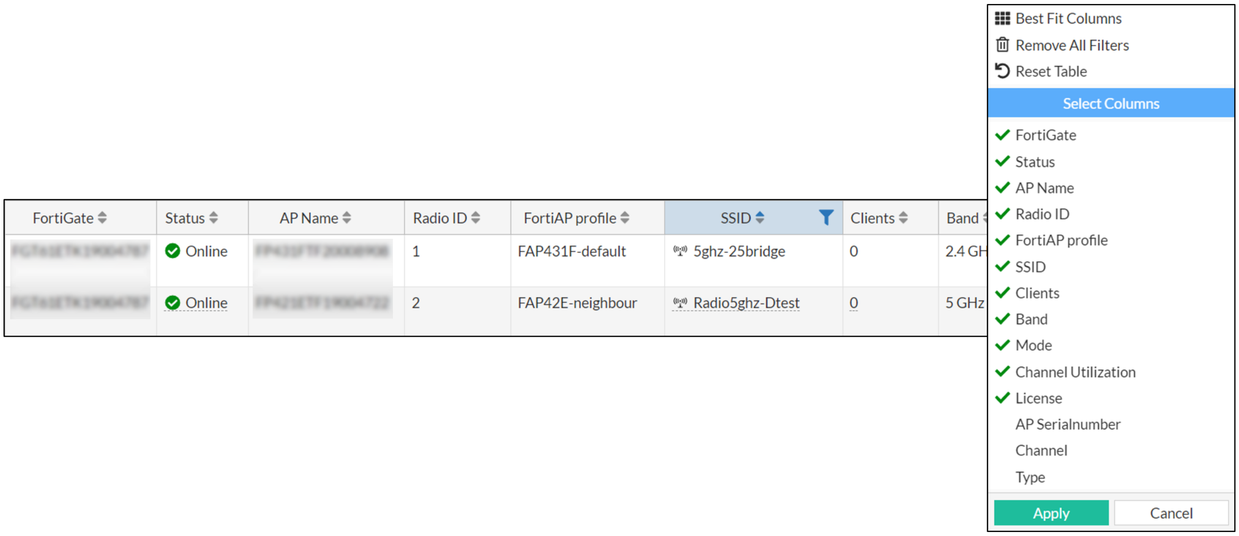
Channel

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.

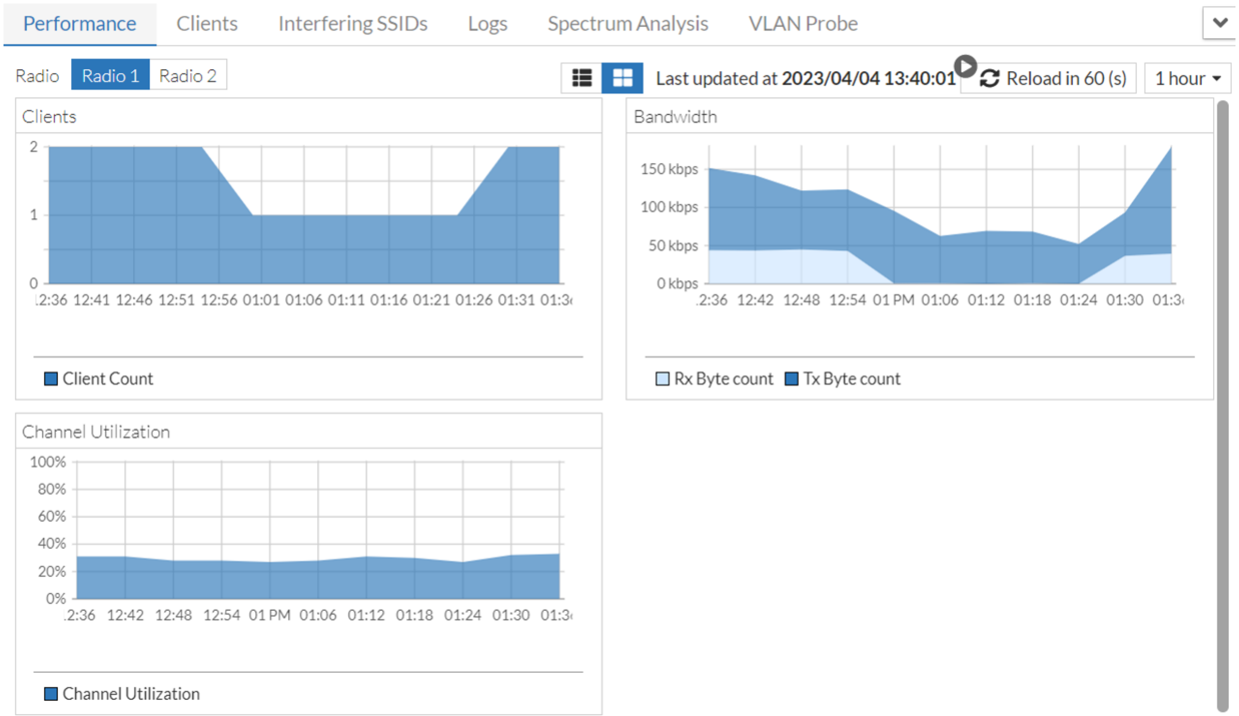
Access Points Diagnostics and Tools

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

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

Performance

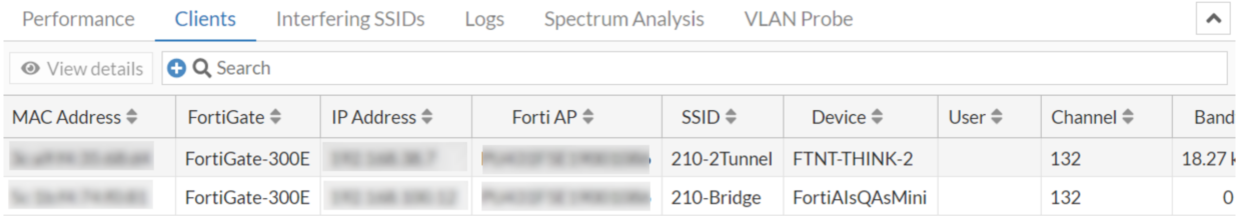
The performance tab displays the performance data for selected interval. It includes charts for Clients, Bandwidth and Channel Utilization. The default interval is 1 hour and can it be changed according to your requirements.



Clients

The Clients tab displays a list of clients currently connected to the selected AP, along with details such as the MAC address, FortiGate, IP Address, FortiAP, SSID, Device, User, Channel and other information. This information is useful for identifying any clients that may be experiencing connectivity issues or data usage problems.

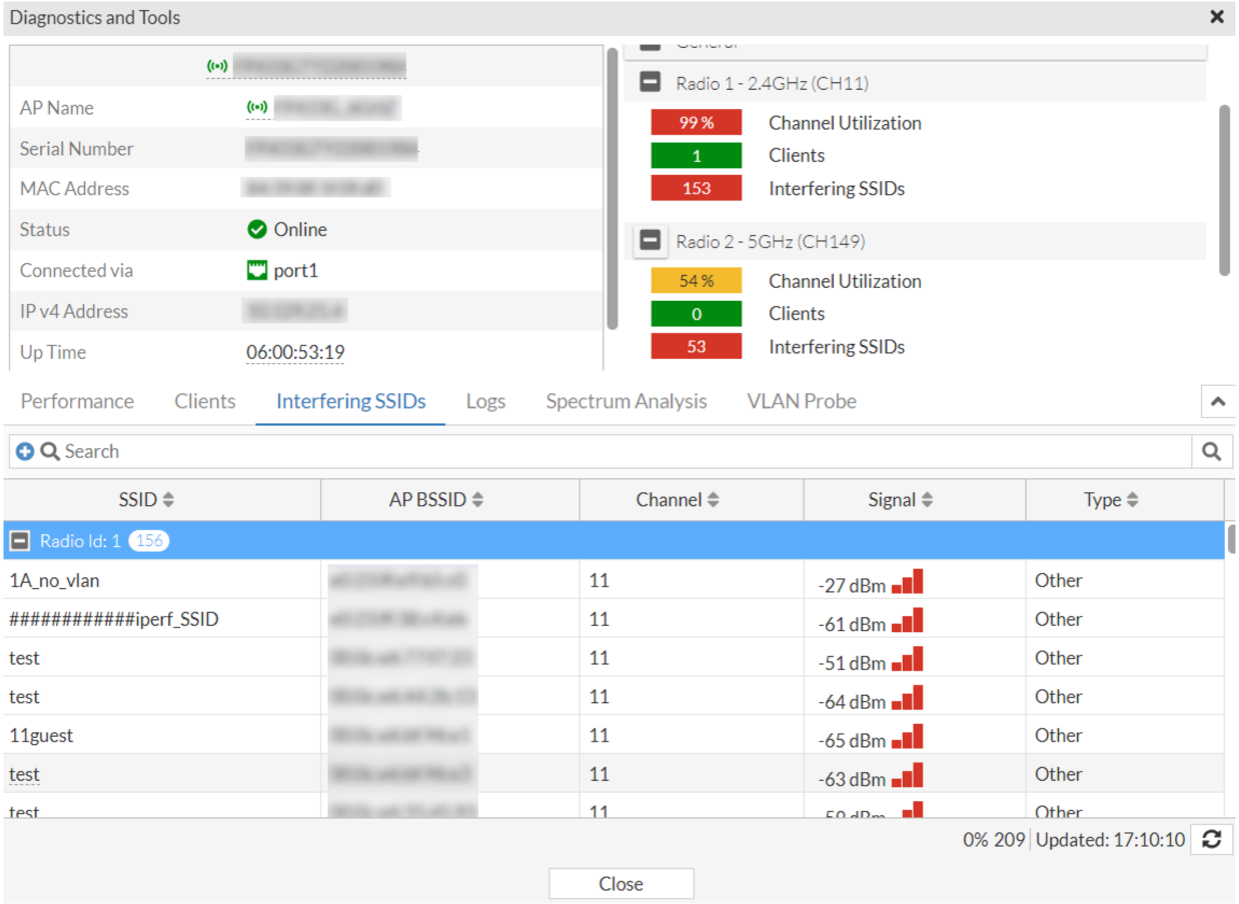
To view detailed information of a client, select the client and click **View details**.



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 SSID name, related AP BSSID, channel, signal strength and the Radio ID 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).



Diagnostics and Tools

	[redacted]
AP Name	[redacted]
Serial Number	[redacted]
MAC Address	[redacted]
Status	Online
Connected via	port1
IP v4 Address	[redacted]
Up Time	06:00:53:19

Radio 1 - 2.4GHz (CH11)

99 %	Channel Utilization
1	Clients
153	Interfering SSIDs

Radio 2 - 5GHz (CH149)

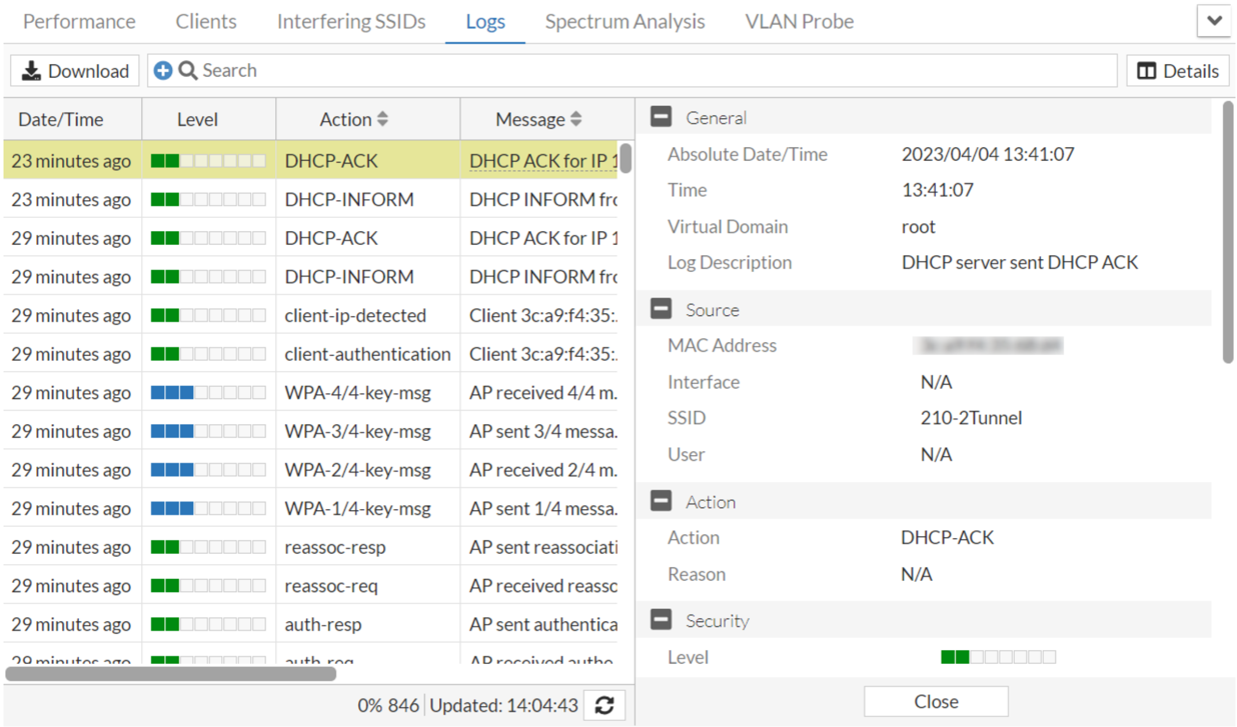
54 %	Channel Utilization
0	Clients
53	Interfering SSIDs

SSID	AP BSSID	Channel	Signal	Type
Radio Id: 1 156				
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
11guest	[redacted]	11	-65 dBm	Other
test	[redacted]	11	-63 dBm	Other
test	[redacted]	11	-50 dBm	Other

0% 209 Updated: 17:10:10

Logs

The Logs tab provides detailed logs of events related to the selected AP/Radio. To view detailed information, select log and click **Details**. Click **Download** to download all the logs in .csv format.



Date/Time	Level	Action	Message
23 minutes ago	🟩🟩□□□□□□	DHCP-ACK	DHCP ACK for IP 1
23 minutes ago	🟩🟩□□□□□□	DHCP-INFORM	DHCP INFORM fro
29 minutes ago	🟩🟩□□□□□□	DHCP-ACK	DHCP ACK for IP 1
29 minutes ago	🟩🟩□□□□□□	DHCP-INFORM	DHCP INFORM fro
29 minutes ago	🟩🟩□□□□□□	client-ip-detected	Client 3c:a9:f4:35:.
29 minutes ago	🟩🟩□□□□□□	client-authentication	Client 3c:a9:f4:35:.
29 minutes ago	🟦🟦🟦□□□□□	WPA-4/4-key-msg	AP received 4/4 m.
29 minutes ago	🟦🟦🟦□□□□□	WPA-3/4-key-msg	AP sent 3/4 messa.
29 minutes ago	🟦🟦🟦□□□□□	WPA-2/4-key-msg	AP received 2/4 m.
29 minutes ago	🟦🟦🟦□□□□□	WPA-1/4-key-msg	AP sent 1/4 messa.
29 minutes ago	🟩🟩□□□□□□	reassoc-resp	AP sent reassociati
29 minutes ago	🟩🟩□□□□□□	reassoc-req	AP received reassc
29 minutes ago	🟩🟩□□□□□□	auth-resp	AP sent authentica
29 minutes ago	🟩🟩□□□□□□	auth-req	AP received authe

0% 846 Updated: 14:04:43

General

Absolute Date/Time	2023/04/04 13:41:07
Time	13:41:07
Virtual Domain	root
Log Description	DHCP server sent DHCP ACK

Source

MAC Address	[redacted]
Interface	N/A
SSID	210-2Tunnel
User	N/A

Action

Action	DHCP-ACK
Reason	N/A

Security

Level	🟩🟩□□□□□□

Close

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 not available for G Series FortiAPs.
- Spectrum analysis is only supported when the radio is in the monitor 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 both 2.4 GHz and 5 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.

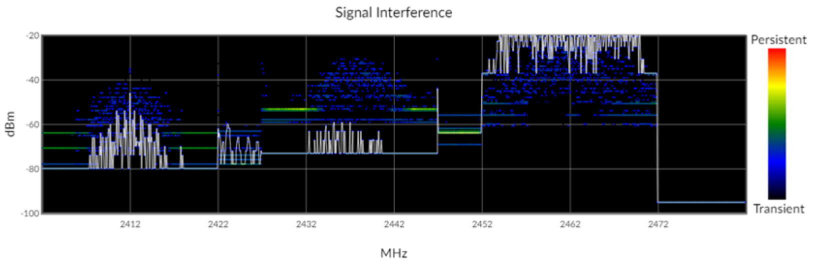
- You can select the **AP**, **Radio**, and **Channels** to be scanned for interferences.
- The **Scan Duration** can be set to 1, 5, 30, or 60 minutes.
- The **Sampling Interval** and the number of **Spectrogram Samples** cannot be modified.

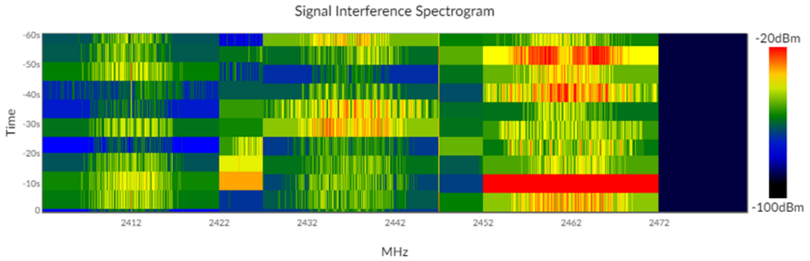
Select **Start** and the GUI periodically polls the spectrum analysis data based on the fixed sampling interval of 1000 milliseconds. Data is visualized as 4 charts representing signal interference marking the noise levels for each channel, signal interference spectrogram representing 60 samples for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

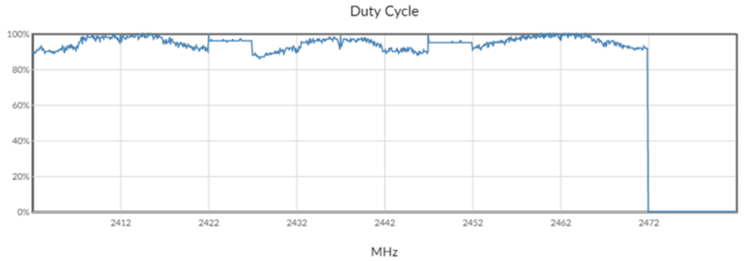
The tabular data for non-WiFi interference displays the time and frequency of last detection and any of the following type of devices causing the interference.

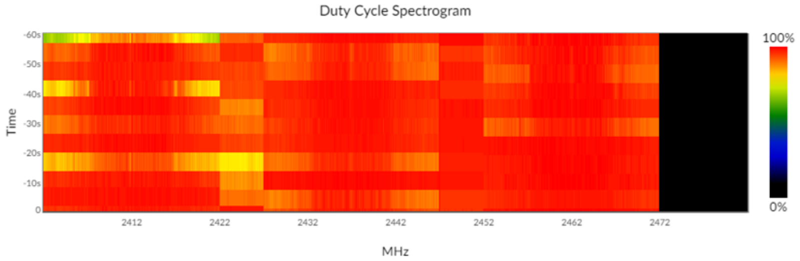
- Microwave ovens
- Video bridges
- Wi-Fi, DSSS cordless phones
- Bluetooth, FHSS cordless phones

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







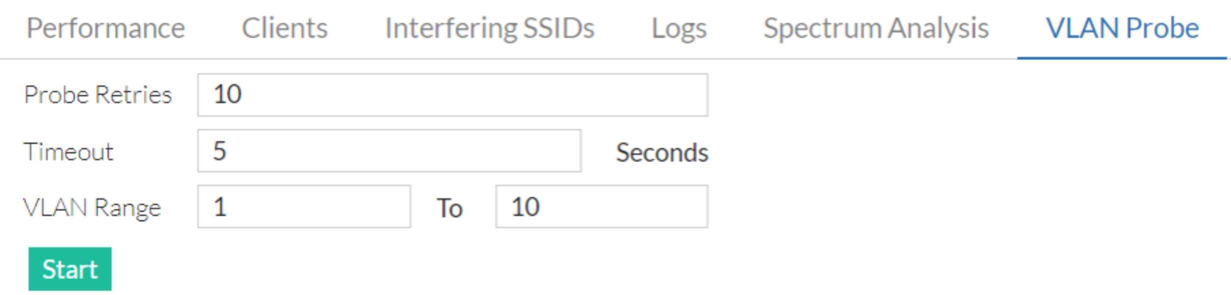


VLAN Probe

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.



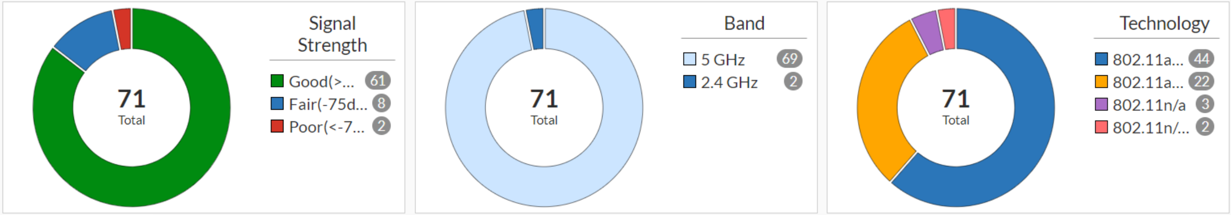
Probe Retries: 10

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.



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

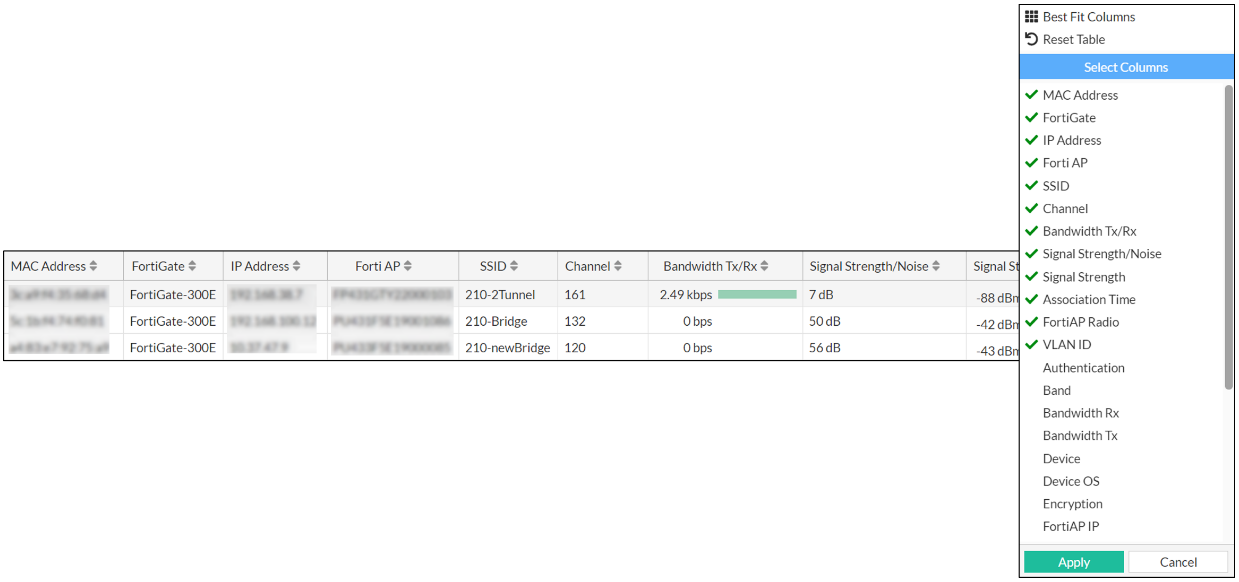
The band widget displays the band that each client is connected to. It indicates whether the client is connected to the 2.4 GHz, 5 GHz or 6 GHz band.

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.

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.

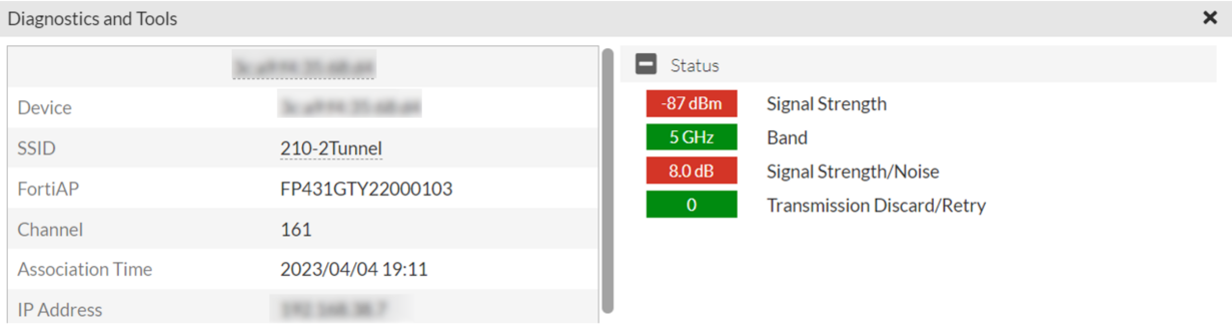


MAC Address	FortiGate	IP Address	Forti AP	SSID	Channel	Bandwidth Tx/Rx	Signal Strength/Noise	Signal St
[redacted]	FortiGate-300E	[redacted]	[redacted]	210-2Tunnel	161	2.49 kbps	7 dB	-88 dBm
[redacted]	FortiGate-300E	[redacted]	[redacted]	210-Bridge	132	0 bps	50 dB	-42 dBm
[redacted]	FortiGate-300E	[redacted]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



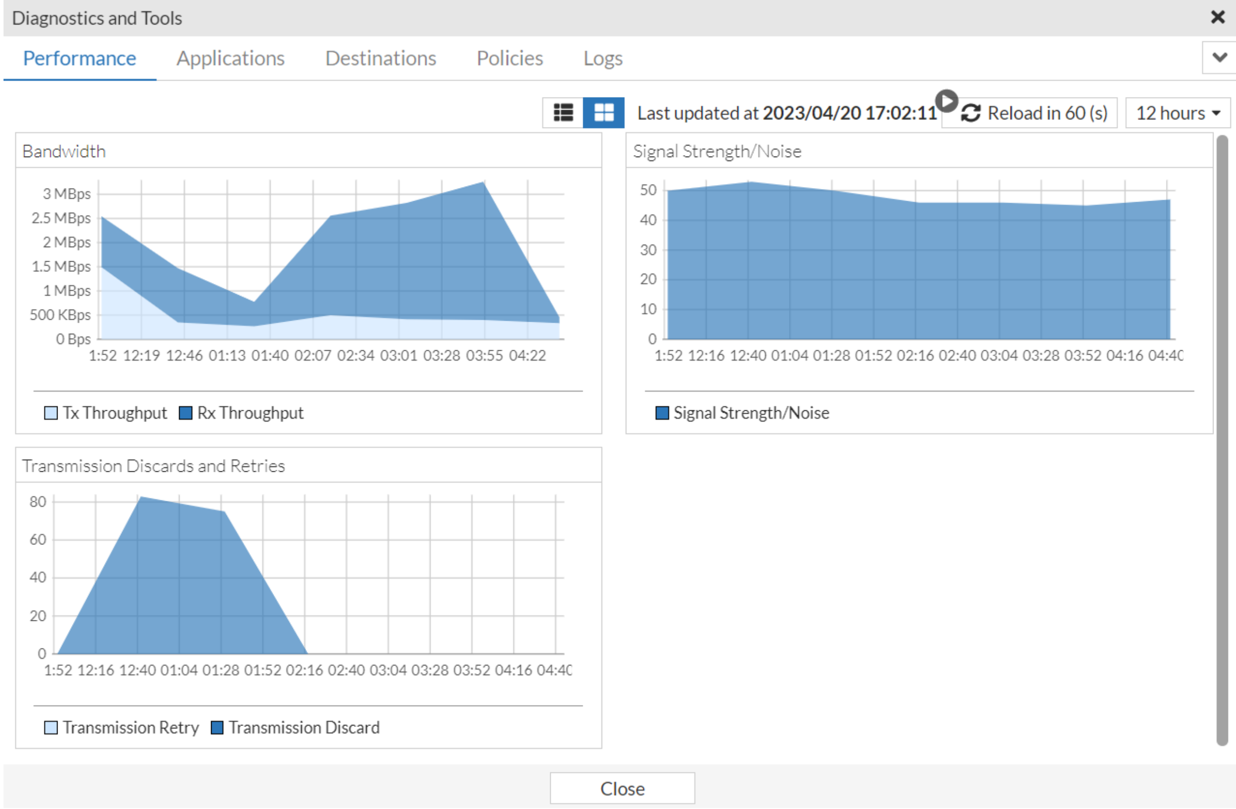
[redacted]

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

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

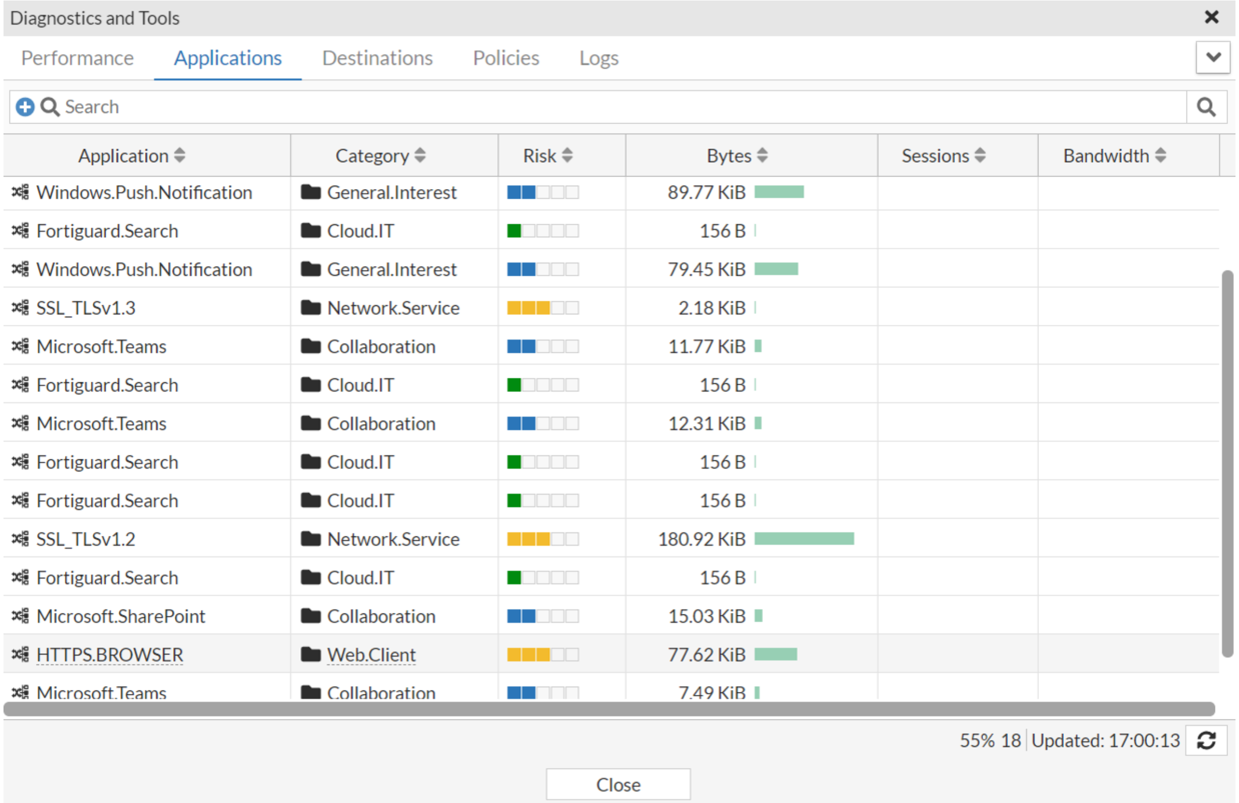
Performance

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



Applications

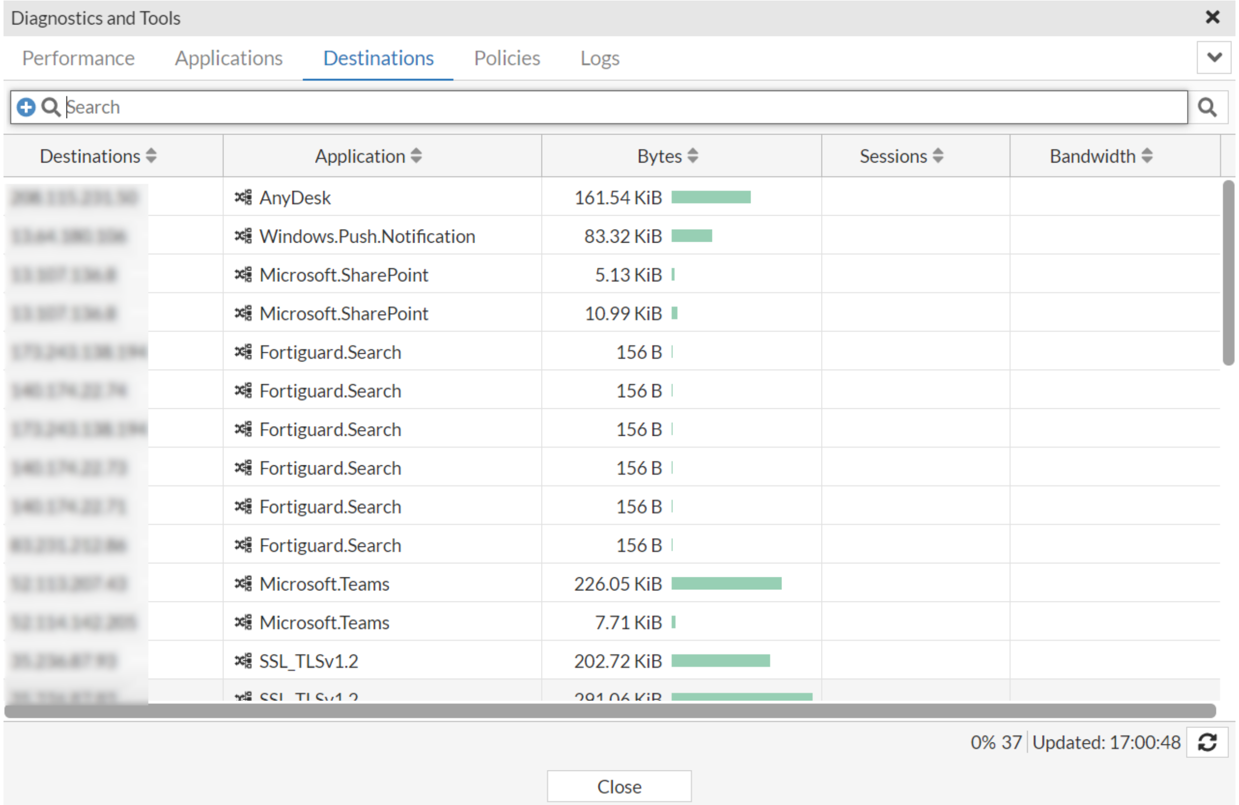
The Applications tab displays a list of applications in use by the selected client, along with details such as the application name, category, risk, data usage, session and bandwidth details.



Application	Category	Risk	Bytes	Sessions	Bandwidth
Windows.Push.Notification	General.Interest	🟦🟦□□□	89.77 KiB		
Fortiguard.Search	Cloud.IT	🟩□□□□	156 B		
Windows.Push.Notification	General.Interest	🟦🟦□□□	79.45 KiB		
SSL_TLSv1.3	Network.Service	🟨🟨🟨□□	2.18 KiB		
Microsoft.Teams	Collaboration	🟦🟦□□□	11.77 KiB		
Fortiguard.Search	Cloud.IT	🟩□□□□	156 B		
Microsoft.Teams	Collaboration	🟦🟦□□□	12.31 KiB		
Fortiguard.Search	Cloud.IT	🟩□□□□	156 B		
Fortiguard.Search	Cloud.IT	🟩□□□□	156 B		
SSL_TLSv1.2	Network.Service	🟨🟨🟨□□	180.92 KiB		
Fortiguard.Search	Cloud.IT	🟩□□□□	156 B		
Microsoft.SharePoint	Collaboration	🟦🟦□□□	15.03 KiB		
HTTPS.BROWSER	Web.Client	🟨🟨🟨□□	77.62 KiB		
Microsoft.Teams	Collaboration	🟦🟦□□□	7.49 KiB		

Destinations

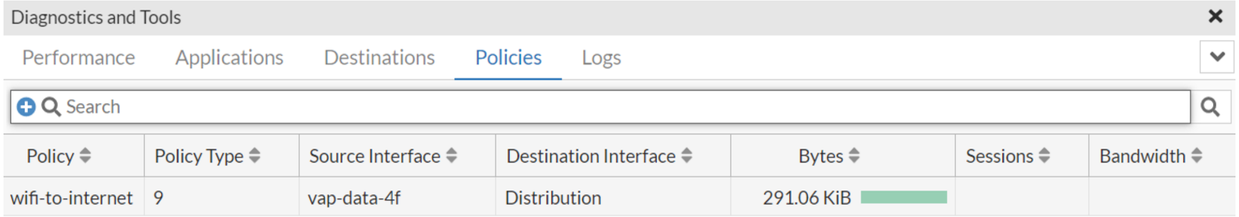
The Destinations tab displays a list of network destinations accessed by the selected client, along with details such as the destination IP address, application name, data usage, session and bandwidth details.



Destinations	Application	Bytes	Sessions	Bandwidth
[redacted]	AnyDesk	161.54 KiB		
[redacted]	Windows.Push.Notification	83.32 KiB		
[redacted]	Microsoft.SharePoint	5.13 KiB		
[redacted]	Microsoft.SharePoint	10.99 KiB		
[redacted]	Fortiguard.Search	156 B		
[redacted]	Fortiguard.Search	156 B		
[redacted]	Fortiguard.Search	156 B		
[redacted]	Fortiguard.Search	156 B		
[redacted]	Fortiguard.Search	156 B		
[redacted]	Fortiguard.Search	156 B		
[redacted]	Microsoft.Teams	226.05 KiB		
[redacted]	Microsoft.Teams	7.71 KiB		
[redacted]	SSL_TLSv1.2	202.72 KiB		
[redacted]	SSL_TLSv1.2	291.06 KiB		

Policies

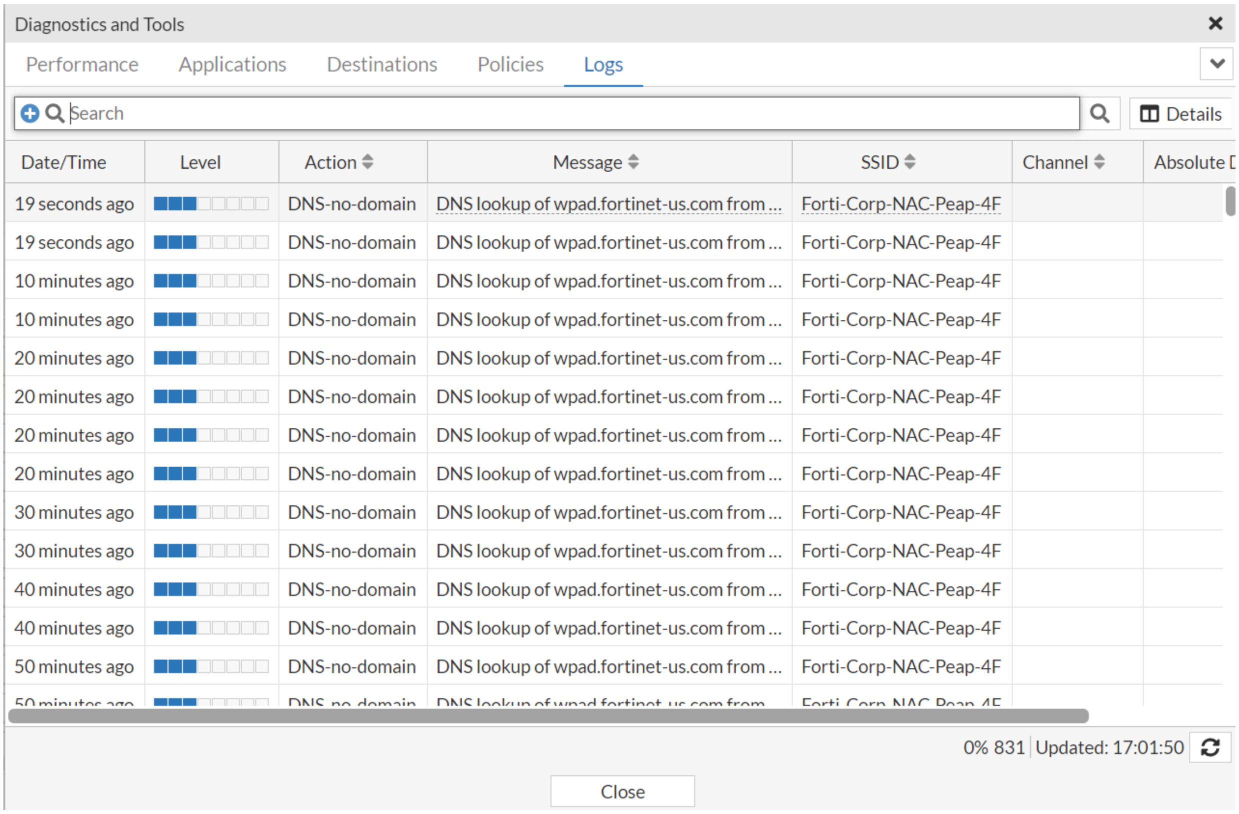
The Policies tab displays information about any policies applied to the selected client, such as policy name, policy type, source interface, destination interface, data usage, session and bandwidth details.



Policy	Policy Type	Source Interface	Destination Interface	Bytes	Sessions	Bandwidth
wifi-to-internet	9	vap-data-4f	Distribution	291.06 KiB		

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**.

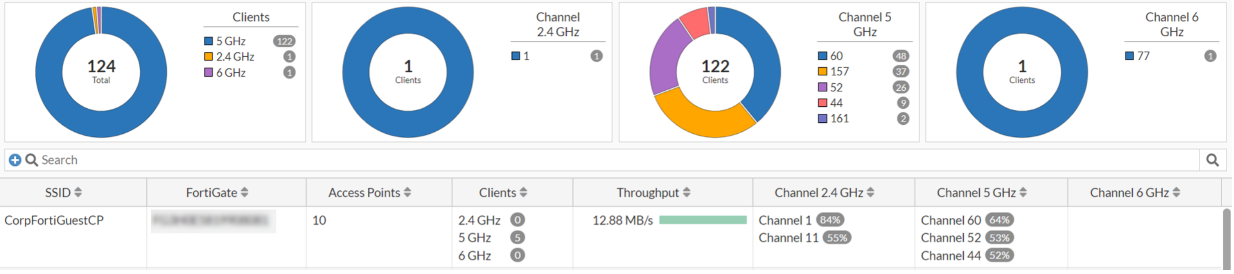


Date/Time	Level	Action	Message	SSID	Channel	Absolute
19 seconds ago	■■■□□□□□	DNS-no-domain	DNS lookup of wpad.fortinet-us.com from ...	Forti-Corp-NAC-Peap-4F		
19 seconds ago	■■■□□□□□	DNS-no-domain	DNS lookup of wpad.fortinet-us.com from ...	Forti-Corp-NAC-Peap-4F		
10 minutes ago	■■■□□□□□	DNS-no-domain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

The Channel Summary page provides detailed summary of channel utilization. It consists of four widgets - Stations, Channel 2.4 GHz, Channel 5 GHz and Channel 6 GHz.



SSID	FortiGate	Access Points	Clients	Throughput	Channel 2.4 GHz	Channel 5 GHz	Channel 6 GHz
CorpFortiGuestCP	[redacted]	10	2.4 GHz 0 5 GHz 5 6 GHz 0	12.88 MB/s	Channel 1 84% Channel 11 55%	Channel 60 64% Channel 52 53% Channel 44 52%	

Stations

The Stations widget displays the number of stations currently connected to the wireless network. This includes both the total number of stations and the number of clients connected to each band - 2.4 GHz, 5 GHz and 6 GHz.

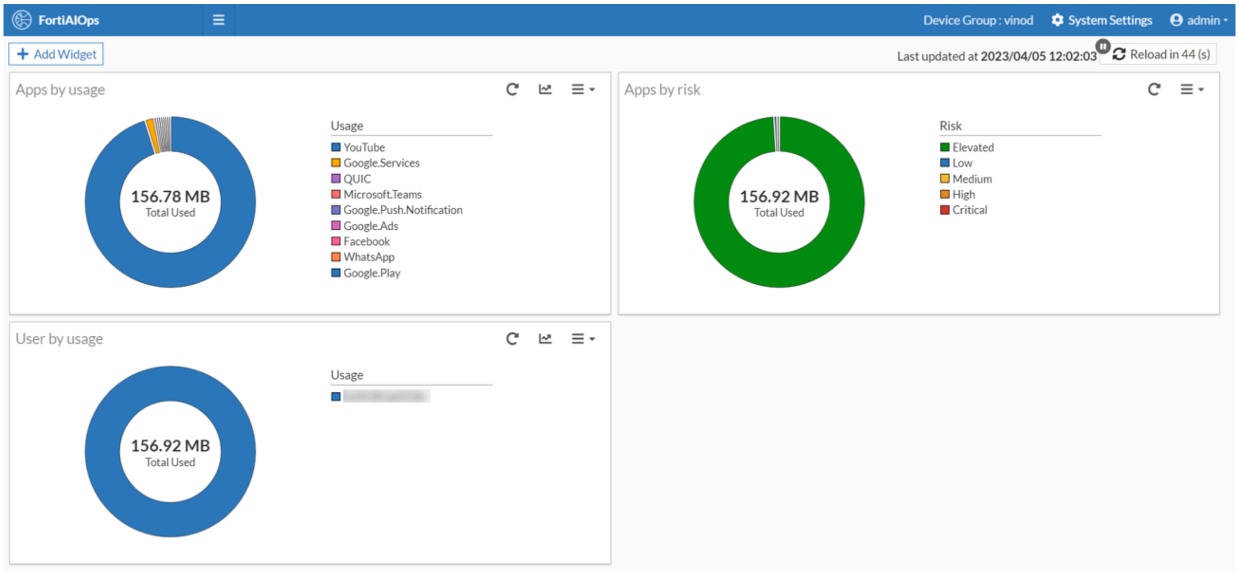
Channel

The Channel widget displays information about the channels used by the wireless network. This includes the channel number, and the number of access points using each channel.

The Channel List provides detailed information about each channel used by the wireless network. This includes the SSID, FortiGate, access points, stations, throughput and channel 2.4 GHz, channel 5 GHz and channel 6 GHz. details.

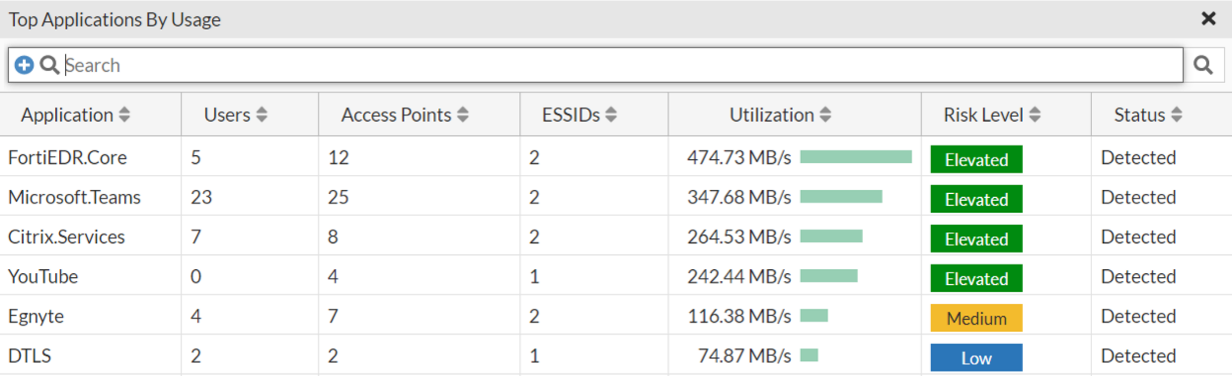
Applications

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.

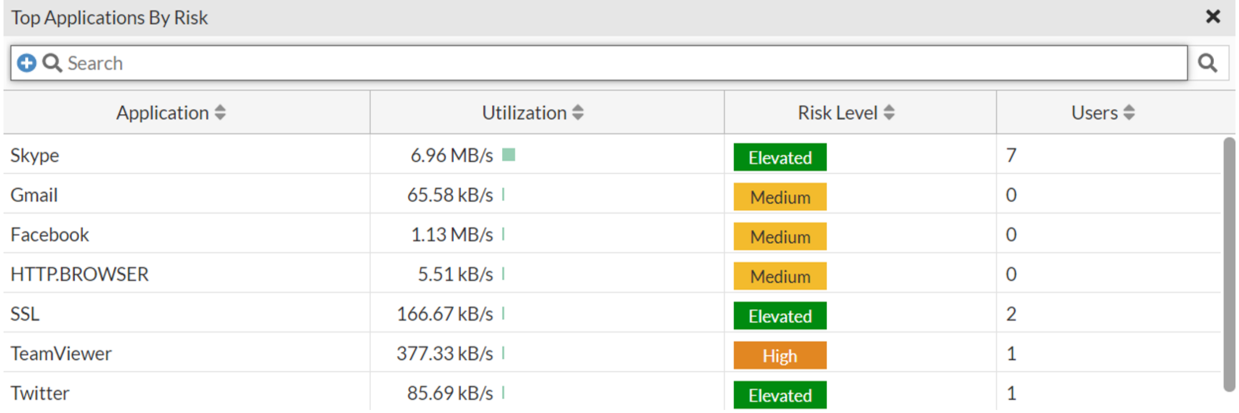

Top Applications By Usage

Search

Application	Users	Access Points	ESSIDs	Utilization	Risk Level	Status
FortiEDR.Core	5	12	2	474.73 MB/s	Elevated	Detected
Microsoft.Teams	23	25	2	347.68 MB/s	Elevated	Detected
Citrix.Services	7	8	2	264.53 MB/s	Elevated	Detected
YouTube	0	4	1	242.44 MB/s	Elevated	Detected
Egnyte	4	7	2	116.38 MB/s	Medium	Detected
DTLS	2	2	1	74.87 MB/s	Low	Detected

Apps by risk

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



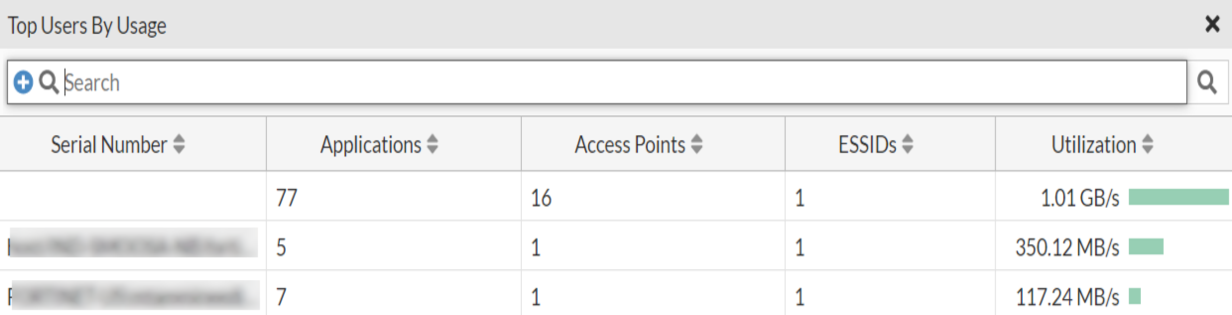
Top Applications By Risk

Search

Application	Utilization	Risk Level	Users
Skype	6.96 MB/s	Elevated	7
Gmail	65.58 kB/s	Medium	0
Facebook	1.13 MB/s	Medium	0
HTTP.BROWSER	5.51 kB/s	Medium	0
SSL	166.67 kB/s	Elevated	2
TeamViewer	377.33 kB/s	High	1
Twitter	85.69 kB/s	Elevated	1

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

Serial Number	Applications	Access Points	ESSIDs	Utilization
	77	16	1	1.01 GB/s
[redacted]	5	1	1	350.12 MB/s
[redacted]	7	1	1	117.24 MB/s

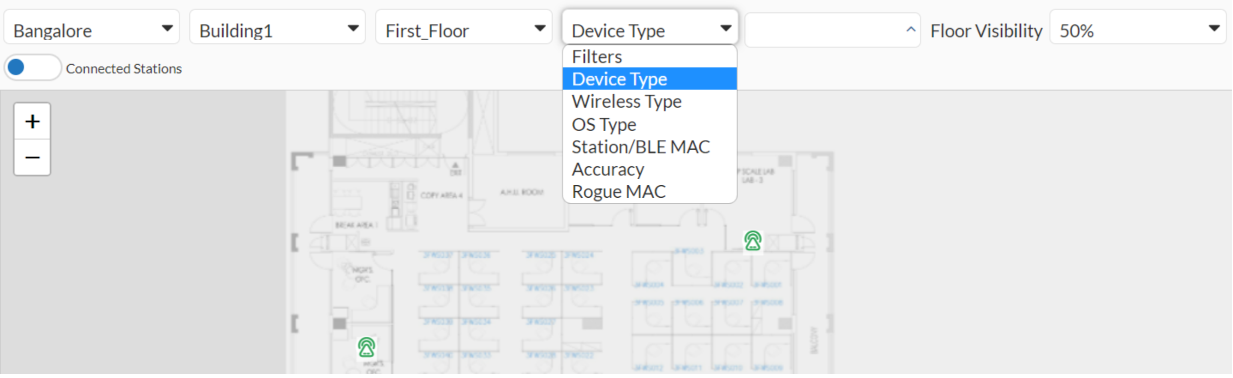
Location Services Monitor

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

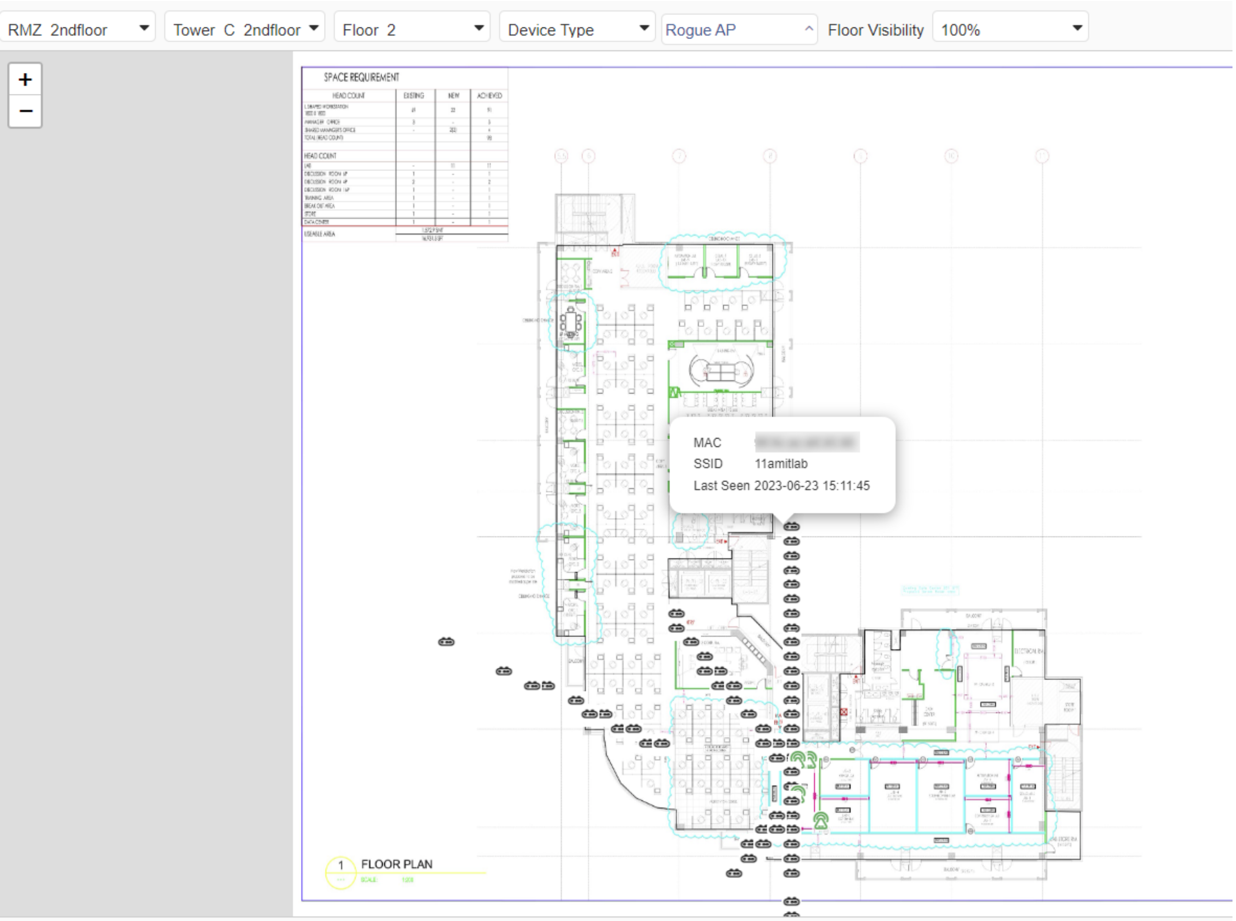
You can set the Floor Visibility and magnify the floor view.



Bangalore | Building1 | First_Floor | Device Type | Floor Visibility 50%

Connected Stations

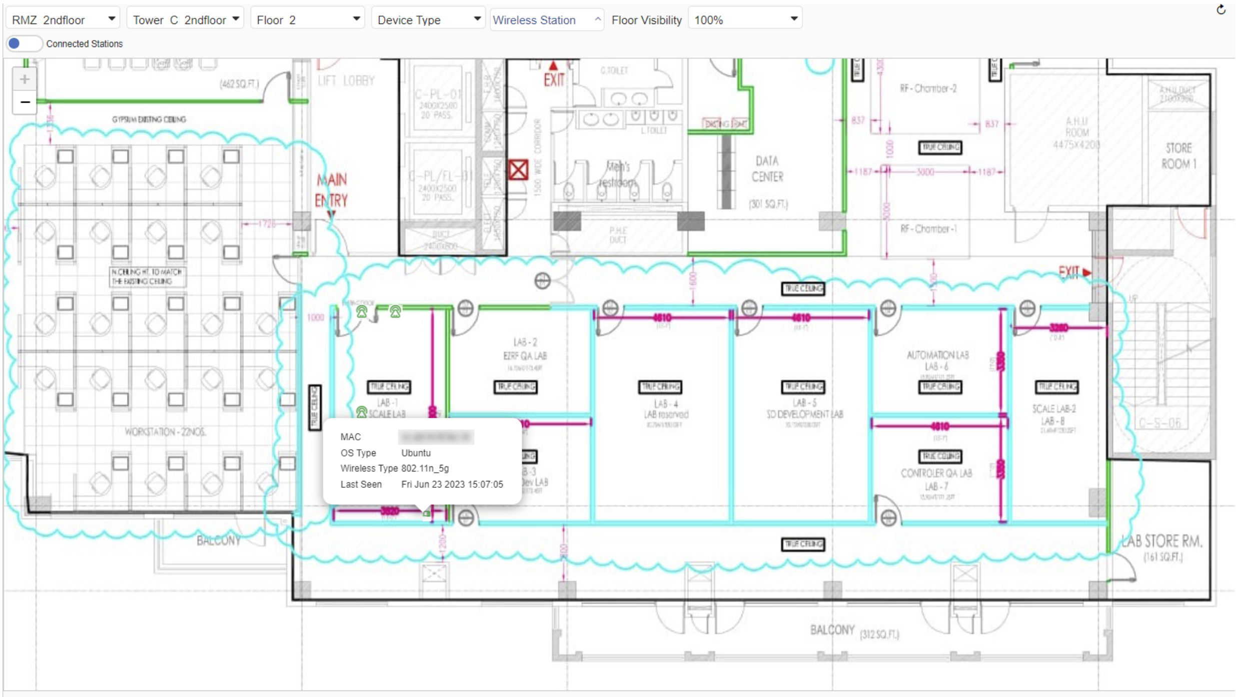
Select **Rogue AP** as the **Device Type**, to view the rouge AP location.



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.



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.

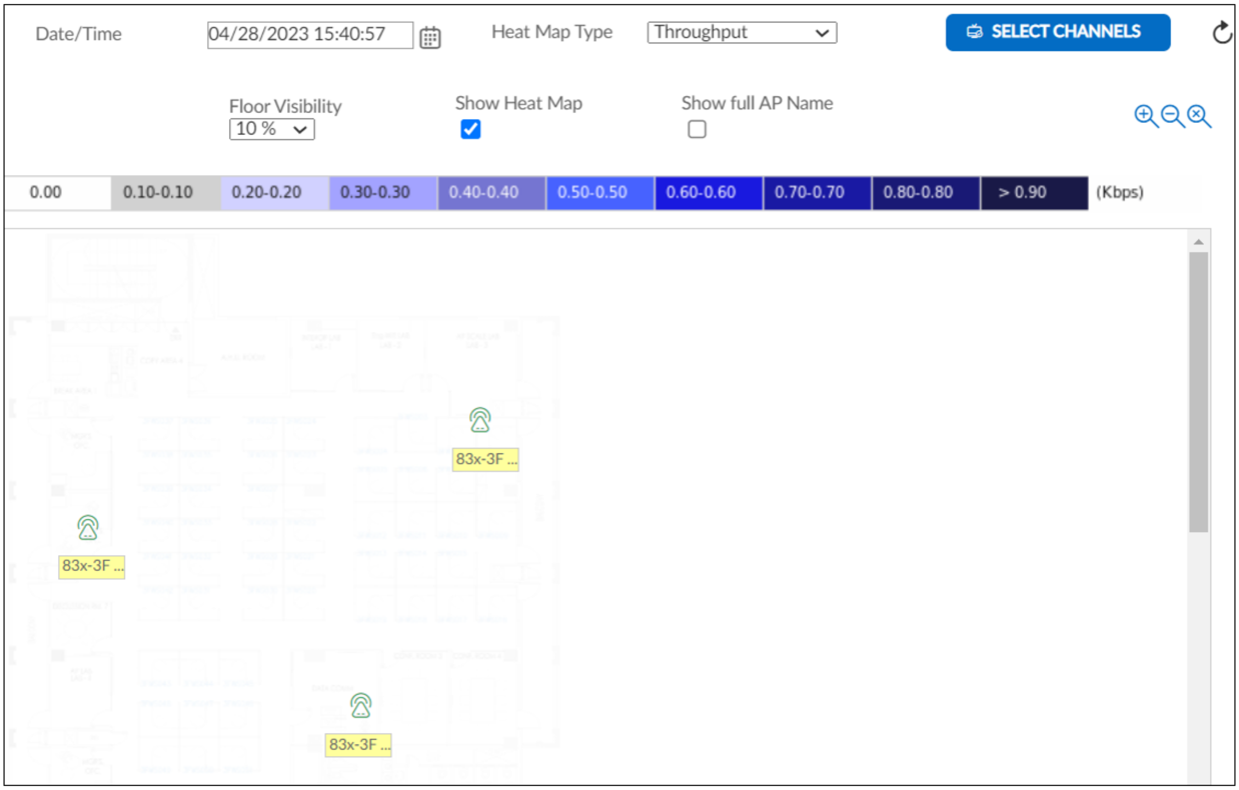
Heat Maps

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

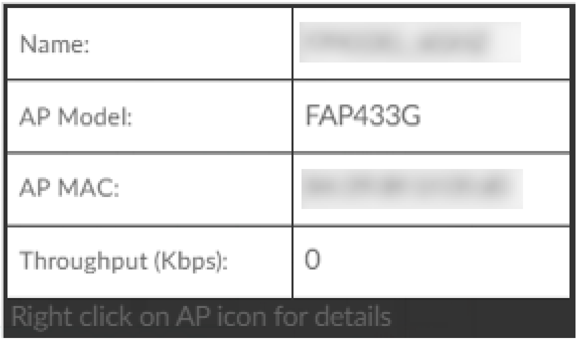
Floor Visibility 10 %

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.



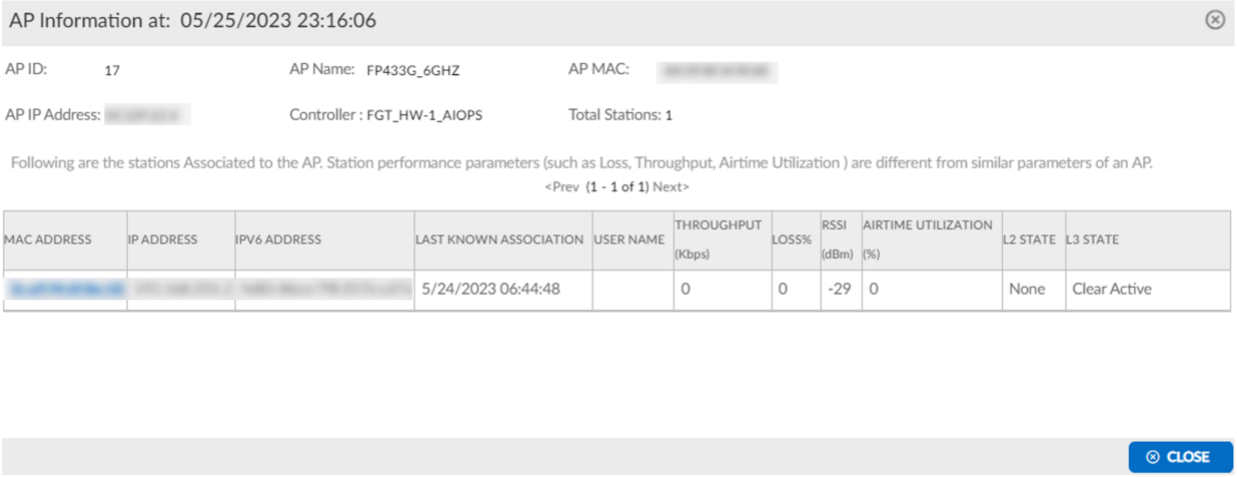
Name:	[redacted]
AP Model:	FAP433G
AP MAC:	[redacted]
Throughput (Kbps):	0

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.

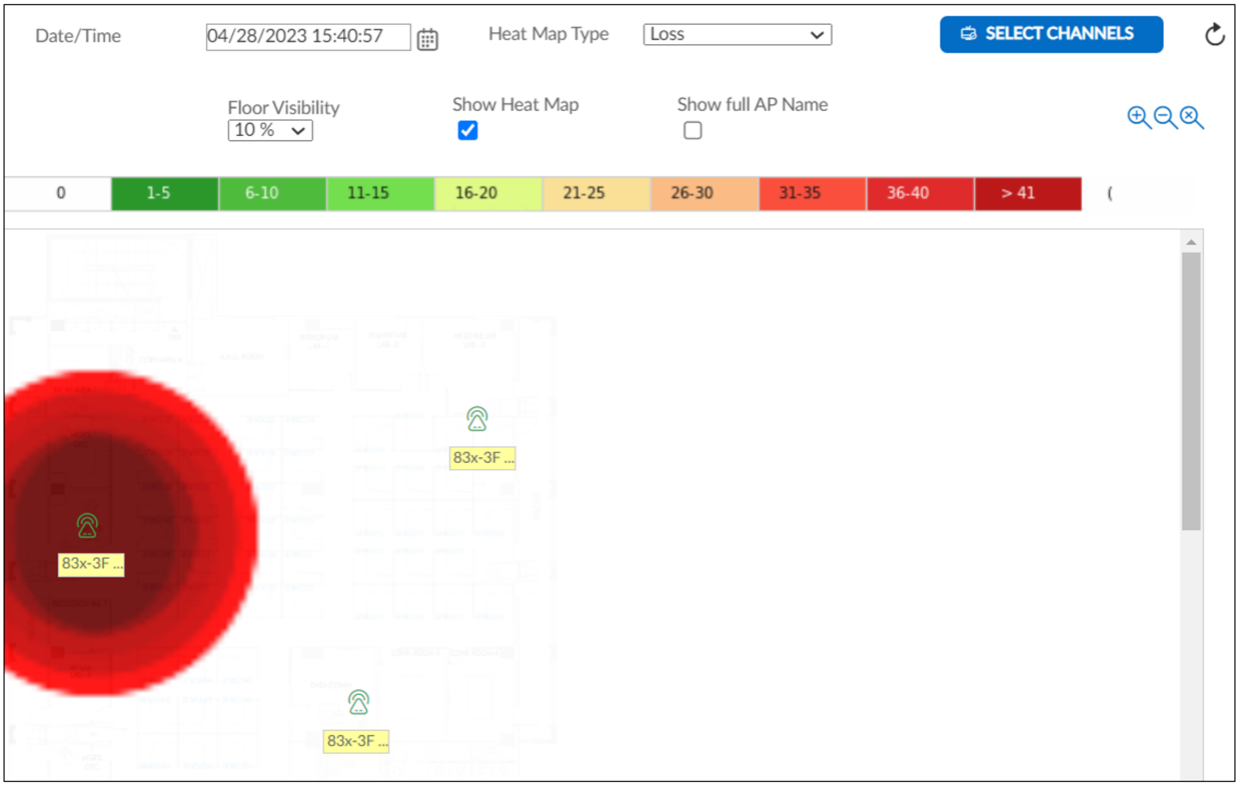
<Prev (1 - 1 of 1) Next>

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 %

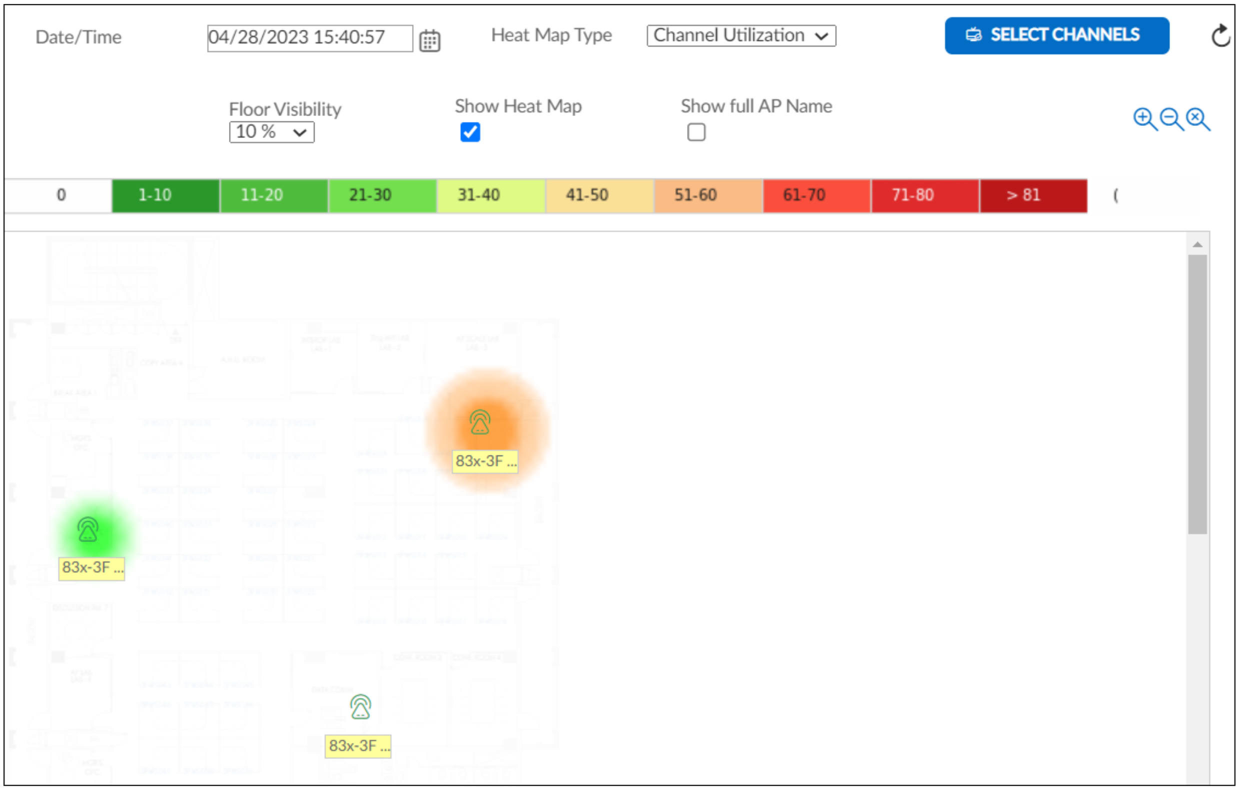
Show Heat Map ☑

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 %

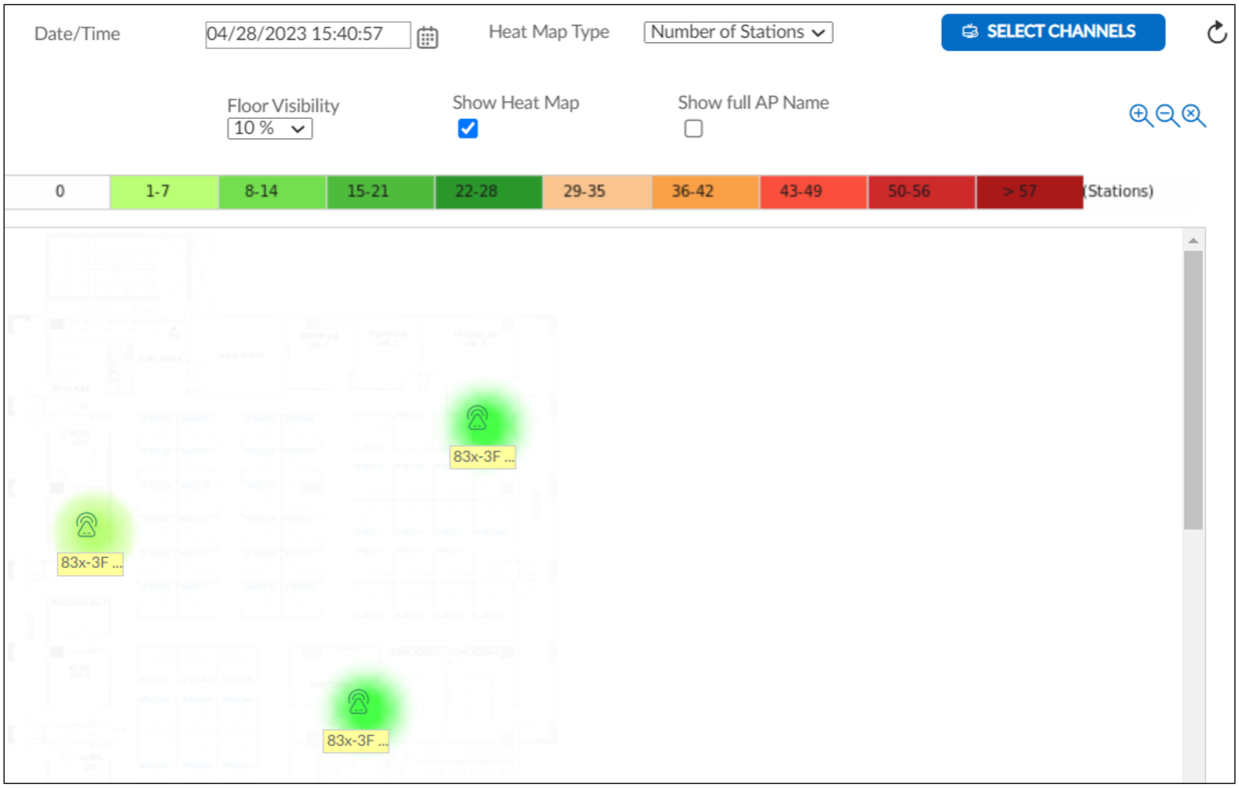
Show Heat Map ☑

Show full AP Name □

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 ☑

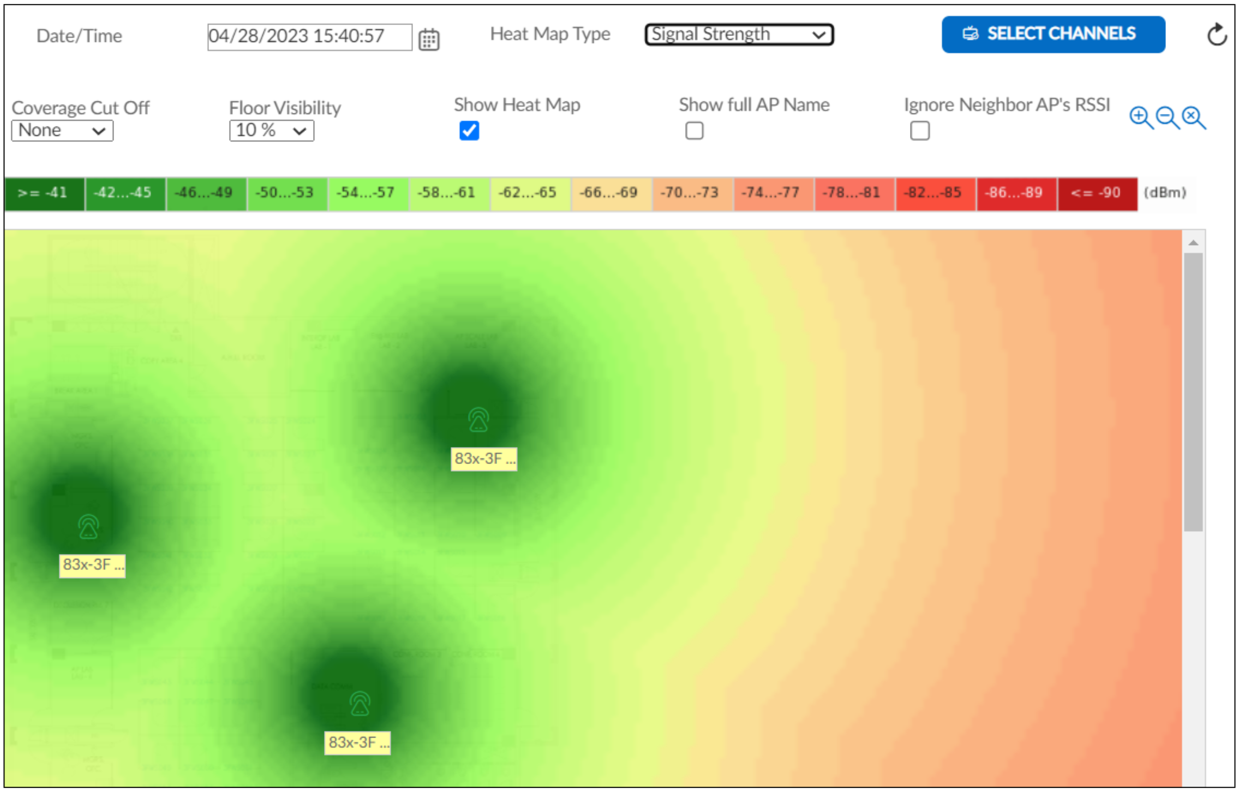
Show full AP Name ☐

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 ☐

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.

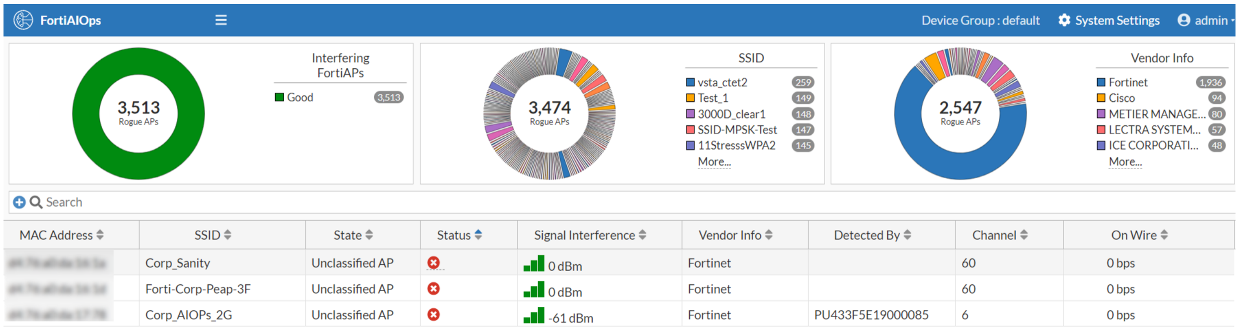
Coverage Cut Off: Coverage cutoff [default being none] can be used to see the signal coverage region within the cutoff value specified. The cutoff range is from -42dBM to -90dBM.

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.



FortiAIOps ☰ Device Group : default ⚙ System Settings admin

3,513
Rogue APs

Interfering FortiAPs	
🟩 Good	3,513

3,474
Rogue APs

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

2,547
Rogue APs

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

Search

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.

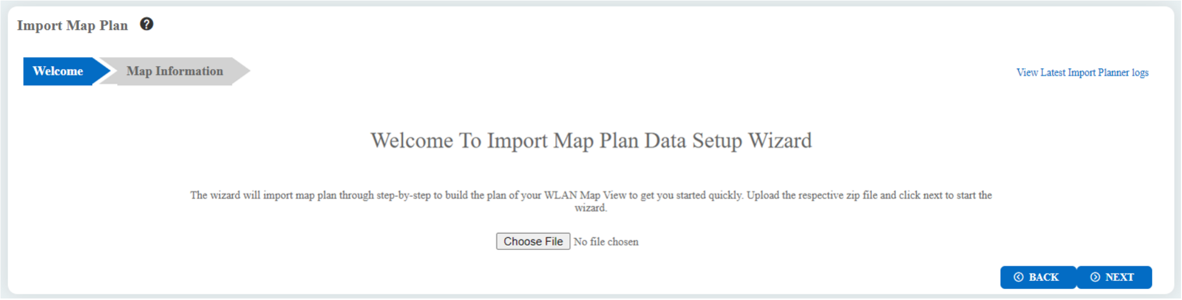
Next, add controllers and APs to the map.

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.



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:

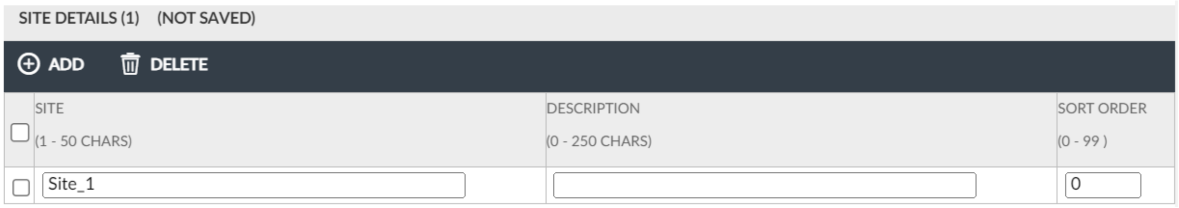
- **Add APs** - Select the APs to be added to the floor map.
- **Floor APs** - Select the APs to be deleted from the floor map.
- **Landmarks** - Add or delete landmarks on the floor map.
- **Change Image** - Upload a new image or delete an existing image from the floor map.

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:

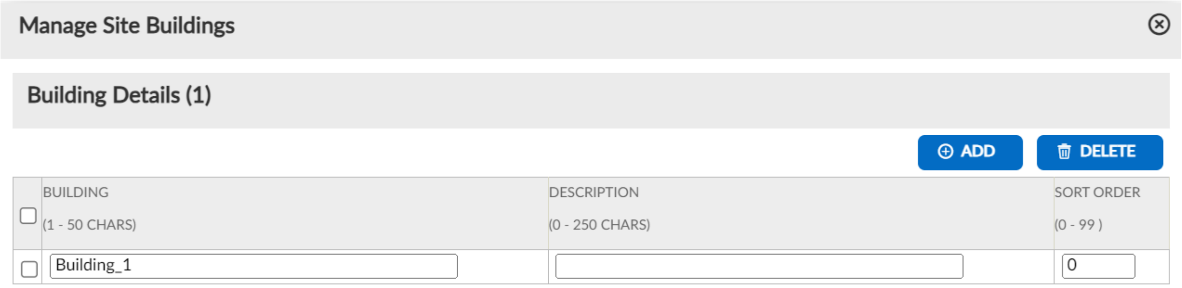
1. Navigate to **Wireless > Map Management** page. All current maps are displayed on the Map Management page.
2. To add a new site, click on the **Site Details** section and then click on **Add**. A new site can only be added to the top level, Enterprise, which is the default.



SITE DETAILS (1) (NOT SAVED)

□	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**.

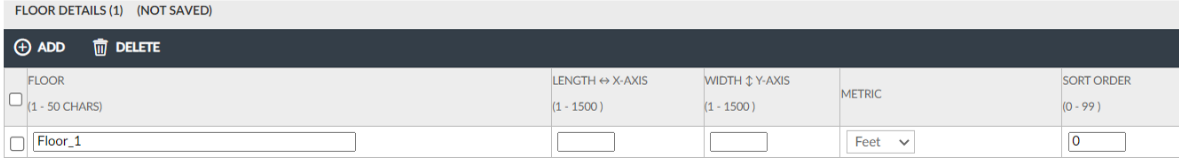


Manage Site Buildings

Building Details (1)

□	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)

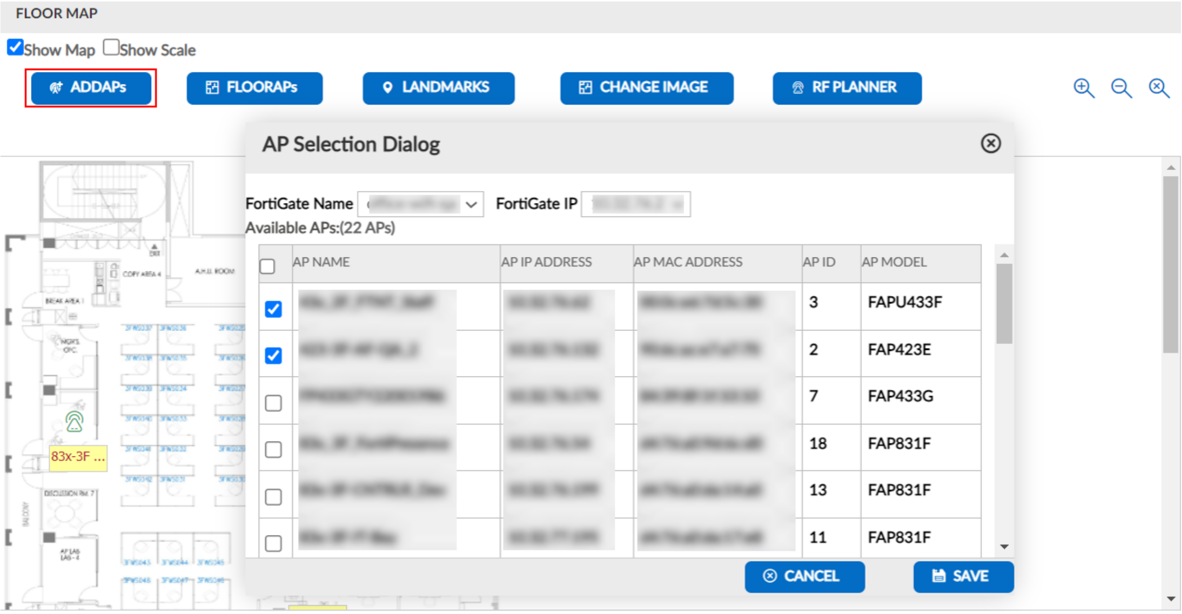
□	FLOOR (1 - 50 CHARS)	LENGTH ↔ X-AXIS (1 - 1500)	WIDTH ↕ Y-AXIS (1 - 1500)	METRIC	SORT ORDER (0 - 99)
□	Floor_1			Feet	0

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.



☑ Show Map ☐ Show Scale

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

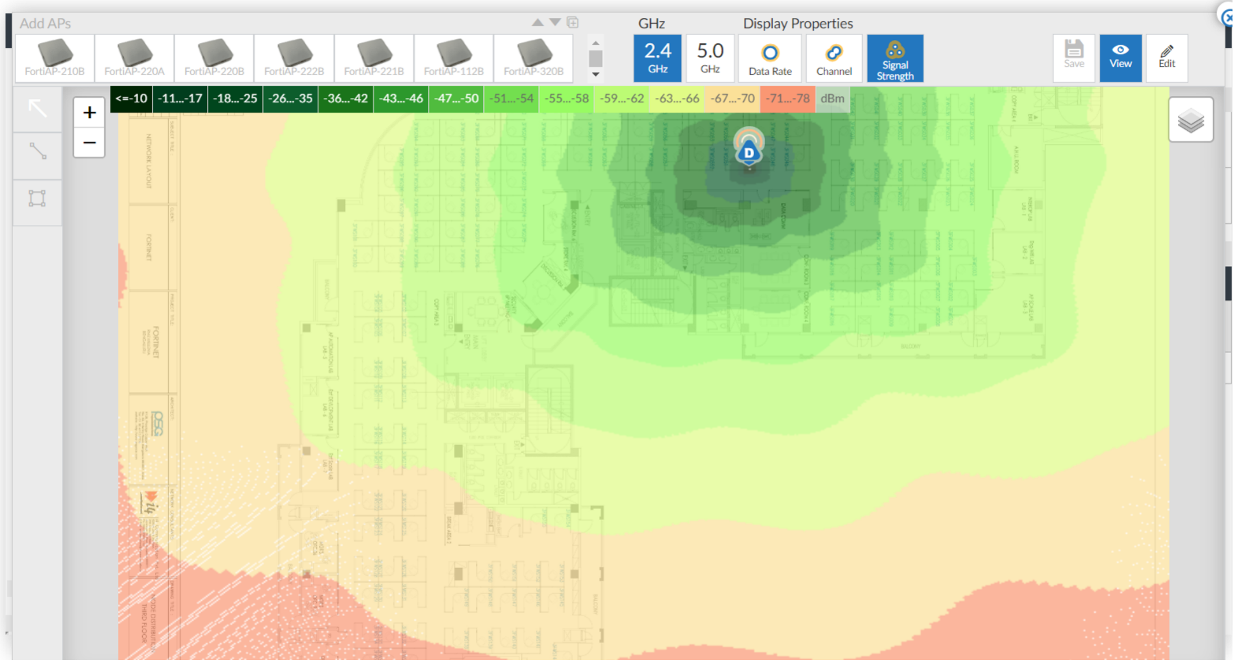
Heat map coloring depends on the distance between APs and selected attribute (throughput, loss, channel utilization, or stations) for all the APs on the floor. If there is only one AP on the floor, the entire floor will show the same coverage. See Heat Maps.

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.

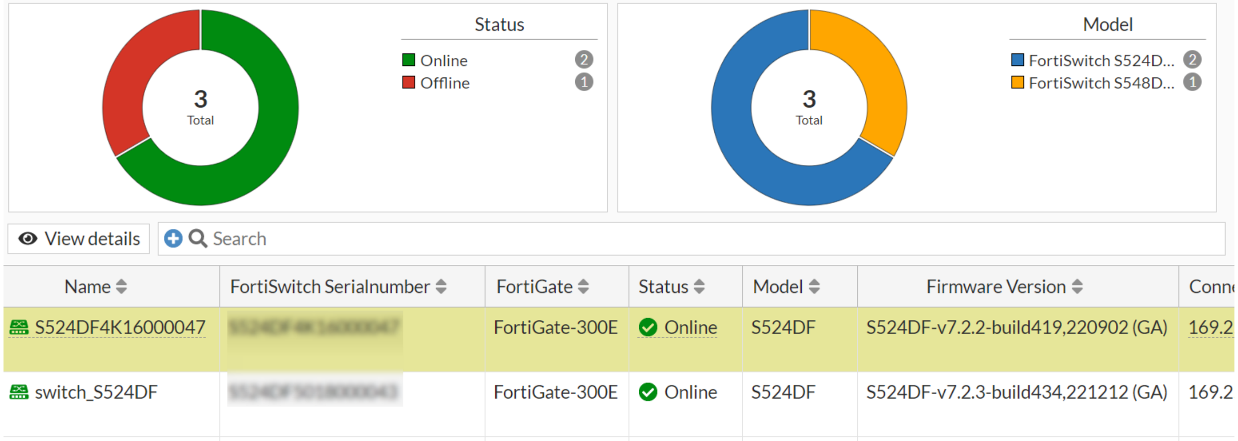
Switch

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

- FortiSwitch
- FortiSwitch Clients

FortiSwitch

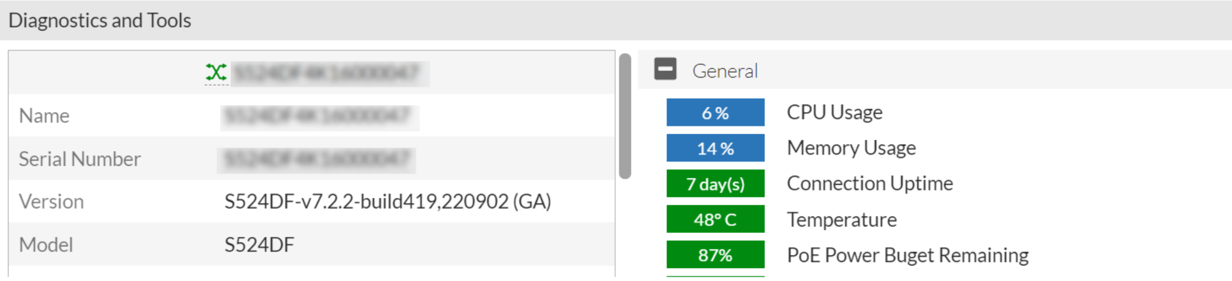
You can monitor the FortiSwitches in your network that are in the purview of FortiAIOps. This page displays a graphical snapshot of the FortiSwitch activity such as, the total number of FortiSwitches, their status (online/offline/unauthorized), and the deployed model details.



Name	FortiSwitch Serialnumber	FortiGate	Status	Model	Firmware Version	Conn
S524DF4K16000047	[redacted]	FortiGate-300E	✓ Online	S524DF	S524DF-v7.2.2-build419,220902 (GA)	169.2
switch_S524DF	[redacted]	FortiGate-300E	✓ Online	S524DF	S524DF-v7.2.3-build434,221212 (GA)	169.2

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

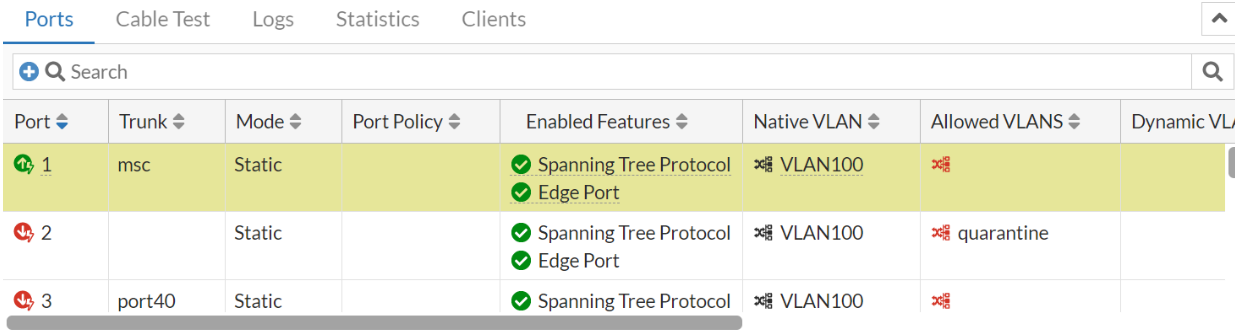
6 %	CPU Usage
14 %	Memory Usage
7 day(s)	Connection Uptime
48° C	Temperature
87%	PoE Power Buget Remaining

- 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	Dynamic VL
1	msc	Static		✓ Spanning Tree Protocol ✓ Edge Port	VLAN100		
2		Static		✓ Spanning Tree Protocol ✓ Edge Port	VLAN100	quarantine	
3	port40	Static		✓ Spanning Tree Protocol	VLAN100		

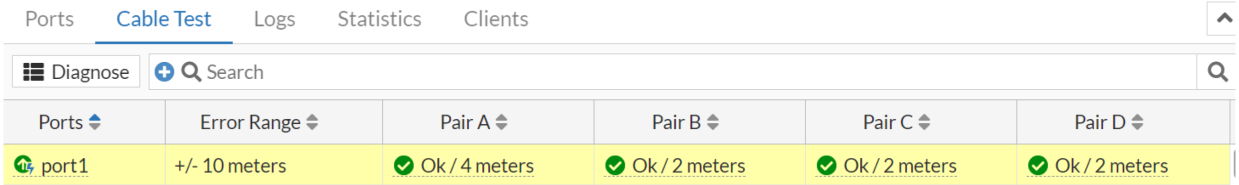
Each entry in the port list displays the following information.

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**.

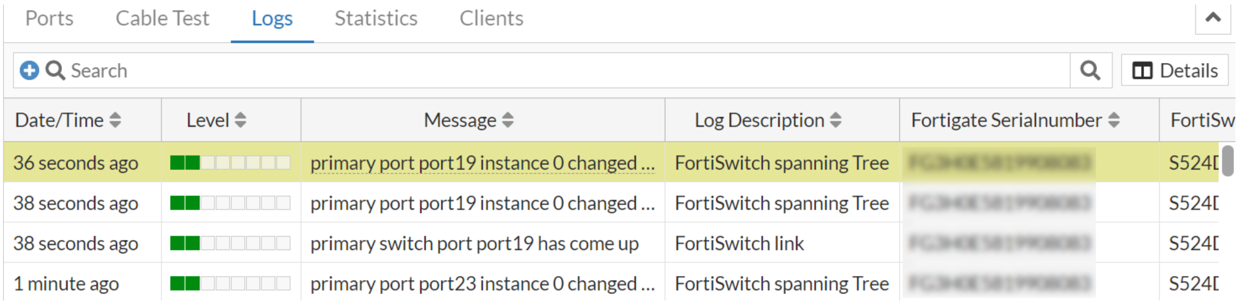


Ports	Error Range	Pair A	Pair B	Pair C	Pair D
port1	+/- 10 meters	✓ Ok / 4 meters	✓ Ok / 2 meters	✓ Ok / 2 meters	✓ Ok / 2 meters

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.

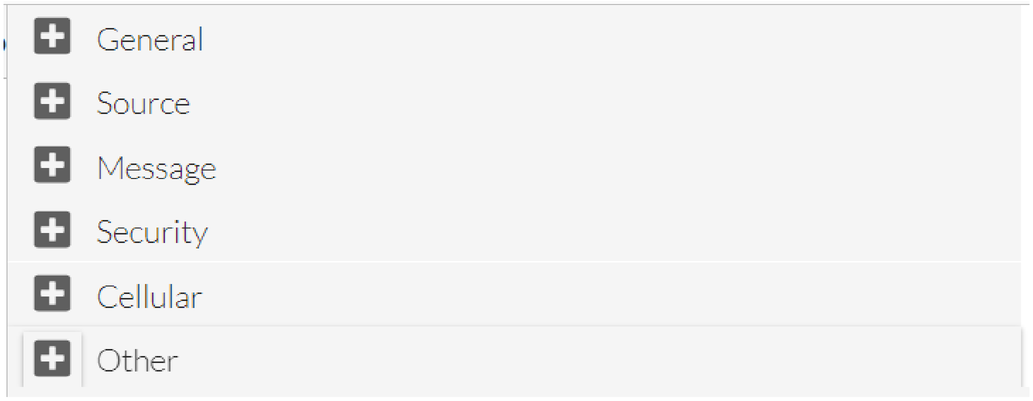


Date/Time	Level	Message	Log Description	Fortigate Serialnumber	FortiSw
36 seconds ago		primary port port19 instance 0 changed ...	FortiSwitch spanning Tree	[redacted]	S524[
38 seconds ago		primary port port19 instance 0 changed ...	FortiSwitch spanning Tree	[redacted]	S524[
38 seconds ago		primary switch 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.

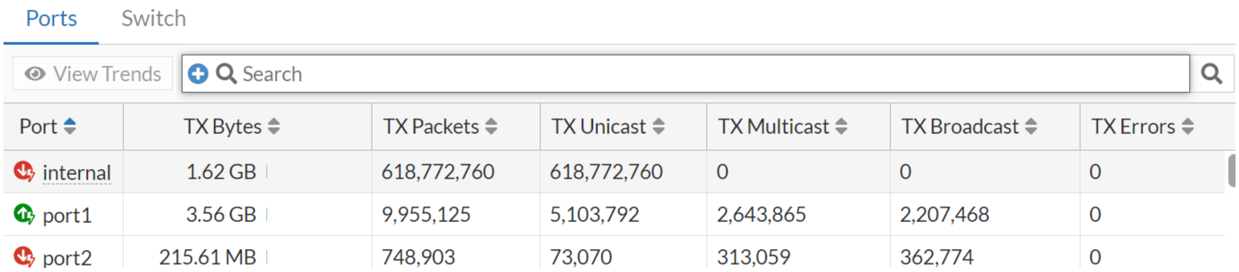
Select a log message and click **Details** to view specific related information. This view provides the following information.



- **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.



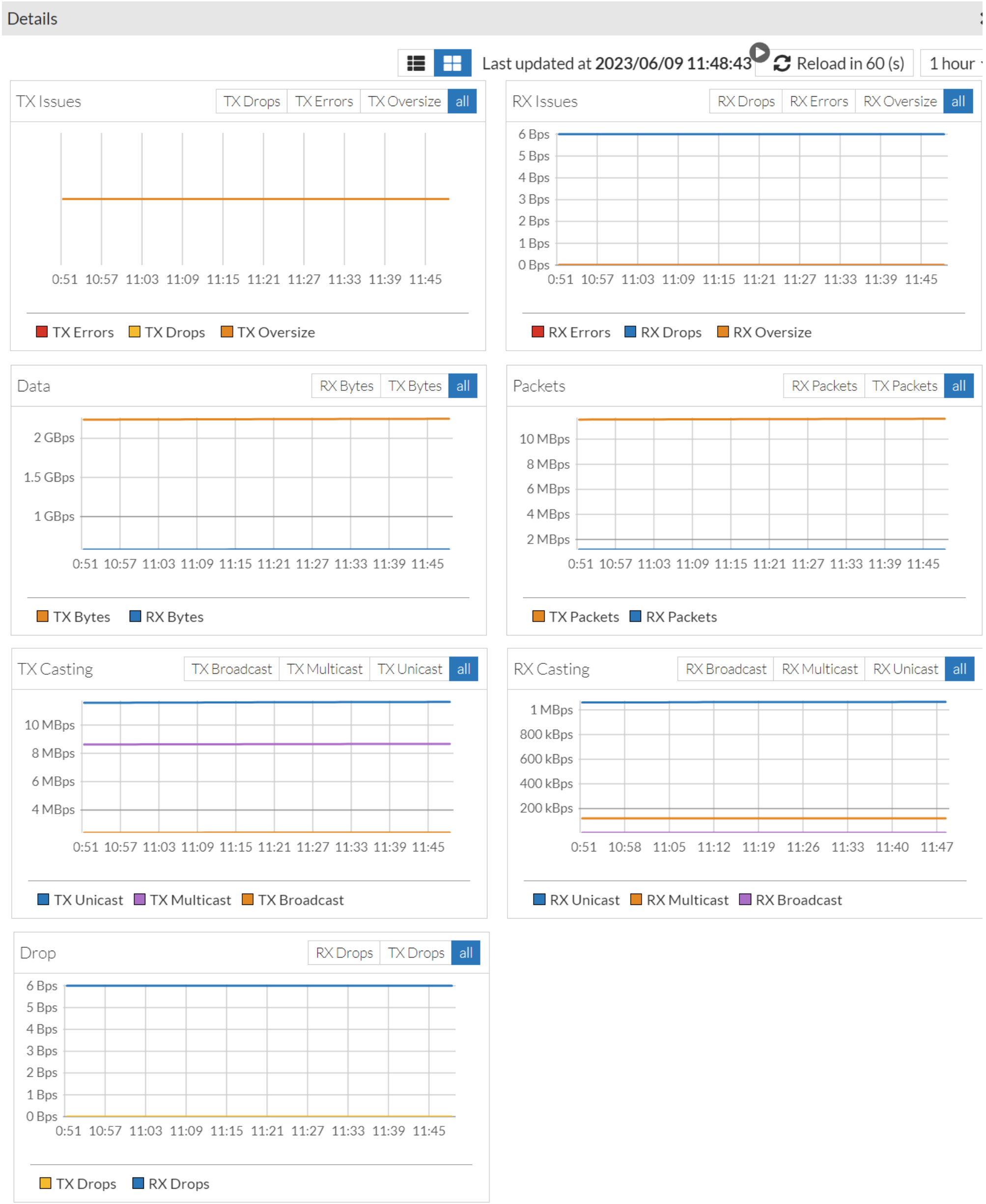
Port	TX Bytes	TX Packets	TX Unicast	TX Multicast	TX Broadcast	TX Errors
internal	1.62 GB	618,772,760	618,772,760	0	0	0
port1	3.56 GB	9,955,125	5,103,792	2,643,865	2,207,468	0
port2	215.61 MB	748,903	73,070	313,059	362,774	0

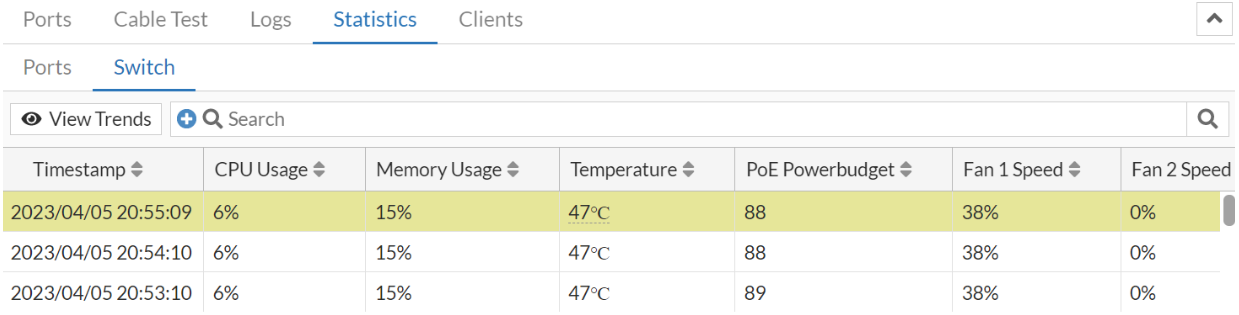
The **Ports** view provides the following information.

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.

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

Select a particular port and click **View Trends** to view a graphical representation of the trends in FortiSwitch statistics over a period of time.



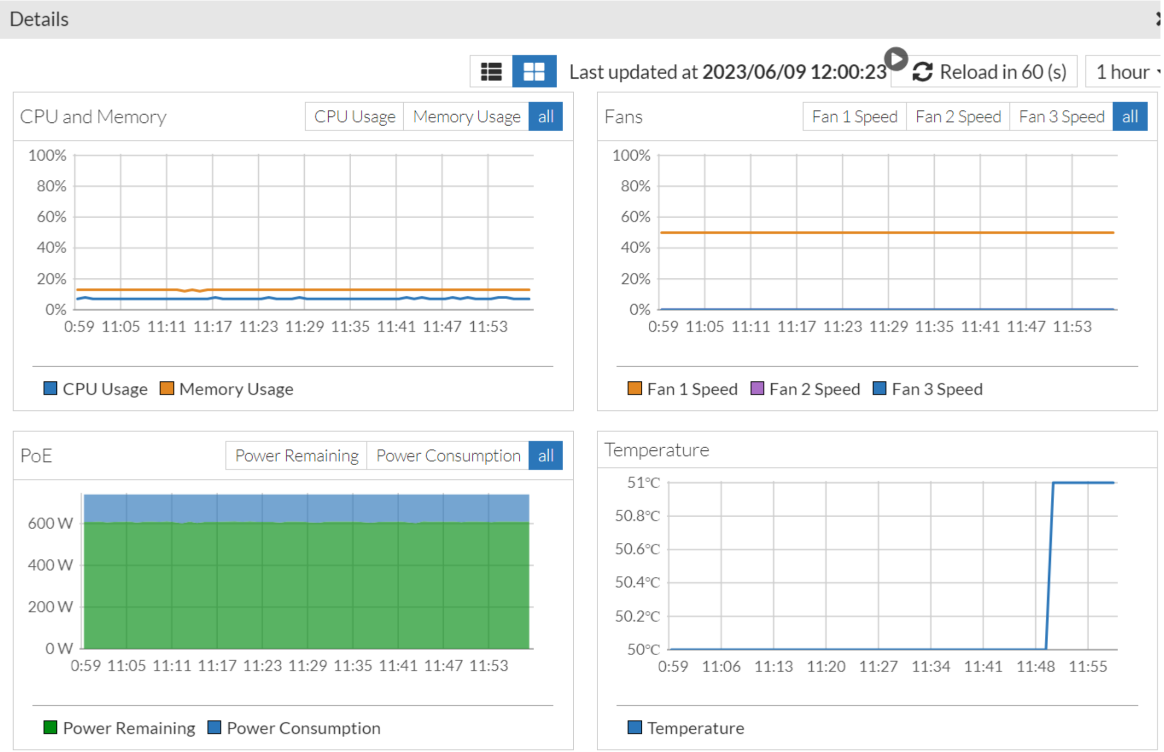


Timestamp	CPU Usage	Memory Usage	Temperature	PoE Powerbudget	Fan 1 Speed	Fan 2 Speed
2023/04/05 20:55:09	6%	15%	47°C	88	38%	0%
2023/04/05 20:54:10	6%	15%	47°C	88	38%	0%
2023/04/05 20:53:10	6%	15%	47°C	89	38%	0%

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

Parameter	Description
CPU Usage	The % of CPU usage.
Memory Usage	The % of memory usage.
Temperature	The PCB temperature in celsius.
PoE Powerbudget	PoE power budget in watts.
PoE Power Consumption	PoE power consumption in watts.
Fan Speed	Speed of the fans on the FortiSwitch unit.

Select a particular switch and click **View Trends** to view a graphical representation of the trends in FortiSwitch statistics over a period of time.



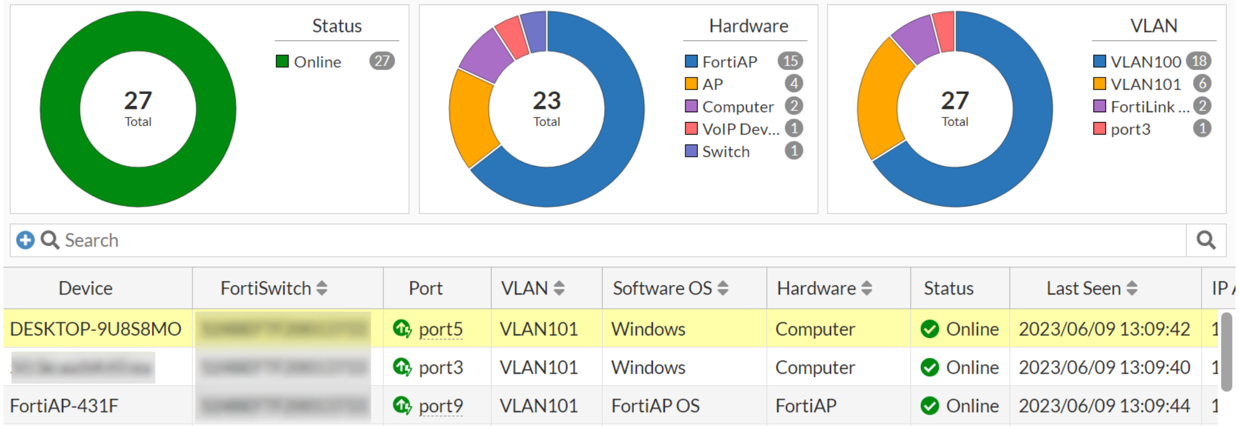
Clients

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.



Device	FortiSwitch	Port	VLAN	Software OS	Hardware	Status	Last Seen	IP
DESKTOP-9U8S8MO	[redacted]	port5	VLAN101	Windows	Computer	✓ Online	2023/06/09 13:09:42	1
[redacted]	[redacted]	port3	VLAN101	Windows	Computer	✓ Online	2023/06/09 13:09:40	1
FortiAP-431F	[redacted]	port9	VLAN101	FortiAP OS	FortiAP	✓ Online	2023/06/09 13:09:44	1

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.

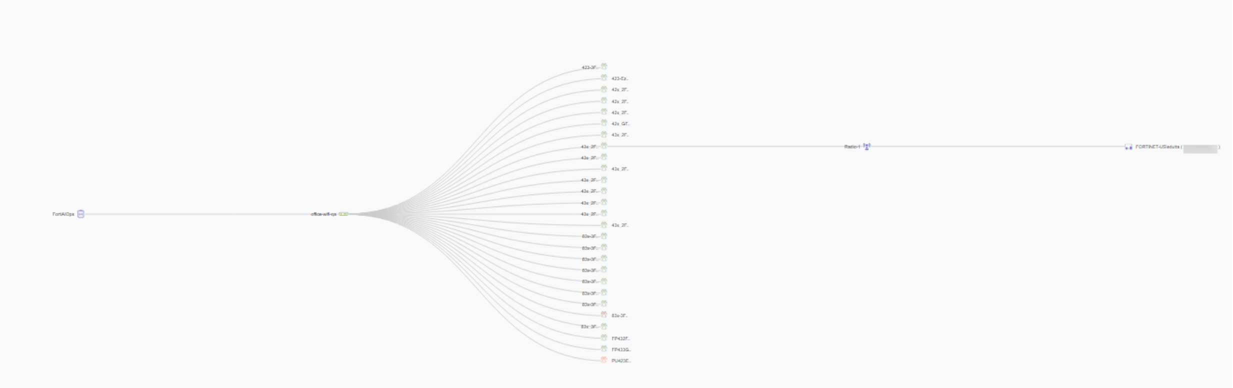
Note: The physical and logical topologies provide wireless client information.

- 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, the filter options available are FortiGate controllers, APs, and device OS. The collapsible/expandable hierarchy of devices in the physical topology is ***FortiGate~ AP ~ 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.

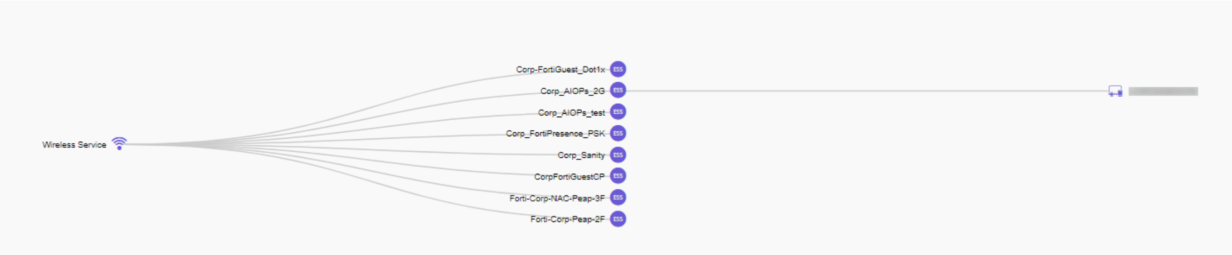
- *Green*: Online and active
- *Orange*: Online and unknown (unmanaged)
- *Red*: Offline

If the FortiGate and AP name is on the right of the specific icon, it implies that the device has no child associated with it in the hierarchy.

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. 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.

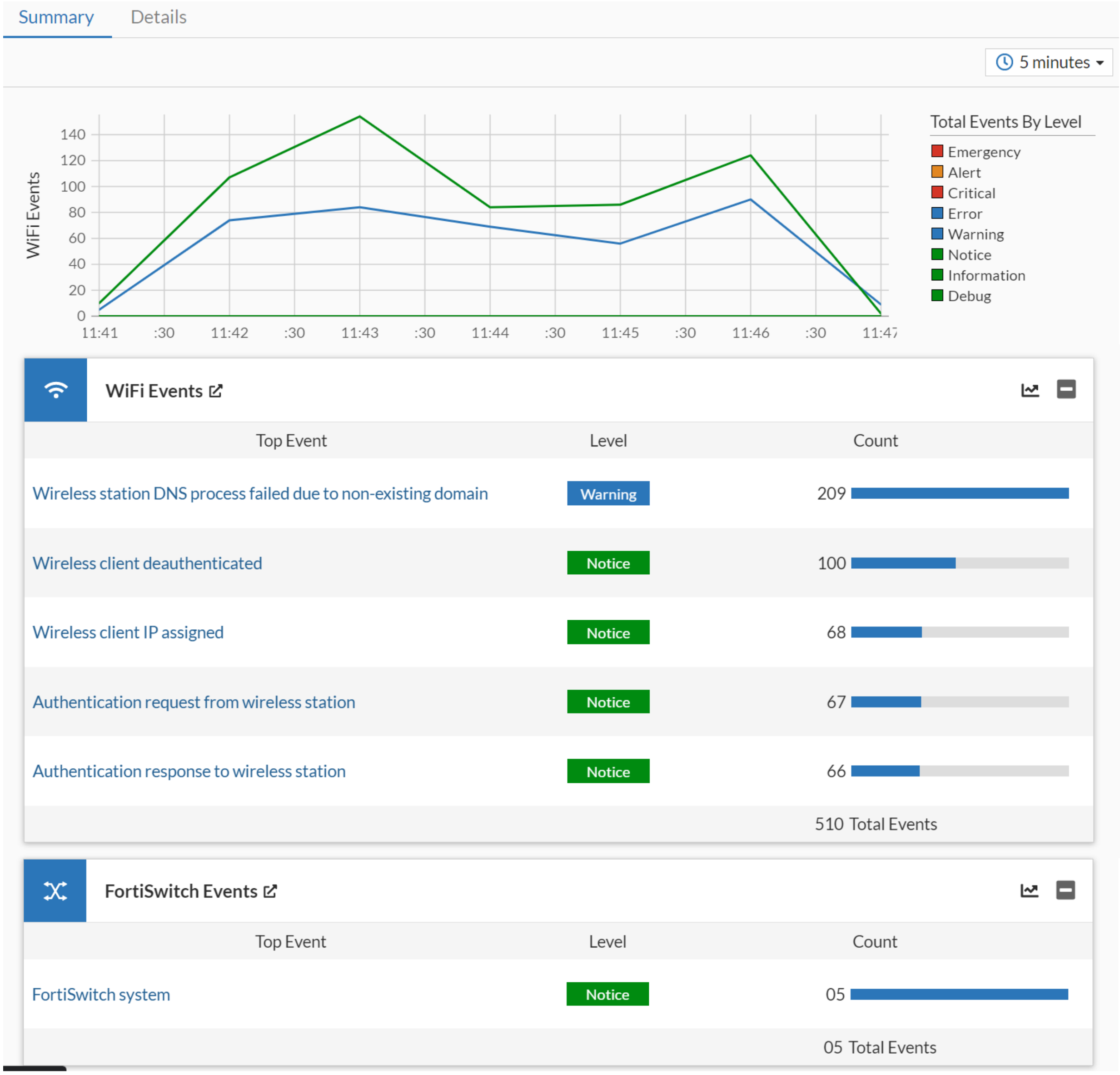
Logs and Reports

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

- Event Logs
- 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.



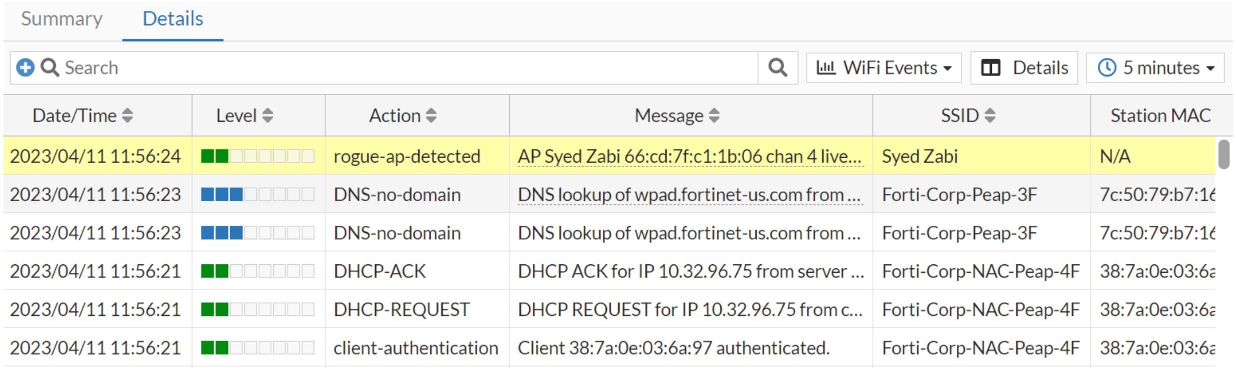
WiFi Events

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.

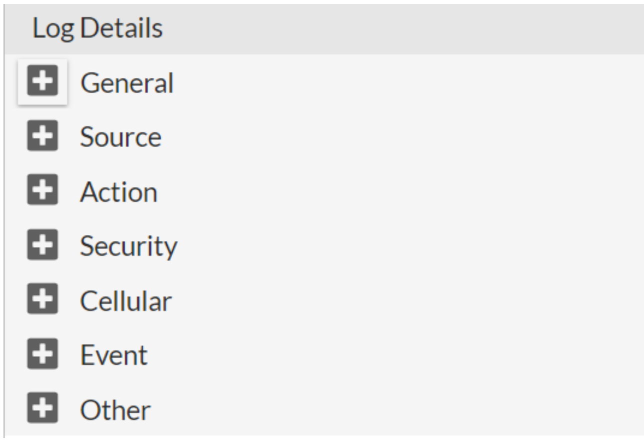


Date/Time	Level	Action	Message	SSID	Station MAC
2023/04/11 11:56:24	🟩🟩□□□□□□	rogue-ap-detected	AP Syed Zabi 66:cd:7f:c1:1b:06 chan 4 live...	Syed Zabi	N/A
2023/04/11 11:56:23	🟦🟦🟦□□□□□	DNS-no-domain	DNS lookup of wpad.fortinet-us.com from ...	Forti-Corp-Peap-3F	7c:50:79:b7:1ϵ
2023/04/11 11:56:23	🟦🟦🟦□□□□□	DNS-no-domain	DNS lookup of wpad.fortinet-us.com from ...	Forti-Corp-Peap-3F	7c:50:79:b7:1ϵ
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.

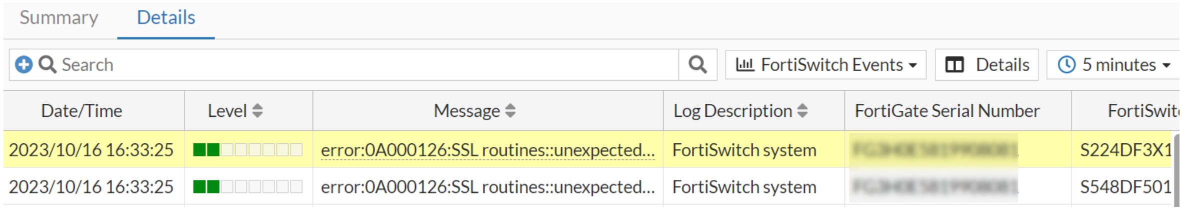
Parameter	Description
Date/Time	The Date/time of log event generation.
Level	The log severity level. • Emergency, Critical (red) • Alert (orange) • Error, Warning (blue) • Notice, Information, Debug (green)
Action	The action leading to the event generation.
Message	The event log message that is generated.
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

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.

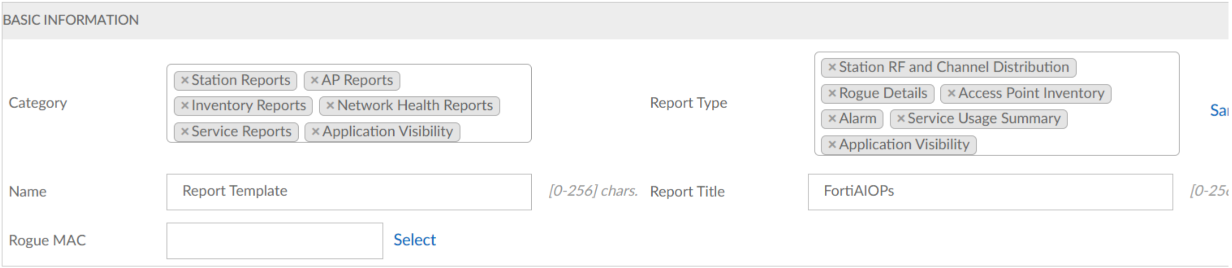
- Creating Reports
- Viewing Reports
- Scheduled Reports
- PCI Reports

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 ×Network Health Reports ×Service Reports ×Application Visibility		Report Type	×Station RF and Channel Distribution ×Rogue Details ×Access Point Inventory ×Alarm ×Service Usage Summary ×Application Visibility
Name	Report Template	[0-256] chars.	Report Title	FortiAIOPs
Rogue MAC		Select		

The following categories of reports are supported.

- Station Reports
- AP Reports

- Inventory Reports
- Network Health Reports
- Service Reports

Station Reports

The following types of station reports are supported.

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

Category	Description
Top Stations	The *Top Stations* report type generates reports for the busiest stations based on the *Throughput* and Airtime Utilization. This report type generates the top N stations based on the number of bytes transferred and received and total Rx/Tx. The information includes each station's Station Mac, Controller, AP Id, SSID, Throughput (Kbps) and Date/Time (GMT).
Unique Stations	Provides the unique station details based on all stations connected to a network within the reporting interval. A graphical summary of the stations distributed by RF type, stations distributed across 2.4GHz, 5GHz, and 6GHz bands, stations distributed by OUI, stations distributed by device type, and stations distributed by OS type is displayed. The *Unique Station* reports are available to all groups and list stations connected to network during last 24 hours. The following details are displayed. • Summary - This section provides the total number of Unique Stations. • Graphs - The graphs are of the following types. ◦ *Finger Print OS Distribution* - This graph displays the station distribution based on the OS Type. ◦ *Finger Print Device Distribution* - This graph displays the station distribution based on the Device Type. ◦ *OUI Distribution* - This graph displays the station distribution based on the OUI. ◦ *Station Distribution* - This graph displays the station distribution based on the RF Type. • Unique Station Details - This section provides the station's OUI, Date/Time (CST), Station MAC, User, IPv4 Address, IPv6 Address, RF Type, SSID, Device Type, OS Type and Floor.
EAP-AKA Error	The EAP-AKA Error type generates a report with details of EAP-AKA errors associated with specific ESSIDs and on specific stations connected to network within the reporting interval. The following details are displayed. • User selected Top 5 EAP-AKA Errors - The top 5 most common EAP-AKA errors with the number of stations the errors were reported on and the number of EAP authentication failures for each station. • User selected Top 5 Station by Errors - The top 5 stations (MAC addresses) with highest EAP-AKA errors reported and the number of EAP authentication failures for each station. • EAP-AKA Errors - The list of EAP-AKA errors within the reporting interval. The details displayed are, date and time of the error, associated controller, access point, station MAC address, and the ESSID, and the error description/reason.

AP Reports

The following types of AP reports are supported.

Category	Description
Rogue Details	The *Rogue Details* report type generates the report on the individual rogue. It displays the rogue mobility trend. The trend is plotted against time and APs detecting the rogue. The data displayed is a Max of hourly data sample. The following details are displayed. • Summary - This section provides the details of the selected rogue • Rogue Mobility Trend graph - Trend is plotted against AP which detects rogues with high strength and its time as samples. • Rogue Details - This section provides details about the APs detecting the rogue along with Date/Time, Controller, AP Detecting Rogue, AP Location, SSID, Channel and RSSI.
Rogue Summary	Summarizes the rogue device information on the trend of the number of rogues reported on a per controller basis, per hour. The rogue APs and rogue station count is displayed. A graphical summary of the trend on rogue AP, trend on rogue station, and trend on controllers is displayed. The following details are displayed. • Summary - This section provides the details of the total number of rogues. • Graph - The graphs are of the following types. • *Rogue Trend By Type* - The two types of *Rogue Trend By Type* graphs are displayed as follows. • *Trend on Rogue Station* - This graph displays the trend type based on the number of rogue Stations. • *Trend On Rogue AP* - This graph displays the trend type based on the number of rogue APs. • *Rogue Trend By Controllers* - This graph displays the top 10 controllers with the highest number of rogues. • New Rogues Detected During Reporting Interval - This section provides the details of the new rogues detected during reporting 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

Category	Description
	of the distribution of Access Points. - AP Inventory Summary - This section provides the details of Access Point Inventory. The details are Name, Mac address, Model, Software Version, IP Address, Controller, Availability State, Connectivity Preference and Floor.
Controller Inventory	Lists and tracks all the controllers, with its model and software versions on the network. - Summary - This section provides the total number of Controllers. - Graph - The graphs are of the following types. - *Controller Software Version Distribution* - This graph displays the Controllers based on the controller software version distribution. - *Controller Model Distribution* - This graph displays the Controllers based on the controller model distribution. - Controller Inventory Summary - This section provides the details of Controller Inventory. The details are Hostname, IP Address, Mac address, Node Name, Software Version, Model, Description, Availability State, Management State and Location.
Device Availability	Lists all the controllers and access points with its availability, uptime and down time of each of them. This report generates the report for each Controller and AP. It displays the Device Name, UP Duration, Down Duration time and Availability(%) for the AP and Controller.

Network Health Reports

The following types of network health reports are generated.

Category	Description
Alarm Report	Lists the total number of critical, major and minor alarms raised on the network. A graphical summary of the alarms distribution by category and top 10 controllers and access points with high alarms is displayed. - Summary - This section provides the total number of Alarms raised. This includes the Critical Alarms, Major Alarms and Minor Alarms. - Graph - The graphs are of the following types. - *Top 10 Access Points with High Alarms* - This graph displays the Alarm distribution based on the Access Points with High Alarms. - *Top 10 Controller with High Alarms* - This graph displays the Alarm distribution based on the Controller with High Alarms. - *Alarm Distribution By Category* - This graph displays the Alarm distribution based on Category. - Alarm Report tables - The following types of Alarm Reports are generated. - *Devices With High Alarms* - This table provides a statistical output of the devices with high alarms raised. It displays the alarms

Category	Description
	Device and Number of Occurrence. • *List of Standing Alarms* - This table provides a statistical output of the top 10 standing alarms raised. It displays the alarms Date/Time (GMT), Source, Device Name, Category, Alarm Type, Severity and Message. • *Longest Duration Alarms* - This table provides a statistical output of the top 10 longest duration alarms raised. It displays the alarms Source, Device ID, Category, Alarm Type, Severity, Raise Date/Time (GMT), Clear Date/Time (GMT), Duration and Message. • *Most Frequent Alarms* - This table provides a statistical output of the top 10 most frequent alarms raised. It displays the alarms Category, Alarm Type, Severity and Number of Occurrence.

Service Reports

The following types of service reports are supported.

Category	Description
Service Usage Summary	Provides the service usage summary based on the ESSIDs. A graphical summary of the top SSIDs based on throughput and number of stations is displayed. • Graph - The graphs are of the following types. • *Top SSIDs Based on Throughput* - This graph displays the top SSIDs based on the throughput. • *Top SSIDs Based on Number Stations* - This graph displays the top SSIDs based on number of stations. • Network Usage Summary - The Network Usage Summary displays the ESSID, Average Station Count, Max Station Count, Time When Max Station Occurred, Total Unique Stations and Maximum Throughput are displayed.
Service Usage Trend	Provides the service usage trends based on the ESSIDs. A graphical summary of the top SSIDs based on throughput and number of stations is displayed. • Server Usage Trend graphs - These are displayed with a trend of Max, Minimum and Average stations connected and stations throughput on hourly basis during reporting interval. This is a graphical report represented with a line chart having two lines, one for Max and second one for Average station count. • Service Usage Trend Details - The service usage trend report type displays Date/Time (GMT), Max Stations Connected, Min Stations Connected, Avg Stations Connected and Throughput (Kbps).

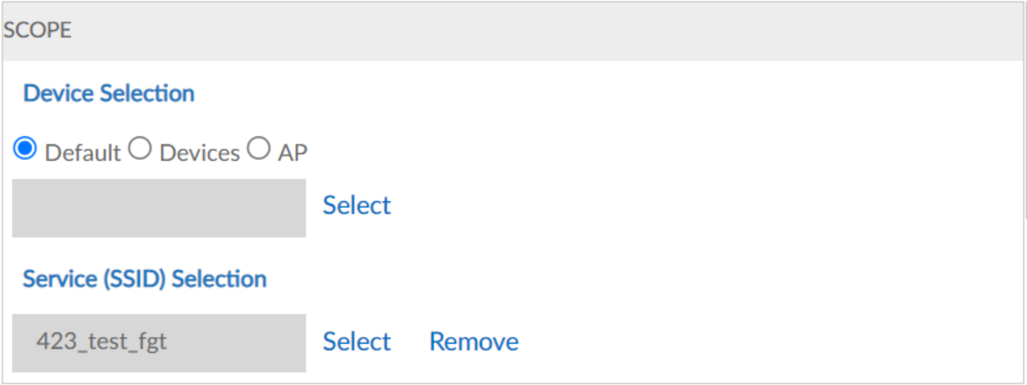
Application Visibility Reports

The application visibility reports provide the following information.

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

Scope

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



SCOPE

Device Selection

● Default ○ Devices ○ AP

Select

Service (SSID) Selection

423_test_fgt

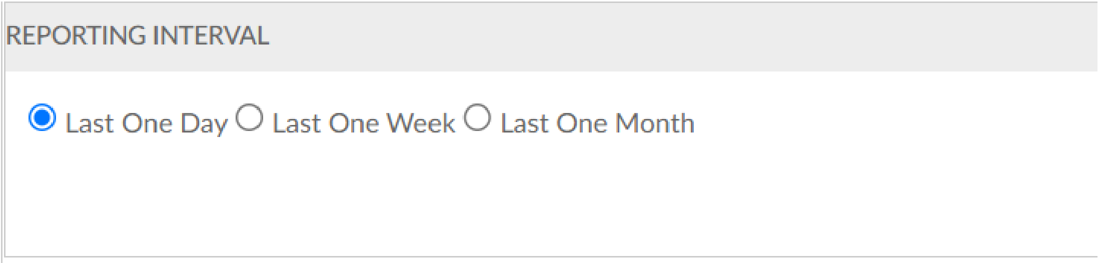
Select Remove

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.



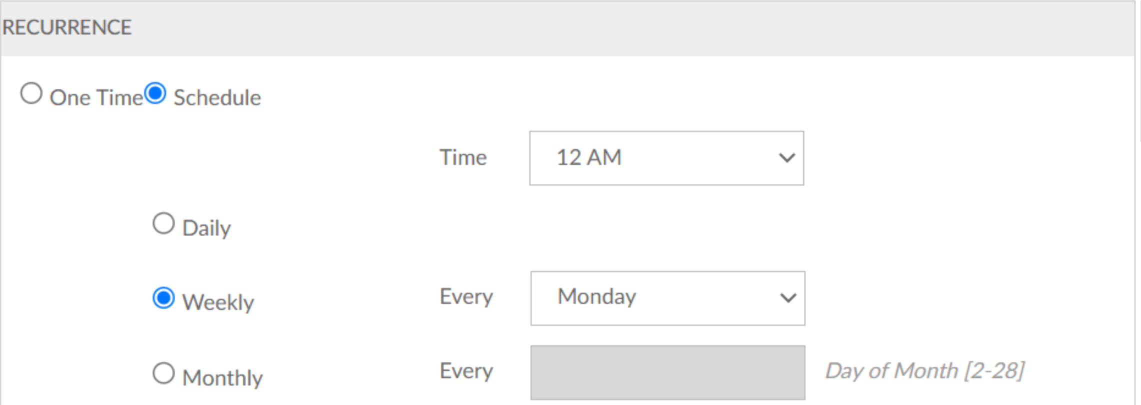
REPORTING INTERVAL

● 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

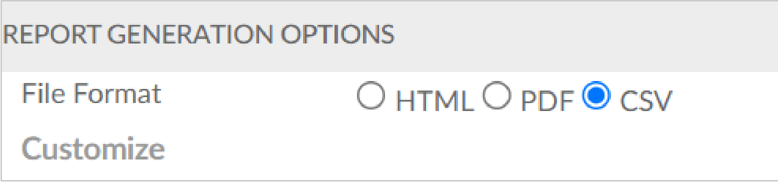
● Weekly — Every: Monday

○ 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.



REPORT GENERATION OPTIONS

File Format: ○ HTML ○ PDF ● CSV

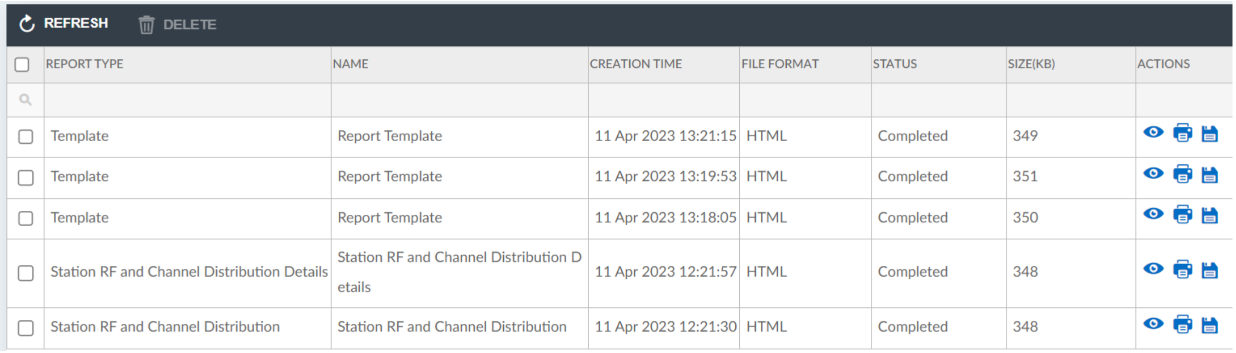
Customize

- **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

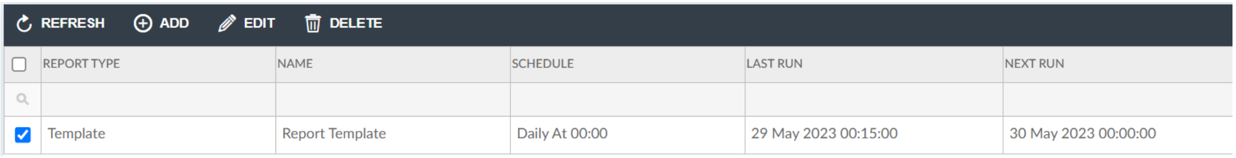
This screen displays a list of all the reports that are generated. These reports can be generated in HTML, CSV, or PDF format. They can be viewed, printed or saved locally.



☐	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

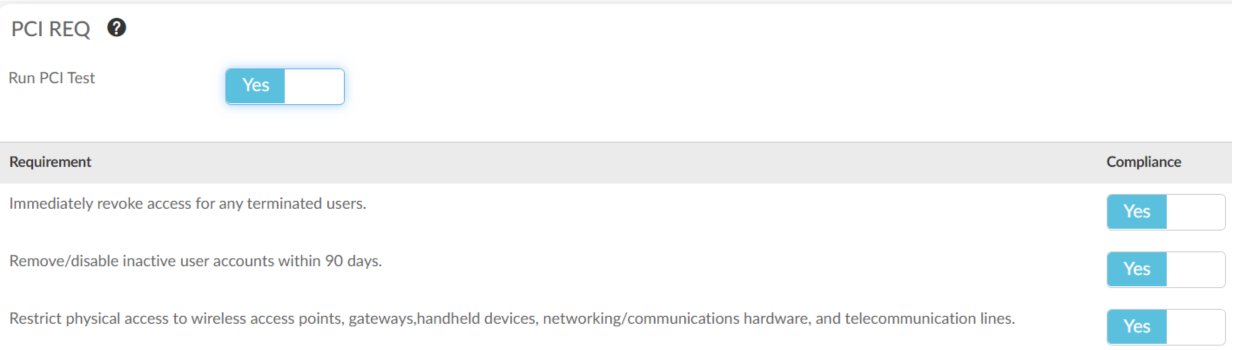
This page displays a list of current running reports and reports scheduled to run in the future. In case of recurring reports, the next run time is displayed. To create a new report, click **Add**.



☐	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**.

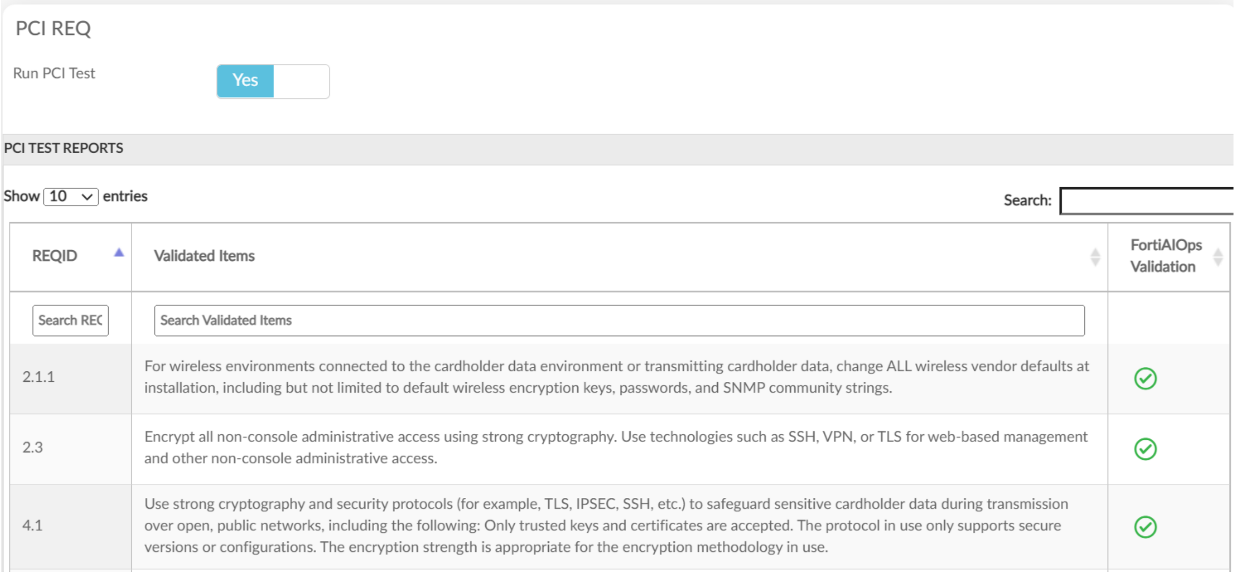


PCI REQ ❓

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

System

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

- User Management
- Backup and Restore
- Settings
- Licensing
- Location Services
- Certificates

User Management

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

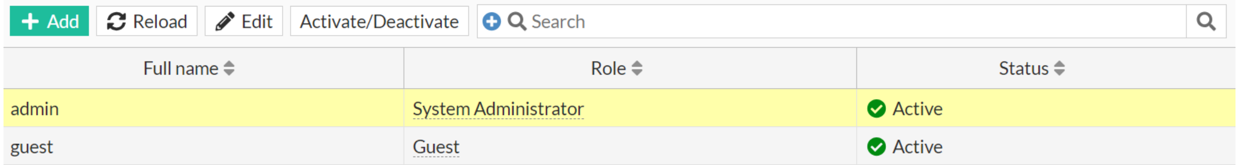
- Users
- User Groups

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

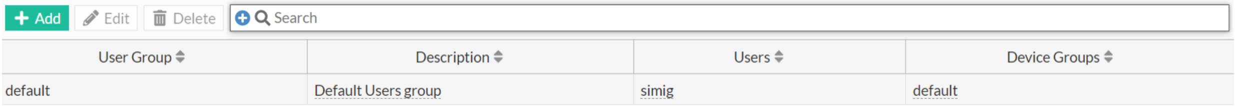
Select a user and click **Edit** to modify user information. This includes changing the user's full name, role or password.

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.



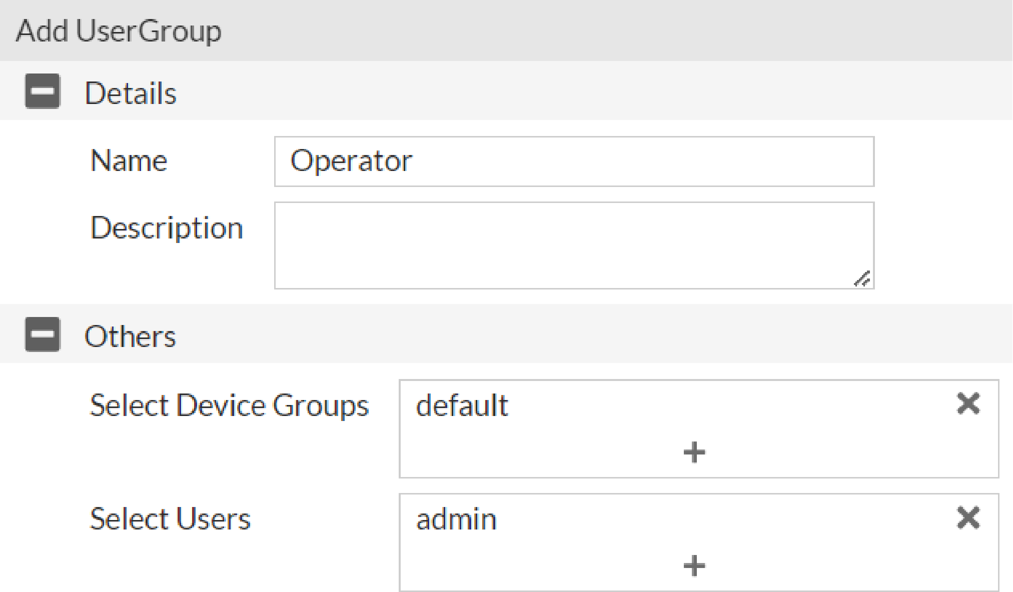
User Group	Description	Users	Device Groups
default	Default Users group	simig	default

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

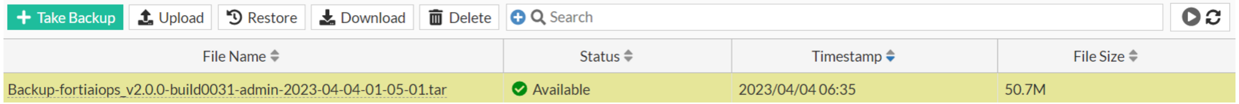
To edit an user group, select an existing user group from the list and click **Edit**.

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 and data. 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

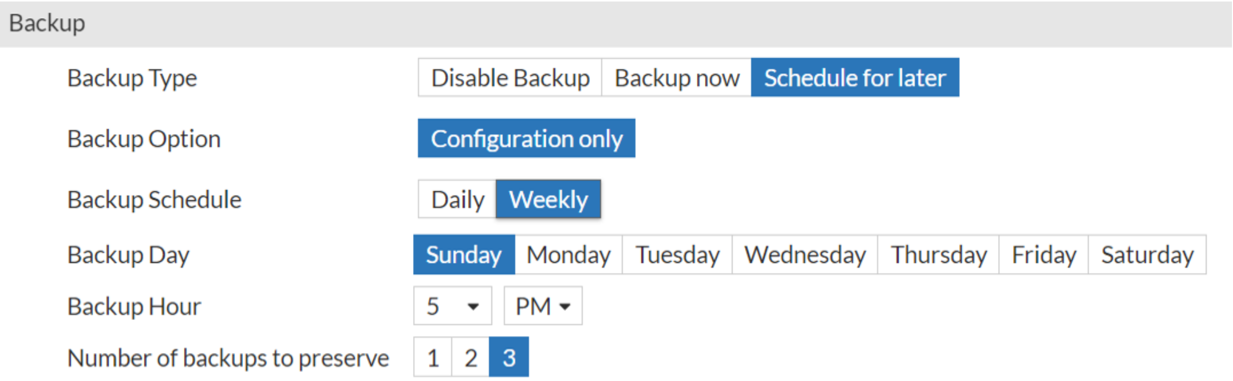
Take Backup

The Take Backup function allows you to take a backup of the FortiAIOps configuration and data. 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, either **Configuration only**. Backing up only the configuration includes information like maps, controller details, and AP details except statistics data.
4. Select the Backup Type, either **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:

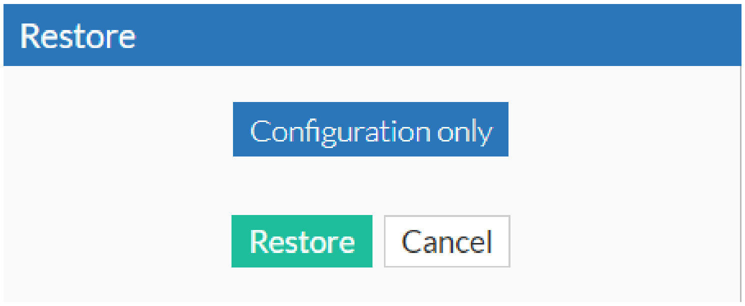
1. Navigate to System>Backup and Restore
2. Click **Upload.**
3. Browse and select the backup file (.tar) file.
4. Click **Upload.**

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.**

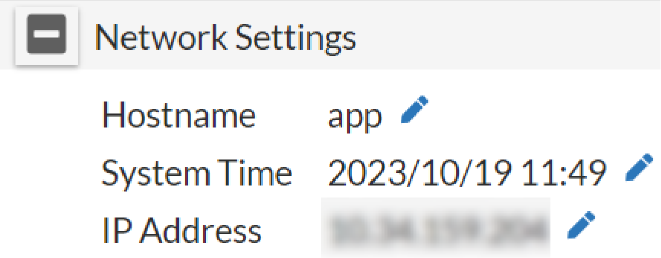
Settings

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

- Network Settings
- Statistics
- OUI

Network Settings

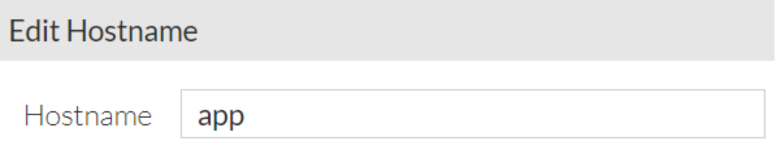
This section allows you to configure various system settings. Click ✎ icon to edit the system settings.



Network Settings

Hostname app ✎
System Time 2023/10/19 11:49 ✎
IP Address [redacted] ✎

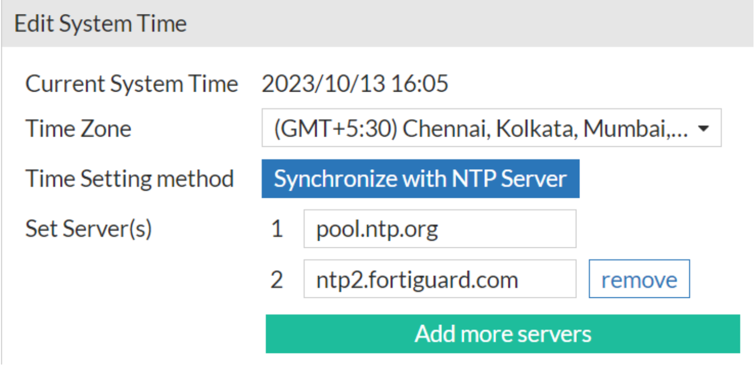
The **Hostname** displays the hostname of the system currently in use.



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.



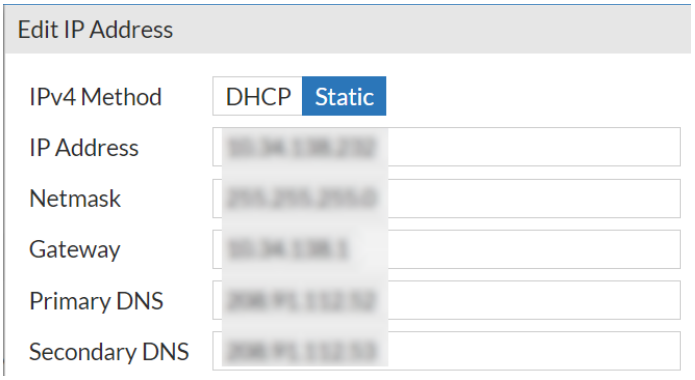
Edit System Time

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.

Configure the **IP address** settings to set dynamic or static IP address.

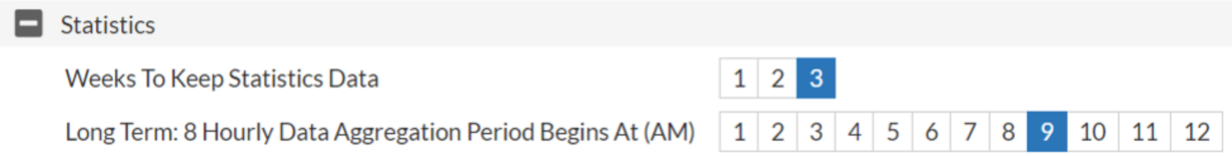


Edit IP Address

IPv4 Method	DHCP [✓ Static]
IP Address	[redacted]
Netmask	[redacted]
Gateway	[redacted]
Primary DNS	[redacted]
Secondary DNS	[redacted]

Statistics

- **Weeks to keep statistics data** - The Weeks to keep statistics data option allows you to set the number of weeks to preserve the statistics data. The statistics data older than the number of weeks specified in this field from the current date will be automatically deleted from the server.
- **Long Term: 8 Hourly Data Aggregation Period Begins At (AM)** - The Long term: 8 hourly data aggregation period begins at (AM) option allows you to enter the start period for the data aggregation. Enter the time for the data aggregation to begin.

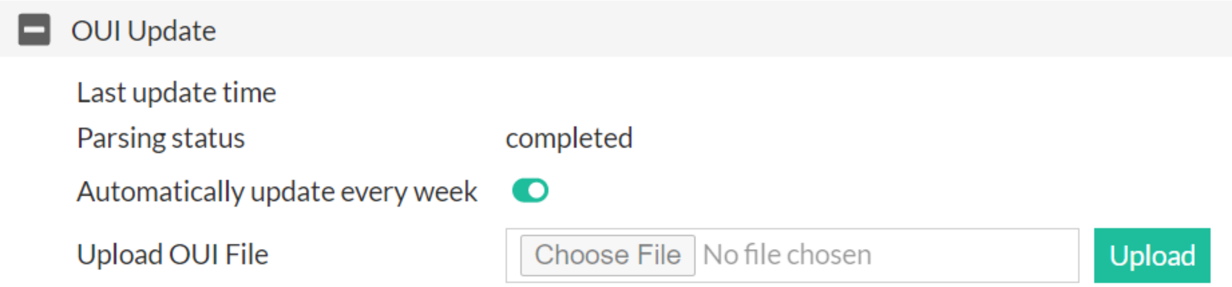


Statistics

Weeks To Keep Statistics Data	1 2 [✓ 3]
Long Term: 8 Hourly Data Aggregation Period Begins At (AM)	1 2 3 4 5 6 7 8 [✓ 9] 10 11 12

OUI

- **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	● (enabled)
Upload OUI File	Choose File No file chosen Upload

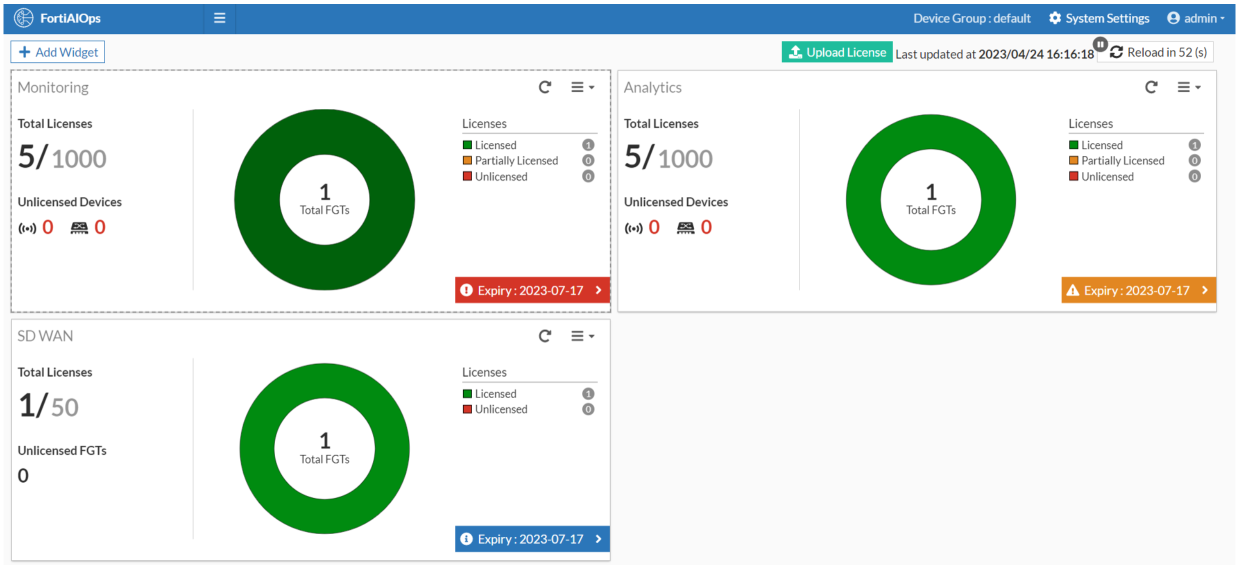
Licensing

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.



Last updated at 2023/04/24 16:16:18 Reload in 52 (s)

Monitoring

Total Licenses 5/1000

Unlicensed Devices 0 0

1 Total FGTs

Licenses	
🟩 Licensed	1
🟧 Partially Licensed	0
🟥 Unlicensed	0

Expiry : 2023-07-17

Analytics

Total Licenses 5/1000

Unlicensed Devices 0 0

1 Total FGTs

Licenses	
🟩 Licensed	1
🟧 Partially Licensed	0
🟥 Unlicensed	0

Expiry : 2023-07-17

SD WAN

Total Licenses 1/50

Unlicensed FGTs 0

1 Total FGTs

Licenses	
🟩 Licensed	1
🟥 Unlicensed	0

Expiry : 2023-07-17

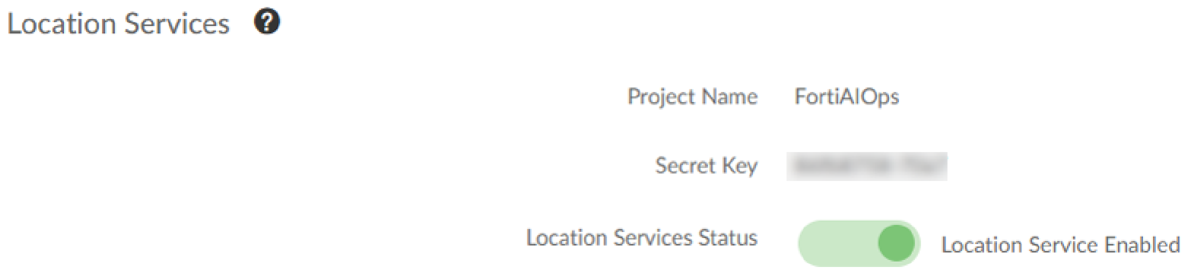
Location Services

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.

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

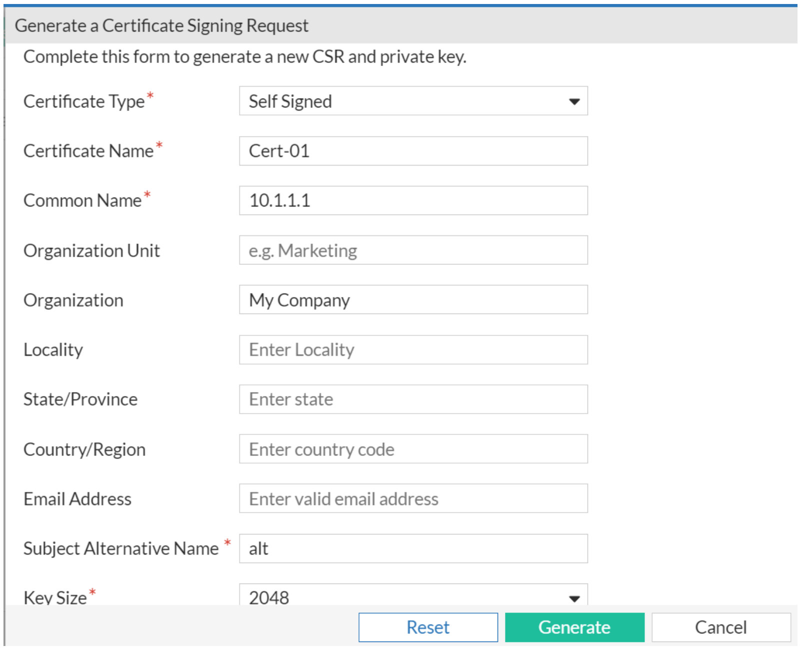
Local Certificates

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 FortiAPs
  - Bridge mode SSIDs
  - WPA2 PSK security mode
  - Radios in AP mode.
- 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.

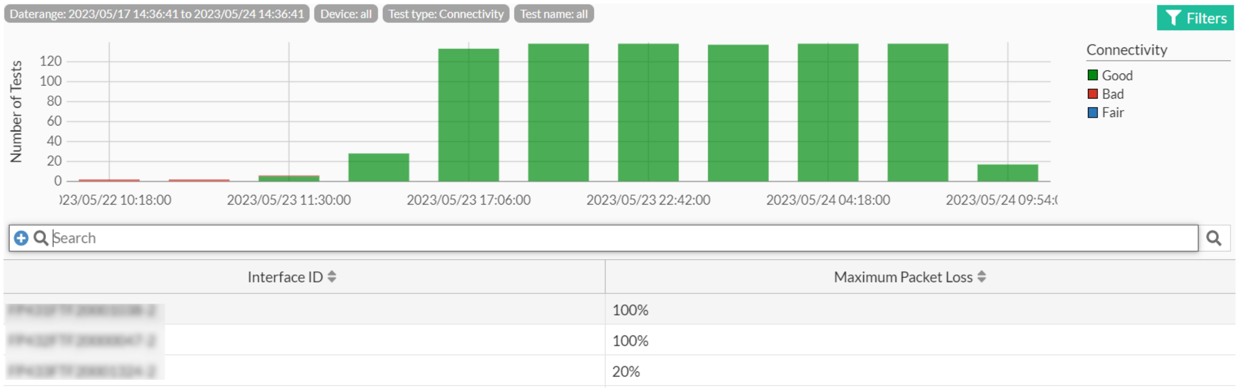
- Trends
- Results
- Baseline
- Schedule

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.

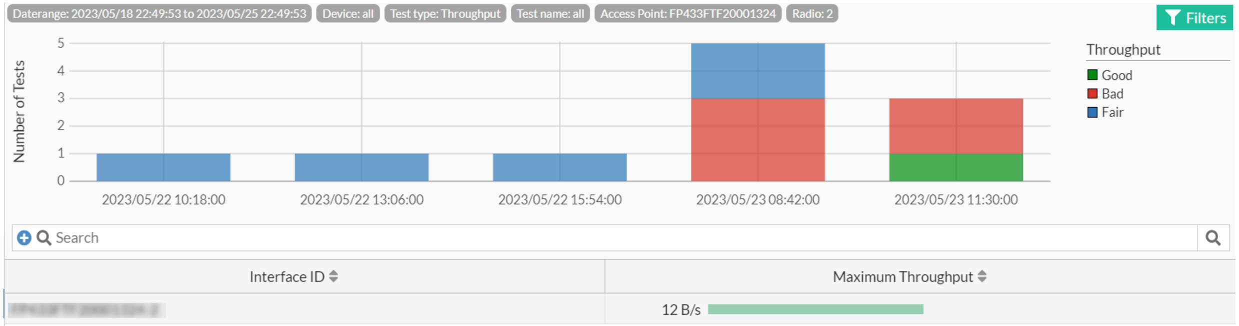
If the **connectivity** test type is selected, the Trends page presents a table with the *Interface ID* and the *Maximum Packet Loss* for each interface.



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

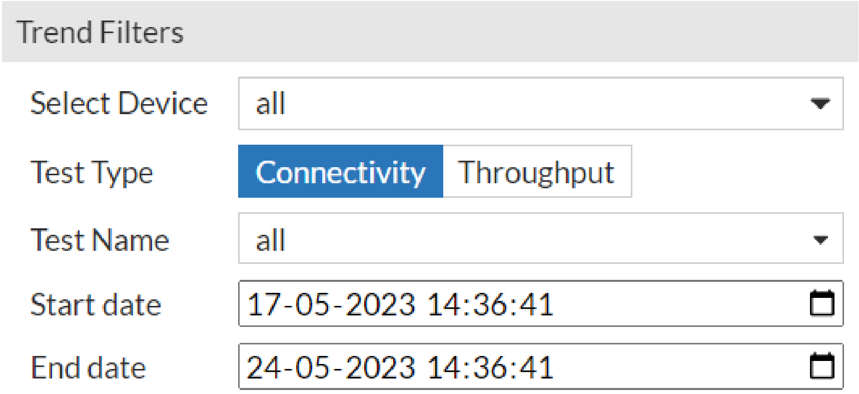
Interface ID	Maximum Throughput
[redacted]	12 B/s

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.



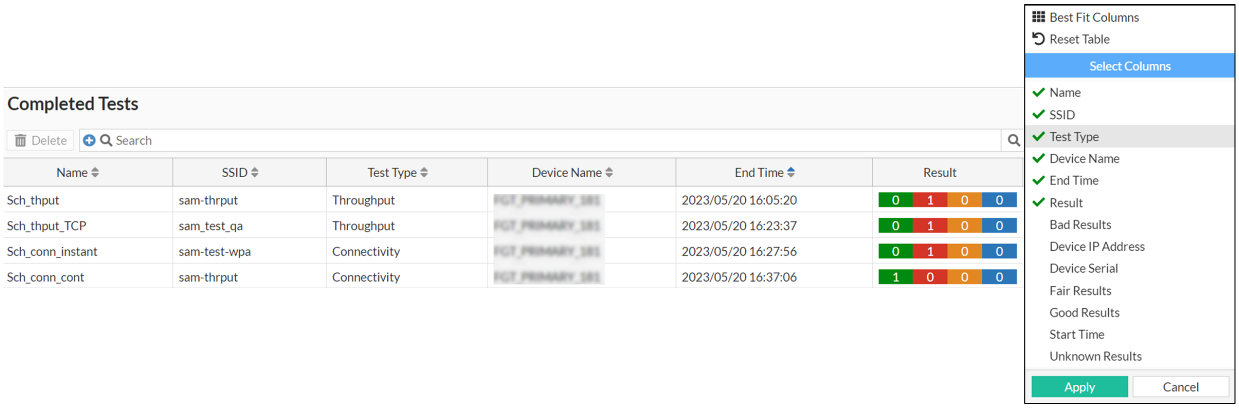
Trend Filters

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

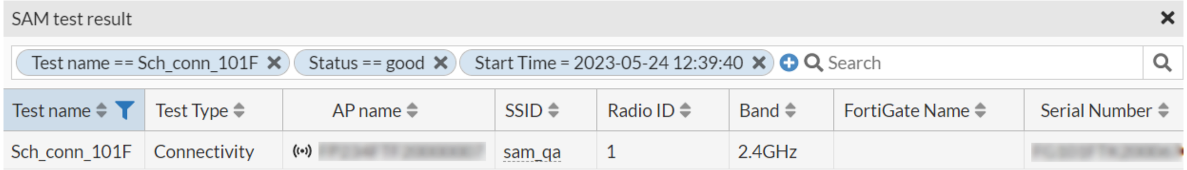


Completed Tests

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

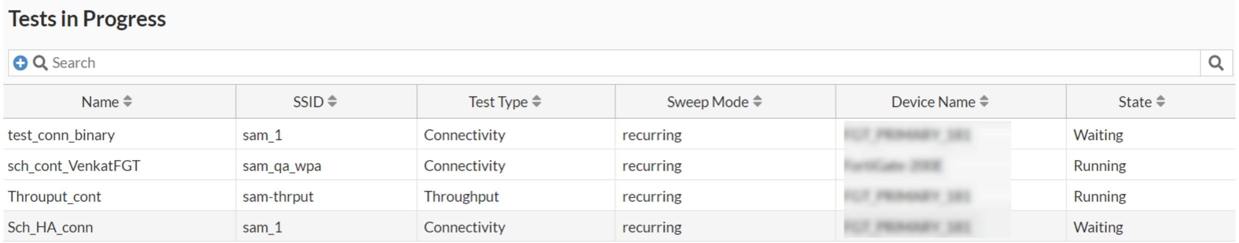
Test name == Sch_conn_101F ✕
Status == good ✕
Start Time = 2023-05-24 12:39:40 ✕
Search

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

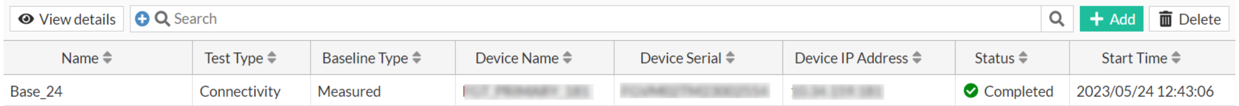
Name	SSID	Test Type	Sweep Mode	Device Name	State
test_conn_binary	sam_1	Connectivity	recurring	[redacted]	Waiting
sch_cont_VenkatFGT	sam_qa_wpa	Connectivity	recurring	[redacted]	Running
Throuput_cont	sam-thrput	Throughput	recurring	[redacted]	Running
Sch_HA_conn	sam_1	Connectivity	recurring	[redacted]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

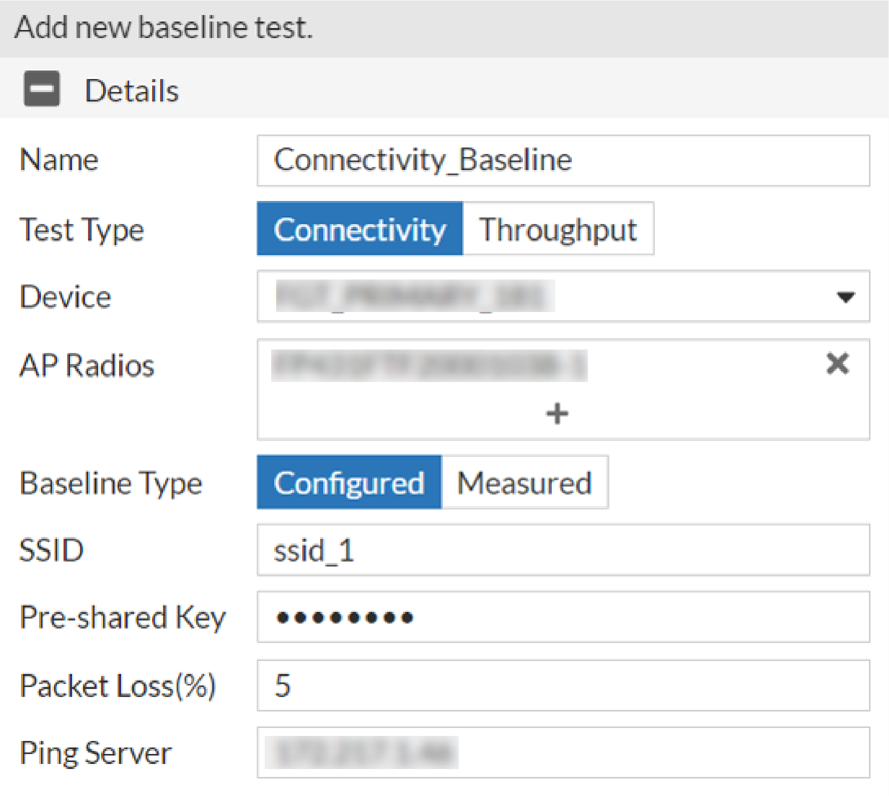
You have two options to execute the baseline tests.

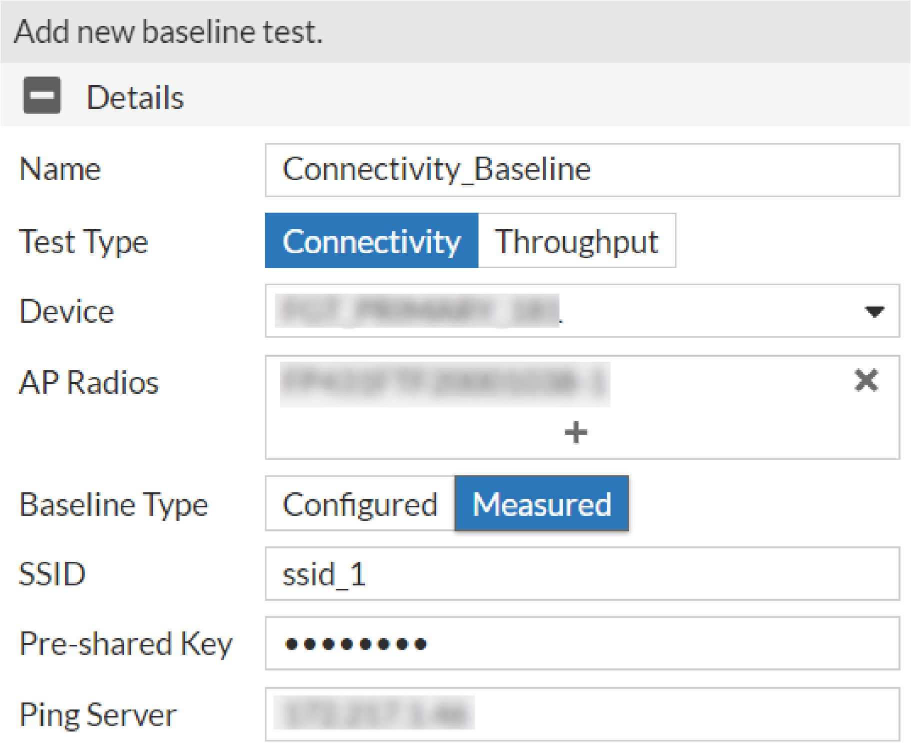
- **Configured Test**: This option allows you to create a baseline test by providing theoretical values.
- **Measured Test**: This option allows you to create a baseline test by providing the actual baseline values. It is important to run a measured baseline when the wireless network is operating either 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. 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] Throughput Device: [redacted] AP Radios: [redacted] Baseline Type: [✓ Configured] Measured SSID: ssid_1 Pre-shared Key: •••••••• Packet Loss(%): 5 Ping Server: [redacted] 2.
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] Throughput
Device	[redacted]
AP Radios	[redacted]
Baseline Type	Configured [✓ Measured]
SSID	ssid_1
Pre-shared Key	•••••••••
Ping Server	[redacted]

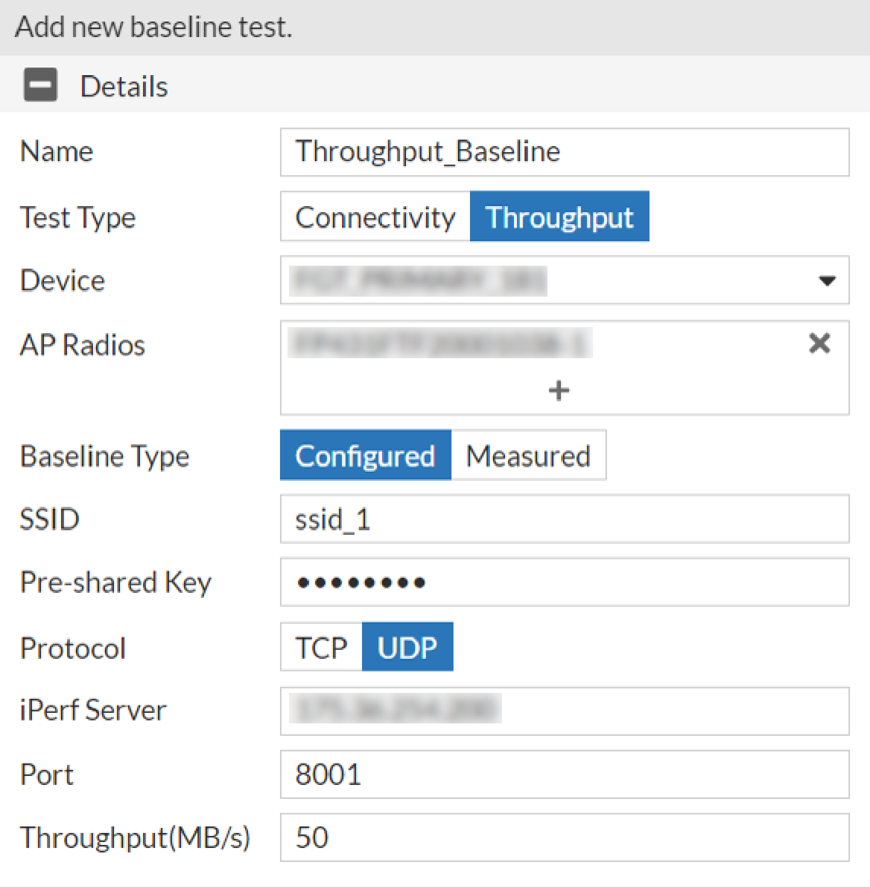
4. Click **Add.**

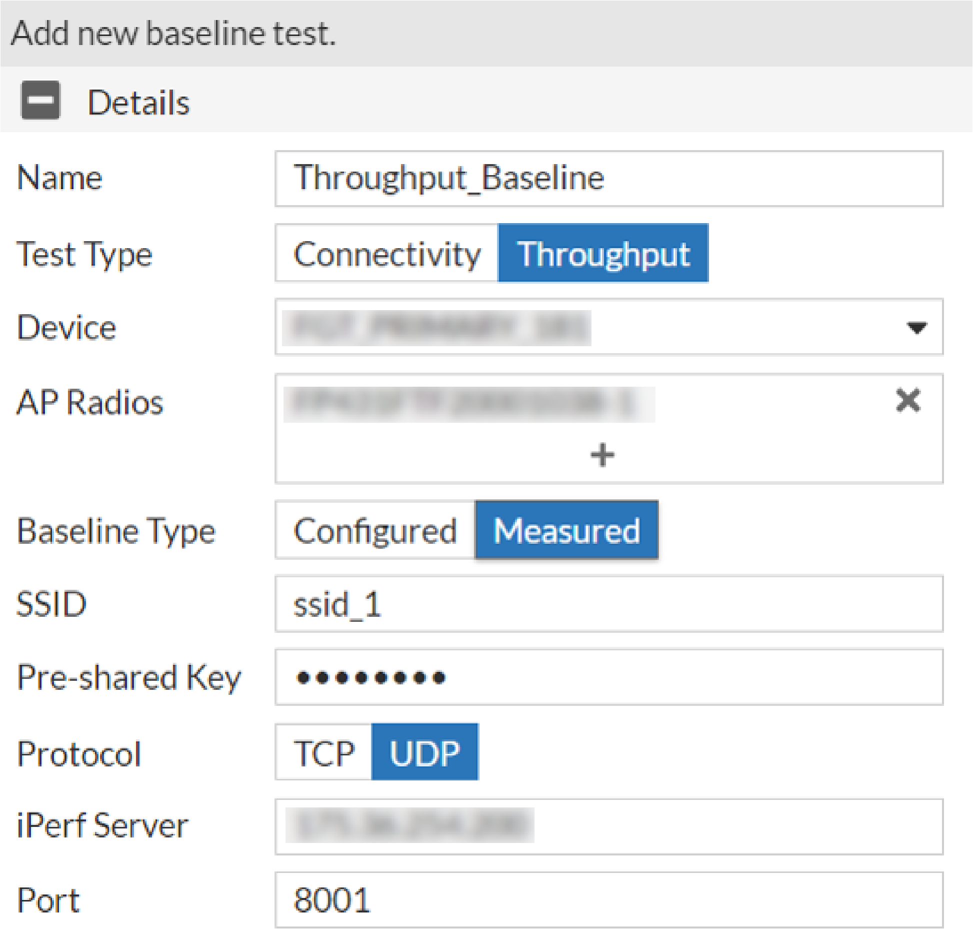
Throughput Baseline

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



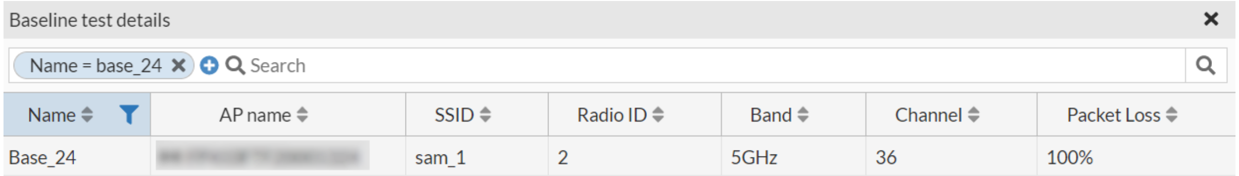
Add new baseline test.

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 Search

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.

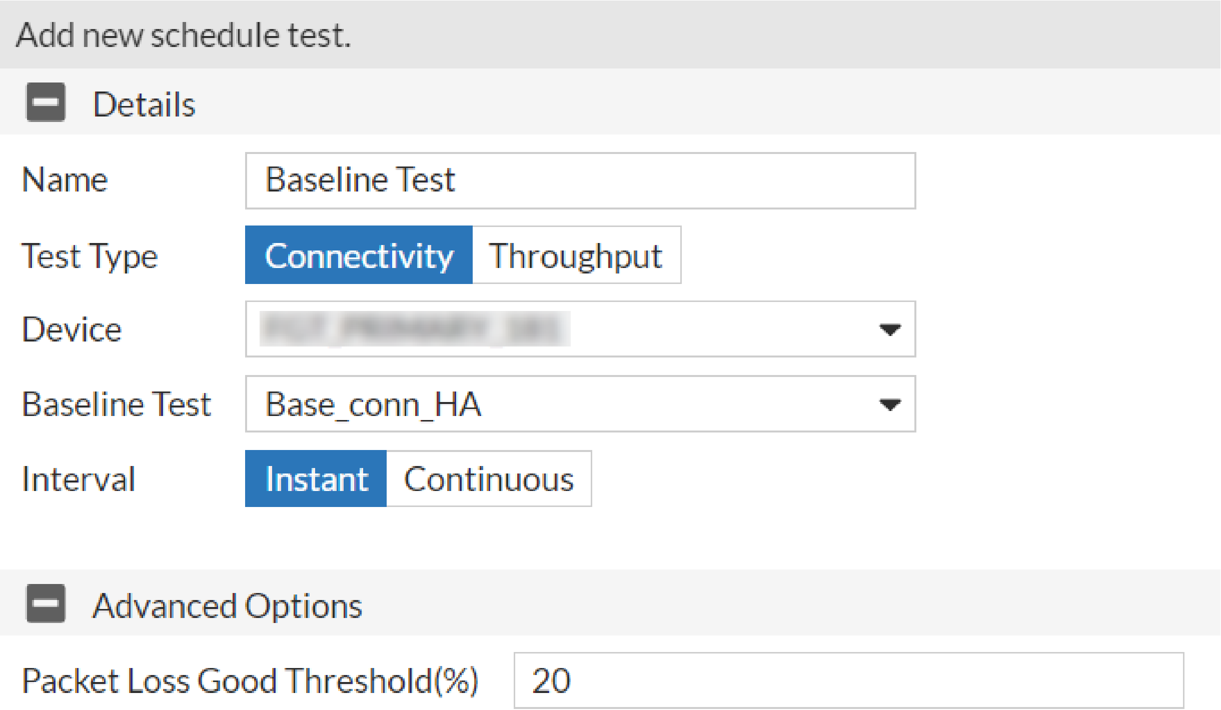
Scheduled tests are measured against a baseline test for Connectivity and Throughput using the configurations provided while creating the test. Only APs and SSIDs within the baseline test is measured in subsequent tests.

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 new schedule test.

Details

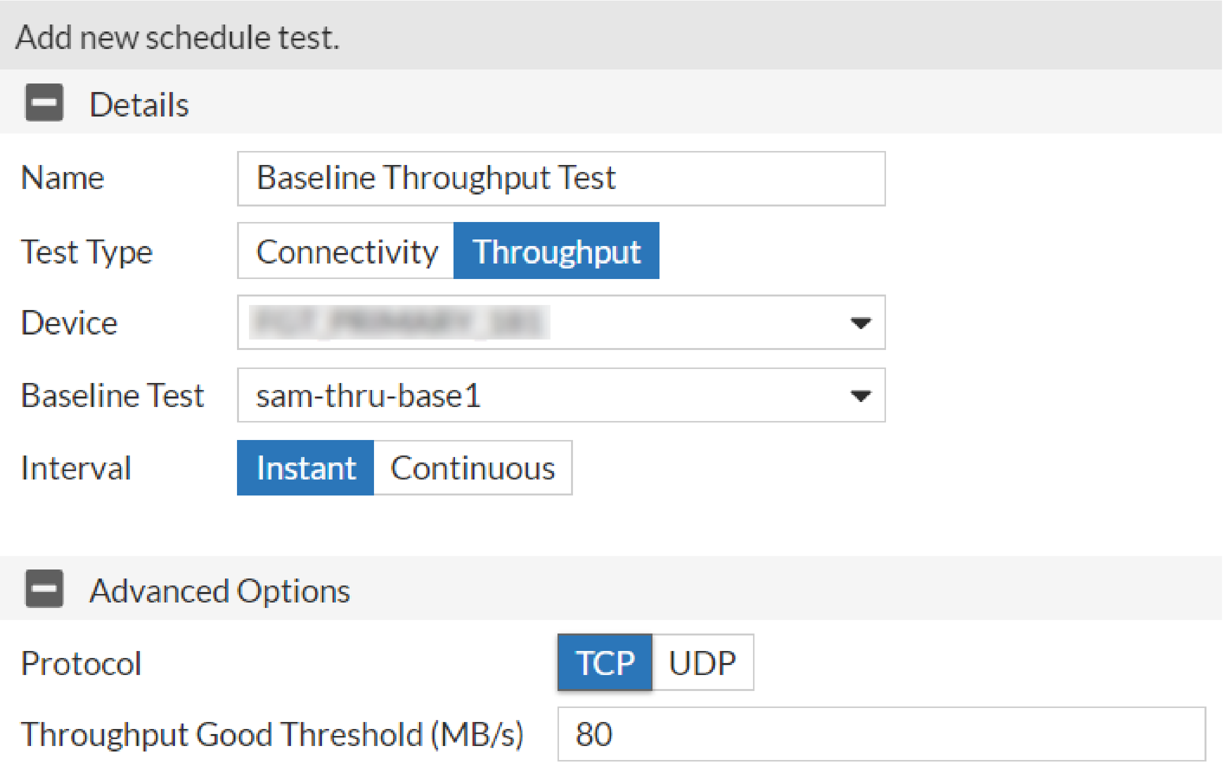
Name	Baseline Test
Test Type	[✓ Connectivity] Throughput
Device	[redacted]
Baseline Test	Base_conn_HA
Interval	[✓ Instant] Continuous

Advanced Options

Packet Loss Good Threshold(%)	20

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

Field	Description
Protocol	Select TCP or UDP.
Throughput Good Threshold (MB/s)	Type a value for the Throughput Good Threshold in MB/s. If the measured throughput is above this threshold, the test result is classified as *Good*. If it falls between the threshold and the baseline, it is considered *Fair*, while values below the threshold are categorized as *Bad*.



Add new schedule test.

Details

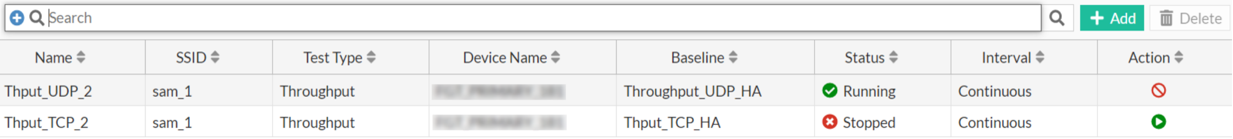
Name	Baseline Throughput Test
Test Type	Connectivity / **Throughput**
Device	[redacted]
Baseline Test	sam-thru-base1
Interval	**Instant** / Continuous

Advanced Options

Protocol	**TCP** / UDP
Throughput Good Threshold (MB/s)	80

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